Perfect Combinatorial Structures in Coding Theory and Cryptography

Vladimir N. Potapov

Contents

Preface **6**

1 Graphs and Their Colorings **8**
1.1 Graph Theory: Definitions and Notation 8
1.2 Graph Colorings 11
1.3 Perfect Colorings and Information Transmission 13
1.4 Perfect and MDS Codes in Hypercubes 14
1.5 Problems 16

2 Algebraic Properties of Perfect Colorings **17**
2.1 Stochastic and Symmetrizable Matrices 17
2.2 Matrix Equation of a Perfect Coloring 20
2.3 Theorem on the Spectral Decomposition of Adjacency Matrices 22
2.4 Perfect Colorings and Eigenfunctions 24
2.5 Orthogonality of Perfect Colorings 26
2.6 Problems 27

3 Extremal Properties of Perfect Colorings **28**
3.1 Extremal Property of Perfect 2-Colorings 28
3.2 Cuts and Independent Sets in Graphs 29
3.3 Delsarte Cliques in Transitive Graphs 33
3.4 Problems 34

4 Lattice of Perfect Colorings **35**
4.1 Merging of Colors 35
4.2 Weisfeiler–Leman Algorithm 37
4.3 Induced Colorings 39
4.4 Coverings of Graphs 40
4.5 Problems 43

5 Cartesian Products of Graphs **43**
5.1 Eigenfunctions of the Cartesian Product of Graphs 43
5.2 Perfect Colorings of Cartesian Products of Graphs 46
5.3 k-Fold Coverings and Examples 48
5.4 Relevant Variables and Wegener's Theorem 49
5.5 Problems 51

6 Amply Regular Graphs **51**
6.1 Average Degree of Vertices 51
6.2 Generalizations of Delsarte–Hoffman Bound 54

7 Distance-Regular Graphs **56**
7.1 Intersection Array and Krawtchouk Polynomial 56
7.2 Strongly Regular Graphs 60
7.3 Minimum Support of Eigenfunctions 61
7.4 Orthogonality Relations for Krawtchouk-Type Polynomials . 63
7.5 Completely Regular Codes 65
7.6 Delsarte Cliques in Distance-Regular Graphs 69
7.7 Middle Layer of Boolean Hypercube as a Testing Set 72
7.8 Problems 73

8 Automorphisms of Graphs and Perfect Colorings **75**
8.1 Orbit Colorings 75
8.2 Perfect Colorings of Cayley Graphs 76
8.3 Problems 80

9 Fourier Transform **80**
9.1 Characters of Abelian Groups 80
9.2 Krawtchouk Polynomials 86
9.3 Definition and Properties of the Fourier Transform 88
9.4 Fourier Transform and Convolution 94
9.5 Problems 96

10 Correlation Immune Functions and Orthogonal Arrays **97**
10.1 Functions Balanced on Faces 97
10.2 Correlation Immune Functions: Definition and Applications . 99
10.3 Correlation Immunity and the Fourier Transform 100
10.4 Correlation Immunity of Perfect Colorings 102
10.5 Orthogonal Arrays and Rao's Inequality 103
10.6 Total Influence of Boolean Functions 105
10.7 Bierbrauer–Friedman Inequality 107
10.8 Fon-Der-Flaass Theorem 108
10.9 Problems 109

11 Dual Code and Sarkar Identity **110**
11.1 Dual Code 110
11.2 Hadamard Code and Plotkin Bound 113

11.3 Extended 1-Perfect Code 114
11.4 Sarkar's Identity 116
11.5 Relevant Variables of Perfect Colorings 118
11.6 Testing Sets of Perfect Colorings 119
11.7 Problems 120

12 MacWilliams Identity and Weight Distributions 120
12.1 MacWilliams Transform 120
12.2 Linear Programming Bound 122
12.3 Few-Weight Codes 124
12.4 Weight Distributions of Perfect Colorings 126
12.5 Problems 128

13 Bent Functions 130
13.1 Definition and Basic Properties of Bent Functions 130
13.2 Boolean Bent Functions and Plateaued Functions 132
13.3 Nonlinearity of q-ary Functions 135
13.4 Problems 138

14 Algebraic Normal Form of Boolean Functions 139
14.1 Möbius Transformation 139
14.2 Algebraic Degree of Boolean Functions 141
14.3 Polynomial Representation of Linear Codes 145
14.4 Algebraic Degrees of Bent and Plateaued Functions 146
14.5 Algebraic Immunity 148
14.6 Problems 151

15 Perfect Colorings of Multigraphs and Hypergraphs 152
15.1 Perfect Colorings of Hypergraphs 152
15.2 Line Graphs and Transversals 155
15.3 Problems 156

16 Latin Squares and 1-Factorizations of Graphs 157
16.1 Latin Squares 157
16.2 Theorems of Vizing and Ryser 158
16.3 Theorems of Hall, Kőnig and Egerváry 161
16.4 Perfect Matchings 163
16.5 Permanents and Doubly Stochastic Matrices 164
16.6 Symmetric Latin Squares 169
16.7 Problems 171

17 MDS Codes **171**
17.1 Basic Properties of MDS Codes . . . 171
17.2 n-ary Quasigroups . . . 173
17.3 Orthogonal Systems of Quasigroups . . . 175
17.4 Systems of mutually orthogonal Latin squares . . . 178
17.5 Transversals of Latin Hypercubes . . . 183
17.6 Linear MDS Codes . . . 184
17.7 Applications of MDS Codes . . . 186
17.8 Problems . . . 187

18 Combinatorial t-Designs **188**
18.1 Designs as Perfect Colorings of Graphs and Hypergraphs . . . 188
18.2 Steiner Systems . . . 191
18.3 Symmetric Designs and Projective Planes . . . 195
18.4 Hadamard Matrices . . . 197
18.5 Problems . . . 200

19 Perfect Codes and Tilings **200**
19.1 Tilings of Groups . . . 200
19.2 Tilings of Graphs and the Code-Anticode bound . . . 202
19.3 Perfect Codes with Minimum Distance Greater Than 3 . . . 203
19.4 Perfect Codes in Hamming Graphs . . . 206
19.5 Problems . . . 210

20 Difference Sets and Other Combinatorial Configurations **211**
20.1 Difference Sets . . . 211
20.2 Difference Sets and Strongly Regular Graphs as Perfect Colorings . . . 214
20.3 Association Schemes . . . 216
20.4 Bent Functions as Perfect Colorings . . . 217
20.5 Spreads . . . 221
20.6 Problems . . . 223

References **225**

Preface

This book develops algebraic and combinatorial methods for studying discrete structures. It brings together graph theory, Boolean functions, Fourier analysis on finite groups, coding theory, perfect colorings and perfect codes, association schemes, Latin squares, and related topics. A central theme is the interaction between different representations of the same object: combinatorial, algebraic, spectral, and coding-theoretic. The main mathematical object studied in this book is a perfect coloring of a graph, or, equivalently, an equitable partition of a graph.

The book is intended for advanced undergraduate and graduate students in mathematics and computer science, as well as for researchers in discrete mathematics, combinatorics, coding theory, and related fields.

Prerequisites

The reader is expected to have a basic knowledge of linear algebra. Some familiarity with graph theory, coding theory, and algebra will be useful for understanding the more advanced topics.

Methods and References

The book is based primarily on methods from algebraic graph theory and Fourier analysis on finite abelian groups. For an introduction to algebraic graph theory, I recommend Godsil's monograph [52]. For Fourier analysis and other methods in the theory of Boolean functions, I recommend Carlet's monograph [29]. I also recommend the classical books on coding theory by van Lint [92], MacWilliams and Sloane [99], and Delsarte [36]. A more detailed and rigorous treatment of a substantial part of the material presented in this handbook can be found in [82].

Acknowledgments

The author is grateful to Sergey Avgustinovich, who inspired me to study perfect combinatorial structures; Denis Krotov, whose important results form a substantial basis for this book; Anna Taranenko, who carefully read previous versions of the text and provided many useful comments; and Ev Sotnikova, who prepared the notes of my lectures.

I am also grateful to all participants of the weekly Friday meetings at the Sobolev Institute of Mathematics: Evgeny Bespalov, Sergey Malyugin, Ivan Mogilnykh, Alexey Perezhogin, Yuriy Tarannikov, Alexandr Valyuzhenich, Anastasia Vasil'eva, and Konstantin Vorob'ev. Their results and comments have been valuable in preparing this book.

The English translation of the book was prepared using Google Translate, DeepSeek and ChatGPT.

Notation

Throughout the handbook, we use the following notation.

$\mathbb{R}$ and $\mathbb{C}$ denote the fields of real and complex numbers, respectively.

$GF(q)$ denotes the Galois field of order q, where q is a prime power.

$\mathbb{Z}_q$ denotes the ring of integers modulo q and, when appropriate, its additive group.

$Q_q^n = \{0, 1, \ldots, q-1\}^n$ denotes the q-ary hypercube. This set may be equipped with the Hamming metric, in which case Q_q^n is the Hamming graph $H(n, q)$, or with the structure of a vector space over $GF(q)$, or with the structure of the abelian group $\mathbb{Z}_q^n$.

G usually denotes a graph with adjacency matrix M.

S denotes the quotient matrix of a perfect coloring or equitable partition.

$\widehat{f}$ denotes the Fourier transform of f, normalized to be an isometry.

Open problems

Below is a list of well-known open problems related to the subject of the book.

- Existence of 1-perfect codes for non prime power alphabets p. 15
- Asymptotic number of 1-perfect binary codes p. 15
- Number of iterations of the Weisfeiler–Leman algorithm p. 38
- Fourier Entropy – Influence conjecture p. 107
- Description of the vertices of the generalized Birkhoff polytope p. 174
- Existence of 3 mutually orthogonal Latin squares of order 10 p. 181
- Existence of projective geometries for non prime power orders p. 182
- Ryser – Wanless conjecture on the existence of transversals p. 184
- Unrestricted main MDS conjecture p. 186
- Existence of Hadamard matrices for all orders divisible by 4 p. 200

1 Graphs and Their Colorings

1.1 Graph Theory: Definitions and Notation

Consider an undirected *graph* G without multiple edges or loops (a loop is an edge with the same vertex as both its beginning and end). Such graphs are called *simple*. Throughout this text, whenever we use the term "graph", we mean a simple graph, unless explicitly stated otherwise. $V(G)$ denotes the set of *vertices* of the graph G, and $E(G) \subset \binom{V(G)}{2}$ denotes the set of *edges* of the graph $G = (V(G), E(G))$. Here and throughout, $\binom{A}{k}$ denotes the set of unordered k-element subsets of A.

A graph is called *connected* if any two of its vertices are connected by a *path* of edges. A connected graph corresponds to a discrete metric space $X(V(G), d(G))$. The points of $X(V(G), d(G))$ are the vertices of the graph, and the *distance* $d(G)$ between two points is the number of edges in the shortest path connecting them. The maximum distance between vertices of a graph is called the *diameter* of the graph.

Example 1.1. Consider a set $Q_q = \{0, 1, \ldots, q-1\}$. Two n-tuples $x, y \in Q_q^n$ are connected by an edge if x and y differ in only one position. This graph is called the *Hamming graph* and denoted by $H(n, q)$. The distance $d(x, y)$ in the corresponding metric space (Q_q^n, d) is called the *Hamming distance*. $d(x, y)$ is equal to the number of positions at which n-tuples $x, y \in Q_q^n$ differ. The metric space (Q_q^n, d) and the corresponding graph are also called an *n-dimensional q-ary hypercube*; if $q = 2$, then it is a *Boolean n-cube*.

A *spanning subgraph* of G is a subgraph that contains every vertex of G but only a subset of the edges. An *induced subgraph* of G by $C \subset V(G)$ is another graph, formed from C and all of the edges, from G, connecting pairs of vertices in C.

A *clique* in a graph is an induced subgraph all of whose vertices are pairwise connected by edges. A one-dimensional q-ary cube is a clique on q vertices. In graph theory, a clique on q vertices has the standard notation K_q. However, for convenience, we will henceforth use the notations Q_q and Q_q^n in the multidimensional case, both for the metric space and for the corresponding graph, as well as for the set of its vertices.

The *degree* of a graph vertex is the number of edges incident to it. In a simple graph, the degree of a vertex is equal to the number of adjacent vertices.

A graph is called *regular* if the degrees of all its vertices are equal. If the degrees of all vertices in a graph are r, then the graph is called *r-regular*.

Let's arbitrarily enumerate the vertices of the graph: $V(G) = \{v_i\}$.

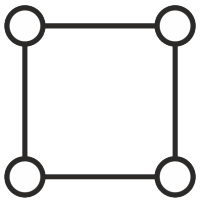
The adjacency matrix of a graph is defined by the equality

$$M_{n\times n}(G) = (m_{ij}) = \begin{cases} 1, \text{ if}(v_i, v_j) \in E(G); \\ 0, \text{ otherwise.} \end{cases}$$

An undirected graph without multiple edges has a symmetric $(0,1)$-adjacency matrix. If G is a regular graph, then each row and each column of the adjacency matrix contains the same number of ones, equal to the degree of the graph.

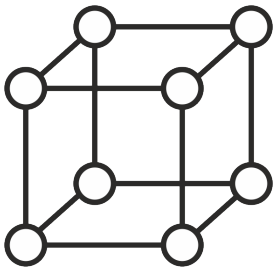
The complement of a graph G is the graph $\overline{G}$ with the same vertex set $V(\overline{G}) = V(G)$ and an edge set $E(\overline{G}) = \binom{V(G)}{2} \setminus E(G)$. The adjacency matrix of $\overline{G}$ satisfies the equality $\overline{M} = J - I - M$. Here and throughout, I is the identity matrix and J is a matrix all of whose elements are equal to 1. We will also use notations I_n and J_n for matrices of size $n \times n$.

Example 1.2. The simplest graph Q_2 consists of one edge. A cycle on four vertices, also known as the Boolean 2-cube, has the following adjacency matrix:



$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Example 1.3. The adjacency matrix of a Boolean cube Q_2^3 with eight vertices is given below.



$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

The vertices of these Boolean cubes are numbered lexicographically.

A graph G is called *k-partite* if its vertices can be divided into k parts such that no two vertices in the same part are adjacent, i.e., there are no edges connecting two vertices in the same part. If we number the vertices of the graph so that each part is numbered consecutively, then the adjacency matrix

of a k-partite graph will contain zero square submatrices on the diagonal. For example, the adjacency matrix of a bipartite graph with this vertex numbering has the form $M = \begin{pmatrix} O & B \\ B^T & O \end{pmatrix}$, where O is a matrix of all zeros, and B is the adjacency matrix of the bipartite subgraph between two parts. For every n the Boolean n-cube Q_2^n is a bipartite graph. In particular, after renumbering the vertices, the adjacency matrix of a 2-dimensional Boolean cube takes the form $\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$. A bipartite graph in which the degree of a vertex depends only on the part of the graph is called *biregular*.

Two graphs are called *isomorphic* if it is possible to establish a one-to-one correspondence between their vertices such that adjacency is preserved. Note that graphs are isomorphic if and only if their adjacency matrices map to each other by a synchronous permutation of rows and columns.

The set of vertices of a hypercube Q_q^n that have a fixed value of one coordinate, for example $x_n = 0$, is called a *hyperface* or axis-aligned *hyperplane*. The subgraph of the hypercube induced by the vertices of a hyperface is isomorphic to a hypercube of one lower dimension, i.e., Q_q^{n-1}. By fixing m coordinates, we obtain an $(n-m)$-dimensional *face* that corresponds to the subgraph isomorphic to Q_q^{n-m}. Here and below, we mean the induced subgraph, i.e., a subset of the graph's vertices with edges incident only to these vertices.

For brevity, we will call an arbitrary subset of the graph's vertices a *code*. This name stems from the fact that the main application of the theory of perfect combinatorial structures presented below is coding theory.

An *automorphism* of a graph G is a permutation of its vertices $\pi : V(G) \to V(G)$ such that edges map to edges, i.e.,

$$\{u, v\} \in E(G) \Leftrightarrow \{\pi(u), \pi(v)\} \in E(G).$$

The set of automorphisms of a graph is a group with respect to composition and it is denoted $Aut(G)$. Automorphisms of the code $C \subset V(G)$ are automorphisms $\pi \in Aut(G)$ of the graph G that preserve the code, i.e., $\pi(C) = C$.

Example 1.4. Automorphisms of a Boolean n-cube are permutations of coordinates, additions of arbitrary binary vectors modulo 2 and all their compositions.

By definition, a permutation of $V(G)$ is an automorphism if it preserves the distance 1, and therefore all other distances in the discrete metric space $X(V(G), d(G))$ corresponding to G. Thus, the set of automorphisms of a graph coincides with the set of isometries of this space. So, graph automorphisms, especially those of a hypercube, are often called isometries, and isomorphic subsets of graph vertices are called *equivalent* (or *isometric*) codes.

A graph G is called *vertex-transitive* if, for any two graph vertices $v, v' \in V(G)$, there exists $\pi \in Aut(G)$ such that $v' = \pi(v)$. A code $C \subset V(G)$ is called vertex-transitive if, for any two vertices of the code, there exists an automorphism of the code mapping one vertex to the other. A vertex-transitive graph G is called *arc-transitive* if for any two edges of the graph $e, e' \in E(G)$, there exists $\pi \in Aut(G)$ such that $e' = \pi(e)$, where $e = \{u, v\}$ and $\pi(e) = \{\pi(u), \pi(v)\}$. Each n-dimensional q-ary hypercube is an example of an edge-transitive graph. Their automorphism groups are discussed in the section 8.2.

1.2 Graph Colorings

Let $\{1, \ldots, k\}$ be a set of k colors. A *coloring* or *k-coloring* of vertices of a graph G is a mapping $f : V(G) \to \{1, \ldots, k\}$. We will use other color sets if it is convenient. In graph theory, one considers not only vertices but also edges coloring. Further, we always mean a vertex coloring, unless explicitly stated otherwise. $f^{-1}(i)$ is the set of vertices of the ith color. $P(f) = \{f^{-1}(i) : i = 1, \ldots, k\}$ is a *partition* of $V(G)$. Two colorings f and g of G are *equivalent* if there exists an automorphism $\pi \in Aut(G)$ such that $P(f) = P(g \circ \pi)$.

For each vertex $x \in V(G)$, the neighborhood of a vertex (the unit sphere centered at the vertex) is defined as follows:

$$A_1(x) = \{y \in V(G) \mid \{x, y\} \in E(G)\},$$

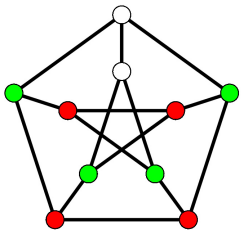
i.e., $A_1(x)$ consists of the vertices adjacent to x. A unit sphere together with its center is called a unit ball: $B_1(x) = A_1(x) \cup \{x\}$. Let $f(x) = i$, and denote $s_{ij}(x) = |A_1(x) \cap f^{-1}(j)|$.

A coloring is called *perfect* if the value $s_{ij}(x) = s_{ij}$ does not depend on the choice of vertex x and color i.

Partitions corresponding to perfect colorings are called *equitable*.

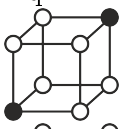
The matrix $S_{k \times k} = (s_{ij})$ is called the *quotient matrix* of the perfect coloring.

Example 1.5. A perfect coloring of the Petersen graph. We order the colors in the following way: white, green, and red.

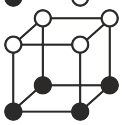


$$S = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 1 \end{pmatrix}$$

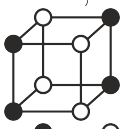
Example 1.6. All nonequivalent perfect 2-colorings of the Boolean 3-cube and their quotient matrices. The first color is black, the second is white.



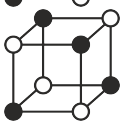
$$S = \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}$$



$$S = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$



$$S = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$



$$S = \begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix}$$

Proposition 1.1. *Every coloring of the complete graph is perfect.*

Proof. Consider two vertices x and y of the same color. Their neighborhoods coincide, except for the vertices y and x, respectively. But x and y have the same color. □

As is often the case with useful and easily defined mathematical objects, concepts equivalent to a perfect graph coloring were independently introduced in various fields of discrete mathematics. In particular, the term "equitable partition" is used in the paper by Godsil, Koolen, and their students [51], [101]. The equivalent term "partition design" was introduced in the paper by Delsarte et al. [23] and has been used by specialists in the field of combinatorial design. This refers to the theory of group designs, where groups are sets of vertices of the same color, and blocks are unit spheres. An equivalent term for a perfect coloring, "distributive coloring", was also used by Vizing [154].

The term "intriguing set" [73] is used in the field of finite geometry to denote the set of vertices of the same color in a two-color perfect coloring. The term "extremal graphical design" [58] is used in the field of extremal graph problems. The term "(c_0, c_1)-regular function" is used by specialists in Boolean functions to refer to perfect 2-colorings of the Boolean hypercube [142]. The term "perfect coloring" was introduced by Avgustinovich. This term was first used in a paper by his student Puzynina [121]. The epithet "perfect" arose because the set of vertices of the first color in a coloring

with the quotient matrix $\begin{pmatrix} 0 & r \\ 1 & r-1 \end{pmatrix}$ turns out to be a perfect code in the graph (see the next section).

Combinatorial configurations that can be described as perfect colorings in some graph, multigraph, or hypergraph are considered as *perfect combinatorial structures*.

Another, more widely studied, type of graph coloring is proper coloring. A coloring is called *proper* if no vertex has neighbors of the same color as itself. Obviously, each perfect coloring whose quotient matrix has zeros on the main diagonal is proper. Most proper colorings are quite chaotic. Unlike perfect colorings, proper colorings do not have to have a homogeneous local structure.

1.3 Perfect Colorings and Information Transmission

Perfect colorings often arise as a solution to some extremal problem, i.e., as a result of optimizing mappings with respect to some parameters. Several such problems, arising in coding theory and cryptography, will be considered below. Here, we will consider two simple examples related to data transmission over noisy communication channels.

Consider the following model of data transmission. We encode all possible messages by the vertices of a graph G. Let us connect two vertices $u, v \in V(G)$ by an edge in G if the noisy communication channel can transform message u into message v. A communication channel is called symmetric if the probabilities of errors transforming u into v and v into u are equal. Such a communication channel corresponds to a simple graph G. A subset of the graph's vertices is called a 1-*error-correcting code* if balls of radius 1 centered at the code vertices do not intersect. If we transmit only those messages that correspond to the vertices of the code, then we can fix any error in the received message. The greater the cardinality of the code, the more information can be transmitted over the communication channel per unit time. Let all balls of radius 1 in the graph G have the same cardinality $r+1$, i.e., the graph G is r-regular. Then the inequality $(r+1)|C| \le |V(G)|$ holds, where $|C|$ is the cardinality of a 1-error-correcting code C. This inequality is called the *Hamming bound*. It is easy to see that a code has maximum cardinality when the graph is completely partitioned into balls of radius 1 centered at the code vertices. This means that a coloring in which the code vertices have one color and non-code vertices have another color is perfect with the quotient matrix $\begin{pmatrix} 0 & r \\ 1 & r-1 \end{pmatrix}$. Here the set of vertices of the

first color is called a 1-*perfect* code. The theory of error-correcting codes is described in [44], [99], [92], and [133].

Next we suppose that it is sufficient to know whether an error occurred in the received message. For example, we assume that we can request a retransmission of a corrupted message. A subset of graph vertices is called *independent* if it does not contain adjacent vertices. If only messages corresponding to some independent set are transmitted over a communication channel, then all erroneous messages are detected.

In an r-regular graph, an independent set cannot contain more than half of the vertices because any edge contains one vertex of the independent set at most. If a graph contains an independent set containing exactly half of the vertices, then the other half of the vertices is also an independent set. So, the coloring of the two parts of the graph in different colors is perfect with the quotient matrix $\begin{pmatrix} 0 & r \\ r & 0 \end{pmatrix}$. Moreover, the graph is bipartite by the definition. In Section 3.2, we will obtain an upper bound for the cardinality of an independent set for regular non-bipartite graphs and will show that when this bound is reached, the independent set also turns out to be a perfect coloring.

In Example 1.6, the first coloring of the Boolean 3-cube corresponds to a perfect code, and the last one corresponds to a partition of the 3-cube into independent sets.

1.4 Perfect and MDS Codes in Hypercubes

A subset of Q_q^n is called a code with distance d if the Hamming distance between any two distinct vertices of the code is at least d. Let $q = p^k$ be a power of a prime p. Then, on the set Q_q, we can define the structure of a Galois field $GF(q)$, and the set Q_q^n can be viewed as an n-dimensional vector space over $GF(q)$. Linear subspaces of Q_q^n are called q-ary *linear codes*.

Consider an arbitrary matrix A of size $m \times n$ with elements from Q_q and the solution set of the system of equations $Ax = \bar{0}$ over the field $GF(q)$.

Proposition 1.2 ([62],[63]). *If matrix A does not contain collinear or zero columns, then the set $C = \{x \in Q_q^n \mid Ax = \bar{0}\}$ does not contain distinct vectors with Hamming distance less than* 3.

Proof. Suppose that $Ax = Ay = 0$. Then $A(x-y) = 0$. Vector $(x-y)$ defines a nontrivial linear combination of the columns of A. Since the matrix has no collinear columns, vector $(x - y)$ has at least three nonzero coordinates. Therefore, $d(x, y) \geq 3$. □

Proposition 1.3 ([57],[62]). *If $n = \frac{q^t-1}{q-1}$ and q is a prime power, then the hypercube Q_q^n has a 1-perfect code C, i.e., there exists a perfect coloring $\mathbf{1}_C$ with quotient matrix* $\begin{pmatrix} 0 & n(q-1) \\ 1 & n(q-1)-1 \end{pmatrix}$.

Proof. Consider a subset $\mathcal{A} \subset Q_q^t$ consisting of all possible vectors whose first nonzero coordinate is equal to 1. It is clear that the set $\{ax \mid a \in GF(q) \setminus \{0\}, x \in \mathcal{A}\}$ consists of all nonzero vectors from Q_q^t, and each vector is represented uniquely. Then $|\mathcal{A}| = \frac{|Q_q^t|-1}{q-1} = n$ and no two vectors from $\mathcal{A}$ are collinear. Let A be a matrix whose columns are vectors from $\mathcal{A}$. By Proposition 1.2, $C = \{x \in Q_q^n \mid Ax = \bar{0}\}$ is a code with a distance of at least 3.

The matrix A contains an identity submatrix of order t, so it has rank exactly t. Therefore, the code C is a linear subspace of dimension $n-t$. Then $|C| = q^{n-t}$. Each non-code vertex $x \notin C$ has at most one code vertex at distance 1, since the distance between two codewords is at least 3. Since the number of vertices in the unit ball is $n(q-1)+1 = q^t$, the number of vertices that are contained in C or adjacent to vertices in C is $q^t|C|$. From the equality $|Q_q^n| = q^t|C|$ it follows that every non-code vertex has exactly one neighbor in the code. Thus, the code C is 1-perfect. □

The matrix A is called the *parity-check matrix* of the code C. A linear 1-perfect code C defined above is called the *Hamming code*. It can be shown that all linear 1-perfect codes in a hypercube are equivalent and can be obtained from C by linear transformations.

Remark 1.1. Vasil'ev [152] constructed the first nonlinear 1-perfect codes. He proved that there are at least $2^{2^{n/2-o(n)}}$ nonequivalent binary 1-perfect codes with length $n = 2^t - 1$. There exist many different constructions of nonlinear 1-perfect codes (see [133], [44]). It is a well-known problem to find an effective (i.e., less than $2^{2^{n-o(n)}}$) asymptotic upper bound on the number of such codes.

Example 1.7. The parity-check matrix of a binary Hamming code of length $n = 7$: $A = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$.

Remark 1.2. From Proposition 2.1, it is easy to see that the condition $n = \frac{q^t-1}{q-1}$ is necessary for the existence of a 1-perfect code in the hypercube Q_q^n. For q that is not a prime power, the well-known conjecture claims that 1-perfect codes in Q_q^n, $n > 1$, do not exist.

Consider a group structure with the operation $\circ$ on the set Q_q, for example, an abelian group $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$. Define the set

$$L = \{x \in Q_q^n \mid x_1 \circ x_2 \circ \cdots \circ x_n = \varepsilon\}$$

where ε is the identity element of the group.

Proposition 1.4. *The function $\mathbf{1}_L$ is a perfect coloring with the quotient matrix* $\begin{pmatrix} 0 & n(q-1) \\ n & n(q-2) \end{pmatrix}$.

Proof. Let $x \in L$ and $d(x, y) = 1$ for some vertex $y \in Q_q^n$. Suppose $y_i \neq x_i$. Then we have $x_1 \circ \cdots \circ x_i = (x_{i+1} \circ \cdots \circ x_n)^{-1}$, and

$$y_1 \circ \cdots \circ y_{i-1} \circ y_i = x_1 \circ \cdots \circ x_{i-1} \circ y_i \neq (x_{i+1} \circ \cdots \circ x_n)^{-1}.$$

Therefore, $y \notin L$. From the definition of a group, it follows that the equality $x_1 \circ x_2 \circ \cdots \circ x_n = \varepsilon$ is equivalent to $(x_1 \circ x_2 \circ \cdots \circ x_{n-1})^{-1} = x_n$. Consequently, all coordinates of a vertex $x \in L$ except one can be chosen arbitrarily. Therefore, $|L| = q^{n-1}$. Since $|L|q = |Q_q^n|$, each clique (one-dimensional face) of Q_q^n should contain exactly one vertex from L. Each vertex of Q_q^n is contained in n cliques (one for each coordinate), therefore, any non-code vertex has exactly n neighbors in L. □

As will be shown below, the first color of the coloring from Proposition 1.4 is a maximal independent set in Q_q^n. More precisely, it will be proved that the minimum eigenvalue of the adjacency matrix of Q_q^n is $-n$, so the cardinality of the set of vertices of the first color reaches the Delsarte–Hoffman bound (Proposition 3.2). Such subsets of the hypercube are called MDS codes (see Section 17.1) with code distance 2.

1.5 Problems

1. Prove that the sum of the eigenvalues of the adjacency matrix of every simple graph is zero.

2. Prove that if the adjacency matrix of a bipartite graph has an eigenvalue λ, then it also has an eigenvalue $-\lambda$.

3. Prove that the adjacency matrices of a connected regular graph G and its complement have the same eigenvectors. Calculate the eigenvalues of the adjacency matrix of the complement if the eigenvalues of the adjacency matrix of G are known.

4. The Seidel matrix of a graph $G = (V, E)$ is defined by the equality

$$Z_{n\times n}(G) = \begin{cases} 1, \text{ if } & (v_i, v_j) \in E(G); \\ -1, \text{ if } & (v_i, v_j) \notin E(G); \\ 0, \text{ if } & i = j. \end{cases}$$

Prove that the Seidel matrix of a regular connected graph has the same eigenvectors as the adjacency matrix of the graph. Calculate the eigenvalues of the Seidel matrix if the eigenvalues of the adjacency matrix of the graph are known.

5. Prove that a perfect coloring of a graph is a perfect coloring of its complement.

6. Prove that a coloring of a regular graph G is perfect if the subgraphs induced by vertices of any two different colors are biregular bipartite and the subgraphs induced by vertices of any one color are regular.

7. Prove that any linear set (code) in Q_q^n (over the field $GF(q)$) can be defined by a parity-check matrix A. Find a necessary and sufficient condition on the columns of A that ensures that the code has distance d.

8. A subset S of a Boolean n-cube is called a Sidon set if all pairwise sums of elements of S are distinct. Prove that a linear binary code has code distance of at least 5 if and only if the columns of its parity-check matrix, together with the all-zero vector, form a Sidon set.

2 Algebraic Properties of Perfect Colorings

2.1 Stochastic and Symmetrizable Matrices

A simple necessary condition for an integer matrix to be the quotient matrix of some perfect coloring is the symmetry of the set of positions of nonzero elements (support) of the matrix. Indeed, if a vertex of the first color has neighbors of the second color, then a vertex of the second color also should also have neighbors of the first one. However, this condition is not sufficient. In this section, we establish necessary and sufficient conditions.

A square matrix of nonnegative elements is called *stochastic* if the sums of its elements by rows (or by columns) are equal to 1.

From the definitions, it is clear that if S is the quotient matrix of a perfect coloring of an r-regular graph, then the matrix $\frac{1}{r}S$ is stochastic. Let n_i be

the number of vertices of the ith color, and

$$\sum_{i=1}^{k} n_i = n \tag{1}$$

be the number of vertices in the graph. By calculating the number of edges which are incident to vertices of colors i and j, we obtain the following relation:

$$n_i s_{ij} = n_j s_{ji}. \tag{2}$$

We obtain a simple necessary condition for the existence of perfect colorings.

Proposition 2.1. *If there is a perfect coloring of a graph on n vertices with a quotient matrix S, then the system of equations (1), (2) has nonnegative integer solutions n_i.*

Let N be a diagonal matrix of size $k \times k$, consisting of elements n_i:

$$N = \begin{pmatrix} n_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & n_k \end{pmatrix}.$$

From the equality (2), we conclude that NS is a symmetric matrix, since we can rewrite the relation (2) in matrix form:

$$S^{\mathsf{T}} N = NS.$$

Matrices S with this property are called *symmetrizable*. We always can choose a nonnegative integer matrix N if S is nonnegative and integer.

This implies that the following proposition is true.

Proposition 2.2. *The quotient matrix S is symmetrizable by a diagonal matrix, and there exists a basis consisting of its eigenvectors.*

Proof. Since $n_i > 0$, let us consider the diagonal matrix $N^{\frac{1}{2}}$. We have the equality $N^{-\frac{1}{2}} S^{\mathsf{T}} N^{\frac{1}{2}} = N^{\frac{1}{2}} S N^{-\frac{1}{2}}$. Thus, the matrix $N^{\frac{1}{2}} S N^{-\frac{1}{2}}$ is symmetric, and, consequently, there is a basis for the space $\mathbb{R}^k$ consisting of its eigenvectors. The matrix S is similar to the matrix $N^{\frac{1}{2}} S N^{-\frac{1}{2}}$, and therefore there is also a basis of its eigenvectors. □

It turns out that the symmetrizability property of a stochastic matrix S is not only necessary but also sufficient. After multiplying by a common denominator of its elements, S becomes a quotient matrix of some perfect coloring. More precisely,

Theorem 2.1 ([76], [33]). *Let the elements of an integer nonnegative symmetrizable matrix S satisfy the equalities $\sum_{j=1}^{k} s_{ij} = r$. Then there exists an r-regular graph G and its perfect coloring with quotient matrix S.*

Proof. Take i, j, $1 \le i < j \le k$. We will show that if the equality $n_i s_{ij} = n_j s_{ji}$ holds, there exists a bipartite biregular graph with parts of cardinalities n_i and n_j, and vertex degrees in the parts s_{ij} and s_{ji}. It is sufficient to construct the adjacency matrix for such a biregular graph. We need a matrix B of size $n_i \times n_j$ which provides an adjacency of the parts of the bipartite graph. Let the kth row of matrix B contain a block of ones at positions $(k-1)s_{ij} + 1$ through ks_{ij}, where both position numbers are considered modulo n_j. We fill the remaining elements of matrix B with zeros. Each row of matrix B contains exactly s_{ij} ones by construction. Furthermore, by the construction, the number of ones in the columns of matrix B differs by no more than one. When the equality (2) holds, these numbers are equal to $s_{ji} = n_i s_{ij}/n_j$.

By the condition, there exists a diagonal nonnegative matrix N such that the matrix NS is symmetric. We will assume that the elements of the matrix N are even, since multiplication by 2 preserves the equality (2). For each $i = 1, \ldots, k$, we take a set V_i of n_i vertices, where n_i is the ith diagonal element of the matrix N. For each pair i, j, $i \ne j$, we draw edges so as to obtain a bipartite biregular graph with parts V_i and V_j, and vertex degrees in parts s_{ij} and s_{ji}. This is possible, since $|V_i| s_{ij} = |V_j| s_{ji}$. For each $i = 1, \ldots, k$, we divide the vertices of the ith part into two equal parts, V_i' and V_i'', and construct a bipartite s_{ii}-regular graph. This is possible by the above construction, since the required equality $|V_i'| s_{ii} = |V_i''| s_{ii}$ holds. The desired graph has been constructed; it remains to color the vertices of V_i with the ith color for all $i = 1, \ldots, k$. □

Theorem 130 can be generalized to irregular graphs (see [33] and [86]).

We have established necessary and sufficient conditions to be a quotient matrix of a perfect coloring of some graph. But can a given graph be colored according to a given quotient matrix? This question remains unanswered in many specific cases.

Remark 2.1. Any stochastic matrix $T = (t_{ij})$ can be viewed as the transition probability matrix of a Markov chain, where t_{ij} are the conditional transition probabilities from state i to state j. Thus, a perfectly colored graph G generates a Markov chain whose states are the colors of the vertices, and the choice of the next edge to move along is equiprobable. Note

that the vector of color frequencies $q = \left(\frac{n_1}{n}, \ldots, \frac{n_k}{n}\right)$ is the vector of stationary probabilities of the states of the Markov chain, since it satisfies the equation $q^{\mathsf{T}}T = q$. However, not every discrete Markov chain can be interpreted as a random walk on an undirected colored graph. We can simulate only such chains whose trajectory probabilities are independent on the order in which the states are traversed: from right to left or from left to right. This property is equivalent to the symmetrizability of the matrix T.

2.2 Matrix Equation of a Perfect Coloring

Let $f : V(G) \to \{1, \ldots, k\}$ be a graph coloring. Consider a matrix $F = F[f]$ of size $n \times k$, in which column f_i is the characteristic function of color i:

$$f_i(x) = \begin{cases} 1 & \text{for } f(x) = i, \\ 0 & \text{for } f(x) \neq i. \end{cases} \tag{3}$$

The matrices $F[f]$ will also be called graph colorings, since they are in one-to-one correspondence with the functions $f : V(G) \to \{1, \ldots, k\}$. Note that each row of the matrix F contains exactly one 1. We will assume throughout that the function defined on the vertices of the graph is a column vector.

Proposition 2.3 (algebraic criterion of perfect coloring [101],[60],[52])**.** *Let M be the adjacency matrix of G. $F = F[f]$ is a perfect coloring of a graph G with quotient matrix S if and only if $MF = FS$.*

Proof. To prove the equality, consider the (v, j)-th elements of the matrices on the left- and right-hand sides of the equality $MF = FS$, $j = 1, \ldots, k$, $v \in V(G)$. $(MF)_{vj}$ is the number of neighbors of color j of vertex v. Now consider the right-hand side of the equality. In the vth row of F, the entry 1 is in the position corresponding to the color $f(v)$. We obtain that $(FS)_{vj}$ is the number of vertices of color j adjacent to a vertex of color $f(v)$. Thus, the right-hand side depends only on the color of vertex v. □

Note that if matrix S is a solution to the equation $MF = FS$, where M is a nonnegative integer matrix and F satisfies condition (3), then matrix S is also nonnegative and integer. Properties of arbitrary matrices F satisfying the equation $MF = FS$ were studied in [139].

Corollary 2.1 (Lloyd's Theorem [94])**.** *Let F be a perfect coloring with the quotient matrix S of a graph with adjacency matrix M. Let z be an eigenvector of S, i.e., $Sz = \lambda z$ and $z \neq \mathbf{0}$. Then Fz is an eigenvector of the adjacency matrix M with the same eigenvalue λ.*

Proof. By using Proposition 2.3 and the associativity of matrix multiplication, we obtain the following chain of equalities:

$$MFz = FSz = F\lambda z = \lambda Fz.$$

If $z \neq \mathbf{0}$ then $Fz \neq \mathbf{0}$ by the definition of F. □

Since M is a symmetric matrix, all its eigenvalues are real.

Corollary 2.2. *Every eigenvalue of a quotient matrix is real.*

Since M is a symmetric matrix, there is a basis consisting of its eigenvectors. That is, $\mathbb{R}^n = X_{\lambda_1} \oplus \ldots \oplus X_{\lambda_m}$, where X_{λ_i} is the eigenspace of M, corresponding to λ_i.

Corollary 2.3. *Any column vector of a perfect coloring F is contained in the subspace $X_{\lambda_1} \oplus \ldots \oplus X_{\lambda_{m'}}$, where λ_1, ..., $\lambda_{m'}$ are the eigenvalues of S. Moreover, all columns of F are not contained in $X_{\lambda_1} \oplus \ldots \oplus X_{\lambda_{m''}}$, where $m'' < m'$.*

Proof. By Proposition 2.2, S has a basis of eigenvectors. Therefore, the vector $e_i = (0 \ldots \underset{i}{1} \ldots 0)$ can be expanded in this basis: $e_i = \sum \alpha_j z_j$, where z_j are the eigenvectors of the matrix S. We obtain:

$$Fe_i = F \sum \alpha_j z_j = \sum \alpha_j F z_j$$

By Corollary 2.1, Fz_j is an eigenvector of the matrix M, thus, we have obtained the required expansion. Since $\{e_i\}$ is a basis, all eigenvectors of the matrix S are used in the expansions. □

Note that column vectors of a perfect coloring F are characteristic functions of the elements (cells) of the equitable partition corresponding to the coloring.

A subspace V is called *invariant* with respect to the matrix M if $MV \subseteq V$. In particular, the eigensubspaces of the matrix are invariant. A *projector* onto a linear subspace is a linear operator acting as the identity on this subspace and as zero on its complement. Consider the subspace V_F generated by the columns of the coloring matrix F. From the definition of a perfect coloring, it follows that

Proposition 2.4. *F is a perfect coloring if and only if V_F is an invariant subspace.*

Proof. F is a perfect coloring if and only if the rows of the matrix MF corresponding to vertices of the same color coincide. This means precisely that all columns of the matrix MF are linear combinations of columns of the matrix F. □

Let F be a k-coloring of a graph with adjacency matrix M. Then $N = F^{\mathsf{T}}F$ is a diagonal matrix of size $k \times k$, whose (ii)-th element is n_i, the number of vertices of color i.

Proposition 2.5. *The linear operator defined by the matrix $P = FN^{-1}F^{\mathsf{T}}$ is a projector to the subspace V_F generated by the characteristic vectors of the colors of the coloring F.*

Proof. Let f_i be the i-th column of the matrix F, i.e., the characteristic vector of the i-th color. It is easy to see that $Pf_i = f_i$ for any i, $i = 1, \ldots, k$. Since the rank of F is k, the rank of P is no greater than k. Therefore, the dimension of the image of the operator P is k, and the vectors f_i form a basis for the image. It is well-known that an operator is a projection if and only if $P^2 = P$. We have $P^2 = FN^{-1}F^{\mathsf{T}}FN^{-1}F^{\mathsf{T}} = FN^{-1}NN^{-1}F^{\mathsf{T}} = P$. □

It is easy to see that P can be defined by the formula

$$P(x,y) = \begin{cases} \frac{1}{n_i} & \text{if vertices } x \text{ and } y \text{ have color } i, \text{i.e., } F(x,i) = F(y,i) = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

Proposition 2.6. *Let G be a graph with adjacency matrix M. A coloring F of G is perfect if and only if $MP = PM$, where P is the projector corresponding onto the subspace V_F.*

Proof. 1. ($\Leftarrow$) Let us multiply the equality $MFN^{-1}F^{\mathsf{T}} = FN^{-1}F^{\mathsf{T}}M$ by the matrix F on the right. We have $MF = FN^{-1}F^{\mathsf{T}}MF$. Then, by Proposition 2.3, F is a perfect coloring of G with quotient matrix $S = N^{-1}F^{\mathsf{T}}MF$.

2. ($\Rightarrow$) Let F be a perfect coloring with quotient matrix S. Then, by Proposition 2.3, we have the equality $MF = FS$. By the definition of P, we have $PF = F$. Then $MF = PFS = PMF$. Multiplying the equality $MF = PMF$ on the left by $N^{-1}F^{\mathsf{T}}$, we obtain $MP = PMP$. Since P and M are symmetric, we have $PM = (MP)^{\mathsf{T}} = (PMP)^{\mathsf{T}} = PMP$. □

2.3 Theorem on the Spectral Decomposition of Adjacency Matrices

Let X_{λ_i} be an eigenspace of a symmetric matrix M corresponding to an eigenvalue λ_i. Consider some orthonormal basis $\{u_1^i, \ldots, u_{m_i}^i\}$ of X_{λ_i} and a

matrix U_i of size $n \times m_i$ whose columns are the vectors u_j^i, $j = 1, \ldots, m_i$. We define a matrix E_{λ_i} of size $n \times n$ by the equality $E_{\lambda_i} = U_i U_i^{\mathsf{T}}$.

Theorem 2.2 (on spectral decomposition [52]). *For any symmetric matrix M, the matrices E_{λ_i} satisfy the conditions*
(a) $E_{\lambda_i}^2 = E_{\lambda_i}$; $E_{\lambda_i} E_{\lambda_j} = 0$ *for* $i \neq j$;
(b) $\sum_i E_{\lambda_i} = I_n$; *the matrix E_{λ_i} does not depend on the choice of an orthonormal basis of the space X_{λ_i};*
(c) $M E_{\lambda_i} = \lambda_i E_{\lambda_i}$; *For any polynomial p, the following equality holds:* $p(M) = \sum_i p(\lambda_i) E_{\lambda_i}$.

Proof. (a) By the definition, $E_{\lambda_i} = U_i U_i^{\mathsf{T}}$. Since the basis is orthonormal, we have $U_i^{\mathsf{T}} U_i = I_{m_i}$. Then $E_{\lambda_i}^2 = U_i (U_i^{\mathsf{T}} U_i) U_i^{\mathsf{T}} = E_{\lambda_i}$. The eigenspaces of a symmetric matrix corresponding to different eigenvalues are orthogonal, therefore $U_i^{\mathsf{T}} U_j = 0$ for $i \neq j$. Then $E_{\lambda_i} E_{\lambda_j} = U_i (U_i^{\mathsf{T}} U_j) U_j^{\mathsf{T}} = 0$.

(b) The squares of the eigenvalues of M are the eigenvalues of M^2. From the equality $E_{\lambda_i}^2 = E_{\lambda_i}$ it follows that the eigenvalues of E_{λ_i} are either 0 or 1. The rank of E_{λ_i} is equal to the dimension of the subspace X_{λ_i}, since the rank of $I_{m_i} = U_i^{\mathsf{T}} (U_i U_i^{\mathsf{T}}) U_i$ is equal to m_i and does not exceed the rank of $E_{\lambda_i} = U_i U_i^{\mathsf{T}}$. Then the eigenvalue 1 has multiplicity m_i and $\operatorname{tr}(E_{\lambda_i}) = m_i$. Let $E = \sum_i E_{\lambda_i}$. We have $\operatorname{tr}(E) = \sum_i \operatorname{tr}(E_{\lambda_i}) = \sum_i m_i = n$. Furthermore, from item (a) it follows that $E^2 = E$ and E is symmetric, due to the symmetry of the terms. This means that all eigenvalues of E is equal to 1. Consequently, $E = I_n$. If we change the orthonormal basis in one of the eigenspaces X_{λ_i}, then in the equality $\sum_i E_{\lambda_i} = I_n$, only one term can change. However, this is impossible in the equality.

(c) $M E_{\lambda_i} = (M U_i) U_i^{\mathsf{T}} = \lambda_i U_i U_i^{\mathsf{T}} = \lambda_i E_{\lambda_i}$. Then $M^k E_{\lambda_i} = \lambda_i^k E_{\lambda_i}$ for any natural k. From item 2), we have $M^k I_n = \sum_i \lambda_i^k E_{\lambda_i}$. Then for any polynomial p, we have the equality $p(M) = \sum_i p(\lambda_i) E_{\lambda_i}$. □

Corollary 2.4. *The matrices E_λ can be represented as polynomials of M.*

Proof. From the spectral decomposition theorem, we have the equality $p(M) = \sum_i p(\lambda_i) E_{\lambda_i}$, where p is an arbitrary polynomial. Consider the polynomial $q(t) = (\prod_i (t - \lambda_i))/(t - \lambda)$. We have $q(M) = q(\lambda) E_\lambda$. □

Corollary 2.5. *The dimension of the linear space of matrices generated by powers of a symmetric matrix M is equal to the number of distinct eigenvalues of M.*

Proof. The matrices E_{λ_i} are linearly independent by item 1) and constitute a basis for this space by item 3) of the spectral decomposition theorem. □

Recall that J_n is the matrix of size $n \times n$, all elements of which are equal to 1. For the maximum eigenvalue of an r-regular connected graph, the eigenspace X_r consists of vectors collinear with the vector $\mathbf{1}$ (see Problem 12). Therefore, $E_r = \frac{1}{n} J_n$. Then J_n can be represented as polynomials in the adjacency matrix M by Corollary 2.4. We will show that this property of a regular graph is a criterion.

Theorem 2.3 (Hoffman [52]). *A graph G is regular and connected if and only if there exists a polynomial p such that $J_n = p(M)$, where M is the adjacency matrix of G.*

Proof. ($\Leftarrow$) If $J_n = p(M)$ for some polynomial p, then $Mp(M) = p(M)M$ and $MJ_n = J_n M$, which means that the graph G is regular. If G is disconnected, then there exist vertices i and j such that the element (i, j) in the matrix M^d is zero for any degree d.

($\Rightarrow$) Let G be an r-regular connected graph and $p(x) = (x - r)(x - \lambda_1) \cdots (x - \lambda_l) = (x - r)q(x)$, where $r, \lambda_1, \ldots, \lambda_l$ are all distinct eigenvalues of the matrix M. Since $p(M) = 0$, we have $Mq(M) = rq(M)$. Therefore, the columns of the matrix $q(M)$ are the eigenvectors with the maximum eigenvalue r. Since G is connected, all these columns are collinear with the vector $\mathbf{1}$. Since $q(M)$ is symmetric, all its rows are equal to its columns; hence all entries of $q(M)$ are equal. Therefore, $q(M) = cJ_n$ for some c. $\square$

2.4 Perfect Colorings and Eigenfunctions

Consider a perfect coloring of a connected r-regular graph in two colors. Let $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r-b & b \\ c & r-c \end{pmatrix}$ be the matrix of parameters of this coloring. The main parameters of the coloring are the numbers b, c, i.e., the numbers of neighboring vertices of a different color. The eigenvalues of this matrix are $\lambda_1 = r - (b + c)$ and $\lambda_2 = r$. Note that the eigenvalues of the quotient matrix of size 2×2 are integer and the adjacency matrix of the r-regular graph has the same eigenvalues.

We calculate the number of vertices of each color (n_1 and n_2, respectively) by the system of equations:
$n_1 b = n_2 c$ is the number of two-color edges and
$n_1 + n_2 = n = |V(G)|$.
From this, we obtain the equalities $n_1 = \frac{nc}{b+c} = \frac{n}{1+\frac{b}{c}}$ and $n_2 = \frac{nb}{b+c} = \frac{n}{1+\frac{c}{b}}$.

In this case, a necessary condition for the existence of a perfect graph coloring (Proposition 2.1) means the divisibility of the numbers nc and nb by $b + c$.

Let A be the set of vertices of the first color and let $\mathbf{1}$ be a vector of ones, which is an eigenvector of the matrix S with eigenvalue r. From Corollary 2.3, we obtain that $\mathbf{1}_A = f + \alpha\mathbf{1}$, where f is the eigenfunction corresponding to the number λ_1. We have $n_1 = (\mathbf{1}_A, \mathbf{1}) = \alpha(\mathbf{1}, \mathbf{1}) = \alpha n$, from which we obtain:

$$f(x) = \begin{cases} 1 - \frac{c}{b+c} & x \in A; \\ -\frac{c}{b+c} & x \notin A. \end{cases}$$

Therefore, a perfect 2-color coloring can be associated with an eigenfunction that takes only two different values. We will now show that the converse is also true. For colorings with a larger number of colors, such a correspondence arises under certain additional conditions. By Corollary 2.1 we have

Corollary 2.6. *Consider a perfect k-coloring of a regular graph G with quotient matrix S. Let $v = (v_1, \ldots, v_k)$ be an eigenvector of S, where all components of the vector v are distinct. Then the function Fv is an eigenfunction of graph G, which takes values v_i at points of color i.*

This means that Fv determines the same coloring as the initial perfect k-coloring.

Proposition 2.7. *Let f be a k-coloring of a regular graph G and let there be k linearly independent eigenfunctions of the adjacency matrix of the graph, which can be obtained as linear combinations of the characteristic functions of the colors. Then f is a perfect coloring.*

Proof. Let the eigenfunctions $(h_1, \ldots, h_k)$ be linear combinations of the characteristic functions of the colors $(f_1, \ldots, f_k)$, i.e., $(h_1, \ldots, h_k) = (f_1, \ldots, f_k)A$ or $H = FA$, where the eigenfunctions are the columns of the matrices H. A is a nonsingular matrix because the eigenfunctions $h_1, \ldots, h_k$ are linearly independent by assumption. Since $h_1, \ldots, h_k$ are eigenvectors of the adjacency matrix M of G, we have the equality $MH = H\Lambda$, where Λ is a diagonal matrix and λ_{ii} is an eigenvalue corresponding to the vector h_i. We obtain the equality $MFA = FA\Lambda$. Then, by Proposition 2.3, the coloring f is perfect with quotient matrix $A\Lambda A^{-1}$. □

Corollary 2.7 ([47])**.** *Let f take only two values on the vertices of an r-regular graph G and $f = g + c\mathbf{1}$, where g is an eigenfunction of the adjacency matrix of G with an eigenvalue distinct from r. Then f is a perfect 2-coloring.*

Proof. Let v_0 be a vertex. We define the characteristic functions of the colors $f_1(v) = 1$ if $f(v) = f(v_0)$ and $f_1(v) = 0$ if $f(v) \neq f(v_0)$; $f_2 = \mathbf{1} - f_1$. Then

the sum $f_1 + f_2 = \mathbf{1}$ is an eigenfunction with eigenvalue r and $g = f - c\mathbf{1}$ is a linear combination of f_1 and f_2. Then f is a perfect 2-coloring. □

2.5 Orthogonality of Perfect Colorings

Proposition 2.8. *Let G be a connected r-regular graph, and let g and h be perfect colorings of G, such that the sets of eigenvalues of the quotient matrices corresponding to g and h intersect only at the maximum eigenvalue r. Then, for any color i of coloring g and any color j of coloring h, the proportion of vertices of color j among the vertices of color i is the same as the proportion of vertices of color j in the entire graph.*

Proof. Denote by B the set of vertices of color i and by A the set of vertices of color j. We define the function $f = \mathbf{1}_B - \frac{|B|}{|V(G)|}\mathbf{1}$. By the construction, $(f, \mathbf{1}) = 0$. By Corollary 2.3 the function f is contained in the union of the subspaces $X_{\lambda_1} \oplus \cdots \oplus X_{\lambda_k}$, where $\lambda_1, \ldots, \lambda_k$ are eigenvalues of the coloring g without the eigenvalue r. Then $(f, \mathbf{1}_A) = 0$, since by the hypothesis $\mathbf{1}_A$ lies in a subspace that is orthogonal to the function f (see Corollary 2.3). Consequently, $(f, \mathbf{1}_A) = |B \cap A| - \frac{|B||A|}{|V(G)|} = 0$. Then $\frac{|B \cap A|}{|B|} = \frac{|A|}{|V(G)|}$. □

In probability theory, two partitions $\{A_i\}$ and $\{B_j\}$ of the event space are called independent if the events A_i and B_j are pairwise independent for any i and j, i.e., the equalities $Pr(A_iB_j) = Pr(A_i)Pr(B_j)$ hold. Thus, equitable partitions whose spectra intersect only at the maximum eigenvalue can be considered as independent partitions of the graph vertices (here $Pr(A) = |A|/|V(G)|$).

By the proof of Proposition 2.8 we see that the following statement is also true.

Proposition 2.9. *Let two sets of eigenspaces containing the characteristic functions of vertex sets A and B, respectively, intersect only in a subspace consisting of constant functions. Then $\frac{|A|}{|V(G)|} = \frac{|A \cap B|}{|B|}$.*

For hypercubes, Proposition 2.9 is a special case of the Proposition 9.10, which will be formulated and proved in Section 9.

Proposition 2.10. *Let $f, g : V(G) \to \{0, 1\}$ be perfect 2-colorings of a connected regular graph G. Suppose that the vertex sets of colors $f^{-1}(1)$ and $g^{-1}(1)$ in the coloring g are disjoint ($f^{-1}(1) \cap g^{-1}(1) = \varnothing$). Then the coloring $f + g$ is perfect.*

Proof. Since

$$\frac{|f^{-1}(1) \cap g^{-1}(1)|}{|f^{-1}(1)|} = 0$$

while

$$\frac{|g^{-1}(1)|}{|V(G)|} > 0,$$

Proposition 2.8 implies that the spectra of the two quotient matrices must have a nontrivial common eigenvalue (i.e., they do not intersect only at r). Since each quotient matrix of a perfect 2-coloring has exactly one nontrivial eigenvalue, these nontrivial eigenvalues must coincide. Therefore, the colorings f and g correspond to eigenfunctions $f_1 = f - \frac{|f^{-1}(1)|}{|V(G)|}\mathbf{1}$ and $g_1 = g - \frac{|g^{-1}(1)|}{|V(G)|}\mathbf{1}$ with the same eigenvalue. We denote $c = \frac{|f^{-1}(1)|+|g^{-1}(1)|}{|V(G)|}$. The sum $h = f_1 + g_1$ is also an eigenfunction and takes two values $1-c$ and $-c$. Therefore, by Corollary 2.7, the function h is a perfect coloring. The function $f + g = h + c\mathbf{1}$ differs from h by a constant, and therefore it is a perfect coloring with values 0 and 1. □

2.6 Problems

9. Let P be a projector corresponding to a coloring F (see Proposition 2.5). Prove that a coloring F of a graph with adjacency matrix M is perfect if and only if the equality $MF = PMF$ holds. In other words, the columns of MF are eigenvectors of the projector P.

10. Prove that for any invariant subspace of a symmetric matrix A, there exist matrices F and S such that the image $F(\mathbb{R}^k)$ is this invariant subspace and the equality $AF = FS$ holds.

11. Let M be an adjacency matrix of a regular graph and let S be a quotient matrix of a perfect coloring of this graph. Prove that the polynomial $\det(S - xI)$ divides the polynomial $\det(M - xI)$.

12. Let M be an adjacency matrix of an r-regular graph and let S be a quotient matrix of a perfect coloring of this graph. Prove that the maximal eigenvalues of the matrices M and S are equal to r and that the eigenspace X_r of the connected graph is one-dimensional.

13. We define the support of the matrix A as the matrix $\mathrm{supp}(A)$ by the equality $(\mathrm{supp}(A))_{ij} = \begin{cases} 1 & \text{for } (A)_{ij} \neq 0, \\ 0 & \text{for } (A)_{ij} = 0. \end{cases}$ Prove that any symmetric $(0,1)$-matrix is the support of some symmetrizable stochastic matrix.

14. Let d be the diameter of a graph. Prove that its adjacency matrix has at least $d+1$ distinct eigenvalues.

15. Prove that for any finite set of eigenvalues, there are only finitely many (possibly 0) connected regular graphs with such set of eigenvalues.

16. Prove that half of the vertices of any 1-perfect code in a Boolean hypercube have even weight (number of ones), and the other half have odd weight.

17. Let $v = (v_1, \dots, v_k)$ be an eigenvector of quotient matrix S of a k-perfect coloring F of a connected regular graph G, where all components of the vector v are distinct. Prove that the linear span of the columns of F coincides with the linear span of the set of vectors $f^0, f^1, \dots, f^{k-1}$, where $f = Fv$ and components of f^j are jth powers of the corresponding components of f.

18. Let G be a regular graph with adjacency matrix M. An M-invariant subspace V is closed with respect to the Hadamard (pointwise) product if and only if it is generated by the characteristic functions of the colors of a perfect coloring of G.

3 Extremal Properties of Perfect Colorings

3.1 Extremal Property of Perfect 2-Colorings

Many years ago, Avgustinovich postulated the following principle in his report. Each perfect coloring is a solution of some optimization problem and on the other hand, a tight (reached a theoretical bound) solution of any optimization problem in combinatorics is equivalent to a perfect coloring with some parameters that depend on the problem. We illustrate this principle below.

Let $f : V(G) \to \{1, 2\}$ be a coloring of graph G. Denote by $a(x)$ the number of vertices of the first color adjacent to the vertex x of the first color, and by $c(y)$ the number of vertices of the first color adjacent to a vertex y of the second color.

Proposition 3.1. *Suppose that for some coloring f of graph G and for all vertices x and y, we have $a(x) \le a$ and $c(y) \le c$. Then the proportion of vertices of the first color in an r-regular graph G is at most $\frac{c}{r-a+c}$. If this proportion is attained, then f is a perfect coloring of the graph G with quotient matrix $S = \begin{pmatrix} a & r-a \\ c & r-c \end{pmatrix}$.*

Proof. Let $n = |V(G)|$, $n_i = |f^{-1}(i)|$, and f_i be the characteristic function of the i-th color. From the assumptions on the quantities $a(x)$ and $c(y)$, we obtain the inequalities

$$(Mf_1, f_1) \leq an_1, \quad (Mf_1, \mathbf{1} - f_1) = (f_1, Mf_2) \leq cn_2 = c(n - n_1) \tag{5}$$

and $(Mf_1, \mathbf{1}) = rn_1$. Since

$$(Mf_1, \mathbf{1}) = (Mf_1, \mathbf{1} - f_1) + (Mf_1, f_1),$$

we obtain $rn_1 \leq c(n - n_1) + an_1$.

Suppose that $a(x) < a$ for at least one vertex of the first color or that $c(y) < c$ for at least one vertex of the second color. Then at least one of the inequalities (5) is strict. In this case, we obtain $rn_1 < c(n - n_1) + an_1$ that is, $\frac{n_1}{n} < \frac{c}{r+c-a}$. Consequently, if the required proportion is attained, then $a(x) = a$ for any vertices of the first color and $c(y) = c$ for any vertices of the second color. □

Corollary 3.1. *Let G be an r-regular graph and let A be some subset of its vertices. Suppose that any ball of radius 1 contains at most one vertex from A. If $\frac{|A|}{|V(G)|} \geq \frac{1}{r+1}$, then A is a perfect code.*

Proof. We assume that the vertices of A are colored the first color, and the rest are colored the second. Then, by assumption, $a = 0$ and $c = 1$. Therefore, by Proposition 3.1, the coloring is perfect with quotient matrix $\begin{pmatrix} 0 & r \\ 1 & r-1 \end{pmatrix}$. □

3.2 Cuts and Independent Sets in Graphs

Let A and B be subsets of the vertex set of a simple graph G. We denote by $e(A, B) = |\{\{a, b\} \in E(G) : a \in A, b \in B\}|$ the number of edges between A and B. Note that if $a, b \in A \cap B$, then the edge $\{a, b\}$ is counted twice in $e(A, B)$. So, $e(A, B) = (\mathbf{1}_A, M\mathbf{1}_B)$, where M is the adjacency matrix of G.

Lemma 3.1 (Expander Mixing Lemma [1], [39])**.** *Let G be an r-regular connected graph and let λ be an eigenvalue of its adjacency matrix M of maximum absolute value among all eigenvalues different from r, i.e., $|\lambda| > |\lambda'|$ for all eigenvalues λ', $\lambda' \neq \lambda$, $\lambda' \neq r$. Then, for any subsets of vertices A and B, we have*

$$|e(A, B) - \frac{r|A||B|}{|V(G)|}| \leq |\lambda| \sqrt{|A||B|(1 - |A|/|V(G)|)(1 - |B|/|V(G)|)}.$$

Moreover, if equality holds, then $\mathbf{1}_A$ *is a perfect* 2*-coloring with eigenvalue* λ *and* $B = A$ *or* $B = V(G) \setminus A$.

Proof. The characteristic functions $\mathbf{1}_A$ and $\mathbf{1}_B$ can be represented as $\mathbf{1}_A = \sum_i \alpha_i \phi_i$ and $\mathbf{1}_B = \sum_i \beta_i \phi'_i$, where ϕ_i and ϕ'_i are the normalized eigenfunctions of the matrix M corresponding to the eigenvalue λ_i. The normalized eigenfunction corresponding to the eigenvalue r is the constant $\phi_0 = \phi'_0 = \mathbf{1}/\sqrt{n}$, $n = |V(G)|$. We have $\alpha_0 = (\mathbf{1}_A, \phi_0) = |A|/\sqrt{n}$, $\beta_0 = (\mathbf{1}_B, \phi_0) = |B|/\sqrt{n}$. Then

$$(\mathbf{1}_A - \alpha_0\phi_0, M(\mathbf{1}_B - \beta_0\phi_0)) = \sum_{i\neq 0} \lambda_i \alpha_i \beta_i (\phi_i, \phi'_i). \tag{6}$$

From the Cauchy–Schwarz inequality we have

$$|\sum_{i\neq 0} \lambda_i \alpha_i \beta_i (\phi_i, \phi'_i)| \leq |\lambda| \sum_{i\neq 0} |\alpha_i \beta_i| \leq |\lambda| (\sum_{i\neq 0} \alpha_i^2)^{1/2} (\sum_{i\neq 0} \beta_i^2)^{1/2}. \tag{7}$$

On the other hand

$$(\mathbf{1}_A - \alpha_0\phi_0, M(\mathbf{1}_B - \beta_0\phi_0)) = (\mathbf{1}_A, M\mathbf{1}_B) - \beta_0(\mathbf{1}_A, M\phi_0) - (\alpha_0\phi_0, M(\mathbf{1}_B - \beta_0\phi_0))$$

$$= e(A,B) - \frac{r|A||B|}{n}, \tag{8}$$

since $(\phi_0, M(\mathbf{1}_B - \beta_0\phi_0)) = (M\phi_0, \mathbf{1}_B - \beta_0\phi_0) = (r\phi_0, \mathbf{1}_B - \beta_0\phi_0) = 0$.

From the equality $(\mathbf{1}_A, \mathbf{1}_A) = \sum_i \alpha_i^2$ it follows that $\sum\limits_{i\neq 0} \alpha_i^2 = (\mathbf{1}_A, \mathbf{1}_A) - \alpha_0^2 = |A| - |A|^2/n$. A similar inequality holds for B. Then from (6)–(8) we have

$$\left| e(A,B) - \frac{r|A||B|}{n} \right| = |(\mathbf{1}_A - \alpha_0\phi_0, M(\mathbf{1}_B - \beta_0\phi_0))| \leq$$

$$\leq |\lambda| \sqrt{(|A| - |A|^2/n)(|B| - |B|^2/n)}.$$

Equality in the Cauchy–Schwarz inequality holds only if the vector $\mathbf{1}_A - \alpha_0\phi_0$ is collinear with the vector $\mathbf{1}_B - \beta_0\phi_0$, i.e. $\alpha_i = \beta_i$ or $\alpha_i = -\beta_i$ for all $i \neq 0$. Then equality in the first inequality of (7) holds only if $\mathbf{1}_B - \beta_0\phi_0$ is an eigenfunction, with eigenvalue λ. By Corollary 2.7, we obtain that $\mathbf{1}_B$ is a perfect 2-coloring. If the vector $\mathbf{1}_A - \alpha_0\phi_0$ is codirectional with the vector $\mathbf{1}_B - \beta_0\phi_0$, then $B = A$; if it is directed oppositely, then $B = V(G) \setminus A$. $\square$

Let's consider in detail the cases where $B = V(G) \setminus A$ and $B = A$.

A *cut* of a graph G is a pair of vertex sets $A \subset V(G)$ and $B = V(G) \setminus A$, or the set of edges between them. The *cut size* is the number $e(A, B)$. In the graph theory it is considered problems of finding both minimum and maximum cuts of a graph.

This following inequalities were proved in [2] and [135] but Golubev [58] proved that equality is attained if and only if the corresponding partition is equitable.

Corollary 3.2 ([58]). *Let G be an r-regular connected graph and let $\lambda_k < \lambda_{k-1} < \cdots < \lambda_1 < \lambda_0 = r$ be the eigenvalues of its adjacency matrix M. Let $A \subset V(G)$, $B = V(G) \setminus A$. Then the following inequalities hold:*

$$\frac{(r-\lambda_1)|A||B|}{|V(G)|} \leq e(A,B) \leq \frac{(r-\lambda_k)|A||B|}{|V(G)|}.$$

Moreover, if equality holds in either inequality, then $\{A, B\}$ is an equitable partition.

Proof. The proof is similar to the proof of Lemma 3.1. In this case we have $\mathbf{1}_B = \sqrt{n}\phi_0 - \mathbf{1}_A$, therefore the equality (6) takes the form

$$(\mathbf{1}_A - \alpha_0\phi_0, M(\mathbf{1}_B - \beta_0\phi_0)) = -\sum_{i\neq 0} \lambda_i \alpha_i^2$$

and

$$-\lambda_1 \sum_{i\neq 0} \alpha_i^2 \leq -\sum_{i\neq 0} \lambda_i \alpha_i^2 \leq -\lambda_k \sum_{i\neq 0} \alpha_i^2.$$

Using equality (8), we obtain required inequality. Obviously, equality holds only if $\mathbf{1}_A - \alpha_0\phi_0$ is an eigenfunction of M with the eigenvalue λ_1 or λ_k. □

Corollary 3.2 implies

Corollary 3.3. *The size of a maximum cut of G is at most $(r-\lambda_k)|V(G)|/4$, and if equality holds, then the cut corresponds to a perfect 2-coloring associated with the minimal eigenvalue.*

Corollary 3.4 (Haemers [59]). *Let G be an r-regular connected graph and let $\lambda_k < \lambda_{k-1} < \cdots < \lambda_1 < \lambda_0 = r$ be the eigenvalues of its adjacency matrix M. Let $C \subset V(G)$, $C \neq V(G)$, and let $e(C, C)$ denote twice the number of edges induced by C. Then the following inequalities hold:*

$$\lambda_k|C| + \frac{(r-\lambda_k)|C|^2}{|V(G)|} \leq e(C,C) \leq \lambda_1|C| + \frac{(r-\lambda_1)|C|^2}{|V(G)|}.$$

Moreover, if equality holds either inequalities, then $\{C, V(G) \setminus C\}$ is an equitable partition.

Proof. We proceed similarly to the proof of Lemma 3.1. In this case, we have $\mathbf{1}_C = \mathbf{1}_B = \mathbf{1}_A$, so the equality (6) takes the form

$$(\mathbf{1}_C - \alpha_0\phi_0, M(\mathbf{1}_C - \beta_0\phi_0)) = \sum_{i\neq 0} \lambda_i \alpha_i^2$$

and

$$\lambda_k \sum_{i\neq 0} \alpha_i^2 \leq \sum_{i\neq 0} \lambda_i \alpha_i^2 \leq \lambda_1 \sum_{i\neq 0} \alpha_i^2.$$

Using the equality (8), we obtain the required inequality. Obviously, the equality holds only if $\mathbf{1}_A - \alpha_0\phi_0$ is an eigenfunction of M with eigenvalue λ_1 or λ_k. □

Recall that an independent subset of graph vertices is a subset that does not contain adjacent vertices. A subset $C \subseteq V(G)$ is called *dominating* if every vertex of G either belongs to C or is adjacent to a vertex of C. From the definition, it is clear that every inclusion-maximal independent set is dominating. It is easy to see that every color of a perfect 2-coloring of a connected graph generates a dominating set. Moreover, if a regular graph has a 1-perfect code, then it is a minimum dominating set.

Proposition 3.2 (Delsarte–Hoffman bound [67])**.** *Let G be an r-regular graph and let λ_{min} be the minimum eigenvalue of its adjacency matrix M. Then the cardinality of any independent set in G does not exceed $\frac{\lambda_{min}|V(G)|}{\lambda_{min}-r}$. An independent set attains this bound if and only if its characteristic function is a perfect coloring with quotient matrix $S = \begin{pmatrix} 0 & r \\ -\lambda_{min} & r+\lambda_{min} \end{pmatrix}$.*

Proof. Without loss of generality, we can assume that the graph G is connected, since otherwise the connected components could be considered separately. The definition of an independent set is equivalent to the equality $e(C, C) = 0$. Then, from Corollary 3.4, we have the desired inequality $\lambda_{min}|C| + \frac{(r-\lambda_{min})|C|^2}{|V(G)|} \leq 0$.

Furthermore, Corollary 3.4 asserts that the equality $\frac{|C|}{|V(G)|} = \frac{\lambda_{min}}{\lambda_{min}-r}$ holds only if $\mathbf{1}_C$ is a perfect coloring. The coefficient $a = s_{11}$ of S is equal to 0 by the definition of independent set. The entry $c = s_{21}$ of S can be determined by counting the edges joining vertices of different colors: $|C|r = c(|V(G)| - |C|)$.

Consider a perfect 2-coloring with quotient matrix $S = \begin{pmatrix} 0 & r \\ -\lambda_{min} & r+\lambda_{min} \end{pmatrix}$. Since $s_{11} = 0$, the first color of a perfect coloring with parameter matrix S is an independent set. The number of vertices in the first color is easily calculated from the relation $|C|r = -\lambda_{min}(|V(G)| - |C|)$. Thus, the cardinality of the first color class attains the Delsarte–Hoffman bound. □

Remark 3.1. Instead of the adjacency matrix M, we can consider any other nonnegative symmetric matrix M' whose row sums are all equal to r' and whose support is contained in the support of M. Under this condition, for any indicator function f, $(Mf, f) = 0$ implies that $(M'f, f) = 0$. The proof of the Delsarte–Hoffman theorem does not use the fact that M is a $(0,1)$-matrix, it uses only the nonnegativity and symmetry of M. Therefore, every independent set in G satisfies the bound, where λ'_{min} is the minimum eigenvalue of M'.

3.3 Delsarte Cliques in Transitive Graphs

Recall that a clique in a graph is a set of vertices that are pairwise adjacent. It is easy to see that a clique in a graph corresponds to an independent set in its complement, and vice versa. For an r-regular connected graph G on n vertices, it is easy to show that the minimum eigenvalue of its complement is $-\lambda_2 - 1$, where $\lambda_2 < r$ is the maximum nontrivial eigenvalue of G, and $n-r-1$ is the degree of the complement (see Problem 3). Therefore, by the Delsarte–Hoffman bound, every clique in G has cardinality at most $\frac{(\lambda_2+1)n}{\lambda_2+n-r}$. Another, usually stronger, bound can be obtained for the size of a clique in an arc-transitive graph.

Theorem 3.1 (on the Delsarte clique [52])**.** *Every clique in an arc-transitive r-regular graph G has cardinality at most $1 - \frac{r}{\lambda_{min}}$, where λ_{min} is the minimum eigenvalue of G.*

Proof. Let $u_1, \ldots, u_m$ be an orthonormal basis of the eigensubspace $X_{\lambda_{min}}$. Consider some automorphism π of G. Obviously, each automorphism of a graph maps one orthonormal basis of the eigenspace $X_{\lambda_{min}}$ to another. Let Q_π denote the corresponding orthogonal matrix of size $m \times m$.

Consider the vectors $w(x) = (u_1(x), \ldots, u_m(x))$, where $x \in V(G)$. We will claim that the scalar product $(w(x), w(y))$ is the same for every pair of adjacent vertices x and y. Indeed, consider the automorphism π of the graph G, mapping the edge $\{x, y\}$ to the edge $\{\pi(x), \pi(y)\}$. Then $(u_1(x), \ldots, u_m(x))Q_\pi = (u_1(\pi(x)), \ldots, u_m(\pi(x)))$. We have $(w(x), w(y)) =$

$(w(x)Q_\pi, w(y)Q_\pi) = (w(\pi(x)), w(\pi(y)))$. Let $(w(x), w(y)) = \beta$ for any adjacent vertices $x, y \in V(G)$. Similarly, since G is vertex-transitive, we obtain $(w(x), w(x)) = \alpha$ for every vertex $x \in V(G)$.

