Perfect codes in Doob graphs

Denis Krotov
Sobolev Institute of Mathematics
Novosibirsk, Russia

Graphs and Groups, Cycles and Coverings (G2C2)
Novosibirsk, 2014

Outline

- Definitions (Doob graph, perfect codes)
- Doob graphs: the structure of a module over the ring $\mathrm{GR}(4^2)$ of $\mathbb{Z}_4$.
- Linear and additive codes; restrictions on the parameters
- Constructions

Outline

- Definitions (Doob graph, perfect codes)
- Doob graphs: the structure of a module over the ring $\mathrm{GR}(4^2)$ of $\mathbb{Z}_4$.
- Linear and additive codes; restrictions on the parameters
- Constructions

Outline

- Definitions (Doob graph, perfect codes)
- Doob graphs: the structure of a module over the ring $\mathrm{GR}(4^2)$ of $\mathbb{Z}_4$.
- Linear and additive codes; restrictions on the parameters
- Constructions

Outline

- Definitions (Doob graph, perfect codes)
- Doob graphs: the structure of a module over the