From the definition of eigenfunctions, we have the equality $\sum_{y \in A_1(x)} u_i(y) = \lambda_{min} u_i(x)$, i.e., $\sum_{y \in A_1(x)} w(y) = \lambda_{min} w(x)$. Taking the inner product of the previous equality with $w(x)$, we obtain the equation $r\beta = \lambda_{min}\alpha$.

Let $C \subset V(G)$ be a clique in graph G. Consider the Gram matrix W of size $|C| \times |C|$, whose elements are $(w(x), w(y))$, $x, y \in C$. As proven above,

$$W = \begin{pmatrix} \alpha & \beta & \beta & \dots & \beta \\ \beta & \alpha & \beta & \dots & \beta \\ \dots & \dots & \dots & \dots & \dots \\ \beta & \dots & \dots & \beta & \alpha \end{pmatrix}.$$

The Gram matrix is positive semidefinite, so $(W\overline{1}, \overline{1}) \geq 0$, and therefore $\alpha + (|C| - 1)\beta \geq 0$. The minimum eigenvalue λ_{min} is negative (see Problem 1). Combining this with $r\beta = \lambda_{min}\alpha$, we obtain $|C| \leq 1 - \frac{r}{\lambda_{min}}$. □

A clique of cardinality $1 - \frac{r}{\lambda_{min}}$ in an r-regular graph G is called a *Delsarte clique*.

Corollary 3.5. *Let G be an arc-transitive graph which contains Delsarte cliques and an independent set C. If C attains the Delsarte–Hoffman bound, then each Delsarte clique in G contains exactly one vertex from C, and each vertex from C belongs to the same number of Delsarte cliques.*

Proof. Since the graph is transitive, each vertex belongs to the same number of Delsarte cliques. We denote this number by s. Then the number of Delsarte cliques is equal to $s|V(G)|/(1 - \frac{r}{\lambda_{min}})$. Since C is an independent set, each Delsarte clique contains at most one vertex of C. Then $|C|s \leq s|V(G)|/(1 - \frac{r}{\lambda_{min}})$. Since C attains the Delsarte–Hoffman bound, each clique contains a vertex from C. □

3.4 Problems

19. Let G be an r-regular graph and $f : V(G) \to \mathbb{C}$. Prove the equality $((rI - M)f, f) = \sum_{\{x,y\} \in E(G)} |f(x) - f(y)|^2$.

20. Let $f : V(G) \to \{0, 1\}$ be a coloring of an r-regular graph G. An edge of G is called bichromatic if its endpoints are colored differently. Prove the inequality $(r - \lambda)|f^{-1}(1)||f^{-1}(0)| \geq m|V(G)|$, where m is the number of

bichromatic edges and λ is the minimum eigenvalue of the adjacency matrix of G. Prove that if equality is reached, then the coloring f is perfect.

21. Let G be an r-regular graph and λ be the minimum eigenvalue of its adjacency matrix M. Suppose that every vertex of A has at most $t < r$ neighbors in A. Prove that $|A| \leq \frac{(t-\lambda)|V(G)|}{r-\lambda}$. Moreover, if equality holds, then $\mathbf{1}_A$ is a perfect 2-coloring of the graph G.

22. The chromatic number $\chi(G)$ of a graph G is the minimum number of colors in its proper coloring. Prove that $\chi(G) \geq \frac{\lambda-r}{\lambda}$ for an r-regular graph G with minimum eigenvalue λ. Prove that if $\chi(G) = \frac{\lambda-r}{\lambda}$, then every proper coloring of the graph G with $\chi(G)$ colors is perfect.

23. Let G be an r-regular graph and λ be the second largest eigenvalue of its adjacency matrix M. Prove that the cardinality of any clique in G does not exceed $\frac{\lambda+1}{1-(r-\lambda)/|V(G)|}$.

4 Lattice of Perfect Colorings

4.1 Merging of Colors

For any set V, the collection of all partitions of V, ordered by refinement, is a *lattice*. The maximum element of this lattice is one-element partition $\{V\}$, and the minimum element is the partition consisting of all one-element subsets of $\{V\}$. For two partitions B and C of the same set V, the finest partition of V that is coarse than both B and C are its refinements is denoted by $B \vee C$; the coarsest partition of V that refines both B and C is denoted by $B \wedge C$. So, $\vee$ is the least upper bound and $\wedge$ is the greatest lower bound in the natural lattice of partitions. A partially ordered set containing the least upper bound (or greatest lower bound) for any pair of its elements is called a *semilattice*.

Let G be a graph. Partitions of $V(G)$ correspond to colorings of G. We will regard the elements of partitions as colors. Recall that a partition of $V(G)$ arising from a perfect coloring is called equitable. Consider a sublattice consisting of equitable partitions of $V(G)$.

Proposition 4.1. *Let C^1 and C^2 be equitable partitions of $V(G)$. Then $C^1 \vee C^2$ is an equitable partition of $V(G)$.*

Proof. Denote by F^i a matrix whose columns are indicator functions of elements of C^i, where $i = 1, 2$. Let L_i be the subspace generated by the columns of the matrix F^i. By Proposition 2.4, a partition C is equitable if and only

if the subspace generated by the indicator functions of its cells is invariant under the adjacency matrix of G. Clearly, the intersection of invariant subspaces $L_0 = L_1 \cap L_2$ is an invariant subspace. It is easy to see that a basis of L_0 consists of indicator functions of the cells of $C^1 \vee C^2$. Therefore, $C^1 \vee C^2$ is an equitable partition of $V(G)$ by Proposition 2.4. □

Corollary 4.1. *For every graph G the sublattice of equitable partitions is a semilattice.*

In the lattice of partitions, the operation of combining several cells of a partition into one is called a *merging*. By merging, we obtain a coarse partition from the original one.

Let B be a partition, $|B| = k$, and let F_B be a matrix whose columns are indicator functions of elements (colors) of B. Consider a $(0,1)$-matrix $H = (h_{ij})$ of size $k \times m$, $m < k$, which describe the merging the original k colors into m new colors: $h_{ij} = 1$ if and only if the i-th color of the original coloring is merged into the j-th color in the new coloring. The matrix H is called a *merging matrix*.

Proposition 4.2. *Applying the merging matrix H of a perfect coloring with quotient matrix S, we obtain a perfect coloring with quotient matrix S' if and only if $SH = HS'$.*

Proof. Let F be the matrix of a perfect coloring with quotient matrix S of a graph with adjacency matrix M. Then FH is the matrix of the coloring obtained by merging colors. Then, from the equality $MF = FS$ and the condition $SH = HS'$, we have the equalities $MFH = FSH = FHS'$. By the algebraic criterion of perfect coloring (Proposition 2.3) it follows that the merged coloring is perfect.

Conversely, from the equalities $MFH = FHS'$ and $MFH = FSH$, as well as the non-singularity of the matrix F, we obtain $SH = HS'$. □

The Cartesian product of perfectly colored graphs generates perfect colorings with a larger number of colors (see Proposition 5.2). Below, we consider sufficient conditions under which the number of colors of a perfect coloring can be reduced, that is, conditions under which certain colors can be merged.

Two colors i and j of a perfect coloring are said to be *equivalent* if the i-th and j-th rows in the quotient matrix of the coloring coincide, with the possible exception of the i-th and j-th coordinates in each row.

Proposition 4.3. *The equivalence relation of colors of a perfect coloring satisfies the transitivity property.*

Proof. Suppose that the first color is equivalent to the second and third colors in a perfect coloring with quotient matrix S. Then, from the definition of equivalent colors, it follows that $s_{13} = s_{23}$ and $s_{12} = s_{32}$. Let n_i be the number of vertices of color i. Then we have the relations $n_1 s_{13} = n_3 s_{31}$, $n_2 s_{21} = n_1 s_{12}$, and $n_3 s_{32} = n_2 s_{23}$ (see equality (2)). Multiplying the right and left sides of the equalities and applying the equalities $s_{13} = s_{23}$ and $s_{12} = s_{32}$, we obtain $s_{21} = s_{31}$. This means the second and third colors are equivalent. □

Proposition 4.4. *Consider an r-regular graph G. Let the coloring f' be obtained from the perfect coloring f of G by merging of a pair of equivalent colors. Then f' is a perfect coloring.*

Proof. By the definition of equivalent colors, vertices of i-th and j-th colors have the same number of neighbors of other fixed color. Therefore, it remains only to show that every vertex in the merged color class has the same number of neighbors within this class. Let S be a quotient matrix of the initial coloring. The equality $s_{ii} + s_{ij} = s_{jj} + s_{ji}$ follows from the equation $\sum_m s_{jm} = r$ for every j. □

It is easy to see that the merger of any subset of an equivalence class is again equivalent to the remaining colors of that class. Consequently, any collection of equivalent colors in a perfect coloring can be merged, and the resulting coloring is again perfect.

4.2 Weisfeiler–Leman Algorithm

There is a natural algorithm that constructs the coarsest equitable refinement of a given partition of the vertex set of a graph. Thus, for any partition of the vertex set, this algorithm produces the coarsest equitable refinement of the given partition (see Theorem 4.1). In the modern literature, this algorithm is often called the Weisfeiler–Leman (WL) algorithm (to be exact, the one-dimensional Weisfeiler–Leman algorithm) [157], although it was independently discovered many times, including earlier works, see, e.g. [110]. The algorithm is used in the software that recognizes the isomorphism of graphs, see [104].

We describe the algorithm in terms of colorings. Suppose we have a graph colored with several colors. Consider the vertices of a fixed color. Partition them into groups consisting of vertices with the same neighborhood color composition. Perform this operation simultaneously for all color classes. Color each group with its own (new) color. The recoloring process

stops if a perfect coloring is obtained, i.e., no color is divided into groups. Otherwise, we repeat the recoloring procedure. Note that no two vertices that already have different colors can be assigned the same color during the algorithm. Since at each step of the algorithm the number of colors increases, but cannot exceed the number of vertices in the graph, we will always end up with a perfect coloring in the final graph. It is possible that, in the end, all vertices receive distinct colors. Obtaining a sharp upper bound on the number of iterations of the WL algorithm remains an open problem. There are examples of graphs for which the number of steps of the WL algorithm is approximately equal to the number of vertices and many times greater than the graph diameter, even for a regular graph (if the initial coloring is not monochromatic).

Theorem 4.1 (Vizing [154]). *Let $g : V(G) \to \{1, \ldots, k\}$ be a coloring of some graph G. Let f be a perfect coloring such that every color class of g is obtained by merging color classes of f. Then the perfect coloring obtained by applying the WL algorithm to g does not split the colors of f. In other words, the partition produced by WL algorithm coarser than the partition corresponding to f.*

Proof. We will prove the theorem by induction. Assume that after the i-th step of the algorithm, every color class of the current coloring is obtained by merging color classes of f. We will show that this holds true at the $(i+1)$-th step. The induction base is valid by assumption. Consider two vertices $x_1, x_2 \in f^{-1}(j)$ of the same color in coloring f. Then they have the same neighborhood color composition in coloring f, and therefore, by the induction hypothesis, they will have the same neighborhood color composition in the current coloring as well. Then the next step of the WL algorithm colors the vertices x_1 and x_2 with the same color. □

Remark 4.1. Essentially, the WL algorithm finds an M-invariant subspace closed with respect to the Hadamard (pointwise) product, where M is the adjacency matrix. Such subspaces are equivalent to equitable partitions (see Problem 18). Initially, we have the subspace spanned by the characteristic functions of the colors of the starting coloring. Each step acts on the subspace by A and then finds the Hadamard-product closure of the resulting subspace. The algorithm stops when we get a subspace closed both under the action of M and under the Hadamard product.

The WL algorithm can be used to check whether a set A of vertices in a graph is a color of some perfect coloring or not. It suffices to apply the

algorithm to a 2-coloring, where the first color is A and the second color is the remaining vertices. If the algorithm at some step splits the vertices of the first color, then Vizing's theorem implies that the set A is not a color of any perfect coloring. Denote the perfect coloring obtained by the WL algorithm by f_A. We have

Corollary 4.2. *If A is a color class of a perfect coloring f, then f can be obtained from f_A by splitting the remaining color classes.*

Remark 4.2. Consider random r-regular graph with N vertices, where $N - r_0 \geq r \geq r_0$ for sufficiently large r_0. Then the following holds with high probability ($N \to \infty$): for every non-trivial initial partition of the vertex set of G, WL algorithm runs at most $2\mathrm{diam}(G) + 3$ steps on G and outputs an N-colouring (see [69]). This means that a random regular graph with high probability does not have an equitable partition, except those with 1 part or N parts.

4.3 Induced Colorings

Consider a bipartite graph. Suppose that one part of the graph is colored and the other part is left uncolored. The coloring obtained after one step of the WL algorithm is called an *induced coloring*.

Proposition 4.5 ([93])**.** *If a coloring of one part of a bipartite graph can be extended to a perfect coloring of the entire graph, then the induced coloring is also perfect.*

Proof. Suppose that a coloring of one part of a bipartite graph can be extended to a perfect coloring g of the entire graph. If some color i of g appears in both parts of the graph, then the vertices of color i in the two parts can be separated into distinct colors, and the resulting coloring remains perfect. Therefore, without loss of generality, we may assume that the two parts of the graph use disjoint sets of colors in the coloring g.

Consider the coloring f that coincides with g on the first part of the graph and is monochromatic on the second part. By Theorem 4.1, the colors of f in the first part are not split at any step of the WL algorithm. Hence, the color compositions of the neighborhoods of vertices in the second part do not change during the algorithm. Consequently, the WL algorithm terminates after the first step and produces the induced coloring. □

Note that an induced coloring uses disjoint sets of colors on the two parts of the graph. However, some colors belonging to different parts may still be

merged. Induced colorings can be used to reduce the search space when searching for perfect colorings of bipartite graphs.

4.4 Coverings of Graphs

The most efficient method for transferring perfect colorings from one graph to another is the covering.

Let G_1 and G_2 be regular graphs of the same degree. A *covering* $\phi : V(G_1) \to V(G_2)$ is a mapping that induces a one-to-one correspondence in each sphere. In other words, for all $x \in V(G_1)$ the restriction of ϕ to the neighborhood $A_1^1(x)$ is a bijection onto $A_1^2(\phi(x))$.

It follows immediately from the definition that the composition of two coverings is again a covering. Moreover, a composition of a covering with a perfect coloring is again a perfect coloring.

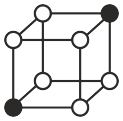
Proposition 4.6. *Let $\phi : V(G_1) \to V(G_2)$ be a covering and $f : V(G_2) \to \{1, \ldots, k\}$ be a perfect coloring of G_2. Then $f \circ \phi : V(G_1) \to \{1, \ldots, k\}$ is a perfect coloring of G_1 with the same quotient matrix.*

Proof. Let the colors of the vertices x_1, $x_2 \in V(G_1)$ be the same, i.e., $f \circ \phi(x_1) = f \circ \phi(x_2)$. Then the vertices $\phi(x_1)$ and $\phi(x_2)$ also have the same color. The neighborhood color compositions $f(A_1^2(\phi(x_1)))$ and $f(A_1^2(\phi(x_2)))$ of the vertices $\phi(x_1)$ and $\phi(x_2)$ are the same, since f is a perfect coloring. Because ϕ induces a bijection between the neighborhoods of a vertex and its image, the neighborhood color compositions of x_1 and x_2 in the coloring $f \circ \phi$ also coincide. □

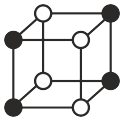
Example 4.1. Define a covering $\phi : Q_2^3 \to Q_4$ according to the rule: each pair of opposite vertices of the Boolean cube corresponds to one vertex of the complete graph Q_4.

$$\begin{aligned}
\phi^{-1}(0) &= \{(000), (111)\},\\
\phi^{-1}(1) &= \{(100), (011)\},\\
\phi^{-1}(2) &= \{(010), (101)\},\\
\phi^{-1}(3) &= \{(001), (110)\}.
\end{aligned}$$

As mentioned above (Proposition 1.1), every coloring of the complete graph is perfect. The perfect 2-colorings of the Boolean cube obtained by this covering and 2-colorings of the complete graph are in the figure below.



$$S = \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}$$



$$S = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

From the definitions it follows that a covering $\phi : V(G_1) \to V(G_2)$ can be viewed as a perfect coloring of the vertices of G_1 by vertices of G_2 considered as colors. The converse is also true. Let f be a perfect coloring of G_1 whose quotient matrix of the coloring is the adjacency matrix of G_2. Then the mapping $f : V(G_1) \to V(G_2)$ is a covering.

Since a covering can be viewed as a perfect coloring, the covering ϕ corresponds to a rectangular matrix Φ, satisfying $M_1\Phi = \Phi M_2$, where M_1 and M_2 are the adjacency matrices of graphs G_1 and G_2, respectively. Therefore, Proposition 4.6 is a special case of Proposition 4.2 on color merging. Indeed, from the equalities $M_2F = FS$ and $M_1\Phi = \Phi M_2$ it follows that $M_1\Phi F = \Phi FS$. Moreover, we obtain that the set of eigenvalues of the covered graph is a subset of the set of eigenvalues of the covering graph (see Corollary 2.1). An isomorphism between two graphs is equivalent to a one-to-one covering. In this case, the matrix Φ is a square permutation matrix, and we have the equalities $M_1\Phi = \Phi M_2$, $M_2\Phi^{-1} = \Phi^{-1}M_1$. An automorphism is an isomorphism from a graph to itself.

The examples above (perfect colorings, mergings, isomorphism and coverings) motivate us to consider the algebraic equation $M_1F = FM_2$ in its own itself. A matrix M_2 of size $k \times k$ is called a *divisor* of matrix M_1 of size $n \times n$, where $k \leq n$ if there exist a $(0,1)$-matrix F containing exactly one 1 in every row such that $M_1F = FM_2$. We define a natural partial order on the set of nonnegative integer symmetrizable matrices by setting $M_2 \leq M_1$ whenever M_2 is a divisor of M_1. By the next theorem and its generalization, this partial order forms a semilattice.

Theorem 4.2 ([4]). *For any two r-regular graphs G_1 and G_2, there exists a graph G_0 that can cover each of them.*

Proof. First, we construct a covering ϕ of G_1 by the bipartite graph G_1'. The vertex set of the bipartite graph G_1' with parts V and V' consists of twice the vertex set of G_1, i.e., $V(G_1') = V \cup V'$ and there is a mapping $\phi_1 : V \cup V' \to V(G_1)$, one-to-one on V and on V'. Vertices $u \in V$ and $u' \in V'$ of G_1' are connected by an edge if and only if the vertices $\phi_1(u)$ and $\phi_1(u')$ are adjacent in G_1. It is easy to see that the mapping ϕ_1 is a covering by construction. Similarly, we define a bipartite graph G_2' that covers G_2 and a covering ϕ_2.

Now we define a graph G_0 that covers G_1' and G_2'. By a corollary of König's theorem, which will be proved in Section 16.2, the edges of a bipartite r-regular graph can be colored with r colors such that each vertex is incident to exactly one edge of each color. We color the edges of G_1' and G_2' in this manner. Let $V(G_0) = V(G_1') \times V(G_2')$. Vertices (u_1, u_2) and (v_1, v_2) are

connected by an edge in graph G_0 if and only if vertices u_1 and v_1 in graph G'_1 are connected by an edge of the same color as vertices u_2 and v_2 in graph G'_2. By the construction, the mapping $\psi_1 : V(G_0) \to V(G'_1)$, defined by the equality $\psi_1(u_1, u_2) = u_1$, is a covering of graph G'_1. Indeed, each edge color corresponds to unique vertex v_1 adjacent to u_1 in the graph G'_1, and one vertex (v_1, v_2) adjacent to (u_1, u_2) in the graph G_0. Similarly, the mapping $\psi_2 : V(G_0) \to V(G'_2)$, defined by the equality $\psi_2(u_1, u_2) = u_2$, is a covering of the graph G'_2. The compositions $\psi_1 \circ \phi_1$ and $\psi_2 \circ \phi_2$ are coverings of the graphs G_1 and G_2, respectively, by the graph G_0. □

Theorem 4.2 can be generalized to irregular graphs. Namely, two graphs have a common covering if and only if they admit a perfect coloring with the same quotient matrix (see [86]).

Note that the vertices of the graphs G_1 and G_2 have the same degrees, but the number of vertices in the graphs can differ greatly. The graphs (or one of them) can have an infinite number of vertices. Thus, a covering of a "small" graph G_2 by a "large" graph G_1 allows us to lift a perfect coloring of G_2 to a perfect coloring of G_1 with the same quotient matrix.

From equality (2) for the parameters of a perfect coloring, it follows that the ratio of the number of vertices of two colors $\frac{n_i}{n_j}$ is equal to the ratio of the elements of the quotient matrix $\frac{s_{ji}}{s_{ij}}$ if $s_{ij} \neq 0$. In the case of a covering, the quotient is the adjacency matrix of the graph being covered, whose elements are either 0 or 1. Therefore, under the covering map $\phi : V(G_1) \to V(G_2)$, the preimages of all vertices of G_2 have the same cardinality $k = |V(G_1)|/|V(G_2)|$. Such a covering is called a *k-covering*. Note that a covering of the complete graph Q_q by a graph G is both a proper and a perfect coloring of G with q colors.

Proposition 4.7. *If there exists a covering of the complete graph Q_{q+1} by a q-regular graph G, then G contains a 1-perfect code.*

Proof. Since every coloring of a complete graph is a perfect coloring, there exists a perfect coloring of the graph Q_{q+1} with parameter matrix $S = \begin{pmatrix} 0 & q \\ 1 & q-1 \end{pmatrix}$. By Proposition 4.6, there exists a perfect coloring of the graph G with the same parameter matrix. Then the first color of this coloring is a 1-perfect code by definition. □

4.5 Problems

24. Let P be a equitable partition of a bipartite connected graph. Prove that if at least one cell of the partition is contained entirely in one part, then this is true for vertices of every color.

25. Let P be a equitable partition of a bipartite graph. Prove that if one cell $P_i \in P$ is contained in both parts of the graph then this cell can be split into two cells such that the partition remains equitable.

26. Suppose there is a coloring of the graph G with colors from the sets A and B such that merging all the colors from A into a single color while preserving all the colors from B, and conversely, merging all the colors from B into a single color while preserving all the colors from A, both result in perfect colorings. Prove that the original coloring is perfect.

27. Let $\phi : V(G_1) \to V(G_2)$ be a covering. Prove that the number of common neighbors of vertices $u, v \in V(G_1)$ is no greater than the number of common neighbors of vertices $\phi(u), \phi(v) \in V(G_2)$. Deduce that the size of a maximum clique in the covering graph is no greater than in the covered graph.

28. Suppose that G_1 covers G_2. Prove that if G_2 has a perfect matching (see Section 16.4), then the graph G_1 also has a perfect matching.

29. Prove that an infinite r-regular tree covers every r-regular graph.

30. Give an example of a graph and an initial partition whose color-indicator functions lie in an invariant subspace of the graph, but for which the equitable partition obtained by the WL algorithm lie in an invariant subspace with a new eigenvalue.

5 Cartesian Products of Graphs

5.1 Eigenfunctions of the Cartesian Product of Graphs

The *Kronecker product* of matrices A of size $n_1 \times m_1$ and B of size $n_2 \times m_2$ is a matrix $A \otimes B$ of size $n_1 n_2 \times m_1 m_2$, consisting of the elements $(A \otimes B)_{(i_1,i_2),(j_1,j_2)} = A_{i_1,j_1} B_{i_2,j_2}$. For matrices of compatible sizes, we have $(A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD)$ and $(A \otimes B) + (A \otimes D) = A \otimes (B + D)$.

The *Cartesian product* of two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is a graph $G = G_1 \square G_2$ such that $V(G) = V_1 \times V_2$, $E(G) = \Big\{ \{(v_1, v_2), (u_1, u_2)\} : (v_1 = u_1 \text{ and } \{v_2, u_2\} \in E_2) \text{ or } (v_2 = u_2 \text{ and } \{v_1, u_1\} \in E_1) \Big\}$.

Let $|V_1| = n$ and $|V_2| = m$. Then the adjacency matrix M of graph G can be expressed in terms of the Kronecker products of the adjacency matrices M_1 and M_2 of graphs G_1 and G_2 and identity matrices. With an appropriate numbering of the vertices of G, the equality $M = M_1 \otimes I_m + I_n \otimes M_2$ holds. Thus, the matrix M is obtained from M_1 by replacing each entry 1 with the block I_m, each entry 0 with the zero matrix of order m, and then adding the block-diagonal matrix with copies of M_2 on the main diagonal.

In particular, the n-dimensional q-ary cube Q_q^n is defined as the Cartesian product of cubes of lower dimension, namely $Q_q^n = Q_q^{n-1} \square Q_q$. We obtain the following recurrence representation of its adjacency matrix

$$M_n = \begin{pmatrix} M_{n-1} & I_{q^{n-1}} & \cdots & I_{q^{n-1}} \\ I_{q^{n-1}} & M_{n-1} & \cdots & I_{q^{n-1}} \\ \cdots & \cdots & \cdots & \cdots \\ I_{q^{n-1}} & I_{q^{n-1}} & \cdots & M_{n-1} \end{pmatrix}$$

The definition of the Cartesian product of graphs implies that the subgraph of $G = G_1 \square G_2$ induced by the set of vertices $V(G_1) \times \{y\}$ is isomorphic to G_1 for any vertex $y \in V(G_2)$. Similarly, the subgraph induced by $\{x\} \times V(G_2)$ is isomorphic to G_2.

From the definition of the Cartesian product of graphs, for any function $f(x, y) : V(G) \to \mathbb{C}$, we have the equality

$$Mf(x, y) = \sum_{x' \in A_1^1(x)} f(x', y) + \sum_{y' \in A_1^2(y)} f(x, y'),$$

where $A_1^1(x)$ and $A_1^2(y)$ are the unit spheres in G_1 and G_2, respectively.

Proposition 5.1. *Let $f_1, \ldots, f_n$ be an orthogonal basis of eigenfunctions of graph G_1 with eigenvalues $\alpha_1, \ldots, \alpha_n$; and $g_1, \ldots, g_m$ be an orthogonal basis of eigenfunctions of graph G_2 with eigenvalues $\beta_1, \ldots, \beta_m$. Then $\{f_i \otimes g_j\}$ is an orthogonal basis of eigenfunctions of graph $G = G_1 \square G_2$ with eigenvalues $\alpha_i + \beta_j$.*

Proof. $M(f_i \otimes g_j) = (M_1 \otimes I_m) \cdot (f_i \otimes g_j) + (I_n \otimes M_2) \cdot (f_i \otimes g_j)$
$= M_1 f_i \otimes g_j + f_i \otimes M_2 g_j = \alpha_i f_i \otimes g_j + \beta_j f_i \otimes g_j = (\alpha_i + \beta_j) f_i \otimes g_j$.

Now let's check the orthogonality of the basis. The well-known equality

$$(f_{i_1} \otimes g_{j_1}, f_{i_2} \otimes g_{j_2}) = (f_{i_1}, f_{i_2})(g_{j_1}, g_{j_2}),$$

immediately implies orthogonality. The products $f_i \otimes g_j$ form a basis, since the number of these functions is $|V(G)| = nm$. $\square$

Consider the graph Q_q, isomorphic to a clique on q vertices. A basis of eigenfunctions of Q_q is given by $\Phi_0 = (1, 1, 1, \ldots, 1)$ with eigenvalue $q-1$, and for any $i, j \in \{1, \ldots, q\}$, $i \neq j$, $\Phi_{ij} = (0, \ldots, \underset{i}{1}, 0, \ldots, 0, \underset{j}{-1}, 0, \ldots, 0)$ with eigenvalue -1. Among the listed functions, we can choose a basis for the entire space, therefore, the graph Q_q has no other eigenvalues.

Corollary 5.1. *The eigenvalues of Q_q^n are $(q-1)n-qk$, where $k = 0, \ldots, n$.*

Proof. By the definition $Q_q^n = Q_q^{n-1} \square Q_q$. The eigenvalues of Q_q are $q-1$ and -1. Suppose that we know the eigenvalues of Q_q^{n-1}. By Proposition 5.1, every eigenvalue of Q_q^n is equal to $(q-1)(n-1)-qk+q-1 = (q-1)n-qk$ or $(q-1)(n-1)-qk-1 = (q-1)n-q(k+1)$, where $k = 0, \ldots, n-1$. $\square$

Next we will show how, from the eigenfunctions of the Cartesian product of graphs and one of the factors, we can obtain the eigenfunction of the second factor.

Lemma 5.1 (contraction theorem [139])**.** *Let $G = G_1 \square G_2$; $f(x, y)$ is an eigenfunction of G with eigenvalue λ; ϕ_0 is an eigenfunction of G_2 with eigenvalue α_0. Then $c_0(x) = \sum\limits_{y \in V(G_2)} f(x, y) \cdot \phi_0(y)$ is an eigenfunction of G_1 with eigenvalue $(\lambda - \alpha_0)$.*

Proof. It is known that any vector can be included in some orthogonal basis containing this vector. Therefore, without loss of generality, we can assume that $\phi_0, \ldots, \phi_{m-1}$ form an orthonormal basis of eigenfunctions of G_2 with eigenvalues $\alpha_0, \ldots, \alpha_{m-1}$. For any fixed $x \in V(G_1)$, the function f can be expanded in the basis: $f(x, y) = \sum\limits_{i=0}^{m-1} c_i(x)\phi_i(y)$, since by fixing x we obtain a graph isomorphic to G_2. Thus we have $f = \sum\limits_{i=0}^{m-1} c_i \otimes \phi_i$ and $\sum\limits_{y \in V(G_2)} f(x, y)\phi_i(y) = c_i(x)$ due to orthonormality of the basis.

Since f is an eigenfunction of G, it holds the equality

$$(M_1 \otimes I_m + I_n \otimes M_2) \left(\sum_{i=0}^{m-1} c_i \otimes \phi_i \right) = \lambda \left(\sum_{i=0}^{m-1} c_i \otimes \phi_i \right).$$

Since ϕ_i, $i = 0, \ldots, m-1$, are eigenfunctions of G_2, we obtain a new equality

$$\sum_{i=0}^{m-1} (M_1 c_i + \alpha_i c_i) \otimes \phi_i = \sum_{i=0}^{m-1} \lambda c_i \otimes \phi_i. \tag{9}$$

It is easy to see that scalar product with one of the factors in the Cartesian product yields the following equalities:

$$g(x)(h_1,h_2)=\sum_{y\in V(G_2)} g(x)h_1(y)h_2(y)=\sum_{y\in V(G_2)}(g\otimes h_1)(x,y)\cdot h_2(y).$$

Therefore, scalar product of both sides of the equality (9) by the function ϕ_0 yields the equality $M_1c_0+\alpha_0c_0=\lambda c_0$. □

Lemma 5.1 is used for construction of eigenfunctions of hypercubes in [147]. Consider some eigenfunction f with eigenvalue λ in $Q_q^{n+1}=Q_q^n\square Q_q$. By Lemma 5.1 the sum of the f over parallel hyperfaces $g(x_1,\dots,x_n)=\sum\limits_{z\in Q_q} f(x_1,\dots,x_n,z)$ is an eigenfunction of Q_q^n with eigenvalue $\lambda-q+1$. Similarly, for two hyperfaces of the same direction, the difference $g_{ij}(x_1,\dots,x_n)=f(x_1,\dots,x_n,i)-f(x_1,\dots,x_n,j)$ is an eigenfunction of Q_q^n with eigenvalue $\lambda+1$.

5.2 Perfect Colorings of Cartesian Products of Graphs

Let us consider methods for constructing perfect colorings of Cartesian products of graphs by perfect colorings of factors.

Proposition 5.2 ([139]). *Let f_i be a perfect k_i-coloring of graph G_i with quotient matrix S_i, $i=1,2$. Then $f_1\times f_2$ is a (k_1k_2)-perfect coloring of $G=G_1\square G_2$ with quotient matrix $S=S_1\otimes I_{k_2}+I_{k_1}\otimes S_2$.*

Proof. Consider the neighborhood of the vertex (x,y). It consists of vertices (x,y'), $y'\in S_1^2(y)$ of colors $(f_1(x),f_2(y'))$ and vertices (x',y), $x'\in S_1^1(x)$ of colors $(f_1(x'),f_2(y))$. Moreover, the multisets of colors $f_2(y')$ and $f_1(x')$ depend only on the colors $f_2(y)$ and $f_1(x)$, respectively, and therefore only on the color of (x,y). Thus, $f_1\times f_2$ is a perfect coloring.

Below we calculate the quotient matrix of the resulting coloring and independently verify that this coloring is perfect. As noted earlier, the adjacency matrix of graph $G_1\square G_2$ has the form $M=M_1\otimes I_{m_2}+I_{m_1}\otimes M_2$, where M_i is the adjacency matrix of graph G_i, $m_i=|V(G_i)|$, $i=1,2$. Let F_1 be the matrix of size $m_1\times k_1$ corresponding to the perfect coloring f_1 of graph G_1, and F_2 be the matrix of size $m_2\times k_2$ corresponding to the perfect coloring f_2 of graph G_2. It is easy to see that the matrix $F_1\otimes F_2$ corresponds to the coloring $f_1\times f_2$. From Proposition 2.3, we have $M_iF_i=F_iS_i$, where $i=1,2$. Using the following equality $(A_1\otimes B_1)(A_2\otimes B_2)=(A_1A_2)\otimes(B_1B_2)$ for Kronecker products of matrices of suitable size, we obtain the equalities

$$(M_1\otimes I_{m_2}+I_{m_1}\otimes M_2)(F_1\otimes F_2)=(F_1S_1)\otimes F_2+F_1\otimes(F_2S_2)=(F_1\otimes F_2)(S_1\otimes I_{k_2}+I_{k_1}\otimes S_2).$$

Thus, the coloring $f_1 \times f_2$ is perfect by the algebraic criterion for a perfect coloring (Proposition 2.3). □

Consider the special case when f_2 is a trivial one-coloring. Let f_1 be a perfect coloring of the graph G_1 with quotient matrix S. Then $f(x,y) = f_1(x)$ is a perfect coloring of the graph $G_1 \square G_2$ with quotient matrix $S + rI$, where r is the degree of G_2.

Proposition 5.3. *Let $g : V(G) \to \{0,1\}$ be a perfect coloring of a graph G with quotient matrix $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ and $h : V(H) \to \{0,1\}$ be a perfect coloring of graph H with quotient matrix $\begin{pmatrix} c & d \\ d & c \end{pmatrix}$. Then the coloring $f(x,y) = g(x) \oplus h(y)$, where $\oplus$ is addition modulo 2, is perfect with the quotient matrix $\begin{pmatrix} a+c & b+d \\ b+d & a+c \end{pmatrix}$ in the graph $G \square H$.*

Proof. Consider the number of neighbors of color 1 of a vertex (x,y). If $g(x) = h(y) = 0$, then there are b neighbors of $(g(x'), h(y))$ and d neighbors $(g(x), h(y'))$ of color 1. If $g(x) = h(y) = 1$, then there are b neighbors of $(g(x'), h(y))$ and d neighbors of $(g(x), h(y'))$ of color 1. The remaining cases are analogous. □

Proposition 5.4. *If the mappings $\phi_i : V(G_i) \to V(H_i)$, $i = 1, 2$, are coverings, then the mapping $\bar{\phi} : V(G_1 \square G_2) \to V(H_1 \square H_2)$, where $\bar{\phi}(x,y) = (\phi_1(x), \phi_2(y))$ is also a covering.*

Proof. We have $M_i \Phi_i = \Phi_i N_i$, where the matrix Φ_i corresponds to the covering ϕ_i, M_i is the adjacency matrix of G_i, and N_i is the adjacency matrix of H_i, $i = 1, 2$. By definitions, the mapping $\bar{\phi}$ has matrix $\Phi_1 \otimes \Phi_2$. The matrix $M_1 \otimes I_{m_2} + I_{m_1} \otimes M_2$ is the adjacency matrix of the Cartesian product of graphs G_1 and G_2 with adjacency matrices M_1 and M_2, and the matrix $N_1 \otimes I_{n_2} + I_{n_1} \otimes N_2$ is the adjacency matrix of the Cartesian product of graphs H_1 and H_2 with the adjacency matrices N_1 and N_2 . Therefore we have

$$(M_1 \otimes I_{m_2} + I_{m_1} \otimes M_2)(\Phi_1 \otimes \Phi_2) = M_1\Phi_1 \otimes \Phi_2 +$$
$$+ \Phi_1 \otimes M_2\Phi_2 = (\Phi_1 \otimes \Phi_2)(N_1 \otimes I_{n_2} + I_{m_1} \otimes N_2),$$

which, by the algebraic criterion of perfect coloring (Proposition 2.3), proves that $\bar{\phi}$ is a covering. □

Example 5.1. The mapping $\bar{\phi}_n : (Q_2^3)^n \to Q_4^n$, $\bar{\phi}_n(x_1, \ldots, x_n) = (\phi(x_1), \ldots, \phi(x_n))$, where ϕ is defined in Example 4.1, is a covering.

5.3 k-Fold Coverings and Examples

Let G_1 be an mr-regular graph and G_2 an r-regular graph. An *m-fold covering* $\phi : V(G_1) \to V(G_2)$ is a mapping such that for all $x \in V(G_1)$ we have $\phi(S_1^1(x)) = S_1^2(\phi(x))$ and for all $y \in S_1^2(\phi(x))$ we have $|\phi^{-1}(y) \cap S_1^1(x)| = m$.

Proposition 5.5. *Let $\phi : V(G_1) \to V(G_2)$ be an m-fold covering and let $f : V(G_2) \to \{1, \dots, k\}$ be a perfect coloring of G_2 with quotient matrix S. Then $f \circ \phi : V(G_1) \to \{1, \dots, k\}$ is a perfect coloring of G_1 with quotient matrix mS.*

Proof. From the definition of an m-fold covering, ϕ correspond to $(0,1)$-matrix Φ such that $M_1\Phi = \Phi(mM_2)$, where M_1 and M_2 are the adjacency matrices of the graphs G_1 and G_2, respectively. By the algebraic criterion of perfect coloring (Proposition 2.3) we have $M_2F = FS$. Therefore, $M_1\Phi F = \Phi(mM_2)F = \Phi F(mS)$. □

Example 5.2. Let $pch : Q_2^k \to Q_2$ be the perfect coloring with parameter matrix $\begin{pmatrix} 0 & k \\ k & 0 \end{pmatrix}$, i.e., $pch(x) = 1$, if x contains an odd number of ones, and $pch(x) = 0$ if x contains an even number of ones. Then the mapping $p_m^k : Q_2^{km} \to Q_2^m$, defined by the equality $p_m^k(x_1, \dots, x_m) = (pch(x_1), \dots, pch(x_m))$, $x_i \in Q_2^k$, is a k-fold covering.

Example 5.3. Let $*$ be a group operation on the set Q_q. Consider the mapping $\ell : Q_q^n \to Q_q$ defined by the equality $\ell(x_1, \dots, x_n) = x_1 * x_2 * \cdots * x_n$. It is easy to show that ℓ is an n-fold covering of Q_q. Let id be a coloring of the graph Q_q with q different colors (with quotient matrix $J_q - I_q$), then quotient matrix of $id \circ \ell$ is $n(J_q - I_q) = \begin{pmatrix} 0 & n & \dots & n \\ n & 0 & \dots & n \\ \vdots & \vdots & \ddots & \vdots \\ n & \dots & \dots & 0 \end{pmatrix}$. Such a coloring is called *latin coloring*, and a hypercube with such a coloring is called *latin hypercube*.

Example 5.4. Consider a 2-coloring h of Q_q: one vertex receives the first color, the rest are colored by the second one. The coloring $h \circ \ell$, where the mapping ℓ is defined in Example 5.3, is a perfect coloring of the graph Q_q^n with quotient matrix $\begin{pmatrix} 0 & n(q-1) \\ n & n(q-2) \end{pmatrix}$. Thus, the vertices of the first color

form an MDS code (see Section 1.4, and the non-code vertices can be viewed as the union of the remaining colors of the latin coloring $h \circ \ell = h \circ (id \circ \ell)$.

Example 5.5. Consider the covering $\bar{\phi}_n : Q_2^{3n} \to Q_4^n$ from Example 5.1 and an MDS code in the hypercube Q_4^n, i.e., the coloring f with parameter matrix $S = \begin{pmatrix} 0 & 3n \\ n & 2n \end{pmatrix}$. By Proposition 4.6, it follows that $f \circ \bar{\phi}_n$ is a perfect coloring of Q_2^{3n} with quotient matrix S. A perfect 2-coloring with the same quotient matrix can also be defined as $\phi \circ p_3^n$, where the mapping p_3^n is defined in Example 5.2, and the mapping ϕ is defined in Example 4.1. Perfect colorings with this quotient matrix attains the Fon-Der-Flaass bound on correlation immunity (see Section 10.8).

Further constructions of perfect colorings of hypercubes can be found in [12].

5.4 Relevant Variables and Wegener's Theorem

Let $T_0, T_1, \ldots, T_n$ be arbitrary nonempty sets. Let $f : T_1 \times \cdots \times T_n \to T_0$ a function. A variable x_i, $1 \le i \le n$, is called *relevant* (essential, or effective) if there exist $a_j \in T_j$, $j \ne i$ and $b, c \in T_i$ such that

$$f(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n) \ne f(a_1, \ldots, a_{i-1}, c, a_{i+1}, \ldots, a_n).$$

Otherwise, the variable is said to be irrelevant. The coloring of a Cartesian product of graphs $G = G_1 \Box \cdots \Box G_n$ can be considered as a function of n variables. Thus, it is natural to consider the relevant variables of such colorings.

A coloring of a Boolean n-cube $f : Q_2^n \to \{1, \ldots, k\}$ can be viewed as a function in n Boolean variables. We denote by $\eta(f)$ the number of relevant variables of f. For each vertex $x \in Q_2^n$, let $c(x)$ denote the number of neighbors whose color differs from the color of x. Denote $c(f) = \max_x c(x)$.

Theorem 5.1 (Wegener [156])**.** *For any coloring f of a Boolean n-cube, the inequality $\eta(f) \le c(f) 2^{2c(f)-2}$ holds.*

Proof. First, we prove the following statement by induction. If every vertex of a nonempty induced subgraph of the Boolean n-cube has degree at least $r \le n$, then the subgraph contains at least 2^r vertices. For $n = 1$, the statement is obvious. Let us prove the induction step. Assume the statement is true for the n-dimensional cube. Consider a vertex set T in Q_2^{n+1} such that every vertex of the induced subgraph on T has degree at least r. Choose

an arbitrary edge of the subgraph induced by T. Without loss of generality, we assume that this is an edge in the n-th direction. Consequently, the sets $T_0 = Q_2^n\square\{0\} \cap T$ and $T_1 = Q_2^n\square\{1\} \cap T$ are nonempty. Subgraphs induced by T_0 and T_1 have vertex degrees at least $r-1$, since any vertex in T_0 is adjacent to at most one vertex in T_1 and vice versa. Then, by the induction hypothesis, we have $|T| = |T_0| + |T_1| \geq 2 \cdot 2^{r-1}$.

We proceed to the proof of the theorem. Without loss of generality, we can assume that the n-th variable of f is relevant. Then there exists a nonmonochromatic edge $\{x, y\}$ of the n-th direction. The vertices incident with this edge have different colors: $f(x) = \alpha$ in $Q_2^{n-1}\square\{0\}$ and $f(y) = \beta \neq \alpha$ in $Q_2^{n-1}\square\{1\}$. Let us estimate the number of nonmonochromatic edges in the n-th direction adjacent to $\{x, y\}$. At most $c(f)-1$ vertices in $Q_2^n\square\{0\}$ adjacent to vertex x have a color different from α. Similarly, at most $c(f)-1$ vertices in $Q_2^n\square\{1\}$ adjacent to vertex y have a color different from β. Vertices adjacent to vertices x and y are pairwise connected by edges in the n-th direction. Therefore, among the $n-1$ edges parallel to $\{x, y\}$, at least $n-1-2(c(f)-1)$ are nonmonochromatic. Consider the subgraph of the graph $Q_2^{n-1}\square\{0\}$ consisting of the vertices that are incident to nonmonochromatic edges in the n-th direction. As we showed above, the degree of the vertices of this subgraph is at least $n-2c(f)+1$. Consequently, the number of nonmonochromatic edges in the n-th direction and any other essential direction is at least $2^{n-2c(f)+1}$.

By the definition of $c(f)$, there are at most $c(f)2^{n-1}$ nonmonochromatic edges in the Boolean n-cube. Therefore $\eta(f)2^{n-2c(f)+1} \leq c(f)2^{n-1}$. □

Corollary 5.2. *For any $c, b \in \mathbb{N}$, there exists $n_0 \in \mathbb{N}$ such that for $n > n_0$, any perfect coloring of the Boolean n-cube with quotient matrix $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ has irrelevant variables.*

Proof. By the definition of the perfect coloring, $c(f) = \max\{c, b\}$. Thus, by Wegener's theorem, the number of relevant variables in the coloring does not exceed the constant $n_0 = \max\{c, b\}2^{2\max\{c,b\}-2}$. □

Any function with an irrelevant variable is a trivial extension of a function of fewer variables. It is easy to see that if a perfect coloring of a Boolean hypercube with quotient matrix $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ has an irrelevant variable, then it is the Cartesian product of a monochromatic edge and a perfect coloring with quotient matrix $\begin{pmatrix} n-b-1 & b \\ c & n-c-1 \end{pmatrix}$. Therefore, a constructive

description of perfect 2-colorings of Boolean n-cubes requires determining the maximum dimension n for which there exists a perfect coloring with quotient matrix $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ without irrelevant variables.

5.5 Problems

31. Suppose there exists a perfect coloring of Q_2^k with quotient matrix S. Prove that there exists a perfect coloring of Q_2^{mk} with quotient matrix mS.

32. Suppose there exists a perfect coloring of Q_q^k with quotient matrix S. Prove that there exists a coloring of Q_{pq}^k with quotient matrix $pS+k(p-1)I$.

33. Find the eigenvalues of the graph $Q_2^m \square Q_3^k$.

34. Formulate and prove an analogue of Wegener's Theorem for the ternary hypercube.

6 Amply Regular Graphs

6.1 Average Degree of Vertices

Let M be the adjacency matrix of some graph G. Then $M\mathbf{1}$ is the vector of vertex degrees of G, $n = (\mathbf{1}, \mathbf{1})$ is the number of vertices of G and $(M\mathbf{1}, \mathbf{1})/n$ is the average degree of vertices of G. The i-th coordinate of $M(M\mathbf{1}) = M^2\mathbf{1}$ is equal to the sum of the neighbors of the i-th vertex (if a vertex is adjacent to k neighbors, then it is counted k times). Equivalently, it is the number of walks of length 2 ending at the i-th vertex. Thus, $(M^2\mathbf{1}, \mathbf{1})/n$ is the average sum of the degrees of the neighbors of the vertices in G.

Proposition 6.1. *For any graph, the square of the average degree of vertices does not exceed the average of the sums of the degrees of the vertex's neighbors. Moreover, if these are equal, then the graph is regular.*

Proof. From the Cauchy–Schwarz inequality we have

$$(M\mathbf{1}, \mathbf{1})^2 \le (M\mathbf{1}, M\mathbf{1})(\mathbf{1}, \mathbf{1}),$$

hence

$$\left(\frac{(M\mathbf{1}, \mathbf{1})}{(\mathbf{1}, \mathbf{1})}\right)^2 \le \frac{(M^2\mathbf{1}, \mathbf{1})}{(\mathbf{1}, \mathbf{1})}.$$

Moreover, equality is achieved only if the vectors $M\mathbf{1}$ and $\mathbf{1}$ are collinear. It is equivalent to the regularity of the graph. □

Consider a 2-coloring $f : V(G) \to \{0, 1\}$ of a regular graph G. Let G_i be the subgraph induced by the vertices of color $i \in \{0, 1\}$. For each of these subgraphs, Proposition 6.1 holds. Define $g = f \cdot Mf$ and $g' = f' \cdot Mf'$, where $f' = \mathbf{1} - f$ and $\cdot$ denotes entrywise (Hadamard) product. From the Cauchy–Schwarz inequality, we have $(g, f)^2 \le (g, g)(f, f)$ and $(g', f')^2 \le (g', g')(f', f')$. Let us show that equality in both inequalities is simultaneously reached if and only if the coloring of f is perfect.

Remove all vertices of color 0 from the graph. Then, for the induced subgraph G_1, the functions f and g play the roles of $\mathbf{1}$ and $M\mathbf{1}$. In the case of equality, all vertices of color 1 have the same number of neighbors of color 1, and hence, by the regularity of G, the same number of neighbors of color 0. The same arguments apply to the characteristic function f' of color 0. Conversely, if the coloring of f is perfect, then the vectors f and g, as well as f' and g', are collinear. Then Cauchy–Schwarz inequalities become equalities.

Below we give another example of the extremal property of a perfect coloring. Denote by $M_2 = M_2(G)$ the adjacency matrix of distances 2 of the graph G, i.e.,

$$M_2(x, y) = \begin{cases} 1, & d(x, y) = 2; \\ 0, & \text{otherwise.} \end{cases}$$

As noted above, the (x, y)-entry of M^2 is the number of walks of length 2 from x to y. In particular, traversing an edge twice gives a walk of length 2 that starts and ends at the same vertex.

A regular graph is called *amply regular* if every pair of adjacent vertices has the same number of common neighbors and every pair of vertices at distance 2 has the same number of common neighbors.

In other words, every pair of adjacent vertices in such a graph has λ common neighbors, and every pair of nonadjacent vertices has 0 or $\mu > 0$ common neighbors. Consider a graph that is amply regular. It is clear that between any two vertices at distance of 1 there is the same number $a_1 = \lambda$ of walks of length 2, and between any two vertices at distance of 2 there is the same number $c_2 = \mu$ of walks of length 2. Therefore, $M^2 = c_2 M_2 + a_1 M + b_0 I$, where b_0 is the degree of the graph. The notations c_2, a_1, b_0 are consistent with the standard notation for distance-regular graphs (see Section 7.1). Thus,

$$M_2 = p_2 M^2 + p_1 M + p_0 I, \tag{10}$$

for some p_0, p_1, p_2. Note that for an amply r-regular graph $r = -p_0/p_2$. Let f be an arbitrary k-coloring of the graph G, let f_i be the characteristic function of color i, and let n_i be the number of vertices of color i. As above, we denote

by $s_{ij}(x)$ the number of neighbors of x colored by j. Here we imply that x has i-th color. We define the *average quotient matrix* $S_f = (\bar{s}_{ij})$, where $\bar{s}_{ij} = \frac{1}{n_i} \sum_{f(x)=i} s_{ij}(x)$, i.e., $\bar{s}_{ij}$ is the average number of neighbors of color j of a vertex of color i.

Theorem 6.1 (Krotov [79]). *Let G be an amply regular graph, i.e., its adjacency matrix M_2 with respect to distance 2 satisfies the equality $M_2 = P(M) = p_2M^2 + p_1M + p_0I$, and let f be a k-coloring of G with average quotient matrix S_f. Then, for any color i, the number of pairs of vertices of color i at distance 2 from each other does not exceed $n_i(p(S_f))_{ii}/2$, and if equality is reached for each color i, then f is a perfect k-coloring with quotient matrix S_f.*

Proof. Let f_i be the characteristic function of i-th color. Every function on $V(G)$ can be decomposed into a sum of functions supported on individual color classes. Then we can define the functions g^i_j such that $Mf_i = \sum_j g^i_j$, where $\mathrm{supp}(g^i_j) \subseteq \mathrm{supp}(f_j)$.

By definition $(g^i_j, f_j) = (Mf_i, f_j) = \bar{s}_{ij}n_i = \bar{s}_{ji}n_j$. By the Cauchy–Schwarz inequality, we have $(g^i_j, f_j)^2 \le (g^i_j, g^i_j)(f_j, f_j)$, and equality is reached only if the vectors g^i_j and f_j are collinear. Since $g^i_j(x) = s_{ji}(x)f_j(x)$ for any vertex of color j, we have $g^i_j = \bar{s}_{ji}f_j$ if the vectors g^i_j and f_j are collinear.

Twice the number of pairs of vertices of color i at distance 2 from each other is equal to (M_2f_i, f_i). Therefore,

$$(M_2f_i, f_i) = (P(M)f_i, f_i) = (p_0f_i + p_1Mf_i + p_2M^2f_i, f_i)$$

$$= p_0(f_i, f_i) + p_1(Mf_i, f_i) + p_2(Mf_i, Mf_i)$$

$$= p_0n_i + p_1\bar{s}_{ii}n_i + p_2(\sum_j g^i_j, \sum_j g^i_j) = p_0n_i + p_1\bar{s}_{ii}n_i + p_2\sum_j (g^i_j, g^i_j)$$

$$\ge p_0n_i + p_1\bar{s}_{ii}n_i + p_2\sum_j (g^i_j, f_j)^2/n_j$$

$$= p_0n_i + p_1\bar{s}_{ii}n_i + p_2\sum_j \bar{s}_{ij}\bar{s}_{ji}n_in_j/n_j = n_i(P(S_f))_{ii}.$$

Moreover, equality holds only if $g^i_j = \bar{s}_{ij}f_j$ for all i, j, i.e., if f is a perfect coloring with quotient matrix S_f. □

Denote by $\sigma(C)$ the average number of neighbors lying in $C \subset V$, i.e., $\sigma(C) = e(C,C)/|C| = (M\mathbf{1}_C, \mathbf{1}_C)/|C|$; and denote by $\sigma_2(C)$ the average number of vertices of C at distance 2, i.e., $\sigma_2(C) = (M_2\mathbf{1}_C, \mathbf{1}_C)/|C|$. Below we formulate Theorem 6.1 for 2-colorings.

Corollary 6.1. *Let G be an amply r-regular graph with polynomial P, and let $C \subset V(G)$. If $\sigma(C) = a$ and $\sigma(V\backslash C) = d$, then $\sigma_2(C) \le (P(S))_{11}$ and $\sigma_2(V\backslash C) \le (P(S))_{22}$, where $S = \begin{pmatrix} a & r-a \\ r-d & d \end{pmatrix}$. Moreover, both inequalities are equalities if and only if $\mathbf{1}_C$ is a perfect 2-coloring with quotient matrix S.*

By Corollary 6.1, we obtain the following criterion for perfect 2-colorings with the minimum eigenvalue in amply regular graphs.

Corollary 6.2. *Let G be an amply r-regular graph with polynomial P, and let $C \subset V$ be an independent set. Then $\sigma_2(C) \le -p_2 r(\lambda_{min}+1)$, where λ_{min} is the minimum eigenvalue of G. Moreover, equality holds whenever $\mathbf{1}_C$ is a perfect 2-coloring with the eigenvalue λ_{min}.*

Proof. Let S be the average quotient matrix of $\mathbf{1}_C$. It is clear that $\sigma(C) = 0$ and $\sigma(V\backslash C) = \frac{(|V(G)|-|C|)r-|C|r}{|V(G)|-|C|} = r(1 - \frac{|C|}{|V(G)|-|C|})$ for each independent set C. A straightforward computation shows that $P(S)_{11} = p_2(r(r - \sigma(V\backslash C)) - r)$. By Theorem 6.1, it holds that $\sigma_2(C) \le p_2(\frac{r^2|C|}{|V(G)|-|C|} - r)$. By the Delsarte–Hoffman bound, we get $\frac{r^2|C|}{|V(G)|-|C|} \le -\lambda_{min} r$. Thus $\sigma_2(C) \le -p_2 r(\lambda_{min}+1)$. For any perfect 2-coloring with the eigenvalue λ_{min}, the equality $\sigma_2(C) = -p_2 r(\lambda_{min}+1)$ follows from Corollary 6.1 and the Delsarte–Hoffman bound (Proposition 3.2). □

6.2 Generalizations of Delsarte–Hoffman Bound

By the definition, a quotient matrix determines how many vertices of one color are adjacent to a vertex of another color. In an amply regular graph, the quotient matrix also determines the number of vertices of one color that lie at distance 2 from a vertex of the other color. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a quotient matrix and let C be the set of first color vertices. Then we have $\sigma(C) = a$, $\sigma_2(C) = (p_2(a^2+bc)+p_1 a+p_0)$, and $|C| = \frac{c|V(G)|}{b+c}$. Define $\beta = p_2(a^2+bc)+p_1 a+p_0$, then $\frac{c}{b+c} = \frac{bc}{b^2+bc} = \frac{\beta - P(a)}{p_2 b^2 + \beta - P(a)}$.

Next we will show that, in an amply regular graph an upper bound on $\sigma_2(C)$ yields an upper bound on the cardinality of $|C|$. Moreover, when

this upper bound is attained, the characteristic function of C is a perfect 2-coloring.

Theorem 6.2. *Let G be an amply r-regular graph with polynomial P, and let $C \subset V$. If $a = \sigma(C)$ and $\beta = \sigma_2(C)$ then $|C| \le \frac{(\beta - P(a))n}{p_2(r-a)^2 + \beta - P(a)}$. Moreover, if $|C| = \frac{(\beta - P(a))n}{p_2(r-a)^2 + \beta - P(a)}$ then $\mathbf{1}_C$ is a perfect 2-coloring of G.*

Proof. Without loss of generality, we suppose that G is connected. Otherwise, the theorem can be proved separately for each connected component. Expand $\mathbf{1}_C$ in an orthonormal basis of eigenfunctions of G: $\mathbf{1}_C = \sum_i \alpha_i \phi_i$, where ϕ_i is an eigenfunction of M with eigenvalue λ_i. Without loss of generality, we assume $\|\phi_i\|_2 = 1$ for all i. The eigenfunction with eigenvalue r is equal to $\phi_0 = \mathbf{1}_V/\sqrt{n}$. From $(\mathbf{1}_C, \mathbf{1}_C) = \sum_i \alpha_i^2$ we obtain

$$\text{(I)} \qquad \sum_{i \ne 0} \alpha_i^2 = (\mathbf{1}_C, \mathbf{1}_C) - \alpha_0^2 = |C| - \varrho|C|,$$

where $\varrho = |C|/n$. From $(M\mathbf{1}_C, \mathbf{1}_C) = a|C|$ and $(M\mathbf{1}_C, \mathbf{1}_C) = \sum_i \alpha_i^2 \lambda_i$, it follows

$$\text{(II)} \quad r\varrho|C| + \sum_{i \ne 0} \alpha_i^2 \lambda_i = a|C|.$$

From (10) and the hypothesis of the theorem we obtain

$$(M^2\mathbf{1}_C, \mathbf{1}_C) = \frac{1}{p_2}((M_2 - p_1 M - p_0 I)\mathbf{1}_C, \mathbf{1}_C) = \frac{|C|}{p_2}(\beta - p_1 a - p_0).$$

Therefore,

$$\text{(III)} \quad r^2\varrho|C| + \sum_{i \ne 0} \alpha_i^2 \lambda_i^2 = \frac{|C|}{p_2}(\beta - p_1 a - p_0).$$

Consider the linear combination $\text{(III)} - 2\theta\text{(II)} + \theta^2\text{(I)}$. Then for any $\theta \in \mathbb{R}$ we obtain the inequalities

$$r^2\varrho|C| - 2r\varrho\theta|C| + \sum_{i \ne 0} \alpha_i^2(\lambda_i - \theta)^2 = \frac{|C|}{p_2}(\beta - p_1 a - p_0) - 2a\theta|C| + |C|(1-\varrho)\theta^2.$$

Since $\sum\limits_{i \ne 0} \alpha_i^2(\lambda_i - \theta)^2 \ge 0$, we obtain

$$r^2\varrho - 2r\varrho\theta \le \frac{1}{p_2}(\beta - p_1 a - p_0) - 2a\theta + (1-\varrho)\theta^2, \tag{11}$$

$$\varrho \le \frac{\frac{1}{p_2}(\beta - P(a)) + (a-\theta)^2}{(r-\theta)^2}.$$

Let $\theta = a - \frac{\beta - P(a)}{p_2(r-a)}$. Then we conclude that

$$\varrho \le \frac{(a-\theta)(r-a) + (a-\theta)^2}{(r-a+a-\theta)^2} = \frac{a-\theta}{r-\theta} = \frac{\beta - P(a)}{p_2(r-a)^2 + \beta - P(a)}.$$

It is clear that (11) holds with equality if and only if $\mathbf{1}_C = \phi + \alpha_0\varphi_0$, where ϕ is an eigenfunction with eigenvalue θ. By Proposition 2.7, this implies that $\mathbf{1}_C$ is a perfect 2-coloring. □

For $a = 0$ and $\beta = 0$, the new bound coincides with the Hamming bound $|C| \le \frac{|V(G)|}{r+1}$. If C is an independent set, then $a = 0$, $P(0) = p_0 = -rp_2$ and $\varrho \le 1/(1 + \frac{p_2 r^2}{\beta + p_2 r})$. This bound and the Delsarte–Hoffman bound are reached simultaneously on perfect 2-colorings with the minimum eigenvalue. In this case, it holds that $\sigma_2(C) = -p_2 r(\lambda_{min} + 1)$. By Corollary 6.2, we have $\sigma_2(C) \le -p_2 r(\lambda_{min} + 1)$ for any independent set C. Consequently, it is meaningful to consider only the case $\beta < -p_2 r(\lambda_{min} + 1)$.

Corollary 6.3. *Let C be an independent set in an amply r-regular graph G with polynomial P. If $\beta = \sigma_2(C) < -p_2 r(\lambda_{min} + 1)$, then the bound $\frac{|C|}{|V(G)|} \le 1/(1 + \frac{p_2 r^2}{\beta + p_2 r})$ is better than the Delsarte–Hoffman bound.*

Proof. $1/(1 + \frac{p_2 r^2}{\beta + p_2 r}) < 1/(1 + \frac{p_2 r^2}{-p_2 r \lambda_{min}}) = \frac{-\lambda_{min}}{r - \lambda_{min}}$. □

7 Distance-Regular Graphs

7.1 Intersection Array and Krawtchouk Polynomial

Let G be a simple graph. For a fixed vertex x_0 we consider the *distance partition* of the graph G with respect to x_0:

$$A_t(x_0) = \{x \in V(G) \mid d(x, x_0) = t\}.$$

A simple connected graph G is called *distance-regular* if, for every vertex x_0, the distance partition of G is equitable and its quotient matrix is independent of the choice of x_0.

Consider layer $A_t(x_0)$ in detail. A vertex $x \in A_t(x_0)$ is adjacent to a_t vertices in its layer, to b_t vertices in the next layer, and to c_t vertices in the previous layer. In a distance-regular graph, these parameters a_t, b_t, c_t are

independent of the choice of the initial vertex x_0 and the vertex $x \in A_t$ from a layer.

The set of values $(b_0, \ldots, b_{d-1}; c_1, \ldots, c_d)$ is called the *intersection array* of a distance-regular graph of diameter d.

Any distance-regular graph is regular; the degree of each vertex in it is $b_0 = r$. Strictly speaking, one should say $a_t + b_t + c_t = r$, $0 \le t \le d$, with conventions $c_0 = 0$ and $b_d = 0$.

From the definition, the distance coloring of a distance-regular graph with respect to any vertex x_0 is perfect with quotient matrix

$$S[G] = \begin{pmatrix} 0 & b_0 & 0 & 0 & \ldots & 0 \\ c_1 & a_1 & b_1 & 0 & \ldots & 0 \\ 0 & c_2 & a_2 & b_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & 0 & c_d & a_d \end{pmatrix}.$$

The quotient matrix of the distance coloring is called the intersection matrix of G. Therefore, every eigenvalue of $S[G]$ is an eigenvalue of G.

Example 7.1. The Boolean n-cube $Q_2^n = \{0,1\}^n$ is a distance-regular graph of diameter n with parameters $a_t = 0$, $b_t = n - t$, $c_t = t$.

Example 7.2. The hypercube Q_q^n is a distance-regular graph of diameter n with parameters $a_t = (q-2)t$, $b_t = (n-t)(q-1)$, $c_t = t$.

Example 7.3. The Johnson graph $J(n,k)$ is defined as follows. We take all binary n-tuples of weight k as a set of vertices. Vertices are connected by an edge if the Hamming distance between two n-tuples is equal to 2. The Johnson graph $J(n,k)$ is distance-regular with parameters $b_t = (k-t)(n-k-t)$, $c_t = t^2$, $a_t = k(n-k) - (k-t)(n-k-t) - t^2 = t(n-2t)$.

Constructions and properties of special distance-regular graphs is available in [18].

Remark 7.1. A natural question arises: is a distance-regular graph uniquely determined by its intersection array? It turns out not. For example, Q_4^2 and the Shrikhande graph (see Example 8.4 below) have the same intersection array $(b_0, b_1; c_1, c_2) = (6, 3; 1, 2)$. Moreover, Cartesian products (see Section 5) of these graphs with the same number of factors are nonequivalent distance-regular graphs with matching intersection arrays.

Remark 7.2. Listed above distance-regular graphs are transitive. However, these two classes are incomparable: there exist distance-regular graphs that are not transitive and transitive graphs that are not distance-regular (see [18]).

A *distance-t graph* is a graph with adjacency matrix M_t. A distance-t graph, obtained from a distance-regular graph, is usually no longer distance-regular. But there are exceptions. For example, the distance-2 graph obtained from the Boolean n-cube for any n is distance-regular.

Let M_t be the adjacency matrix of the distance-t graph, that is

$$M_t(x,y) = \begin{cases} 1, & d(x,y) = t; \\ 0, & \text{otherwise.} \end{cases}$$

The main property of a distance-regular graph is the following. Matrices M_t for any t can be represented as a polynomial in the adjacency matrix M of the graph. Note that the (ij)th element of M^k is equal to the number of walks of length k between ith and jth vertices. These walks are not required to be simple and may traverse the same edge several times. For example, $(M^2)_{ii}$ is the twice number of the degree of ith vertex.

Example 7.4. Let M be the adjacency matrix of the Boolean n-cube $Q_2^n = \{0,1\}^n$. Any vertex at distance 2 from the original can be reached in two ways: by moving first along the edge of direction i, then j, $j \neq i$, and vice versa.

$M_0 = I_{2^n}$, $M_1 = M$,

$M^2 = b_0 I_{2^n} + c_2 M_2 = n I_{2^n} + 2M_2$.

Proposition 7.1. *A graph of diameter d is distance-regular if and only if each of its distance-t adjacency matrices, $t = 2, \ldots, d$, is a polynomial of degree t in its adjacency matrix M.*

Proof. Fix a vertex y of a distance-regular graph, take a vertex x_i at distance t from it, and consider its neighbors. For the adjacency matrices of a distance-regular graph, the following equality holds:

$$M_t M = a_t M_t + b_{t-1} M_{t-1} + c_{t+1} M_{t+1}. \tag{12}$$

Indeed, in the matrix $M_t M$, position (i,j) indicates the number of ways to get from vertex x_i to x_j by first moving to an intermediate vertex z adjacent to x_j, located at a distance t from x_i, and then from there to vertex x_j. Clearly, the element of the matrix $(a_t M_t)_{ij}$ is equal to the number of ways to complete such a path if $d(x_i, x_j) = t$; $(b_{t-1} M_{t-1})_{ij}$, if $d(x_i, x_j) = t-1$; $(c_{t+1} M_{t+1})_{ij}$, if $d(x_i, x_j) = t+1$. Thus, the recurrence relations (12) hold. By induction, we obtain $M_t = P_t(M)$, where P_t is a polynomial of degree t. This shows that the multiplication of adjacency matrices by different

distances is commutative, i.e., $M_t M_s = M_s M_t$. Moreover, from (12) follows the recurrence relation

$$xP_t(x) = a_t P_t(x) + b_{t-1} P_{t-1}(x) + c_{t+1} P_{t+1}(x). \tag{13}$$

Let's prove that the converse is also true. If $M_t = P_t(M)$ then by induction we see that M^{t+1} and $M_t M$ are linear combinations of $I, M, \ldots, M_{t+1}$. Since an edge changes the distance to a fixed vertex by at most one, every walk contributing to $M_t M$ ends at distance $t-1$, t, or $t+1$. So, $M_t M$ is a nonnegative linear combination of M_{t-1}, M_t, M_{t+1}. We obtain equation (12) for some coefficients a_t, b_{t-1}, c_{t+1}. Let e_0 be the indicator function of the initial vertex. Then $M_t e_0$ is the characteristic function of tth color and $(M_t M e_0)_j = (M M_t e_0)_j$ indicates how many neighbors of the tth color the jth vertex has. From (12) we obtain that if jth vertex has tth color then the number of such vertex is a_t; if jth vertex has $(t-1)$th color then the number of such vertex is b_{t-1} and if jth vertex has $(t+1)$th color then the number of such vertex is c_{t+1}. Therefore, we prove that the distance coloring is perfect and its quotient does not depend on the initial vertex. □

In the case of a Boolean n-cube, the polynomial P_t (13) is called the Krawtchouk polynomial. A strict form of Krawtchouk polynomial will be calculated in Section 9.2. If we consider a q-ary cube, then the polynomial P_t is called the q-Krawtchouk polynomial $P_t[n, q](y)$. For Johnson graphs, the polynomial P_t is called the Eberlein polynomial. For other distance-regular graphs we treat P_t as a Krawtchouk-type polynomial.

Theorem 7.1 (Lloyd, Shapiro and Zlotnik, Martin)**.** *Let G be a distance-regular graph, G_t be the t-distance graph obtained from G, i.e., $V(G_t) = V(G)$, $M(G_t) = M_t$. If f is a perfect coloring of G with quotient matrix S, then f is a perfect coloring of G_t with quotient matrix $P_t(S)$.*

Proof. We have $MF = FS$, where F is the matrix corresponding to the coloring f. From the equality $M_t = P_t(M)$, we have $M_t F = P_t(M)F$. Furthermore, we have the equations $M^t F = M^{t-1} MF = M^{t-1}(FS) = FS^t$. Then $P_t(M)F = FP_t(S)$. By Proposition 2.3, we see that f is a perfect coloring of G_t with quotient matrix $P_t(S)$. □

Corollary 7.1. *For any perfect coloring of a distance-regular graph, the color composition of a sphere of radius t depends only on the color of the center of the sphere.*

This fact was originally established by Lloyd [94] for perfect codes in the Boolean n-cube. Shapiro and Zlotnik [131] found the weight distribution (see below) of a perfect code. Martin established this claim for any distance-regular graph in his thesis [101].

Theorem 7.1 provides a way to prove the nonexistence of a perfect coloring. Substituting the quotient matrix S of a perfect coloring into the polynomial P_t, we should obtain a matrix whose entries are nonnegative integer. Furthermore, the vector of color proportions calculated from the matrix $P_t(S)$ and multiplied by the size of the graph must also be integral. To the best of our knowledge, no examples are known in which a matrix S satisfies the conditions of Theorem 130, but some matrix $P_t(S)$ fails to have nonnegative integer entries .

7.2 Strongly Regular Graphs

A distance-regular graph of diameter 2 is called *strongly regular*.

It is easy to see that intersection array $(b_0, b_1; c_1, c_2)$ of a strongly regular graph calculated from only three parameters: degree r of the graph, the number λ of common neighbors of two adjacent vertices and the number μ of common neighbors of two non-adjacent vertices. Thus, $b_0 = r$, $b_1 = r-\lambda-1$, $c_1 = 1$, $c_2 = \mu$.

Proposition 7.2 ([55]). *A connected regular graph G with exactly three distinct eigenvalues is strongly regular.*

Proof. Let M be the adjacency matrix of an r-regular graph G. The matrix M is the root of its characteristic polynomial P, therefore $(M-rI)P(M) = 0$, where $P(x) = (x-\lambda_1)(x-\lambda_2)$ and $\lambda_1 < \lambda_2 < r$ are the eigenvalues of M. From the equality $(M-rI)P(M) = 0$ it follows that M^3 is equal to a linear combination of the matrices I, M, and M^2. Then any walk of length 3 in graph G connects vertices that are at distance 0, 1, or 2. Consequently, the graph G has diameter 2, i.e., $M_2 = J-M-I$. Since the graph G is connected, it follows that the matrix M has a unique eigenvector $\mathbf{1}$ with eigenvalue r. Then, from the equation $(M-rI)P(M) = 0$, it follows that all columns of the matrix $P(M)$ are collinear with the vector $\mathbf{1}$. Similarly, all rows of the matrix $P(M)$ are collinear with the vector $\mathbf{1}$. Then $P(M) = \alpha J$, where all components of J are equal to 1. We have $P(M) = \alpha(M_2 + M + I)$. □

If the complement of a strongly regular graph G with parameters $(v = |V(G)|, r, \lambda, \mu)$ is connected then it is also a strongly regular graph with

parameters $(v, v-r-1, v-2-2r+\mu, v-2r+\lambda)$. The eigenvalues of a strongly regular graph with parameters (v, r, λ, μ) are (see, e.g. [20, Theorem 9.1.3])

$$r, \quad \frac{\lambda-\mu \pm \sqrt{(\lambda-\mu)^2+4(r-\mu)}}{2},$$

with multiplicities, respectively,

$$1, \quad \frac{1}{2}\left(v-1 \mp \frac{2r+(v-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2+4(r-\mu)}}\right).$$

7.3 Minimum Support of Eigenfunctions

In this section, we will explore how large the minimum difference between two perfect colorings can be. At first we need to consider the cardinality of an eigenfunction's support. The *support* of a function $f : V(G) \to \mathbb{C}$ is the set $\mathrm{supp}(f) = \{x \in V(G) \mid f(x) \neq 0\}$. The *weight distribution* of a function $f : V(G) \to \mathbb{C}$ with respect to a vertex $a \in V(G)$ of a graph G is the sequence $\left(f(a), \ldots, \sum\limits_{d(y,a)=t} f(y), \ldots, \sum\limits_{d(y,a)=d} f(y)\right)$, where d is the diameter of G.

Proposition 7.3. *Let f be an eigenfunction of a distance-regular graph G with eigenvalue λ, i.e., $Mf = \lambda f$. Then $\sum\limits_{d(y,a)=t} f(y) = P_t(\lambda) f(a)$.*

Proof. Similarly to the proof of Theorem 7.1, we have the equalities $M^i f = \lambda^i f$ and $M_t f = P_t(M) f = P_t(\lambda) f$. Consequently, $\sum\limits_{d(y,a)=t} f(y) = (M_t f)(a) = P_t(\lambda) f(a)$. □

Thus, in a distance-regular graph, the sum of the values of an eigenfunction over the sphere depends only on the eigenvalue and the value of the function at the center of the sphere. For definiteness, we can assume that $f(a) = 1$. Then the set $[1, P_1(\lambda), \ldots, P_d(\lambda)]$ is the weight distribution (spectrum) of an eigenfunction with eigenvalue λ.

Any function $g : V(G) \to \mathbb{C}$ can be represented as a linear combination of the graph eigenfunctions: $g = \sum_i \alpha_i f_i$, where f_i is an eigenfunction of G with eigenvalue λ_i. Then we have

Corollary 7.2. *Let g be defined on the vertices of a distance-regular graph G. Then $\sum\limits_{d(y,a)=t} g(y) = \sum_i \alpha_i P_t(\lambda_i) f_i(a)$.*

Proposition 7.4 ([81]). *Let f be an eigenfunction with eigenvalue λ in a distance-regular graph. Then $|\mathrm{supp}(f)| \geq \sum_{t=0}^{d} |P_t(\lambda)|$, where d is the diameter of the graph.*

Proof. Choose a vertex a such that f has its maximum absolute value, that is, $|f(a)| = \max_{x \in V(G)} |f(x)|$. From Proposition 7.3 we have $\sum_{d(y,a)=t} f(y) = P_t(\lambda) f(a)$, which yields:

$$|\{y \mid d(y,a) = t, f(y) \neq 0\}| \geq \sum_{d(y,a)=t} \frac{|f(y)|}{|f(a)|} \geq |P_t(\lambda)|.$$

□

Consider perfect colorings f_1 and f_2 of a distance-regular graph G with two colors 0 and 1 with the same quotient matrix. Since f_1 and f_2 have the same quotient matrix, their difference is orthogonal to the constant function and is an eigenfunction corresponding to the nontrivial eigenvalue λ of the quotient matrix. The number of vertices, where f_1 and f_2 differ can be estimated by Proposition 7.4: $|\mathrm{supp}(f_1 - f_2)| \geq \sum_{t=0}^{d} |P_t(\lambda)|$.

A detailed review of minimum supports of eigenfunctions of graphs is available in [134].

The function $u : V(G) \to \{0, \pm 1\}$ is called a *bitrade (ball bitrade)* in graph G if for any ball $B(x)$, $x \in V(G)$, of radius 1 the following holds $\begin{cases} |B(x) \cap u^{-1}(1)| = 1, \\ |B(x) \cap u^{-1}(-1)| = 1, \end{cases}$ or $u(B(x)) = \{0\}$. In other words, the function takes the values 0 and ± 1 and either takes exactly one value each of 1 and -1 in a ball of radius 1, or only zeros in this ball. The difference of the characteristic functions of two 1-perfect codes is a bitrade. It is easy to see that a bitrade is an eigenfunction with eigenvalue -1. Indeed, if the ball $B(x)$ contains only zeros, then $Mu(x) = 0 = -u(x)$, otherwise the ball contains one 1 and one -1, so $u(x) + Mu(x) = 0$. By Proposition 7.4, we have $|\mathrm{supp}(u)| \geq \sum_{t=0}^{d} |P_t(-1)|$, where d is the graph diameter.

Denote by A_t the set of vertices at distance t from some fixed vertex x_0 in G.

Proposition 7.5. *Let f_1, f_2 be eigenfunctions of a distance-regular graph G of diameter d with the same eigenvalue λ, $P_d(\lambda) \neq 0$. If the functions f_1 and f_2 coincide on the set $A_{t-1} \cup A_t$, where $t < d/2$, then $f_1|_{A_i} = f_2|_{A_i}$ for $i \leq t$.*

Proof. Let $x' \in A_i$ and $f_1(x') \neq f_2(x')$. Denote by A'_d the set of vertices that are at distance d from some fixed vertex x'. The triangle inequality implies that $A'_d \cap A_i = \varnothing$ for $i \leq t$. Indeed, if $y \in A'_d \cap A_i$ then $d(y, x') \leq i + i < d$. From the condition $P_d(\lambda) \neq 0$ and Proposition 7.3 it follows that $\sum\limits_{x \in A'_d} f_1(x) \neq \sum\limits_{x \in A'_d} f_2(x)$. Consider the function f_3 defined by the equality

$$f_3(x) = \begin{cases} f_1(x), & x \in A_i, i \leq t \\ f_2(x), & x \in A_i, i > t. \end{cases}$$

Since f_1 and f_2 coincide on the set $A_{t-1} \cup A_t$, every vertex outside $A_{t-1} \cup A_t$, has all its neighbors in layers on which f_3 agrees with either f_1 or f_2. Then f_3 is an eigenfunction with eigenvalue λ. By Proposition 7.3 it follows that

$$\sum_{x \in A'_d} f_3(x) = P_d(\lambda) f_3(x') = P_d(\lambda) f_1(x') = \sum_{x \in A'_d} f_1(x).$$

But by construction, $f_3|_{A'_d} = f_2|_{A'_d}$. We obtain a contradiction. □

Corollary 7.3. *If $P_d(-1) \neq 0$, then the support of a bitrade has diameter at least $\lceil d/2 \rceil - 2$.*

In particular, the diameter of Q_2^n is n, the eigenvalues are $\lambda_k = n - 2k$, $k = 0, \ldots, n$, and $P_d(\lambda_k) = (-1)^{k+1}$ (see Section 9.2). Then any bitrade has diameter at least $(n-3)/2$ if n is odd and $(n-4)/2$ if n is even.

7.4 Orthogonality Relations for Krawtchouk-Type Polynomials

Let $s_t = |A_t|$. Since a constant is an eigenfunction with eigenvalue r of an r-regular graph, by Proposition 7.3 we have $s_t = P_t(r)$.

Proposition 7.6. *Let λ be an eigenvalue of a distance-regular graph G of diameter d and*

$$z(\lambda) = (z_0(\lambda), \ldots, z_d(\lambda)), \qquad z_t(\lambda) = P_t(\lambda)/s_t, \qquad t = 0, \ldots, d.$$

Then the vector $z(\lambda)$ is an eigenvector of the intersection matrix $S[G]$ of G with eigenvalue λ.

Proof. Consider some eigenfunction f of graph G with eigenvalue λ. By the definition of an eigenfunction for an arbitrary vertex $x \in A_t$, we have the

equality

$$\lambda f(x) = \sum_{y:y\in A_{t-1},d(x,y)=1} f(y) + \sum_{y:y\in A_t,d(x,y)=1} f(y) + \sum_{y:y\in A_{t+1},d(x,y)=1} f(y). \tag{14}$$

Let us sum both sides of the equality over all vertices $x \in A_t$. Since every vertex of A_t has exactly c_t neighbors in A_{t-1}, the number of edges between A_{t-1} and A_t is $c_t|A_t|$. By distance regularity, each vertex $y \in A_{t-1}$ is adjacent to the same number $\frac{c_t|A_t|}{|A_{t-1}|}$ of vertices in A_t. We have the equality $\sum_{x\in A_t} \sum_{y:y\in A_{t-1},d(x,y)=1} f(y) = \frac{c_t|A_t|}{|A_{t-1}|} \sum_{y\in A_{t-1}} f(y)$. Similarly, transforming the other terms and applying Proposition 7.3, we obtain the equality

$$\lambda P_t(\lambda) = \frac{c_t|A_t|P_{t-1}(\lambda)}{|A_{t-1}|} + \frac{a_t|A_t|P_t(\lambda)}{|A_t|} + \frac{b_t|A_t|P_{t+1}(\lambda)}{|A_{t+1}|},$$

which is equivalent to the required equality $\lambda z_t(\lambda) = c_t z_{t-1}(\lambda) + a_t z_t(\lambda) + b_t z_{t+1}(\lambda)$. □

Remark 7.3. Since a graph G of diameter d has at least $d+1$ distinct eigenvalues (see Problem 14), $S[G]$ has $d+1$ distinct eigenvalues, and the sets of eigenvalues of G and $S[G]$ coincide.

Corollary 7.4. *Let $\bar{z}^\lambda(x) = z_t(\lambda)$ if $x \in A_t$. Then $\bar{z}^\lambda$ is an eigenfunction of G with eigenvalue λ.*

Proof. The equation $\lambda z_t(\lambda) = c_t z_{t-1}(\lambda) + a_t z_t(\lambda) + b_t z_{t+1}(\lambda)$ is equivalent to equality (14), which coincides with the definition of an eigenfunction. □

Corollary 7.5 (Orthogonality of Krawtchouk-type Polynomials)**.** *We introduce the notation $\widetilde{z}_t(\lambda) = \sqrt{s_t} z_t(\lambda) = P_t(\lambda)/\sqrt{s_t}$. If $\lambda_1 \neq \lambda_2$ are eigenvalues of a distance-regular graph G, then the vectors $\widetilde{z}(\lambda_1)$ and $\widetilde{z}(\lambda_2)$ are orthogonal.*

Proof. From the orthogonality of the eigenfunctions $\bar{z}^{\lambda_1}$ and $\bar{z}^{\lambda_2}$ of a graph G with different eigenvalues, we have the equalities

$$0 = \sum_{x\in V(G)} \bar{z}^{\lambda_1}(x)\bar{z}^{\lambda_2}(x) = \sum_{t=0}^{d} s_t\, z_t(\lambda_1) z_t(\lambda_2)$$
$$= \sum_{t=0}^{d} s_t \frac{P_t(\lambda_1)}{s_t} \frac{P_t(\lambda_2)}{s_t} = \sum_{t=0}^{d} \widetilde{z}_t(\lambda_1)\widetilde{z}_t(\lambda_2).$$

□

Equivalently, $\sum_{t=0}^{d} \frac{P_t(\lambda_i)P_t(\lambda_j)}{s_t} = 0, \qquad i \neq j.$

7.5 Completely Regular Codes

A subset of the vertices of a graph is called a *completely regular code* if the distance coloring with respect to it is a perfect coloring.

In this case, we assume that the code is the zero color, the set of vertices at distance 1 from the code is the first color, and so on. It is clear that every one-element subset of a distance-regular graph is a completely regular code. Every color of 2-perfect coloring in any regular graph is completely regular code by definition. It is easy to show that in a distance-regular graph, any perfect code with arbitrary code distance (see Section 19.3) is completely regular. The theory of completely regular codes is presented in detail in [77] and [83].

Consider a graph G and a vertex $x_0 \in V(G)$. Recall that by A_i we denote the set of vertices at distance i from the vertex x_0. Let C be a code and $|A_i \cap C|$ be the weight of its intersection with the i-th layer A_i. Then the *weight distribution (spectrum)* of the code (relative to the vertex x_0, $A_0 = \{x_0\}$) is the weight distribution of its characteristic function, i.e., the set $[|A_0 \cap C|, |A_1 \cap C|, \ldots, |A_d \cap C|]$.

By the Theorem 7.1, in distance-regular graphs the weight distribution of a completely regular code depends only on the parameters of the distance coloring and a color of the initial vertex relative to which the distance refinement is considered. In particular, all 1-perfect codes in a distance-regular graph that contain the initial vertex have the same weight distribution.

Let G be a distance-regular graph, and let C be a code in G. For $t \geq 0$, let $C_t = \{x \in V(G) : d(x, C) = t\}$, where $d(x, C) = \min_{y \in C} d(x, y)$. Let ρ be a largest integer such that $C_\rho \neq \varnothing$. The number ρ is called the *covering radius* of the code C.

The following theorem is actually the standard characterizations of completely regular codes (see [18]).

Theorem 7.2. *A code C in a distance-regular graph G is completely regular if and only if, for every t and every $i \geq t$, each vertex $x \in C_t$ has the same number of vertices from C at distance i from x.*

Proof. ($\Rightarrow$) Follows from Theorem 7.1.

($\Leftarrow$) From the matrix equation of a perfect coloring (Proposition 2.3 or

Proposition 2.4) it follows that for any j it suffices to prove the equality

$$M\mathbf{1}_{C_j} = \sum_{i=0}^{d} s_{ji}\mathbf{1}_{C_i} \tag{15}$$

with some coefficients s_{ji}. By the hypothesis, for every i the value $M_i\mathbf{1}_C(x)$ depends only on the distance $t = d(x, C)$. Thus, for any i, $i = 0, \ldots, d$, we have the equality

$$M_i\mathbf{1}_C = \sum_{j=0}^{d} p_{ji}\mathbf{1}_{C_j}.$$

By the definition of C_t, we have $p_{ti} = 0$ for $t > i$ and $p_{tt} > 0$. For $t = 0$ (15) is true by the hypothesis. Let's assume it is proven for $j < t$. Then

$$M_tM\mathbf{1}_C = MM_t\mathbf{1}_C = \sum_{j=0}^{t} p_{jt}M\mathbf{1}_{C_j} = \sum_{j=0}^{t-1} p_{jt}\left(\sum_{i=0}^{d} s_{ji}\mathbf{1}_{C_i}\right) + p_{tt}M\mathbf{1}_{C_t}. \tag{16}$$

From equality (12) for a distance-regular graph, we have

$$M_tM\mathbf{1}_C = a_tM_t\mathbf{1}_C + b_{t-1}M_{t-1}\mathbf{1}_C + c_{t+1}M_{t+1}\mathbf{1}_C.$$

Therefore,

$$M_tM\mathbf{1}_C = \sum_{i=0}^{d} q_{ti}\mathbf{1}_{C_i},$$

for some coefficients q_{ti}. Since $p_{tt} > 0$, the coefficient of $M\mathbf{1}_{C_t}$ in (16) is nonzero. Therefore, $M\mathbf{1}_{C_t}$ is a linear combination of the vectors $\mathbf{1}_{C_0}, \ldots, \mathbf{1}_{C_d}$, proving (15) for $j = t$. Thus, the induction step is proved. □

Example 7.5. Consider the hypercube Q_q^n. The set $C = V(Q_q^k) \times \{a\}$ is a k-dimensional face of Q_q^n. Every face of Q_q^n of dimension k is a completely regular code with the quotient matrix $S = S[Q_q^{n-k}]$.

Example 7.6. A famous example of completely regular code is Preparata code (see [116] and [92]), which consist of the vertices of the first color in a perfect coloring of the Boolean n-cube with quotient matrix $\begin{pmatrix} 0 & n & 0 & 0 \\ 1 & 0 & n-1 & 0 \\ 0 & 2 & n-3 & 1 \\ 0 & 0 & n & 0 \end{pmatrix}$. Preparata codes exist in Boolean n-cubes if $n = 2^{2t} - 1$ and t is an integer.

Example 7.7. Another well-known example of completely regular code is constructed in [25]. It consists of the vertices of the first color in a perfect coloring of the Boolean n-cube with quotient matrix $\begin{pmatrix} 0 & n & 0 & 0 \\ 1 & 0 & n-1 & 0 \\ 0 & 2 & \frac{n-7}{2} & \frac{n+3}{2} \\ 0 & 0 & \frac{n-1}{2} & \frac{n+1}{2} \end{pmatrix}$. Preparata codes exist in Boolean n-cubes if $n = 2^{2t-1} - 1$ and t is an integer.

Examples of completely regular in Johnson graphs are available in [6] and [7].

Proposition 7.7. *Let G be a distance-regular graph and let C be a completely regular code in G with covering radius d. Suppose that $\mathbf{1}_C = \sum_{i=1}^{n} a_i f_i$, where f_i are eigenfunctions of G. Then, for any t, $t \le d$, $\mathbf{1}_{C_t}$ is a linear combination of the same eigenfunctions, i.e., $\mathbf{1}_{C_t} = \sum_{i=1}^{n} b_i f_i$.*

Proof. The proposition is true if $t = 0$. Suppose it is true for $j < t$. By the definition of completely regular codes, we have equality

$$M_t \mathbf{1}_C = \sum_{j=0}^{t-1} p_{jt} \mathbf{1}_{C_j} + p_{tt} \mathbf{1}_{C_t},$$

where $p_{tt} > 0$. By Proposition 7.3 we have equalities $M_t f_i = P_t(M) f_i = P_t(\alpha_i) f_i$. Then by the induction hypothesis we obtain the required result. □

Let G be a regular graph and $C \subset V(G)$ a completely regular code. Consider the distance refinement of vertices with respect to C: $C_j = \{x \in V(G) \mid \min_{y \in C} d(x,y) = j\}$. Clearly, $C_0 = C$. By the definition of a completely regular code, C_j is the set of vertices of the jth color in some perfect coloring h with quotient matrix S_C. Let $f : V(G) \to \{1, \dots, k\}$ be another perfect coloring of G. We will call the weight distribution of a coloring f with respect to C the sets of vectors $w_0 = (|C_0 \cup f^{-1}(1)|, \dots, |C_0 \cup f^{-1}(k)|), \dots, w_j = (|C_j \cup f^{-1}(1)|, \dots, |C_j \cup f^{-1}(k)|), \dots$.

Theorem 7.3 (Krotov [78])**.** *The weight distribution $w_0, \dots, w_j, \dots$ of a perfect coloring f of G with respect to a completely regular code $C \subset V(G)$ can be recovered from w_0.*

Proof. Let M be the adjacency matrix of graph G and S_f the quotient matrix of f. Then, by Proposition 2.3 and the definition of a completely regular

code, we have the equalities $MF = FS_f$ and $MH = HS_{C}$, where $H_{ij} = 1$ only if the i-th vertex of G is at distance j from C.

Consider the matrix $W = F^{\mathsf{T}}H$. By definition, its columns are w_j. We have the equalities $S_f^{\mathsf{T}}F^{\mathsf{T}}H = F^{\mathsf{T}}M^{\mathsf{T}}H = F^{\mathsf{T}}MH = F^{\mathsf{T}}HS_{C}$. By the condition, we know the first (with distance 0 from the code C) column of the matrix W.

Since S_{C} is a distance coloring matrix, it is tridiagonal:

$$S_{C} = \begin{pmatrix} a_0 & b_0 & 0 & 0 & \dots & 0 \\ c_1 & a_1 & b_1 & 0 & \dots & 0 \\ 0 & c_2 & a_2 & b_2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & c_d & a_d \end{pmatrix},$$

where d is the maximum possible distance from the code C to an arbitrary vertex in G. Moreover, $c_i \neq 0$ and $b_i \neq 0$ for all i, since some vertices of consistent layers in the distance-from-code refinement should be adjacent. We reconstruct the columns $w_1, w_2, \dots, w_d$ of W recursively. From the equation $WS_{C} = S_f^{\mathsf{T}}W$, we have $a_0w_0 + c_1w_1 = S_f^{\mathsf{T}}w_0$, i.e., $w_1 = (S_f^{\mathsf{T}}w_0 - a_0w_0)/c_1$. Similarly, for column w_i, $i = 1, \dots, d-1$, we have the equality $b_{i-1}w_{i-1} + a_iw_i + c_{i+1}w_{i+1} = S_f^{\mathsf{T}}w_i$. From these equalities, we can sequentially calculate all columns of the matrix W, and hence reconstruct the weight distribution of the coloring f with respect to the code C. □

Consider the Cartesian product $G_1 \square G_2$, in which G_1 is an r-regular graph, and G_2 is a distance-regular graph with quotient matrix $S[G_2]$. Consider the vertex set $C = V(G_1) \times \{a\}$, $a \in G_2$.

Proposition 7.8. *The distance coloring f of the graph $G_1 \square G_2$ with respect to C ($f(x, y) = d(y, a)$) is perfect with quotient matrix $S[G_2] + rI$. Thus, the code C is completely regular in $G_1 \square G_2$.*

Proof. Let a vertex $y \in V(G_2)$ be at distance i from a vertex a. By the definition of a distance-regular graph, it is adjacent to vertices c_i, a_i, b_i at distances $i-1, i, i+1$ from a, respectively, where c_i, a_i, b_i are from the intersection array of G_2. By the definition of the Cartesian product, a vertex (x, y) of graph $G_1 \square G_2$ has c_i neighbors of color $i-1$, b_i neighbors of color $i+1$, and $a_i + r$ neighbors of color i. □

For the code $C \subset V(G)$, we define $s^*(C)$ such that $s^*(C) + 1$ is the minimum number of eigenfunctions of the graph G, a linear combination of which is the characteristic function $\mathbf{1}_C$.

Theorem 7.4 ([19]). *Let G be a distance-regular graph of diameter d. Then*
(a) *for any code C, the equality* $\mathrm{diam}(C) + s^*(C) \geq d$ *holds;*
(b) *if* $\mathrm{diam}(C) + s^*(C) = d$, *then C is completely regular.*

Proof. Let M_t be the adjacency matrix of G over distance t. Consider a matrix B of size $(d+1)\times V(G)$, whose rows are the vectors $M_t\mathbf{1}_C$, $t = 0, \ldots, d$. Let $C_0, \ldots, C_\rho$, $d - \mathrm{diam}(C) \leq \rho \leq d$, be the distance refinement of vertices of graph G with respect to code C.

(a) From the Proposition 7.3, the row rank of matrix B is $s^*(C) + 1$. From the definition of the diameter of a code, it follows that in the columns of matrix B corresponding to vertices from C_i, only positions from i to $\mathrm{diam}(C) + i$ are nonzero. After ordering the columns according to the partition $C_0, \ldots, C_\rho$ the matrix B contains upper-triangle submatrix of order $d + 1 - \mathrm{diam}(C)$. Therefore, the column rank of matrix B is at least $d + 1 - \mathrm{diam}(C)$.

(b) If $\mathrm{diam}(C) + s^*(C) = d$, then the rank of matrix B is equal to the number of distinct supports of the columns. Hence, we conclude that columns with the same supports are collinear. Since the sum of the elements in each column is $|C|$, columns with the same supports coincide. By Theorem 7.2 this condition is equivalent to the definition of a completely regular code. □

7.6 Delsarte Cliques in Distance-Regular Graphs

Let λ be an eigenvalue of a distance-regular graph G of diameter d. Let $u_1, \ldots, u_m$ be an orthonormal basis of the eigenspace X_λ of G. Consider the vectors $w^\lambda(x) = (u_1(x), \ldots, u_m(x))$, where $x \in V(G)$. Their scalar products are the elements of the matrix E_λ defined in Section 2.3.

From Corollary 2.4 and Proposition 7.1 we have

Proposition 7.9. *If G is a distance-regular graph of diameter d, then the matrices E_λ can be represented as linear combinations of the distance-t adjacency matrices of G, where $t = 0, \ldots, d$.*

Corollary 7.6. *If G is a distance-regular graph of diameter d, then the element $E_\lambda(x, y)$ depends only on the distance between vertices x and y in G.*

We define the vector $\gamma(\lambda) = (\gamma_0, \ldots, \gamma_d)$, where $\gamma_t = E_\lambda(x, y)$ if $d(x, y) = t$. Fix an arbitrary vertex $x_0 \in V(G)$ as the initial vertex and the distance refinement $[A_0, \ldots, A_d]$ of G with respect to it. Recall the notation from Section 7.3: $z_t(\lambda) = P_t(\lambda)/s_t$, $t = 0, \ldots, d$, where $s_t = |A_t|$.

Proposition 7.10. *Let G be a distance-regular graph of diameter d. Then the vectors $z(\lambda)$ and $\gamma(\lambda)$ are collinear.*

Proof. Consider an orthonormal basis of the eigenspace X_λ of G corresponding an eigenvalue λ. By the definition of an eigenfunction, for each $x \in A_t$, we have the equality

$$\lambda u_i(x) = \sum_{y:y\in A_{t-1},d(x,y)=1} u_i(y) + \sum_{y:y\in A_t,d(x,y)=1} u_i(y) + \sum_{y:y\in A_{t+1},d(x,y)=1} u_i(y).$$

Then

$$\lambda w^\lambda(x) = \sum_{y:y\in A_{t-1},d(x,y)=1} w^\lambda(y) + \sum_{y:y\in A_t,d(x,y)=1} w^\lambda(y) + \sum_{y:y\in A_{t+1},d(x,y)=1} w^\lambda(y). \tag{17}$$

Consider the scalar product of both sides of (17) by the vector $w^\lambda(x_0)$. We obtain the equality

$$\lambda\gamma_t(\lambda) = c_t\gamma_{t-1}(\lambda) + a_t\gamma_t(\lambda) + b_t\gamma_{t+1}(\lambda), \tag{18}$$

where a_t, c_t, b_t are elements of the intersection array of G.

Then the vector $\gamma(\lambda)$ is an eigenvector of the intersection matrix $S[G]$ of G with eigenvalue λ. By Remark 7.3, every eigenspace of $S[G]$ is one-dimensional. By Proposition 7.6, the vector $z(\lambda)$ is contained in the same eigenspace of $S[G]$. □

Next we prove an analog of Theorem 3.1 for a distance-regular graph.

Theorem 7.5 (on the Delsarte clique [52])**.** *Let G be an r-regular graph. If G is a distance-regular graph then the cardinality of any clique in G does not exceed $1 + \frac{r}{-\lambda_{min}}$, where λ_{min} is the minimum eigenvalue of G.*

Proof. Let $u_1, \ldots, u_m$ be an orthonormal basis of the eigensubspace $X_{\lambda_{min}}$. Consider the vectors $w(x) = (u_1(x), \ldots, u_m(x))$, where $x \in V(G)$. Their scalar products are elements of the matrix $E_{\lambda_{min}}$. By Corollary 7.6, their scalar products are the same for all pairs of adjacent vertices x and y, as well as for pairs of coinciding vertices. Let $(w(x), w(y)) = \beta$ for any pair of adjacent vertices $x, y \in V(G)$ and $(w(x), w(x)) = \alpha$ for any vertex $x \in V(G)$.

From the definition of an eigenfunction, we have the equality $\sum_{y\in A_1(x)} u_i(y) = \lambda_{min}u_i(x)$, i.e., $\sum_{y\in A_1(x)} w(y) = \lambda_{min}w(x)$. The scalar product of both sides of the previous equality by $w(x)$ gives that $r\beta = \lambda_{min}\alpha$.

Let $C \subset V(G)$ be a clique in G. Consider the Gram matrix W of size $|C| \times |C|$, whose elements are $(w(x), w(y))$, $x, y \in C$. We have

$$W = \begin{pmatrix} \alpha & \beta & \beta & \dots & \beta \\ \beta & \alpha & \beta & \dots & \beta \\ \dots & \dots & \dots & \dots & \dots \\ \beta & \dots & \dots & \beta & \alpha \end{pmatrix}.$$

The Gram matrix is positive semidefinite, so $(W\overline{1}, \overline{1}) \geq 0$, therefore, $\alpha + (|C| - 1)\beta \geq 0$. Since the minimum eigenvalue λ_{min} is negative (see Problem 1), this and the equality $r\beta = \lambda_{min}\alpha$ yield $|C| \leq 1 + \frac{r}{-\lambda_{min}}$. □

Recall that a clique of cardinality $1 - \frac{r}{\lambda_{\min}}$ in an r-regular graph G is called a Delsarte clique.

Theorem 7.6 ([52]). *Every Delsarte clique in a distance-regular graph of diameter d is a completely regular code with covering radius $d - 1$.*

Proof. Let C be a Delsarte clique and C_t be the set of vertices at distance t from $C = C_0$. By Theorem 7.2, it suffices to verify that for any t and $i \geq t$, each vertex $x \in C_t$ has the same number of vertices from C at distance i. We need to check the number of vertices only at distance t, since the definition of a clique implies that the distance can only be t or $t + 1$.

Below, we will use the notation of Theorem 7.5. From the proof of Theorem 7.5, it is clear that for every Delsarte clique, the equality $\alpha + (|C| - 1)\beta = 0$ holds, i.e., $(\sum_{x \in C} w(x), \sum_{x \in C} w(x)) = 0$. Consequently, $\sum_{x \in C} w(x) = \bar{0}$.

By definition, $E_{\lambda_{min}}(x, y) = (w(x), w(y))$. From Corollary 7.6, we see that $(w(x), w(y))$ depends only on the distance between vertices x and y. Let $(w(x), w(y)) = \gamma_t$ if $d(x, y) = t$. Consider $y \in C_t$. We have equality

$$0 = (w(y), \sum_{x \in C} w(x)) = (w(y), \sum_{x \in C, d(x,y)=t} w(x)) + (w(y), \sum_{x \in C, d(x,y)=t+1} w(x)) =$$

$$= \gamma_t k_t(y) + \gamma_{t+1}(|C| - k_t(y)) = (\gamma_t - \gamma_{t+1})k_t(y) + \gamma_{t+1}|C|,$$

where $k_t(y) = |\{x \in C, d(x, y) = t\}|$. If $\gamma_t - \gamma_{t+1} = 0$, then $\gamma_{t+1} = 0$ and $\gamma_t = 0$. By using (18) and induction, we obtain $\gamma_i = 0$ for all $i < t$. It contradicts Proposition 7.10 ($P_0(\lambda) = 1$). Therefore, $\gamma_t - \gamma_{t+1} \neq 0$ for $t = 0, \dots, d-1$. Then $k_t(y) = \frac{\gamma_{t+1}|C|}{\gamma_{t+1} - \gamma_t}$ is independent of y. Furthermore, the graph has no vertices at distance $d + 1$. Therefore, $\gamma_d k_d(y) = 0$. □

Corollary 7.7. *Let C be a Delsarte clique in a distance-regular graph G with minimal eigenvalue λ_{min}. Then the function $\mathbf{1}_C$ is orthogonal to the eigenspace $X_{\lambda_{min}}$ of G.*

Proof. Since $u_1, \ldots, u_m$ is an orthonormal basis of the eigenspace $X_{\lambda_{min}}$, we have $(\mathbf{1}_C, u_i) = \sum\limits_{x \in C} (w(x))_i$. Then the statement is equivalent to the equality $\sum\limits_{x \in C} w(x) = \bar{0}$. □

Example 7.8. A maximal clique in Q_q^n is isomorphic to the complete graph $K_q = Q_q$. As mentioned above the minimum eigenvalue of Q_q^n is $-n$. Since $|Q_q| = q = 1 + \frac{(q-1)n}{n}$, every maximal cliques in Q_q^n is a Delsarte clique.

7.7 Middle Layer of Boolean Hypercube as a Testing Set

A graph G of diameter d is called *antipodal* if for any vertex $x \in V(G)$, there is a unique vertex $y \in V(G)$ at maximum distance d from x, called the antipode (or opposite vertex) of x. For example, a Boolean n-cube is antipodal since at distance n from a vertex x there is a unique vertex $x \oplus \bar{1}$. Note that q-ary hypercubes for $q > 2$ are not antipodal graphs.

Proposition 7.11. *For a perfect coloring in an antipodal distance-regular graph, the color of any vertex is uniquely determined by the color of its opposite vertex.*

Proof. By Theorem 7.1, a perfect vertex coloring of a graph remains perfect in a graph with a distance equal to the diameter d of the graph. In an antipodal graph, there is exactly one vertex at distance d from each vertex, i.e., the distance-d graph is a perfect matching, and the color of a vertex is determined by the color of its neighbor. □

Recall that the number of units in n-tuple $x \in Q_2^n$ is called the *weigh* of x and denoted by $\mathrm{wt}(x)$. $\{x \in Q_2^n : \mathrm{wt}(x) = t\}$ is a tth layer of Q_2^n. The layer of weight $\frac{n}{2}$ (if n is even) and layers of weight $\frac{n-1}{2}$ and $\frac{n+1}{2}$ (if n is odd) are called the *middle* layers.

Theorem 7.7 ([5])**.** *Let n be odd, f_1 and f_2 be perfect colorings of Q_2^n with the same quotient matrix, and for any vertex $x \in Q_2^n$ of weight $\mathrm{wt}(x) = \frac{n-1}{2}$ (or $\mathrm{wt}(x) = \frac{n+1}{2}$), we have $f_1(x) = f_2(x)$. Then $f_1 = f_2$.*

Proof. Vertices opposite to vertices of weight $\mathrm{wt}(x) = \frac{n-1}{2}$ have weight $\frac{n+1}{2}$. Therefore, by Proposition 7.11 it follows that there is a correspondence φ between the colors such that $f_1(x \oplus \bar{1}) = \varphi(f_1(x)) = \varphi(f_2(x)) = f_2(x \oplus \bar{1})$, where $i = 1, 2$, $\mathrm{wt}(x) = \frac{n+1}{2}$ (or $\mathrm{wt}(x) = \frac{n-1}{2}$).

Consider the coloring $f(x) = \begin{cases} f_1(x), & \mathrm{wt}(x) \le \frac{n+1}{2} \\ f_2(x), & \mathrm{wt}(x) \ge \frac{n-1}{2} \end{cases}$. This definition of f is correct by the previous arguments. The coloring f is perfect with the

same quotient matrix as f_1 and f_2, since in every ball of radius 1 around a vertex of weight t involves only vertices of weights $t-1$ and $t+1$. So, on every radius 1 ball f coincides with f_1 or f_2. From Proposition 7.11 we have $f_1(x) = f(x) = \varphi(f(x \oplus \bar{1})) = \varphi(f_2(x \oplus \bar{1})) = f_2(x)$ and for every $x \in Q_2^n$ with weight $\mathrm{wt}(x) \le \frac{n-1}{2}$. Therefore, $f_2(x) = f_1(x)$ for every $x \in Q_2^n$. $\square$

A *testing set* for a function from a certain class is a subset of its domain such that the function can be completely reconstructed if one know values of the function on this subset.

Here we are discussing only "unconditional" testing sets, when the set should not depend on the function. Sometimes, for example if we need better upper bound on the number of some combinatorial configurations, it is useful to consider "conditional" testing sets, when the choice of the next testing argument depends on the function value at previous testing arguments.

By Theorem 7.7 the middle layer is a testing set for perfect colorings of the Boolean n-cube when n is odd. Moreover, Theorem 7.7 provides best known upper bound on the number of 1-perfect codes in the Boolean n-cube. Since a 1-perfect code is uniquely determined by its intersection with the middle layer, the number of 1-perfect codes is at most $2^{\binom{n}{(n-1)/2}}$. Testing sets for perfect colorings of nonbinary hypercubes will be considered in Section 11.6.

7.8 Problems

35. Prove that for the Krawtchouk-type polynomials P_t of a distance-regular graph G the equality $(x-b_0)\sum\limits_{t=0}^{s} P_t(x) = c_{s+1}P_{s+1}(x) - b_s P_s(x)$ holds, if $s+1$ does not exceed the diameter of G.

36. Prove the equality
$2n\sum\limits_{t=0}^{s}(-1)^{t+1}\binom{n}{t} = (-1)^{s+1}\left((s+1)\binom{n}{s+1} + (n-s)\binom{n}{s}\right)$.

37. Prove that if a graph is the complement of a strongly regular graph and it is connected, then it is strongly regular.

38. Describe all graphs with exactly two eigenvalues of its adjacency matrix.

39. Prove that for the quotient matrix $S[G]$ of each distance-regular graph G, the sequence b_i is decreasing (non-strictly), while the sequence c_i is increasing (non-strictly).

40. Prove that for every distance-regular graph, the equality $|A_2|P_1(-1) = |A_1|P_2(-1)$ holds, where A_i is a sphere of radius i.

41. Prove that for every distance-regular graph, the number of positive values of an eigenfunction with eigenvalue α is not less than $\sum_{t=0}^{d} \max\{P_t(\alpha), 0\}$.

42. Let C be a completely regular code in a distance-regular graph. Prove that the quotient matrix of distance coloring with respect to the code C has eigenvalues that coincide with the eigenvalues of the minimal set of eigensubspaces containing the function $\mathbf{1}_C$.

43. Let f be a perfect coloring of the Boolean cube. Faces of the Boolean n-cube that have the same set of fixed coordinates but completely different fixed coordinate values are called opposite. Prove that if two faces of a Boolean n-cube have the same color composition (i.e., equal numbers of vertices of each color in both faces), then the color composition of the opposite faces them also match.

44. Let $C \subset Q_2^n$ (n is odd) be a completely regular code. Prove that C is completely recoverable from the set of its vertices of weight $\frac{n+1}{2}, \frac{n+1}{2} + 1, \ldots, \frac{n+1}{2} + r$, where r is the covering radius of C.

45. Let G be a distance-regular graph and the characteristic function $\mathbf{1}_C$ of the set $C \subset V(G)$ is the sum of k eigenfunctions of G with k distinct eigenvalues. Prove that 1) if the set C is a color of some perfect coloring, then it has at least k colors; 2) if after $k-1$ steps of the WL algorithm the function $\mathbf{1}_C$ yields a coloring with k colors, then the resulting coloring is perfect.

46. Let G be a distance-regular graph and let C is a color of some equitable partition of G. Prove that for two vertices of any other color C', the number of paths of arbitrary fixed length to vertices from C' is the same. Give an example showing that the coincidence of the path lengths to the vertices of C is not a sufficient condition for the WL algorithm, starting from a 2-color partition $\{C, V(G) \setminus C\}$, to color these vertices by the same color.

47. Let P be an equitable partition of an antipodal distance-regular graph. Prove that for every cell $P_i \in P$ there exists $P_j \in P$ such that if $x \in P_i \in P$ and vertex y is antipodal to x then $y \in P_j$. It is possible that i is equal to j.

8 Automorphisms of Graphs and Perfect Colorings

8.1 Orbit Colorings

Let G be a graph and let H be a subgroup of its automorphism group, i.e., $H \leq Aut(G)$. An *orbit* with respect to H is a minimal set with respect to inclusion $O \subset V(G)$ such that $\pi(O) = O$ for any automorphism $\pi \in H$.

Since H is a subgroup, each orbit O coincides with the image

$$H(v) = \{\pi(v) \mid \pi \in H\}$$

of any element $v \in O$. Indeed, if $v', v \in O$ then $v' = \pi_1 \circ \cdots \circ \pi_k(v)$, where $\pi_1, \ldots, \pi_k \in H$ and, consequently, $\pi_1 \circ \cdots \circ \pi_k \in H$. So, the vertex set of a graph is partitioned into disjoint orbits.

Proposition 8.1. *Let $P = \{O_1, \ldots, O_k\}$ be a partition of $V(G)$ into orbits with respect to the subgroup H. Then partition P is equitable.*

Proof. Let elements v and v' be contained in the same orbit. Then $v' = \pi(v)$ for some automorphism $\pi \in H$. Consider an arbitrary vertex u adjacent to v. Then, by the definition of an automorphism, the vertex $u' = \pi(u)$ is adjacent to the vertex $\pi(v)$. Therefore, vertices u and u' belong to the same orbit. The mapping π is bijective, therefore, the color composition of the neighborhoods of vertices v and v' coincide. □

The perfect coloring defined in Proposition 8.1 will be called an *orbit coloring*.

Corollary 8.1. *Let $C \subset V(G)$ be a transitive code in graph G. Then C is a color of some orbit coloring.*

Example 8.1. Consider a graph whose vertices are the numbers $0, \ldots, 8$, and vertices x and y are connected by an edge if $(x-y) \mod 9 \in \{\pm 1, \pm 2\}$. It is easy to see that the mapping $\varphi(x) = (x+3) \mod 9$ is an automorphism of the graph, and generates the subgroup $H = \{\varepsilon, \varphi, \varphi^2\}$. Here and throughout, ε is the identity element of the group (the identity permutation). With respect to H, the graph is partitioned into three orbits, according to the residue modulo 3. The coloring $h(x) = x \mod 3$ is perfect with quotient matrix $\begin{pmatrix} 0 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{pmatrix}$.

Describing all orbital colorings reduces to finding the group of graph automorphisms. Isometries (automorphisms) of hypercubes are described by Markov's theorem. To state it, we need some definitions.

defined by the equality $\overline{\sigma}(x_1, x_2, \ldots, x_n) = (\sigma_1 x_1, \sigma_2 x_2, \ldots, \sigma_n x_n)$, where each σ_i is a permutation of the elements of the set Q_q.

A *parastrophy* is an isometry of Q_q^n defined by the equality $\tau(x_1, x_2, \ldots, x_n) = (x_{\tau 1}, x_{\tau 2}, \ldots, x_{\tau n})$, where τ is a permutation of the set $\{1, \ldots, n\}$.

Theorem 8.1 (Markov [100], [106]). *Any isometry of a hypercube is the composition of an isotopy and a parastrophy. More precisely, the full automorphism group of the Hamming graph $H(n, q)$ is the wreath product of the symmetric group S_q by the symmetric group S_n, which is isomorphic to the semidirect product $\mathbb{Z}_2^n \rtimes S_n$ for $q = 2$.*

Some isometries of Q_q^n can be viewed as affine transformations in a vector space over a finite field $GF(q)$, if q is a prime power. In this case we can identify Q_q and $GF(q)$ and regard Q_q^n as an n-dimensional vector space over $GF(q)$. Consider a linear transformation of the hypercube whose matrix has exactly one 1 in each row and column, and the remaining elements are zero. Clearly, such a linear transformation is a parastrophy. Consider a translation map that adds a fixed vector to each vertex of the hypercube. Clearly, such affine transformation is an isotopy. It can be shown (see Problem 50) that for $q = 2, 3$, all isometries of the hypercubes Q_q^n are affine transformations.

A group action on a graph is called *regular* if for every ordered pair of vertices of the graph there is a unique element of the group that maps the first vertex to the second. A graph on q vertices such that a cyclic subgroup $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ of its automorphism group acting regularly on its vertices, is called *circulant*. The graph considered in Example 8.1 is circulant.

A description of perfect colorings for some circulant graphs with two colors can be found in the papers [75] and [114].

A vertex-transitive graph has exactly one orbit with respect to its automorphism group. Transitive graphs with a subgroup-rich automorphism group admit many orbit colorings.

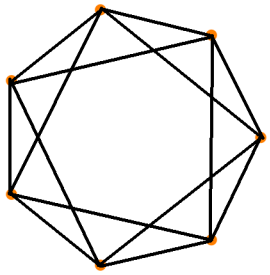
8.2 Perfect Colorings of Cayley Graphs

The main examples of transitive graphs are Cayley graphs.

Let Gr be a group and let $A \subset Gr$ be a *set of generators* such that $A^{-1} = A$ (otherwise we obtain a directed graph), $\varepsilon \notin A$ (otherwise we get loops). A *Cayley graph* $Cay(Gr, A)$ is a graph whose vertices are elements of

the group, and two vertices $x, y \in Gr$ are adjacent by an edge when $y = xa$ for some $a \in A$.

The elements $g \in Gr$ define automorphisms φ_g of the graph $Cay(Gr, A)$ by the rule $\varphi_g(x) = gx$. The group Gr is a subgroup of the automorphism group of $Cay(Gr, A)$. Thus, every Cayley graph is vertex-transitive. For each generator set A, the Cayley graph $Cay(\mathbb{Z}_q, A)$ is circulant.



The figure shows the graph $Cay(\mathbb{Z}_7, A)$, where $A = \{\pm 1, \pm 2\}$.

It is easy to show that the Cayley graph of the Cartesian square of $Gr \times Gr$ with generator set $A \times \{\varepsilon\} \cup \{\varepsilon\} \times A$ is the Cartesian product of the Cayley graphs $Cay(Gr, A) \square Cay(Gr, A)$. The complete graph Q_q can be viewed as the Cayley graph of the group $\mathbb{Z}_q$ with generator set consisting of all nonzero elements of the group. The hypercube Q_q^n can be viewed as the Cayley graph $Cay(\mathbb{Z}_q^n, A)$, where A is the set of n-tuples containing exactly one nonzero element.

A special case of the Cayley graph arises when the generator set $A = A^{-1}$ as the set of representatives of cosets of some subgroup H, i.e., $A \simeq (Gr/H) \backslash \{\varepsilon\}$. Then, any element $g \in Gr$ of the group is uniquely representable as $g = ha$ or $g = h \in H$, i.e., each vertex of the graph $Cay(Gr, A)$ is adjacent to exactly one element of H, or itself belongs to the subgroup H. Thus, the set H forms a 1-perfect code in $Cay(Gr, A)$. As proved in the statement below, H can be any normal subgroup. A *normal* subgroup is a subgroup of H for which $gH = Hg$ for any $g \in Gr$.

Proposition 8.2. *Let H be a normal subgroup of Gr. Then, from the cosets of H, we can choose a set of representatives of A satisfying the property $A = A^{-1}$.*

Proof. Since H is a normal subgroup, the equality $Ha = Hb$ implies the equality $Ha^{-1} = Hb^{-1}$ ($b = ha \Rightarrow b^{-1} = a^{-1}h^{-1} = h'a^{-1}$), which means that elements of A can be chosen in pairs $\{a, a^{-1}\}$ when a and a^{-1} belong to different cosets of H. If a pair of mutually inverse elements a and a^{-1} belongs to the same coset, then it contains an element of order $b^2 = \varepsilon$, which can be chosen in the set A. Indeed, let $a^{-1} = ha$ for some $h \in H$, i.e.,

$\varepsilon = ha^2$. Consequently, a^2 and all even powers of a are contained in H, and all odd powers are contained in the coset Ha. Since the group H is finite, there exists a minimal integer $s > 0$ such that $a^{2s} = \varepsilon$. Moreover, the parity of s contradicts the condition that a and a^{-1} belong to different cosets. Therefore, $a^s \in Ha$. □

Example 8.2. Consider the symmetric group S_n and a subgroup H consisting of permutations fixing some element. Without loss of generality, we can assume that $\pi(1) = 1$ for all $\pi \in H$. Let $A = (S_n/H)\backslash\{\varepsilon\}$. It is easy to see that $A = \{(1i) \mid i = 2, \ldots, n\}$ and $H \simeq S_{n-1}$. The graph $Cay(S_n, A)$ is called a *star graph*. The subgroup H forms a 1-perfect code in the star graph.

Other sufficient conditions for a subgroup of a given group to be a perfect code in a Cayley graph are studied in [68]. Examples of non-group 1-perfect codes in star graphs can be found in [107].

A *homomorphism* is a mapping $\varphi : Gr_1 \to Gr_2$, satisfying the equality $\varphi(x * y) = \varphi(x) \circ \varphi(y)$ for any elements $x, y \in Gr_1$. Here $*$ and $\circ$ are group operations in Gr_1 and Gr_2, respectively.

Proposition 8.3. *Let Gr_1 and Gr_2 be some groups, and there is a homomorphism $\varphi : Gr_1 \to Gr_2$, which is bijective on the generator set $A \subset Gr_1$. Then φ is a covering of the graph $Cay(Gr_2, \varphi(A))$ by the graph $Cay(Gr_1, A)$.*

Proof. Let $g \in Gr_1$. Then $\{ga : a \in A\} = S_1^1(g)$. From the definition of homomorphism, we have $\varphi(ga) = \varphi(g)\varphi(a)$. Thus, $\varphi(S_1^1(g)) = S_1^2(\varphi(g))$, and the mapping φ is bijective on $S_1^1(g)$ for any $g \in Gr_1$ by the assumption. □

The mapping $f : Gr_1 \times Gr_2 \to Gr_1$, defined by $f((a, b)) = a$ is a natural homomorphism from the direct product $Gr_1 \times Gr_2$ to a factor. Let us consider other examples.

Example 8.3. The mapping $\varphi(n) = n \,(\mathrm{mod}\, 4)$ is a homomorphism of the group $\mathbb{Z}$ to the group $\mathbb{Z}_4$. Then the mapping $\varphi : Cay(\mathbb{Z}, \pm 1) \to Cay(\mathbb{Z}_4, \pm 1)$ is a covering.

The groups $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are not isomorphic. However, their Cayley graphs (with any two generators) are both isomorphic to the square $Q_2 \square Q_2$. The isomorphism $\iota : Cay(\mathbb{Z}_2 \times \mathbb{Z}_2, \{(0,1), (1,0)\}) \leftrightarrow Cay(\mathbb{Z}_4, \pm 1)$ such that $\iota((0,0)) = 0$ is called the *Gray map*.

Consider the group $\mathbb{Z}_4^n$. Let $e_i = (0, \ldots, \underset{i}{1}, \ldots, 0)$. We have graph isomorphisms $Cay(\mathbb{Z}_4^n, \{\pm e_i\}) \leftrightarrow Cay(\mathbb{Z}_2^{2n}, \{e_i\}) \leftrightarrow Q_2^{2n}$. From Proposition 5.4

and Example 8.3 it follows that there exists a covering of the graph Q_2^{2n} by the graph $Cay(\mathbb{Z}^n, \{\pm e_i\})$ of the n-dimensional rectangular grid. Consequently, from any perfect coloring of the Boolean $2n$-cube, one can obtain a perfect coloring of the n-dimensional rectangular grid with the same quotient matrix.

Example 8.4. Consider the covering ψ of the graph Q_5 by a two-dimensional rectangular grid $(\mathbb{Z}^2, \{(\pm 1, 0), (0, \pm 1)\})$, defined by the formula $\psi(x, y) = x + 2y(\mod 5)$. Every coloring of the complete graph Q_5 is perfect. Hence, the two-dimensional rectangular grid can be colored perfectly with the following quotient matrices $\begin{pmatrix} 0 & 4 \\ 1 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$, $\begin{pmatrix} 0 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 2 & 1 \end{pmatrix}$.

Consider the *Shrikhande graph*

$$Sh = Cay(\mathbb{Z}_4^2, \{(1, 0), (-1, 0), (0, 1), (0, -1), (1, 1), (-1, -1)\}).$$

We define the mapping

$$\theta : V(Cay(\mathbb{Z}_4^3, \{\pm e_i\})) \to V(Sh).$$

by the equality $\theta(x_1e_1 + x_2e_2 + x_3e_3) = x_1(1, 0) + x_2(0, 1) + x_3(1, 1)$. To verify that θ is a covering, it suffices to consider the image of a neighborhood of one point, since both graphs are transitive. As noted above, $Cay(\mathbb{Z}_4^3, \{\pm e_i\})$ is isomorphic to Q_2^6. Therefore, there is a covering of the Shrikhande graph by the Boolean 6-cube. It is not difficult to find a perfect 2-coloring of the Shrikhande graph with quotient matrix $\begin{pmatrix} 1 & 5 \\ 3 & 3 \end{pmatrix}$.

Then $\mathbb{Z}_2^6$ admits a perfect 2-coloring with the same quotient matrix. This coloring was first found by Tarannikov. It is an example of a coloring that attains the Fon-Der-Flaass bound of correlation immunity (see Section 10.8).

Example 8.5. Consider the symmetric group S_n and the generator set T_n consisting of all transpositions. $Cay(S_n, T_n)$ is called the *transposition graph*. Choose an arbitrary subset $\{a_1, \ldots, a_k\}$ of cardinality $k, 1 < k < n$, in the domain of permutations. We define a mapping $\nu : V(Cay(S_n, T_n)) \to V(J(n, k))$ by the following rule. An n-tuple $\nu(\sigma)$ contains 1 exactly at the positions $\sigma(a_i)$, $i = 1, \ldots, k$, $\sigma \in S_n$. It is easy to see that ν covers the Johnson graph (see Example 7.3) with additional $\binom{k}{2} + \binom{n-k}{2}$ loops at each vertex of the Johnson graph.

8.3 Problems

48. Prove that the k-dimensional rectangular grid covers Q_3^k.

49. Prove that the k-dimensional rectangular grid has a 1-perfect code.

50. Using Markov's theorem prove that for $q = 2$ and $q = 3$, all isometries of the hypercubes Q_q^n are affine transformations.

51. Let q be a prime power and let A be a matrix of size $k \times n$ over the field $GF(q)$. Define the color class of color $b \in Q_q^n$ as $\{x \in Q_q^n : Ax = b\}$. Prove that this coloring of Q_q^n is perfect.

52. Let q be a prime number. Prove that there exists a covering $\varphi : Cay(\mathbb{Z}_q^{\frac{n(q-1)}{2}}, \{\pm e_i : i = 1, \ldots, (q-1)/2\}) \to Q_q^n$.

53. Consider the symmetric group S_n and the generator set $A \subset S_n$, $A^{-1} = A$, such that $|A| = n$. For each permutation $\pi \in A$, define the permutation matrix P_π, where $P_\pi(i,j) = 1$ if $\pi(i) = j$, and $P_\pi(i,j) = 0$ otherwise. Consider a coloring of $Cay(S_n, A)$ with n colors according to the rule: a permutation $\sigma \in S_n$ has color i if $\sigma(0) = i$. Prove that the resulting coloring is perfect with quotient matrix $S = \sum_{\pi \in A} P_\pi$.

54. Prove that for $n \equiv 1, 3 \pmod 6$ in the permutation graph $Cay(S_n, T_n)$ (see Example 8.5) there exist perfect 2-colorings with quotient matrix $S = \begin{pmatrix} 3 + \binom{n-3}{2} & 3(n-3) \\ 3 & 3(n-3) + \binom{n-3}{2} \end{pmatrix}$.

9 Fourier Transform

9.1 Characters of Abelian Groups

We denote by $\mathbb{V}(K) \stackrel{\text{def}}{=} \{f : K \to \mathbb{C}\}$ the set of functions acting from the group $(K, \circ)$ to the field of complex numbers.

A mapping $\phi \in \mathbb{V}(K)$ is called a *character* of a group if it satisfies the following conditions:

$$\forall x \in K \quad |\phi(x)| = 1; \qquad \forall x, y \in K \quad \phi(x \circ y) = \phi(x) \cdot \phi(y). \tag{19}$$

Thus, any character is a homomorphism from the group K to the group of points on the unit circle $T = \{x \in \mathbb{C} : \quad |x| = 1\}$ with the operation of multiplication. The group T is isomorphic to the unitary group U(1) and the special orthogonal group SO(2).

Let e be an identity element of the group, then $\phi(x) = \phi(ex) = \phi(e)\phi(x)$. So, $\phi(e) = 1$. For a finite group the condition $|\phi(x)| = 1$ is actually redundant, since every element of the group has finite order. Then from $mx = e$ it follows $\phi(x)^m = \phi(mx) = 1$.

We show that the characters form an abelian group, which we will denote by $X(K)$. Define the product of characters by the equality

$$(\phi_1 \cdot \phi_2)(x) = \phi_1(x)\phi_2(x).$$

Let us verify that the product of characters $\phi_1, \phi_2 \in X(K)$ is a character:

$$|(\phi_1 \cdot \phi_2)(x)| = |\phi_1(x)||\phi_2(x)| = 1;$$

$$(\phi_1 \cdot \phi_2)(x \circ y) = \phi_1(x \circ y)\phi_2(x \circ y) = \phi_1(x)\phi_1(y)\phi_2(x)\phi_2(y) = (\phi_1 \cdot \phi_2)(x)(\phi_1 \cdot \phi_2)(y).$$

Associativity and commutativity of the multiplication of characters follow from the associativity and commutativity of the multiplication of complex numbers. The identity of the group $X(K)$ is the identically one function $\mathbf{1}$, where $\mathbf{1}(x) = 1$ for every $x \in K$. The inverse element is the character $(\phi)^{-1} = \bar{\phi}$, which is the complex conjugate of the original one. The character group $X(K)$ is called the dual group of K.

Henceforth we will consider only abelian groups $(K, +)$, i.e., we assume the group operation $+$ to be commutative. Consider the characters of the character group $X(K)$. Define the character $\Theta_x \in X(X(K))$ by the equality $\Theta_x(\phi) = \phi(x)$ for all $\phi \in X(K)$. Note that characters do not distinguish between conjugate elements of the group $\phi(a^{-1}ba) = \phi(b)$. However, for a finite abelian group (more generally, a locally compact abelian group) it is possible to prove that for every pair of elements $x, y \in K$ there exists $\phi \in X(K)$ such that $\phi(x) \neq \phi(y)$. Therefore, $x \neq y \Leftrightarrow \Theta_x \neq \Theta_y$ and K is a subgroup of the group $X(X(K))$.

Theorem 9.1 (Pontryagin–van Kampen duality theorem [111], [123]). *If K is a locally compact commutative group, then $K \simeq X(X(K))$.*

Explanation of the term "locally compact". A topological group is a group equipped with a topology for which multiplication and inversion are continuous. A group equipped with such a topology is called a topological group. The characters of a topological group are only the continuous (with respect to this topology) functions satisfying conditions (19). A topological group is locally compact if every element of the group has a compact neighborhood. In the case of any finite group and the group $\mathbb{Z}$, the discrete topology possesses the required properties. For $\mathbb{R}$ and $\mathbb{C}$, the standard topology given by the absolute value of the number is suitable.

In the case when $K \simeq X(X(K))$, one can introduce an operator $\Phi : K \times X(K) \to \mathbb{C}$ such that for a fixed $y \in X(K)$ the function $\Phi(x, y)$ is a character of the group K, and for a fixed $x \in K$ it is a character of the group $X(K)$.

Example 9.1. Consider the group $(\mathbb{R}, +)$. As mentioned above, it is locally compact with respect to the natural topology defined by the absolute value of a number. It is easy to check that functions of the form $\phi_y(x) = e^{ixy}$, $y \in \mathbb{R}$, satisfy conditions (19). Indeed, $\phi_y(x_1 + x_2) = e^{i(x_1+x_2)y} = e^{ix_1y} \cdot e^{ix_2y} = \phi_y(x_1) \cdot \phi_y(x_2)$, $|\phi_y(x)| = |e^{ixy}| = 1$. It can be shown that there are no other continuous functions on $\mathbb{R}$ satisfying conditions (19).

From the equality $\phi_{y_1}(x) \cdot \phi_{y_2}(x) = e^{ixy_1} \cdot e^{ixy_2} = e^{ix(y_1+y_2)} = \phi_{y_1+y_2}(x)$ it follows that $X(\mathbb{R}, +) \simeq (\mathbb{R}, +)$.

Example 9.2. Consider the group $(\mathbb{Z}, +)$, as a subgroup of $(\mathbb{R}, +)$. We have $\phi_y(n) = e^{iyn}$, $n \in \mathbb{Z}$. Since $\phi_{y+2\pi}(n) = \phi_y(n)$, to each character ϕ_y one can assign a point on the unit circle having angle y. Using the natural isomorphism $\phi_y \leftrightarrow e^{iy}$, $y \in \mathbb{R}$, we obtain that $X(\mathbb{Z}, +) \simeq U(1) \simeq SO(2)$. Strictly speaking, we have only shown that $U(1) \leq X(\mathbb{Z}, +)$. Since $X(U(1)) \simeq \mathbb{Z}$ by the duality theorem, in both cases we have an isomorphism. It is clear that the character group will not change (up to equivalence) upon changing the argument y; therefore, one can define $\phi_z(n) = e^{2\pi izn}$, $z \in [0, 1)$. By the duality theorem we have $X(U(1)) \simeq (\mathbb{Z}, +)$. Indeed, if we consider the operators $\phi_z(n)$ as functions of the variable z, we have the equality $\phi_z(n_1)\phi_z(n_2) = \phi_z(n_1 + n_2)$.

Example 9.3. Consider the cyclic group $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$. Now we need characters of the group $(\mathbb{Z}, +)$ that do not distinguish between elements that are comparable modulo q, i.e., such that $\phi_y(n+q) = \phi_y(n)$ for any $n \in \mathbb{Z}$. Again we seek characters in the form $\phi_y(n) = e^{iyn}$. Then $y(n + q) = yn + 2\pi k$, i.e., $y = \frac{2\pi k}{q}$. Put $\xi = e^{2\pi i/q}$; then the characters of the group $\mathbb{Z}_q$ can be represented in the form $\phi'_k(n) = \xi^{n \cdot k} = e^{\frac{2\pi ink}{q}}$. Since $\phi'_{k_1}(n) \cdot \phi'_{k_2}(n) = e^{\frac{2\pi in}{q}(k_1+k_2)} = e^{\frac{2\pi in}{q}((k_1+k_2) \mod q)} = \phi'_{(k_1+k_2) \mod q}(n)$, we have $X(\mathbb{Z}_q) \simeq \mathbb{Z}_q$.

Proposition 9.1. *If ϕ is a character of a finite group K, then the equalities*

$$\sum_{x \in K} \phi(x) = 0, \text{ if } \phi \neq \mathbf{1};$$

$$\sum_{x \in K} \phi(x) = |K|, \text{ if } \phi = \mathbf{1}$$

hold.

Proof. For any $a \in K$ the equalities

$$\sum_{x \in K} \phi(x) = \sum_{x \in K} \phi(x + a) = \phi(a) \sum_{x \in K} \phi(x)$$

hold. If $\phi \not\equiv 1$, then there exists $a \in K$ for which $\phi(a) \neq 1$. Hence it follows that $\sum\limits_{x \in K} \phi(x) = 0$. Otherwise $\sum\limits_{x \in K} \phi(x) = |K|$. □

From Theorem 9.1 and Proposition 9.1 we have

Corollary 9.1. *For a finite abelian group K, the equalities*

$$\sum_{\phi \in X(K)} \phi(x) = |X(K)|, \quad \text{if } x \text{ is the identity element of the group } K;$$
$$\sum_{\phi \in X(K)} \phi(x) = 0 \qquad \text{otherwise}$$

hold.

Proposition 9.2. *Let $\xi = e^{2\pi i/q}$, $m = 1, \ldots, q-1$. Then $\sum\limits_{k=0}^{q-1} \xi^{mk} = 0$. If q is a prime number and $\sum\limits_{k=0}^{q-1} \alpha_k \xi^{mk} = 0$ then $\alpha_k = \alpha_0$ for all k.*

Proof. The first statement is a special case of Proposition 9.1 for $\mathbb{Z}_q$. It also follows from the equations

$$0 = \xi^{mq} - 1 = (\xi^m - 1) \sum_{k=0}^{q-1} \xi^{mk}.$$

The second one follows from the well-known property that ξ^m is not a root of any equation of degree less than $q - 1$. □

In $\mathbb{V}(K)$ one can define a scalar product. In the case of a finite group K, $\mathbb{V}(K)$ is a finite-dimensional space and the scalar product in $\mathbb{V}(K)$ can be defined by the equality $(f, g) = \sum\limits_{x \in K} f(x)\overline{g(x)}$.

Proposition 9.3. *The set of characters of a finite abelian group forms an orthogonal basis in the space $\mathbb{V}(K)$.*

Proof. We begin by proving the orthogonality of the characters. Let $a \in K$. From the definition of characters and the invariance of the inner product under shifts of the argument, we have the equalities

$(\phi_1, \phi_2) = \sum\limits_{x \in K} \phi_1(x)\overline{\phi_2(x)} = \sum\limits_{x \in K} \phi_1(x+a)\overline{\phi_2(x+a)} = \phi_1(a) \cdot \overline{\phi_2(a)} \cdot (\phi_1, \phi_2)$. If $\phi_1 \neq \phi_2$, then there exists $a \in K$ such that $\phi_1(a)\overline{\phi_2(a)} \neq 1$. Consequently $(\phi_1, \phi_2) = \sum\limits_{x \in K} \phi_1(x) \cdot \overline{\phi_2(x)} = 0$.

Now we prove that the system of characters is complete. We have the inequality $\dim \mathbb{V}(K) = |K| \geq |X(K)|$. The reverse inequality follows from the Pontryagin–van Kampen duality theorem. Indeed, consider the characters on the group $X(K)$: $\dim \mathbb{V}(X(K)) = |X(K)| \geq |X(X(K))| = |K|$, since $X(X(K)) \simeq K$. Thus, the number of characters coincides with the dimension of the space $\mathbb{V}(K)$. □

Corollary 9.2. *For a finite abelian group K we have $|X(K)| = |K|$.*

As can be seen from the proof, the characters of any, in particular non-abelian, group are orthogonal. But in the non-abelian case they do not form a basis. Note that if the constructed set of characters constitutes a basis of the space $\mathbb{V}(K)$, then there are no other characters of the group K. It follows that in Examples 9.2 and 9.3 all characters of the groups $U(1)$ and $\mathbb{Z}_q$ are defined.

Proposition 9.4. *Let K_1 and K_2 be finite abelian groups and $K = K_1 \times K_2$ be the direct product of the groups. Then $X(K) = X(K_1) \times X(K_2)$.*

Proof. Consider the characters $\phi_{z_1} \in X(K_1)$, $\phi_{z_2} \in X(K_2)$. Their product $(\phi_{z_1} \cdot \phi_{z_2})(x_1, x_2) \stackrel{\text{def}}{=} \phi_{z_1}(x_1) \cdot \phi_{z_2}(x_2)$ is a character of the group K. Conditions (19) are easily verified directly. The number of constructed characters is equal to $|X(K_1)||X(K_2)|$. It coincides with the cardinality of the group $X(K)$ equal to $|K_1||K_2|$. □

It is known that any finite abelian group K is isomorphic to the Cartesian product (direct sum) of cyclic groups $\mathbb{Z}_q$, $q \in \mathbb{N}$. Then from Proposition 9.4 and Example 9.3 it follows that $K \simeq X(K)$ for any finite abelian group K.

Proposition 9.5. *Let K_1 be a subgroup of a finite abelian group K. Then for any character $\phi \in X(K_1)$ there exists a character $\widetilde{\phi} \in X(K)$ such that $\phi = \widetilde{\phi}|_{K_1}$.*

Proof. Consider the factor group K/K_1. Each element $x \in K$ can be uniquely represented as a sum $x = x_1 + x_2$, where $x_1 \in K_1$, $x_2 \in K_2$, and the group K_2 is isomorphic to the factor group K/K_1. Define $\widetilde{\phi}(x) = \phi(x_1)$. It is easy to verify that $\widetilde{\phi}$ satisfies condition (19). □

Let $K_1 \subset K$. Define the subgroup $K_1^\perp$ in $X(K)$ by the equality

$$K_1^\perp = \{z \in X(K) \mid \phi_z(x) = 1, \text{ if } x \in K_1\}.$$

If a finite abelian group K is representable as a direct product of groups $K = K_1 \times K_2$, then one can consider the subgroups $K_1 \simeq K_1 \times \{e_2\}$ and $K_2 \simeq \{e_1\} \times K_2$ as subsets of K, where e_1 and e_2 are the identity elements of the groups K_1 and K_2. From Proposition 9.4 we have $X(K) = X(K_1) \times X(K_2)$. It is easy to see that in this case $K_1^\perp \simeq X(K_2)$. Let us prove a similar fact in a slightly more general case.

Proposition 9.6. *Let K_1 be a subgroup of a finite abelian group K. Then $K_1^\perp \simeq X(K/K_1)$.*

Proof. Let K_2 be a subgroup of K such that $K_2 \simeq K/K_1$ and each element $x \in K$ can be uniquely represented as a sum $x = x_1 + x_2$, where $x_1 \in K_1$, $x_2 \in K_2$. For every $\phi \in K_1^\perp$ we have $\phi(x_1 + x_2) = \phi(x_2)$, i.e., there exists a homomorphism $K_1^\perp \to X(K_2)$.

For every $\phi \in X(K_2)$ define $\widetilde{\phi}(x) = \phi(x_2)$. By Proposition 9.5 we have an injective map $X(K_2) \to K_1^\perp$ acting as $\phi \to \widetilde{\phi}$. Thus, it is an isomorphism. □

Corollary 9.3. *Let K_1 be a subgroup of a finite abelian group K. Then $|K_1^\perp| \cdot |K_1| = |K|$.*

Example 9.4. As shown in Example 9.3, the characters of the group $\mathbb{Z}_q$ are the functions $\phi_y(x) = \xi^{x \cdot y}$, where $\xi = e^{2\pi i/q}$ and $x, y \in \mathbb{Z}_q$. Then the characters of the group $\mathbb{Z}_q^n$ are the functions $\xi^{\langle x,y \rangle}$, where $x, y \in \mathbb{Z}_q^n$ and $\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n \mod q$.

Note that in the character formula $\xi^{\langle x \cdot y \rangle}$, the inner product $\langle x \cdot y \rangle = x_1 y_1 + \cdots + x_n y_n$ can be considered both modulo q and in integers, since $\xi^a = \xi^{a \mod q}$.

Let K be a finite abelian group. $A \subset K$, $0 \notin A$, $-A = A$. Recall that $\mathrm{Cay}(K, A)$ is the Cayley graph of the group K with generating set A.

Proposition 9.7 ([8])**.** *A character ϕ of the group K is an eigenvector of the adjacency matrix M of the graph $\mathrm{Cay}(K, A)$ with eigenvalue $\sum\limits_{a \in A} \phi(a)$.*

Proof. $(M\phi)(x) = \sum\limits_{a \in A} \phi(x + a) = \sum\limits_{a \in A} \phi(x)\phi(a) = \phi(x) \left(\sum\limits_{a \in A} \phi(a) \right)$. □

Corollary 9.4. *Every eigenspace of the adjacency matrix of the graph* $\mathrm{Cay}(K, A)$ *has a basis consisting of characters of the group* K.

Proposition 9.8. *A character* ϕ *of the group* K *is a perfect coloring (here we use complex numbers as the colors) of the graph* $\mathrm{Cay}(K, A)$.

Proof. A vertex of color $\phi(x)$ is adjacent to vertices of colors $\{\phi(x+a) \mid a \in A\} = \{\phi(x)\phi(a) \mid a \in A\}$. Therefore, if the colors of two vertices coincide, i.e., $\phi(x_1) = \phi(x_2)$, then the color composition of their neighborhoods also coincides. □

Corollary 9.5. *The characters* ϕ_z *of the group* $\mathbb{Z}_q^n$ *are perfect colorings of the hypercube* Q_q^n *with quotient matrix depending only on* $\mathrm{wt}(z)$.

9.2 Krawtchouk Polynomials

The hypercube Q_q^n is a Cayley graph of the group $\mathbb{Z}_q^n$ with the generating set A consisting of tuples of weight 1. We find the eigenvalues corresponding to the characters $\phi_z(x) = \xi^{\langle x \cdot z \rangle}$, where $\xi = e^{2\pi i/q}$. Recall that $\mathrm{wt}(z) = d(z, \bar{0}) = |\operatorname{supp}(z)|$ is the weight of the tuple z. We have the equalities

$$\sum_{a \in A} \phi_z(a) = \sum_{a \in A} \xi^{<a,z>} = \sum_{\substack{a \in A \\ \operatorname{supp}(z) \cap \operatorname{supp}(a) = \varnothing}} \xi^{<a,z>} + \sum_{\substack{a \in A \\ \operatorname{supp}(z) \cap \operatorname{supp}(a) \neq \varnothing}} \xi^{<a,z>}.$$

We compute the terms separately. Any element $a \in A$ has the form $a = (0, \ldots, 0, a_i, 0, \ldots, 0)$ for some $a_i = b \in \mathbb{Z}_q$, $b \neq 0$. For any fixed $z \in \mathbb{Z}_q$, we represent both sums as

$$\sum_{\substack{a \in A \\ \operatorname{supp}(z) \cap \operatorname{supp}(a) = \varnothing}} \xi^{<a,z>} = \sum_{i : z_i = 0} \sum_{a \in A, a_i \neq 0} \xi^{<a,z>};$$

$$\sum_{\substack{a \in A \\ \operatorname{supp}(z) \cap \operatorname{supp}(a) \neq \varnothing}} \xi^{<a,z>} = \sum_{i : z_i \neq 0} \sum_{a \in A, a_i \neq 0} \xi^{<a,z>}.$$

For a fixed i we have

$$\sum_{a \in A, a_i \neq 0} \xi^{<a,z>} = \sum_{b \in \mathbb{Z}_q \setminus \{0\}} 1 = q - 1, \text{ if } z_i = 0; \tag{20}$$

$$\sum_{a \in A, a_i \neq 0} \xi^{<a,z>} = \sum_{b \in \mathbb{Z}_q \setminus \{0\}} \xi^{z_i b} = -1, \text{ if } z_i \neq 0;$$

where the last equality follows from Proposition 9.1. Then

$$\sum_{a\in A}\phi_z(a) = (n-\mathrm{wt}(z))(q-1) + (-1)\,\mathrm{wt}(z) = n(q-1) - \mathrm{wt}(z)q.$$

Thus, the eigenvalues of the hypercube Q_q^n are the numbers $-n, -n+q, \ldots, n(q-1)$. This agrees with Corollary 5.1.

Now we compute the values of the Krawtchouk polynomials $P_t[n,q]$ for hypercubes Q_q^n. From Proposition 7.3 we have

$$P_t[n,q](n(q-1)-\mathrm{wt}(z)q) = \phi_z(\bar{0})\left(\sum_{x:\mathrm{wt}(x)=t}\phi_z(x)\right).$$

Without loss of generality, we assume that $z=(1,\ldots,1,0,\ldots,0)$, $\mathrm{wt}(z)=k$. Divide the set of vectors of weight t into groups, each containing vectors with the same support. Suppose that in some group, exactly m nonzero coordinates of the vectors lie in the 1-st through k-th positions. From formulas (20), the sum $\sum_x \phi_z(x)$ over all vectors x from such a group is equal to

$$(q-1)^{t-m}\sum_x \xi^{x_{i_1}+\cdots+x_{i_m}} =$$

$$= (q-1)^{t-m}\left(\sum_{x_{i_1}\neq 0}\xi^{x_{i_1}}\right)\cdots\left(\sum_{x_{i_m}\neq 0}\xi^{x_{i_m}}\right) = (-1)^m(q-1)^{t-m}.$$

For each m, the number of such groups is equal to $\binom{n-k}{t-m}\binom{k}{m}$. Then the equality

$$P_t[n,q](n(q-1)-kq) = \sum_{m=0}^{t}(-1)^m(q-1)^{t-m}\binom{n-k}{t-m}\binom{k}{m},$$

holds, where for $k<m$ or $n-k<t-m$ the corresponding terms are equal to zero.

Further, we find the generating function for the Krawtchouk polynomials. Denote by y an independent variable. For any $x\in Q_q^n$, the equality $y^{\mathrm{wt}(x)} = y^{\mathrm{wt}(x_1)}\cdots y^{\mathrm{wt}(x_n)}$ holds. As before, we assume that $z=(1,\ldots,1,0,\ldots,0)$, $\mathrm{wt}(z)=k$. Using Proposition 7.3 and formulas (20), we obtain the equalities

$$\sum_{x\in Q_q^n}\phi_z(x)y^{\mathrm{wt}(x)} = \sum_{t=0}^{n}y^t\left(\sum_{x:\mathrm{wt}(x)=t}\phi_z(x)\right) = \sum_{t=0}^{n}y^tP_t[n,q](n(q-1)-\mathrm{wt}(z)q);$$

$$\sum_{x\in Q_q^n}\phi_z(x)y^{\mathrm{wt}(x)}=\sum_{x\in Q_q^n}\xi^{x_1}\cdots\xi^{x_k}y^{\mathrm{wt}(x_1)}\cdots y^{\mathrm{wt}(x_n)}=$$

$$=\left(\prod_{i=1}^{k}\sum_{x_i\in Q_q}\xi^{x_i}y^{\mathrm{wt}(x_i)}\right)\left(\prod_{i=k+1}^{n}\sum_{x_i\in Q_q}y^{\mathrm{wt}(x_i)}\right)=(1-y)^k(1+(q-1)y)^{n-k}.$$

Thus,

$$(1+(q-1)y)^{n-k}(1-y)^k=\sum_{t=0}^{n}P_t[n,q](\lambda_k)y^t, \tag{21}$$

where $\lambda_k=n(q-1)-kq$.

Let us express the powers of the adjacency matrix in terms of the Krawtchouk polynomials. Let M be the adjacency matrix of a distance-regular graph. As noted above, $(M^r)_{ij}$ is the number of walks of length r between vertices x_i and x_j in the graph. The coefficients of the Krawtchouk-type polynomials P_t define a triangular matrix with a nonzero diagonal, so there are inverse relations:

$$M^r=\alpha_0^rI_N+\alpha_1^rM_1+\cdots+\alpha_r^rM_r$$

with some coefficients α_i^r, $i=1,\dots r$.

In the case of the Boolean n-cube from the previous equality and equalities $M_iM=(n-i+1)M_{i-1}+(i+1)M_{i+1}$ for $i=1,\dots r$ we obtain equality

$$M^{r+1}=\alpha_0^rM+\alpha_1^r(nI_{2^n}+2M_2)+\cdots+\alpha_r^r((n-r+1)M_{r-1}+(r+1)M_{r+1}).$$

We have recurrent relations $\alpha_i^{r+1}=i\alpha_{i-1}^r+(n-i)\alpha_{i+1}^r$ for $i=1,\dots r$ and $\alpha_{r+1}^r=0$. It is not difficult to verify that the values $\alpha_i^r=(\cosh^{n-i}(x)\sinh^i(x))^{(r)}\mid_{x=0}$ satisfy the same recurrence relations. Indeed

$$\frac{d}{dx}(\cosh^{n-i}(x)\sinh^i(x))=i\cosh^{n-i+1}(x)\sinh^{i-1}(x)+(n-i)\cosh^{n-i-1}(x)\sinh^{i+1}(x)$$

which yields exactly the same recurrence after taking the r-th derivative at $x=0$. Thus, to find the coefficients α_i^r for the Boolean n-cube, it suffices to calculate the r-th derivative at $x=0$ of the product of the powers of the hyperbolic cosines and sines.

9.3 Definition and Properties of the Fourier Transform

Let ϕ_z be the characters of a group K. The *Fourier transform* of a function $f\in V(K)$ is the function $\widehat{f}(z)=\mu\cdot(f,\phi_z)$ mapping the character group $X(K)$ into $\mathbb{C}$. The factor $\mu\in\mathbb{R}$ is chosen so that the Fourier transform preserves the norm of the function: $\|\widehat{f}\|_2=\|f\|_2=\sqrt{(f,f)}$.

Example 9.5. If $K = (\mathbb{R}, +)$, then the scalar product is defined by

$$(a, b) = \int\limits_{\mathbb{R}} a(x)\overline{b(x)}\, dx$$

and

$$\widehat{f}(z) = \frac{1}{\sqrt{2\pi}} \int\limits_{\mathbb{R}} f(x) e^{-ixz} dx.$$

Example 9.6. If $K = U(1)$, then the scalar product is defined by

$$(a, b) = \int\limits_{0}^{2\pi} a(x)\overline{b(x)}\, dx$$

and

$$\widehat{f}(n) = \frac{1}{\sqrt{2\pi}} \int\limits_{0}^{2\pi} f(x) e^{-inx} dx.$$

In this case the result of the Fourier transform can be regarded as the set of coefficients of the Fourier series expansion.

Example 9.7. If $K = \mathbb{Z}_q^n$, then the scalar product is defined by

$$(a, b) = \sum_{x \in \mathbb{Z}_q^n} a(x)\overline{b(x)}$$

and

$$\widehat{f}(z) = \frac{1}{q^{n/2}} \sum_{x \in \mathbb{Z}_q^n} f(x) \overline{\xi}^{\langle x, z \rangle}.$$

In the case $K = \mathbb{Z}_q$, i.e. when $n = 1$, this Fourier transform is called the *discrete Fourier transform*.

Consider the special case $K = \mathbb{Z}_2^n$. We have $\xi = -1$ and

$$\widehat{f}(z) = \frac{1}{2^{n/2}} \sum_{(x_1, \ldots, x_n) \in \mathbb{Z}_2^n} f(x_1, \ldots, x_n) \cdot (-1)^{x_1 z_1} \cdots (-1)^{x_n z_n} = \frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}_2^n} f(x) (-1)^{<x, z>}.$$

Note that in all the listed cases, except $K = U(1)$, the group $X(K)$ is isomorphic to the group K. As noted above, the group $X(K)$ is isomorphic to K for any finite abelian group. In this case one can regard the Fourier transform as acting from $\mathbb{V}(K)$ to $\mathbb{V}(K)$. In what follows we always assume

that K is a finite abelian group and the Fourier transform acts from $\mathbb{V}(K)$ to $\mathbb{V}(K)$ according to the formula

$$\widehat{f}(z) = \frac{1}{|K|^{1/2}}(f, \phi_z) = \frac{1}{|K|^{1/2}} \sum_{x \in K} f(x)\overline{\phi_z(x)}.$$

Remark 9.1. The rows of the generalized Hadamard matrix $H_{q,n}$ are the vectors of values of the characters on the group $\mathbb{Z}_q^n$. Therefore the Fourier transform of a function on the group $\mathbb{Z}_q^n$ coincides with the multiplication of the matrix $H_{q,n}$ by the vector of function values, i.e. $\widehat{f} = \frac{1}{q^{n/2}} H_{q,n} f$.

Proposition 9.9. *The following equality holds:*

$$f(x) = \frac{1}{|K|^{1/2}} \sum_{z \in K} \widehat{f}(z)\phi_z(x).$$

Proof. From the definition of a character we have $\phi_z(x)\phi_z(-x) = \phi_z(0) = 1$, hence $\phi_z(-x) = \overline{\phi_z(x)}$. Then we have the equality $\|\phi_z\|_2^2 = \sum_{x \in K} \phi_z(x)\overline{\phi_z(x)} = \sum_{x \in K} \phi_z(x)\phi_z(-x) = |K|$. From Proposition 9.3 it follows that the functions $\phi_z/|K|^{1/2}$ form an orthonormal basis. From the definition of the Fourier transform it follows that the numbers $\widehat{f}(z)$ are the coefficients of the expansion of f with respect to the basis of characters. □

Proposition 9.10 (Plancherel theorem)**.** *For functions on finite abelian groups the equality* $(f, g) = (\widehat{f}, \widehat{g})$ *holds.*

Proof. Apply complex conjugation to the equality from Proposition 9.9:

$$\overline{g(x)} = \frac{1}{|K|^{1/2}} \sum_{z \in K} \overline{\widehat{g}(z)\phi_z(x)}.$$

Using the orthogonality of the characters, we obtain

$$(f, g) = \frac{1}{|K|} \sum_{z \in K} \widehat{f}(z)\overline{\widehat{g}(z)}\|\phi_z\|^2 = \sum_{z \in K} \widehat{f}(z)\overline{\widehat{g}(z)} = (\widehat{f}, \widehat{g}).$$

□

From Proposition 9.10 with $f = g$ follows Parseval's identity:

$$\|f\|_2^2 = (f, f) = \frac{1}{|K|} \sum_{z \in K} |\widehat{f}(z)|^2 \|\phi_z\|_2^2 = \sum_{z \in K} |\widehat{f}(z)|^2 = \|\widehat{f}\|_2^2.$$

Proposition 9.11. $\widehat{\widehat{f}}(x) = f(-x)$.

Proof. From the definition of the Fourier transform we have

$$\widehat{\widehat{f}}(x) = \frac{1}{|K|^{1/2}}(\widehat{f}, \phi_x) = \frac{1}{|K|^{1/2}} \sum_{z \in K} \widehat{f}(z)\overline{\phi_x(z)}.$$

From Proposition 9.9 we have

$$f(-x) = \frac{1}{|K|^{1/2}} \sum_{z \in K} \widehat{f}(z)\phi_z(-x).$$

From the Pontryagin–van Kampen duality theorem it follows (it also follows from Proposition 9.4 and Example 9.3) that characters satisfy $\Phi(x, z) = \overline{\phi_z(x)} = \phi_x(z)$. And from the definition of a character we have $\phi_z(-x) = \overline{\phi_z(x)}$. □

Proposition 9.12. *A nonzero function $f : Q_q^n \to \mathbb{C}$ is an eigenfunction with eigenvalue $\lambda = n(q-1) - kq$ if and only if $\widehat{f}(z) = 0$ for all $z \in Q_q^n$ with $\mathrm{wt}(z) \neq k$.*

Proof. As shown above, the characters form a basis of the space $\mathbb{V}(K)$ and are eigenfunctions of the hypercube Q_q^n. Hence one can form bases of the eigenspaces of the hypercube from them. Since the eigenspace corresponding to $\lambda = n(q-1) - kq$ is spanned by precisely those characters with $\mathrm{wt}(z) = k$, the proposition follows. □

Proposition 9.13 (Properties of the Fourier transform)**.**
(*a*) $\widehat{f+g} = \widehat{f} + \widehat{g}$; $\widehat{c \cdot f} = c \cdot \widehat{f}$, *where c is a constant (linearity);*
(*b*) $\widehat{f(-x)}(z) = \widehat{f}(-z)$, *and if f is a real-valued function, then* $\widehat{f}(-z) = \overline{\widehat{f}(z)}$;
(*c*) $\widehat{f(x+a)}(z) = \phi_z(a)\widehat{f}(z)$ *and* $\widehat{f}(z+a) = \widehat{f \cdot \overline{\phi_a}}(x)(z)$ *(shift of the argument).*

Proof. The linearity of the Fourier transform (a) is obvious from the definition. Proof of (b):

$$\widehat{f(-x)}(z) = \frac{1}{|K|^{1/2}} \sum_{x \in K} f(-x)\overline{\phi_z(x)} = \frac{1}{|K|^{1/2}} \sum_{y \in K} f(y)\overline{\phi_z(-y)}.$$

From the duality theorem and the definition of a character we have the equalities $\phi_z(-y) = \phi_{-z}(y) = \overline{\phi_z(y)}$. Then

$$\widehat{f(-x)}(z) = \frac{1}{|K|^{1/2}} \sum_{y \in K} f(y)\overline{\phi_{-z}(y)} = \widehat{f}(-z).$$

If $f(y) = \overline{f(y)}$, then

$$\widehat{f(-x)}(z) = \frac{1}{|K|^{1/2}} \sum_{y \in K} \overline{f(y)\phi_z(-y)} = \frac{1}{|K|^{1/2}} \sum_{y \in K} \overline{f(y)}\phi_z(y) = \overline{\widehat{f}(z)}.$$

Proof of the shift property (c). Changing the variable x to $y = x + a$, we obtain the equalities

$$\widehat{f(x+a)}(z) = \frac{1}{|K|^{1/2}} \sum_{x \in K} f(x+a)\overline{\phi_z(x)} = \frac{1}{|K|^{1/2}} \sum_{y \in K} f(y)\overline{\phi_z(y-a)} =$$

here we use the equalities

$$\overline{\phi_z(y-a)} = \overline{\phi_z(y)} \cdot \overline{\phi_z(-a)} = \overline{\phi_z(y)} \cdot \phi_z(a)$$

therefore

$$= \frac{\phi_z(a)}{|K|^{1/2}} \sum_{y \in K} f(y)\overline{\phi_z(y)} = \phi_z(a)\widehat{f}(z).$$

Proof of the second identity in (c):

$$\widehat{f \cdot \overline{\phi_a}(x)}(z) = \frac{1}{|K|^{1/2}} \sum_{x \in K} f(x)\overline{\phi_a(x)} \cdot \overline{\phi_z(x)} = \frac{1}{|K|^{1/2}} \sum_{x \in K} f(x)\overline{\phi_{a+z}(x)} = \widehat{f}(z+a).$$

□

Define the Dirac delta function on the group K:

$$\delta(x) = \begin{cases} |K|^{1/2}, & x = 0 \\ 0, & x \neq 0. \end{cases}$$

Apply the Fourier transform to a character:

$$\widehat{\phi_z(x)}(y) = \frac{1}{|K|^{1/2}}(\phi_z(x), \phi_y(x)) = \delta(y - z).$$

We have the equality $\widehat{\phi_0} = \widehat{\mathbf{1}} = \delta$. By Proposition 9.11 it follows the converse equality $\widehat{\delta} = \mathbf{1}$.

Proposition 9.14 (Uncertainty principle [136]). *For any function $f \in \mathbb{V}(K)$ the inequality*

$$|K| \le |\mathrm{supp}(f)| \cdot |\mathrm{supp}(\widehat{f})|$$

holds.

Proof. From Parseval's identity it follows that

$$\|f\|_2^2 = \sum_{z \in K} |\widehat{f}(z)|^2 \le (\max_z |\widehat{f}(z)|^2) \cdot |\mathrm{supp}(\widehat{f})|.$$

From the equality $|\phi_z(x)|^2 = 1$ for every $x \in K$ and the Cauchy–Schwarz inequality $(u, v)^2 \le \|u\|_2^2 \cdot \|v\|_2^2$ we obtain

$$|\widehat{f}(z)|^2 = \frac{1}{|K|} \Big| \sum_{x \in \mathrm{supp}(f)} f(x) \overline{\phi_z(x)} \Big|^2 \le \frac{1}{|K|} \|f\|_2^2 \cdot |\mathrm{supp}(f)|.$$

If the inequality holds for every $z \in K$, then it is also true for the maximal $|\widehat{f}(z)|^2$. Hence

$$\|f\|_2^2 \le \frac{1}{|K|} \|f\|_2^2 \cdot |\mathrm{supp}(f)| \cdot |\mathrm{supp}(\widehat{f})|.$$

□

Equality in the uncertainty principle inequality is attained, for example, when f is a character or when f is the characteristic function of a subgroup of K multiplied by a character.

Proposition 9.15 (Poisson summation formula). *Let K_1 be a subgroup of a finite abelian group K. For any function $f \in \mathbb{V}(K)$ the equality*

$$|K|^{1/2} \sum_{x \in K_1} f(x) = |K_1| \sum_{z \in K_1^\perp} \widehat{f}(z)$$

holds.

Proof.

$$\sum_{z \in K_1^\perp} \widehat{f}(z) = \frac{1}{|K|^{1/2}} \sum_{z \in K_1^\perp} \sum_{x \in K} f(x) \overline{\phi_z(x)} = \frac{1}{|K|^{1/2}} \sum_{x \in K} f(x) \sum_{z \in K_1^\perp} \overline{\phi_z(x)}.$$

As noted above, an element $x \in K$ can be regarded as an element of $X(X(K))$, i.e., every $x \in K$ induces a character of the subgroup $K_1^\perp$, $K_1^\perp \subset$

$X(K)$ by Proposition 9.5. Moreover, every $x \in K_1$ induces the identity element of the subgroup $K_1^\perp$ by the definition of the group $K_1^\perp$. By using the isomorphism $K \simeq X(X(K))$, from Proposition 9.6 we obtain $|(K_1^\perp)^\perp| = |X(K)|/|K_1^\perp| = |K|/|K_1^\perp| = |K_1|$. Then $x \in K$ induces the identity element of $K_1^\perp$ only if $x \in K_1$. By Corollary 9.1 we have

$$\sum_{z \in K_1^\perp} \overline{\phi_z(x)} = 0, \text{ if } x \notin K_1,$$

$$\sum_{z \in K_1^\perp} \overline{\phi_z(x)} = |K_1^\perp|, \text{ if } x \in K_1.$$

Then

$$\frac{1}{|K|^{1/2}} \sum_{x \in K} f(x) \sum_{z \in K_1^\perp} \overline{\phi_z(x)} = \frac{|K_1^\perp|}{|K|^{1/2}} \sum_{x \in K_1} f(x).$$

By Proposition 9.6 we have $\frac{|K_1^\perp|}{|K|^{1/2}} = \frac{|K|^{1/2}}{|K_1|}$. □

9.4 Fourier Transform and Convolution

Let K be a finite group and $f, g : K \to \mathbb{C}$. We define the *convolution* of two functions as follows:

$$(f * g)(y) = \sum_{x \in K} f(x) \cdot g(y - x).$$

Note that for real functions convolution is defined similarly, only the sum is replaced by an integral. We continue to assume that K is a finite abelian group. The following properties of convolution are well known.

Proposition 9.16 (Properties of convolution)**.**

1. $f * g = g * f$;
2. $f * (g * h) = (f * g) * h$;
3. $f * (g_1 + g_2) = f * g_1 + f * g_2$;
4. $f * (\alpha g) = \alpha (f * g)$;
5. $f * \delta = |K|^{1/2} f$.

Proposition 9.17. $\widehat{f * g} = |K|^{\frac{1}{2}} \widehat{f} \cdot \widehat{g}$.

Proof. By the definition of characters we have $\phi_z(y) = \phi_z(x)\phi_z(y-x)$. Then from the definition of convolution we obtain the equalities

$$\widehat{f * g}(z) = \frac{1}{|K|^{1/2}} \sum_{y \in K} \overline{\phi_z(y)} \sum_{x \in K} f(x)g(y-x) =$$

$$= \sum_{x \in K} f(x)\overline{\phi_z(x)} \frac{1}{|K|^{1/2}} \sum_{y \in K} g(y-x)\overline{\phi_z(y-x)} = \sum_{u \in K} g(u)\overline{\phi_z(u)} = |K|^{1/2} \cdot \widehat{f} \cdot \widehat{g}.$$

□

Proposition 9.18. $\widehat{f} * \widehat{g} = |K|^{\frac{1}{2}} \widehat{f \cdot g}$.

Proof. Substituting the functions $\widehat{f}$ and $\widehat{g}$ for f and g in the equality $\widehat{f * g} = |K|^{\frac{1}{2}} \widehat{f} \cdot \widehat{g}$ and applying the Fourier transform to both sides and using the fact that $\widehat{\widehat{f}}(z) = f(-z)$, we obtain

$$(\widehat{f} * \widehat{g})(-z) = |K|^{1/2} [f(-\widehat{x) \cdot g}(-x)](z).$$

Using the equality $\widehat{f(-x)}(z) = \widehat{f}(-z)$ from Proposition 9.13(b), we have $[f(-\widehat{x) \cdot g}(-x)](z) = [(\widehat{f \cdot g})(-x)](z) = [(\widehat{f \cdot g})(x)](-z)$. Replacing z to $-z$, we obtain the required equality. □

The transform $\widehat{(-1)^f}$ of a Boolean-valued function $f : K \to \{0, 1\}$ is called the *Walsh–Hadamard transform*.

Theorem 9.2 (Titsworth [144])**.** *For any function $f : K \to \{0, 1\}$ we have*

$$\widehat{(-1)^f} * \widehat{(-1)^f} = |K|^{1/2} \delta$$

Proof. By Proposition 9.18 we obtain

$$\widehat{(-1)^f} * \widehat{(-1)^f} = |K|^{1/2} (-1)\widehat{^{f} \cdot (-1)^f} = |K|^{1/2} \widehat{\mathbf{1}} = |K|^{1/2} \delta.$$

□

Thus, for the function $h = \widehat{(-1)^f}$, where f is an arbitrary Boolean-valued function, we have

$$h * h(y) = \sum_{z \in K} h(z) \cdot h(y-z) = 0 \quad \text{for } y \neq 0.$$

From Proposition 9.13(b) we have $h(-z) = \overline{h(z)}$, since $(-1)^f$ is a real-valued function. Then

$$(h(z), h(z-y)) = \sum_{z \in K} h(z) \cdot \overline{h(z-y)} = 0 \quad \text{for } y \neq 0.$$

Since $h(\bar{0}) = |K|^{1/2}$, the vectors are nonzero. It follows that the family of functions $\{h(z-y) \mid y \in K\}$ is an orthogonal basis of the space $\mathbb{V}(K)$.

9.5 Problems

55. Prove that all eigenvalues of any Cayley graph on the groups $\mathbb{Z}_2^n$ and $\mathbb{Z}_4^n$ are integers.

56. Prove the equality $P_k[n,q](\lambda_m)|A_m| = P_m[n,q](\lambda_k)|A_k|$, where $\lambda_t = n(q-1) - tq$ and A_t is the sphere of radius t in Q_q^n.

57. Prove the equality $\sum\limits_{k=0}^{t} P_k[n,q](\lambda_m) = P_t[n-1,q](\lambda_{m-1})$.

58. Prove the equality
$\sum\limits_{m=0}^{n} P_k[n,q](\lambda_m) = \frac{1}{q}\binom{n+1}{k+1}((q-1)^{k+1} - (-1)^{k+1})$.

59. Prove that $|P_n[n,q](\lambda_m)| = 1$ for every $m = 0, \ldots, n$.

60. Prove that for any $x \in Q_2^n$ the number of Boolean functions f for which the Walsh–Hadamard coefficient $\widehat{(-1)^f}(x)$ equals zero is $\binom{2^n}{2^{n-1}}$.

61. Let $f : Q_2^n \to \mathbb{C}$ be a function that equals zero at vertices of odd weight. Prove that its Fourier coefficients coincide at antipodal points of the Boolean hypercube, i.e. $\widehat{f}(z) = \widehat{f}(z \oplus \bar{1})$.

62. Prove that for any Boolean function $f : Q_2^n \to Q_2$ the r-th moments $\sum\limits_{z \in Q_2^n} \widehat{f}^r(z) \geq 0$ are nonnegative. Prove that, among all Boolean functions with fixed weight $\mathrm{wt}(f)$, the minimum of the r-th moment is attained by the characteristic function of the set of columns of a parity-check matrix of a code with minimum distance $d+1$.

63. Prove that multiplication by the parity function $(-1)^{\mathrm{wt}(x)}$ transforms an eigenfunction of the Boolean hypercube with eigenvalue λ into an eigenfunction with eigenvalue $-\lambda$. Describe a transformation that turns perfect colorings of the Boolean hypercube with quotient matrix $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ into perfect colorings of the Boolean hypercube with quotient matrix $\begin{pmatrix} b & a \\ a & b \end{pmatrix}$.

64. Let $C \subset Q_2^n$ and suppose $\widehat{\mathbf{1}_C}(z) \neq 0$ only if the weight $\mathrm{wt}(z)$ is odd or $z = \bar{0}$. Prove that $|C| = 2^{n-1}$, except for the cases $C = Q_2^n$ and $C = \varnothing$.

65. Let A_t be the set of vertices of weight t in Q_q^n. Prove that $\widehat{\mathbf{1}_{A_t}}(z) = \frac{1}{q^{n/2}} P_t[n,q](n(q-1) - \mathrm{wt}(z)q)$.

66. Let $f : Q_2^n \to \mathbb{R}$ be an eigenfunction of the Boolean hypercube with eigenvalue $\lambda_k = n - 2k$. Prove that $|\mathrm{supp}(f)| \geq 2^{(n+|\lambda_k|)/2}$. Give examples of functions for which equality holds.

67. Let $g, f : Q_q^n \to \mathbb{C}$. Define the matrix A_f by $A_f(x,y) = f(x-y)$. Prove that $A_f A_g = A_{f*g}$. Prove that $\det A_f = q^{n/2} \prod_{y \in Q_q^n} \widehat{f}(-y)$.

68. Consider the Boolean n-cube whose edges are directed from vertices of smaller weight to adjacent vertices of larger weight. The adjacency matrix of the directed graph is skew-symmetric; it contains 1 in position i,j if the edge is directed from vertex i to vertex j, and -1 if the edge is directed from vertex j to vertex i. Find the eigenvalues and eigenvectors of the adjacency matrix of the directed n-cube.

69. Prove that if $f \in \mathbb{V}(K)$ is an eigenfunction of the graph $Cay(K,A)$, then $f * g$ is either an eigenfunction or the identically zero function of $Cay(K,A)$ for any function $g \in \mathbb{V}(K)$.

70. Prove that if $f, g \in \mathbb{V}(K)$ are eigenfunctions of the graph $Cay(K,A)$ with different eigenvalues, then their convolution $f * g$ is the identically zero function.

71. Let $f : Q_q^n \to \mathbb{C}$. Prove that f depends essentially on the variable x_i if and only if there exists a vertex $z \in Q_q^n$, $z_i \neq 0$, for which $\widehat{f}(z) \neq 0$.

72. Let $f : Q_q^n \to \mathbb{C}$ take only two distinct values. Prove that there exist constants $c_1, c_2 \in \mathbb{C}$ such that $\widehat{f} * \widehat{f} = c_1 \widehat{f} + c_2 \delta$.

73. Let $C \subset Q_p^n$, p a prime. Prove that if $|C|$ is not divisible by p, then $\mathrm{supp}(\widehat{\mathbf{1}_C}) = Q_p^n$.

10 Correlation Immune Functions and Orthogonal Arrays

10.1 Functions Balanced on Faces

In this section, we will consider only the q-ary hypercubes Q_q^n. Accordingly, the characters have the form $\phi_z(x) = \xi^{\langle x,z \rangle}$, where $\xi = e^{\frac{2\pi i}{q}}$. However, many

results in this section can be generalized to arbitrary Cayley graphs of finite abelian groups.

Recall that a face Γ of dimension $\dim \Gamma = k$ in the n-dimensional q-ary cube Q_q^n is a subset of its vertices which consists of vectors in which $n-k$ coordinates fixed while the remaining k coordinates are arbitrary.

Two faces of the same dimension are said to have the same direction if they have the same sets of fixed and free coordinates. A face with exactly one fixed coordinate is called a hyperface. The subgraph of the hypercube Q_q^n induced by a face of dimension k is isomorphic to the hypercube Q_q^k.

A function $f : Q_q^n \to \mathbb{C}$ is called *balanced on faces of dimension* k, if for every face Γ of dimension k, the equality $\sum\limits_{x\in\Gamma} f(x) = 0$ holds. Note that if a function is balanced on faces of dimension k, then it is also balanced on faces of every dimension greater than k.

Proposition 10.1. *Let a function $f : Q_2^n \to \mathbb{C}$ be balanced on faces of dimension k. Then f is uniquely determined from its values in the ball of radius $k-1$, i.e., from the values at vertices of weight at most $k-1$.*

Proof. We prove the proposition by induction. Consider an arbitrary vertex z of weight k. There is a face of dimension k that contains z and the all-zero vector. Clearly, z is the unique vertex of weight at least k in this face. Since the function f is balanced, value $f(z)$ is uniquely determined. If f is balanced on faces of dimension k, then it is balanced on faces of dimension $k+i$, $i \geq 0$. Therefore, after finding the values $f(z)$ for all vertices z of weight k, we can find the values $f(z)$ for all vertices of weight $k+1$, and so on. □

The functions balanced on faces of a fixed dimension form a linear subspace of $\mathbb{V}(Q_q^n)$. We next show that a basis of this space can be formed from the characters of the group $\mathbb{Z}_q^n$.

Proposition 10.2. *If $\mathrm{wt}(z) = k$, then the character ϕ_z is balanced on faces of dimension $n-k+1$ and there exists a family of faces of dimension $(n-k)$ having the same direction such that ϕ_z is constant on all faces of that direction.*

Proof. Without loss of generality, assume that $z = (z_1, \ldots, z_k, 0, \ldots, 0)$, $z_i \neq 0$, $i = 1, \ldots, k$. Consider an arbitrary face Γ of dimension $n-k+1$. Such a face necessarily has at least one free coordinate x_i among the first k. Without loss of generality, assume that $i = 1$. By Proposition 9.2 we have $\sum\limits_{x\in Q_q} \xi^{xz_i} = 0$. Then

$$\sum_{x\in\Gamma}\phi_z(x)=\sum_{x_{i_2},\ldots,x_{i_{n-k}}}\sum_{x_1}\phi_z(x)=\sum_{x_{i_2},\ldots,x_{i_{n-k}}}\xi^{\langle(z_2,\ldots,z_n),(x_2,\ldots,x_n)\rangle}\sum_{x_1}\xi^{z_1x_1}=0.$$

Next consider a face Γ of dimension $n-k$ whose first k coordinates are fixed: $x_1=a_1,\ldots,x_k=a_k$. For any vertex $x\in\Gamma$ the equality

$$\phi_z(x)=\xi^{\langle(z_1,\ldots,z_k,0,\ldots,0),(x_1,\ldots,x_n)\rangle}=\xi^{z_1a_1+\cdots+z_ka_k}$$

holds. □

Proposition 10.3. *A function $f:Q_q^n\to\mathbb{C}$ is balanced on faces of dimension k if and only if $\widehat{f}(z)=0$ for all $z\in Q_q^n$ of weight $\mathrm{wt}(z)\le n-k$.*

Proof. ($\Leftarrow$) Assume that $\widehat{f}(z)=0$ for $\mathrm{wt}(z)\le n-k$. From Proposition 9.9 we have

$$f(x)=\frac{1}{q^{n/2}}\sum_{\mathrm{wt}(z)>n-k}\widehat{f}(z)\phi_z(x).$$

By Proposition 10.2, all characters $\phi_z(x)$ with $\mathrm{wt}(z)\ge n-k+1$ are balanced on faces of dimension k.

($\Rightarrow$) Consider

$$\widehat{f}(z)=\frac{1}{q^{n/2}}(f,\phi_z),\ \text{ where}\,\mathrm{wt}(z)\le n-k.$$

By Proposition 10.2, ϕ_z is constant on faces Γ of dimension k (or greater than k if $\mathrm{wt}(z)<n-k$) of some direction. Since f is balanced on every face Γ, we have $\sum\limits_{x\in\Gamma}f(x)\overline{\phi_z(x)}=\overline{\phi_z(a)}\sum\limits_{x\in\Gamma}f(x)=0$. Since the vertex set of the hypercube is partitioned into the faces of any fixed direction, summing over all such faces yields $\widehat{f}(z)=0$. □

10.2 Correlation Immune Functions: Definition and Applications

Let $Im(f)$ be the set of values taken by the function f.

A function f is called *correlation immune of order k* if, for every $b\in Im(f)$, the value b occurs equally often in every face of dimension $n-k$.

If a function is uniformly distributed in faces of small dimension, then this same property will also hold for faces of larger dimension. For this reason, it is convenient to introduce the notation $\mathrm{cor}(f)$ for the maximum order of correlation immunity of the function f.

It follows from the definition of an MDS code (see Section 17.1) that for the characteristic function of an MDS code C with code distance d we have that $\mathrm{cor}(\mathbf{1}_C) = n - d + 1$. Clearly, if an MDS code exists, then this is the minimum cardinality nonempty set with such correlation immunity.

Example 10.1. For a constant function in an n-dimensional hypercube we have $\mathrm{cor}(const) = n$. The Boolean parity function $f(x_1, \ldots, x_n) = x_1 + \cdots + x_n \mod 2$ it has $\mathrm{cor}(f) = n - 1$.

Example 10.2. Latin colorings (see Example 5.3) in Q_q^n are correlation-immune functions of order $n - 1$.

Correlation immune functions are used in cryptography to simulate a random distribution of values at the vertices of the q-ary hypercube. Consider the problem of determining the value of a function when only part of its argument is known. Suppose that an adversary knows the function $f : Q_q^n \to Im(f)$ and the values of k out of n arguments. Their aim is to determine the value of the function. If $\mathrm{cor}(f) \geq k$, then in each face of dimension $n-k$ the function takes any value b with the same frequency as in the whole hypercube. Therefore, knowing the values of k variables provides no additional information about the value of the function. One can also consider the problem where the adversary knows the value $f(x) = b$ and the values of k out of n variables, and their aim is to determine the remaining coordinates of the argument. If $\mathrm{cor}(f) \geq k$, then the information available to the adversary does not help at all to find the values of the remaining variables, since in each face of dimension $n - k$ the function takes any value b with the same frequency. The very name "correlation immune" comes from the fact that the set of $k+1$ random variables (the value of the function and k arbitrary variables) is independent (uncorrelated).

In cryptographic algorithms, Boolean-valued and even Boolean functions are most often considered. The use of the Boolean parity check function, which possesses the maximum correlation immunity for non-constant functions, has limitations, since in this case the frequencies of 0 and 1 are equal. Furthermore, an a priori unknown function creates additional difficulties for the adversary. The possibility of constructing sufficiently diverse correlation immune Boolean-valued functions with different proportions of ones will be considered below.

10.3 Correlation Immunity and the Fourier Transform

Proposition 10.4. *Let $f : Q_q^n \to \mathbb{C}$ and $\mathrm{cor}(f) = k$. Then the function $g = f - \frac{\mathrm{wt}(f)}{q^n}\mathbf{1}$, where $\mathrm{wt}(f) = \sum_x f(x)$, is balanced on faces of dimension*

$n-k$.

Proof. By assumption, the sum of the values of the function f in each face of dimension $n-k$ is the same, and adding a constant function does not change this property. By definition, the function g is balanced in the hypercube; consequently, it is balanced on faces of dimension $n-k$. □

Theorem 10.1 ([29]). *For a function $f : Q_q^n \to \{0,1\}$, the equality $\mathrm{cor}(f) = k$ holds if and only if $\widehat{f}(z) = 0$ for all $z \in Q_q^n$ of weight $0 < \mathrm{wt}(z) \le k$ and $\widehat{f}(v) \neq 0$ for some $v \in Q_q^n$ of weight $\mathrm{wt}(v) = k+1$.*

Proof. ($\Rightarrow$) Let $g = f - \frac{\mathrm{wt}(f)}{q^n}\mathbf{1}$. By Proposition 10.4, the function g is balanced on faces of dimension $n-k$. Then $\widehat{g}(z) = 0$ for all $z \in Q_q^n$ of weight $\mathrm{wt}(z) \le k$ by Proposition 10.3. The Fourier transform of $\mathbf{1}$ is a δ-function; therefore, the functions $\widehat{f}$ and $\widehat{g}$ differ only at $\bar{0}$.

If $\widehat{f}(v) = 0$ for all $v \in Q_q^n$ of weight $\mathrm{wt}(v) = k+1$, then the function g is balanced also on faces of dimension $n-k-1$ by Proposition 10.3. Then the sums $\sum_{x\in\Gamma} f(x)$ are the same for all faces Γ of dimension $n-k-1$. Since f takes only two values 0 and 1, it must take the value 1 the same number of times in each face of dimension $n-k-1$. Then $\mathrm{cor}(f) \ge k+1$, a contradiction.

($\Leftarrow$) It is easy to see that $\widehat{g}(\bar{0}) = 0$. From the condition we have $\widehat{g}(z) = 0$ for $0 < \mathrm{wt}(z) \le k$. Then from Proposition 10.3 we obtain that g is balanced on faces of dimension $n-k$. By Proposition 10.3, the existence of a nonzero Fourier coefficient $\widehat{g}(v) \neq 0$ for some $v \in Q_q^n$ of weight $\mathrm{wt}(v) = k+1$ implies that g is not balanced on some face of dimension $n-k-1$. Since the function g takes only two values, we have $\mathrm{cor}(g) = k$. The functions f and g differ by a constant, hence $\mathrm{cor}(f) = \mathrm{cor}(g)$. □

In this theorem, only the cardinality of the image of the function matters. We will also apply the theorem when $Im(f) = \{-1, 1\}$. If the function f takes more than two distinct values (i.e., colors), then $\mathrm{cor}(f)$ equals the minimum of the correlation immunities of the characteristic functions of the colors. Indeed, if all colors are uniformly distributed over faces of some dimension, then so is each individual color. If at least one of the colors is not uniformly distributed over faces of some dimension k, then the function as a whole, by definition, is not correlation immune of order $n-k$.

Theorem 10.1 can be viewed as an analogue of Proposition 2.8 and it is a corollary of the orthogonality of the eigenspaces of the adjacency matrix of the graph with distinct eigenvalues. Indeed, the characteristic function of a face of dimension $n-k$ is a linear combination of the characters ϕ_z,

where $\mathrm{wt}(z) \leq k$. Conversely, the characters are linear combinations of the indicators of faces of the corresponding dimension. Hence every linear combination of the characters ϕ_z with $\mathrm{wt}(z) > k$ is orthogonal to a face of dimension $n-k$. Conversely, every function orthogonal to all faces of dimension $n-k$ can be represented as such a linear combination.

10.4 Correlation Immunity of Perfect Colorings

Proposition 10.5. *Let f be a perfect coloring of Q_q^n with quotient matrix S. Then $\widehat{f}(z) \neq 0$ only if $(n-\mathrm{wt}(z))(q-1)-\mathrm{wt}(z)$ is an eigenvalue of S.*

Proof. The function f can be represented as a linear combination of eigenfunctions of Q_q^n whose eigenvalues coincide with the eigenvalues of S (see Corollary 2.3). By Corollary 9.4, the characters form a basis of every eigenspace of Q_q^n. Therefore, every such eigenfunction is a linear combination of characters. The character ϕ_z has the eigenvalue $(n-\mathrm{wt}(z))(q-1)-\mathrm{wt}(z)$ (see Section 9.2). □

If f is the characterictic function of a cell of an equitable partition corresponding to a perfect coloring, then Proposition 10.5 remains true.

Proposition 10.6. *Let f be a perfect coloring of Q_q^n and $\lambda_1 < n(q-1)$ the largest nontrivial eigenvalue of its quotient matrix. Then* $\mathrm{cor}(f) = \frac{n(q-1)-\lambda_1}{q} - 1$.

Proof. Let $\{C_1, \ldots, C_k\}$ be an equitable partition corresponding to f. By Proposition 2.3, for every i, $i = 1, \ldots, k$, $\mathbf{1}_{C_i}$ is a linear combination of eigenfunctions of Q_q^n with eigenvalues from the spectrum of the quotient matrix. Moreover, for every eigenvalue λ of the quotient matrix there exists a cell C_i such that its linear expansion has a nontrivial summand with eigenvalue λ in the linear expansion. Thus, the proposition follows from Proposition 10.5. □

Proposition 10.7. *Let f be a perfect 2-coloring of Q_q^n with quotient matrix* $S = \begin{pmatrix} n(q-1)-b & b \\ c & n(q-1)-c \end{pmatrix}$. *Then* $\mathrm{cor}(f) = \frac{b+c}{q} - 1$.

Proof. The eigenvalues of S are $\lambda_0 = n(q-1)$ and $\lambda_1 = n(q-1)-(b+c)$. Solving $(n-\mathrm{wt}(z))(q-1)-\mathrm{wt}(z) = \lambda_0 = n(q-1)$ gives $\mathrm{wt}(z) = 0$, while solving $(n-\mathrm{wt}(z))(q-1)-\mathrm{wt}(z) = \lambda_1 = n(q-1)-(b+c)$, gives $\mathrm{wt}(z) = \frac{b+c}{q}$. Then by Theorem 10.1 and Proposition 10.5 we obtain $\mathrm{cor}(f) = \frac{b+c}{q} - 1$. □

Corollary 10.1. *For the characteristic function f of a 1-perfect code in Q_q^n, the equality* $\mathrm{cor}(f) = \frac{(n-1)(q-1)}{q}$ *holds.*

Constructing perfect 2-colorings is one method of obtaining correlation immune functions with prescribed parameters. It will be shown below that correlation immune functions of the maximum possible order for some parameters are perfect colorings.

The following theorem is a generalization of Theorem 7.7 on recovering a perfect coloring from the average layer. Here, however, two layers are required to recover the function. A generalization of Theorem 7.7 on recovering a perfect coloring from one layer under other additional conditions is given in [150].

Theorem 10.2. *Let f be a perfect coloring of Q_2^n with quotient matrix S. Let v be an eigenvector of S corresponding to the eigenvalue λ_k of S, where $-n < \lambda_k = n - 2k < 0$. If all entries of v are distinct, then f is uniquely determined by its values on vectors of weight $n-k$ and $n-k-1$.*

Proof. By Remark 2.6, there exists an eigenfunction f' of the hypercube with eigenvalue λ_k, whose distinct values correspond to distinct colors of f. Since f' is an eigenfunction, $\widehat{f'}(z) = 0$ for $\mathrm{wt}(z) \neq k$ by Proposition 9.12. Then by Propositions 10.1 and 10.3, f' is uniquely determined by its values at vertices of weight at most $n-k$. By Proposition 7.5, recovering f' inside the ball of radius $n-k$ requires only the values of f' on the spheres of radii $n-k$ and $n-k-1$, provided that $n-k < n/2$. The latter inequality holds by the hypothesis. □

Note that in Theorem 10.2, the condition $-n < \lambda_k = n - 2k < 0$ can be replaced by $0 < \lambda_k = n - 2k < n$, and the spheres of radius $n-k$ and $n-k-1$ by the spheres of radii k and $k-1$, since the Hadamard (pointwise) multiplication of an eigenfunction with eigenvalue λ and the function $g(x) = (-1)^{\mathrm{wt}(x)}$ yields an eigenfunction with eigenvalue $-\lambda$. This follows from the equality $(\widehat{(-1)^{\mathrm{wt}(x)} f})(y) = \widehat{f}(y \oplus \bar{1})$.

10.5 Orthogonal Arrays and Rao's Inequality

An *orthogonal array* of type $OA(N, k, q, t)$ is an $N \times k$ array whose entries come from a fixed finite set of q symbols (without loss of generality, Q_q), such that in every subset of t columns of the array, every ordered t-tuple of symbols occurs the same number of times. The number t is called the

strength of the orthogonal array. The number of repeats is usually denoted by λ. Obviously, $\lambda = N/q^t$.

An orthogonal array of general form may contain repeated rows and corresponds to the value table of a function $f : Q_q^n \to \{0, 1, \ldots, m\}$: if $f(x) = s$, then the row x appears in the array s times. By the definition of orthogonal arrays, the function f differs from a function balanced on $(n-k)$-dimensional faces by a constant.

A simple orthogonal array (i.e., without repeated rows) of strength k is a table whose set of rows is precisely the support of f, where $f : Q_q^n \to \{0, 1\}$ is a correlation immune function of order k.

An orthogonal array of type $OA(N, k, q, t)$ of minimum cardinality $N = q^t$ is precisely the list of codewords of an MDS code with length k and minimum code distance $k - t + 1$ (see Section 17.1).

Example 10.3. A binary orthogonal array of strength 2:

$$\begin{array}{ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}.$$

Correlation immune functions in the form of orthogonal arrays are used for experiment design. Suppose we have a program with n parameters, each of which can take q values. To test the program for all possible parameter sets, one would need to run q^n computational experiments, which may require unreasonably many resources. Suppose it is sufficient to verify the program's operation for any values of any k parameters. Then we need to set the parameters as rows of an orthogonal array of strength k of minimal possible size. A similar solution can be applied not only for testing the correctness of the program, but also when collecting data to evaluate the performance of the program. Of course, to solve such a problem, one needs orthogonal arrays of as small a size as possible or, equivalently, correlation immune functions with as small a support size as possible.

Several theorems proved below for Boolean-valued correlation immune functions can be generalized to functions taking nonnegative integer values and to the corresponding orthogonal arrays.

Theorem 10.3 (Rao's inequality [122])**.**

Let $f : Q_q^n \to \{0,1\}$, $f \neq \mathbf{0}$ and $k = \mathrm{cor}(f)$. Then,
if k is even, then $|\mathrm{supp}(f)| \geq \sum_{i=0}^{k/2} \binom{n}{i}(q-1)^i$;
if k is odd, then $|\mathrm{supp}(f)| \geq \binom{n-1}{(k-1)/2}(q-1)^{\frac{k+1}{2}} + \sum_{i=0}^{(k-1)/2} \binom{n}{i}(q-1)^i$.

Proof. Since f takes only values 0 and 1, and $|\phi_u(x)| = 1$ for every $x \in Q_q^n$, we have

$$(f\phi_v, f\phi_u) = (f\phi_v, \phi_u) = (f, \phi_{-v}\phi_u) = (f, \phi_{u-v}) = q^{n/2}\widehat{f}(u-v).$$

From Theorem 10.1 it follows that $\widehat{f}(z) = 0$ for all $z \in Q_q^n$ of weight $0 < \mathrm{wt}(z) \leq k$. Consequently, all functions $f\phi_v$ for $0 \leq \mathrm{wt}(v) \leq k/2$ are pairwise orthogonal.

There can be at most N pairwise orthogonal vectors of length N. We have $\mathrm{supp}(f\phi_v) = \mathrm{supp}(f)$. Therefore, the number of distinct vectors $f\phi_v$, where $0 \leq \mathrm{wt}(v) \leq k/2$, is at most $|\mathrm{supp}(f)|$. Hence for even k we obtain the inequality $|\mathrm{supp}(f)| \geq \sum_{i=0}^{k/2} \binom{n}{i}(q-1)^i$.

In the case when k is odd, we can consider all functions $f\phi_v$ for $0 \leq \mathrm{wt}(v) \leq (k-1)/2$ and all functions $f\phi_u$, $u_1 \neq 0$, $\mathrm{wt}(u) = (k+1)/2$. Then the weight of the differences of any two such vectors does not exceed k. □

Note that for any Boolean-valued function f, the number $q^{\mathrm{cor}(f)}$ divides $|\mathrm{supp}(f)|$, since in each face of dimension $n - \mathrm{cor}(f)$ contains the same number of ones.

10.6 Total Influence of Boolean Functions

Let $f : Q_q^n \to \{0,1\}$ be a characteristic function of a set $C \subset Q_q^n$. Denote by $I[f]$ the number of edges whose endpoints have different values of f. For a constant function this quantity is zero, while for the Boolean parity function it is $n2^{n-1}$. Note that $I[f]$ equals the size of the cut $I[f] = e(f^{-1}(0), f^{-1}(1))$ in the Hamming graph.

Proposition 10.8 (Nisan and Szegedy[112]). $I[f] = \frac{q}{4} \sum_{z \in Q_q^n} \mathrm{wt}(z)|\widehat{(-1)^f}(z)|^2$.

Proof. Let M be the adjacency matrix of Q_q^n. It is straightforward to verify that

$$2I[f] - (n(q-1)q^n - 2I[f]) = -(M(-1)^f, (-1)^f), \tag{22}$$

since in the right-hand sum each edge is counted twice.

Recall that the characters are eigenfunctions of the matrix M, i.e., $M\phi_z = \lambda_z\phi_z$, where $\lambda_z = (q-1)n - q\mathrm{wt}(z)$ (see Section 18.4). We represent the function $(-1)^f$ as a linear combination of characters: $(-1)^f = \frac{1}{q^{n/2}} \sum_{z\in Q_q^n} \widehat{(-1)^f}(z)\phi_z$. Substituting this expression into (22) and using the orthogonality of the characters, as well as Parseval's equality $\sum_{z\in Q_q^n} |\widehat{(-1)^f}(z)|^2 = q^n$, we obtain the equalities

$$4I[f] = n(q-1)q^n - \sum_{z\in Q_q^n} \lambda_z |\widehat{(-1)^f}(z)|^2 = \sum_{z\in Q_q^n} q\mathrm{wt}(z)|\widehat{(-1)^f}(z)|^2.$$

□

Define the density $\rho(f) = \frac{|C|}{q^n}$ of an indicator function $f = \mathbf{1}_C$.

Theorem 10.4. *Let $f : Q_q^n \to \{0,1\}$, $f \neq \mathbf{0}$.*
(a) $\frac{I[f]}{q^{n+1}} \geq (\mathrm{cor}(f)+1)(\rho(f) - \rho^2(f))$.
(b) $\frac{I[f]}{q^{n+1}} = (\mathrm{cor}(f)+1)(\rho(f) - \rho^2(f))$ *if and only if f is a perfect 2-coloring.*

Proof. (a) Since $(-1)^f = \mathbf{1} - 2f$, the coefficients $\widehat{(-1)^f}(z)$ and $\widehat{f}(z)$ vanish simultaneously for $\mathrm{wt}(z) > 0$. By Theorem 10.1 it follows that $\widehat{(-1)^f}(z) = 0$ for $0 < \mathrm{wt}(z) \leq \mathrm{cor}(f)$. Hence, from Proposition 10.8 we have the inequality

$$4I[f] \geq \sum_{z\in Q_q^n\setminus\bar{0}} q(\mathrm{cor}(f)+1)|\widehat{(-1)^f}(z)|^2. \tag{23}$$

Next we estimate the sum $\sum_{z\in Q_2^n\setminus\bar{0}} |\widehat{(-1)^f}(z)|^2$. From Parseval's equality we have $\sum_{z\in Q_q^n} |\widehat{(-1)^f}(z)|^2 = q^n$, and moreover $\widehat{(-1)^f}(\bar{0}) = q^{n/2}(1-2\rho(f))$. Then

$$\sum_{z\in Q_q^n\setminus\bar{0}} |\widehat{(-1)^f}(z)|^2 = q^n - q^n(1-2\rho(f))^2 = 4q^n\rho(f)(1-\rho(f)). \tag{24}$$

(b) Obviously, equality in (23) holds if and only if $(-1)^f - (\widehat{(-1)^f}(0))\phi_{\bar{0}}$ is an eigenfunction with eigenvalue $(q-1)n - q(\mathrm{cor}(f)+1)$. By Propositions 2.7 and 10.7 it holds if and only if the function $(-1)^f$ is a perfect 2-coloring. □

Finally, we consider Boolean functions. Let $I_i[f]$ denote the probability that flipping the i-th input bit changes the output value of f. The sum $\bar{I}[f] = \sum_i I_i[f]$ is called the *total influence* (or *average sensitivity*) of f. It is easy to see that $\bar{I}[f] = I[f]/2^{n-1}$. Consider also the normalized Walsh–Hadamard coefficients $\bar{W}_f(u) = \widehat{(-1)^f}(u)/2^{n/2}$. By Parseval's identity we have $\sum_z \bar{W}_f^2(z) = 1$ for every Boolean function $f : Q_2^n \to \{0,1\}$. Hence the values $\bar{W}_f^2(z)$ define a probability distribution on Q_2^n. The *Fourier entropy* of f is defined by $H(f) = \sum_{z \in Q_2^n} \bar{W}_f^2(z) \log_2 \frac{1}{\bar{W}_f^2(z)}$. By Proposition 10.8 we have $\bar{I}[f] = \sum_{z \in Q_2^n} \bar{W}_f^2(z) wt(z)$.

The celebrated Fourier Entropy–Influence (FEI) conjecture was introduced by Friedgut and Kalai in 1996 [48]. The conjecture asserts the existence of a universal constant C such that $H[f] \leq C \cdot \bar{I}[f]$ for every Boolean function f.

10.7 Bierbrauer–Friedman Inequality

We derive Bierbrauer–Friedman inequality on the size of orthogonal arrays as a corollary of Theorem 10.4.

Theorem 10.5 (Bierbrauer–Friedman inequality [14], [49]).
Let $f : Q_q^n \to \{0,1\}$, $f \neq \mathbf{0}$.
(a) *Then $\rho(f) \geq 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$.*
(b) *If $\rho(f) = 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$ then f is a perfect 2-coloring.*

Proof. Without loss of generality, we assume that $\rho(f) \leq 1/2$.
$\frac{I[f]}{q^n} \leq (q-1)\rho(f)n$, since each vertex with value 1 is adjacent to at most $n(q-1)$ vertices with value 0. By Theorem 10.4(a) we obtain

$$\frac{(q-1)\rho(f)n}{q} \geq \frac{I[f]}{q^{n+1}} \geq (\mathrm{cor}(f)+1)(\rho(f) - \rho^2(f)).$$

This inequality is equivalent to part (a). Part (b) follows directly from Theorem 10.4(b). □

Note that equality in the Bierbrauer–Friedman inequality cannot be attained by a non-simple orthogonal array, since in that case

$$(f,f) = \sum_{x \in Q_q^n} |f(x)|^2 > |\mathrm{supp}(f)|,$$

and, therefore, equality (24) does not hold.

Corollary 10.2 (Ostergard, Pottonen, Phelps, [113]). *Let $f : Q_q^n \to \{0,1\}$. The function f is the characteristic function of a 1-perfect code if and only if $\rho = \frac{1}{n(q-1)+1}$ and $\mathrm{cor}(f) = \frac{n(q-1)+1}{q} - 1$.*

Proof. ($\Rightarrow$) The equality $\rho = \frac{1}{n(q-1)+1}$ follows immediately from the definition of a 1-perfect code. The value of $\mathrm{cor}(f)$ is obtained from Claim 10.7 by substituting the specific values $b = 1$, $c = n(q-1)$.

($\Leftarrow$) Substituting these values into the Bierbrauer–Friedman inequality gives

$$\frac{1}{n(q-1)+1} \geq 1 - \frac{n(q-1)}{q \cdot \frac{n(q-1)+1}{q}}, \quad \text{i.e.,} \quad \frac{1}{n(q-1)+1} \geq \frac{1}{n(q-1)+1}.$$

Hence, equality holds. Then by Theorem 10.5(b) we obtain that f is a perfect 2-coloring.

The value of the density implies that, on average, each radius-one ball contains exactly one vertex x such that $f(x) = 1$. Since f is a perfect 2-coloring, every radius-one ball contains vertices of both colors. Consequently, each ball contains exactly one 1, and f is the characteristic function of a 1-perfect code. □

It follows from the proof that equality in the Bierbrauer–Friedman inequality can occur only when $(Mf, f) = 0$, that is, when the perfect 2-coloring f has no adjacent vertices colored 1. However, one can show that every perfect 2-coloring of Q_q^n is extremal in the sense of attaining equality in some inequality similar to the Bierbrauer–Friedman inequality.

Proposition 10.9 ([117]). *Let $f : Q_q^n \to \{0,1\}$. The following inequality holds:*

$$\rho(f) \cdot q(\mathrm{cor}(f) + 1) \leq \bar{s}_{01}(f), \tag{25}$$

where $\bar{s}_{01}(f)$ denotes the average number of neighbors of color 1 of a vertex of color 0 (see Section 6). Equality (25) holds if and only if f is a perfect coloring.

The proof follows the same argument as that of the Bierbrauer–Friedman inequality.

10.8 Fon-Der-Flaass Theorem

A Boolean correlation-immune function f is called *resilient* if $(-1)^f$ is balanced, i.e., f takes the values 0 and 1 equally often. It is easy to see that a Boolean function f is resilient only if $\widehat{(-1)^f}(\bar{0}) = 0$.

Theorem 10.6 (Fon-Der-Flaass [47]). *If a Boolean function $f : Q_2^n \to \{0,1\}$ is neither constant nor resilient, then* $\mathrm{cor}(f) \le \frac{2n}{3} - 1$. *Moreover, if equality is attained in this inequality, then f is a perfect 2-coloring.*

Proof. Let $g = \widehat{(-1)^f}$. Since f is not constant, there exists $y \ne \bar{0}$ such that $g(y) = \widehat{(-1)^f}(y) \ne 0$. Since f is not resilient, $g(\bar{0}) = \widehat{(-1)^f}(\bar{0}) \ne 0$. By Theorem 9.2, for the chosen y we have

$$0 = (g * g)(y) = \sum_{x \in Q_2^n} g(x)g(y-x).$$

Hence the sum must contain at least one additional nonzero term besides the two terms $g(\bar{0})g(y)$ and $g(y)g(\bar{0})$ since these two terms alone cannot sum to zero. Note that $\mathrm{cor}(f) = \mathrm{cor}((-1)^f)$. By Theorem 10.1 we have $g(x) = 0$ for $0 < \mathrm{wt}(x) \le \mathrm{cor}(f)$. Therefore,

$$0 = (g * g)(y) = 2g(\bar{0})g(y) + \sum_{\substack{x \in Q_2^n \\ \mathrm{wt}(x) \ge \mathrm{cor}(f)+1 \\ \mathrm{wt}(y-x) \ge \mathrm{cor}(f)+1}} g(x)g(y-x),$$

and the sum contains nonzero terms. Assume that $\mathrm{cor}(f) > \frac{2n}{3} - 1$. Then $\mathrm{wt}(y) > \frac{2n}{3}$ and there exists x for which $g(x)g(y-x) \ne 0$. From this it follows that $\mathrm{wt}(x) > \frac{2n}{3}$ and $\mathrm{wt}(y-x) > \frac{2n}{3}$. However, from the triangle inequality for the Hamming metric we have $\mathrm{wt}(y-x) = d(x,y) \le d(\overline{1},x) + d(\overline{1},y) = n - \mathrm{wt}(x) + n - \mathrm{wt}(y) < \frac{2n}{3}$. Contradiction.

Now let $\mathrm{cor}(f) = \frac{2n}{3} - 1$. If $g(y) \ne 0$ at some vertex of weight $\mathrm{wt}(y) > \frac{2n}{3}$, then we obtain a contradiction in the same manner. Hence, g is supported only at $\bar{0}$ and at vertices of weight $\frac{2n}{3}$. Then f is a perfect coloring by Proposition 2.7. □

The inequality in Theorem 10.6 is called the Fon-Der-Flaass bound. The proof given above is due to Khalyavin. As shown by Khalyavin [74], the Fon-Der-Flaass bound also remains valid for binary orthogonal arrays. In contrast to the Rao and Bierbrauer–Friedman inequalities, no analogue of the Fon-Der-Flaass theorem is currently known for the q-ary hypercubes with $q \ne 2$. The only known extension is to Q-polynomial distance-regular graphs (see [82]).

10.9 Problems

74. Let $f : Q_2^n \to \mathbb{C}$ and $\mathrm{cor}(f) = n - k$. Prove that f is uniquely determined by its values in the ball of radius $k-1$ (i.e., from the values at vertices of weight at most $k-1$).

75. Let $f : Q_q^n \to \mathbb{C}$ and $\mathrm{cor}(f) = n - k$. Prove that f is uniquely determined by its values outside the ball of radius $n-k$ (i.e., from the values at vertices of weight at least $n - k + 1$).

76. Let q be prime. Regard Q_q^n as the n-dimensional vector space over the field $GF(q)$. Prove that if a function $f : Q_q^n \to \mathbb{C}$ is balanced on all hyperplanes, then f is identically zero.

77. Prove that the support size of a function $f : Q_2^n \to \mathbb{C}$ that is balanced on faces of dimension k is at least 2^{n-k+1}.

78. Prove that the functions $f : Q_q^n \to \mathbb{C}$ balanced on faces of dimension k form a linear subspace, and that this subspace is the orthogonal complement of the span $L(n, k, q)$ of the set of indicators of all k- dimensional faces.

79. Let $f \in L(n, k_1, q)$ and $g \in L(n, k_2, q)$. Prove that $f \cdot g \in L(n, k_2 + k_1 - n, q)$ if $k_2 + k_1 > n$.

80. Let f be a perfect coloring of Q_2^n, and let λ be the largest eigenvalue of its quotient matrix other than n. Prove that $\mathrm{cor}(f) = \frac{n-\lambda}{2} - 1$.

81. Let f be some coloring of Q_2^n, and let λ be the largest eigenvalue of the average quotient matrix S_f (see Section 6) other than n. Prove that $\mathrm{cor}(f) \le \frac{n-\lambda}{2} - 1$.

82. A *covering array of strength* k is a table whose rows are tuples from $P \subset Q_q^n$ such that the set P intersects all k-dimensional faces in Q_q^n. Prove that the number of rows of a covering array of strength 2 in Q_2^n is at least $\lceil \log_2 n \rceil$.

83. Let a Boolean function $f : Q_2^n \to \{0, 1\}$ be neither constant nor resilient and attain equality in the Fon-Der-Flaass bound. Prove that in every face of dimension greater than $n/3$, the numbers of x on which $f(x) = 1$ among even-weight and odd-weight vertices are equal.

11 Dual Code and Sarkar Identity

11.1 Dual Code

In this section, we regard Q_q as the ring $\mathbb{Z}_q$. So, for $u, v \in Q_q^n$ we write $v \perp u$ if $\langle v, u \rangle = \sum v_i u_i = 0 \mod q$. Moreover, for a code $C \subset Q_q^n$ we write $v \perp C \subset Q_q^n$ if for all $u \in C$ the equality $\langle v, u \rangle = \sum v_i u_i = 0 \mod q$ holds. The set $C^\perp = \{v \in Q_q^n \mid v \perp C\}$ is called the *dual code* of C. It is

easy to verify that the set $C^\perp$ is closed under addition and multiplication in the ring $\mathbb{Z}_q$, and $C \subseteq (C^\perp)^\perp$ by definition. A code $C \subset Q_q^n$ is called *additive* if it is closed under addition and scalar multiplication in the ring $\mathbb{Z}_q$. In particular, an additive code in Q_q^n is a subgroup of $\mathbb{Z}_q^n$. Moreover, for every additive code $C \subset \mathbb{Z}_q^n$ the dual code $C^\perp$ coincides with the subgroup $C^\perp \subset X(\mathbb{Z}_q^n) \simeq \mathbb{Z}_q^n$.

Remark 11.1. It is well-known that a field structure can be defined on a set of cardinality q if and only if $q = p^t$ is a prime power. For $t > 1$ the addition and multiplication operations in the field $GF(p^t)$ will not coincide with addition and multiplication modulo q. Therefore, the definition of the dual code used here and in Section 17.6 coincides only for prime q.

Proposition 11.1. *Let Γ be a k-dimensional face in Q_q^n, with $\bar{0} \in \Gamma$, and let its free coordinates be indexed by $I \subset \{1, \ldots, n\}$. Then $\Gamma^\perp$ is an $(n-k)$-dimensional face in Q_q^n, with $\bar{0} \in \Gamma^\perp$ and $\{1, \ldots, n\} \setminus I$ being the indices of its free coordinates.*

Proof. The sets of free coordinates of the two faces are disjoint. Therefore, for any $i \in \{1, \ldots, n\}$ and for any vertex u of one face and any vertex v of the other face, $u_i = 0$ or $v_i = 0$. It remains to show that any tuple v having a nonzero coordinate $v_i \neq 0$, $i \in I$, is not contained in $\Gamma^\perp$. Indeed, we have $e_i \in \Gamma$ and $\langle v, e_i \rangle = v_i \neq 0$. □

Proposition 11.2. *$v \perp C$ if and only if $\widehat{\mathbf{1}_C}(v) = \frac{|C|}{q^{n/2}}$.*

Proof. We have the equality $\widehat{\mathbf{1}_C}(v) = \frac{1}{q^{n/2}} \sum\limits_{x \in C} \overline{\phi_v(x)} = \frac{1}{q^{n/2}} \sum\limits_{x \in C} \xi^{-\langle v, x \rangle}$. It is clear that $\sum\limits_{x \in C} \xi^{-\langle v, x \rangle} = |C|$ if and only if all terms are equal to 1. And this is equivalent to the condition $v \perp C$. □

Proposition 11.3. *Let $C \subset Q_q^n$ be a cell of an equitable partition and let $v \in C^\perp$. Then $\lambda = n(q-1) - \mathrm{wt}(v)q$ is an eigenvalue of its quotient matrix.*

Proof. From Proposition 11.2 we have $\widehat{\mathbf{1}_C}(v) = \frac{|C|}{q^{n/2}} \neq 0$. By Proposition 10.5 $\lambda = n(q-1) - \mathrm{wt}(v)q$ is an eigenvalue of the quotient matrix. □

Corollary 11.1. *For any $\Gamma \subset Q_q^n$, $\bar{0} \in \Gamma$, the equality*

$$\widehat{\mathbf{1}_\Gamma} = \frac{q^{\dim \Gamma}}{q^{n/2}} \mathbf{1}_{\Gamma^\perp}$$

holds.

Proof. $\widehat{\mathbf{1}_\Gamma}(v) = \frac{q^{\dim \Gamma}}{q^{n/2}}$ for $v \in \Gamma^\perp$ by Proposition 11.2. From Parseval's identity together with the fact $|\Gamma||\Gamma^\perp| = q^n$ it follows that $\widehat{\mathbf{1}_\Gamma}(u) = 0$ for $u \notin \Gamma^\perp$. □

Every face in the hypercube can be represented as $\Gamma + a$, where the face Γ contains zero. We now determine the Fourier transform of the characteristic function of an arbitrary face. By the properties of the Fourier transform (Proposition 9.13(c)) it follows that $(\widehat{\mathbf{1}_\Gamma(x+a)})(z) = \frac{\phi_a(z) q^{\dim \Gamma}}{q^{n/2}} \mathbf{1}_{\Gamma^\perp}(z)$. Thus, for any $z \in \mathrm{supp}(\widehat{\mathbf{1}_{\Gamma+a}})$ we have $\mathrm{wt}(z) \leq \dim(\Gamma^\perp) = n - \dim(\Gamma)$. Note that Theorem 10.1 is an immediate consequence of Corollary 11.1 and Proposition 2.8.

If q is prime, then Q_q can be regarded as the finite field $GF(q)$ with addition and multiplication modulo q. It is well known from linear algebra that the solution set of a homogeneous system of equations

$$C = \{x \in Q_q^n | Hx = \bar{0}\} \tag{26}$$

is a linear subspace, and conversely, any linear subspace $C \subset Q_q^n$ can be represented as the solution set of a system of equations (26). Recall that the matrix $H = \{h_{ij}\}$ is called a parity-check matrix of the code C. The rows of H belong to the linear code $C^\perp$ and, when they are linearly independent, form its basis. For the linear code $C^\perp$, the matrix H is called a *generator matrix*.

It is easy to see that the system of equations (26) determines an additive code over the ring $\mathbb{Z}_q$ for arbitrary q and rows of H generate the dual code.

Example 11.1. Let $C \subset \mathbb{Z}_4^2$, $C = \{(0,0),(2,2)\}$. By definition C is an additive code. $C^\perp = \{(0,0),(1,1),(2,2),(3,3),(1,3),(3,1)\}$ is also an additive code.

Next, we calculate the minimum distance of a binary code in terms of its generator matrix. Let H be a $t \times n$ binary generator matrix, let $C = \{uH : u \in Q_2^t\}$, and let $M(H)$ be the multiset of columns of H. Define

$$W_{M(H)}(u) = \sum_{a \in M(H)} (-1)^{\langle u,a \rangle}.$$

Proposition 11.4. *The minimum distance of C is*

$$d(C) = \frac{n - \max_{u \neq 0} W_{M(H)}(u)}{2}.$$

Proof. For a fixed $u \neq 0$, a coordinate is one exactly when $\langle u, a \rangle = 1$. Hence $\mathrm{wt}(uH) = \frac{1}{2}\sum_{a \in M(H)}(1 - (-1)^{u \cdot a})$. Taking the minimum over nonzero u gives the formula. □

Proposition 11.5. *If C is an additive code in Q_q^n, then $C = (C^\perp)^\perp$.*

Proof. As mentioned above, $C \subseteq (C^\perp)^\perp \subset C$ for every additive code C. By Corollary 9.3 it follows $|(C^\perp)^\perp| = |C|$. □

Corollary 11.2. *Let q be prime. A code $C \subset Q_q^n$ is linear if and only if $\widehat{\mathbf{1}_C} = \frac{|C|}{q^{n/2}}\mathbf{1}_{C^\perp}$.*

Proof. From the definitions of linear and dual codes we have $\dim C + \dim C^\perp = n$. Hence $|C||C^\perp| = q^n$. Then necessity follows from Proposition 11.2 and Parseval's equality.

From the equalities $\widehat{\mathbf{1}_C} = \frac{|C|}{q^{n/2}}\mathbf{1}_{C^\perp}$ and $\widehat{\widehat{\mathbf{1}_C}} = \mathbf{1}_{-C}$ we obtain $\mathbf{1}_{-C} = \frac{|C|}{q^{n/2}}\widehat{\mathbf{1}_{C^\perp}}$. Since the code $(C^\perp)^\perp$ is linear, $-C$ is also a linear code. Then $C = -C$. □

An affine subspace is a translate of a linear subspace by some vector. The cardinality of any affine subspace in Q_q^n equals q^s for some integer $s \geq 0$. The intersection of two affine subspaces is an affine subspace. In particular, the following proposition holds.

Proposition 11.6. *Let $C \subset Q_q^n$ be a linear code and Γ a face of the hypercube Q_q^n with $\bar{0} \in \Gamma$. Then the cardinality of the intersection $|C \cap (x + \Gamma)|$ equals 0 or q^s for each $x \in Q_q^n$, where s does not depend on x.*

Proof. A system of linear equations over $GF(q)$ has either no solutions or exactly q^s solutions, depending on the right-hand side. The exponent s depends only on the rank of the corresponding system of linear equations and is therefore independent of the right-hand side. □

11.2 Hadamard Code and Plotkin Bound

Proposition 11.7. *Let q be prime and let $C \subset Q_q^n$ be a Hamming code. Then the code $C^\perp$ has the minimum distance $n - \frac{n-1}{q}$ and cardinality $n(q-1)+1$.*

Proof. Since C is a linear code, we have $|C^\perp| = q^n/|C|$. Since C is a 1-perfect code, the number $q^n/|C|$ equals the size of a ball of radius 1, i.e., $n(q-1)+1$. By Proposition 11.3 we obtain that $n(q-1) - \mathrm{wt}(v)q = -1$

for nonzero $v \in C^\perp$ because $\lambda = -1$ is the only nontrivial eigenvalue of a 1-perfect code. Since $C^\perp$ is a linear code, it contains all differences of pairs of codewords and its minimum distance equals the minimum weight of nonzero elements. □

The dual code to the Hamming code is called the Hadamard code. Consider in more detail the binary case $q = 2$. In the binary case the Hadamard code of length n contains $n + 1$ vectors, and all nonzero vectors of the Hadamard code of length n have weight $\frac{n+1}{2}$. We now show that this is optimal, i.e., there exists no code of larger cardinality for the same length with the same (or larger) minimum distance.

Proposition 11.8 (Plotkin bound)**.** *Let the minimum distance of a code $C \subset Q_2^n$ be at least βn, where $\beta > \frac{1}{2}$. Then $|C| \le \frac{1}{2\beta - 1} + 1$.*

Proof. Consider the vectors $(-1)^v = ((-1)^{v_1}, \ldots, (-1)^{v_n})$, where $v \in C$. The squared norm $((-1)^v, (-1)^v)$ equals n for any vector v. If $d(u, v) = r$, then $((-1)^v, (-1)^u) = n - 2r$. We have the inequalities

$$0 \le (\sum_{v \in C} (-1)^v, \sum_{v \in C} (-1)^v) \le mn + 2\binom{m}{2}(n - 2\beta n),$$

where $m = |C|$. Then $0 \le 1 + (m - 1)(1 - 2\beta)$. □

The inequality proved in Proposition 11.8 is known as the Plotkin bound. Substituting the minimum distance and cardinality of the Hadamard code into it, it is easy to see that the Hadamard code attains the Plotkin bound.

For the existence of a 1-perfect code in Q_2^n it is necessary and sufficient that $n = 2^t - 1$ (see Proposition 1.3). Therefore, the minimum distance $\frac{n+1}{2}$ of the Hadamard code is even. Hence balls of radius $\frac{n-1}{4}$ with centers at the vertices of the Hadamard code do not intersect, and vertices at distance $\frac{n+1}{4}$ from a codeword are not contained in such balls. Consequently, the binary Hadamard code can correct $\frac{n-1}{4}$ errors and detect $\frac{n+1}{4}$ errors.

A generalization of the Plotkin bound to q-ary codes will be proven in Section 12.2.

11.3 Extended 1-Perfect Code

To each vector v of a binary 1-perfect code C, we add one more coordinate equal to the parity of its weight, $|v| = v_1 + \cdots + v_n \mod 2$. The code $\overline{C} = \{(|v|, v) \mid v \in C\}$ is called the *extended 1-perfect code*. Since all vectors of the code $\overline{C}$ have even weight, the minimum distance of $\overline{C}$ is even and at

least the minimum distance of C. Therefore the code distance of $\overline{C}$ equals 4.

The extended 1-perfect code can be regarded as a perfect coloring of the Boolean hypercube into three colors. Let $f = \mathbf{1}_C$ be a perfect coloring with quotient matrix $S = \begin{pmatrix} 0 & n \\ 1 & n-1 \end{pmatrix}$. The coloring $f'(x_0, \overline{x}) = f(\overline{x})$, obtained by copying the coloring f to the two parallel hyperfaces, has quotient matrix $S + I = \begin{pmatrix} 1 & n \\ 1 & n \end{pmatrix}$. The non-trivial eigenvalue 0 of this matrix does not coincide with the non-trivial eigenvalue $-(n+1)$ of the parity counter in Q_2^{n+1}. Proposition 2.8 implies that half of the vertices of each color have even weight, and the other half have odd weight. Since vertices of the same parity in the Boolean hypercube are not adjacent, we can split each of the colors into even and odd, and obtain a perfect coloring with quotient matrix $\begin{pmatrix} 0 & 0 & 1 & n \\ 0 & 0 & 1 & n \\ 1 & n & 0 & 0 \\ 1 & n & 0 & 0 \end{pmatrix}$. The first color class in the resulting perfect coloring is the extended 1-perfect code by construction. It follows from the matrix that the first two colors (as well as the two other ones) are equivalent. By Corollary 4.4 after merging the last two colors we obtain a perfect coloring with quotient matrix $\overline{S} = \begin{pmatrix} 0 & 0 & n+1 \\ 0 & 0 & n+1 \\ 1 & n & 0 \end{pmatrix}$.

The linearity of C implies the linearity of $\overline{C}$. It is easy to see that the parity-check matrix $\overline{H}$ of the code $\overline{C}$ is obtained from the parity-check matrix of the binary Hamming code by first adding a column of all zeros and then a row of all ones.

Example 11.2. The parity-check matrix of the extended Hamming code of length 8 is $\overline{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$.

Since the eigenvalues of the quotient matrix $\overline{S}$ are $0, \pm(n+1)$, Proposition 11.3 implies that every codeword of the dual code $\overline{C}^{\perp}$ has weight 0, m, or $m/2$, where $m = n+1$ is the code length. Then for any vectors $u, v \in \overline{C}^{\perp}$ either $(-1)^u = -(-1)^v$, or $((-1)^v, (-1)^u) = m - 2d(u,v) = 0$. From the equalities $|\overline{C}||\overline{C}^{\perp}| = 2^m$ and $|\overline{C}| = |C| = 2^{m-1}/m$ we have $|\overline{C}^{\perp}| = 2m$.

Choosing one vector from each pair of opposite vectors of the code $\overline{C}^{\perp}$, we obtain a set of m orthogonal vectors in m-dimensional space. Thus, taking these vectors as rows, we obtain a Hadamard matrix (see Section 18.4). It can be shown by induction that the Hadamard matrix obtained from the linear Hadamard code is the Hadamard–Sylvester matrix.

11.4 Sarkar's Identity

Theorem 11.1 (Sarkar at al. [26], [146], and [99]). *Let $f : Q_q^n \to \mathbb{C}$. Then (a) For every face $\Gamma \subset Q_q^n$, $\bar{0} \in \Gamma$, the equality $\widehat{f} * \mathbf{1}_{\Gamma^\perp} = q^{n-\dim \Gamma} \widehat{f \cdot \mathbf{1}_\Gamma}$ holds. (b) Let q be prime. For every linear code $C \subset Q_q^n$, the equality $\widehat{f} * \mathbf{1}_{C^\perp} = q^{n-\dim C} \widehat{f \cdot \mathbf{1}_C}$ holds.*

Proof. (a) From Proposition 9.18 we have the equality $\widehat{f} * \widehat{\mathbf{1}_\Gamma} = q^{n/2} \widehat{f \cdot \mathbf{1}_\Gamma}$. Next we use the equality $\widehat{\mathbf{1}_\Gamma} = \frac{q^{\dim \Gamma}}{q^{n/2}} \mathbf{1}_{\Gamma^\perp}$ (Corollary 11.1).

(b) Replacing Corollary 11.1 with Corollary 11.2, we obtain part (b) in the same way as part (a). □

From the Sarkar's identity or Theorem 9.15 one can deduce

Corollary 11.3 ([129]). *Let $f : Q_q^n \to \mathbb{C}$ and let the face Γ contain $\bar{0}$. Then* $\sum\limits_{z \in \Gamma^\perp} \widehat{f}(z) = q^{n/2 - \dim \Gamma} \sum\limits_{x \in \Gamma} f(x)$.

Proof. By the Sarkar's identity we have the equalities

$$\widehat{f} * \mathbf{1}_{\Gamma^\perp}(0) = q^{n-\dim \Gamma} \widehat{f \cdot \mathbf{1}_\Gamma}(0), \text{ hence}$$

$$\sum_{z \in \Gamma^\perp} \widehat{f}(z) = q^{n-\dim \Gamma} \cdot \frac{1}{q^{n/2}} \sum_{x \in \Gamma} f(x) \phi_0(x).$$

Since $\phi_0(x) = 1$, we obtain the required equality. □

Note that this corollary can also be obtained by using Proposition 9.10 (Plancherel's theorem).

Theorem 11.2 ([29], [142]). *Let $f : Q_2^n \to \{0, 1\}$ be a Boolean function, $\mathrm{cor}(f) = k$. Then the coefficients $\widehat{f}(z)$ have the form $2^{k - \frac{n}{2}} \cdot m$, where m is an integer. If the function f is resilient, then the coefficients $\widehat{f}(z)$ have the form $2^{1 + k - \frac{n}{2}} \cdot m$, where m is an integer.*

Proof. By Theorem 10.1, $\widehat{f}(z) = 0$ for $0 < \mathrm{wt}(z) \le k$. We first prove the statement for coefficients satisfying $\widehat{f}(z)$ with $\mathrm{wt}(z) = k+1$. Consider an $(n-k-1)$-dimensional face Γ. The face $\Gamma^\perp$, $\bar{0} \in \Gamma$, has dimension $\dim \Gamma^\perp = k+1$ and contains exactly one n-tuple z of weight $k+1$. Hence, by Corollary 11.3 we have the equality

$$\widehat{f}(z) + \widehat{f}(\bar{0}) = 2^{\frac{n}{2}-(n-k-1)} \cdot \sum_{x \in \Gamma} f(x).$$

Let $m'' = \sum\limits_{x \in \Gamma} f(x)$ be the number of values 1 of f in the face Γ. The number of ones of f in every $(n-k)$-dimensional face is the same, since $\mathrm{cor}(f) = k$. Let it be m'. Then $\widehat{f}(\bar{0}) = 2^{-\frac{n}{2}+k} \cdot m'$. Thus, we obtain the equality

$$\widehat{f}(z) = 2^{k+1-\frac{n}{2}} \cdot m'' - 2^{-\frac{n}{2}+k} \cdot m' = 2^{k-\frac{n}{2}} \cdot m.$$

For a resilient function we have $\widehat{f}(\bar{0}) = \frac{1}{2^{n/2}} \sum\limits_{x \in Q_2^n} f(x) = 2^{\frac{n}{2}-1}$. For $k \le n-2$ it holds that $k+1-\frac{n}{2} \le \frac{n}{2}-1$. Boolean functions with $\mathrm{cor}(f) > n-2$ are only the parity counter, its negation and constants. In these cases we can verify the required equality directly.

For the coefficients $\widehat{f}(z)$ with $\mathrm{wt}(z) = k+s$, $s > 1$, the statement can be proved by induction on s. Indeed, consider a face Γ of dimension $n-k-s$. The face $\Gamma^\perp$ of dimension $k+s$ contains only one vertex of weight $k+s$, for vertices of smaller weight the statement has already been established by the induction hypothesis. □

Remark 11.2 ([142])**.** If instead of the Boolean function f we consider the function $(-1)^f$, then a similar argument shows that $\widehat{(-1)^f}(z) = 2^{k-n/2+1}m$, where m is an integer, since the function $(-1)^f$ has even sums in all faces of nonzero dimension. If the function f is resilient, then $\widehat{(-1)^f}(z) = 2^{k-n/2+1}m$, where m is even, when $k < n-1$, since in this case every $(n-k)$-dimensional face contains an even number of ones and the second term $\widehat{(-1)^f}(\bar{0})$ equals zero.

Corollary 11.4. *Let $f : Q_2^n \to \{0,1\}$. If $\widehat{(-1)^f}(z) = 0$ for $\mathrm{wt}(z) \ge k$, then all coefficients $\widehat{(-1)^f}(z)$ have the form $m2^{\frac{n}{2}-k+1}$, where m is an integer.*

Proof. Let $g(x) = f(x) \oplus x_1 \oplus \cdots \oplus x_n$. $\widehat{(-1)^g}(z) = \widehat{(-1)^f}(z \oplus \bar{1})$ by Proposition 9.13 (c). Then $\widehat{(-1)^g}(z) = 0$ for $\mathrm{wt}(z) \le n-k$. Consequently, by Theorem 11.2, $\widehat{(-1)^g}(z) = 2^{n-k-n/2+1}m$, where m is an integer. □

11.5 Relevant Variables of Perfect Colorings

The following theorem is a direct application of the Nisan–Szegedy theorem [112] to perfect colorings.

Theorem 11.3 (Valyuzhenich [148]). *Let f be a perfect coloring of Q_2^n with quotient matrix $S = \begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$. Then the number of relevant variables of f does not exceed $\frac{bc2^{(b+c)/2}}{b+c}$.*

Proof. Without loss of generality, assume that f takes values ± 1. Proposition 10.5 implies that $\widehat{f}(z) \neq 0$ only if $n-(b+c) = n - 2\mathrm{wt}(z)$, i.e., $\mathrm{wt}(z) = (b+c)/2$ or $z = \bar{0}$. Therefore, by Corollary 11.4 every coefficient $\widehat{f}(z)$ has the form $m2^{\frac{n-(b+c)}{2}+1}$, where m is an integer. Let f_0 and f_1 be the restrictions of f to the hyperfaces defined by the equations $x_n = 0$ and $x_n = 1$, respectively. Denote the $(n-1)$-variable function $h = f_0 - f_1$. It is easy to verify directly that

$$\widehat{h}(z_1, \dots, z_{n-1}) = \frac{1}{\sqrt{2}}(f(x) - \widehat{f(x \oplus e_n)})(z_1, \dots, z_{n-1}, 1).$$

Therefore the coefficients $\widehat{h}$ are divisible by $2^{\frac{n-(b+c)+1}{2}}$.

Since h takes values in $\{0, \pm 2\}$, from Parseval's identity we have

$$4|\mathrm{supp}(h)| = \|h\|^2 = \|\widehat{h}\|^2 \geq 2^{n-(b+c)+1}|\mathrm{supp}(\widehat{h})|.$$

By Proposition 9.14 we have

$$|\mathrm{supp}(h)| \geq \frac{2^{n-1}}{|\mathrm{supp}(\widehat{h})|}.$$

Then

$$|\mathrm{supp}(h)| \geq \frac{2^{2n-(b+c)-2}}{|\mathrm{supp}(h)|}.$$

Thus, $|\mathrm{supp}(h)| \geq 2^{n-1-(b+c)/2}$.

Consequently, if f depends essentially on the n-th coordinate, then the values of f differ in at least $2^{n-1-(b+c)/2}$ vertices adjacent along this coordinate. Hence if f depends essentially on t coordinates, then $I[f] \geq t2^{n-1-(b+c)/2}$, where $I(f)$ is the number of edges whose endpoints have different values. On the other hand, by Proposition 10.8 and Theorem 10.4 we have

$$I[f] = 2^{n-1}(b+c)(\rho(f) - \rho^2(f)),$$

where $\rho(f) = \frac{c}{b+c}$ or $\rho(f) = \frac{b}{b+c}$. Then $t \leq \frac{2^{(b+c)/2}bc}{b+c}$. □

11.6 Testing Sets of Perfect Colorings

Consider the generalized Hadamard matrix $H_{q,n}$ whose rows are characters, i.e., $H_{q,n}(z,x) = \phi_z(x)$. Let A_d be the square matrix obtained from $H_{q,n}$ by selecting the rows and columns corresponding to vertices of weight at least d.

Proposition 11.9. *(a) For any $d \geq 0$, the matrix A_d is nondegenerate.*

(b) If $f(x) = 0$ for all $x \in Q_q^n$ with $\mathrm{wt}(x) \leq d$ and $\widehat{f}(z) = 0$ for all $z \in Q_q^n$ with $\mathrm{wt}(z) > d$, then $f = \mathbf{0}$.

Proof. By definition of $H_{q,n}$ we have $\frac{1}{q^{n/2}} H_{q,n} f = \widehat{f}$. The matrix A_d is degenerate if and only if there exists a nonzero solution $A_d u = 0$. By definition of A_d this solution is a function $f : Q_q^n \to \mathbb{C}$ such that $f(x) = 0$ if $\mathrm{wt}(x) > d$ and $\widehat{f}(z) = 0$ for $\mathrm{wt}(z) \leq d$. So, the conditions (a) and (b) are equivalent. It therefore suffices to prove (b).

By the condition of the proposition, $f \cdot \mathbf{1}_\Gamma = 0$ for any face Γ of dimension d containing $\bar{0}$. From Sarkar's identity (Theorem 11.1 (a)) we have $\widehat{f} * \mathbf{1}_{\Gamma^\perp} = 0$. Thus, the sum of the values of $\widehat{f}$ over any face of dimension $n-d$ (not necessarily containing $\bar{0}$) equals zero. It is clear that $\widehat{f}$ is also balanced in faces of larger dimension. For each vertex a of weight d there exists a face $\Gamma_a = \{y \in Q_q^n : y_i = a_i, \text{ if } a_i \neq 0\}$ of dimension $n-d$, which contains exactly one vertex of weight d and the remaining vertices have larger weight. From the definition of $\widehat{f}$ we have $\widehat{f}(a) = 0$. Thus, we have shown that $\widehat{f}$ equals zero on any vertex of weight d. Using faces of dimension $n-d+1$ we can similarly show that $\widehat{f}$ equals zero on vertices of weight $d-1$. Then, by induction we obtain $\widehat{f} = \mathbf{0}$ and, consequently, $f = \mathbf{0}$. □

Proposition 11.10. *An eigenfunction f in Q_q^n with eigenvalue $\lambda_k = n(q-1) - qk$ is uniquely determined by its values in the ball $B_k = \{x \in Q_q^n : \mathrm{wt}(x) \leq k\}$.*

Proof. Suppose that f is not uniquely determined by its values in the ball $B_k = \{x \in Q_q^n : \mathrm{wt}(x) \leq k\}$, i.e., there exists an eigenfunction f' with eigenvalue λ_k such that $f|_{B_k} = f'|_{B_k}$. Consider the difference $g = f - f'$. By Proposition 9.12, $\widehat{g}(z) \neq 0$ only if $\mathrm{wt}(z) = k$. Consequently, $g|_{B_k} = 0$ and $\widehat{g}|_{Q_q^n \setminus B_k} = 0$. By Proposition 11.9 (b), $g = 0$. □

By Proposition 7.5 (see also Problem 59) and Proposition 11.10, it follows

Corollary 11.5. *If $k < n/2$, then an eigenfunction f in Q_q^n with eigenvalue $\lambda_k = n(q-1) - qk$ is uniquely determined by its values on the two spheres A_k and A_{k-1}.*

In the paper [151], sufficient conditions are given for recovering an eigenfunction from a single sphere. Corollary 11.5 and Remark 2.6 allow us to generalize Theorem 10.2 to the q-ary hypercube.

Corollary 11.6. *Let f be a perfect coloring of Q_q^n with quotient matrix S. Let v be an eigenvector of S corresponding to the eigenvalue $\lambda_k = n(q-1) - qk$, with $k < n/2$. If all coordinates of v are distinct, then f is uniquely determined by its values on the two spheres A_k and A_{k-1}.*

11.7 Problems

84. Let $f : Q_q^n \to \mathbb{C}$ and let $C \subset Q_q^n$ be a linear code. Prove that $\frac{1}{q^{n/2}} \sum\limits_{x \in C} f(x) = \frac{1}{|C^\perp|} \sum\limits_{z \in C^\perp} \widehat{f}(z)$.

85. Let $A \subset Q_q^n$, q prime, and $C = \mathrm{supp}(\widehat{\mathbf{1}_A})$. Prove that for any $v \in Q_q^n$ the equality $A + v = A$ holds if and only if $v \in C^\perp$.

86. Let $C \subset Q_q^n$, q prime, and $f = \widehat{\mathbf{1}_C}$. Prove that $|f| = c\mathbf{1}_A$ for some $c > 0$ and $A \subset Q_q^n$ if and only if C and A are affine subspaces.

87. Prove that if every pair of vectors in an n-dimensional Euclidean space forms either an obtuse or a right angle, then their number does not exceed $2n$. Prove that the cardinality of a binary code of length $2n$ with code distance at least n does not exceed $4n$.

88. Prove that two distinct correlation-immune functions of order k in the Boolean hypercube differ from each other on a set of cardinality at least 2^{k+1}.

89. Let $\Gamma \subset Q_2^n$ be an arbitrary face containing $\bar{0}$. Suppose two Boolean functions f and g satisfy $\widehat{f}|_\Gamma = \widehat{g}|_\Gamma$. Prove that the equality $\sum\limits_{x \in z \oplus \Gamma^\perp} (-1)^{f(x)} = \sum\limits_{x \in z \oplus \Gamma^\perp} (-1)^{g(x)}$ holds for any $z \in Q_2^n$.

90. Let $f : Q_2^n \to \{0,1\}$ be a perfect coloring with the largest eigenvalue other than n is $\lambda = n - 2k$. Prove that the function f is completely determined by its values in the ball of radius $n - k$.

12 MacWilliams Identity and Weight Distributions

12.1 MacWilliams Transform

Let M be the adjacency matrix of the hypercube Q_q^n. Recall that $M_k = P_k(M)$, where M_k is the distance-k adjacency matrix and P_k is the q-ary

Krawtchouk polynomial of degree k. If $M\psi = \lambda\psi$, then from Proposition 7.3 we have the equality $\sum\limits_{x,d(x,a)=k} \psi(x) = (M_k\psi)(a) = P_k(\lambda)\psi(a)$. Since the eigenvalue of a character ϕ_z depends only on the weight $\mathrm{wt}(z)$, we will further index the eigenvalues by the weights of their corresponding characters $M\phi_z(x) = \lambda_{\mathrm{wt}(z)}\phi_z(x)$.

Consider an arbitrary function $f : Q_q^n \to \mathbb{C}$. Introduce the notation $A_k[f] = \sum\limits_{x,d(x,\bar{0})=k} f(x)$ and $\widehat{A}_k[f] = \sum\limits_{z,d(z,\bar{0})=k} \widehat{f}(z)$ for the *weight distribution* of the function and its Fourier transform.

Proposition 12.1 ([99]). *Let $f : Q_q^n \to \mathbb{C}$. Then $\widehat{A}_k[f] = \frac{1}{q^{n/2}} \sum\limits_m P_k(\lambda_m)A_m[f]$.*

Proof. Taking into account that $\overline{\phi_z} = \phi_{-z}$, from the definitions we obtain the chain of equalities

$$\widehat{A}_k[f] = \frac{1}{q^{n/2}} \sum_{z,d(z,\bar{0})=k} \sum_x f(x)\overline{\phi_z(x)} = \frac{1}{q^{n/2}} \sum_x f(x) \sum_{z,d(z,\bar{0})=k} \phi_z(x) =$$

$$= \frac{1}{q^{n/2}} \sum_x f(x) \sum_{z,d(z,\bar{0})=k} \phi_x(z) = \frac{1}{q^{n/2}} \sum_x f(x)P_k(\lambda_{\mathrm{wt}(x)}) = \frac{1}{q^{n/2}} \sum_{m=0}^{n} P_k(\lambda_m)A_m[f].$$

□

Note that Proposition 12.1 can be regarded as a special case of Proposition 9.10 (Plancherel's theorem), where the indicator of the sphere of radius k is taken as the second function.

The linear transform taking the coefficients $A_m[f]$ into the coefficients $\widehat{A}_k[f]$ is called the *MacWilliams transform*. From the formula $\widehat{\widehat{f(x)}} = f(-x)$ it follows that the MacWilliams transform is nondegenerate and idempotent for $q = 2$.

Assume that q is a prime number and that C is a linear code. Denote $A_k(C) = A_k[\mathbf{1}_C]$. Then from Proposition 12.1 and Corollary 11.2 we have

$$|C|A_k(C^\perp) = \sum_m P_k(\lambda_m)A_m(C).$$

The latter equality is called the *MacWilliams identity*. Note that the MacWilliams identity can be proved using Problems 65 and 84.

Let C be a code. Note that the number $f_C(a) = (\mathbf{1}_C * \mathbf{1}_{-C})(a)$ is the number of ordered pairs $(x, x-a)$ of vertices of the code differing by the

vector a. Define the weight spectrum $(A_0[C], \ldots, A_n[C])$ of the code C as $\frac{1}{|C|}(A_0[f_C], \ldots, A_n[f_C])$. Note that $A_0[f_C] = \sum_x \mathbf{1}_C^2(x) = |C|$ and

$$\sum_m A_m[C] = \frac{1}{|C|} \sum_x f_C(x) = \frac{1}{|C|} \sum_x \sum_a \mathbf{1}_C(x)\mathbf{1}_C(x-a) = |C|.$$

By the definition of a linear code, $\mathbf{1}_C * \mathbf{1}_{-C} = |C|\mathbf{1}_C$. Therefore for a linear code $(A_0[C], \ldots, A_n[C]) = (A_0(C), \ldots, A_n(C))$.

Then $\widehat{A}_k[\mathbf{1}_C * \mathbf{1}_{-C}] = \widehat{A}_k[f_C] = \frac{1}{q^{n/2}} \sum_m P_k(\lambda_m) A_m[f_C]$. Moreover, $\widehat{\mathbf{1}_C * \mathbf{1}_{-C}} = q^{n/2}|\widehat{\mathbf{1}_C}|^2$ by Propositions 9.13 and 9.17. By Proposition 12.1 for any k, $0 \le k \le n$, we have the equality

$$q^n \cdot \sum_{z, \mathrm{wt}(z)=k} |\widehat{\mathbf{1}_C}(z)|^2 = |C| \sum_m P_k(\lambda_m) A_m[C]. \tag{27}$$

12.2 Linear Programming Bound

The equalities (27) provide the basis for applying linear programming methods to compute an upper bound on the size of a code with minimum distance d. Indeed, if the code C does not contain two vertices at distance less than d, then $A_m[C] = 0$ for $m = 1, \ldots, d-1$, since $\mathbf{1}_C * \mathbf{1}_{-C}(y) = 0$ for $0 < \mathrm{wt}(y) < d$. From this we obtain a *linear programming problem* on the set of quantities $A_m[C]$ to find an upper bound on the size of a code with code distance d:

$$P_k(\lambda_0) + \sum_{m \ge d} P_k(\lambda_m) A_m[C] \ge 0 \text{ for any } k \tag{28}$$

$$|C| = 1 + \sum_{m \ge d} A_m[C] \to \max.$$

It is known that every solution of the dual minimization problem is an upper bound for the value of the linear programming problem, i.e., for the code size in this case. This is the basis for the linear programming bound on the size of a code with known minimum distance, which is proved in the following theorem.

Theorem 12.1 (Delsarte [35]). *Let C be a code in Q_q^n with code distance d, and let $(y_0, \ldots, y_n) \in \mathbb{R}^{n+1}$ satisfy the conditions $y_0 > 0$, $y_i \ge 0$ for $i = 1, \ldots, n$, and $\sum_{k=0}^{n} y_k P_k(\lambda_m) \le 0$ for $m \ge d$. Then $|C| \le \frac{1}{y_0} \sum_{k=0}^{n} y_k P_k(\lambda_0)$.*

Proof. As before, we formally assume that the polynomial $P_0(x)$ is identically equal to one. Then $|C| = P_0(\lambda_0) + \sum\limits_{m \geq d} P_0(\lambda_m) A_m[C]$. By the assumption of the theorem and (28) we obtain the inequalities

$$y_0|C| \leq \sum_{k=0}^{n} y_k \left(P_k(\lambda_0) + \sum_{m \geq d} P_k(\lambda_m) A_m[C] \right)$$

$$\leq \sum_{k=0}^{n} y_k P_k(\lambda_0) + \sum_{m \geq d} A_m[C] \left(\sum_{k=0}^{n} y_k P_k(\lambda_m) \right) \leq \sum_{k=0}^{n} y_k P_k(\lambda_0).$$

□

Note that $P_i(\lambda_0)$ is the size of a ball of radius i in Q_q^n.

Let us discuss how to obtain upper bounds on code size using linear programming. Suppose that we wish to bound the size of a code whose pairwise distances between vertices take values only from a list $W = \{w_1, \ldots, w_m\}$. Consider a polynomial R of degree m such that $R(\lambda_{w_i}) \leq 0$, where $\lambda_{w_i} = n(q-1) - qw_i$ for $i = 1, \ldots, m$. Any polynomial of degree at most m can be represented as a linear combination of the polynomials P_i for $i = 0, 1, \ldots, m$. Let $R = \sum\limits_{i=0}^{m} y_i P_i$. If $y_0 > 0$ and $y_i \geq 0$ for $i = 1, \ldots, m$, then Theorem 12.1 implies the inequality $|C| \leq \frac{1}{y_0} \sum\limits_{i=0}^{m} y_i P_i(\lambda_0) = R(\lambda_0)/y_0$.

As an example, let us prove the Plotkin bound on the size of a code with large minimum distance. Let the minimum distance of code be $d_C > (1 - \frac{1}{q})n$, i.e., if $w_i \in W$, then $w_i \geq d_C$ and $\lambda_{w_i} = n(q-1) - qw_i \leq n(q-1) - qd_C < 0$. Consider the polynomial $R(x) = 1 - \frac{x}{n(q-1)-qd_C}$.

$$R(\lambda_{w_i}) = 1 - \frac{n(q-1) - qw_i}{n(q-1) - qd_C} \leq 0$$

for all $w_i \in W$. Then

$$|C| \leq R(\lambda_0) = 1 - \frac{n(q-1)}{n(q-1) - qd_C} = \frac{qd_C}{qd_C - n(q-1)}. \tag{29}$$

Inequality (29) is the Plotkin bound (Proposition 11.8) for q-ary codes. In the case $q = 2$ and $d_C = \frac{n+1}{2}$, n odd, we obtain the Hadamard bound $|C| \leq n + 1$.

Note that Theorem 12.1 remains true not only for codes but also for any functions $F : Q_q^n \to \mathbb{R}$, provided $A'_k[F] = \sum_{\mathrm{wt}(x)=k} F(x) \geq 0$ and

$A'_0[F] = 1$. In this case the role of the code size is played by the sum of the values of F, i.e., $\sum_{k=0}^{n} A'_k[F]$. Consider a correlation-immune function $f = \mathbf{1}_C$, $\mathrm{cor}(f) + 1 > (1 - \frac{1}{q})n$, and define $F = \frac{q^{n/2}\widehat{f * f}}{|C|^2}$. Then $F(x) = \frac{q^n |\widehat{f}(x)|^2}{|C|^2}$, i.e., $A'_k[F] \geq 0$, $A'_0[F] = 1$, $A'_k[F] = 0$ for $k \leq \mathrm{cor}(f)$. For this function the Plotkin bound (29) also holds:

$$\sum_{k=0}^{n} A'_k[F] \leq \frac{q(\mathrm{cor}(f)+1)}{q(\mathrm{cor}(f)+1) - n(q-1)}.$$

Moreover, from Parseval's identity we have $\sum_{k=0}^{n} A'_k[F] = q^n/|C|$. Then we obtain

$$\frac{|C|}{q^n} \geq 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}.$$

Thus, we recover the Bierbrauer–Friedman bound (Theorem 10.5), which is called the dual Plotkin bound in [15].

12.3 Few-Weight Codes

A *few-weight code* is a code in which the set of nonzero codeword weights (or, for non-linear codes, the set of pairwise distances between codewords) contains only a small number of distinct values. For example, the Hadamard code is an *equidistant or constant-weight code*. In this section we estimate the cardinality of few-weight codes.

Theorem 12.2 (Delsarte [36]). *Let $f : Q_q^n \to \mathbb{C}$, and suppose there exist k nonzero weights $W = \{w_1, \ldots, w_k\}$ such that $\widehat{f}(x) = 0$ for $\mathrm{wt}(x) \notin W$ and $\widehat{f}(\bar{0}) \neq 0$. Then $|\mathrm{supp}(f)| \geq q^n/b(q,k)$, where $b(q,k)$ is the cardinality of a ball of radius k.*

Proof. Let $\lambda_i = n(q-1) - qw_i$ be the eigenvalue corresponding to weight w_i. By assumption, we have $f = \rho\mathbf{1} + \sum_{i=1}^{k} \varphi_i$, where φ_i is an eigenfunction with eigenvalue λ_i and $\rho = \frac{\widehat{f}(\bar{0})}{q^{n/2}} \neq 0$. Let $A = (M - \lambda_1 I) \cdots (M - \lambda_k I)$ be a polynomial in M of degree k, where M is the adjacency matrix of the hypercube Q_q^n. We have $Af = \rho A\mathbf{1}$, since $A\varphi_i = \bar{0}$. From the equality $M\mathbf{1} = n(q-1)$ it follows that $A\mathbf{1} = (n(q-1) - \lambda_1) \cdots (n(q-1) - \lambda_k)\mathbf{1} = \alpha\mathbf{1}$, where $\alpha \neq 0$.

On the other hand, since the q-ary hypercube is a distance-regular graph, every polynomial of M is a linear combination of distance-i adjacency matrices. Thus, $A = \sum_{i=0}^{k} \beta_i M_i$, where M_i is the distance-i adjacency matrix. Hence $Af = g * f$, where $\mathrm{supp}(g)$ is contained in the ball of radius k. For any $x \in Q_q^n$ we have $0 \neq Af(x) = g * f(x)$. Therefore every ball of radius k contains at least one vertex $y \in Q_q^n$ such that $f(y) \neq 0$. □

We can consider Theorem 12.2 as a generalization of the simple fact that every cell of an equitable $(k+1)$-partition intersects every ball of radius k.

Corollary 12.1. *Let a linear code $C \subset Q_q^n$ contain words of only k distinct nonzero weights. Then $|C| \leq b(q,k)$.*

Proof. Consider the dual code $C^\perp$. By Delsarte's theorem we obtain $|C^\perp| \geq q^n/b(q,k)$. From the equality $|C||C^\perp| = q^n$ we obtain the desired inequality. □

However, the statement of Corollary 12.1 remains true for nonlinear codes as well. We prove this in the case $q = 2$.

Theorem 12.3 (Delsarte [36])**.** *Let a code $C \subset Q_2^n$ consist of codewords whose pairwise distances take only k distinct nonzero values. Then $|C| \leq b(2,k)$.*

Proof. Let D be the set of pairwise distances of the code C, $|D| = k$. Consider the set of functions $f : \{-1,1\}^n \to \mathbb{R}$ as a 2^n-dimensional linear space V_n. It is easy to see that the monomials of the form $x_{i_1} \cdots x_{i_m}$, $m = 0, \ldots, n$, form an orthogonal basis of V_n, which corresponds to the basis of characters of the group $\mathbb{Z}_2^n$.

To each codeword $v \in C$ we associate the function

$$f_v(x) = \prod_{t \in D} (((-1)^v, x) - (n - 2t)).$$

Since $((-1)^v, (-1)^u) = n - 2d(u,v)$, we have $f_v((-1)^u) = 0$ for any $u \in Q_2^n$ such that $d(u,v) \in D$, and $f_v((-1)^v) \neq 0$. Let us show that the set of functions $\{f_v : v \in C\}$ is linearly independent. Let $L = \sum_{v \in C} \alpha_v f_v = 0$. Then $L((-1)^v) = \alpha_v f_v((-1)^v) = 0$ and $\alpha_v = 0$.

Each function f_v is a polynomial of degree at most k, in which the basis is formed by monomials of degree at most k. The number of monomials of degree at most k equals $b(2,k)$. □

12.4 Weight Distributions of Perfect Colorings

The weight distribution of a 2-coloring of the hypercube completely determines whether the coloring is perfect.

Proposition 12.2. *Let C be a code in the hypercube Q_q^n, and let its weight distribution $(A_0[C], \dots, A_n[C])$ be the same as that of a cell B of some equitable 2-partition with quotient matrix S. Then $\mathbf{1}_C$ is a perfect 2-coloring with the same quotient matrix.*

Proof. The function $\mathbf{1}_C$ is a perfect 2-coloring if and only if $\mathrm{supp}(\widehat{\mathbf{1}_C})$ contains only the zero vector and vectors of some fixed weight (see Propositions 2.7 and 10.5). By the formula $q^n \cdot \sum\limits_{z,\mathrm{wt}(z)=k} |\widehat{\mathbf{1}_C}(z)|^2 = |C| \sum\limits_m P_k(\lambda_m) A_m[C]$ the Fourier weight distributions of C and B coincide. Thus, $\mathbf{1}_C$ is a perfect 2-coloring. By the weight distribution we can also determine its quotient matrix. Indeed, if $S = \begin{pmatrix} (q-1)n-b & b \\ c & (q-1)n-c \end{pmatrix}$ then the nontrivial eigenvalue equals $(q-1)n-b-c$. It can be found from the Fourier weight distribution of C. Moreover, $\frac{b}{c} = \frac{|C|}{q^n-|C|}$ if C is the first cell of the partition and $\frac{b}{c} = \frac{q^n-|C|}{|C|}$ if C is the second one. □

By Theorem 6.1 the following statement follows directly.

Proposition 12.3. *Let f be a k-coloring of an amply regular graph. Suppose that for every i, $i = 1, \dots, k$, the averaged color composition of the neighborhood of the i-th color C_i of the coloring f is the same as that of the i-th color D_i of a perfect coloring g. If $A_2[C_i] = A_2[D_i]$ for every i, $i = 1, \dots, k$, then f is a perfect coloring with the same quotient matrix as g.*

For the case of 2 colors Proposition 12.3 implies that the first three weight coefficients $A_0[C], A_1[C], A_2[C]$ of C and the first three weight coefficients $(A_0[Q_q^n \setminus C], A_1[Q_q^n \setminus C], A_2[Q_q^n \setminus C])$ of its complement are sufficient to determine whether the coloring is perfect.

By Proposition 9.13, for any function taking only real values, the equalities $\widehat{f(-x)} = \overline{\widehat{f(x)}}$ and $\widehat{\widehat{f(-x)}} = f(x)$ hold. Therefore, the equality $\widehat{A}_k[f] = \frac{1}{q^{n/2}} \sum\limits_m P_k(\lambda_m) A_m[f]$ can be inverted:

$$A_k[f] = \frac{1}{q^{n/2}} \sum_m P_k(\lambda_m) \widehat{A}_m[f(-x)] = \frac{1}{q^{n/2}} \sum_m P_k(\lambda_m) \overline{\widehat{A}_m[f]}.$$

In particular it means that the matrix $W = (P_k(\lambda_m))_{k,m}$ is nondegenerate.

Moreover, MacWilliams identity can be rewritten for the case of Cartesian products. Suppose $K = Q_{q_1}^{n_1} \times Q_{q_2}^{n_2}$. Proposition 9.4 implies that the basis of characters on K consists of products of characters of $Q_{q_1}^{n_1}$ and characters of $Q_{q_2}^{n_2}$. For a function $f : K \to \mathbb{C}$ we define $A_{k_1k_2}[f] = \sum_{\mathrm{wt}(x_1)=k_1} \sum_{\mathrm{wt}(x_2)=k_2} f(x_1, x_2)$ and $\widehat{A}_{k_1k_2}[f] = \sum_{wt(z_1)=k_1} \sum_{\mathrm{wt}(z_2)=k_2} \widehat{f}(z_1, z_2)$. Then, by arguments similar to the proof of Proposition 12.1, we obtain the equality

$$\widehat{A}_{k_1k_2}[f] = \frac{1}{q_1^{n_1/2} q_2^{n_2/2}} \sum_{m_1,m_2} P_{k_1}[n_1, q_1](\lambda_{m_1}) P_{k_2}[n_2, q_2](\lambda_{m_2}) A_{m_1m_2}[f]. \tag{30}$$

In equality (30), the coefficients $\widehat{A}_{k_1k_2}[f]$ and $A_{k_1k_2}[f]$ can also be swapped (with the addition of complex conjugation if $q \neq 2$).

Let $f : Q_q^n \to \mathbb{C}$ and let $\Gamma \subset Q_q^n$ be some face. Define the local distribution of the function f in the face Γ as the weight distribution of the restriction $f|_\Gamma$ of f to the face Γ.

Theorem 12.4 (Vasil'eva [149]). *Let $g : Q_q^n \to \mathbb{C}$ be an eigenfunction of the hypercube Q_q^n. Then the local distribution of g in the face $\Gamma^\perp$ linearly depends on the local distribution of g in the face Γ.*

Proof. Consider the hypercube Q_q^n as the Cartesian product of faces: $Q_q^n = \Gamma \times \Gamma^\perp$. From equality (30) we have

$$A_{k_1k_2}[g] = \frac{1}{q^{n/2}} \sum_{m_1,m_2} P_{k_1}[n_1, q](\lambda_{m_1}) P_{k_2}[n_2, q](\lambda_{m_2}) \overline{\widehat{A}_{m_1m_2}[g]},$$

where $n_1 = \dim \Gamma$ and $n_2 = n - n_1 = \dim \Gamma^\perp$.

By the definition of $\widehat{A}_{m_1m_2}[g]$, we have $\widehat{A}_{m_1m_2}[g] = 0$ for $m_1 + m_2 \neq m$, where $n(q-1) - mq = \lambda$ is the eigenvalue of g. Note that $P_0[n_2, q] = 1$. Then for $k_1 = 0, \ldots, \dim \Gamma$ we have the equalities

$$A_{k_10}[g] = \frac{1}{q^{n/2}} \sum_{m_1+m_2=m} P_{k_1}[n_1, q](\lambda_{m_1}) \overline{\widehat{A}_{m_1m_2}[g]}. \tag{31}$$

Since the MacWilliams transform is invertible, the last equality expresses the coefficients $\overline{\widehat{A}_{m_1m_2}[g]}$ in the term of the numbers $A_{k_10}[g]$. Similarly, for $k_2 = 0, \ldots, \dim \Gamma^\perp$ we have

$$A_{0k_2}[g] = \frac{1}{q^{n/2}} \sum_{m_1+m_2=m} P_{k_2}[n_2, q](\lambda_{m_2}) \overline{\widehat{A}_{m_1m_2}[g]}.$$

The set of quantities $A_{0k_2}[g]$ is the local distribution of g in the face $\Gamma^\perp$. We have shown that it can be expressed linearly in terms of the set $A_{k_10}[g]$, which is the local distribution of g in the face Γ. $\square$

Corollary 12.2. *Let $f : Q_q^n \to \{0,1\}$ be a perfect 2-coloring with quotient matrix S. Then the weight distribution of the coloring f in the face Γ determines the weight distribution of f in the face $\Gamma^\perp$.*

Proof. Let f_1 and f_2 be two perfect 2-colorings with quotient matrix S. Consider the function $g = f_1 - f_2$. Since f_1 and f_2 are perfect 2-colorings with the same parameters, Proposition 2.7 implies that g is an eigenfunction in Q_q^n. By Theorem 12.4 it follows that if g has zero local distribution in the face Γ, then it also has zero local distribution in the face $\Gamma^\perp$. Obviously, $A_{m_1m_2}[g] = A_{m_1m_2}[f_1] - A_{m_1m_2}[f_2]$. Therefore, if the local distributions of f_1 and f_2 coincide in the face Γ, then they also coincide in the face $\Gamma^\perp$. $\square$

Vasil'eva's theorem states that the weight spectra of an eigenfunction g in orthogonal faces are related by linear relations. Suppose that all coefficients in these relations are nonzero. In this case the values of the eigenfunction $g : Q_2^n \to \mathbb{C}$ on vertices of weight less than d, $d \le n/2$, are uniquely recovered from its values on vertices of weight d. Suppose eigenfunctions g and g' coincide on vertices of weight d. Consider the function $f = g - g'$. Let u be a vertex of minimal weight $\mathrm{wt}(u) = d' < d$ for which $f(u) \neq 0$. Consider the face Γ of dimension d' containing the vertices $\bar{0}$ and u. The local weight coefficients with respect to this face satisfy $A_{00}[f] = 0, \ldots, A_{(d'-1)0}[f] = 0$, $A_{d'0}[f] = f(u) \neq 0$. Consider the face $\Gamma^\perp$. On the one hand, $A_{0d}[f] = 0$, since $f(v) = 0$ for all vertices of weight $\mathrm{wt}(v) = d$. On the other hand, $A_{0d}[f] = \alpha A_{d'0}[f]$, where $\alpha \neq 0$ by assumption. It is a contradiction.

12.5 Problems

91. Prove the equality
$2^{n-t}\binom{t}{k} = \sum_{m=0}^{n-t} P_k[n,2](\lambda_m)\binom{n-t}{m}$ for $0 < k < t < n$.

92. Using the generating function of Krawtchouk polynomials (21), prove that for any function $f : Q_q^n \to \mathbb{C}$ the following polynomial equality holds:
$q^{n/2} \sum_{k=0}^{n} \widehat{A}_k[f] z^k = \sum_{m=0}^{n} A_m[f](1-z)^m(1+(q-1)z)^{n-m}$.
In particular, for a linear code $C \subset Q_q^n$ the equality holds:
$|C| \sum_{k=0}^{n} A_k(C^\perp) z^k = \sum_{m=0}^{n} A_m(C)(1-z)^m(1+(q-1)z)^{n-m}$.

93. For any function $f : Q_q^n \to \mathbb{C}$ and $i = 0, \ldots, n$ prove the polynomial equality
$\sum\limits_{k=0}^{n} \widehat{A}_k[f]\binom{k}{i} = q^{\frac{n}{2}-i} \sum\limits_{m=0}^{n} (-1)^m (q-1)^{i-m} A_m[f]\binom{n-m}{n-i}$, where binomial coefficients $\binom{a}{b}$ are taken to be zero when $a < b$.

94. Prove that for any function $f : Q_q^n \to \mathbb{C}$ the following equality holds:
$\sum\limits_{k=0}^{n} k\widehat{A}_k[f] = q^{\frac{n}{2}-1}((q-1)nA_0[f] - A_1[f])$. In particular, for a linear code $C \subset Q_q^n$ of dimension m the equality holds:
$\sum\limits_{k=0}^{n} kA_k(C) = q^{m-1}((q-1)n - A_1(C^\perp))$.

95. For a linear code $C \subset Q_2^n$ prove the polynomial equality in two variables:
$|C| \sum\limits_{v \in C^\perp} x^{\mathrm{wt}(v)} y^{n-\mathrm{wt}(v)} = \sum\limits_{u \in C} (y-x)^{\mathrm{wt}(u)} (x+y)^{n-\mathrm{wt}(u)}$.

96. Let $C \subset Q_2^n$ be a code of odd cardinality with distance d. Prove the inequality $P_k(\lambda_0) + \sum\limits_{m \geq d} P_k(\lambda_m) A_m[C] \geq \frac{\binom{n}{k}}{|C|}$ for every k, $0 \leq k \leq n$.

97. Let a code $C \subset Q_2^n$ consist of codewords whose pairwise distances take values only from a set D, with the numbers t and $n-t$ both belonging to D and $0, n \notin D$. Prove that
1) if $n/2 \notin D$, then $|C| \leq 1 + \binom{n}{2} + \binom{n}{4} + \cdots + \binom{n}{|D|}$;
2) if $n/2 \in D$, then $|C| \leq \binom{n}{1} + \binom{n}{3} + \cdots + \binom{n}{|D|}$.

98. Let $A \subset Q_q^n$ be an affine equidistant code and let w be a nonzero weight of codewords. Prove that $|A| \leq q^n / L(w)$, where $L(w)$ is the minimum cardinality of the support of an eigenfunction with eigenvalue $\lambda = n(q-1) - qw$.

99. Let $A \subset Q_2^n$ be an affine equidistant code and let w be a nonzero weight of codewords. Prove that $|A| \leq 2^{(n-|n-2w|)/2}$ (see Problem 66). Prove that this bound is attained for the affine codes $A = \{(x, x \oplus \bar{1}, \bar{0}) : x \in Q_2^{(n-i)/2}\}$, $i = n - 2k$.

100. Let $\mathbf{1}_C$ be a linear perfect 2-coloring in the hypercube. Prove that $C^\perp$ is an equidistant code.

101. Let $C \subset Q_q^n$ be an equidistant code with code distance $d > n(q-1)/q$. Prove that $|C| \leq 1/(1 - \frac{(q-1)n}{qd})$.

13 Bent Functions

13.1 Definition and Basic Properties of Bent Functions

We regard the lines $\{\alpha\phi_z \mid \alpha \in \mathbb{C}\}$, generated by the characters, as coordinate axes. The distance between a vector g and a coordinate axis can be defined as the length of the vector g', where $g = g' + \alpha_z\phi_z$ and $(g', \phi_z) = 0$. Then $\|g'\|_2^2 = \|g\|_2^2 - q^n|\alpha_z|^2$. Since, by Parseval's identity, $q^n \sum_z |\alpha_z|^2 = \|g\|_2^2$ the function that is farthest from all the coordinate axes is the one whose Fourier coefficients have equal absolute values.

A mapping $b : Q_q^n \to Q_q$ is called a *bent function* if $|\widehat{\xi^b}(z)| = \frac{1}{q^{n/2}}|(\xi^b, \phi_z)| = 1$ for all $z \in Q_q^n$. For every bent function b, we have, by definition $q^{n/2}|\alpha_z| = |\widehat{\xi^b}(z)| = 1$. Consequently, bent functions are precisely those functions whose corresponding vectors are at equal distance from all coordinate axes generated by the characters. The axes correspond, in terms of exponents, not only to linear functions $\xi^{\langle x,a\rangle}$ but also to affine functions $\langle x, a\rangle + c$. Further, we will prove that bent functions are at the maximum possible Hamming distance from the class of affine functions.

Recall that $\widehat{\xi^b}$ is called the Walsh–Hadamard transform of $b : Q_q^n \to Q_q$ and $\widehat{\xi^b}(z)$ is the Walsh–Hadamard coefficients of b.

Remark 13.1. For simplicity, throughout this section we assume that q is prime, so the hypercube Q_q^n can be regarded as the vector space $(GF(q))^n$. In this case every affine function $f : Q_q^n \to Q_q$ can be represented in the form $\langle x, a\rangle + c$. If $q = p^k$ then it is necessary to use $Tr(x \cdot a)$ instead of $\langle x, a\rangle$, where $Tr : GF(q) \to GF(p)$ is a linear function.

Bent functions are used in block and stream ciphers to increase resistance to linear cryptanalysis, in which an attacker attempts to find the best affine approximation to an unknown function. A detailed survey of the theory of bent functions can be found in [103] and [145].

Proposition 13.1. *A function b is a bent function if and only if $\xi^b * \widetilde{\xi^b}(z) = q^{n/2}\delta$, where $\tilde{b}(x) = -b(-x)$ and $\delta = q^{n/2}\mathbf{1}_{\{\bar{0}\}}$ is the Dirac delta function.*

Proof. Apply the Fourier transform to the equality $\xi^b * \widetilde{\xi^b}(z) = q^{n/2}\delta$. From the properties of the Fourier transform $\widehat{f(-x)}(z) = \widehat{f(x)}(-z)$ and $\widehat{f * g} = q^{n/2}\widehat{f} \cdot \widehat{g}$ (see Propositions 9.13 and 9.17) we obtain the equivalent equality $\widehat{\xi^b} \cdot \widehat{\widetilde{\xi^b}} = \widehat{\xi^b} \cdot \overline{\widehat{\xi^b}} = \widehat{\delta} = \mathbf{1}$. Thus $|\widehat{\xi^b}(z)| = 1$ for every z, which is precisely the definition of a bent function. □

Proposition 13.2. *Let $b : Q_q^n \to Q_q$ be a bent function and suppose that $\widehat{\xi^b} = \xi^f$ for some function $f : Q_q^n \to Q_q$. Then f is a bent function.*

Proof. We have the equalities $\widehat{\xi^{f(x)}} = \widehat{\widehat{\xi^{b(x)}}} = \xi^{b(-x)}$. Then $|\widehat{\xi^f}| = |\xi^{b(-x)}| = 1$ and hence f is a bent function. □

A bent function is called *regular* if it satisfies the condition of Proposition 13.2. For $q = 2$ all bent functions are regular since the Fourier transform maps real-valued functions to real-valued functions. A bent function b is called *weakly regular* if $\widehat{\xi^b} = \alpha\xi^f$ for some q-ary function f and some constant α with $|\alpha| = 1$.

Example 13.1. Define the quadratic form $g : Q_q^{2n} \to Q_q$ by the equation $g(x, y) = \langle x, y\rangle = \sum_{i=1}^{n} x_i y_i \bmod q$. We show that g is a bent function. We have

$$\widehat{\xi^g}(u, v) = \frac{1}{q^n} \sum_{x,y} \xi^{\langle x,y\rangle - \langle x,u\rangle - \langle y,v\rangle} = \frac{1}{q^n} \sum_{y} \xi^{-\langle y,v\rangle} \sum_{x} \xi^{\langle x,y-u\rangle}.$$

The sum of a character over all vertices vanishes unless the character is ϕ_0 (see Proposition 9.1). Therefore, $\sum_x \xi^{\langle x,y-u\rangle} = 0$ when $y \neq u$. Hence, $\widehat{\xi^g}(u, v) = \xi^{-\langle u,v\rangle}$ and consequently g is a bent function by definition.

For an arbitrary function $f : Q_q^n \to Q_q$ we define the operator $D_y[f](x) = f(x+y)-f(x)$, which can be called the *discrete derivative* of f in the direction y.

Proposition 13.3. *For any nonzero y, the function $D_y[f]$ takes each of the q values equally often if and only if f is a bent function.*

Proof. We have

$$\xi^f * \xi^{\widetilde{f}}(z) = \sum_{x \in Q_q^n} \xi^{f(z-x)} \xi^{-f(-x)} = \sum_{y \in Q_q^n} \xi^{f(z+y)-f(y)}.$$

If $z \neq \bar{0}$, the last sum is the sum of the q^n values of $\xi^{D_z[f]}$. If $D_z[f]$ takes each value of Q_q equally often, then, since $\sum_{a \in Q_q} \xi^a = 0$, we obtain

$$\xi^f * \xi^{\widetilde{f}}(z) = 0 \qquad \text{for } z \neq \bar{0}.$$

By Proposition 13.1, f is therefore bent.

Conversely, if f is bent, then

$$\xi^f * \xi^{\widetilde{f}}(z) = 0 \qquad \text{for } z \neq \bar{0}.$$

Hence $\sum_{y \in Q_q^n} \xi^{D_z f} = 0$ for every nonzero z. By Proposition 9.2, this is equivalent to $D_z[f]$ taking each value of Q_q equally often. □

Proposition 13.4. *Let $f : Q_q^n \to Q_q$ be a bent function, let $L : Q_q^n \to Q_q^n$ be a non-degenerate affine transformation and let $\ell : Q_q^n \to Q_q$ be an affine function. Then $g = (f \circ L) + \ell$ is a bent function.*

Proof. A non-degenerate affine transformation of the argument of a function implies a non-degenerate affine transformation of the argument of its Walsh–Hadamard transform. Adding of a linear function permutes the Walsh–Hadamard coefficients. Adding of a constant function corresponds to multiplying the Walsh–Hadamard coefficients by a constant with absolute value equal to one. Consequently, g is a bent function by definition. □

The functions f and g satisfying the conditions of Proposition 13.4 are called *EA-equivalent*.

13.2 Boolean Bent Functions and Plateaued Functions

Let us consider the case $q = 2$ in more detail. Recall that the Walsh–Hadamard transform of a Boolean function $f : Q_2^n \to Q_2$ is defined as the Fourier transform $\widehat{(-1)^f}$. Consequently, a Boolean function is bent if and only if all its Walsh–Hadamard coefficients have absolute value 1.

Proposition 13.5. *If f is a Boolean bent function, then*

$$\widehat{f}(\bar{0}) = \frac{1}{2}\left(2^{n/2} - \widehat{(-1)^f}(\bar{0})\right) = \frac{1}{2}\left(2^{n/2} \pm 1\right).$$

Proof. It is easy to see that $(-1)^f = \mathbf{1} - 2f$, and hence $\widehat{(-1)^f} = \widehat{\mathbf{1}} - 2\widehat{f} = \delta - 2\widehat{f}$. In particular, $\widehat{(-1)^f}(\bar{0}) = 2^{n/2} - 2\widehat{f}(\bar{0})$. Since f is bent, the definition of a bent function gives $\left|\widehat{(-1)^f}(\bar{0})\right| = 1$. □

So, the weight of every Boolean bent function equals either $2^{n-1} + 2^{\frac{n}{2}-1}$ or $2^{n-1} - 2^{\frac{n}{2}-1}$.

Let $\mathcal{A}$ be the set of affine Boolean functions, i.e., functions of the form

$$f(x) = \langle x, z \rangle \qquad \text{or} \qquad f(x) = \langle x, z \rangle \oplus 1.$$

The *nonlinearity* of a Boolean function f is its Hamming distance from the set of affine functions:

$$nl(f) = \min_{\ell \in \mathcal{A}} d_H(f, \ell), \text{ where } d_H(f, \ell) = |\mathrm{supp}(f \oplus \ell)|.$$

The Hamming distance between two Boolean functions f and g can be expressed in terms of the inner product of the corresponding functions $(-1)^f$ and $(-1)^g$. Namely, $d_H(f,g) = \frac{1}{2}\left(2^n - ((-1)^f, (-1)^g)\right)$. Indeed, $2^n - 2d_H(f,g) = ((-1)^f, (-1)^g)$, since the inner product is the difference between the number of vertices at which f and g coincide and the number at which they differ.

Proposition 13.6. *The nonlinearity of a Boolean function f is*

$$nl(f) = \frac{1}{2}\left(2^n - 2^{n/2} \max_z \left|\widehat{(-1)^f}(z)\right|\right).$$

Proof. A Boolean function ℓ is affine if and only if

$$(-1)^\ell = \phi_z \qquad \text{or} \qquad (-1)^\ell = -\phi_z$$

for some $z \in Q_2^n$. From the definition of the Fourier transform, we have $((-1)^f, \pm\phi_z) = \pm 2^{n/2}\widehat{(-1)^f}(z)$. Substituting this expression into the formula for the Hamming distance and minimizing over all affine functions gives the result. □

Proposition 13.7 ([126])**.** *The inequality $nl(f) \le \frac{1}{2}\left(2^n - 2^{n/2}\right)$ holds for every Boolean function f. Equality is attained if and only if f is a bent function.*

Proof. By Parseval's identity,

$$\sum_{z \in Q_2^n} \left|\widehat{(-1)^f}(z)\right|^2 = \sum_{x \in Q_2^n} |(-1)^f(x)|^2 = 2^n.$$

Therefore, $\max_z \left|\widehat{(-1)^f}(z)\right|^2 \ge 1$. Equality can hold only if $\left|\widehat{(-1)^f}(z)\right| = 1$ for every $z \in Q_2^n$. Thus, by Proposition 13.6, $nl(f) \le \frac{1}{2}\left(2^n - 2^{n/2}\right)$, with equality if and only if f is bent. □

Since the nonlinearity of a Boolean function is an integer, Boolean bent functions cannot exist for odd n. On the other hand, Example 13.1 shows that bent functions exist for every even n.

A Boolean function f is called *plateaued* if its Walsh–Hadamard coefficients take only three distinct values, $0, \quad \pm a$, for some $a \in \mathbb{R}$. It follows from Parseval's identity that a^2 divides 2^n. Hence $a^2 = 2^s$ for some nonnegative integer s. A plateaued function whose Walsh–Hadamard coefficients take the values $0, \quad \pm 2^{s/2}$ is called *s-plateaued*. In particular, a 0-plateaued function is a bent function. It is obvious that EA-equivalent functions either are or are not s-plateaued functions.

Proposition 13.8. *A Boolean function f is plateaued if and only if $(-1)^f * (-1)^f * (-1)^f = a^2 2^n (-1)^f$ for some $a \in \mathbb{R}$.*

Proof. By the convolution property of the Fourier transform (Proposition 9.17), the equality $(-1)^f * (-1)^f * (-1)^f = a^2 2^n (-1)^f$ is equivalent to $2^n \left(\widehat{(-1)^f}\right)^3 = a^2 2^n \widehat{(-1)^f}$. Thus, $\widehat{(-1)^f}\left(\left(\widehat{(-1)^f}\right)^2 - a^2\right) = 0$. Therefore, every Walsh–Hadamard coefficient satisfies $\widehat{(-1)^f}(z) \in \{0, \pm a\}$, which is precisely the definition of a plateaued function. The converse follows immediately by reversing the argument. □

Theorem 13.1 (Tarannikov at al. [141], [130], [160])**.** *Let f be a Boolean function with $\mathrm{cor}(f) \le n-2$. Then the following inequalities hold:*
$nl(f) \le 2^{n-1} - 2^{\mathrm{cor}(f)}$ if f is not resilient, and
$nl(f) \le 2^{n-1} - 2^{1+\mathrm{cor}(f)}$ if f is resilient.
If equality is attained in either inequality, then f is plateaued.

Proof. Suppose first that f is not balanced. By Remark 11.2, which follows from Sarkar's identity, the Walsh–Hadamard coefficients have the form $m 2^{1+\mathrm{cor}(f)-n/2}$, where m is an integer. Hence

$$\max_z \left|\widehat{(-1)^f}(z)\right| \ge 2^{1+\mathrm{cor}(f)-n/2}.$$

By Proposition 13.6, we obtain $nl(f) \le 2^{n-1} - 2^{\mathrm{cor}(f)}$.

If equality is attained, then all nonzero Walsh–Hadamard coefficients must have absolute value $2^{\mathrm{cor}(f)+1-n/2}$. Thus all Walsh–Hadamard coefficients belong to $\{0, \pm 2^{\mathrm{cor}(f)+1-n/2}\}$, and f is plateaued.

The balanced case is analogous. □

We describe a method of constructing bent functions and plateaued functions that generalizes Example 13.1. Let $x \in Q_2^n$ and $s \le n$. Denote by x^s the vector of the first s coordinates of the vector x.

Proposition 13.9 (Maiorana–McFarland construction). *Let $x, y, u, v \in Q_2^n$, $z, w \in Q_2^s$, $s \le n$. Consider permutations $\tau : Q_2^n \to Q_2^n$ and $\sigma : Q_2^s \to Q_2^s$ and an arbitrary function $f : Q_2^n \to Q_2$. Then $F(x, y, z) = \langle \tau(x), y\rangle + \langle \sigma(x^s), z\rangle + f(x)$ is a s-plateaued function of $2n + s$ variables.*

Proof. By the definition of the Fourier transform,

$$2^{n+\frac{s}{2}}\widehat{(-1)^F}(u,v,w) = \sum_{x,y,z\in Q_2^n} (-1)^{\langle\tau(x),y\rangle+\langle\sigma(x^s),z\rangle+f(x)-\langle x,u\rangle-\langle v,y\rangle-\langle w,z\rangle}$$

$$= \sum_{x\in Q_2^n} (-1)^{f(x)-\langle x,u\rangle} \sum_{y\in Q_2^n} (-1)^{\langle\tau(x),y\rangle-\langle v,y\rangle} \sum_{z\in Q_2^s} (-1)^{\langle\sigma(x^s),z\rangle-\langle w,z\rangle}.$$

The sums $\sum_{z\in Q_2^s} (-1)^{\langle\sigma(x^s),z\rangle-\langle w,z\rangle}$ are equal to 2^s if $w = \sigma(x^s)$, and is equal to 0 otherwise. Similarly, the sums $\sum_{y\in Q_2^n} (-1)^{\langle\tau(x),y\rangle-\langle v,y\rangle}$ is equal to 2^n if $v = \tau(x)$ and is equal to 0 otherwise.

Consequently, $2^{n+\frac{s}{2}}\widehat{(-1)^F}(u,v,w) = 2^{n+s}(-1)^{f(x)-\langle x,u\rangle}$ if $v = \tau(x)$ and $w = \sigma(x^s)$; otherwise $\widehat{(-1)^F}(u,v,w) = 0$.

Thus every nonzero Walsh–Hadamard coefficient of F has absolute value $\frac{2^{n+s}}{2^{n+s/2}} = 2^{s/2}$. Hence F is s-plateaued. □

13.3 Nonlinearity of q-ary Functions

Every affine function $g : Q_q^n \to Q_q$ can be represented as $g(x) = \langle z, x\rangle + a$. For an arbitrary function $f : Q_q^n \to Q_q$ we define the following quantities $\delta_f^{z,a} = \frac{q-1}{q} - \frac{d_H(f,g)}{q^n}$, where $g(x) = \langle z, x\rangle + a$.

The following properties of the quantities $\delta_f^{z,a}$ follow directly from the definition.

Proposition 13.10.
(a) *For any fixed $a \in Q_q$ and $z \in Q_q^n$ $\sum\limits_f \delta_f^{z,a} = 0$, where the sum is taken over all functions $f : Q_q^n \to Q_q$.*
(b) *For any function f and $z \in Q_q^n$ we have $\sum\limits_{a\in Q_q} \delta_f^{z,a} = 0$.*
(c) *The minimum value of $\delta_f^{z,a}$ is $-\frac{1}{q}$, and the maximum value is $\frac{q-1}{q}$.*

As in the Boolean case, we define the nonlinearity of a q-ary function $f : Q_q^n \to Q_q$ as the Hamming distance from f to the set of affine functions. From the definitions follows the equality

$$nl(f) = q^{n-1}(q-1) - q^n \max_{z,a} \delta_f^{z,a}. \tag{32}$$

The following theorem can be viewed as another representation of Parseval's identity.

Theorem 13.2 (Ryabov [127]). $\sum_{z\in Q_q^n, a\in Q_q} (\delta_f^{z,a})^2 = \frac{q-1}{q}$.

Proof. We prove the theorem by induction on n. For $n = 0$ the equality is easily verified directly. Let us prove the induction step. From the definitions we have

$$\delta_f^{z,a} = \frac{1}{q} \sum_{c\in Q_q} \delta_{f|_{x_n=c}}^{z',a+cz_n}, \qquad \text{where} \quad z = (z', z_n).$$

Therefore,

$$(\delta_f^{z,a})^2 = \frac{1}{q^2} \sum_{c_1,c_2\in Q_q} \delta_{f|_{x_n=c_1}}^{z',a+c_1z_n} \delta_{f|_{x_n=c_2}}^{z',a+c_2z_n} = \frac{1}{q^2} \sum_{c_1\neq c_2} \delta_{f|_{x_n=c_1}}^{z',a+c_1z_n} \delta_{f|_{x_n=c_2}}^{z',a+c_2z_n} + \frac{1}{q^2} \sum_{c\in Q_q} (\delta_{f|_{x_n=c}}^{z',a+cz_n})^2.$$

By the induction hypothesis we have

$$\sum_{z\in Q_q^n, a\in Q_q} \frac{1}{q^2} \sum_{c\in Q_q} (\delta_{f|_{x_n=c}}^{z',a+cz_n})^2 = \frac{1}{q^2} \sum_{c\in Q_q} \sum_{z_n\in Q_q} \sum_{z'\in Q_q^{n-1}, a\in Q_q} (\delta_{f|_{x_n=c}}^{z',a+cz_n})^2 = \frac{q^2}{q^2} \frac{q-1}{q}.$$

It remains to show that the contribution of the first term is zero. We have

$$\sum_{z\in Q_q^n, a\in Q_q} \sum_{c_1\neq c_2} \delta_{f|_{x_n=c_1}}^{z',a+c_1z_n} \delta_{f|_{x_n=c_2}}^{z',a+c_2z_n} = \sum_{c_1\neq c_2} \sum_{z'\in Q_q^{n-1}} \sum_{z_n\in Q_q} \sum_{a\in Q_q} \delta_{f|_{x_n=c_1}}^{z',a+c_1z_n} \delta_{f|_{x_n=c_2}}^{z',a+c_2z_n} =$$

$$= \sum_{c_1\neq c_2} \sum_{z'\in Q_q^{n-1}} \left(\sum_{a_1\in Q_q} \delta_{f|_{x_n=c_1}}^{z',a_1} \right) \left(\sum_{a_2\in Q_q} \delta_{f|_{x_n=c_2}}^{z',a_2} \right) = 0.$$

The penultimate equality follows from the fact that the system of equations $\begin{cases} a + c_1z_n = a_1; \\ a + c_2z_n = a_2. \end{cases}$ has a unique solution for the variables a and z_n. The last equality follows from Proposition 13.10(b). □

Proposition 13.11. *For any function $f : Q_q^n \to Q_q$, the following statements hold.*
(a) $\widehat{\xi^f}(z) = q^{n/2} \sum_{a\in Q_q} \delta_f^{z,a} \xi^a$.
(b) *If $\delta_f^{z,a} = 0$ for all $a \in Q_q$, then $\widehat{\xi^f}(z) = 0$. The converse holds if q is prime.*

Proof. (a) Let $L_a = |\{x \in Q_q^n : f(x) - \langle x, z\rangle = a\}|$. Express $\widehat{\xi^f}(z)$ and $\delta_f^{z,a}$ in terms of L_a.

$$\widehat{\xi^f}(z) = \frac{1}{q^{n/2}} \sum_{x \in Q_q^n} \xi^{f(x)-\langle x,z\rangle} = \frac{1}{q^{n/2}} \sum_{a \in Q_q} L_a \xi^a. \tag{33}$$

$$\delta_f^{z,a} = \frac{q-1}{q} - \frac{q^n - L_a}{q^n} = \frac{L_a}{q^n} - \frac{1}{q}.$$

Consequently, $L_a = q^n \delta_f^{z,a} + q^{n-1}$. Using $\sum\limits_{a \in Q_q} \xi^a = 0$ we obtain

$$\widehat{\xi^f}(z) = \frac{1}{q^{n/2}} \sum_{a \in Q_q} (q^n \delta_f^{z,a} + q^{n-1}) \xi^a = q^{n/2} \sum_{a \in Q_q} \delta_f^{z,a} \xi^a.$$

This proves the first statement.

(b) If $\delta_f^{z,a} = 0$ for every $a \in Q_q$, then the first statement immediately gives $\widehat{\xi^f}(z) = 0$.

Using equality (33) and Proposition 9.2, we conclude that if q is prime and $\widehat{\xi^f}(z) = 0$, then $L_a = q^{n-1}$ for every $a \in Q_q$. Consequently, $\delta_f^{z,a} = 0$ for every $a \in Q_q$. □

Theorem 13.3 (Ryabov [128]).
Let q be prime. For any function $f : Q_q^n \to Q_q$ the following statement holds.
(a) $nl(f) \le (q-1)q^{n-1} - q^{\frac{n}{2}-1}$.
(b) *If $nl(f) = (q-1)q^{n-1} - q^{\frac{n}{2}-1}$, then f is a weakly regular bent function and n is even.*

Proof. (a) To maximize $nl(f)$, we need to solve the following optimization problem:

$$\sum_{z \in Q_q^n, a \in Q_q} (\delta_f^{z,a})^2 = \tfrac{q-1}{q},$$
$$\sum_{a \in Q_q} \delta_f^{z,a} = 0 \text{ for every } z \in Q_q^n,$$
$$\max_{z \in Q_q^n, a \in Q_q} \delta_f^{z,a} \longrightarrow \min.$$

Consider the following auxiliary problem: $\sum\limits_{a \in Q_q} \sigma_a = 0$, $\sum\limits_{a \in Q_q} \sigma_a^2 = A\frac{q-1}{q}$ and $\max\limits_a \sigma_a \to \min$. It is easy to see that, up to permutation, the unique solution is $\sigma_0 = -\frac{q-1}{q}\sqrt{A}$, $\sigma_a = \frac{\sqrt{A}}{q}$ for $a \ne 0$.

The value $\max\limits_a \sigma_a$ increases with A. Then the optimal solution of the original problem corresponds to the case when all the sums $\sum\limits_{a \in Q_q} (\delta_f^{z,a})^2$ are

equal. Take $A = \frac{1}{q^n}$. Then we obtain that $\min_f(\max_{z\in Q_q^n, a\in Q_q} \delta_f^{z,a}) \geq \frac{1}{q^{\frac{n}{2}+1}}$. This proves (a).

(b) Suppose now that equality is attained. Then equality must hold at every step of the above optimization argument. In particular, for every $z \in Q_q^n$ the values $\delta_f^{z,a}$, $a \in Q_q$, must consist of one value $-\frac{q-1}{q^{\frac{n}{2}+1}}$ and $q-1$ values $\frac{1}{q^{\frac{n}{2}+1}}$. Hence, by Propositions 13.11 (a), $\widehat{\xi^f}(z) = -\xi^a$ for some $a \in Q_q$. Then f is a weakly regular bent function. Since the number $nl(f)$ is an integer, n must be even. □

13.4 Problems

102. Let f be a Boolean function and $F(y) = \sum_{x\in Q_2^n} (-1)^{D_y[f](x)}$. Prove that each Fourier coefficient of F is nonnegative.

103. Let f be a Boolean function. Prove that

$$\sum_{x,y,z\in Q_2^n} (-1)^{D_z[xD_y[f]](x)} = 2^n \sum_{v\in Q_2^n} (\widehat{(-1)^f}(v))^4.$$

104. Let f be a Boolean function. Prove that

$$\sum_{x,y,z\in Q_2^n} (-1)^{D_z[xD_y[f]](x)} \geq 2^{2n}$$

and this equality holds if and only if f is a bent function.

105. Prove that the Hamming distance between two distinct bent functions in the Boolean n-cube cannot be less than $2^{n/2}$.

106. For an arbitrary Boolean function $f : Q_2^n \to Q_2$ define the entropy $H(f)$ by $H(f) = -\sum_{x\in Q_2^n} p(x)\log_2 p(x)$, where $p(x) = (\widehat{(-1)^f}(x))^2/2^n$. Prove that for even n the maximum entropy equal to $n2^n$ is attained only by bent functions.

107. Prove that the restriction of a bent function to a hyperface is a plateaued function.

108. Prove that there are no Boolean functions of n variables that attain the Tarannikov bound when $\mathrm{cor}(f) \leq n/2$.

14 Algebraic Normal Form of Boolean Functions

14.1 Möbius Transformation

Two bases $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ in a vector space over a field F are called *biorthogonal* if $\langle u_i, v_j \rangle = 0$ for $i \neq j$ and $\langle u_i, v_i \rangle = 1$ for all $i, j \in \{1, \ldots, n\}$. Let U and V be the square matrices whose rows are the corresponding basis vectors. Then $U^{\mathsf{T}} V = I_n$, that is, $U^{\mathsf{T}} = V^{-1}$.

Consider a finite set T equipped with a partial order $\leq$. For each $z \in T$, define the function

$$\omega_z(x) = \begin{cases} 1, & x \leq z, \\ 0, & \text{otherwise.} \end{cases}$$

Consider the vector space $\mathbb{V}(T)$ of functions $f : T \to F$. The number of functions ω_z is equal to the dimension $|T|$ of the space $\mathbb{V}(T)$. Let W be the matrix whose rows are the vectors of values of the functions ω_z. It is easy to see that, if the elements of T are ordered compatibly with the partial order, then W is a lower triangular matrix with ones on the main diagonal. Consequently, W is nonsingular, and there exists a basis $\{\nu_y : y \in T\}$ biorthogonal to the basis $\{\omega_z : z \in T\}$.

Multiplication of a vector $f : T \to F$ by the matrix W is called the *Möbius transformation* of f. Multiplication by the matrix V^{T}, where V is formed from the functions ν_y, is called the *inverse Möbius transformation*.

The matrices W and V^{T} are mutually inverse by definition, i.e.,

$$V^{\mathsf{T}}(Wf) = (V^{\mathsf{T}} W)f = f.$$

It follows that V^{T} is also lower triangular with ones on the main diagonal, while V is upper triangular. Thus,

$$Wf(z) = \sum_{x \leq z} \omega_z(x) f(x)$$

and

$$V^{\mathsf{T}} g(y) = \sum_{z \leq y} \nu_z(y) g(z),$$

since

$$V^{\mathsf{T}}(y, z) = V(z, y) = \nu_z(y).$$

Since the matrices W and V^{T} are mutually inverse lower triangular matrices, we also obtain the following.

Proposition 14.1. *For any distinct $y, z \in T$,*

$$\sum_{x:\, y \le x \le z} \nu_x(z) = 0 \qquad \text{and} \qquad \sum_{x:\, y \le x \le z} \nu_y(x) = 0.$$

Proof. We have

$$\sum_{x:\, y \le x \le z} \nu_x(z) = \sum_{x:\, y \le x \le z} V^{\mathsf{T}}(z,x)$$
$$= \sum_{x:\, y \le x \le z} V^{\mathsf{T}}(z,x) W(x,y) = \sum_{x} V^{\mathsf{T}}(z,x) W(x,y) = 0.$$

The second equality follows in the same way by using that $WV^{\mathsf{T}} = I_n$. □

In the case of a linear order, the matrix W has ones in all positions on and below the main diagonal, while the matrix V^{T} has only two nonzero diagonals: the main diagonal, consisting of ones, and the first subdiagonal, consisting of -1's.

As a partially ordered set, we can consider the Boolean hypercube with the lexicographic order. In this case, the basis vectors ω_z are the characteristic functions of the faces containing $\bar{0}$ and z. Let $F = \mathbb{C}$. It is easy to verify that the biorthogonal basis $\{\nu_y\}$ consists of the characteristic functions of the faces containing $\bar{1}$ and y, multiplied by the parity character $(-1)^{x_1 \oplus \cdots \oplus x_n}$. If the field F has characteristic 2, multiplication by the parity character is not needed (see Proposition 14.3).

Proposition 14.2. *Let $f : Q_2^n \to \mathbb{C}$ be an eigenfunction with eigenvalue $\lambda = n - 2k$. Then:*

(a) *f is determined by the sums of its values over the $(n-k)$-dimensional faces containing the vertex $\bar{0}$;*

(b) *the restriction of f to the ball of radius $d \le n - k$ centered at the vertex $\bar{0}$ is determined by the sums of its values over the d-dimensional faces containing $\bar{0}$.*

Proof. (a) Consider Corollary 11.3 of Sarkar's identity

$$\sum_{z \in \Gamma^\perp} \widehat{f}(z) = 2^{n/2 - \dim \Gamma} \sum_{x \in \Gamma} f(x)$$

for $\dim \Gamma = n - k$. By Proposition 9.12, $\widehat{f}(z) \neq 0$ only if $\mathrm{wt}(z) = k$. Hence, the sum on the left-hand side has exactly one nonzero term, and therefore

$$\widehat{f}(z) = 2^{k - n/2} \sum_{x \in \Gamma} f(x).$$

The function f can then be recovered from $f = \widehat{\widehat{f}}$.

(b) We first show that, from the sums $\sum_{x\in\Gamma'} f(x)$ over faces Γ' of dimension $m \le n-k$, one can compute the sums $\sum_{x\in\Gamma} f(x)$ over faces Γ of dimension $m-1$.

There are $n-(m-1)$ faces Γ' of dimension m containing a fixed face Γ of dimension $m-1$. Any two of these faces intersect exactly in Γ. Therefore,

$$\sum_{\Gamma\subset\Gamma'}\sum_{x\in\Gamma'} f(x) - (n-(m-1))\sum_{x\in\Gamma} f(x) = \sum_{x\in\Gamma}\sum_{y:\, d(x,y)=1} f(y) - (m-1)\sum_{x\in\Gamma} f(x).$$

Indeed, the left-hand side counts the values of f on all faces Γ' of dimension m containing Γ, after subtracting the contribution of their common intersection Γ. The right-hand side counts the values of f on all neighbors of vertices from Γ.

Since f is an eigenfunction, $\sum_{y:\, d(x,y)=1} f(y) = \lambda f(x)$. Consequently,

$$\sum_{\Gamma\subset\Gamma'}\sum_{x\in\Gamma'} f(x) = \big(n-2(m-1)+\lambda\big)\sum_{x\in\Gamma} f(x).$$

Let $m \le d \le n-k$. By the assumption on λ,

$$n-2(m-1)+\lambda \ge n-2(n-k-1)+n-2k = 2.$$

Therefore, the sum of the values of f over any face of dimension less than d can be computed recursively if the corresponding sums over faces of dimension d are known.

Consider a natural partial order on the Boolean hypercube (see the next section). Then functions $\omega_z(x)$ are indicator functions of faces. The inverse Möbius transformation then recovers the values of f from sums over faces. □

Note that, instead of the vertex $\bar{0}$, any vertex of the hypercube can be taken as the common intersection of all the faces.

14.2 Algebraic Degree of Boolean Functions

We next consider a particular case of the Möbius transformation over $GF(2)$ on the Boolean hypercube with the following natural order. We define

$$x \le y \quad\Longleftrightarrow\quad \mathrm{supp}(x) \subseteq \mathrm{supp}(y).$$

Notice that $\{x \in Q_2^n : x \leq y\}$ is a face of dimension $\mathrm{wt}(y)$ containing the vertex $\bar{0}$.

Every Boolean function $f : Q_2^n \to Q_2$ can be represented by in *algebraic normal form*,

$$f(x_1, \ldots, x_n) = \bigoplus_{y \in Q_2^n} G[f](y) x_1^{y_1} \cdots x_n^{y_n}, \tag{34}$$

where $x^0 = 1$, $x^1 = x$, and $G[f] : Q_2^n \to Q_2$. The existence of such a representation follows from the fact that addition and multiplication over $GF(2)$, together with the constants 0 and 1, form a complete basis. In particular, multiplication coincides with conjunction, while disjunction can be expressed as

$$x \vee y = x \oplus y \oplus xy.$$

A Boolean function has a unique representation in algebraic normal form, since the operator G maps Boolean functions to Boolean functions in the same number of variables.

The *algebraic degree* of a Boolean function f is the maximum degree of a monomial in its algebraic normal form, i.e.,

$$\deg(f) = \max_{G[f](y)=1} \mathrm{wt}(y).$$

The algebraic degree of a set $C \subset Q_2^n$ is defined as the algebraic degree of its characteristic function. The following statement holds.

Proposition 14.3. *For every Boolean function f,*

$$G[f](y) = \bigoplus_{x \in Q_2^n,\, x \leq y} f(x),$$

i.e., G is the Möbius transformation of f over $GF(2)$. Moreover, $G[G[f]] = f$.

Proof. It is easy to see that if $\mathrm{supp}(y) \not\subseteq \mathrm{supp}(x)$, then $x_1^{y_1} \cdots x_n^{y_n} = 0$, whereas otherwise $x_1^{y_1} \cdots x_n^{y_n} = 1$. Fix $z \in Q_2^n$. We show that

$$\bigoplus_{x \in Q_2^n,\, x \leq z} x_1^{y_1} \cdots x_n^{y_n} = 1$$

if and only if $z = y$. Indeed, if $y < z$, then the sum contains $2^{\mathrm{wt}(z) - \mathrm{wt}(y)}$ ones and hence is equal to 0. If z and y are incomparable or $z < y$, then all summands are equal to 0. Summing both sides of (34) over the face

$$\{x \in Q_2^n : x \leq z\},$$

we obtain

$$\bigoplus_{x \in Q_2^n,\, x \le z} f(x) = G[f](z).$$

Now fix $x \in Q_2^n$. On the right-hand side of (34), the monomial $x_1^{y_1} \cdots x_n^{y_n}$ is equal to 1 precisely when $y \le x$. Therefore,

$$f(x) = \bigoplus_{y \in Q_2^n,\, y \le x} G[f](y).$$

Hence $G[G[f]] = f$ for every Boolean function f. □

We say that a Boolean function is *balanced modulo* 2 on a face Γ if the Boolean sum of its values on Γ is equal to 0.

Proposition 14.4. *A Boolean function $f : Q_2^n \to Q_2$ is balanced modulo 2 on all faces of dimension $m+1$ if and only if* $\deg(f) \le m$.

Proof. On the one hand, every monomial of degree less than the dimension of a face Γ takes the value 1 an even number of times on Γ. Therefore, f is balanced modulo 2 on every face whose dimension is greater than $\deg(f)$.

On the other hand,

$$\bigoplus_{x \in Q_2^n,\, x \le z} x_1^{y_1} \cdots x_n^{y_n} = 1$$

if and only if $z = y$. Therefore, if the algebraic normal form contains a monomial of degree k, $k > m$, then there exists a k-dimensional face containing $\bar{0}$ on which the sum of the values of f is equal to 1. Every k-dimensional face can be partitioned into disjoint $(m+1)$-dimensional faces. Then the sum of the values of f on one of these faces is equal to 1. □

Proposition 14.5. *Suppose that a Boolean function f has an even number of ones on a face of dimension $m = n - \mathrm{cor}(f)$. Then* $\deg(f) \le m - 1$. *If this number is odd, then* $\deg(f) = m$ *and $G[f](z) = 1$ for every $z \in Q_2^n$ with* $\mathrm{wt}(z) = m$.

Proof. By the definition of correlation immunity, f has the same number of ones on all faces of dimension m. If this number is even, then $\deg(f) \le m-1$ by Proposition 14.4. If it is odd, then every face of dimension $m+1$ contains an even number of ones. Moreover, since every face of dimension m contains an odd number of ones,

$$G[f](z) = \bigoplus_{x \in Q_2^n,\, x \le z} f(x) = 1$$

for every $z \in Q_2^n$ with $\mathrm{wt}(z) = m$. $\square$

Corollary 14.1 (Siegenthaler inequality)**.** *For every Boolean function* $f : Q_2^n \to Q_2$*,*

$$\deg(f) \le n - \mathrm{cor}(f),$$

and

$$\deg(f) \le n - \mathrm{cor}(f) - 1$$

for resilient functions f*, except for affine functions.*

By Proposition 10.7, a perfect coloring of the n-dimensional Boolean hypercube with quotient matrix

$$\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix} \tag{35}$$

is a correlation-immune function of order

$$\frac{b+c}{2} - 1.$$

Therefore, Proposition 14.5 implies the following.

Corollary 14.2. *Let* $f : Q_2^n \to Q_2$ *be a perfect coloring with quotient matrix (35). Then*

$$\deg(f) \le n - \frac{b+c}{2} + 1.$$

Boolean functions $f : Q_2^n \to Q_2$ can be represented by their vectors of values and hence regarded as elements of the Boolean cube of dimension 2^n. The set of value vectors of Boolean functions of algebraic degree at most m is called the *Reed–Muller code* of type $\mathcal{R}(m, n)$ in $Q_2^{2^n}$. The Reed–Muller code is linear, since the degree of the sum of two polynomials does not exceed the maximum of their degrees.

Proposition 14.6 ([99])**.** *For every nonzero Boolean function* f*,*

$$|\mathrm{supp}(f)| \ge 2^{n-\deg(f)}.$$

If $|\mathrm{supp}(f)| = 2^{n-\deg(f)}$*, then* $\mathrm{supp}(f)$ *is an affine subspace.*

Proof. We use induction on n. If the function f is equal to 1 at a single point, then its sum over the entire Boolean hypercube is odd, and hence its algebraic normal form contains a term of degree n.

Suppose that f takes the value 1 at more than one point. Then, in at least one direction, each of the two hyperfaces contains at least one point at which f takes the value 1. The degree of the restriction of f to a hyperface does not exceed the degree of f. By the induction hypothesis, each of the two hyperfaces contains at least $2^{(n-1)-\deg(f)}$ ones of f.

A Boolean function is an indicator function of an affine subspace if and only if its intersection with every face in every direction has cardinality 2^i, $i = 0, \ldots, n$, or 0. The equality case can be proved by induction as well. $\square$

Corollary 14.3. *The minimum distance of the Reed–Muller code $\mathcal{R}(m, n)$ is 2^{n-m}.*

14.3 Polynomial Representation of Linear Codes

By Theorem 8.1 every isometry of a Boolean hypercube is the composition of a shift and permutation of variables. A shift of a set $C \subset Q_2^n$ by any vector $y \in Q_2^n$ is performed by the change of variables $x' = x \oplus y$ of the indicator function $\mathbf{1}_C$. Therefore, isometric transformations do not change the degree of the characteristic function of a set. An affine subspace C can be transformed into a linear subspace by adding to it any vector belonging to C. Any linear subspace C can be specified by a full-rank parity-check matrix H, i.e.,

$$C = \{x \in Q_2^n \mid Hx = \bar{0}\},$$

where $H = \{h_{ij}\}$ is a $k \times n$ matrix and $\operatorname{rank}(C) = n - k$.

Proposition 14.7. *The degree of the characteristic function of a linear code $C \subset Q_2^n$ is equal to $n - \operatorname{rank}(C)$.*

Proof. Let $C = \{x \in Q_2^n \mid Hx = \bar{0}\}$, where $H = \{h_{ij}\}$ is a $k \times n$ matrix and $k = n - \operatorname{rank}(C)$. Consider the set $C' = \{x \in Q_2^n \mid Hx = \bar{1}\}$. Clearly, C' is an affine subspace equivalent to the code C. It is easy to see that

$$\mathbf{1}_{C'}(x) = \prod_i \left(\bigoplus_j h_{ij} x_j \right),$$

i.e., the product of the sums of the rows of the matrix $H[x]$. Clearly, $\deg(\mathbf{1}_{C'}) \leq k$.

Consider a nonsingular $k \times k$ submatrix A of H. Since A is a matrix over $GF(2)$, its nonsingularity is equivalent to $\det(A) = 1$. It follows from

$\det(A) = 1$ that the monomial corresponding to the columns of A occurs an odd number of times in the product

$$\prod_i \left(\bigoplus_j h_{ij} x_j \right).$$

Hence this product contains a monomial of degree k, and therefore $\deg(\mathbf{1}_{C'}) = k$. Since C' is equivalent to C, we obtain $\deg(\mathbf{1}_C) = k = n - \mathrm{rank}(C)$. □

Corollary 14.4. *Let $C \subset Q_2^n$ be a Hamming code, where $n = 2^t - 1$. Then $\deg(\mathbf{1}_C) = t$.*

14.4 Algebraic Degrees of Bent and Plateaued Functions

The following statement is obtained from Sarkar's identity.

Proposition 14.8. *Let f be a Boolean function and suppose that, for every $v \in Q_2^n$, $\widehat{(-1)^f}(v) = 2^k m(v)$, where $m(v)$ and k are integer. Then $\deg(f) \le \frac{n}{2} - k + 1$.*

Proof. Consider a monomial $x_1^{y_1} \cdots x_n^{y_n}$ of maximum degree in the algebraic normal form of f, i.e.,

$$G[f](y) = 1 \qquad \text{and} \qquad \mathrm{wt}(y) = \deg(f).$$

Then

$$\sum_{x \le y} f(x) \equiv 1 \pmod 2,$$

and hence

$$\sum_{x \le y} (-1)^{f(x)} = 2(m' + 1),$$

where m' is even and may be negative.

By Sarkar's identity (Corollary 11.3),

$$\sum_{v \in Q_2^n,\, v \le y \oplus \bar{1}} \widehat{(-1)^f}(v) = 2^{n/2 - \mathrm{wt}(y)} \sum_{v \in Q_2^n,\, x \le y} (-1)^{f(x)} = (1 + m') 2^{n/2 - \deg(f) + 1}. \tag{36}$$

By the assumption, the left-hand side is divisible by 2^k. Therefore, $k \le \frac{n}{2} - \deg(f) + 1$, which proves the proposition. □

Note that k in this statement may also be negative.

Theorem 14.1.
(a) *If f is a bent function, then* $\deg(f) \le n/2$ *for* $n \ge 4$;
(b) *If f is resilient and* $nl(f) = 2^{n-1} - 2^{\mathrm{cor}(f)+1}$, *then* $\deg(f) = n - \mathrm{cor}(f) - 1$;
(c) *f is not resilient and* $nl(f) = 2^{n-1} - 2^{\mathrm{cor}(f)}$, *then* $\deg(f) = n - \mathrm{cor}(f)$ *and, moreover,* $G[f](y) = 1$ *for every y with* $\mathrm{wt}(y) = n - \mathrm{cor}(f)$.

Proof. (a) For a bent function, we have $\left|\widehat{(-1)^f}\right| = \mathbf{1}$. It follows from Proposition 14.8 that $\deg(f) \le \frac{n}{2} + 1$. We now improve this bound. Let $\mathrm{wt}(y) = \deg(f)$. A face of dimension $n - \deg(f)$ contains $2^{n-\deg(f)}$ points, and $n - \deg(f) > 0$ for $n > 2$. Therefore, the sum

$$\sum_{v \in Q_2^n,\, v \le y \oplus \bar{1}} \widehat{(-1)^f}(v)$$

in (36) is even. It follows from (36) that $2^{n/2-\deg(f)}$ is an integer. Hence $\deg(f) \le n/2$.

(b) By Corollary 14.1, it is sufficient to prove that

$$\deg(f) \ge n - \mathrm{cor}(f) - 1.$$

By Sarkar's identity (Remark 11.2) and Proposition 13.6, all nonzero Walsh–Hadamard coefficients of f have the form $\pm 2^{2+\mathrm{cor}(f)-n/2}$. By Theorem 10.1, there exists $y \in Q_2^n$ with $\mathrm{wt}(y) = \mathrm{cor}(f) + 1$ such that

$$\left|\widehat{(-1)^f}(y)\right| = 2^{2+\mathrm{cor}(f)-n/2}.$$

Similarly to (36), we have

$$\pm 2^{2+\mathrm{cor}(f)-n/2} = \sum_{v \in Q_2^n,\, v \le y} \widehat{(-1)^f}(v) = 2^{\frac{n}{2} - \mathrm{wt}(y \oplus \bar{1})} \sum_{x \le y \oplus \bar{1}} (-1)^{f(x)}$$

$$= 2^{\mathrm{cor}(f) - \frac{n}{2} + 1} \sum_{x \le y \oplus \bar{1}} (-1)^{f(x)}.$$

Consequently,

$$\sum_{x \le y \oplus \bar{1}} (-1)^{f(x)} = \pm 2.$$

This is possible only if $\sum_{x \le y \oplus \bar{1}} f(x) \equiv 1 \pmod 2$. Therefore,

$$\deg(f) \ge \mathrm{wt}(y \oplus \bar{1}) = n - \mathrm{cor}(f) - 1.$$

(c) By Corollary 14.1, it is sufficient to prove that

$$\deg(f) \geq n - \mathrm{cor}(f).$$

By Sarkar's identity (Remark 11.2) and Proposition 13.6, all nonzero Walsh–Hadamard coefficients of f have the form $\pm 2^{\mathrm{cor}(f)+1-n/2}$.

Since f is not resilient,

$$\left|\widehat{(-1)^f}(\bar{0})\right| = 2^{\mathrm{cor}(f)+1-n/2}.$$

By Theorem 10.1, $\widehat{(-1)^f}(z) = 0$ for all z satisfying $0 < \mathrm{wt}(z) \leq \mathrm{cor}(f)$.

Consider an arbitrary y such that

$$\mathrm{wt}(y) = n - \mathrm{cor}(f) \qquad \text{and} \qquad \mathrm{wt}(y \oplus \bar{1}) = \mathrm{cor}(f).$$

Then, from the left-hand side of (36),

$$2^{n/2-\mathrm{wt}(y)} \sum_{x \leq y} (-1)^{f(x)} = \widehat{(-1)^f}(\bar{0}) = \pm 2^{\mathrm{cor}(f)+1-n/2}.$$

Therefore,

$$\sum_{x \leq y} (-1)^{f(x)} = \pm 2.$$

This is possible only if $\sum_{x \leq y} f(x) \equiv 1 \pmod 2$. Hence $G[f](y) = 1$.

□

Theorem 14.1 means that a maximally nonlinear function for a fixed correlation immunity is not only plateaued, but also attains equality in the Siegenthaler inequality.

14.5 Algebraic Immunity

The following problem arises in the cryptanalysis of certain ciphers. Suppose that a Boolean function $f : Q_2^n \to Q_2$, an affine transformation $L : Q_2^n \to Q_2^n$, and an output sequence

$$b_0 = f(x), \qquad b_1 = f(L(x)), \qquad \ldots, \qquad b_i = f(L^i(x)), \qquad \ldots$$

are known. The task is to determine the key $x \in Q_2^n$. The complexity of the resulting system of equations depends on the degree of f. Therefore, if there exists a Boolean function g such that

$$\deg(g) < \deg(f) \qquad \text{and} \qquad gf = \mathbf{0},$$

then one can search for possible values of x as solutions of the simpler system

$$g(x)b_0 = 0, \qquad \ldots \qquad g(L^i(x))b_i = 0, \qquad \ldots$$

The algebraic immunity of f is introduced to measure the resistance of f to this type of cryptanalysis.

The *algebraic immunity* of a Boolean function f is defined by

$$AI(f) = \min_g \{\deg(g) : gf = \mathbf{0} \text{ or } g(f \oplus \mathbf{1}) = \mathbf{0}, \quad g \neq \mathbf{0}\}.$$

Theorem 14.2 (Courtois and Meier [32]). *For every Boolean function $f : Q_2^n \to Q_2$, there exists a Boolean function g such that*

$$\deg(g) \leq \left\lceil \frac{n}{2} \right\rceil \qquad \textit{and} \qquad \deg(fg) \leq \left\lfloor \frac{n}{2} \right\rfloor.$$

Proof. Let A_d be the set of all monomials of degree at most d,

$$|A_d| = \sum_{i=0}^{d} \binom{n}{i}.$$

Take $d_1 = \left\lfloor \frac{n}{2} \right\rfloor$, $d_2 = \left\lceil \frac{n}{2} \right\rceil$. Consider the set of functions $B = \{fw : w \in A_{d_2}\}$. If B is a linearly dependent set then there exist $w_1, \ldots, w_k \in A_{d_2}$ such that $fw_1 \oplus \cdots \oplus fw_k = 0$. Then we have found a function $g = w_1 \oplus \cdots \oplus w_k$ satisfying the conditions of the theorem. Otherwise, B is linearly independent and $|B| = |A_{d_2}|$.

We have

$$|B| + |A_{d_1}| = \sum_{i=0}^{d_1} \binom{n}{i} + \sum_{i=0}^{d_2} \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} + \binom{n}{\lfloor n/2 \rfloor} > 2^n.$$

Since the vector space of Boolean functions over $GF(2)$ has dimension 2^n, the set of functions $B \cup A_{d_1}$ is linearly dependent. Hence there exists a linear combination of the form $h \oplus fg = \mathbf{0}$, where h is a linear combination of monomials from A_{d_1} and g is a linear combination of monomials from A_{d_2}. Therefore, $fg = h$, and so

$$\deg(fg) \leq d_1, \qquad \deg(g) \leq d_2.$$

□

Corollary 14.5. *For every Boolean function f on the n-dimensional Boolean cube,*

$$AI(f) \leq \left\lceil \frac{n}{2} \right\rceil.$$

Proof. By Theorem 14.2, there exists a Boolean function g such that

$$\deg(g \oplus fg) \leq \left\lceil \frac{n}{2} \right\rceil.$$

Set $h = g \oplus fg$. Then $fh = fg \oplus fg = \mathbf{0}$. Hence

$$AI(f) \leq \deg(h) \leq \left\lceil \frac{n}{2} \right\rceil.$$

□

Proposition 14.9 (Canteaut [24]). *For every Boolean function f on the n-dimensional Boolean cube,*

$$nl(f) \geq \sum_{i=0}^{AI(f)-2} \binom{n}{i}.$$

Proof. We first estimate the weight $\mathrm{wt}(f) = |\mathrm{supp}(f)|$. Consider the system of $|\mathrm{supp}(f)|$ Boolean equations

$$\sum_{w \in A_d} a_w w(x) = 0$$

in the unknowns a_w, where x ranges over all elements of $\mathrm{supp}(f)$. If this system has a nonzero solution (a_w), then $f \cdot \left(\sum_{w \in A_d} a_w w \right) = \mathbf{0}$. Choose d so that

$$AI(f) = d + 1.$$

Then the system has only the zero solution. Consequently, the number of equations is at least the number of variables, i.e.,

$$\sum_{i=0}^{AI(f)-1} \binom{n}{i} \leq \mathrm{wt}(f).$$

Now consider the function $f \oplus \ell$, where ℓ is an arbitrary affine function. If $(f \oplus \ell)g = \mathbf{0}$ for some function g, then $fg = g\ell$. Therefore,

$$fg(1 \oplus \ell) = g\ell(1 \oplus \ell) = g\ell \oplus g\ell = \mathbf{0}.$$

Moreover,

$$\deg(g(1 \oplus \ell)) \leq \deg(g) + 1.$$

Consequently, $AI(f \oplus \ell) \le AI(f) + 1$. Applying the same argument to $f \oplus \ell$ and ℓ, we obtain

$$AI(f) = AI(f \oplus \ell \oplus \ell) \le AI(f \oplus \ell) + 1.$$

It follows that

$$\sum_{i=0}^{AI(f)-2} \binom{n}{i} \le \sum_{i=0}^{AI(f\oplus\ell)-1} \binom{n}{i} \le \mathrm{wt}(f \oplus \ell).$$

By the definition of the nonlinearity, $nl(f) = \min_\ell \mathrm{wt}(f \oplus \ell)$, and hence the desired inequality follows. □

Exact relations between algebraic immunity and nonlinearity (i.e., the distance from a function to affine functions or, more generally, to functions of bounded degree) were obtained by Lobanov [95].

14.6 Problems

109. Prove that every function $f : Q_p^n \to Q_p$, where p is prime, can be represented uniquely as a polynomial over $GF(p)$ of degree at most $n(p-1)$, with the degree of each variable in every monomial not exceeding $p-1$.

110. Prove that, for prime q, the degree of the characteristic function of a linear code $C \subset Q_q^n$ is equal to $n - \mathrm{rank}(C)$.

111. Prove that for a non-resilient plateaued function f the following property holds: $|\widehat{(-1)^f}(z)| = |\widehat{(-1)^f}(y)|$ whenever $\mathrm{wt}(y) = \mathrm{wt}(z)$. In particular, $|\widehat{(-1)^f}(z)| = 2^{\mathrm{cor}(f)+1-\frac{n}{2}}$ for $\mathrm{wt}(z) = \mathrm{cor}(f) + 1$.

112. Prove that a Boolean function $f : Q_2^n \to Q_2$ depends linearly on the variable x_i (over $GF(2)$) if and only if $\widehat{(-1)^f}(z) = 0$ for all $z \in Q_2^n$ such that $z_i = 0$.

113. Prove that for every $k \ge 0$ there exists $n(k)$ such that, for $n \ge n(k)$, the following holds: if $\mathrm{cor}(f) \ge n-k$, then the Boolean function $f : Q_2^n \to Q_2$ depends linearly on some of its variables.

114. Prove that for every $k \ge 0$ there exists $n(k)$ such that, for $n \ge n(k)$, the following holds: if $\widehat{f}(z) = 0$ whenever $\mathrm{wt}(z) \ge k$, then the Boolean function $f : Q_2^n \to Q_2$ does not depend on some of its variables.

115. Prove that the size of the support of a Boolean function of degree k in n variables is divisible by $2^{\lceil n/k \rceil - 1}$. (the McEliece theorem)

116. Prove that the degree of the characteristic function of a binary 1-perfect code of length n is at most $\frac{n+1}{2}$. Estimate the minimum Hamming distance between two binary 1-perfect codes.

117. Estimate the minimum Hamming distance between two s-plateaued functions.

118. Prove that the Reed–Muller codes $\mathcal{R}(m,n)$ and $\mathcal{R}(n-m-1,n)$ are dual and

$$\mathcal{R}(k,n) \subseteq \mathcal{R}(m,n)^{\perp}$$

whenever $k+m<n$. Determine when $\mathcal{R}(m,n)$ is self-dual.

119. Prove that $\mathcal{R}(1,n)$ is the extended Hadamard code, while $\mathcal{R}(n-2,n)$ is the extended Hamming code.

120. Prove that if two Boolean functions f and g, both of degree at most r, agree on the ball B_r of radius r, then $f=g$.

121. Prove that if two Boolean functions f and g are EA-equivalent and $\deg(f) \geq 2$ then $\deg(f) = \deg(g)$.

122. Prove that every n-variable Boolean function of algebraic degree 2 is EA-equivalent to quadratic form $\bigoplus_{0<i<k} x_{2i-1}x_{2i}$ for some $k \leq n/2$ (Dickson's theorem).

15 Perfect Colorings of Multigraphs and Hypergraphs

15.1 Perfect Colorings of Hypergraphs

A *multigraph* is a generalization of a graph that admits multiple edges and loops. A graph or multigraph is called *directed* if it consists of ordered pairs of vertices, called *arcs*, instead of edges. Any nonnegative integer square matrix can be the adjacency matrix of a directed multigraph. The definition of a perfect coloring of a directed multigraph is similar to the definition of a perfect coloring of a simple graph. However, in the case of directed multigraph, we consider as the neighborhood of a vertex only those vertices that are the endpoints of arcs originating at that vertex. The neighborhood

or sphere of a vertex is a multiset, since some vertices can be the endpoints of several parallel arcs. It is easy to see that the algebraic criterion for perfect coloring (Proposition 2.3) also holds for multigraphs. Note that the quotient matrix of any perfect coloring can be viewed as the adjacency matrix of some directed multigraph. Then a perfect coloring of a graph with this quotient matrix can be considered as a covering. Furthermore, a merging of colors can be viewed as a perfect coloring of this multigraph.

Let G be a bipartite graph with parts V and U. Consider an undirected multigraph $\mathcal{M}_{12}(G)$ whose vertices are the vertices of the first part of G and the vertices $v_i, v_j \in V$ are connected by m_{ij} edges if G has m_{ij} distinct vertices from U adjacent to both v_i and v_j simultaneously. For convenience, we assume that the multigraph $\mathcal{M}_{12}(G)$ contains loops at its vertices of multiplicity equal to the vertex degree in G. If G is biregular, then the loops in $\mathcal{M}_{12}(G)$ have the same multiplicity. Let the graph G be amply biregular, i.e., pairs of vertices in both parties that are at distance 2 have the same number of adjacent vertices. Then all edges in the multigraph $\mathcal{M}_{12}(G)$ have the same multiplicity. Below, we assume that the graph G is biregular (not necessarily regular) and consider only those perfect colorings of G for which all colors in different parts are distinct.

Proposition 15.1 ([118]). *Let $f : V \cup U \to \{1, \dots, k\}$ be a perfect coloring of the bipartite graph G with parts V and U. Then $f|_V$ is a perfect coloring of $\mathcal{M}_{12}(G)$.*

Proof. The adjacency matrix of G can be represented as $M = \begin{pmatrix} 0 & Y \\ Y^{\mathsf{T}} & 0 \end{pmatrix}$. Let $S = \begin{pmatrix} 0 & S_1 \\ S_2 & 0 \end{pmatrix}$ be the quotient matrix of a perfect coloring. Then, from the algebraic criterion of perfect coloring (Proposition 2.3), we have the equality $MF = FS$, which is equivalent to the pair of equalities $YF_2 = F_1S_1$ and $Y^{\mathsf{T}}F_1 = F_2S_2$, where $F = \begin{pmatrix} F_1 & 0 \\ 0 & F_2 \end{pmatrix}$, and the matrices F_1 and F_2 correspond to the colorings of the first and second parts of G. We have $YY^{\mathsf{T}}F_1 = YF_2S_2 = F_1S_1S_2$. It remains to note that YY^{T} is the adjacency matrix of the multigraph $\mathcal{M}_{12}(G)$ and, by Proposition 2.3, S_1S_2 is the quotient matrix of the perfect coloring $f|_V$. □

The converse, generally speaking, is false. A perfect coloring of $\mathcal{M}_{12}(G)$ need not be the restriction of any perfect coloring of G. In particular, such examples are easy to find when $\mathcal{M}_{12}(G)$ is a complete graph.

A *hypergraph* is another generalization of the concept of a graph, in which we consider unordered sets of more than two vertices as edges. A hypergraph is called *k-uniform* if its edge consists of k vertices. The *incidence matrix* of a hypergraph G is a $(0,1)$-matrix $Y = (y_{ij})$ of size $n \times m$, where n is the number of vertices and m is the number of edges in G. Moreover,

$$y_{ij} = \begin{cases} 1, \text{ if } v_i \in e_j \in E(G); \\ 0, \text{ else.} \end{cases}$$

For a hypergraph G, we define a bipartite graph $\mathcal{D}(G)$, whose first part is the vertices of G, and whose second part is the edges of G. A vertex $v \in V(G)$ of the first part is adjacent to a vertex $e \in E(G)$ of the second part if $v \in e$. It is easy to see that the adjacency matrix of $\mathcal{D}(G)$ can be represented as $\begin{pmatrix} 0 & Y \\ Y^{\mathsf{T}} & 0 \end{pmatrix}$, where Y is the incidence matrix of G.

A vertex coloring of a hypergraph G is called *perfect* if the induced (see Section 4.3) coloring of the bipartite graph $\mathcal{D}(G)$ is perfect.

In other words, a hypergraph coloring is perfect if, for any fixed edge color, any two vertices of the same color are incident with an equal number of edges of that fixed color. This definition was first proposed by Godsil [53].

Similar to the algebraic criterion of perfect coloring (Proposition 2.3), we obtain that the definition of a perfect hypergraph coloring is equivalent to the equation

$$\begin{pmatrix} 0 & Y \\ Y^{\mathsf{T}} & 0 \end{pmatrix} \begin{pmatrix} 0 & F_1 \\ F_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & F_1 \\ F_2 & 0 \end{pmatrix} \begin{pmatrix} 0 & S_1 \\ S_2 & 0 \end{pmatrix},$$

where the matrices F_1 and F_2 correspond to colorings of the vertices and hyperedges of G, respectively. This equality is equivalent to the pair of equalities $YF_2 = F_1S_1$ and $Y^{\mathrm{T}}F_1 = F_2S_2$.

Consider the adjacency matrix M of the multigraph $\mathcal{M}_{12}(\mathcal{D}(G))$. It is easy to see that the entries m_{ij} of M are equal to the number of edges of the hypergraph G that contain both the i-th and j-th vertices. In particular, m_{ii} is the degree of the i-th vertex in G. Clearly, $M = YY^{\mathsf{T}}$, where Y is the incidence matrix of G.

By Proposition 15.1, we have the following corollary.

Corollary 15.1. *A perfect coloring of a hypergraph G is a perfect coloring of $\mathcal{M}_{12}(\mathcal{D}(G))$.*

The definition of perfect colorings of graphs is equivalent to the definition of perfect colorings of 2-uniform hypergraphs. Indeed, a perfect coloring of

a graph induces a coloring of its edges into pairs of colors corresponding to their endpoints. This is a perfect coloring of $\mathcal{D}(G)$ by the definition of a perfect coloring. The converse is also true: the induced colors of edges incident to a vertex uniquely determine the colors of vertices.

15.2 Line Graphs and Transversals

Let G be a k-uniform hypergraph. $\mathcal{E}(G)$ is a multigraph whose vertices are the edges of G; two vertices of $\mathcal{E}(G)$ are connected by l edges if the intersection of the corresponding edges of G has cardinality l.

From the definition, it is clear that the adjacency matrix of the line graph $\mathcal{E}(G)$ is $M = Y^{\mathsf{T}}Y - kI$, where Y is the incidence matrix of G. If the multigraph $\mathcal{E}(G)$ does not contain multiple edges, then the multigraph $\mathcal{E}(G)$ is called a *line graph* of G. Of course, the line graph of a simple graph is always a simple graph.

A coloring f' of $\mathcal{E}(G)$ is called *induced* by a coloring f of G if the color of a vertex e of $\mathcal{E}(G)$ is the multiset (taking multiplicity into account) of colors of the vertices of G contained in e, i.e., $f'(e) = \{f(v_1), f(v_2), \ldots, f(v_k)\}$, where $e = \{v_1, v_2, \ldots, v_k\}$.

Proposition 15.2. *The coloring of the graph $\mathcal{E}(G)$ induced by a perfect coloring of G is perfect.*

Proof. Let f be a perfect t-coloring of G. Consider an edge e of color composition $\{i_1, \ldots, i_t\}$, i.e., an edge containing i_j vertices of color j. By the definition of a perfect coloring, a vertex of color j is contained in a known number of hyperedges of each color composition. We collect the vectors of these colors for all vertices of the hyperedge to obtain the color composition of its adjacent hyperedges. Perhaps some edge e' intersects edge e at $s > 1$ vertices; in which case its color composition will be added s times. However, in the graph $\mathcal{E}(G)$, there are exactly s edges between the vertices corresponding to e and e'. □

A *transversal* in a hypergraph is a set of vertices that intersects (cover) every hyperedge exactly once.

In particular, in a bipartite graph, either of its parts is a transversal. It is easy to see that in a k-uniform r-regular hypergraph, a transversal is a color class of a perfect 2-coloring. Moreover, the following holds:

Proposition 15.3 ([118])**.** *A function $f : V \to \{0, 1\}$ is the characteristic function of a transversal of a k-uniform r-regular hypergraph G if and only*

if it is a perfect coloring of the multigraph $\mathcal{M}_{12}(\mathcal{D}(G))$ *with quotient matrix* $S = \begin{pmatrix} r & (k-1)r \\ r & (k-1)r \end{pmatrix}$.

Proof. Since G is r-regular, the vertices of the first part of $\mathcal{D}(G)$ have degree r. Then each vertex of $\mathcal{M}_{12}(\mathcal{D}(G))$ is incident to r loops. Vertices of the transversal are not adjacent to other vertices from the transversal in $\mathcal{M}_{12}(\mathcal{D}(G))$. Moreover, each vertex not from the transversal is adjacent to r vertices of the transversal in $\mathcal{M}_{12}(\mathcal{D}(G))$, since each vertex contained in exactly r edges, each of which contains one vertex from the transversal. Therefore, f is a perfect coloring of the multigraph $\mathcal{M}_{12}(\mathcal{D}(G))$. Moreover, this fact also follows from Proposition 15.1, since the transversal induces a 3-coloring of the graph $\mathcal{D}(G)$.

If f is a perfect coloring with quotient matrix S, then any vertex of the first color is adjacent only to itself and is not adjacent to other vertices of the first color in $\mathcal{M}_{12}(\mathcal{D}(G))$. This means that each edge of G contains at most one vertex of the first color. Furthermore, any vertex of the second color is adjacent to r vertices of the first color, which means that every hyperedge incident to it contains a vertex of the first color. □

Remark 15.1. For k-uniform hypergraphs, it is natural to define the concept of a k-dimensional adjacency matrix. Methods for determining of ordinary eigenvalues and eigenvectors of multidimensional matrices are known, preserving some. A detailed exposition of the theory of perfect hypergraph colorings can be found in [140]. In particular, analogous of Theorems 4.1, 4.2, Proposition 2.3 (algebraic criterion of perfect coloring), and Corollary 2.1 (Lloyd's theorem) were proved to be valid for k-uniform hypergraphs as well.

15.3 Problems

123. Let f be an eigenfunction of the bipartite graph G. Prove that the restriction of f to the first part, is an eigenfunction of $\mathcal{M}_{12}(G)$.

124. Prove that the eigenvalues of the multigraph $\mathcal{M}_{12}(\mathcal{D}(G))$ are nonnegative.

125. Let F_1 and F_2 be perfect colorings of the vertices and hyperedges of a hypergraph with quotient matrices S_1 and S_2, respectively. Prove the equality $F_1^{\mathsf{T}} F_1 S_1 = S_2^{\mathsf{T}} F_2^{\mathsf{T}} F_2$.

126. Let T be a transversal of a uniform regular hypergraph G. Prove that T is an independent set in the multigraph $\mathcal{M}_{12}(\mathcal{D}(G))$. Prove that if $\mathcal{D}(G)$ is amply regular, then T attains the Delsarte–Hoffman bound in the graph obtained from $\mathcal{M}_{12}(\mathcal{D}(G))$ by removing loops and edge multiplicities.

127. Let G be a regular bipartite graph. Prove that the restriction of to the first part of G an eigenfunction f with eigenvalue λ is an eigenfunction of the multigraph $\mathcal{M}_{12}(G)$ with eigenvalue λ^2. Conversely, an eigenfunction of the multigraph $\mathcal{M}_{12}(G)$ with a positive eigenvalue extends to an eigenfunction of G.

128. Let G be a biregular bipartite graph and let G' be the graph obtained from $\mathcal{M}_{12}(\mathcal{D}(G))$ by removing loops and edge multiplicities. Prove that any perfect coloring of G is a perfect coloring G'.

129. Let G_1 be a regular graph. Let $\Gamma(G_1)$ be a multigraph in which edges connect vertices at distances 1 and 2 in G_1, with taking multiplicities into account. Prove that if φ is a covering from G_2 to G_1, then φ is a covering from $\Gamma(G_2)$ to $\Gamma(G_1)$.

130. Formulate and prove an analogue of Theorem for uniform regular hypergraphs.

16 Latin Squares and 1-Factorizations of Graphs

16.1 Latin Squares

A *Latin rectangle* is an $m_1 \times m_2$ table filled with symbols (for example, elements of Q_q) such that each symbol occurs at most once in every line (row or column).

If the number of rows, columns, and distinct symbols are all equal to q, then such a Latin rectangle is called a *Latin square of order* q. The Latin coloring of the graph Q_q^2 introduced above can be regarded as an equivalent definition of a Latin square. The theory of Latin squares can be found in [38].

Example 16.1. Latin squares of orders 3, 4, and 5.

0	1	2
1	2	0
2	0	1

0	1	2	3
1	0	3	2
2	3	1	0
3	2	0	1

0	1	2	3	4
1	0	3	4	2
2	3	4	0	1
3	4	1	2	0
4	2	0	1	3

A binary operation $\circ : A^2 \to A$ is called a *quasigroup* if for every $a, b \in A$ the equations $x \circ a = b$ and $a \circ x = b$ have unique solutions. The cardinality of the set A is called the *order* of the quasigroup. More precisely, a quasigroup is a pair consisting of a set and a binary operation defined on it, in this case $(A, \circ)$. Throughout this book we consider only quasigroups of finite order. Since the nature of the underlying set is irrelevant, we will always assume that $A = Q_q$ for some $q \in \mathbb{N}$. The following proposition is an immediate consequence of the definitions.

Proposition 16.1. *A table of size $q \times q$, filled with q distinct symbols, is a Latin square if and only if it is the Cayley table of a quasigroup.*

Proposition 16.2. *If a quasigroup $(Q_q, \circ)$ is a semigroup (i.e., the operation $\circ$ is associative), then it is a group.*

Proof. Fix $a \in Q_q$. By the definition of a quasigroup, there exists $e \in Q_q$ such that $a \circ e = a$. Then, for every $b \in Q_q$, associativity yields $a \circ (e \circ b) = (a \circ e) \circ b = a \circ b$. Since left division is uniquely defined in a quasigroup, it follows that $e \circ b = b$ and, in particular, $e \circ a = a$. Applying the same argument on the other side, we obtain $b \circ e = b$ for all $b \in Q_q$. Thus, e is an identity element, and therefore $(Q_q, \circ)$ is a group. □

Let τ_i, $i = 0, 1, 2$, be permutations of the elements of the set Q_q. It is straightforward to verify that the operation $x * y = \tau_0(\tau_1(x) \circ \tau_2(y))$ is a quasigroup operation whenever $\circ$ is. The permutations τ_1 and τ_2, acting on the arguments of the quasigroup, correspond to permutations of rows and columns of the associated Latin square, and τ_0 renames its symbols.

Furthermore, the inverse operation of a quasigroup with respect to any argument is also a quasigroup. More precisely, the operations $*$ and $*'$, defined by the equality $x * z = y \Leftrightarrow x \circ y = z$ or the equality $z *' y = x \Leftrightarrow x \circ y = z$, are also quasigroup operations.

16.2 Theorems of Vizing and Ryser

The adjacency matrix of a bipartite graph has a block structure $\begin{pmatrix} 0 & M \\ M^{\mathsf{T}} & 0 \end{pmatrix}$, where M is a rectangular matrix of size $n_1 \times n_2$, where n_1 and n_2 are the sizes of two parts of the graph. The matrix M is called the *reduced adjacency matrix* of the bipartite graph.

Let $A = \{a_{ij}\}$ be an $n_1 \times n_2$ matrix. Define the graph $g(A)$ as follows. Its vertex set $V(g(A)) = \{(i, j) \mid a_{ij} \neq 0\}$ consists of the nonzero entries of the matrix. Two vertices (i, j) and (i', j') are adjacent by an edge of the first

direction if $i = i'$, and by an edge of the second direction if $j = j'$. If A is the reduced adjacency matrix of some bipartite graph G, then $g(A)$ is the line graph of G. The following observation is immediate.

Proposition 16.3. *If two vertices of $g(A)$ belongs to the same connected component, then there exists a path between them whose edges alternate between the first and second directions.*

Next we prove a weak version of Vizing's theorem.

Theorem 16.1 (Vizing)**.** *Suppose that every row and every column of a rectangular $(0,1)$-matrix A contains at most q ones. Then the ones of the matrix can be properly colored with q colors, that is, adjacent ones receive distinct colors.*

Proof. Assume, to the contrary, that such a coloring does not exist. Let $f : W \to Q_q$ be a proper coloring of a subset $W \subset V(g(A))$ of vertices of the graph $g(A)$, where the subset W has maximal possible cardinality. Then there exists a vertex $x \in V(g(A)) \setminus W$, whose neighborhood contains vertices of all q colors.

Since x has at most $q-1$ neighbors in each direction, there exist two distinct colors that are absent among the neighbors in one of the two directions. Assume that color 0 occurs only among the neighbors of x in the first direction and color 1 only among its neighbors in the second direction. Let y and z denote the neighbors of x colored 0 and 1, respectively. Consider the subgraph of $g(A)$ induced by all vertices of colors 0 and 1. Since the coloring is proper, this subgraph is bipartite. If y and z belonged to the same connected component of this subgraph, then adjoining the vertex x to a path connecting y and z would produce a cycle whose edge directions alternate by Proposition 16.3. Then the length of the path between y and z is even. It is impossible because y and z have different colors. Hence y and z belong to different connected components. Now interchange colors 0 and 1 throughout the connected component containing z. The resulting coloring remains proper. Consequently, color 1 is now available for x, and we may extend the coloring to $W \cup \{x\}$, contradicting the maximality of W. □

Let A be the reduced adjacency matrix of a bipartite graph G. By Theorem 16.1, if the maximum degree of the vertices of G is at most r, then there exists a proper edge coloring of G with r colors. This is a special case of the well-known theorem of Vizing [153], which states that every graph of maximum degree r admits a proper edge coloring with at most $r+1$ colors.

Theorem 16.2 (Ryser). *A Latin rectangle P of size $m_1 \times m_2$ can be extended to a Latin square of order q if and only if each of the q symbols occurs at least $m_1 + m_2 - q$ times.*

Proof. ($\Rightarrow$) Each letter occurs exactly $q - m_1$ times in the last $q - m_1$ rows, and exactly $q - m_2$ times in the last $q - m_2$ columns of the Latin square. Hence it occurs at most $2q - m_1 - m_2$ times outside P. Since every letter occurs q times in total, it occurs in P at least $m_1 + m_2 - q$ times.

($\Leftarrow$) First suppose that $m_2 = q$. In this case, the condition is automatically satisfied, since every symbol occurs exactly once in each of the m_1 rows, and therefore exactly m_1 times.

Construct from the Latin rectangle P a table $A = Inv(P)$ of size $q \times q$ according to the rule

$$A(i,j) = \begin{cases} k, \text{ if there exists } k \in \{1,\dots,m_1\} \text{ such that } P(k,j) = i; \\ 0, \text{ otherwise.} \end{cases}$$

Observe that if P can be extended to a Latin square, then the operation Inv corresponds to the inversion with respect to the first argument of the quasigroup defining this Latin square.

Here it is convenient to regard the alphabet of the Latin rectangle as $\{1, 2, \dots, q\}$, while the symbol 0 denotes an empty cell. By $\mathrm{supp}(A)$ we denote the $(0,1)$-matrix obtained from A by replacing every nonzero entry with 1.

For example,

$$P = \begin{array}{|c|c|c|c|} \hline 4 & 1 & 2 & 3 \\ \hline 1 & 4 & 3 & 2 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline \end{array} \qquad A = \begin{array}{|c|c|c|c|} \hline 2 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 2 \\ \hline 0 & 0 & 2 & 1 \\ \hline 1 & 2 & 0 & 0 \\ \hline \end{array} \qquad \mathrm{supp}(A) = \begin{array}{|c|c|c|c|} \hline 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 1 & 1 \\ \hline 1 & 1 & 0 & 0 \\ \hline \end{array}.$$

In every column and every row of $\mathrm{supp}(A)$ there are exactly m_1 ones. Let $B = J - \mathrm{supp}(A)$, where J is the all-ones matrix. Then every row and every column of B contains exactly $q - m_1$ ones. By Vizing's theorem, the ones of B can be properly colored with the colors $m_1 + 1, \dots, q$. It is immediate that the union of the matrices A and B forms a Latin square L.

Now compute $Inv(L)$. By the definition, the operation Inv maps Latin squares to Latin squares, and satisfies $Inv(Inv(L)) = L$. Therefore, the first m_1 rows of the Latin square $Inv(L)$ coincide with the original Latin rectangle P.

Now assume that $m_2 < q$. Applying Inv to P yields a $q \times m_2$ rectangle $A = Inv(P)$. Each column of $\mathrm{supp}(A)$ contains exactly m_1 ones, while each row contains at least $m_1 + m_2 - q$ ones by assumption. Let $B = J - \mathrm{supp}(A)$,

where J is the $q \times m_2$ of all-ones matrix. Each column of B contains $q - m_1$ ones, and each row contains at most $m_2 - (m_1 + m_2 - q) = q - m_1$ ones. Therefore, by Vizing's theorem, the ones of B can be properly colored with $q - m_1$ colors. Together with A, this yields a Latin rectangle of size $q \times m_2$. By the first part of the proof, this rectangle can be extended to a Latin square L, and the Latin square $Inv(L)$ contains the original rectangle P. □

Corollary 16.1. *Every Latin rectangle of size $m_1 \times q$ containing q distinct symbols can be extended to a Latin square.*

Note that a direct generalization of Corollary 16.1 to Latin parallelepipeds is impossible, since there exists a Latin parallelepiped of size $2 \times 5 \times 5$ which cannot be extended even to a Latin parallelepiped of size $3 \times 5 \times 5$ over an alphabet of 5 elements [105].

16.3 Theorems of Hall, Kőnig and Egerváry

A *matching* in a graph G is a set of edges such that every vertex of G is incident to at most one edge of the set.

It follows from Vizing's theorem that if the maximum degree of a bipartite graph is at most r, then its edge set can be partitioned into r matchings. We now consider the problem of determining the maximum cardinality of a matching.

A *vertex cover* of a graph G is a set of vertices such that every edge of G is incident to at least one vertex of the set.

Theorem 16.3 (Kőnig–Egerváry)**.** *In every bipartite graph, the cardinality of a maximum matching equals the cardinality of a minimum vertex cover.*

We now formulate the Kőnig–Egerváry theorem in terms of matrices.

Theorem 16.4 (Kőnig–Egerváry)**.** *Let A be a matrix. Then the minimum total number of rows and columns covering all nonzero entries of A equals the cardinality of a maximum independent set in the graph $g(A)$.*

The equivalence of these formulations is immediate if we regard $\mathrm{supp}(A)$ as the reduced adjacency matrix of a bipartite graph. Rows and columns covering all nonzero entries correspond to a vertex cover of the graph, while an independent set in $g(A)$ corresponds to a matching. We now prove the theorem.

Proof. It is clear that each row or column of a cover of $\mathrm{supp}(A)$ contains at most one vertex of an independent set. Therefore, the cardinality of an independent set cannot exceed the number of rows and columns in the cover.

Let C be a maximum independent set in $g(A)$. Then every vertex of $V(g(A)) \setminus C$ is adjacent to at least one vertex of C.

Suppose that some vertex $c \in C$ has two neighbors $a_1, a_2 \in V(g(A)) \setminus C$ in different directions, neither of which is adjacent to any other vertex of C. Then $C' = (C \setminus \{c\}) \cup \{a_1, a_2\}$ is an independent set of larger cardinality, contradicting the maximality of C.

Hence every vertex $c \in C$ may have neighbors that are adjacent to no other vertex of C only in one of the two directions, namely, either along its row or along its column. Let C_1 denote the set of vertices of the first type and C_2 the set of vertices of the second type.

Suppose that a vertex $c_1 \in C_1$ is connected to a vertex $c_2 \in C_2$ by an alternating path whose vertices alternately belong to C and to $V(g(A)) \setminus C$. There exist vertices $a_i \in V(g(A)) \setminus C$, $i = 1, 2$, adjacent only to c_i. Replacing the vertices of C on the path by the remaining vertices of the path, including a_1 and a_2, yields an independent set whose cardinality exceeds that of C, a contradiction.

Thus the vertices of C can be partitioned into three classes: C_1', consisting of vertices connected by alternating paths to vertices of C_1, $C_1 \subseteq C_1'$; C_2', consisting of vertices connected by alternating paths to vertices of C_2, $C_2 \subseteq C_2'$; and the remaining vertices.

For each vertex of C_1', select its row, and for each vertex of C_2', select its column. Let $X \subseteq V(g(A))$ denote the set of vertices covered by these lines.

Now consider a vertex $a \in V(g(A)) \setminus X$. There exist vertices from C adjacent to a both by row and by column by definition of C_i. Both these vertices belong to $C \setminus (C_1' \cup C_2')$, since if one of them belongs to C_i', then the other also belongs to C_i' by the construction. For each vertex of $C \setminus (C_1' \cup C_2')$, take the row containing it. The selected rows and columns together cover all nonzero entries of $\mathrm{supp}(A)$, and their total number is exactly $|C|$. □

Consider a bipartite graph with parts U and W. For every subset $U' \subseteq U$, let $S(U') \subseteq W$ denote the set of vertices adjacent to at least one vertex of U'.

Theorem 16.5 (Hall)**.** *A bipartite graph with parts U and W has a matching of cardinality $|U|$ if and only if $|U'| \le |S(U')|$ for every subset $U' \subseteq U$.*

We now formulate Hall's theorem in terms of matrices.

Theorem 16.6 (Hall). *Let A be an $n_1 \times n_2$ matrix. The graph $g(A)$ contains an independent set of cardinality n_1 if and only if* $\operatorname{supp}(A)$ *contains no all-zero submatrix of size $k_1 \times k_2$ satisfying $k_1 + k_2 > n_2$.*

The equivalence of these formulations is immediate if we regard $\operatorname{supp}(A)$ as the reduced adjacency matrix of a bipartite graph. By definition, sizes of largest all-zero submatrices are $|U'| \times (n_2 - |S(U')|)$, where $U' \subset U$. Then the condition $|U'| \le |S(U')|$ is equivalent to $k_2 = n_2 - |S(U')| \le n_2 - k_1$ for every all-zero submatrix. Now let us prove the theorem.

Proof. Suppose that A contains an all-zero submatrix of size $k_1 \times k_2$ with $k_1 + k_2 > n_2$. Then among these k_1 rows one can choose at most $n_2 - k_2 < k_1$ independent vertices of the graph $g(A)$.

Conversely, let $k_1 \times k_2$ be a largest zero submatrix of A. Then a minimum cover of $\operatorname{supp}(A)$ consists of

$$n_1 - k_1 + n_2 - k_2$$

rows and columns. Since

$$k_1 + k_2 \le n_2,$$

we have

$$n_1 - k_1 + n_2 - k_2 \ge n_1.$$

Therefore, by the Kőnig–Egerváry theorem, the graph $g(A)$ contains an independent set of cardinality at least n_1. □

16.4 Perfect Matchings

A *perfect matching (1-factor)* in a graph (or hypergraph) G is a set of edges (hyperedges) such that every vertex of G is incident to exactly one edge of the set.

Clearly, a necessary condition for the existence of a perfect matching in a graph is that the number of vertices be even. In the case of a bipartite graph, it is additionally necessary that the two parts have equal cardinality.

A 1-*factorization* of a graph G is a partition of its edge set into perfect matchings.

A necessary condition for the existence of a 1-factorization is that the graph be regular.

We first consider an r-regular bipartite graph G. Regularity implies that the two parts of G have equal cardinality, and its reduced adjacency matrix M contains exactly r ones in every row and every column. Diagonals

consisting entirely of ones in M correspond to perfect matchings of G, while a proper coloring of $g(M)$ with r colors is equivalent to a 1-factorization of G. Therefore, Vizing's theorem immediately yields the following result.

Corollary 16.2. *Every regular bipartite graph admits a* 1*-factorization.*

We now turn to arbitrary (not necessarily bipartite) graphs. A perfect matching in a r-regular graph G corresponds to a symmetric (with respect to the main diagonal) diagonal consisting of ones in its adjacency matrix M. Consequently, a 1-factorization of G is equivalent to a symmetric proper (and perfect at the same time) coloring of the ones of M, i.e., a perfect coloring of $g(M)$ with quotient matrix

$$2(J-I) = \begin{pmatrix} 0 & 2 & \dots & 2 \\ 2 & 0 & 2 & \dots \\ \vdots & \vdots & \ddots & \vdots \\ 2 & \dots & 2 & 0 \end{pmatrix}. \tag{37}$$

A line graph $\mathcal{E}(G)$ differs from the graph $g(M)$ in that we consider opposite points to be the same, i.e., $g(M)$ covers $\mathcal{E}(G)$. Since G is r-regular, $\mathcal{E}(G)$ is $2(r-1)$-regular. By definitions, a perfect matching of G is a cell of an equitable 2-partition of $\mathcal{E}(G)$ with quotient matrix

$$\begin{pmatrix} 0 & 2(r-1) \\ 2 & 2(r-2) \end{pmatrix}.$$

Moreover, every 1-factorization of G induces a perfect coloring of $\mathcal{E}(G)$ with quotient matrix (37).

The concepts of a perfect matching and 1-factorization are naturally generalized to uniform hypergraphs. It is easy to see that a perfect matching and 1-factorization of a regular hypergraph G also correspond to perfect colorings of $\mathcal{E}(G)$. Consider a hypergraph G' obtained from G as follows: $V(G') = E(G)$, $E(G') = V(G)$, and $v \in e$ in G' if and only if $e \in v$ in G. Then perfect matchings of G one-to-one correspond to transversals of G'.

16.5 Permanents and Doubly Stochastic Matrices

The *permanent* $\mathrm{per}(A)$ of a $k \times m$ matrix A, where $k \le m$, is defined by

$$\mathrm{per}(A) = \sum_{\sigma} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{k\sigma(k)},$$

where the sum is taken over all injective mappings

$$\sigma : \{1, \ldots, k\} \to \{1, \ldots, m\}.$$

Observe that, for every nonnegative matrix A,

$$\operatorname{per}(A) = 0 \quad \Longleftrightarrow \quad \operatorname{per}(\operatorname{supp}(A)) = 0.$$

If M is the reduced adjacency matrix of a bipartite graph G, then $\operatorname{per}(M)$ equals the number of matchings of maximum possible cardinality. In particular, when $k = m$, $\operatorname{per}(M)$ equals the number of perfect matchings.

Theorem 16.7 ([3]). *Let M be the adjacency matrix of a graph G. Then the number of perfect matchings in G does not exceed $\sqrt{\operatorname{per}(M)}$.*

Proof. Consider an arbitrary pair of perfect matchings in G. Their union forms a 2-regular spanning (containing all graph's vertices) subgraph (allowing multiple edges), called a 2-*factor*. If every cycle of the 2-factor f is even (counting a pair of parallel edges as a 2-cycle), then its edges can be partitioned into two perfect matchings in exactly $2^{s(f)}$ ways, where $s(f)$ denotes the number of cycles of length at least four. If the 2-factor contains an odd cycle, such a decomposition is impossible. Hence the square of the number of perfect matchings equals $\sum_f 2^{s(f)}$, where the sum ranges over all 2-factors whose cycles are all even.

Now consider a diagonal consisting entirely of ones in the adjacency matrix M. Each vertex of the graph is adjacent to two edges along the diagonal: one 1 in the row and another 1 in the column corresponding to the vertex. Therefore, a diagonal of 1s corresponds to some 2-factor in the graph G. Such a diagonal determines a 2-factor of G. Moreover, on every cycle of length at least three we may replace each selected entry by its symmetric counterpart without changing the corresponding 2-factor. Consequently, $\operatorname{per}(M) \geq \sum_f 2^{s(f)}$, where the sum ranges over all 2-factors. The theorem follows immediately. □

For a bipartite graph G with equally sized parts, the square root of the permanent of its adjacency matrix equals the permanent of its reduced adjacency matrix and therefore equals the number of perfect matchings.

Proposition 16.4. *Let G be a bipartite graph with reduced adjacency matrix M of size $k \times m$. Then the total number of matchings in G equals* $\operatorname{per}(A)$, *where $A = (I_k \mid M)$ is the $k \times (k + m)$ matrix obtained by adjoining the identity matrix to M.*

Proof. We establish a bijection between diagonals of k ones in A and matchings in G. Each such diagonal consists of a partial diagonal in M, representing the edges of the matching, together with diagonal entries of I_k, representing those vertices of the first part not incident to the matching. Since every edge of a bipartite graph is incident to a unique vertex of the first part, this correspondence is bijective. □

A nonnegative matrix is called *doubly stochastic* if the sum of the entries in every row and every column equals 1. In particular, every permutation matrix

$$P_{ij}(\tau) = \begin{cases} 1, & j = \tau(i), \\ 0, & \text{otherwise}, \end{cases}$$

is doubly stochastic.

Theorem 16.8 (Kőnig–Frobenius)**.** *For every doubly stochastic matrix A, we have*

$$\operatorname{per}(A) > 0.$$

Proof. Suppose that a doubly stochastic matrix A of size $m \times m$ contains exactly m nonzero entries ($|\operatorname{supp}(A)| = |V(g(A))| = m$). Then A is a permutation matrix, and therefore $\operatorname{per}(A) = 1$.

Assume, to the contrary, that there exists a doubly stochastic matrix of size $m \times m$ with zero permanent. Among all such matrices, choose one, denoted by B, having the minimum number of entries satisfying $0 < b_{ij} < 1$. As observed above, $|V(g(B))| > m$, so such an entry necessarily exists.

For every entry satisfying $0 < b_{ij} < 1$, there exist neighboring entries

$$0 < b_{i'j} < 1, \qquad 0 < b_{ij'} < 1,$$

where $i' \neq i$ and $j' \neq j$. Hence every vertex of the subgraph of $g(B)$ induced by the entries $0 < b_{ij} < 1$ has degree at least two. Consequently, this subgraph contains an even cycle c whose edge directions alternate.

Let

$$\alpha = b_{i_0 j_0} = \min\{b_{ij}\} \leq \beta = \min\{1 - b_{ij}\},$$

where both minimums are taken over the vertices of the cycle c.

Construct a matrix C whose entries are zero except on the cycle c, where they are equal to $-\alpha$ at vertices lying at even distance (including distance zero) from (i_0, j_0) and to α at vertices lying at odd distance. The sum of the entries of C in every row and every column is zero. Therefore, $B + C$ is again doubly stochastic.

Moreover, $B + C$ contains fewer entries satisfying $0 < b_{ij} < 1$ than B. Since $\operatorname{supp}(B+C) \subseteq \operatorname{supp}(B)$ and $\operatorname{per}(B) = 0$, we also have $\operatorname{per}(B+C) = 0$. This contradicts the minimality of the number of fractional entries in B. The case $\beta < \alpha$ is treated analogously. □

It follows from the Kőnig–Frobenius theorem (or from Vizing's theorem) that every $(0,1)$-matrix having the same number of ones in each row and in each column has positive permanent. Van der Waerden conjectured that the minimum permanent among all $n \times n$ doubly stochastic matrices is achieved by the matrix for which all entries are equal to $1/n$. Proofs of this conjecture were obtained by Egorychev [41] and Falikman [45].

Theorem 16.9 (Birkhoff)**.** *Every doubly stochastic matrix is a convex combination of permutation matrices.*

Proof. If a doubly stochastic matrix A of size $m \times m$ contains exactly m nonzero entries, then A is a permutation matrix.

Assume, to the contrary, that there exists a doubly stochastic matrix that cannot be expressed as a convex combination of permutation matrices. Choose such a matrix B with the minimum number of nonzero entries.

By the Kőnig–Frobenius theorem, $\operatorname{per}(B) > 0$. Hence there exists a diagonal d such that $\alpha = \min\{b_{ij} \mid (i,j) \in d\} > 0$.] Let P be the permutation matrix corresponding to the diagonal d. Since $\frac{1}{1-\alpha} - \alpha = 1$, the matrix

$$\frac{1}{1-\alpha}(B - \alpha P)$$

is doubly stochastic and contains fewer nonzero entries than B. By the minimality of B, there exist permutation matrices P_i and positive coefficients β_i satisfying

$$\sum_i \beta_i = 1, \qquad \frac{1}{1-\alpha}(B - \alpha P) = \sum_i \beta_i P_i.$$

Therefore, $B = \alpha P + (1-\alpha)\sum_i \beta_i P_i$, which expresses B as a convex combination of permutation matrices, a contradiction. □

A *convex polytope* is a bounded subset of $\mathbb{R}^n$ defined by a system of linear inequalities and equalities,

$$M_1 x \le b_1, \qquad M_2 x = b_2,$$

where b_1 and b_2 are real vectors and M_i are $m_i \times n$ real matrices. For example, the set of doubly stochastic matrices forms a convex polytope.

A *vertex* (or *extreme point*) of a convex polytope is a point that cannot be expressed as a convex combination of other points of the polytope. Every convex polytope is the convex hull of its vertices, and, conversely, the convex hull of any finite set of points is a convex polytope.

By Birkhoff's theorem, the vertices of the polytope of doubly stochastic matrices are precisely the permutation matrices.

Let F be an $n \times k$ $(0,1)$-matrix corresponding to a k-coloring of a graph. By Proposition 2.5, $P = F(F^{\mathsf{T}}F)^{-1}F^{\mathsf{T}}$ is the orthogonal projector onto the subspace spanned by the indicator functions of the color classes. By (4), the matrix P is doubly stochastic.

By Proposition 2.6, the coloring defined by F is a perfect coloring of a graph G if and only if the corresponding projector P commutes with the adjacency matrix of G. Since the set of matrices commuting with a fixed matrix forms a linear subspace, it follows that the set of doubly stochastic matrices commuting with the adjacency matrix of G is a convex polytope. We denote this polytope by $DSP(G)$.

Proposition 16.5 (Godsil [54])**.** *If every vertex of $DSP(G)$ is a permutation matrix, then every perfect coloring of G is an orbit coloring.*

Proof. Let F be the $n \times k$ matrix corresponding to a perfect coloring of G. By Proposition 2.6, the corresponding projector P belongs to $DSP(G)$.

Hence

$$P = \sum_i \alpha_i P_i, \text{ where } \qquad \alpha_i \geq 0, \quad \sum_i \alpha_i = 1,$$

and the matrices P_i are permutation matrices. Since $P_i \in DSP(G)$, each P_i commutes with the adjacency matrix of G and therefore represents an automorphism of G (see Section 4.4).

By (4), $P(x,y) > 0$ if and only if the vertices x and y have the same color. Since $P(x,y) = \sum_i \alpha_i P_i(x,y)$, there exists an index i such that $P_i(x,y) = 1$. Thus, for every pair of vertices of the same color, there exists an automorphism of G mapping x to y. Hence the coloring defined by F is an orbit coloring. □

A trivial 1-partition is equitable in every regular graph. Consequently, we obtain the following statement.

Corollary 16.3. *If G is a regular graph, and every vertex of $DSP(G)$ is a permutation matrix, then G is vertex-transitive.*

16.6 Symmetric Latin Squares

Proposition 16.6. *If q is even, then a 1-factorization of the complete graph Q_q is equivalent to a symmetric Latin square of order q with zeros on the main diagonal.*

Proof. Consider a 1-factorization of the graph Q_q. Each edge e corresponds to a pair of symmetric ones in the adjacency matrix of Q_q. Replace this pair by the symbol i whenever e belongs to the i-th 1-factor. The resulting matrix is symmetric of order q, and each symbol $0, 1, \ldots, q-1$ appears exactly once in every row and every column, since every vertex is incident to exactly one edge of each 1-factor. Conversely, reversing this construction yields a 1-factorization of the complete graph from any symmetric Latin square with zeros on the main diagonal. □

A 1-factorization of the complete graph Q_q may be viewed as a schedule for a round-robin tournament. The participants correspond to the vertices of the graph, and if the edge $\{u, v\}$ belongs to the i-th matching, then participants u and v play each other in round i.

A quasigroup $f : Q_q^2 \to Q_q$ and its Cayley table (Latin square) are called *idempotent* if $f(a, a) = a$ for every $a \in Q_q$.

A quasigroup $f : Q_{2q}^2 \to Q_{2q}$ and its Cayley table are called *semi-idempotent* if

$$f(a, a) = a, \quad a \in Q_q, \quad \text{and} \quad f(a, a) = a - q, \quad a \in Q_{2q} \setminus Q_q.$$

We now prove the existence of a 1-factorization of every complete graph of even order, as well as the existence of a symmetric idempotent Latin square of every odd order.

Theorem 16.10 ([124])**.** 1. *For every even $q \geq 2$, there exists a 1-factorization of the graph Q_q and a semi-idempotent symmetric Latin square of order q.*
2. *For every odd $q \geq 1$, there exists an idempotent symmetric Latin square of order q.*

Proof. Let $A_{2q}[Q]$ denote a symmetric Latin square of order $2q$ over the alphabet Q with constant main diagonal, let $B_{2q}[Q]$ denote a symmetric semi-idempotent Latin square of order $2q$ over Q, and let $C_{2q+1}[Q]$ denote a symmetric idempotent Latin square of order $2q + 1$ over Q.

We construct these squares by induction.

The initial squares are

$$A_2[Q_2] = B_2[Q_2] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and

$$C_3[Q_3] = \begin{pmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}.$$

Assume that $A_{2q}[Q_{2q}]$, $B_{2q}[Q_{2q}]$, and $C_{2q+1}[Q_{2q+1}]$ have already been constructed.

Then

$$A_{4q}[Q_{4q}] = \begin{pmatrix} A_{2q}[Q_{2q}] & A_{2q}[Q_{4q} \setminus Q_{2q}] \\ A_{2q}[Q_{4q} \setminus Q_{2q}] & A_{2q}[Q_{2q}] \end{pmatrix},$$

and

$$B_{4q+2}[Q_{4q+2}] = \begin{pmatrix} C_{2q+1}[Q_{2q+1}] & C_{2q+1}[Q_{4q+2} \setminus Q_{2q+1}] \\ C_{2q+1}[Q_{4q+2} \setminus Q_{2q+1}] & C_{2q+1}[Q_{2q+1}] \end{pmatrix}.$$

Next, let E be an arbitrary Latin square of order $2q+1$ over the alphabet Q_{2q+1} with zeros on the main diagonal. Starting from the Latin square

$$\begin{pmatrix} C_{2q+1}[Q_{4q+2} \setminus Q_{2q+1}] & E \\ E^{\mathsf{T}} & C_{2q+1}[Q_{4q+2} \setminus Q_{2q+1}] \end{pmatrix},$$

interchange the main diagonals of the two copies of $C_{2q+1}[Q_{4q+2} \setminus Q_{2q+1}]$ with those of the blocks E and E^{T}. The resulting Latin square is $A_{4q+2}[Q_{4q+2}]$.

Similarly, starting from

$$\begin{pmatrix} B_{2q}[Q_{2q}] & B_{2q}[Q_{4q} \setminus Q_{2q}] \\ B_{2q}[Q_{4q} \setminus Q_{2q}] & B_{2q}[Q_{2q}] \end{pmatrix},$$

interchange the second halves of the main diagonals of the two diagonal blocks. The resulting Latin square is $B_{4q}[Q_{4q}]$.

It remains to construct $C_{4q-1}[Q_{4q-1}]$ and $C_{4q+1}[Q_{4q+1}]$.

Renaming the symbols if necessary, we may assume that the symbols in the first row and first column of $A_{4q}[Q_{4q}]$ appear in increasing order. Replace the diagonal entry in position (i, i) by the symbol i for every $i \in Q_{4q}$. After deleting the first row and the first column, we obtain the Latin square $C_{4q-1}[Q_{4q} \setminus \{0\}]$. Finally, renaming the symbols yields $C_{4q-1}[Q_{4q-1}]$.

The construction of $C_{4q+1}[Q_{4q+1}]$ from $A_{4q+2}[Q_{4q+2}]$ is completely analogous. This completes the induction. □

16.7 Problems

131. Prove that every bipartite graph contains a matching whose edges are incident to all vertices of maximum degree.

132. Prove that a doubly stochastic matrix of size $n \times n$ cannot contain a zero submatrix of size $m_1 \times m_2$, where $m_1 + m_2 > n$.

133. Prove that a nonnegative matrix of size $n \times n$ has zero permanent if and only if it contains a zero submatrix of size $m_1 \times m_2$, where $m_1 + m_2 > n$.

134. [97] Let A be a $(0,1)$-matrix of size $m \times n$ containing ka ones in each row and kb ones in each column, where $k > 0$ is an integer. Prove that one can select a ones from each row of A so that exactly b ones are selected from each column.

135. [97] Prove that every bipartite graph can be extended by adding vertices and edges to one of its parts so that the maximum degree does not increase and the resulting bipartite graph is regular.

136. Prove that every regular graph has a covering graph admitting a 1-factorization.

137. Prove that every partial Latin square of order q, that is, a $q \times q$ array in which cells are filled with at most q distinct symbols and no symbol occurs more than once in any row or column, can be completed to a Latin square of order $2q$.

138. Prove that the maximum of the permanents of doubly stochastic matrices is equal to 1 and it is attained only on permutation matrices.

139. Prove (by using van der Waerden's conjecture on permanents) that the asymptotics of the number of Latin squares of order n is equal to $n^{n^2(1-o(1))}$ as $n \to \infty$.

17 MDS Codes

17.1 Basic Properties of MDS Codes

Let $C \subseteq Q_q^n$. Recall that the minimum distance (code distance) of the code C is defined by

$$d_C = \min_{\substack{x,y \in C \\ x \neq y}} d(x,y).$$

A set $C \subseteq Q_q^n$ is called a *maximum distance separable (MDS) code* with distance d if $|C \cap \Gamma| = 1$ for every $(d-1)$-dimensional face $\Gamma \subset Q_q^n$.

Consider the hypergraph whose vertices are the vertices of the hypercube and whose hyperedges are its $(d-1)$-dimensional faces. It follows directly from the definitions that an MDS code with distance d is precisely a transversal of this hypergraph.

As mentioned above (see Example 5.4), when $d = 2$, the characteristic function of an MDS code in Q_q^n is a perfect 2-coloring with quotient matrix

$$\begin{pmatrix} n & n(q-2) \\ 0 & n(q-1) \end{pmatrix}.$$

Its nontrivial eigenvalue $\lambda = -n$ is the smallest eigenvalue of Q_q^n.

The cardinality of an MDS code is determined directly from the definition.

Proposition 17.1 (Singleton bound)**.**
(a) *For every* $C \subseteq Q_q^n$, $|C| \leq q^{n-d_C+1}$.
(b) *A code* C *with minimum distance* d_C *is an* MDS *code if and only if*

$$|C| = q^{n-d_C+1}.$$

Proof. Part (a) follows from the fact that every face of dimension $d_C - 1$ contains at most one codeword, while Q_q^n is partitioned into q^{n-d_C+1} disjoint faces of dimension $d_C - 1$.

(b) If C is an MDS code, then each of these q^{n-d_C+1} faces contains exactly one codeword. Conversely, if $|C| = q^{n-d_C+1}$, then every face of dimension $d_C - 1$, in every direction, must contain a codeword. □

Let Γ be an m-dimensional face of Q_q^n. The *retract* of a set $C \subseteq Q_q^n$ onto Γ is the subset $C[\Gamma] \subseteq Q_q^m$ consisting of all tuples in $\Gamma \cap C$ after deleting the coordinates fixed in Γ. Thus, the characteristic function $\mathbf{1}_{C[\Gamma]}$ is simply the restriction of $\mathbf{1}_C$ to the face Γ.

Let Γ be an m-dimensional face of Q_q^n. The *projection* of a set $C \subseteq Q_q^n$ onto Γ is the subset of Q_q^m obtained by deleting the coordinates fixed in Γ from every tuple of C.

Thus, the projection onto a face is the union of the retracts over all parallel faces of the same direction. A retract of a code is called a *punctured code*, while a projection is called a *shortened code*. The class of MDS codes is closed under both retracts and projections.

Proposition 17.2. *A subset of Q_q^n is an* MDS *code with distance d ($2 \le d \le n-1$) if and only if*

(a) *all of its retracts of dimension at least d are* MDS *codes with distance d; or*

(b) *all of its projections onto faces of a fixed dimension $m \ge n-d+1$ are* MDS *codes with distance $d-n+m$.*

Proof. (a) The definition of an MDS code is equivalent to the statement that every face of dimension at least d has the property that each of its $(d-1)$-dimensional subfaces contains exactly one codeword.

(b) This follows from Proposition 17.1. Under projection onto a face of dimension m, all vertices of each face of dimension $n-m$ are mapped to a single point. If $n-m \le d-1$, then the projection has the same cardinality as the original code, while its minimum distance can decrease by at most $n-m$. Proposition 17.1(a) therefore implies that the minimum distance decreases by exactly $n-m$, and Proposition 17.1(b) shows that the projection is an MDS code.

Conversely, suppose that the projection onto some m-dimensional face is an MDS code with distance $d-n+m$. Then every $(d-1)$-dimensional face containing all directions along which the projection is taken contains a codeword. Since the projection direction is arbitrary, every $(d-1)$-dimensional face of the hypercube contains a codeword. Finally, if the original code contained two codewords at distance $d' < d$, then some projection would have minimum distance smaller than $d-n+m$, contradicting the assumption that the projection is an MDS code. □

Proposition 17.3. *Let $C \subseteq Q_q^n$ be an* MDS *code with minimum distance $d_C \ge 3$. Then*

$$|C| \le q^{q-1} \qquad \textit{and} \qquad n \le q + d_C - 2.$$

Proof. By Proposition 17.2, there exists a projection C' of C onto a face of dimension $m = n - d_C + 3$, whose minimum distance is 3. We have

$$|C'| = |C| = q^{n-d_C+1} = q^{m-2}.$$

By the Hamming bound (see Section 1.3), $|C'|\big(m(q-1)+1\big) \le q^m$. Hence, $q^2 \ge m(q-1)+1$, which implies $m \le q+1$. Therefore, $n \le q + d_C - 2$. □

17.2 n-ary Quasigroups

An *n-ary quasigroup* of order q is a pair consisting of a set of elements (which, without loss of generality, we take to be Q_q) and an n-ary operation

$f : Q_q^n \to Q_q$ such that $f(x) \neq f(y)$ whenever the Hamming distance between x and y is equal to 1. In other words, any choice of n coordinates in the equation $f(x_1, \ldots, x_n) = x_0$ uniquely determines the remaining coordinate. The function f itself is also called an *n-ary quasigroup*.

The notion of an n-ary quasigroup extends the notion of a binary (2-ary) quasigroup introduced above.

Example 17.1. Let $\circ$ be a group operation on the set Q_q. Then the function

$$f(x_1, \ldots, x_n) = x_1 \circ \cdots \circ x_n$$

is an n-ary quasigroup, called an *iterated group*.

It follows immediately from the definition that an n-ary quasigroup defines a perfect coloring of Q_q^n with quotient matrix

$$n(J_q - I_q) = \begin{pmatrix} 0 & n & n & \ldots & n \\ n & 0 & n & \ldots & n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n & n & \ldots & n & 0 \end{pmatrix},$$

whose unique nontrivial eigenvalue is $\lambda = -n$.

Each color class of the coloring defined by an n-ary quasigroup is an MDS code with minimum distance 2. Moreover, the graph of an n-ary quasigroup,

$$\{\bar{x} \in Q_q^{n+1} \mid x_{n+1} = f(x_1, \ldots, x_n)\},$$

is itself an MDS code in Q_q^{n+1}.

The table of values (Cayley table) of an n-ary quasigroup is called a *Latin n-cube*; for $n = 2$, it is simply a *Latin square*.

Remark 17.1. It is natural to generalize the notion of a doubly stochastic matrix to multidimensional arrays. A function $f : Q_q^n \to [0, 1]$ is called a *polystochastic matrix* if the sum of its values over every line (that is, every 1-dimensional face) equals 1. The set of all polystochastic matrices is a multidimensional analogue of the Birkhoff polytope.

It is easy to see that the indicator function of an MDS code with minimum distance 2 is a polystochastic matrix. Such an MDS code is sometimes called a *multidimensional permutation*. Every multidimensional permutation is a vertex of the generalized Birkhoff polytope. However, an analogue of Birkhoff's theorem does not hold: there exist vertices of the generalized Birkhoff polytope that are not multidimensional permutations (see [89, 120]). The description of the vertices of the generalized Birkhoff polytope and the estimation of their number remain open problems.

17.3 Orthogonal Systems of Quasigroups

Any MDS code with minimum distance greater than 2 can be represented as the set of solutions of a system of equations involving m-ary quasigroups [42]. Indeed, consider an MDS code of length n and minimum distance d. By the definition of an MDS code, every face of the hypercube of dimension $n - m = d - 1$ contains exactly one codeword. In particular, the first m coordinates uniquely determine $(n - m)$-dimensional face, and, therefore, the remaining $n - m$ coordinates. Hence, the MDS code is the solution set of the system

$$x_{m+1} = f_1(x_1, \ldots, x_m), \ \ldots, \ x_n = f_{n-m}(x_1, \ldots, x_m). \tag{38}$$

It follows immediately from the definition of an MDS code that the functions $f_1, \ldots, f_{n-m}$ are m-ary quasigroups. Indeed, since all coordinates of an MDS code play symmetric roles, any choice of m coordinates uniquely determines the remaining coordinates by means of a system of the form (38), although in general with different quasigroups.

If the solution set of a system (38) is an MDS code, then the corresponding collection of m-ary quasigroups $f_1, \ldots, f_{n-m}$ is called *orthogonal*. Proposition 17.2(a) implies that every subset of an orthogonal system is again orthogonal.

A pair of Cayley tables (Latin squares) corresponding to binary (2-ary) quasigroups f and g is called *orthogonal* if all pairs

$$\big(f(x_1, x_2),\, g(x_1, x_2)\big), \qquad (x_1, x_2) \in Q_q^2,$$

are distinct. Thus, a system of mutually orthogonal Latin squares (MOLS) is a special case of an orthogonal system of quasigroups. According to the arity m, one speaks of orthogonal Latin squares, orthogonal Latin cubes, or orthogonal Latin hypercubes.

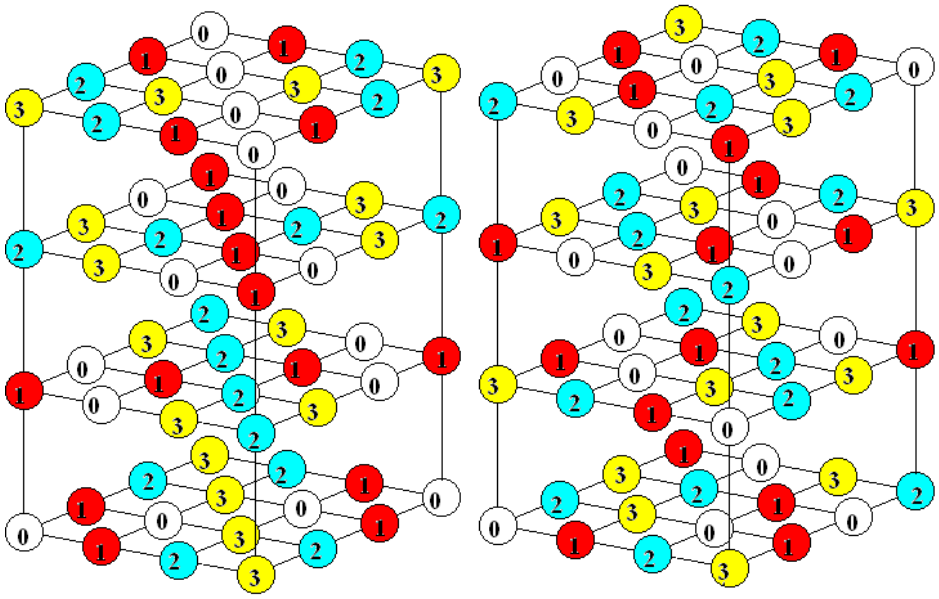
Example 17.2. Mutually orthogonal Latin squares of order 4.

0	**2**	3	1
3	1	0	**2**
1	3	**2**	0
2	0	1	3

0	**2**	3	1
2	0	1	**3**
3	1	**0**	2
1	3	2	0

0	**2**	3	1
1	3	2	**0**
2	0	**1**	3
3	1	0	2

Example 17.3. Orthogonal Latin cubes of order 4.



Proposition 17.4. *If $f_1, \ldots, f_m$ is a system of mutually orthogonal Latin squares (binary quasigroups) of order q, then $m \leq q-1$.*

Proof. It is clear that renaming entries of a Latin square preserves the property of orthogonality. Then, without loss of generality, we may assume that the first rows ($x_1 = 0$) of all Latin squares are identical and that $f_i(0,0) = 0$ for every $i \in \{1, \ldots, m\}$. Consequently, every pair of Latin squares already contains all pairs of the form (a, a) in the first row. Therefore, the values $f_i(1,0)$ must be nonzero and pairwise distinct. Since there are only $q-1$ nonzero elements of Q_q, it follows that $m \leq q-1$. □

The preceding proof immediately implies the following result.

Corollary 17.1. *Let $C \subset Q_q^{q+1}$ be an* MDS *code with minimum distance q. Then C contains no pair of codewords at distance $q+1$, i.e., no pair of codewords differs in every coordinate.*

Proof. Such an MDS code is equivalent to a system of mutually orthogonal Latin squares (see (38)). Since the isometry group of the Hamming graph acts transitively on the vertices, we may assume that $\bar{0} \in C$ and that the first rows of the corresponding Latin squares are identical. The proof of the previous proposition shows that the vertices $(i, \ldots, i)$ do not belong to C, because $(0, i, \ldots, i) \in C$ for every $i \in Q_q$. Hence no codeword of C is at distance $q+1$ from $\bar{0}$. □

Proposition 17.5. *Let $C \subset Q_q^n$ be an* MDS *code with minimum distance d_C, where $n > d_C \geq 3$. Then $d_C \leq q$ and $n \leq 2q - 2$.*

Proof. Let $d_C = m + 1$, where $m \geq 2$. Then the code C corresponds to an orthogonal system of m $(n-m)$-ary quasigroups (see (38)).

By Proposition 17.2, every retract of C of dimension $m+2$ also determines an orthogonal system, namely a system of m mutually orthogonal Latin squares. Proposition 17.4 therefore gives $m \leq q - 1$, which is equivalent to $d_C \leq q$. Finally, Proposition 17.3 yields $n \leq q + d_C - 2 \leq 2q - 2$. □

For $q = 2$, Proposition 17.5 immediately implies the following.

Corollary 17.2. *The Boolean hypercube Q_2^n contains no* MDS *code with minimum distance d satisfying $2 < d < n$.*

Thus, for a fixed alphabet size q, MDS codes of arbitrarily large length exist only for minimum distances 2 and n. MDS codes with minimum distance 2 correspond to Latin hypercubes, whereas an MDS code in Q_q^n with minimum distance n is simply a diagonal of the hypercube.

Since $|Q_q \times Q_p| = qp$, we identify the Cartesian product $Q_q \times Q_p$ with the set Q_{qp}. Let $x \in Q_q$ and $y \in Q_p$; we will consider the pair (x, y) as an element of the set Q_{pq}. The following theorem states that the direct product of MDS codes over alphabets Q_p and Q_q is an MDS code over the alphabet Q_{pq}.

Theorem 17.1 (MacNeish)**.** *If the sets $M_1 \subset Q_q^n$ and $M_2 \subset Q_p^n$ are* MDS *codes with distance d, then the set*

$$M = \{(x, y) = ((x_1, y_1), \ldots, (x_n, y_n)) \mid x \in M_1, y \in M_2\}$$

is also an MDS *code with distance d in Q_{pq}^n.*

Proof. From the condition of the theorem and Proposition 17.1 it follows that $|M| = q^{n-d+1}p^{n-d+1}$. Then M attains the Singleton bound for codes with minimal distance d. It remains to prove that the set M contains no elements at distance less than d. It follows from the inequality

$$d((x, y), (x', y')) = \max\{d(x, x'), d(y, y')\}.$$

□

MacNeish originally formulated this construction for systems of mutually orthogonal Latin squares.

Remark 17.2. Keevash [71] proved that for any fixed $n \in \mathbb{N}$ and code distance $d \leq n$, there exists $q_0 \in \mathbb{N}$ such that for $q \geq q_0$, the hypercube Q_q^n contains an MDS code with distance d.

As mentioned above, the case $d = n-1$ corresponds to the system of $n-2$ MOLS. In this particular case, Keevash's result means that for any k there exists $q_0(k) \in \mathbb{N}$ such that for $q \geq q_0(k)$ there is a system of k orthogonal Latin squares of order q. Bose, Shrikhande and Parker [17] proved that $q_0(2) = 7$, more precisely, for any $q \neq 2, 6$ there exists a pair of orthogonal Latin squares. We will prove this theorem in the next section.

17.4 Systems of mutually orthogonal Latin squares

Let K be an abelian group of order q. Consider permutations $\pi_1, \ldots, \pi_k$ of K satisfying the condition that, for every $i \neq j$, the pointwise difference

$$(\pi_i - \pi_j)(x) = \pi_i(x) - \pi_j(x)$$

is also a permutation of K.

Proposition 17.6. *The functions $f_i(x, y) = x + \pi_i(y)$, $i = 1, \ldots, k$, form an orthogonal system.*

Proof. It is sufficient to show that, for every $i \neq j$, all q^2 pairs

$$\big(f_i(x, y), f_j(x, y)\big)$$

are distinct. Suppose that

$$f_i(x_1, y_1) = f_i(x_2, y_2), \qquad f_j(x_1, y_1) = f_j(x_2, y_2).$$

Subtracting the two equalities gives

$$(\pi_i - \pi_j)(y_1) = (\pi_i - \pi_j)(y_2).$$

Since $\pi_i - \pi_j$ is a permutation by assumption, we obtain $y_1 = y_2$. Substituting this into $f_i(x_1, y_1) = f_i(x_2, y_1)$ yields $x_1 = x_2$. □

Corollary 17.3. *If $q \neq 2$, $q = p^s$ is a prime power, then there exists a system $f_1, \ldots, f_{q-1}$ of mutually orthogonal 2-quasigroups (Latin squares) of order q.*

Proof. We can identify Q_q with the Galois field $GF(q)$. Consider a set of permutations $\{\pi_i : i \in GF(q)\backslash\{0\}\}$, where $\pi_i(x) = ix$. Obviously, the difference $\pi_i - \pi_j = \pi_{i-j}$ is also a permutation. □

Proposition 17.7. *Let the number k have the following decomposition into prime factors: $k = 2^{\delta_1} 3^{\delta_2} \cdots p_i^{\delta_i} \cdots$. Then there exists a system of $\min\limits_{i,\delta_i \neq 0} (p_i^{\delta_i} - 1)$ mutually orthogonal Latin squares of order k.*

Proof. From Corollary 17.3 we obtain that there exists a system of $p_i^{\delta_i} - 1$ mutually orthogonal Latin squares of order $p_i^{\delta_i}$. By Theorem 17.1 it follows that if there exist systems of m MOLS of orders k_1 and k_2, then there exists a system of m MOLS of order $k_1 k_2$. □

Corollary 17.4. *If $k \not\equiv 2 \mod 4$, then there exists a pair of orthogonal Latin squares of order k.*

Lemma 17.1 ([38])**.** *Suppose there exist pairs of orthogonal Latin squares of orders k_1, $k_1 + 1$, k_3 and three mutually orthogonal Latin squares of order k_2, $k_2 \geq k_3$. Then there exists a pair of orthogonal Latin squares of order $k_1 k_2 + k_3$.*

Proof. Let $f_i : Q_{k_2}^2 \to Q_{k_2}$, $i = 0, 1, 2$, be three mutually orthogonal Latin squares of order k_2; $g_i : Q_{k_1}^2 \to Q_{k_1}$, $i = 1, 2$, be a pair of orthogonal Latin squares of order k_1; $h_i : (Q_{k_1} \cup \{q\})^2 \to Q_{k_1} \cup \{q\}$, $i = 1, 2$, be a pair of orthogonal Latin squares of order $k_1 + 1$ such that $h_1(q, q) = h_2(q, q) = q$; $t_i : Q_{k_3}^2 \to Q_{k_3}$, $i = 1, 2$, be a pair of orthogonal Latin squares of order k_3.

The alphabet R of cardinality $k_1 k_2 + k_3$ will be represented in the form $(Q_{k_1} \times Q_{k_2}) \cup Q_{k_3}$, where $Q_{k_3} = \{q_0, \ldots, q_{k_3 - 1}\}$. Define a pair of orthogonal Latin squares F_1, F_2 in the alphabet R according to the following rule.

If $x_1, x_2 \in Q_{k_1}$, $y_1, y_2 \in Q_{k_2}$ and $f_0(y_1, y_2) \geq k_3$, then

$$F_i((x_1, y_1), (x_2, y_2)) = (g_i(x_1, x_2), f_i(y_1, y_2)), \qquad i = 1, 2.$$

If $x_1, x_2 \in Q_{k_1}$, $y_1, y_2 \in Q_{k_2}$ and $f_0(y_1, y_2) < k_3$, then when $h_i(x_1, x_2) \neq q$ we define

$$F_i((x_1, y_1), (x_2, y_2)) = (h_i(x_1, x_2), f_i(y_1, y_2)), \qquad i = 1, 2,$$

and when $h_i(x_1, x_2) = q$ we define

$$F_i((x_1, y_1), (x_2, y_2)) = q_j, \qquad \text{where} \quad f_0(y_1, y_2) = j.$$

Note that by definition, $h_1(x_1, x_2)$ and $h_2(x_1, x_2)$ cannot equal q simultaneously.

If $x_1 \in Q_{k_1}$, $y_1 \in Q_{k_2}$ and $q_j \in \{q_0, \ldots, q_{k_3 - 1}\}$, then we define

$$F_i((x_1, y_1), q_j) = (h_i(x_1, q), f_i(y_1, y)), \qquad i = 1, 2, \qquad \text{where} \quad f_0(y_1, y) = j.$$

Symmetrically, if $x_2 \in Q_{k_1}$, $y_2 \in Q_{k_2}$ and $q_j \in \{q_0, \dots, q_{k_3-1}\}$, then we define

$$F_i(q_j, (x_2, y_2)) = (h_i(q, x_2), f_i(y, y_2)), \qquad i = 1, 2, \qquad \text{where} \quad f_0(y, y_2) = j.$$

For $q_{j_1}, q_{j_2} \in \{q_0, \dots, q_{k_3-1}\}$, we define $F_i(q_{j_1}, q_{j_2}) = t_i(q_{j_1}, q_{j_2})$, $i = 1, 2$.

It suffices to check that F_1 and F_2 are Latin squares in the alphabet R and for any pair $(a, b) \in R$ there exists a pair $u, v \in R$ such that $a = F_1(u, v)$, $b = F_2(u, v)$.

Let us verify that the row of F_i does not contain two equal elements. Since f_0 is a quasigroup, there is at most one $q_j \in Q_{k_3}$ in a row. Equalities $(g_i(x_1', x_2), f_i(y_1', y_2)) = (g_i(x_1, x_2), f_i(y_1, y_2))$ or $(h_i(x_1', x_2), f_i(y_1', y_2)) = (h_i(x_1, x_2), f_i(y_1, y_2))$ imply $x_1' = x_1$ and $y_1' = y_1$ since g_i, h_i and f_i are quasigroups. If $(g_i(x_1', x_2), f_i(y_1', y_2)) = (h_i(x_1, x_2), f_i(y_1, y_2))$ then $y_1' = y_1$. Therefore, the row contains only one type element, either $(g_i(x_1', x_2), f_i(y_1, y_2))$ or $(h_i(x_1, x_2), f_i(y_1, y_2))$ depending on whether $f_0(y_1, y_2) \geq k_3$.

Let $a = (x_3, y_3)$ and $b = (x_4, y_4)$, where $x_3, x_4 \in Q_{k_1}$, $y_3, y_4 \in Q_{k_2}$. There exist $y_1, y_2 \in Q_{k_2}$ such that $f_1(y_1, y_2) = y_3$ and $f_2(y_1, y_2) = y_4$. Let $f_0(y_1, y_2) \geq k_3$, there exist $x_1, x_2 \in Q_{k_1}$ such that $g_1(x_1, x_2) = x_3$, $g_2(x_1, x_2) = x_4$. Then $u = (x_1, y_1)$, $v = (x_2, y_2)$. Let $f_0(y_1, y_2) < k_3$, either there exist $x_1, x_2 \in Q_{k_1}$ such that $h_1(x_1, x_2) = x_3$, $h_2(x_1, x_2) = x_4$ and then $u = (x_1, y_1)$, $v = (x_2, y_2)$; or there exists $x_1 \in Q_{k_1}$ such that $h_1(x_1, q) = x_3$, $h_2(x_1, q) = x_4$ and then $u = (x_1, y_1)$, $v = q_j$, where $j = f_0(y_1, y_2)$; or there exists $x_2 \in Q_{k_1}$ such that $h_1(q, x_2) = x_3$, $h_2(q, x_2) = x_4$ and then $u = q_j$, where $j = f_0(y_1, y_2)$, $v = (x_2, y_2)$.

Let $a = (x_3, y_3)$ and $b = q_j$, where $x_3 \in Q_{k_1}$, $y_3 \in Q_{k_2}$, $q_j \in Q_{k_3}$. There exist $y_1, y_2 \in Q_{k_2}$ such that $f_0(y_1, y_2) = j$ and $f_1(y_1, y_2) = y_3$. Let $f_2(y_1, y_2) = y_4$. There exist $x_1, x_2 \in Q_{k_1}$ such that $h_1(x_1, x_2) = x_3$ and $h_2(x_1, x_2) = q$. Then $u = (x_1, y_1)$, $v = (x_2, y_2)$. The case $a = q_j$ and $b = (x_4, y_4)$, where $x_4 \in Q_{k_1}$, $y_4 \in Q_{k_2}$, $q_j \in Q_{k_3}$, can be considered analogously.

If $a, b \in Q_{k_3}$, then the required follows from the orthogonality of the Latin squares t_1 and t_2. □

Note that in Lemma 17.1 one can take $k_3 = 1$.

Lemma 17.2 ([38]). *For $k \equiv 1 \mod 4$, $k \geq 5$, there exists a triple of mutually orthogonal Latin squares of order k.*

Proof. If k is not divisible by 3, then a triple of mutually orthogonal Latin squares of order k exists by Proposition 17.7.

Let $k = 4t + 1 = 3p$. Then t is not divisible by 3. If $t = 2$ or $t = 4$, then the required follows from Proposition 17.7. If $t = 2^\delta$, $\delta \geq 3$, or all divisors

of t are at least 5, then there exists a system of 4 mutually orthogonal Latin squares f_0, f_1, f_2, f_3 of order t by Proposition 17.7. Let g_1, g_2, g_3 and h_1, h_2, h_3 be triples of mutually orthogonal Latin squares of orders 4 and 5, respectively. From the proof of Lemma 17.1 ($k_1 = 4$, $k_2 = t$, $k_3 = 1$) it is clear that one can obtain three pairs F_1, F_2, F_2, F_3 and F_1, F_3 of orthogonal Latin squares of order k, using the triple f_0, f_i, f_j, and two pairs g_i, g_j and h_i, h_j, where $i, j \in \{1, 2, 3\}$. Thus, a triple F_1, F_2, F_3 of mutually orthogonal Latin squares of order k is obtained. □

Theorem 17.2 (Bose, Shrikhande and Parker, [17]). *For $k \neq 2, 6, 10, 14$, there exists a pair of orthogonal Latin squares of order k.*

Proof. By Corollary 17.4, it remains to investigate the case $k \equiv 2 \mod 4$. Three cases $k \equiv 2, 6, 10 \mod 12$ are possible. Then $k = 3(4t + 1) + 11$, $k = 3(4t + 1) + 3$, or $k = 3(4t + 1) + 7$. From Lemmas 17.1 and 17.2 we obtain the required statement for $k_1 = 3$, $k_2 = 4t + 1$, and $k_3 = 11, 3, 7$, with the exception of the cases $k = 2, 6, 10, 14, 22, 26, 38$. For $k = 22$ and $k = 26$, one can apply Lemma 17.1 with $k_1 = 3$, $k_2 = 7$, $k_3 = 1$ and $k_3 = 5$. For $k = 38$, one can apply Lemma 17.1 with $k_1 = 7$, $k_2 = 5$, and $k_3 = 3$. □

Pairs of orthogonal Latin squares of orders 2 and 6 do not exist. Pairs of orthogonal Latin squares of orders 10 and 14 have been constructed by computer search. In [70], pairs of orthogonal cubes of all orders k, with the exception of $k = 3$ and $k \equiv 2 \mod 4$, have been constructed. The existence of a triple of mutually orthogonal Latin squares of order 10 and of a pair of orthogonal Latin cubes of order 10 remain open problems.

An *affine plane* is a system of points and lines satisfying the following properties.

1) Any two distinct points lie on a unique line.

2) Given any line and any point not on that line there is a unique line which contains the point and does not meet the given line.

3) There exist four points such that no three are collinear (points not on a single line).

It can be shown that in a finite affine plane, each line contains the same number of points k, called the *order* of the plane. Moreover, all lines are partitioned into $k + 1$ classes of k parallel lines each. Thus, an affine plane contains k^2 points.

Proposition 17.8. *Affine planes of order k correspond bijectively to* MDS *codes in Q_k^{k+1} with distance k (systems of $k - 1$ mutually orthogonal Latin squares of order k).*

Proof. Suppose an MDS code $C \subset Q_k^{k+1}$ with minimum distance k is given. We call the elements of the code points, and we take as lines the intersections of the MDS code C with hyperplanes. The property 1) is satisfied by Corollary 17.1. Properties 2) and 3) hold by the construction. Let us prove that an affine plane generates an MDS code. Enumerate k lines of each parallel class with the numbers $0, \ldots, k-1$. To each point we associate a tuple from Q_k^{k+1}, where in the i-th place is the number of the line from the i-th class to which this point belongs. By construction, the resulting set has cardinality k^2, and from property 1) it follows that the distances between points are k. Indeed, if two tuples coincide in two positions then there exist two lines containing both points. The resulting subset of the hypercube is an MDS code by Proposition 17.1 (b). □

No system of $k-1$ mutually orthogonal Latin squares of order k is known when k is not a prime power. The conjecture that such systems, and consequently, affine planes of order not equal to a prime power, do not exist is one of the classical problems of combinatorics.

Recall that a strongly regular graph is a distance-regular graph of diameter 2 (if $k \neq v-1$) with parameters $(b_0, b_1; c_1, c_2) = (k, k-\lambda-1; 1, \mu)$.

Let $C \subset Q_q^n$ be some code with code distance d. Consider the minimum distance graph $G(C)$, whose vertices are the vertices of the code C, and two vertices are joined by an edge if the Hamming distance between them equals d.

Proposition 17.9. *If $C \subset Q_q^n$ is an* MDS *code with distance $n-1$, then $G(C)$ is a strongly regular graph.*

Proof. Since an MDS code with distance $n-1$ in Q_q^n is defined by a system of $n-2$ mutually orthogonal Latin squares, by Proposition 17.4 we have $n \leq q+1$. From Corollary 17.1 it follows that for $n = q+1$, the graph $G(C)$ is complete. We further assume that $n \leq q$. $G(C)$ is a k-regular graph, where $k = n(q-1)$. Indeed, every codeword u belongs to n hyperplanes and every hyperplane contains q codewords. The intersection of two hyperplanes with different directions is a face of dimension $n-2$. Then this intersection contains only the codeword u.

If two vertices of the MDS code are at distance $n-1$, then their common neighbors are all the vertices lying in the $(n-1)$-dimensional face common to them. Then $\lambda = \frac{|C|}{q} - 2 = q-2$. Suppose two vertices $u, v \in C$ are at distance n. Let $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ with $d(u,v) = n$. A common neighbor must agree with u in exactly one coordinate and with v in exactly one different coordinate. There are $n(n-1)$ ordered choices of

these coordinates. The intersection of any two $(n-1)$-dimensional faces of different directions is a face of dimension $n-2$. By the definition of an MDS code, any $(n-2)$-dimensional face of the hypercube contains exactly one code vertex. Then μ equals the number of pairs of such $(n-1)$-dimensional faces, i.e., $\mu = n(n-1)$. □

Every Latin square of order q corresponds to an MDS code with distance 2 in Q_q^3. Moreover, every system of $n-2$ orthogonal Latin squares of order q defines an MDS code with distance $n-1$ in the hypercube Q_q^n. Consequently, every Latin square and every system of MOLS correspond to a strongly regular graph via the minimum-distance graph of the corresponding MDS code.

17.5 Transversals of Latin Hypercubes

A *transversal* of a Latin hypercube (and, in particular, of a Latin square) is a diagonal of the hypercube whose entries are pairwise distinct.

It follows immediately that a Latin square admits an orthogonal Latin square if and only if it can be partitioned into transversals. For Latin hypercubes, however, the situation is different: a necessary condition for the existence of an orthogonal Latin hypercube is that every two-dimensional face (that is, every Latin square contained in the hypercube) can be partitioned into transversals. A partition of the entire hypercube into transversals is not sufficient.

Proposition 17.10. *If q and n are even, then the Latin hypercube defined by the equality $f(x_1, \ldots, x_n) = x_1 + \cdots + x_n \mod q$ has no transversals.*

Proof. We have $\sum_{j=0}^{q-1} j = \frac{q(q-1)}{2} \mod q$. Suppose the Latin hypercube contains a transversal $y^0, y^1, \ldots, y^{q-1} \in Q_q^n$. Then

$$\sum_{i=1}^{n} \sum_{j=0}^{q-1} y_i^j = \sum_{i=1}^{n} \frac{q(q-1)}{2} = q\frac{n(q-1)}{2} = 0 \mod q.$$

While

$$\sum_{j=0}^{q-1} f(y^j) = \sum_{j=0}^{q-1} j = \frac{q(q-1)}{2} = \frac{q}{2} \mod q,$$

which is nonzero because q is even. We obtain a contradiction with the equality that defines the Latin hypercube. □

Remark 17.3. Ryser's well-known conjecture states that any Latin square of odd order has a transversal. By Proposition 17.10 it is clear that not all Latin squares of even order contain a transversal. However, one can ask the question of the existence in Latin squares of a partial transversal of the greatest possible length. Montgomery [109] proved that Latin squares of sufficiently large even order q contain a partial transversal of length $q-1$. For Cayley tables of groups, a criterion of the existence of transversals is known. Hall and Paige conjectured that the Cayley table of a finite group has transversals if and only if its Sylow 2-subgroups are trivial or noncyclic. This conjecture has now been proved (see [21]).

Wanless [155] generalized Ryser's conjecture to Latin hypercubes of odd orders. It is true for orders 1, 3 and 5 (see [115]). Taranenko [138] proved that for order 4 and every even n there is only one Latin n-cube without transversal, up to equivalence. This is described in Proposition 17.10. |

17.6 Linear MDS Codes

Further, we construct linear MDS codes over the Galois field $GF(q)$, where q is a prime power. The hypercube Q_q^n will now be considered as an n-dimensional vector space over $GF(q)$. In this sense, the concepts of linearity, affine hull, dimension, etc., apply to subsets of the hypercube. Recall that the rank of a code is the dimension of its affine hull.

By Proposition 17.1 the rank of a linear MDS code $C \subset Q_q^n$ with minimum distance d equals $r = n - d + 1$. From Proposition 17.3 we note that the rank of a linear MDS code with distance greater than 2 does not exceed $q-1$.

We will use the representation of a linear MDS code in the form of the solution of a system of linear equations $C = \{x \in Q_q^n \mid Ax = \bar{0}\}$. Recall that the matrix A is called a parity-check matrix for the code C. Without loss of generality we admit that the parity-check $r \times n$ matrix A has rank r.

Proposition 17.11. *A linear code C with parity-check $r \times n$ matrix A is an* MDS *code of rank $n-r$ with minimum distance $d = r+1$ if and only if any r columns of the matrix $A = \{a_{ij}\}$ form a nonsingular matrix.*

Proof. Any linear code is the solution set of a system of linear equations. It suffices to note that any face of dimension r in the hypercube contains exactly one codeword of the code C if and only if the corresponding minor in the matrix A is non-zero, i.e., any set of r columns of the matrix A is a linearly independent basis. Indeed, fix $n-r$ coordinates. The remaining r

coordinates satisfy an $r \times r$ linear system. There is a unique solution if and only if the corresponding submatrix is nonsingular. $\square$

The code $C^{\perp} = \{x \in Q_q^n : \sum_i x_i y_i = 0 \text{ for all } y \in C\}$ is called *dual* to C. Obviously, code $C^{\perp}$ is linear. A linear code and its dual code are MDS codes at the same time. In Section 11.1 we considered dual codes over rings $\mathbb{Z}_q$. These notions of duality coincide in the case of prime q.

Proposition 17.12. *If $C \subset Q_q^n$ be a linear* MDS *code of rank $n - r$, then $C^{\perp}$ is a linear* MDS *code of rank r.*

Proof. Let $C = \{x \in Q_q^n \mid Ax = \bar{0}\}$, where A is an $r \times n$ matrix and the linear combinations of the rows of the matrix A form the code $C^{\perp}$. Consider some set consisting of r coordinates. The submatrix of A consisting of these r columns forms a nonsingular square matrix by Proposition 17.11. Without loss of generality we can take the first r coordinates. Consider an arbitrary $u \in Q_q^r$. There is a unique linear combination w of rows of A such that the first r coordinates of w coincide with u. Then there is a unique codeword from $C^{\perp}$ in every $(n-r)$-dimensional face. Thus, the set $C^{\perp}$ is a linear MDS code of rank r. $\square$

Corollary 17.5. *Linear* MDS *codes in Q_q^n with distances d and $n - d + 2$ exist simultaneously.*

Proposition 17.13. *If $q = p^s$ is a prime power, then in Q_q^{q+1} there exist linear* MDS *codes with distance d, for any d, $3 \leq d \leq q$.*

Proof. The matrix $V_r = \begin{pmatrix} 0 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 0 & 1 & 2 & \ldots & q-1 \\ 0 & 0 & 1 & 2^2 & \ldots & (q-1)^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 0 & 1 & 2^{r-1} & \ldots & (q-1)^{r-1} \end{pmatrix}$ satisfies the conditions of Proposition 17.11 for $r < q$, since all its minors of order r are non-zero. More precisely, any r of the last $q-1$ columns of the matrix constitute a Vandermonde determinant, and other sets of r columns can be expressed by Vandermonde determinant of smaller order. $\square$

Proposition 17.14. *Let $q = 2^t$, $t \geq 2$, $n = q + 2$. There exists a linear* MDS *code $C \subset Q_q^n$ of rank $n - 3$.*

Proof. Note that $a^2-b^2=(a-b)^2$ in $GF(2^t)$, i.e., $a^2\neq b^2$ for $a\neq b$. It is easy to check that all minors of dimension 3 of the matrix $\begin{pmatrix} 1 & 0 & 0 & 1 & \dots & 1 \\ 0 & 1 & 0 & 2 & \dots & q-1 \\ 0 & 0 & 1 & 2^2 & \dots & (q-1)^2 \end{pmatrix}$ are non-zero. Then the proposition follows from Proposition 17.11. □

The MDS codes proposed in Proposition 17.14 are called *Asturian codes*.

Remark 17.4. Ball [9] proved that if q is prime, then the length of a linear MDS code does not exceed $q+1$ (when $q=2^t$, $t>1$, the length of a linear MDS code does not exceed $q+2$), except for the cases when the code distance equals 2 or the length of the code.

Ball's result strengthens Proposition 17.5 for linear codes. A well-known MDS conjecture states that the same statement holds for arbitrary MDS codes when $q\neq 2^t$. In particular, Bespalov [13] proved that for odd q there do not exist MDS codes of length $q+2$ or more with minimum distance 4.

Let α be a primitive element in the field $GF(q)$. Consider the matrix

$$RS=\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(q-2)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^r & \alpha^{2r} & \dots & \alpha^{r(q-2)} \end{pmatrix}.$$

Every set of $r+1$ ($r<q-2$) columns of the matrix RS constitutes a Vandermonde matrix. By Proposition 17.11, the matrix RS is a parity-check matrix of an MDS code. It is easy to see that this code is *cyclic*, i.e., words of the form $(y_1,y_2,\dots,y_n)$ and $(y_2,\dots,y_n,y_1)$ are either both contained or both not contained in the code. The MDS code with parity-check matrix RS is called the *Reed–Solomon code*.

The main results of this section were generalized to Galois rings in [40].

17.7 Applications of MDS Codes

MDS codes have numerous applications in information processing.

Consider first the transmission of information over a communication channel with erasures. During transmission, a message $(a_1,a_2,\dots,a_n)$ may be transformed into a word of the form $(a_1,*,a_3,\dots,*,\dots,a_n)$, where the symbol $*$ denotes an erased letter. If the transmitted words are codewords of an MDS code with minimum distance d, then up to $d-1$ erased symbols can be recovered. In fact, every code with minimum distance d allows the recovery of $d-1$ erasures, since every face of dimension less than d contains

at most one codeword. What distinguishes MDS codes is that every face of dimension $d-1$ contains exactly one codeword.

MDS codes are also widely used in distributed storage systems. Suppose that information is stored across n servers and that it must be possible to recover the entire file after the failure of fewer than d servers. This can be achieved by representing the information as codewords of an MDS code with minimum distance d, storing the i-th coordinate of each codeword on the i-th server. The failure of $d-1$ servers is then equivalent to the erasure of $d-1$ coordinates, from which the original information can be recovered uniquely.

Another important application of MDS codes is secret sharing. Suppose there are $n-1$ participants. The goal is to distribute shares of a secret key so that any m participants together can reconstruct the key, whereas any group of at most $m-1$ participants has no information about it.

Assume there exists an MDS code of length n with minimum distance $n-m+1$. The code itself is assumed to be public. Let $(a_1, a_2, \ldots, a_n)$ be an arbitrary codeword. The value $a_i \in Q_q$ is assigned as the private share of the i-th participant, while $a_n \in Q_q$ is taken as the secret key. Since any m coordinates uniquely determine the remaining ones, every group of m participants can reconstruct the entire codeword, and hence the secret key a_n, by solving a system of the form (38). On the other hand, any group of only $m-1$ participants knows the values of only $m-1$ variables. Consequently, the m-ary quasigroup

$$f_{n-m}(x_1, \ldots, x_m) = x_n$$

takes each value of Q_q exactly once as the remaining unknown variable ranges over Q_q. Therefore, every possible value of the secret key is equally likely, and the participants obtain no information about it.

Reed–Solomon codes over the field $GF(2^t)$ are especially useful for applications. These codes are widely used as error-correcting codes. In particular, for $t = 8$, the elements of the alphabet are bytes. The Reed–Solomon code with length $2^t - 1$ and minimum distance $r+1$ can correct up to $r/2$ errors, i.e., corrupted binary blocks of length t. The Reed–Solomon code is used in RAM controllers, when writing information to hard drives, and on CD/DVD disks.

17.8 Problems

140. Prove that if a Latin parallelepiped of size $q \times q \times (q-1)$ is filled with elements of Q_q such that in each line no element occurs twice, then this

parallelepiped can be completed to a Latin cube.

141. Prove that for every $n \geq 2$, there is, up to isometry of Q_3^n, exactly one MDS code with distance 2.

142. Prove that every Latin n-cube of order 3 has transversals.

143. Prove that if there exists a pair of orthogonal Latin hypercubes in a q-ary alphabet, then their dimensions do not exceed $q-1$.

144. Prove that a set of $q-2$ mutually orthogonal Latin squares of order q can always be completed to a set of $q-1$ mutually orthogonal Latin squares of order q.

145 ([119])**.** Prove that every partial Latin n-cube of order q, can be completed to a Latin n-cube of order not greater than q^n.

146. Prove that an MDS code with distance 3 is a completely regular code in Q_q^n, more precisely the first cell of a perfect 3-coloring with parameters $\begin{pmatrix} 0 & n(q-1) & 0 \\ 1 & (n-2)(n-1)+q-2 & (n-1)(q-n+1) \\ 0 & n(n-1) & n(q-n) \end{pmatrix}$.

147. Let an $r \times n-r$ matrix A have only non-zero minors of all sizes over the field $GF(q)$. Prove that the matrix $(I_r|A)$ of size $r \times n$ is a parity-check matrix of an MDS code.

148. Represent the matrix V_r from Proposition 17.13 in the form $V_r = (B|A)$, where B is of size $r \times r$. Prove that the matrix $B^{-1}A$ does not contain any zero minors of any orders.

149. Let $a_1, \ldots, a_n, b_1 \ldots, b_n$ be pairwise distinct elements of the field $GF(q)$. Prove that the Cauchy matrix C, where $c_{ij} = \frac{1}{a_i - b_j}$, has no zero minors of any orders.

150. Let $C \subset Q_q^n$ and suppose each ball of radius ρ contains no more than L elements of C. Prove that $|C| \leq Lq^{n-\lfloor \frac{(L+1)\rho}{L} \rfloor}$ (the generalized Singleton bound).

18 Combinatorial t-Designs

18.1 Designs as Perfect Colorings of Graphs and Hypergraphs

Recall that the Johnson graph $J(n,k)$ is the graph whose vertices are all binary tuples of length n and weight k. Two vertices of the graph are joined

by an edge if the Hamming distance between the corresponding binary tuples is two. Thus, the adjacency matrix of the Johnson graph is a submatrix of the distance-2 matrix in the Boolean hypercube. The vertices of the Johnson graph $J(n,k)$ can be viewed as points of the integer simplex $\{(x_1,\ldots,x_k) \mid x_i \in \mathbb{N}, \sum_{i=1}^{k} x_i \leq n\}$, where $\sum_{i=1}^{j} x_i$ is the index of the coordinate containing the j-th one of the binary tuple.

A *combinatorial design* (more precisely, a t-design) with parameters t-(n,k,λ) is a collection k-element subsets (blocks) of an n-element set, such that any t-element subset is contained in exactly λ blocks.

The blocks of a design with parameters t-(n,k,λ) can be considered as vertices of the graph $J(n,k)$. A combinatorial t-design is conveniently represented as a list of blocks. A block can be specified by the indices of the elements of the block or by the characteristic function of the block, i.e., as a Boolean vector of length n and weight k. A detailed survey of the theory of combinatorial designs can be found in [65].

Example 18.1. Table of blocks of a design with parameters 2-(13,4,1).

2	3	5	11
3	4	6	12
4	5	7	13
1	5	6	8
2	6	7	9
3	7	8	10
4	8	9	11
5	9	10	12
6	10	11	13
1	7	11	12
2	8	12	13
1	3	9	13
1	2	4	10

Proposition 18.1. *The characteristic function of a design D with parameters $(k-1)$-(n,k,λ) is a perfect coloring of the graph $J(n,k)$ with quotient matrix* $S = \begin{pmatrix} k(\lambda-1) & k(n-k-\lambda+1) \\ k\lambda & k(n-k-\lambda) \end{pmatrix}$.

Proof. Two blocks $u, v \in V(J(n,k))$ are adjacent if and only if their intersection contains $(k-1)$ elements. Any $(k-1)$-element set is contained in λ blocks of the design D. Consequently, a block $u \in D$ is adjacent to $\lambda - 1$ vertices $v \in D$ that intersect it in some $(k-1)$-element set. Meanwhile, a k-element block $u \notin D$ has λ adjacent vertices $v \in D$ that intersect it in a fixed

$(k-1)$-element set. Since $u \in D$ includes exactly k subsets of cardinality $k-1$, we have $s_{11} = k(\lambda-1)$ and $s_{21} = k\lambda$. The degree of the graph $J(n,k)$ is $k(n-k)$. Hence, we have $s_{12} = k(n-k-\lambda+1)$ and $s_{22} = k(n-k-\lambda)$. $\square$

For $\lambda = 1$, combinatorial designs with parameters t-(n,k,λ) are usually denoted $S(t,k,n)$, and for $t = k-1$ they are additionally called *Steiner systems* (for $k = 3$, *Steiner triple systems*) of order n.

For $\lambda = 1$, a combinatorial design with parameters t-$(n,k,1)$ can be regarded as a transversal in the hypergraph $G_{n,k,t}$, whose vertices are all possible k-element blocks, and hyperedges are the sets of blocks containing a fixed t-element set.

In the case $t = k-1$, the multigraph $\mathcal{M}_{12}(\mathcal{D}(G_{n,k,t}))$ of vertex adjacency corresponding to hypergraph $G_{n,k,t}$ coincides with the graph $J(n,k)$ after removing all loops.

As a special case of Proposition 18.1 with $\lambda = 1$ (see also Problem 126 and Proposition 3.2 on the Delsarte–Hoffman bound) we have the following corollary.

Corollary 18.1. *Every Steiner system $S(k-1,k,n)$ is a maximum independent sets of $J(n,k)$.*

Define the multigraph $(J(n,k))_{k-t}$ as follows. We take the vertices of the Johnson graph $J(n,k)$; two k-blocks u and v are adjacent if the distance between u and v does not exceed $k-t$ in $J(n,k)$ and the multiplicity of the edge equals the number of common t-subsets of u and v. $(J(n,k))_{k-t}$ is the same as $\mathcal{M}_{12}(\mathcal{D}(G_{n,k,t}))$ (see Section 15.1) without loops.

Proposition 18.2 ([118])**.** *The characteristic function of a design D with parameters t-(n,k,λ) is a perfect coloring of the multigraph $(J(n,k))_{k-t}$ with quotient matrix $S = \begin{pmatrix} \binom{k}{t}(\lambda-1) & \binom{k}{t}(\binom{n-k}{k-t} - \lambda + 1) \\ \binom{k}{t}\lambda & \binom{k}{t}(\binom{n-k}{k-t} - \lambda) \end{pmatrix}$ and the design D is a maximum independent set in $(J(n,k))_{k-t}$ if $\lambda = 1$.*

Proof. We show that if $\lambda = 1$ then the design D is a maximum independent set. Consider the hypergraph $G_{n,k,t}$. The vertices of the graph $(J(n,k))_{k-t}$ are joined by an edge if and only if they are contained in some edge of the hypergraph $G_{n,k,t}$. An independent set in $(J(n,k))_{k-t}$ intersects an edge of the hypergraph in at most one element, therefore its cardinality is not greater than the cardinality of a transversal of the hypergraph. Since the design D is a transversal in $G_{n,k,t}$, it is a maximum independent set in $(J(n,k))_{k-t}$. The proof that the characteristic function of the design D with

parameters t-(n,k,λ) is a perfect 2-coloring of the multigraph $(J(n,k))_{k-t}$ is identical to Proposition 18.1, replacing k $(k-1)$-subsets of a block by its $\binom{k}{t}$ t-subsets. □

The converse is also true: the first cell of a equitable partition of the multigraph $(J(n,k))_{k-t}$ with quotient matrix S is a t-(n,k,λ) design. Let us prove this in the particular case $\lambda = 1$.

Proposition 18.3 ([118]). *A set D is a design with parameters t-$(n,k,1)$ if and only if its characteristic function is a perfect coloring of the multigraph $(J(n,k))_{k-t}$ with quotient matrix* $S = \begin{pmatrix} 0 & \binom{k}{t}\binom{n-k}{k-t} \\ \binom{k}{t} & \binom{k}{t}(\binom{n-k}{k-t}-1) \end{pmatrix}$.

Proof. ($\Rightarrow$) Follows from Propositions 18.2.

($\Leftarrow$) Let D be the first cell in an equitable partition with quotient matrix S. Any t-element set is contained in at most one k-block from D, since $s_{00} = 0$. Consider a k-block $u \notin D$. Every adjacency between u and a block of D arises from one of the $\binom{k}{t}$ t-element subsets of u. Since $s_{10} = \binom{k}{t}$, every one of these t-element subsets belongs to a k-block from D. We conclude that any t-element subset is contained in a k-block from D. □

Note that Proposition 18.3 is essentially a special case of Proposition 15.3.

Remark 18.1. The problem of finding perfect colorings of the Johnson graphs is very complicated. For example, only trivial e-perfect codes in the Johnson graph are currently known. Trivial examples include the entire vertex set ($e = 0$), a single vertex (e is the diameter of the graph), or specific single-element shifts when parameters align trivially. Unlike perfect codes, the existence of t-(n,k,λ) designs has been proven if n is sufficiently large (see Remark 18.2 below).

18.2 Steiner Systems

Recall that a perfect code with minimum distance $2e+1$ or an e-perfect code in a graph is a subset C of the vertices of the graph such that the balls of radius e centered at the codewords are pairwise disjoint and cover all vertices of the graph. e-Perfect codes in hypercubes will be studied in Section 19.4.

Proposition 18.4. *Let C be an e-perfect code in Q_2^n and $\bar{0} \in C$. Then the set $\{u \in C \mid \mathrm{wt}(u) = 2e+1\}$ is an $S(e+1, 2e+1, n)$ design.*

Proof. Consider an arbitrary vertex of weight $e+1$. By the definition of an e-perfect code, it belongs to exactly one ball centered at a point $u \in C$, and $\mathrm{wt}(u) \leq e+1+e = 2e+1$ by the triangle inequality. There are no vertices of weight less than $2e+1$ in the code C, since the balls of radius e centered at such a vertex and at the vertex $\bar{0} \in C$ intersect. Then $\mathrm{wt}(u) = 2e+1$. $\square$

In particular, the set of vertices of weight 3 in a 1-perfect binary code forms a Steiner triple system. The Steiner triple system contained in the Hamming code can be defined as follows: $\{\{x, y, x \oplus y\} \mid x, y \in Q_2^t \setminus \{\bar{0}\}, x \neq y\}$, where the length of the Hamming code is $2^t - 1$. The indices x and y of the coordinates of vertices in the Boolean n-cube can be viewed as elements of the set $Q_2^t \setminus \{\bar{0}\}$, i.e., the columns of the parity-check matrix of the Hamming code.

Proposition 18.5. *Let D be a combinatorial design with parameters t-(n, k, λ). Then its retract $D' = \{u' \in Q_2^{n-1} \mid (u', 1) \in D\}$ is a combinatorial design with parameters $(t-1)$-$(n-1, k-1, \lambda)$.*

Proof. Consider the blocks of the design D that contain the n-th element. Any $(t-1)$-element subset not containing the n-th element is contained in λ such blocks by the definition of a design. Thus, removing the n-th element from these blocks, we obtain a design with the required parameters. $\square$

The design D' is called a *shortening* of the original design D.

Proposition 18.6. *If a combinatorial design with parameters t-(n, k, λ) exists, then the numbers $\lambda\binom{n-i}{t-i}/\binom{k-i}{t-i}$ for $i = 0, \ldots, t-1$ are integers.*

Proof. Let N be the number of blocks in a design with parameters t-(n, k, λ). Consider a bipartite graph, one part of which is the blocks of the design, and the other all possible t-element sets. Join each t-element set by edges to the blocks in which it is contained. From the definition of a design it follows that the number of edges in the graph equals $\lambda\binom{n}{t} = N\binom{k}{t}$. Applying the same counting argument to the shortening obtained by fixing one point yields the corresponding formula for $i = 1$. Repeating this process gives the formulas for all $i = 0, \ldots, t-1$. $\square$

The proof of the following theorem is taking from [124].

Theorem 18.1 (Kirkman)**.** *A Steiner triple system $S(2, 3, n)$ exists if and only if $n \equiv 1 \mod 6$ or $n \equiv 3 \mod 6$.*

Proof. From Proposition 18.6 it follows that a necessary condition for the existence of a Steiner triple system of order n is follows. The number $n(n-1)$ is divisible by 6 and the number $n-1$ is divisible by 2. This condition holds only if $n \equiv 1 \mod 6$ or $n \equiv 3 \mod 6$.

Let us prove the existence of Steiner triple systems for $n \equiv 3 \mod 6$. Note that the number $m = n/3$ is odd. By Theorem 16.10, there exists an idempotent symmetric quasigroup $f : Q_m^2 \to Q_m$ of order m. Consider the n-element set $Q_m \times Q_3$, whose elements we will write in the form xi, where $x \in Q_m$, and $i \in \{0, 1, 2\}$. Define the set S consisting of triples of elements of $Q_m \times Q_3$ of two types
$\{\{x0, x1, x2\} \mid x \in Q_m\}$ and
$\{\{xi, yi, f(x,y)(i+1 \mod 3)\} \mid i \in Q_3, x, y \in Q_m, x \neq y\}$.
Let us check that S is a Steiner triple system. Consider a pair of elements $xi, zj \in Q_m \times Q_3$. If $x = z$, then the pair is contained in a triple of the first type, and if $i = j$ then pair is contained in a triple of the second type. Suppose $x \neq z$ and $i \neq j$. Then $j = i + 1 \mod 3$ or conversely $i = j + 1 \mod 3$ (which does not matter, since the pair $\{xi, zj\}$ is unordered). Without loss of generality, set $j = i + 1 \mod 3$. From the definition of a quasigroup, there exists a unique $y \in Q_m$ such that $z = f(x, y)$; moreover, $y \neq x$ by the idempotence of the quasigroup. Then there is a triple of the second type $\{xi, yi, zj\}$. The triple containing an arbitrary pair of elements is found uniquely; therefore, S is a Steiner system.

Let us prove the existence of Steiner triple systems for $n \equiv 1 \mod 6$. Note that the number $m = (n-1)/3$ is even. By Theorem 16.10, there exists a semi-idempotent symmetric quasigroup $f : Q_m^2 \to Q_m$ of order m. Consider the n-element set $(Q_m \times Q_3) \cup \{\delta\}$, where δ is a special additional symbol. Define three types of triples from the set $(Q_m \times Q_3) \cup \{\delta\}$ which constitute the set S:
$\{\{x0, x1, x2\} \mid x \in Q_{m/2}\}$,
$\{\{xi, yi, f(x,y)(i+1 \mod 3)\} \mid i \in Q_3, x, y \in Q_m, x \neq y\}$ and
$\{\{(x + m/2)i, x(i+1 \mod 3), \delta\} \mid i \in Q_3, x \in Q_{m/2}\}$, Pairs of elements $\{xi, \delta\}$ are contained in triples of the third type. The proof that the remaining pairs of elements, with the exception of pairs
$\{(x + m/2)i, (x + m/2)(i + 1 \mod 3)\}$ and
$\{(x+m/2)i, x(i+1 \mod 3)\}$, $x \in Q_{m/2}$, are covered by triples of the second type is analogous to the previous case $n \equiv 3 \mod 6$. To prove the uniqueness of the covering of pairs, it suffices to show that the pairs $\{(x+m/2)i, x(i+1 \mod 3)\}$, $x \in Q_{m/2}$, are not contained in triples of the second type. While the pairs $\{(x+m/2)i, (x+m/2)(i+1 \mod 3)\}$, $x \in Q_{m/2}$, on the contrary, are contained in triples of the second type. Indeed, $f(x + m/2, y) \neq x$ for

$y \neq x + m/2$, since $f(x + m/2, x + m/2) = x$ by the semi-idempotence of the quasigroup f. However, for any $x \in Q_{m/2}$ there exists $y \neq x + m/2$ such that $f(x + m/2, y) = x + m/2$. □

The constructions of Steiner triple systems used in Theorem 18.1 were devised by Bose [16] and Skolem [132].

Remark 18.2. Hanani [64] proved the existence of Steiner quadruple systems for any n satisfying the necessary conditions $n \equiv 2 \mod 6$ or $n \equiv 4 \mod 6$ (Proposition 18.6). Wilson [159] (for $t = 2$) and Keevash [72] (for arbitrary t) proved that for fixed t, k, λ there exists $n_0 \in \mathbb{N}$ such that a combinatorial design with parameters t-(n, k, λ) exists for $n \geq n_0$ provided the necessary conditions from Proposition 18.6 hold. There is an alternative proof of the last theorem [50].

Let D be a Steiner system $S(2, k, n)$ and $M \subset Q_k^k$ be an MDS code with distance $k - 1$, containing the subcode $\{\underbrace{(i, \ldots, i)}_{k} \mid i = 1, \ldots, k\}$. The code distance $k - 1$ of the MDS code M guarantees that its vectors, with the exception of vectors of the form $(i, \ldots, i)$, do not contain identical symbols. Indeed, if a codeword contains the same symbol twice, then it is at distance at most $k - 2$ from the corresponding constant word. Consequently, every nonconstant codewords is a permutation of Q_k. For every block $\{a_1, \ldots, a_k\} \in D$ and every nonconstant codeword $(\pi_1, \ldots, \pi_k) \in M$, include the ordered k-tuple $(a_{\pi_1}, \ldots, a_{\pi_k})$ in $E[D, M]$.

Proposition 18.7. *The set* $C = E[D, M] \cup \{\underbrace{(i, \ldots, i)}_{k} \mid i = 1, \ldots, n\}$ *is an* MDS *code with minimum distance* $k - 1$ *in the hypercube* Q_n^k.

Proof. The code distance of the set $E[D, M]$ equals $k - 1$. Indeed, since D is a Steiner system, each pair is contained in only one block, consequently, codewords corresponding to distinct blocks are at distance at least $k - 1$. Since M is an MDS code with distance $k - 1$, permutations of the elements of one block differ in at least $k - 1$ positions. Since $E[D, M]$ consists of permutations, the vertices of the form $(i, \ldots, i)$ are at distance $k - 1$ from the vertices of $E[D, M]$. The number of elements in the code equals $n + k(k-1)\binom{n}{2}/\binom{k}{2} = n^2$. By Singleton bound (Proposition 17.1) it follows that C is an MDS code. □

If $k = 3$, one can take the idempotent Latin square of order 3 as M. The MDS codes with distance 2 obtained from a Steiner triple system are graphs

of quasigroups, which are called *totally symmetric*. For $k > 3$, the construction from Proposition 18.7 yields an MDS code equivalent to a system of $k-2$ mutually orthogonal Latin squares.

18.3 Symmetric Designs and Projective Planes

A *projective plane* is a system of points and lines satisfying the following properties.

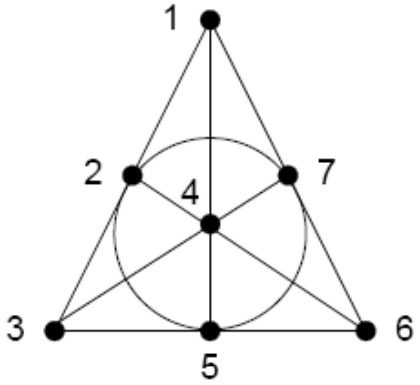
1) Given any two distinct points, there is exactly one line incident with both of them.

2) Given any two distinct lines, there is exactly one point incident with both of them.

3) There are four points such that no line is incident with more than two of them.

It can be shown that in a finite projective plane, each line contains the same number $k+1$ of points, where k is the order of the plane. From the symmetry of points and lines in the definition of a projective plane it follows that through each point there pass $k+1$ lines. In total, a projective plane of order k contains k^2+k+1 points, since each of the $k+1$ lines passing through a fixed point contains k points, besides the fixed point. From properties 1)-2) it follows that all these points are distinct and there are no other points on the plane. Projective planes of order k are Steiner designs $S(2, k+1, k^2+k+1)$, where the points correspond to elements, and the lines to blocks.

Example 18.2. The projective plane of order 2 (Fano plane) contains 7 lines $\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,6\}, \{2,5,7\}, \{3,4,7\}, \{3,5,6\}$.



An affine plane of order k can be obtained from a projective plane of the same order by removing one block and all points of that block from the projective plane. The reverse operation: adding to each line of the affine

plane one point (the same point for parallel lines) and an additional line consisting of all the added points allows one to construct a projective plane from every affine plane of the same order. An affine plane of order k can be viewed as a design $S(2, k, k^2)$.

From the equality $\binom{k^2+k+1}{2} = (k^2+k+1)\binom{k+1}{2}$ it follows that a projective plane contains as many lines, namely k^2+k+1, as points. Any two lines in a projective plane intersect in exactly one point, therefore, by reversing the incidence relation and considering points as blocks and lines as elements of the design, we obtain a design with the same parameters. Projective planes that map to each other under this transformation are called *dual*.

Proposition 18.8. *From any design D of cardinality v with parameters 2-(v, k, λ), after replacing vertices with blocks, i.e., after reversing the incidence relation, one obtains a design with the same parameters.*

Proof. Let M be the incidence matrix of the design $D = \{b_j : j = 1, \ldots, v\}$, i.e.

$$M_{v\times v} = (m_{ij}) = \begin{cases} 1, \text{ if } x_i \in b_j \in D; \\ 0, \text{ otherwise.} \end{cases}$$

From the definition of a design it follows that each column of the matrix M contains k ones. By Proposition 18.5 it follows that each row of the matrix D contains the same number of ones, because all retracts of the design are designs having the same parameters. Since D is a square matrix, its rows also contain k ones. Consider an arbitrary pair of rows; by the definition of a design there are exactly λ columns in which both these rows have ones. Let the numbers a and b satisfy the equation $\lambda a^2+2(k-\lambda)ab+(v-2k-\lambda)b^2 = 0$. Consider the matrix $Q = aM + b(J - M)$, which is obtained from M by replacing 1 with a and 0 with b. From the choice of the numbers a and b it follows that the matrix Q is orthogonal. On the other hand, an arbitrary orthogonal matrix Q whose elements take only two values corresponds to the incidence matrix of some design. It is clear that the matrix Q^{T} corresponds to the design obtained by reversing the incidence relation, and the matrices Q and Q^{T} are orthogonal simultaneously. □

2-Designs in which the number of blocks equals the number of points are called *symmetric*.

In [30], [22] the following conditions for the existence of symmetric 2-designs were proved.

Theorem 18.2 (Bruck, Ryser, Chowla)**.** *Suppose there exists a symmetric* 2-(v, k, λ) *design.*

If v is even, then $k - \lambda = x^2$ for some integer number x.

If v is odd, then there exist integer numbers x, y, and z (not all zero simultaneously) such that the equality holds

$$z^2 = (k - \lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2.$$

This theorem yields an infinite series of arithmetically admissible design parameters for which designs nevertheless do not exist. Note that the statement on the existence of 2-(v, k, λ) with arithmetically admissible parameters [159] becomes true only for sufficiently large v, for fixed k and λ.

Remark 18.3. From the Bruck–Ryser–Chowla theorem one can prove that there do not exist finite projective planes of orders 14, 21, and 22. The non-existence of a projective plane of order 6 follows from the absence of a pair of orthogonal Latin squares of order 6. The non-existence of a projective plane of order 10 was proved by using computer [85]. Exhaustive computer classification [84] showed that for each of the orders 3, 4, 5, 7, and 8 there exists a unique projective plane, corresponding to the complete system of linear orthogonal Latin squares; and for order 9 there are four projective planes, two of which are dual.

18.4 Hadamard Matrices

Consider the matrix $H_{q,n}$ of size $q^n \times q^n$ whose rows are the characters $\phi_z(x)$ of $\mathbb{Z}_q^n$, i.e. $H_{q,n}(z, x) = \phi_z(x)$. From the orthogonality properties of characters (Proposition 9.3) it follows that $H_{q,n}H_{q,n}^* = mI_m$, where $m = q^n$.

Proposition 18.9. *Consider a function $f : Q_q^n \to \mathbb{C}$ as a vector of $\mathbb{V}(\mathbb{Z}_q^n)$. Then $H_{q,n}f = \widehat{f}$.*

Proof follows directly from definitions.

An $m \times m$ matrix H is called a *Hadamard matrix* if it satisfies $HH^{\mathrm{T}} = mI_m$ and consists only of ± 1. Matrices consisting of entries with absolute value 1 and satisfying $HH^* = mI_m$ are called *generalized Hadamard matrices*. If all entries are powers of $\xi = e^{2\pi i/q}$, then the matrix is called *Butson-type* Hadamard matrix.

Obviously, a Hadamard matrix becomes orthogonal (unitary) after multiplying by $\frac{1}{\sqrt{m}}$. From the definitions of the matrices and characters it is clear that the matrices $H_{q,n}$ are symmetric. The $2^n \times 2^n$ matrix $H_{2,n}$ is called the *Hadamard–Sylvester matrix*.

It is clear that permuting the rows or columns of a generalized Hadamard matrix does not take it out of the class of such matrices. Moreover, multiplying a column or a row of a Butson-type Hadamard matrix consisting of powers of $\xi = e^{2\pi i/q}$ by ξ^j does not take the matrix out of this class. Generalized Hadamard matrices obtained from one another by such transformations are called *equivalent*.

Proposition 18.10. *If H_{n_1} and H_{n_2} are generalized Hadamard matrices, then $H_{n_1} \otimes H_{n_2}$ is a generalized Hadamard matrix.*

Proof. $(H_{n_1} \otimes H_{n_2})(H_{n_1} \otimes H_{n_2})^* = (H_{n_1} \otimes H_{n_2})(H_{n_1}^* \otimes H_{n_2}^*) = (H_{n_1} H_{n_1}^*) \otimes (H_{n_2} H_{n_2}^*) = n_1 I_{n_1} \otimes n_2 I_{n_2} = n_1 n_2 I_{n_1 n_2}$. □

Example 18.3. The Hadamard-–Sylvester matrix

$$H_{2,3} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}.$$

Lemma 18.1. *Let $f : Q_q^n \to \mathbb{C}$ be a function. Define the $q^n \times q^n$ matrix A by $A_f(x, y) = f(x - y)$. Then $A_f A_g = A_{f*g}$.*

Proof. We have

$$A_f A_g(x, z) = \sum_{y \in Q_q^n} f(x-y) g(y - z) = \sum_{u \in Q_q^n} f(u) g(x-z-u) = (f*g)(x-z) = A_{f*g}(x, z).$$

□

Proposition 18.11. *A function b is a bent function if and only if $H(x, y) = \xi^{b(x-y)}$ is a generalized Hadamard matrix.*

Proof. We have $H^*(x, y) = \xi^{-b(y-x)} = \xi^{\tilde{b}(x-y)}$. Then from Lemma 18.1 we obtain the equality $HH^*(x, y) = [\xi^b * \xi^{\tilde{b}}](x - y)$. By Proposition 13.1, the equation $HH^* = NI_N$, where $N = q^n$, is equivalent to b being bent. □

For $q = 2$, the matrix $H(x, y) = (-1)^{b(x-y)}$ is a Hadamard matrix.

By multiplying rows and columns by -1, any Hadamard matrix can be transformed so that its first column and first row consist entirely of ones.

Such matrix is called normalized Hadamard matrix. Then in the other rows and columns there will be exactly half of the entries equal to 1 and half equal to -1. Consider the $(4m+3) \times (4m+3)$ matrix A_m obtained from the normalized Hadamard matrix by deleting the first row and the first column and replacing -1 by 0. The rows of the matrix A_m can be regarded as binary vectors of length $4m+3$ and weight $2m+1$.

Proposition 18.12. *The set of rows of the matrix A_m forms a combinatorial design with parameters* 2-$(4m+3, 2m+1, m)$.

Proof. It suffices to verify that for every pair of columns of the matrix A_m there are exactly m rows in which both columns contain a 1. Indeed, in the original Hadamard matrix each column (except the first) contained exactly $2m$ entries equal to 1 and $2m$ entries equal to -1. Then $s(1,1)+s(1,-1) = s(-1,1)+s(-1,-1) = 2m+2$, where $s(\delta_1, \delta_2)$ is the number of pairs (δ_1, δ_2) in the two columns. The orthogonality of the Hadamard matrix implies $s(1,1) + s(-1,-1) = s(1,-1) + s(-1,1)$. Hence $s(1,1) = m+1$. Since the matrix is normalized, every non-first column begins with 1, then by deleting the first row from consideration yields the required result. □

As can be seen from the construction, the number of blocks in a design with parameters $2-(4m+3, 2m+1, m)$ equals the number of points, i.e. $4m+3$. Therefore such a design is symmetric. It is easy to see that if we form a matrix from the blocks of a design with parameters 2-$(4m+3, 2m+1, m)$, replace 0 by -1 in it, and add a row and a column of ones, we obtain a Hadamard matrix. The orthogonality of the columns of the resulting matrix follows from the parameters of the design.

It is not difficult to show that $m \times m$ Hadamard matrices can exist only when m is divisible by 4 (except for orders $m = 1, 2$, which are trivial cases). Indeed, let H be a normalized Hadamard matrix of size $m \times m$. Consider the second and third rows of H as a collection of m pairs. Let x_1 be the number of pairs $(1,1)$, x_2 be the number of pairs $(-1,1)$, x_3 be the number of pairs $(1,-1)$, x_4 be the number of pairs $(-1,-1)$. The orthogonality condition of the first three rows yields the following system of linear equations:

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = m, \\ x_1 + x_2 - x_3 - x_4 = 0, \\ x_1 - x_2 + x_3 - x_4 = 0, \\ x_1 - x_2 - x_3 + x_4 = 0. \end{cases} \tag{39}$$

The matrix of the system (39) is a Hadamard–Sylvester matrix of order 4. The unique solution of (39) is $x_1 = x_2 = x_3 = x_4 = m/4$. Therefore, $m/4$

is an integer. The famous conjecture states that this condition is sufficient for the existence of Hadamard matrices. A detailed survey of the theory of Hadamard matrices is available in [66].

18.5 Problems

151. Prove that designs with parameters t-(n,k,λ) and designs with parameters i-(n,k,λ_i) for $i=1,\ldots,t-1$ and $\lambda_i=\lambda\binom{n-i}{t-i}/\binom{k-i}{t-i}$ determine each other uniquely.

152. Prove that every design with parameters 2-(n,k,λ) generate a design with parameters 2-$(n,n-k,\lambda')$, where $\lambda'=\lambda\binom{n}{2}/\binom{k}{2}-2\lambda\frac{n-1}{k-1}+\lambda$.

153. Prove that a maximum clique in the graph $J(n,k)$ is Delsarte.

154. Prove that a design with parameters $S(k-2,k,n)$ is a completely regular code in the graph $J(n,k)$.

155. In a construction analogous to the construction of the set $E(D,M)$ (see Proposition 18.7), take as D a Steiner quadruple system of order n, and as M the set of even permutations. Prove that the set $E[D,M]\cup\{(i,i,j,j),(i,j,i,j),(i,j,j,i)\mid\ i,j=1,\ldots,n\}$ is an MDS code with minimum distance 3 in the hypercube Q_n^4.

156. Prove that an MDS code in Q_k^{k+1} with distance k does not contain vertices at distance $k+1$. Prove that any such code generates a design with parameters 2-$(k^2,k,1)$.

157. Let M be incidence matrix of a design D with parameters 2-(n,k,λ). Prove the equality $MM^{\mathrm{T}}=\lambda(J_n+\frac{n-k}{k-1}I_n)$.

158. Consider a Hadamard matrix A of order n whose first row and first column consist of 1's. Replace all occurrences of -1's in the matrices A and $-A$ by 0. Prove that the orthogonal array consisting of $2n$ rows of these matrices has strength 2. Prove that if $n=2^k$, then an orthogonal array of strength 2 of smaller cardinality does not exist.

19 Perfect Codes and Tilings

19.1 Tilings of Groups

A *factorization* or *tiling* of a group $(Gr,\circ)$ is a pair (C,B) of subsets $C\subset Gr$ and $B\subset Gr$ such that, for every $x\in Gr$, there exists a unique pair of elements $c\in C$ and $b\in B$ such that $x=c\circ b$, i.e., $Gr=C\circ B$.

If $C \leq Gr$ is a subgroup, then B can be chosen to contain one representative from each coset of C in Gr. It is easy to see that, for a finite group, uniqueness of the representation implies $|Gr| = |C||B|$.

If (C, B) is a tiling, then $(C, B \circ a)$ is also a tiling for every $a \in Gr$. Therefore, we may always assume that the identity element ε of the group belongs to $C \cap B$. In this case, it is clear that $C \cap B = \{\varepsilon\}$.

Proposition 19.1. *A pair (C, B) is a tiling of the group $(Gr, \circ)$ if and only if $(C^{-1} \circ C) \cap (B \circ B^{-1}) = \{\varepsilon\}$ and $|Gr| = |C||B|$.*

Proof. The equality $c_1 \circ b_1 = c_2 \circ b_2$ is equivalent to $c_2^{-1} \circ c_1 = b_2 \circ b_1^{-1}$. Thus, uniqueness of the representation is equivalent to

$$(C^{-1} \circ C) \cap (B \circ B^{-1}) = \{\varepsilon\}.$$

Under this condition, all elements of $C \circ B$ are distinct, and their number is $|C||B| = |Gr|$. Hence every element of Gr has a representation of the form $c \circ b$. □

In the case of an abelian group, this condition takes the more symmetric form

$$(C - C) \cap (B - B) = \{0\}.$$

Let A be the connection set of the Cayley graph $G = \mathrm{Cay}(Gr, A)$. Consider the unit ball $B = A \cup \{\varepsilon\}$. It is easy to see that a subset $C \subset Gr$ is a 1-perfect code in G if and only if (C, B) is a tiling of the group Gr.

Example 19.1. Let $C \subset Q_q^n$ be a Hamming code and let

$$B = \{x \in Q_q^n \mid \mathrm{wt}(x) \leq 1\}$$

be the unit ball. Then (C, B) is a tiling when $n = \frac{q^t - 1}{q - 1}$.

Proposition 19.2. *A pair (C, B) is a tiling of an abelian group K if and only if $\mathbf{1}_C * \mathbf{1}_B = \mathbf{1}$, or, equivalently, $\widehat{\mathbf{1}_C} \cdot \widehat{\mathbf{1}_B} = \frac{\delta}{|K|^{1/2}} = \mathbf{1}_{\{0\}}$.*

Proof. The first equality follows directly from the definition of a tiling. The second follows from Proposition 9.17 and the equality $\widehat{\mathbf{1}} = \delta$. □

As a generalization of tilings of an abelian group K, we can consider pairs of functions (f, g), $f, g : K \to \mathbb{C}$, satisfying

$$f * g = \alpha \mathbf{1}$$

for some $\alpha \in \mathbb{C}$. Similarly to Proposition 19.2, a criterion for a pair (f, g) to be a *multiple tiling* is

$$\mathrm{supp}(\widehat{f}) \cap \mathrm{supp}(\widehat{g}) = \{0\}.$$

A tiling of a group can be used for compact storage of the group. To perform the group operation, its Cayley table is required, which has size $|Gr|^2$. If a tiling (C, B) of Gr is available, it is sufficient to store the multiplication tables of the elements of Gr by the elements of C and by the elements of B, i.e., two tables of sizes $|Gr||C|$ and $|Gr||B|$.

A tiling (C, B) of the group $\mathbb{Z}_2^k$ can be used to construct 1-perfect codes in Q_2^n. We regard the elements of $\mathbb{Z}_2^k$ as binary vectors of length k. Let $\bar{0} \in C$ and $|C| = n + 1$. Taking the nonzero elements of C as columns, construct a matrix H of size $k \times n$.

Proposition 19.3 ([31]). *The union, over all $b \in B$, of the solution sets of the systems $Hx = b$ over $GF(2)$ is a 1-perfect code in Q_2^n.*

Proof. Let $x \in Q_2^n$. We first prove that there is a codeword at distance at most 1 from x. Consider

$$z = x_1 c^1 + \cdots + x_n c^n \in \mathbb{Z}_2^k,$$

where $c^1, \ldots, c^n$ are the columns of H. Since (C, B) is a tiling, there exist $c \in C$ and $b \in B$ such that $z = c + b$. If $c = \bar{0}$, then x is a codeword. Otherwise, c is one of the columns of H, say c^i, and hence $z + c^i = b$.

Therefore, the vector $x + (0 \ldots 0\underset{i}{1}0 \ldots 0)$ is a codeword.

It remains to prove that the distance between distinct codewords is at least 3. Suppose that x and y are two codewords that differ only in positions i and j. Then

$$x_1 c^1 + \cdots + x_n c^n = b^1, \qquad y_1 c^1 + \cdots + y_n c^n = b^2$$

for some $b^1, b^2 \in B$, and hence $c^i + c^j = b^1 + b^2$. Since $c^i, c^j \in C$, this contradicts the definition of a tiling. If x and y differ in only one position, we obtain an analogous contradiction using $\bar{0} \in C$. Thus, the minimum distance of the code is at least 3, and every vector is at distance at most 1 from a codeword. Hence the code is 1-perfect. □

19.2 Tilings of Graphs and the Code-Anticode bound

The notion of a tiling can be extended to vertex-transitive graphs.

A *tiling* of a vertex-transitive graph G is a pair (A, Π), where $A \subset V(G)$ and $\Pi \subset \mathrm{Aut}(G)$, such that

$$V(G) = \bigsqcup_{\varphi \in \Pi} \varphi(A).$$

Clearly, the conditions $|\Pi||A| = |V(G)|$ and

$$\varphi_1(A) \cap \varphi_2(A) = \varnothing \qquad \text{for all } \varphi_1 \neq \varphi_2, \quad \varphi_1, \varphi_2 \in \Pi,$$

are necessary and sufficient for (A, Π) to be a tiling.

Consider a hypergraph Γ whose set of vertices is $V(G)$ and whose hyperedges are $\pi(A)$, where $\pi \in \mathrm{Aut}(G)$. By definition, the set $\{\pi(A) : \pi \in \Pi\}$ is a perfect matching of Γ.

A subset $A \subset V(G)$ whose internal distance does not exceed a given maximum diameter d is called an *anticode*. If G is the Cayley graph of an abelian group K, then we have $|A||C| \leq |K|$ for every code C with minimal distance $d+1$. This inequality is called a *code-anticode bound*. It is easy to see that if the code-anticode bound is attained for C and A then (C, A) is a tiling of K.

The code-anticode bound is generalized to vertex-transitive graphs.

Proposition 19.4. *Let G be a vertex-transitive graph and the internal distance of $A \subset V(G)$ is at most d. Then, for every code $C \subset V(G)$ with minimum distance $d+1$, the bound $|A||C| \leq |V(G)|$ holds.*

Proof. Let $Aut(G)$ cover $V(G)$ $\alpha = |\mathrm{Aut}(G)|/|V(G)|$ times. The proof is based on double-counting the number of pairs (π, c) such that $\pi \in \mathrm{Aut}(G)$, $c \in C$, and $c \in \pi(A)$. On one hand, this number is not greater than $|\mathrm{Aut}(G)|$, but on the other hand, it is equal to $\alpha|C||A|$, because for every pair (c, a) there are α distinct $\pi \in \mathrm{Aut}(G)$ such that $c = \pi(a)$. Consequently, $|\mathrm{Aut}(G)| \geq \alpha|C||A|$. □

It follows from the proof that if the code-anticode bound is reached, then $(A, \mathrm{Aut}(G))$ is a multiple tiling.

19.3 Perfect Codes with Minimum Distance Greater Than 3

A *perfect code with minimum distance* $2e+1$ (an *e-perfect code*) in a graph G is a set $C \subset V(G)$ such that the balls $B(x, e)$ centered at vertices $x \in C$ and of radius e form a partition of the vertices of the graph, i.e.,

$$V(G) = \bigsqcup_{x \in C} B(x, e).$$

A perfect code with minimum distance $2e+1$ in a Cayley graph $G = Cay(Gr, A)$ is equivalent to a tiling $(C, A^e \cup \{\varepsilon\})$, where

$$A^e = \{a_1 \circ \cdots \circ a_k \mid a_i \in A,\ k = 1, \ldots, e\},$$

as well as to a 1-perfect code in the graph $G = Cay(Gr, A^e)$.

In a distance-regular graph with parameters $(b_0, \ldots, b_{d-1}, c_1, \ldots, c_d)$, an e-perfect code C induces a perfect coloring with quotient matrix

$$S_C = \begin{pmatrix} a_0 & b_0 & 0 & 0 & \ldots & 0 \\ c_1 & a_1 & b_1 & 0 & \ldots & 0 \\ 0 & c_2 & a_2 & b_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & 0 & c_e & a_e + b_e \end{pmatrix},$$

where the vertices of the code C are assigned the first color, and the colors of the remaining vertices are determined by their minimum distance from the code vertices.

It is easy to see that a coloring with the quotient matrix S_C is a distance coloring with respect to the code C. Then every e-perfect code is a completely regular code by definition.

Proposition 19.5 (Lloyd's condition)**.** *Let C be an e-perfect code in a distance-regular graph G. Then, for every eigenvalue λ of the matrix S_C, except for $\lambda_0 = \deg G$, we have*

$$1 + P_1(\lambda) + \cdots + P_e(\lambda) = 0,$$

where $P_t(x)$ is the Krawtchouk-type polynomial associated with the graph G (see Section 7.1).

Proof. Let f be the characteristic function of the code C. By the definition of an e-perfect code, we have

$$If + Mf + M_2 f + \cdots + M_e f = \mathbf{1},$$

where $M_i = P_i(M)$ is the distance-i adjacency matrix of the graph G. Let λ_i, $i = 0, \ldots, e$, be the eigenvalues of the quotient matrix S_C.

By Corollary 2.3, there exist suitable coefficients α_i such that

$$f = \sum_{i=0}^{e} \alpha_i \varphi_i,$$

where φ_i is an eigenfunction of the graph G with eigenvalue λ_i.

We show that $\alpha_i \neq 0$ for every $i = 0, \ldots, e$. By Corollary 2.1, for every eigenvalue of the matrix S_C, an eigenfunction of the graph with the same eigenvalue can be obtained as a linear combination of the characteristic functions of the colors. The characteristic function of the color at distance i from the code is $M_i f$. Therefore, all characteristic functions of the colors are linear combinations of the same eigenfunctions of the graph as the first color.

By Proposition 2.8, if $\alpha_i = 0$ for some $i = 0, \ldots, e$, then all characteristic functions of the colors would be orthogonal to the corresponding eigenspace of the matrix M, which is a contradiction.

Thus, by Proposition 7.3,

$$\mathbf{1} = If + Mf + M_2 f + \cdots + M_e f = \sum_{i=0}^{e} \alpha_i \big(1 + P_1(\lambda_i) + \cdots + P_e(\lambda_i)\big)\varphi_i.$$

Since $\mathbf{1}$ is an eigenfunction corresponding to the eigenvalue λ_0, we obtain

$$1 + P_1(\lambda_i) + \cdots + P_e(\lambda_i) = 0, \qquad i = 1, \ldots, e.$$

□

If a distance-regular graph is a Cayley graph of an abelian group, then Lloyd's condition is equivalent to Proposition 19.2. Indeed,

$$\mathbf{1} = If + Mf + M_2 f + \cdots + M_e f = \mathbf{1}_B * f,$$

where $f = \mathbf{1}_C$ and B is the ball of radius e centered at the zero element.

Corollary 19.1. *The matrix S_C has no repeated eigenvalues, and*

$$\det(S_C - xI) = (-1)^{e+1} \left(\prod_{t=1}^{e} c_t \right) (x - \lambda_0) \sum_{t=0}^{e} P_t(x).$$

Proof. Since the matrix $S_C - xI$ is tridiagonal with positive off-diagonal entries, its rank is at least e. Consequently, the matrix S_C has no repeated eigenvalues.

By Lloyd's condition, the polynomials

$$\det(S_C - xI) \quad \text{and} \quad (x - \lambda_0) \sum_{t=0}^{e} P_t(x)$$

have the same roots. By (12), the leading coefficient of the polynomial $P_e(x)$ is

$$\frac{1}{\prod_{t=1}^{e} c_t}.$$

The leading coefficient of the polynomial $\det(S_C - xI)$ is $(-1)^{e+1}$. This proves the stated equality.

□

19.4 Perfect Codes in Hamming Graphs

Proposition 19.6. *Let $C \subset Q_q^n$ be an e-perfect code. Then*

$$(n - \lambda_1) \cdots (n - \lambda_e) = \frac{e! q^n}{|C|},$$

where λ_i, $i = 1, \ldots, e$, are all the eigenvalues of the parameter matrix S_C except for $\lambda_0 = (q-1)n$.

Proof. The degrees of the vertices of the n-dimensional Hamming graph are $(q-1)n$, so $(q-1)n$ is the largest eigenvalue of the matrix S_C. For Hamming graphs, we have $c_i = i$. As was noted in Corollary 19.1, the matrix S_C has no repeated eigenvalues. Therefore,

$$\det(S_C - xI) = (-1)^{e+1}(x - \lambda_0) \cdots (x - \lambda_e).$$

On both sides of the equality

$$\det(S_C - xI) = (-1)^{e+1} e!(x - (q-1)n) \sum_{t=0}^{e} P_t(x),$$

which follows from Corollary 19.1, we cancel the factor $(x - (q-1)n)$. Here $P_t = P_t[n, q]$ are the q-ary Krawtchouk polynomials. By Proposition 7.3, $\sum_{t=0}^{e} P_t(n)$ is the size of a ball of radius e.

Since $C \subset Q_q^n$ is an e-perfect code, the balls of radius e centered at its codewords partition Q_q^n. Hence $|C| \sum_{t=0}^{e} P_t(n) = q^n$. The desired equality follows.

□

Let us consider the Boolean hypercube in more detail.

Proposition 19.7. *Let $A_r \subset Q_2^n$ be the sphere of radius r centered at $\bar{0}$. For any fixed $r \in \mathbb{N}$, and sufficiently large n, we have $\widehat{\mathbf{1}_{A_r}}(z) > 0$ for all z such that $\mathrm{wt}(z) < n/2$.*

Proof. Let $\mathrm{wt}(z) = m$, where m may depend on n. We have

$$2^{n/2}\widehat{\mathbf{1}_{A_r}}(z) = \sum_{\mathrm{wt}(x)=r} (-1)^{\langle x,z\rangle} = \sum_{i=0}^{r} (-1)^i \binom{m}{i}\binom{n-m}{r-i}.$$

If $2mr + m + r \le n$, then

$$\binom{m}{1}\binom{n-m}{r-1} \le \frac{1}{2}\binom{n-m}{r}.$$

Therefore,

$$\sum_{i=0}^{r} (-1)^i \binom{m}{i}\binom{n-m}{r-i} > \frac{1}{2}\binom{n-m}{r}.$$

If $2mr + m + r > n$, then $m \to \infty$ as $n \to \infty$. Applying

$$m(m-1)\cdots(m-i+1) = m^i(1+o(1))$$

as $m \to \infty$, together with the binomial theorem, we obtain

$$\begin{aligned}\sum_{i=0}^{r} (-1)^i \binom{m}{i}\binom{n-m}{r-i} &= \sum_{i=0}^{r} (-1)^i \frac{m^i (n-m)^{r-i}}{i!(r-i)!}(1+o(1)) \\ &= \frac{(n-2m)^r(1+o(1))}{r!}.\end{aligned}$$

Since $m < n/2$, the last expression is positive for sufficiently large n. This proves the proposition.

□

By Proposition 7.3, $2^{n/2}\widehat{\mathbf{1}_{A_r}}(z) = P_r[n,2](\lambda_{\mathrm{wt}(z)})$. Recall that $\lambda_{\mathrm{wt}(z)} = n - 2\mathrm{wt}(z)$. Consequently, for sufficiently large n, the Krawtchouk polynomials $P_r[n,2](x)$ are nonnegative at $x = n, n-2, \ldots, 2$ or at $x = n, n-2, \ldots, 1$. Actually, it is possible to prove that $P_r[n,2](x)$ is nonnegative throughout the interval $x \in [1,n]$ for $n > n_0(r)$.

Remark 19.1. If r grows sufficiently slowly (in particular, if $2^{r/2} \le n$), Proposition 19.7 remains valid. Since $\widehat{\mathbf{1}_{B_r}}(z) > 0$ for $\mathrm{wt}(z) < n/2$ and sufficiently large n, Proposition 19.2 implies that $\widehat{\mathbf{1}_C}(z) = 0$ for $0 < \mathrm{wt}(z) < n/2$, where C is an arbitrary r-perfect code. Thus, the characteristic function $\mathbf{1}_C$ is orthogonal to the eigenspaces of the Hamming graph corresponding to positive eigenvalues (except for n). As follows from the proof of Proposition 19.5 (Lloyd's condition), the decomposition of the characteristic function

$\mathbf{1}_C$ as a linear combination of eigenfunctions contains nonzero components corresponding to every eigenvalue of the matrix S_C. Therefore, the existence of an r-perfect code C implies that S_C has no positive eigenvalues other than n, for sufficiently large n.

1-Perfect linear Hamming codes in Q_q^n were constructed for prime power q and $n = \frac{q^t-1}{q-1}$ (see Proposition 1.3). In addition, in hypercubes Q_q^n of odd dimension $n = 2s+1$, there are perfect codes with maximal distance s, consisting of all vertices of the form $(a, \ldots, a)$, $a \in Q_q$. A one-point set in any graph is formally a perfect code with covering radius equal to (or greater than) the diameter of the graph, but this case is usually not taken into account when listing perfect codes. Next we prove that the number of other parameters of perfect codes in Q_2^n is finite. Our proof follows the book [92].

Theorem 19.1 (Tietäväinen [143], Zinoviev and Leontiev [161]). *There are only finitely many dimensions n for which the binary hypercube Q_2^n contains an e-perfect code with $1 < e < \frac{n-1}{2}$.*

Proof. From Proposition 7.3 and the formula $\lambda_z = n - 2\mathrm{wt}(z)$ for the eigenvalues of the Boolean hypercube, we straightforwardly obtain $P_t[n,2](-n) = P_t(-n) = (-1)^t\binom{n}{t}$ and $P_t(2-n) = (-1)^t\left(\binom{n-1}{t} - \binom{n-1}{t-1}\right)$.

We use the well-known combinatorial identity (see Problem 36)

$$2n\sum_{t=0}^{s}(-1)^t\binom{n}{t} = (-1)^s\left((s+1)\binom{n}{s+1} + (n-s)\binom{n}{s}\right)$$

to calculate $e!\sum_{t=0}^{e} P_t(-n)$ and $e!\sum_{t=0}^{e} P_t(2-n)$. For $e \geq 2$, we obtain

$$e!\sum_{t=0}^{e} P_t(-n) = (-1)^e(n-1)\cdots(n-e),$$

$$\begin{aligned} e!\sum_{t=0}^{e} P_t(2-n) &= (-1)^e(n-2)\cdots(n-e-1) - (-1)^e e(n-2)\cdots(n-e) \\ &= (-1)^e(n-2)\cdots(n-e)(n-2e-1). \end{aligned}$$

Suppose that there exists an e-perfect code $C \subset Q_2^n$, and let λ_i, $i = 0, \ldots, e$, be the eigenvalues of the quotient matrix S_C.

Then, by Corollary 19.1, taking into account that $\lambda_0 = n$, we have

$$(\lambda_1 - x) \cdots (\lambda_e - x) = (-1)^e e! \sum_{t=0}^{e} P_t(x).$$

Substituting $x = -n$ and $x = 2 - n$, respectively, gives

$$(n + \lambda_1) \cdots (n + \lambda_e) = (n-1) \cdots (n-e), \tag{40}$$

and

$$(n + \lambda_1 - 2) \cdots (n + \lambda_e - 2) = (n-2) \cdots (n-e)(n-2e-1). \tag{41}$$

Both sides of (40) are nonzero. Both sides of (41) can be zero only when $n = 2e + 1$. Define $\Delta(n)$ by $n = 2^{\Delta(n)}m$, where m is odd. Among any k consecutive integers, at most every second integer is divisible by 2, every fourth integer by 4, and so on. Therefore,

$$\Delta((m+1) \cdots (m+k)) \leq k + \max_{i=1,\ldots,k} \Delta(m+i). \tag{42}$$

If C is an e-perfect code, then the eigenvalues of the quotient matrix S_C are eigenvalues of the adjacency matrix of the Boolean hypercube (see Corollary 2.1). Since $\lambda_i = n - 2t$ for some $t = 1, \ldots, n$, we have $\Delta(n + \lambda_i) \geq 1$ for $i = 1, \ldots, e$. Moreover,

$$\Delta((n + \lambda_i)(n + \lambda_i - 2)) \geq 3,$$

since one of the factors is divisible by 4.

Multiplying the left- and right-hand sides of (40) and (41), and applying inequality (42), we obtain

$$\begin{aligned} 3e &\leq \Delta((n + \lambda_1) \cdots (n + \lambda_e)(n + \lambda_1 - 2) \cdots (n + \lambda_e - 2)) \\ &= \Delta((n-2e-1)(n-1)(n-2)^2 \cdots (n-e)^2) \\ &\leq \Delta(n-2e-1) + 2e + \max_{i=1,\ldots,e} \Delta(n-i). \end{aligned}$$

Hence $e \leq \max_{i=1,\ldots,e} \Delta(n-i) + \Delta(n-2e-1)$, and therefore $n \geq 2^{e/2}$.

For $q = 2$ the matrix S_C contains coefficients $a_i = 0$, $i = 0, \ldots, e$, and $b_e = n - e$. Hence the sum of the eigenvalues of S_C is $\mathrm{tr}(S_C) = n - e$. Thus

$$\sum_{i=1}^{e} \lambda_i = -e,$$

and all the numbers λ_i are distinct (see Corollary 19.1).

Therefore, for $e > 1$, at least one of them is positive. The inequality $n \geq 2^{e/2}$ and Remark 19.1 imply that, for sufficiently large n, there can be no e-perfect codes in the Boolean n-cube, except for the cases $e = 1$ and $e = \frac{n-1}{2}$.

□

Thus, in order to determine all possible parameters of e-perfect codes in Boolean n-cubes, it suffices to consider finitely many values of n and e. The following conditions are necessary for the existence of an e-perfect code: the size of a ball,

$$\sum_{t=0}^{e} \binom{n}{t},$$

divides the number of vertices of the graph (i.e., the latter is equal to 2^n); the eigenvalues of the quotient matrix S_C are eigenvalues of the adjacency matrix of the Boolean n-cube (integers of the same parity as n); and the equality in Proposition 19.6 holds.

The listed conditions, for $1 < e < \frac{n-1}{2}$, are satisfied only for $n = 23$, with

$$S_C = \begin{pmatrix} 0 & 23 & 0 & 0 \\ 1 & 0 & 22 & 0 \\ 0 & 2 & 0 & 21 \\ 0 & 0 & 3 & 20 \end{pmatrix},$$

whose eigenvalues are $\lambda = 23,\ 7,\ -1,\ -9$. Golay [57] discovered a linear code with these parameters. The Golay code is unique up to isometry.

Zinoviev, Leontiev, and Tietäväinen proved Theorem 19.1, and also proved the nonexistence of perfect codes with nontrivial parameters (except for the ternary Golay code $n = 11$, $e = 2$, $q = 3$ [57]) when $q = p^s$, where p is prime. It is now known ([162],[11]) that for arbitrary q and $2 < e < \frac{n-1}{2}$, there are no e-perfect codes in Q_q^n.

19.5 Problems

159. Let A be a generating set of the Cayley graph $G = Cay(K, A)$ of an abelian group K, and let $B = A \cup \{0\}$. Prove that if (C, B) is a tiling of the group K, then the coloring $f : V(G) \to B$ in which each vertex $x \in K$ is colored by b whenever $x = c + b$ for some $c \in C$ and $b \in B$, is a perfect coloring.

160. Prove that if a distance-regular graph contains an e-perfect code, then for every eigenvalue λ of the quotient matrix S_C, it holds $|A_{e+1}|P_e(\lambda) = |A_e|P_{e+1}(\lambda)$, where A_e is the sphere of radius e.

161. Prove the equality

$$\det(S_C - xI) = (-1)^{e+1}(c_{e+1}P_{e+1}(x) - b_eP_e(x))\prod_{t=1}^{e} c_t.$$

20 Difference Sets and Other Combinatorial Configurations

20.1 Difference Sets

Let K be a finite abelian group. A set $D \subseteq K$ is called a *difference set* with parameters (v, k, λ), if $|K| = v$, $|D| = k$ and for every nonzero $a \in K$ there are exactly λ ordered pairs $d_1, d_2 \in D$ such that $d_1 - d_2 = a$.

Proposition 20.1. *A set $D \subseteq K$ is a difference set with parameters (v, k, λ) if and only if $\mathbf{1}_D * \mathbf{1}_{-D} = \lambda \cdot \mathbf{1} + (k - \lambda)\delta/v^{1/2}$, where $\delta = v^{1/2}\mathbf{1}_{\{0\}}$.*

Proof. Compute the convolution $\sum_{x \in K} \mathbf{1}_D(x) \cdot \mathbf{1}_D(-(y - x))$. For $y \neq 0$, the summand is equal to 1 precisely when $x \in D$ and $x - y \in D$. Thus, the number of such x is exactly the number of pairs $x, x - y \in D$ satisfying $x - (x - y) = y$. By the definition of a difference set, this number is λ. The value of the convolution as $y = 0$ equals $\sum_{x \in K} \mathbf{1}_D(x) \cdot \mathbf{1}_D(x) = k$. The converse follows immediately from the same calculation. □

Corollary 20.1 ([103])**.** *Let b be a Boolean bent function such that $\widehat{(-1)^b}(\bar{0}) = 1$. Consider the set $B = \{x \in \{0,1\}^n \mid b(x) = 1\}$. Then B is a difference set with parameters $(2^n, 2^{n-1} - 2^{n/2-1}, 2^{n-2} - 2^{n/2-1})$. Conversely, if B is a difference set with these parameters, then $\mathbf{1}_B$ is a bent function.*

Proof. We have $|K| = 2^n$ by assumption and $|B| = \frac{1}{2}(2^n - 2^{n/2})$ by Proposition 13.5. Similarly to the proof of Proposition 13.5, we have the equalities $b * b = \frac{1}{4}(\mathbf{1} - (-1)^b) * (\mathbf{1} - (-1)^b) = \frac{1}{4}(2^n\mathbf{1} + 2^{n/2}\delta - 2 \cdot 2^{n/2}\mathbf{1}) = (2^{n-2} - 2^{n/2-1})\mathbf{1} + 2^{n/2-2}\delta$. Here we used the linearity of convolution and the fundamental property of a bent function (Proposition 13.1). Proposition 20.1 shows that B is a difference set with the stated parameters. Relying on Proposition 13.1, it is easy to prove the converse. □

Remark 20.1. If b is a Boolean bent function and $\widehat{(-1)^b}(\bar{0}) = -1$, then, similarly, its support is a difference set with parameters $(2^n, 2^{n-1}+2^{n/2-1}, 2^{n-2}+2^{n/2-1})$. These parameters, together with those in Corollary 20.1 are called *McFarland parameters*.

It will be shown below that any difference set with McFarland parameters can be transformed into a Hadamard matrix.

We next show that any difference set gives rise to an orthogonal matrix whose entries take only two values. Let there be a difference set D with parameters (v, k, λ). For arbitrary $d_1, d_2 \in K$, consider the characteristic functions $f_1(x) = \mathbf{1}_D(x - d_1)$ and $f_2(x) = \mathbf{1}_D(x - d_2)$. By the definition of a difference set, if $d_1 \neq d_2$, the functions f_1 and f_2 are simultaneously equal to 1 in exactly λ points. By symmetry, they differ at $2(k - \lambda)$ points, and they are simultaneously equal to 0 in the remaining $v - \lambda - 2(k - \lambda)$ points. Let a and b satisfy the equation

$$\lambda a^2 + 2(k - \lambda)ab + (v - \lambda - 2(k - \lambda))b^2 = 0.$$

The preceding counting shows that the functions $g_{d_1} = af_1 + b(\mathbf{1} - f_1)$ and $g_{d_2} = af_2 + b(\mathbf{1} - f_2)$ are orthogonal if and only if the above equation holds. Thus, for any distinct $d_1, d_2 \in K$, the functions g_{d_1} and g_{d_2} are orthogonal. Let us show that $a = 1$ and $b = -1$ for difference sets with McFarland parameters. Indeed,

$$\lambda - 2(k - \lambda) + (v - \lambda - 2(k - \lambda)) = v - 4(k - \lambda) = 2^n - 4 \cdot 2^{n-2} = 0.$$

Write the value vectors of the functions g_d, $d \in K$, as rows of a matrix T. The resulting $v \times v$ matrix T is orthogonal up to a scalar factor, since all rows have equal norms. For difference sets with McFarland parameters, the entries of T are ± 1. Hence T is a Hadamard matrix. This also shows directly that $(-1)^{\mathbf{1}_D} * (-1)^{\mathbf{1}_D}(x) = 0$ for $x \neq \bar{0}$. Therefore, by Proposition 13.3 (or equivalently by Proposition 18.11) we obtain the following result.

Corollary 20.2 ([103]). *Let B be a difference set with parameters $(2^n, 2^{n-1} \pm 2^{n/2-1}, 2^{n-2} \pm 2^{n/2-1})$. Then $b = \mathbf{1}_B$ is a Boolean bent function.*

From the orthogonality of T, it follows that the pairs (a, a), (b, a), (a, b), (b, b) occur in any pair of rows (or columns) of T the same number of times. By construction $T(x, y) = a\mathbf{1}_D(x-y)+b(\mathbf{1}-\mathbf{1}_D)(x-y)$. Replace the entries a of T by 1 and the entries b by 0. Thus, consider the matrix $Q_D(x, y) = \mathbf{1}_D(x - y)$. Then each of the pairs $(1, 1)$, $(0, 1)$, $(1, 0)$, $(0, 0)$ occurs equally often in any pair of rows or columns. If we regard the rows of Q_D as the

characteristic vectors of k-subsets of a v-element set, we obtain a 2-design with parameters 2-(v, k, λ). Recall that 2-designs with the same number of points and blocks are called symmetric.

A *partial difference set* with parameters (v, k, λ, μ) is a set $D \subseteq K$ such that $|K| = v$, $|D| = k$ and for any nonzero $a \in D$ there are exactly λ ordered pairs of elements $d_1, d_2 \in D$ satisfying $d_1 - d_2 = a$, whereas for every nonzero $a \in K \setminus D$ there are exactly μ such pairs.

Similarly to Proposition 20.1 it is easy to prove that the definition of a partial difference set implies the equality

$$\mathbf{1}_D * \mathbf{1}_{-D} = \lambda \cdot \mathbf{1}_D + \mu \cdot (\mathbf{1} - \mathbf{1}_D) + \frac{k-\mu}{v^{1/2}}\delta. \tag{43}$$

Indeed, at a nonzero element of D, the left-hand side has value λ; at a nonzero element outside D, it has value μ; and at 0, it has value k.

In other words, if the convolution of the characteristic function of a set with the characteristic function of its negative is a linear combination of the characteristic function of the set, the constant function, and the Dirac δ function, then the set is a partial difference set. Its parameters μ, λ, k can be determined from the coefficients of this linear combination.

Throughout we additionally assume that $D = -D$ and $0 \notin D$. Applying the Fourier transform to (43), we obtain the following quadratic equation for $f = \widehat{\mathbf{1}_D}$

$$f \cdot f = \lambda \cdot f + \mu \cdot (\delta - f) + \frac{k-\mu}{v^{1/2}}\mathbf{1}.$$

Consequently, f can take only the values

$$\frac{\lambda - \mu \pm \Delta}{2}, \quad \text{where} \quad \Delta = \sqrt{(\lambda-\mu)^2 + 4(k-\mu)/v^{1/2}}$$

on the nonzero elements of K, and $f(0) = k/v^{1/2}$.

Let $D^+ = \{x \in K \mid f(x) = \frac{\lambda-\mu+\Delta}{2}\}$.

Proposition 20.2 (Delsarte [98])**.** *D^+ is a partial difference set.*

Proof. It suffices to verify that the characteristic function of D^+ satisfies an identity of the form (43) for some k', λ', and μ'. Since $D = -D$, we have $f(x) = f(-x)$. Hence $D^+ = -D^+$. By the inversion formula for the Fourier transform, $\widehat{\widehat{f(x)}} = f(-x)$ and therefore $\widehat{f} = \mathbf{1}_D$. Consequently, $\widehat{f} \cdot \widehat{f} = \widehat{f}$. Applying the Fourier transform once more and using the convolution property (Proposition 9.17) gives $f * f = v^{1/2} f$. By the definition of D^+ the equality $f = \alpha_1 \mathbf{1}_{D^+} + \alpha_2 \mathbf{1} + \alpha_3 \delta$ holds for some coefficients $\alpha_1, \alpha_2, \alpha_3$.

Substituting this representation of f into $f * f = v^{1/2} f$ and taking into account $\mathbf{1}_{D^+} * \delta = v^{1/2}\mathbf{1}_{D^+}$ and $\mathbf{1}_{D^+} * \mathbf{1} = |D^+|\mathbf{1}$, we obtain that the convolution $\mathbf{1}_{D^+} * \mathbf{1}_{D^+}$ can be expressed as the required linear combination. Thus, there exist some coefficients μ', λ', k' for which the equality

$$\mathbf{1}_{D^+} * \mathbf{1}_{D^+} = \lambda' \cdot \mathbf{1}_{D^+} + \mu' \cdot (\mathbf{1} - \mathbf{1}_{D^+}) + \frac{k' - \mu'}{v^{1/2}}\delta$$

holds. By the characterization of partial difference sets, D^+ is therefore a partial difference set. □

20.2 Difference Sets and Strongly Regular Graphs as Perfect Colorings

Consider the Cayley graph $\mathrm{Cay}(K, D)$ of a group K with connection set D, where $D = -D$ and $0 \notin D$. It follows from the definition of a partial difference set with parameters (v, k, λ, μ) that $\mathrm{Cay}(K, D)$ is a strongly regular graph with parameters (v, k, λ, μ).

Indeed, let $x, y \in K$ be adjacent vertices of $\mathrm{Cay}(K, D)$; thus, $y = x + a$ for some $a \in D$. By the definition of a partial difference set, there are exactly λ ordered pairs $(d_1, d_2) \in D \times D$ such that $a = d_1 - d_2$. For each such pair, $x + d_1 = y + d_2$ is a common neighbor of x and y in $\mathrm{Cay}(K, D)$. Hence, x and y have exactly λ common neighbors. Similarly, if x and y are nonadjacent, then they have exactly μ common neighbors. Therefore, $\mathrm{Cay}(K, D)$ is strongly regular with parameters (v, k, λ, μ).

The converse also holds: if $\mathrm{Cay}(K, D)$ is strongly regular, then D is a partial difference set in K with the corresponding parameters.

As shown in the previous section, any difference set D with parameters (v, k, λ) gives rise to a symmetric 2-(v, k, λ) design. If $D = -D$ and $0 \notin D$, then the matrix $Q_D(x, y) = \mathbf{1}_D(x - y)$ is the adjacency matrix of $\mathrm{Cay}(K, D)$. Moreover, it follows immediately from the definitions that the rows of the adjacency matrix of a strongly regular graph with parameters (v, k, λ, λ) form the incidence vectors of the blocks of a symmetric 2-(v, k, λ) design. Indeed, any two distinct rows have scalar product λ, since two distinct vertices have exactly λ common neighbors.

The converse is also true. Suppose that the rows of a matrix are the characteristic vectors of the k-subsets (blocks) of a symmetric 2-(v, k, λ) design, and suppose that the matrix is symmetric and has zeros on its main diagonal. Then this matrix is the adjacency matrix of a strongly regular graph with parameters (v, k, λ, λ).

We next show that every strongly regular graph gives rise to a perfect coloring of a certain hypergraph.

Consider the complete graph K_n. Let Γ_n be the hypergraph whose vertices are the edges of K_n and whose hyperedges are the triples of edges that form triangles in K_n. Let G be a strongly regular graph on the same vertex set as K_n, with parameters (n, k, λ, μ). Define a 2-coloring of the vertices of Γ_n by

$$f(e) = \begin{cases} 1, & e \in E(G), \\ 0, & e \notin E(G). \end{cases}$$

The color of a hyperedge is the unordered composition of the colors of its three vertices.

We verify that this coloring is perfect. Let $e = \{x, y\}$ be a vertex of Γ_n. Every hyperedge of Γ_n containing e corresponds to a vertex $z \in V(K_n) \setminus \{x, y\}$ and consists of the three edges $\{x, y\}, \{x, z\}, \{y, z\}$.

First suppose that $e = \{x, y\}$ has color 1, so that x and y are adjacent in G. Among the $n-2$ possible vertices z, the numbers for which z is adjacent to both x and y, to exactly one of x, y, or to neither of them are, respectively, $\lambda, 2(k-\lambda-1), n-2k+\lambda$. Hence, the numbers of hyperedges of colors 111, 110, and 100 containing e are, respectively, $\lambda, 2(k-\lambda-1), n-2k+\lambda$.

These numbers depend only on the parameters of G and not on the particular color-1 vertex e.

Now suppose that $e = \{x, y\}$ has color 0, so that x and y are nonadjacent in G. In this case, the corresponding numbers are $\mu, 2(k-\mu), n-2k+\mu-2$.

Consequently, the numbers of hyperedges of colors 011, 010, and 000 containing e are, respectively, $\mu, 2(k-\mu), n-2k+\mu-2$. Again, these numbers depend only on the parameters of G and not on the particular color-0 vertex e.

Thus, for each vertex color and each hyperedge color, every vertex of that color is incident with the same number of hyperedges of that color. Hence, the coloring is perfect. This construction shows that every strongly regular graph determines a perfect 2-coloring of Γ_n.

The converse requires some care. A perfect 2-coloring of Γ_n imposes regularity conditions on the graph formed by the edges of color 1. Apart from certain degenerate cases (disconnected graphs or star graphs), these conditions imply that the resulting graph is strongly regular. In particular, the numbers of common neighbors of two vertices are determined by whether the corresponding edge of Γ_n has color 1 or color 0. The correspondence between perfect 2-colorings of Γ_n and strongly regular graphs is not one-to-one. In particular, the definition of a perfect coloring of a hypergraph

depends only on the unordered composition of the colors of the vertices in a hyperedge and therefore does not distinguish between different orderings of these vertices.

20.3 Association Schemes

It is well known (see [83]) that the above definition of a distance-regular graph is equivalent to the following one, which is also frequently taken as the definition. A connected graph G is distance-regular if and only if, for every pair of vertices x, y with $d(x, y) = i$ and every pair of integers j, k, the number of vertices $\{z \in V(G) \mid d(x, z) = j,\ d(y, z) = k\}$ depends only on i, j, k and not on the particular choice of the vertices x and y.

The latter definition is closely related to the notion of an association scheme.

An *association scheme* $\mathcal{A}$ on a set X is a set of binary relations $R_0, R_1, \ldots, R_m \subseteq X \times X$ satisfying the following conditions:

1) $R_0 = \{(x, x) \mid x \in X\}$.
2) If $R_i \in \mathcal{A}$, then $R_i^* = \{(x, y) \mid (y, x) \in R_i\} \in \mathcal{A}$.
3) For every $(x, y) \in R_k$, the number of vertices $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ depends only on i, j, k.

A distance-regular graph gives rise to an association scheme in the following way. Let $X = V(G)$ be the vertex set of a distance-regular graph G, and let $R_i = \{(x, y) \in X \times X \mid d(x, y) = i\}$. The relations $R_0, R_1, \ldots, R_m$ form an association scheme. A detailed exposition of the theory of association schemes can be found in [10].

Consider an association scheme $\mathcal{A} = \{R_0, R_1, \ldots, R_m\}$ on a set X of n elements, where R_0 is the relation consisting of the pairs (x, x). Suppose that the association scheme is symmetric, i.e., $(x, y) \in R_i \implies (y, x) \in R_i$ for every $i \in 1, \ldots, m$. Then the association scheme determines a perfect coloring of the hypergraph Γ_n with colors $\{R_1, \ldots, R_m\}$.

Indeed, the vertices of Γ_n are the 2-element subsets of X, that is, the edges of the complete graph K_n, and its hyperedges are the triples of pairs that form a triangle. We color a vertex $\{x, y\}$ of Γ_n by the relation R_i containing (x, y). This is well defined because the scheme is symmetric.

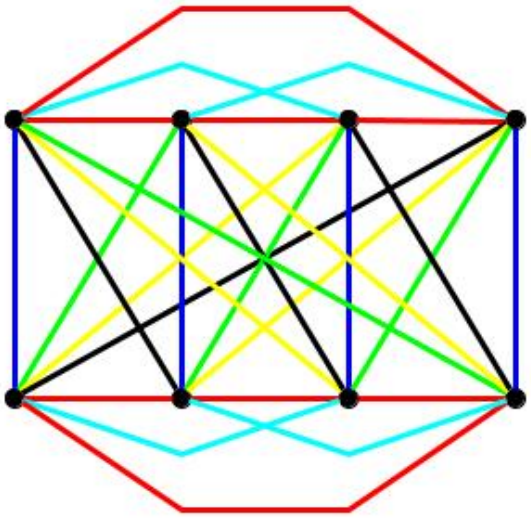
Consider a vertex x, y of color R_k. A hyperedge containing this vertex is determined by a third element $z \in X \setminus \{x, y\}$. The colors of the other two vertices of this hyperedge are determined by the relations containing (x, z) and (z, y). Therefore, the number of hyperedges of each color composition containing x, y is determined by the numbers

$$p_{ij}^k = |\{z \in X \mid (x, z) \in R_i,\ (z, y) \in R_j\}|\,.$$

By condition (3) of the definition of an association scheme, these numbers depend only on i, j, k and not on the particular choice of $(x, y) \in R_k$. Hence, the resulting coloring of Γ_n is perfect.

Despite the close relationship between the definitions of a symmetric association scheme and a perfect coloring of Γ_n, the two notions do not coincide.

Example 20.1. Consider the hypergraph Γ_8 and the following coloring of its vertices (the edges of K_8):



It is easy to see that the coloring shown in the figure is perfect for the hypergraph Γ_8, in which two vertices are considered adjacent if the corresponding edges of K_8 belong to the same triangle. At the same time, this perfect coloring does not define an association scheme. Indeed, for the edges of K_8 of the red color, the two endpoints are not equivalent. Namely, from one endpoint of a red edge there is a blue edge that completes a triangle with a black edge, whereas from the other endpoint there is a green edge. In a symmetric association scheme, the two endpoints of an edge belonging to the same relation must be equivalent.

20.4 Bent Functions as Perfect Colorings

Next, we consider in more detail the abelian group $\mathbb{Z}_2^n$. Denote by Δ_n the 3-uniform hypergraph whose vertices are all nonzero elements of the group $\mathbb{Z}_2^n$. A triple of vertices a_1, a_2, a_3 forms a hyperedge if $a_1 + a_2 + a_3 = 0$. Note that this equality implies that the elements a_i, $i = 1, 2, 3$, are nonzero and

pairwise distinct.

Let D be a partial difference set in $\mathbb{Z}_2^n$ with parameters (v, k, λ, μ). Then the coloring $\mathbf{1}_D$ of the hypergraph Δ_n is perfect. Indeed, in $\mathbb{Z}_2^n$ the equality $a_1 + a_2 + a_3 = 0$ is equivalent to $a_1 = a_2 - a_3$.

For each $a_1 \in D$, there are λ ordered pairs $(d_1, d_2) \in D \times D$ such that $a_1 = d_1 - d_2$. Since the pairs (d_1, d_2) and (d_2, d_1) determine the same hyperedge, the vertex a_1 is contained in $\lambda/2$ hyperedges consisting entirely of elements of D. Similarly, if $a_1 \notin D$, then a_1 is contained in $\mu/2$ hyperedges containing two elements of D.

Every pair of distinct nonzero elements $a, b \in \mathbb{Z}_2^n$ belongs to exactly one hyperedge of Δ_n, namely $\{a, b, a+b\}$. Therefore, the numbers of hyperedges of each possible color composition containing a vertex a can be determined from λ and μ. These numbers depend only on the color of a. Consequently, the coloring $\mathbf{1}_D$ is perfect.

The converse is also true. Let D be the set of vertices of color 1. For a vertex $a \in D$, the number of hyperedges of color composition $(1, 1, 1)$ containing a is $\lambda/2$, where λ is the corresponding partial-difference-set parameter. Similarly, for a vertex $a \notin D$, the number of hyperedges of color composition $(0, 1, 1)$ containing a is $\mu/2$. Hence, the corresponding partial-difference-set parameters are determined by the parameters of the perfect coloring.

Then, from Proposition 20.1, we obtain the following claim.

Proposition 20.3. *Boolean bent functions correspond one-to-one to perfect 2-colorings of the hypergraph Δ_n with the corresponding quotient matrix.*

By Proposition 15.2, a perfect coloring of the hypergraph Δ_n induces a perfect coloring of its line graph $\mathcal{E}(\Delta_n)$. Since the intersection of two hyperedges of Δ_n contains at most one vertex, $\mathcal{E}(\Delta_n)$ is a simple graph. Note that a 2-coloring $\mathbf{1}_D$ of the hypergraph Δ_n induces a 4-coloring of the graph $\mathcal{E}(\Delta_n)$, because each hyperedge of Δ_n consists of three vertices and can contain 0, 1, 2, or 3 vertices of color 1.

Consider the elements of the group $\mathbb{Z}_2^n$ as elements of the vector space $(GF(2))^n$. A hyperedge of Δ_n corresponds to a 2-dimensional subspace of $(GF(2))^n$. Moreover, two hyperedges of Δ_n have a common vertex if and only if the corresponding 2-dimensional subspaces intersect in a 1-dimensional subspace. Thus, the graph $\mathcal{E}(\Delta_n)$ is the Grassmann graph $J_2(n, 2)$.

The *Grassmann graph* $J_q(n, k)$ is the graph whose vertices are the k-dimensional subspaces of the vector space $(GF(q))^n$. Two vertices are adja-

cent if the corresponding subspaces intersect in a $(k-1)$-dimensional subspace. Grassmann graphs are distance-regular (see [18]).

Consider the graph $J_2(n,2)$ whose vertices are the 2-dimensional subspaces of $(GF(2))^n$. Let $f : Q_2^n \to Q_2$ be a Boolean function, and assume that $f(\bar{0}) = 1$. Each 2-dimensional subspace of $(GF(2))^n$ consists of four elements. The function f induces a coloring of the vertices of $J_2(n,2)$ into four colors according to the number of ones of f on the corresponding subspace. Thus, every Boolean function gives rise to a 4-coloring of the graph $J_2(n,2)$.

Theorem 20.1 ([118]). *A bent function $b : Q_2^n \to Q_2$ satisfying the normalization conditions $\widehat{(-1)^b}(\bar{0}) = 1$, $b(\bar{0}) = 1$ corresponds to a perfect 4-coloring of the graph $J_2(n,2)$ with quotient matrix*

$$\begin{pmatrix} 3(2^{n-3}-2^{(n/2)-2}-1) & 3\cdot 2^{n-2}-3 & 3(2^{n-3}+2^{(n/2)-2}) & 0 \\ 2^{n-2}-2^{(n/2)-1} & 5\cdot 2^{n-3}-2^{(n/2)-2}-5 & 2^{n-1}+2^{(n/2)-1} & 2^{n-3}+2^{(n/2)-2}-1 \\ 2^{n-3}-2^{(n/2)-2} & 2^{n-1}-2^{(n/2)-1}-1 & 5\cdot 2^{n-3}+2^{(n/2)-2}-3 & 2^{n-2}+2^{(n/2)-1}-2 \\ 0 & 3(2^{n-3}-2^{(n/2)-2}) & 3\cdot 2^{n-2} & 3(2^{n-3}+2^{(n/2)-2}-2) \end{pmatrix}.$$

Proof. By Proposition 13.5, $|\mathrm{supp}(b)| = \frac{1}{2}\left(2^n + 2^{n/2}\right)$.

For $y \neq \bar{0}$, Proposition 13.3 implies

$$|\{x \in Q_2^n : b(x) \oplus b(x+y) = 0\}| = |x \in Q_2^n : b(x) \oplus b(x+y) = 1|.$$

Consider a 2-dimensional subspace containing $\bar{0}, y$. Denote by $A_{\alpha\beta}$ the number of pairs of values $(\alpha,\beta) = (b(x), b(x+y))$, $x \in (GF(2))^n$.

Then

$$A_{01} + A_{10} = A_{00} + A_{11},$$

and

$$A_{01} + A_{10} + A_{00} + A_{11} = 2^n.$$

Moreover, by the change of variable $x \mapsto x + y$,

$$A_{01} = A_{10}.$$

Finally,

$$A_{10} + A_{11} = |\,\mathrm{supp}(b)|.$$

Using these equalities and the chosen sign of the Walsh coefficient at $\bar{0}$, we obtain

$$A_{01} = A_{10} = 2^{n-2},$$
$$A_{11} = 2^{n-2} + 2^{(n/2)-1}, \qquad A_{00} = 2^{n-2} - 2^{(n/2)-1}.$$

Consequently, if the color of a 2-dimensional subspace is known, then the numbers of adjacent subspaces of each color are determined.

For example, a subspace of color 4 is not adjacent to a subspace of color 1. It is adjacent to $\frac{3A_{00}}{2}$ subspaces of color 2, since each pair of vertices $(x, x+y)$ with $(b(x), b(x+y)) = (0,0)$ is counted twice, namely as $(x, x+y)$ and $(x+y, x)$. It is adjacent to $\frac{3A_{11}-12}{2}$ subspaces of color 4, because it contains four elements, including $\bar{0}$, at which the function b takes the value 1. Fixing each of the three nonzero vertices gives $\frac{A_{11}-4}{2}$ adjacent subspaces of color 4.

Thus, the coloring is perfect, with quotient matrix

$$\frac{1}{2}\begin{pmatrix} 3A_{00}-6 & 6A_{01}-6 & 3A_{11} & 0 \\ 2A_{00} & 4A_{01}+A_{00}-10 & 2A_{01}+2A_{11} & A_{11}-2 \\ A_{00} & 2A_{01}+2A_{00}-2 & 4A_{10}+A_{11}-6 & 2A_{11}-4 \\ 0 & 3A_{00} & 6A_{01} & 3A_{11}-12 \end{pmatrix}.$$

Substituting the values of A_{00}, A_{01}, and A_{11} gives the matrix in the statement. □

The converse is also true: every perfect 4-coloring with the quotient matrix given in Theorem 20.1 corresponds to a Boolean bent function (see [118]).

It is easy to see that a difference set with the corresponding parameters defines a perfect coloring of the graph $J_2(n,2)$ with the parameters from Theorem 20.1. Hence, we obtain the following corollary.

Corollary 20.3. *The characteristic function of a difference set with parameters*

$$\left(2^n, 2^{n-1}-2^{n/2-1}, 2^{n-2}-2^{n/2-1}\right)$$

is a bent function.

It is easy to verify that, by merging the colors pairwise according to their parity in the perfect coloring of $J_2(n,2)$ constructed above, we obtain a perfect coloring with quotient matrix

$$\begin{pmatrix} 3\cdot 2^{n-2}-3 & 3\cdot 2^{n-2}-3 \\ 3\cdot 2^{n-2} & 3\cdot 2^{n-2}-6 \end{pmatrix}.$$

However, one cannot recover a bent function from a perfect 2-coloring with these parameters, because adding an affine function to a bent function does not change the coloring.

20.5 Spreads

Let $q = p^r$ be a prime power. Consider Q_q^n as a vector space over the finite field $GF(q)$. A *spread*, more precisely a k-spread, in the vector space Q_q^n is a collection of k-dimensional linear subspaces that covers every nonzero vector exactly once.

The definition of a k-spread is equivalent to the definition of a 1-factor (perfect matching) in the hypergraph whose vertices are the elements of $Q_q^n \backslash \bar{0}$ and whose hyperedges are k-dimensional subspaces of Q_q^n. Thus, k-spreads are perfect colorings of hypergraphs (see Section 16.4). But sometimes they also generate perfect colorings of Grassmann graphs.

In the Grassmann graph $J_q(n,k)$, the k-dimensional subspaces correspond to vertices. The distance between two k-dimensional subspaces U and V in $J_q(n,k)$ is $d(U,V) = k - \dim(U \cap V)$. Therefore, a k-spread is equivalent to a code in $J_q(n,k)$ with the maximum possible minimum distance k and the maximum possible number of vertices, $c = \frac{q^n-1}{q^k-1}$.

Indeed, subspaces at distance k intersect only in the zero vector, and their nonzero vectors are therefore pairwise disjoint. Since each k-dimensional subspace contains $q^k - 1$ nonzero vectors, the number of such subspaces cannot exceed $(q^n - 1)/(q^k - 1)$.

Proposition 20.4. *2-spreads in $J_2(n,2)$ correspond one-to-one to the first cells of equitable 2-partitions with quotient matrix*

$$\begin{pmatrix} 0 & 6 \cdot 2^{n-2} - 6 \\ 3 & 6 \cdot 2^{n-2} - 9 \end{pmatrix}.$$

Proof. Every vertex of $J_2(n,2)$ corresponds to a 2-dimensional subspace containing three nonzero vectors. Two elements of a 2-spread are not adjacent in $J_2(n,2)$, since they intersect only in the zero vector.

Now consider a vertex of $J_2(n,2)$ that does not belong to the spread. The corresponding 2-dimensional subspace contains three nonzero vectors. Each of these vectors belongs to exactly one element of the spread. These three elements of the spread are distinct, and each intersects the given 2-dimensional subspace in a 1-dimensional subspace. Hence, the vertex is adjacent to exactly three vertices of the spread.

Thus, the partition into the spread and its complement is equitable, with quotient matrix

$$\begin{pmatrix} 0 & 6 \cdot 2^{n-2} - 6 \\ 3 & 6 \cdot 2^{n-2} - 9 \end{pmatrix}.$$

Conversely, suppose that an equitable 2-partition with this quotient matrix is given, and let c and c' denote the sizes of its first and second cells,

respectively. The total number of vertices of $J_2(n,2)$ is $\frac{(2^n-1)(2^n-2)}{6}$. Hence

$$c + c' = \frac{(2^n-1)(2^n-2)}{6}.$$

Counting edges between the two cells in two ways gives

$$c(6 \cdot 2^{n-2} - 6) = 3c'.$$

Solving this system yields $c = \frac{2^n-1}{3}$.

Each vertex in the first cell is nonadjacent to every other vertex in the first cell. Thus, the corresponding 2-dimensional subspaces intersect only in the zero vector. Since there are $(2^n-1)/3$ such subspaces and each contains three nonzero vectors, they cover all nonzero vectors of Q_2^n. Hence, they form a 2-spread. □

It is well known that every 2-spread and every 3-spread in Q_q^n gives a completely regular code in $J_q(n,2)$ and $J_q(n,3)$, respectively (see [102]). Other perfect colorings of Grassmann graphs are considered in [108].

Clearly, a k-spread in Q_q^n can exist only if $\frac{q^n-1}{q^k-1}$ is an integer.

Proposition 20.5. *If k divides n, then there exists a k-spread in Q_q^n.*

Proof. Suppose that $n = kt$. Regard Q_q^n as a t-dimensional vector space over the field $GF(q^k)$. The 1-dimensional linear subspaces of this vector space form a 1-spread. Indeed, every nonzero vector belongs to a unique 1-dimensional subspace over $GF(q^k)$.

Each 1-dimensional subspace over $GF(q^k)$ is a k-dimensional subspace over $GF(q)$. To see this, let $A_v = \{\alpha v : \alpha \in GF(q^k)\}$ be the 1-dimensional subspace containing a nonzero vector v. Since $GF(q^k)$ is a k-dimensional vector space over $GF(q)$, the set A_v is a k-dimensional vector space over $GF(q)$. Thus, the 1-dimensional subspaces over $GF(q^k)$ become k-dimensional subspaces over $GF(q)$.

Moreover, two distinct 1-dimensional subspaces over $GF(q^k)$ intersect only in the zero vector. Therefore, these subspaces form a k-spread in Q_q^n. □

A *partial spread* is a collection of linear subspaces of a fixed dimension that intersect pairwise only in the zero vector.

Proposition 20.6 (Dillon, see [103])**.** *Let $\{V_i : i = 1, \dots, 2^{n-1}\}$ be a partial n-spread in Q_2^{2n}. Then the characteristic function b of the set $B = \bigcup_{i=1}^{2^{n-1}} V_i \setminus \bar{0}$ is a bent function.*

Proof. Since the subspaces V_i intersect pairwise only in $\bar{0}$, the sets $V_i \setminus \bar{0}$ are pairwise disjoint. Hence, $b = \sum_{i=1}^{2^{n-1}} \mathbf{1}_{V_i} - \frac{1}{2}\delta$. Consequently,

$$(-1)^b = 2b - \mathbf{1} = 2\sum_{i=1}^{2^{n-1}} \mathbf{1}_{V_i} - \delta - \mathbf{1}.$$

By using $\widehat{\mathbf{1}_{V_i}} = \mathbf{1}_{V_i^\perp}$ (Corollary 11.2), and $\widehat{\delta} = \mathbf{1}$, $\widehat{\mathbf{1}} = \delta$ (Section 9.3), we obtain

$$\widehat{(-1)^b} = 2\sum_{i=1}^{2^{n-1}} \mathbf{1}_{V_i^\perp} - \mathbf{1} - \delta.$$

For $i \neq j$, $V_i^\perp \cap V_j^\perp = (V_i + V_j)^\perp$. Since $V_i \cap V_j = \{\bar{0}\}$ and both subspaces have dimension n in the $2n$-dimensional space Q_2^{2n}, we have $V_i + V_j = Q_2^{2n}$. Therefore, $V_i^\perp \cap V_j^\perp = \bar{0}$. Thus, the sets $V_i^\perp \setminus \{\bar{0}\}$ are pairwise disjoint. Consequently, the sum $\sum_{i=1}^{2^{n-1}} \mathbf{1}_{V_i^\perp}$ takes only the values 0 and 1 away from $\bar{0}$, and hence $\widehat{(-1)^b}$ takes only the values ± 1. Therefore, b is a bent function. □

20.6 Problems

162. Prove that every partition of a set of $2n$ elements into pairs is a completely regular code in $J(2n, 2)$. Prove that every partition of a set of $3n$ elements into triples is a completely regular code in $J(3n, 3)$.

163. Prove that the complement of a difference set is also a difference set.

164. Let M be the adjacency matrix of a strongly regular graph with parameters $(v, k, \lambda, \lambda + 2)$. Prove that the rows of the matrix $M + I$ are the characteristic vectors of $(k+1)$-blocks of a symmetric 2-$(v, k+1, \lambda+2)$ design.

165. Let D be a 2-(v, k, λ) design of size v. Let the rows of the matrix Q_D be the characteristic vectors of the blocks of the design D. Prove that the columns of Q_D are the characteristic vectors of the blocks of a design with the same parameters.

166. Let $\{V_i : i = 1, \ldots, 2^{n-1} + 1\}$ be a partial n-spread in Q_2^{2n}. Prove that the characteristic function of the set $B = \cup_{i=1}^{2^{n-1}+1} V_i$ is a bent function.

167. Prove that, using the Dillon construction (Proposition 20.6), one can construct at least $\binom{2^n+1}{2^{n-1}}$ distinct bent functions in Q_2^{2n}.

168. Prove that, using the Maiorana–McFarland construction (Proposition 13.9), one can construct at least $(2^n)!2^{2^n}$ distinct bent functions in Q_2^{2n}.

169. Let there be a difference set D with parameters $(v, k, 1)$. Prove that the $v \times v$ matrix Z whose rows are the characteristic vectors of the sets $a - D$, $a \in K$, does not contain a 2×2 submatrix consisting of four ones.

170. Prove that for any prime p there exists a square matrix of size $p(p+1)+1$ containing $(p+1)(p(p+1)+1)$ ones and having no 2×2 submatrix consisting entirely of ones (the *Zarankiewicz problem*).

171. Prove that, for any $p \geq 1$, a square matrix of size $p(p+1)+1$ containing more than $(p+1)(p(p+1)+1)$ ones must contain a 2×2 submatrix consisting entirely of ones.

172. Prove that for any $p \geq 1$ a bipartite graph with $p(p+1)+1$ vertices in each part and R edges contains a cycle of length 4 whenever $R > (p+1)(p(p+1)+1)$. If $R = (p+1)(p(p+1)+1)$ and p is prime, prove that there exists such a graph without cycles of length less than 6.

173. Let f be a perfect 2-coloring of the hypergraph Γ_n (see Section 20.2). Prove that if the edges of either color of f induce a connected regular graph G, then G is strongly regular.

References

[1] N. Alon and F. R. K. Chung, "Explicit construction of linear sized tolerant networks," in *Proceedings of the First Japan Conference on Graph Theory and Applications*, Hakone, 1986, pp. 15–19, 1988.

[2] N. Alon and V. D. Milman, "λ_1, isoperimetric inequalities for graphs, and superconcentrators," *J. Comb. Theory, Ser. B*, vol. 38, no. 1, pp. 73–88, 1985.

[3] N. Alon and S. Friedland, "The maximum number of perfect matchings in graphs with a given degree sequence," *Electron. J. Comb.*, vol. 15, #13, 2008.

[4] D. Angluin and A. Gardiner, "Finite common coverings of pairs of regular graphs," *J. Comb. Theory, Ser. B*, vol. 30, pp. 184–187, 1981.

[5] S. V. Avgustinovich, "On a property of perfect binary codes," *Diskretn. Anal. Issled. Oper.*, vol. 2, no. 1, pp. 4–6, 1995 (Russian).

[6] S. V. Avgustinovich and I. Yu. Mogilnykh, "Perfect 2-colorings of Johnson graphs $J(8,3)$ and $J(8,4)$," *J. Appl. Industr. Math.*, vol. 5, no. 1, pp. 19–30, 2011.

[7] S. V. Avgustinovich and I. Yu. Mogil'nykh, "Induced perfect colorings," *SEMR*, vol. 8, pp. 310–316, 2011.

[8] L. Babai, "Spectra of Cayley graphs," *J. Comb. Theory, Ser. B*, vol. 27, no. 2, pp. 180–189, 1979.

[9] S. Ball, "On sets of vectors of a finite vector space in which every subset of basis size is a basis," *J. Eur. Math. Soc. (JEMS)*, vol. 14, no. 3, pp. 733–748, 2012.

[10] E. Bannai and T. Ito, *Algebraic Combinatorics I: Association Schemes*, Mathematics Lecture Note Series, Menlo Park, CA: Benjamin/Cummings, 1984.

[11] L. A. Bassalygo, V. A. Zinov'ev, V. K. Leont'ev, and N. I. Fel'dman, "Nonexistence of perfect codes over some composite alphabets," *Probl. Peredaci Inform.*, vol. 11, no. 3, pp. 3–13, 1975 (Russian).

[12] E. A. Bespalov, D. S. Krotov, A. A. Matiushev, A. A. Taranenko, and K. V. Vorob'ev, "Perfect 2-colorings of Hamming graphs," *J. Combin. Des.*, vol. 29, no. 6, pp. 367–396, 2021.

[13] E. Bespalov, "On the non-existence of extended 1-perfect codes and MDS codes," *J. Comb. Theory, Ser. A*, vol. 189, Article ID 105607, 11 pp., 2022.

[14] J. Bierbrauer, "Bounds on orthogonal arrays and resilient functions," *J. Combin. Des.*, vol. 3, no. 3, pp. 179–183, 1995.

[15] J. Bierbrauer, *Introduction to Coding Theory*, 2nd ed., Boca Raton, FL: Taylor & Francis, 2017.

[16] R. C. Bose, "On the construction of balanced incomplete block designs," *Ann. Eugenics*, vol. 9, pp. 353–399, 1939.

[17] R. C. Bose, S. S. Shrikhande, and E. T. Parker, "Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture," *Canad. J. Math.*, vol. 12, pp. 189–203, 1960.

[18] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 18, Berlin: Springer-Verlag, 1989.

[19] A. E. Brouwer, C. D. Godsil, J. H. Koolen, and W. J. Martin, "Width and dual width of subsets in polynomial association schemes," *J. Comb. Theory, Ser. A*, vol. 102, no. 2, pp. 255–271, 2003.

[20] A. E. Brouwer and W. H. Haemers, *Spectra of Graphs*, Universitext, Berlin: Springer, 2012.

[21] J. N. Bray, Q. Cai, P. J. Cameron, P. Spiga, H. Zhang, "The Hall-Paige conjecture, and synchronization for affine and diagonal groups", *J. Algebra*, vol. 545. pp. 27–42, 2020.

[22] R. H. Bruck and H. J. Ryser, "The nonexistence of certain finite projective planes," *Canad. J. Math.*, vol. 1, pp. 88–93, 1949.

[23] P. Camion, B. Courteau, and P. Delsarte, "On r-partition designs in Hamming spaces," *Appl. Algebra Engrg. Comm. Comput.*, vol. 2, no. 3, pp. 147–162, 1992.

[24] A. Canteaut, "Open problems related to algebraic attacks on stream ciphers," in *International Workshop on Coding and Cryptography (WCC 2005)*, Bergen, March 2005, Lecture Notes in Computer Science, vol. 3969, Berlin: Springer, 2006, pp. 1–11.

[25] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Des. Codes Cryptography*, vol. 15, no. 2, pp. 125–156, 1998.

[26] C. Carlet and P. Sarkar, "Spectral domain analysis of correlation immune and resilient Boolean functions", *Finite fields and Applications*, vol. 8, pp. 120–130, 2002.

[27] C. Carlet, "Boolean and vectorial plateaued functions, and APN functions," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6272–6289, 2015.

[28] C. Carlet and S. Mesnager, "Four decades of research on bent functions," *Des. Codes Cryptography*, vol. 78, pp. 5–50, 2016.

[29] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge: Cambridge University Press, 2020.

[30] S. Chowla and H. J. Ryser, "Combinatorial problems," *Canad. J. Math.*, vol. 2, pp. 93–99, 1950.

[31] G. Cohen, S. Litsyn, A. Vardy, and G. Zémor, "Tilings of binary spaces," *SIAM J. Discrete Math.*, vol. 9, no. 3, pp. 393–412, 1996. DOI: 10.1137/S0895480195280137.

[32] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Proceedings of Eurocrypt 2003*, Lecture Notes in Computer Science, vol. 2656, pp. 345–359, 2003.

[33] M. B. Crawford, D. J. Marchette, W. Maxwell, and S. S. Mendelson, "Spectral properties of random graphs with fixed equitable partition," E-print 2311.07675, arXiv.org, 2023. DOI: 10.48550/arXiv.2311.07675.

[34] D. M. Cvetković, M. Doob, and H. Sachs, *Spectra of Graphs: Theory and Application*, New York: Academic Press, 1980.

[35] P. Delsarte, "An algebraic approach to the association schemes of coding theory," *Philips Research Reports Supplements*, vol. 10, 1973.

[36] P. Delsarte, "Four fundamental parameters of a code and their combinatorial significance," *Information and Control*, vol. 23, pp. 407–438, 1973.

[37] P. Delsarte and V. I. Levenshtein, "Association schemes and coding theory," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2477–2504, 1998.

[38] J. Dénes and A. D. Keedwell, *Latin Squares: New Developments in the Theory and Applications*, Annals of Discrete Mathematics, vol. 46, Amsterdam: North-Holland, 1991.

[39] K. Devriendt and P. Van Mieghem, "Tighter spectral bounds for the cut size, based on Laplacian eigenvectors," *Linear Algebra Appl.*, vol. 572, pp. 68–91, 2019.

[40] X. D. Dong, C. B. Son, and E. Gunawan, "Matrix characterization of MDS linear codes over modules," *Linear Algebra Appl.*, vol. 277, no. 1, pp. 57–61, 1998.

[41] G. P. Egorychev "The solution of van der Waerden's problem for permanents.," *Adv. Math.* vol. 42, pp. 299–305, 1981.

[42] J. T. Ethier and G. L. Mullen, "Strong forms of orthogonality for sets of hypercubes," *Discrete Math.*, vol. 312, no. 12–13, pp. 2050–2061, 2012.

[43] T. Etzion and A. Vardy, "Perfect binary codes and tilings: problems and solutions," *SIAM J. Discrete Math.*, vol. 11, no. 2, pp. 205–223, 1998.

[44] T. Etzion, *Perfect Codes and Related Structures*, Singapore: World Scientific, 2022.

[45] D. I. Falikman, "Proof of the van der Waerden conjecture regarding the permanent of a doubly stochastic matrix," *Math. Notes*, vol. 29, pp. 475–479, 1981; translation from *Mat. Zametki*, vol. 29, pp. 931–938, 1981.

[46] D. G. Fon-Der-Flaass, "Perfect 2-colorings of a hypercube," *Sib. Math. J.*, vol. 48, no. 4, pp. 740–745, 2007. Translated from *Sib. Mat. Zh.*, vol. 48, no. 4, pp. 923–930, 2007.

[47] D. G. Fon-Der-Flaass, "A bound on correlation immunity," *SEMR*, vol. 4, pp. 133–135, 2007.

[48] E. Friedgut, G. Kalai, "Every monotone graph property has a sharp threshold", *Proceedings of the American Mathematical Society*, vol.124, no. 10, pp. 2993–3002, 1996.

[49] J. Friedman, "On the bit extraction problem," in *Proc. 33rd IEEE Symposium on Foundations of Computer Science*, pp. 314–319, 1992.

[50] S. Glock, D. Kühn, A. Lo, and D. Osthus, "The existence of designs via iterative absorption: hypergraph F-designs for arbitrary F," *Mem. Amer. Math. Soc.*, vol. 284, no. 1406, v+131 pp., 2023.

[51] C. D. Godsil, "Equitable partitions," in *Combinatorics, Paul Erdős is Eighty*, vol. 1, Bolyai Soc. Math. Stud., Budapest: János Bolyai Math. Soc., pp. 173–192, 1993.

[52] C. D. Godsil, *Algebraic Combinatorics*, Chapman and Hall Mathematics Series, New York: Chapman & Hall, 1993.

[53] C. D. Godsil, "Tools from linear algebra," in *Handbook of Combinatorics*, vol. 2, R. L. Graham, M. Grötschel, and L. Lovász, Eds., Amsterdam: Elsevier; Cambridge, MA: MIT Press, pp. 1705–1748, 1995.

[54] C. Godsil, "Compact graphs and equitable partitions," *Linear Algebra and Its Applications*, vol. 255, pp. 259-266, 1997.

[55] C. Godsil and G. Royle, *Algebraic Graph Theory*, Graduate Texts in Mathematics, vol. 207, New York: Springer-Verlag, 2001.

[56] C. Godsil and K. Meagher, *Erdős–Ko–Rado Theorems: Algebraic Approaches*, Cambridge: Cambridge University Press, 2016.

[57] M. J. E. Golay, "Notes on digital coding," *Proc. IRE*, vol. 37, no. 6, p. 657, 1949.

[58] K. Golubev, "Graphical designs and extremal combinatorics," *Linear Alg. Appl.*, vol. 604, pp. 490–506, 2020.

[59] W. H. Haemers, *Eigenvalue Techniques in Design and Graph Theory*, Dissertation, Technische Hogeschool Eindhoven, 1979. Mathematical Centre Tracts, vol. 121, Amsterdam: Mathematisch Centrum, 1980.

[60] W. H. Haemers, "Interlacing eigenvalues and graphs," *Linear Algebra Appl.*, vols. 226–228, pp. 593–616, 1995.

[61] H. Hatami, P. Hatami, and S. Lovett, "Higher-order Fourier analysis and applications," *Foundations and Trends in Theoretical Computer Science*, vol. 13, no. 4, pp. 247–448, 2019.

[62] R. W. Hamming, "Error detecting and error correcting codes," *Bell System Tech. J.*, vol. 29, pp. 147–160, 1950.

[63] R. W. Hamming, *Coding and Information Theory*, Englewood Cliffs, NJ: Prentice-Hall, 1980.

[64] H. Hanani, "On quadruple systems," *Can. J. Math.*, vol. 12, pp. 145–157, 1960.

[65] C. J. Colbourn and J. H. Dinitz, Eds., *Handbook of Combinatorial Designs*, 2nd ed., Discrete Mathematics and Its Applications, Boca Raton, FL: Chapman & Hall/Taylor & Francis, 2007.

[66] K. J. Horadam, *Hadamard matrices and their applications*, Princeton, NJ: Princeton University Press, 263 p., 2007.

[67] A. J. Hoffman, "On eigenvalues and colorings of graphs," in *Graph Theory and Its Applications* (Proc. Advanced Sem., Math. Research Center, Univ. of Wisconsin, Madison, WI, 1969), pp. 79–91, 1970.

[68] H. Huang, B. Xia, and S. Zhou, "Perfect codes in Cayley graphs," *SIAM J. Discrete Math.*, vol. 32, no. 1, pp. 548–559, 2018.

[69] M. Isaev, T. Makai, B. McKay, P. Pralat, J. Tan and M. Zhukovskii "Canonical labelling of random regular graphs," arXiv preprint arXiv:2602.17567, 2026.

[70] L. Ji and J. Yin, "Constructions of new orthogonal arrays and covering arrays of strength three," *J. Combin. Theory Ser. A*, vol. 117, no. 3, pp. 236–247, 2010.

[71] P. Keevash, "The existence of designs II," arXiv preprint arXiv:1802.05900, 2018.

[72] P. Keevash, "A short proof of the existence of designs," arXiv preprint arXiv:2411.18291 , 2024.

[73] S. Kelly, "Constructions of intriguing sets of polar spaces from field reduction and derivation," *Des. Codes Cryptogr.*, vol. 43, no. 1, pp. 1–8, 2007.

[74] A. V. Khalyavin, "Estimates of the capacity of orthogonal arrays of large strength," *Mosc. Univ. Math. Bull.*, vol. 65, no. 3, pp. 130–131, 2010 ; translation from Vest. Mosk. Univ. Mat. Mekh. vol. 65, no. 3, pp. 49-51, 2010.

[75] D. B. Khoroshilova, "On the parameters of perfect 2-colorings of circulant graphs," *Diskretn. Anal. Issled. Oper.*, vol. 18, no. 6, pp. 82–89, 2011 (Russian).

[76] T. E. Kireeva, "Perfect orientation colorings of cubic graphs," *Sib. Èlektron. Mat. Izv.*, vol. 15, pp. 1353–1360, 2018.

[77] J. H. Koolen, W. S. Lee, and W. J. Martin, "Characterizing completely regular codes from an algebraic viewpoint," arXiv preprint arXiv:0911.1828 [math.CO].

[78] D. S. Krotov, "On weight distributions of perfect colorings and completely regular codes," *Des. Codes Cryptogr.*, vol. 61, no. 3, pp. 315–329, 2011.

[79] D. S. Krotov, "On the binary codes with parameters of triply-shortened 1-perfect codes," *Des. Codes Cryptography*, vol. 64, no. 3, pp. 275–283, 2012.

[80] D. S. Krotov, "On calculation of the interweight distribution of an equitable partition," *J. Algebraic Combin.*, vol. 40, no. 2, pp. 373–386, 2014.

[81] D. S. Krotov, I. Yu. Mogilnykh, and V. N. Potapov, "To the theory of q-ary Steiner and other-type trades," *Discrete Mathematics*, vol. 339, no. 3, pp. 1150–1157, 2016.

[82] D. S. Krotov and V. N. Potapov, "Completely regular codes and equitable partitions," in *Completely Regular Codes in Distance-Regular Graphs*, M. Shi and P. Solé, Eds., Boca Raton, FL: Chapman & Hall/CRC, 2025, pp. 1–84.

[83] M. Shi and P. Solé, Eds., *Completely Regular Codes in Distance-Regular Graphs*, Boca Raton, FL: Chapman & Hall/CRC, 2025.

[84] C. W. H. Lam, G. Kolesova, and L. Thiel, "A computer search for finite projective planes of order 9," *Discrete Math.*, vol. 92, no. 1–3, pp. 187–195, 1991.

[85] C. W. H. Lam, L. Thiel, and S. Swiercz, "The nonexistence of finite projective planes of order 10," *Canad. J. Math.*, vol. 41, no. 6, pp. 1117–1123, 1989.

[86] F. T. Leighton, "Finite common coverings of graphs," *J. Combin. Theory Ser. B*, vol. 33, no. 3, pp. 231–238, 1982.

[87] S. Lang, *Algebra*, Graduate Texts in Mathematics, vol. 211, rev. 3rd ed., New York: Springer-Verlag, 2002.

[88] V. I. Levenshtein, "Universal bounds for codes and designs," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Amsterdam: Elsevier, 1998, ch. 6, pp. 499–648.

[89] N. Linial and Z. Luria, "On the vertices of the d-dimensional Birkhoff polytope." *Discrete Comput. Geom.*, vol. 51, no. 1, pp. 161–170, 2014.

[90] J. H. van Lint, "A survey of perfect codes," *Rocky Mt. J. Math.*, vol. 5, pp. 199–224, 1975.

[91] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed., Cambridge: Cambridge University Press, 2001.

[92] J. H. van Lint, *Introduction to Coding Theory*, 3rd ed., Graduate Texts in Mathematics, vol. 86, Berlin: Springer-Verlag, 1999.

[93] M. A. Lisitsyna and S. V. Avgustinovich, "Perfect colorings of the prism graph," *Sib. Èlektron. Mat. Izv.*, vol. 13, pp. 1116–1128, 2016.

[94] S. P. Lloyd, "Binary block coding," *Bell Syst. Tech. J.*, vol. 36, no. 2, pp. 517–535, 1957.

[95] M. S. Lobanov, "Exact relation between nonlinearity and algebraic immunity," *Discrete Math. Appl.*, vol. 16, no. 5, pp. 453–460, 2006. Translated from *Diskretn. Mat.*, vol. 18, no. 3, pp. 152–159, 2006.

[96] O. A. Logachev, A. A. Salnikov, and V. V. Yashchenko, *Boolean Functions in Coding Theory and Cryptography*, Translations of Mathematical Monographs, vol. 241, Providence, RI: American Mathematical Society, 2012. Translated from Russian by S. Nikova.

[97] L. Lovász, *Combinatorial Problems and Exercises*, corrected reprint of the 1993 2nd ed., Providence, RI: AMS Chelsea Publishing, 2007.

[98] S. L. Ma, "A survey of partial difference sets," *Des. Codes Cryptography*, vol. 4, pp. 221–261, 1994.

[99] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Parts I and II, North-Holland Mathematical Library, vol. 16, Amsterdam: North-Holland, 1977.

[100] A. A. Markov, Jr., *Selected Works*, Vol. II: *Theory of Algorithms and Constructive Mathematics. Mathematical Logic. Information Science and Related Questions*, 2003 (Russian).

[101] W. J. Martin, *Completely Regular Subsets*, Ph.D. thesis, University of Waterloo, 1992.

[102] W. J. Martin, "Completely regular designs," *J. Combin. Des.*, vol. 4, pp. 261–273, 1998.

[103] S. Mesnager, *Bent Functions: Fundamentals and Results*, Cham: Springer, 2016.

[104] B. D. McKay, "Practical graph isomorphism," in *Proceedings of the 10th Manitoba Conference*, Winnipeg/Manitoba, 1980, Congressus Numerantium, vol. 30, pp. 45–87, Winnipeg, MB: Combinatorial Press, 1981.

[105] B. D. McKay and I. M. Wanless, "A census of small Latin hypercubes," *SIAM J. Discrete Math.*, vol. 22, pp. 719–736, 2008.

[106] S. M. Mirafzal, M. Ziaee, "A note on the automorphism group of the Hamming graph," *Trans. Comb.*, vol. 10, no. 2, pp. 129–136, 2021.

[107] I. Yu. Mogilnykh, "Perfect codes from PGL(2,5) in star graphs," *Sib. Èlektron. Mat. Izv.*, vol. 17, pp. 534–539, 2020.

[108] I. Yu. Mogilnykh, "Completely regular codes in Johnson and Grassmann graphs with small covering radii," *Electron. J. Comb.*, vol. 29, no. 2, Paper No. P2.57, 15 p. 2022.

[109] R. Montgomery, "A proof of the Ryser–Brualdi–Stein conjecture for large even n," arXiv:2310.19779.

[110] H. L. Morgan, "The generation of a unique machine description for chemical structures: A technique developed at Chemical Abstracts Service," *J. Chem. Doc.*, vol. 5, no. 2, pp. 107–113, 1965.

[111] S. A. Morris, *Pontryagin Duality and the Structure of Locally Compact Abelian Groups*, London Mathematical Society Lecture Note Series, vol. 29, Cambridge: Cambridge University Press, 1977.

[112] N. Nisan and M. Szegedy, "On the degree of Boolean functions as real polynomials," *Comput. Complexity*, vol. 4, no. 4, pp. 301–313, 1994. Special issue on circuit complexity (Barbados, 1992).

[113] P. R. J. Östergård, O. Pottonen, and K. T. Phelps, "The perfect binary one-error-correcting codes of length 15: Part II – Properties," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2571–2582, 2010.

[114] O. G. Parshina and M. A. Lisitsyna, "The perfect 2-colorings of infinite circulant graphs with a continuous set of odd distances," *Sib. Electron. Math. Reports*, vol. 17, pp. 590–603, 2020.

[115] A. L. Perezhogin, V. N. Potapov, S. Yu. Vladimirov, "Every latin hypercube of order 5 has transversals," *Journal of Combinatorial designs*, vol. 32, no. 11, 679–699, 2024.

[116] F. P. Preparata, "A class of optimum nonlinear double-error-correcting codes," *Inform. and Control*, vol. 13, pp. 378–400, 1968.

[117] V. N. Potapov, "On perfect 2-colorings of the q-ary n-cube," *Discrete Math.*, vol. 312, no. 6, pp. 1269–1272, 2012.

[118] V. N. Potapov and S. V. Avgustinovich, "Combinatorial designs, difference sets, and bent functions as perfect colorings of graphs and multigraphs," E-print 2403.02904, arXiv.org, 2024.

[119] V. N. Potapov, "Embedding in MDS codes and Latin cubes," *J. Comb. Des.*, vol. 30, no. 9, pp. 626-633, 2022.

[120] V. N. Potapov and A. A. Taranenko, "Asymptotic bounds on the numbers of vertices of polytopes of polystochastic matrices," *Discrete Math.*, 349, No. 1, Article ID 114653, 7 p. 2026.

[121] S. A. Puzynina, "Periodicity of perfect colourings of an infinite rectangular grid," *Diskretn. Anal. Issled. Oper., Ser. 1*, vol. 11, no. 1, pp. 79–92, 2004 (Russian).

[122] R. C. Rao, "Factorial experiments derivable from combinatorial arrangements of arrays," *Suppl. J. Roy. Statist. Soc.*, vol. 9, pp. 128–139, 1947.

[123] H. Reiter and J. D. Stegeman, *Classical Harmonic Analysis and Locally Compact Groups*, 2nd ed., London Mathematical Society Monographs, New Series, vol. 22, Oxford: Clarendon Press, 2000.

[124] A. Rosa, *Combinatorial Designs with Applications*, Notes, Banská Bystrica: Belianum, 2015.

[125] R. M. Roth, "Higher-order MDS codes," *IEEE Trans. Inf. Theory*, vol. 68, no. 12, pp. 7798–7816, 2022.

[126] O. S. Rothaus, "On 'bent' functions," *J. Combin. Theory, Ser. A*, vol. 20, no. 3, pp. 300–305, 1976.

[127] V. G. Ryabov, "Approximation of restrictions of q-valued logic functions to linear manifolds by affine analogues," *Diskr. Mat.*, vol. 32, no. 4, pp. 89–102, 2020. English translation: *Discrete Math. Appl.*, vol. 31, no. 6, pp. 409–419, 2021.

[128] V. G. Ryabov, "Criteria for maximal nonlinearity of a function over a finite field," *Diskr. Mat.*, vol. 33, no. 3, pp. 79–91, 2021. English translation: *Discrete Math. Appl.*, vol. 33, no. 2, pp. 117–126, 2023.

[129] P. Sarkar, "Spectral domain analysis of correlation immune and resilient Boolean functions," *Cryptology ePrint Archive*, Report 2000/049, September 2000.

[130] P. Sarkar and S. Maitra, "Nonlinearity Bounds and Constructions of Resilient Boolean Functions," *Proceedings of CRYPTO 2000, Lecture Notes in Computer Science,* vol. 1880, pp. 515–532, 2000.

[131] H. S. Shapiro and D. L. Slotnick, "On the mathematical theory of error-correcting codes," *IBM J. Res. Develop.*, vol. 3, pp. 25–34, 1959.

[132] Th. Skolem, "Some remarks on the triple systems of Steiner," *Math. Scand.*, vol. 6, pp. 273–280, 1958.

[133] F. I. Solov'eva, *On Perfect Codes and Related Topics*, Lecture Notes, Pohang University of Science and Technology, 2004.

[134] E. Sotnikova and A. Valyuzhenich, "Minimum supports of eigenfunctions of graphs: a survey," *The Art of Discrete and Applied Mathematics*. DOI: 10.26493/2590-9770.1404.61e.

[135] R. M. Tanner, "Explicit concentrators from generalized n-gons," *SIAM J. Algebraic Discrete Methods*, vol. 5, no. 3, pp. 287–293, 1984.

[136] T. Tao, "An uncertainty principle for cyclic groups of prime order," *Math. Res. Lett.*, vol. 12, no. 1, pp. 121–127, 2005.

[137] T. Tao, *Higher Order Fourier Analysis*, vol. 142, Providence, RI: American Mathematical Society, 2012.

[138] A. A. Taranenko, "Transversals in completely reducible multiary quasigroups and in multiary quasigroups of order 4," *Discrete Math.*, vol. 341, pp. 405–420, 2018.

[139] A. A. Taranenko, "Algebraic properties of perfect structures," *Linear Algebra Appl.*, vol. 607, pp. 286–306, 2020.

[140] A. A. Taranenko, "Perfect colourings of hypergraphs," *Linear Multilinear Algebra*, vol. 73, no. 8, pp. 1566–1590, 2025.

[141] Y. Tarannikov, "On resilient Boolean functions with maximal possible nonlinearity," in *Progress in Cryptology – INDOCRYPT 2000* (Calcutta), Lecture Notes in Computer Science, vol. 1977, Berlin: Springer, pp. 19–30, 2000.

[142] Yu. V. Tarannikov, "On correlation-immune and stable Boolean functions," *Mat. Vopr. Kibern.* vol.11, pp. 91-148, 2002 (Russian).

[143] A. Tietäväinen, "On the nonexistence of perfect codes over finite fields," *SIAM J. Appl. Math.*, vol. 24, pp. 88–96, 1973.

[144] R. Titsworth. *Correlation properties of cyclic sequences*, PhD thesis, California Institute of Technology, 1963.

[145] N. Tokareva, *Bent Functions: Results and Applications to Cryptography*, Amsterdam: Elsevier/Academic Press, 2015.

[146] M. Tsfasman, S. Vlăduţ, and D. Nogin, *Algebraic Geometric Codes: Basic Notions*, Mathematical Surveys and Monographs, vol. 139, Providence, RI: American Mathematical Society, 2007.

[147] A.A. Valyuzhenich, K.V. Vorob'ev, "Minimum supports of functions on the Hamming graphs with spectral constraints," *Discrete Math.*, vol. 342, pp. 1351–1360, 2019.

[148] A. Valyuzhenich, "An upper bound on the number of relevant variables for Boolean functions on the Hamming graph,' *Discrete Math.* vol. 349, no. 2, Article ID 114745, 6 p., 2026.

[149] A. Yu. Vasil'eva, "Local and interweight spectra of completely regular codes and of perfect colorings," *Probl. Inf. Transm.*, vol. 45, no. 2, pp.

151–157, 2009. Translated from *Probl. Peredachi Inf.*, vol. 45, no. 2, pp. 84–90, 2009.

[150] A. Yu. Vasil'eva, "On reconstructive sets of vertices in the Boolean cube," *J. Appl. Ind. Math.*, vol. 6, no. 3, pp. 393–402, 2012.

[151] A. Yu. Vasil'eva, "Reconstruction of eigenfunctions of a q-ary n-dimensional hypercube," *Probl. Inf. Transm.*, vol. 51, no. 3, pp. 231–239, 2015. Translated from *Probl. Peredachi Inf.*, vol. 51, no. 3, pp. 31–40, 2015.

[152] Yu. L. Vasil'ev, "On closely-packed nongroup codes," *Probl. Kibern.*, vol. 8, pp. 337–339, 1962. German translation: *Probl. Kybernetik*, vol. 8, pp. 375–378, 1965.

[153] V. G. Vizing, "On an estimate of the chromatic class of a p-graph," *Diskret. Analiz*, Novosibirsk, vol. 3, pp. 25–30, 1964 (Russian).

[154] V. G. Vizing, "Distributive coloring of graph vertices," *Diskretn. Anal. Issled. Oper.*, vol. 2, no. 4, pp. 3–12, 1995 (Russian).

[155] I. M. Wanless, Transversals in Latin squares: a survey. Surveys in combinatorics 2011, 403-437, London Math. Soc. Lecture Note Ser., 392, Cambridge Univ. Press, Cambridge, 2011.

[156] I. Wegener, *The complexity of Boolean functions.* Wiley-Teubner Series in Computer Science. John Wiley & Sons, Ltd., Chichester; B. G. Teubner, Stuttgart, 1987. xii+457.

[157] B. Yu. Weisfeiler and A. A. Leman. "The reduction of a graph to canonical form and the algebra which appears therein." *Nauchno-Technicheskaya Informatsia*, vol. 2, no 9. pp. 12–16, 1968. (Russian)

[158] J. Wellens, "Relationships between the number of inputs and other complexity measures of Boolean functions," *Discrete Analysis*, 19–21 pp. 2022, arXiv:2005.00566v2

[159] R. M. Wilson, "An existence theory for pairwise balanced designs. III. Proof of the existence conjectures.," *J. Combinatorial Theory Ser. A*, vol. 18. pp. 71-79. 1975.

[160] Y. Zheng and X.-M. Zhang, "Improving upper bound on the nonlinearity of high order correlation immune functions," *Proceedings of Selected Areas in Cryptography 2000, Lecture Notes in Computer Science,* vol. 2012, pp. 262–274, 2001.

[161] V. A. Zinov'ev, V. K. Leont'ev, "On perfect codes," *Probl. Peredaci Inform.* vol 8, mo. 1, pp. 26-35, 1972. (Russian)

[162] V. A. Zinov'ev, V. K. Leont'ev, "On non-existence of perfect codes over Galois fields," *Probl. Control Inf. Theory,* vol. 2, no. 2, pp.16–24. 1973; translation from Probl. Upravl. Teor. Inform. vol. 2, no. 2, pp. 123–132, 1973.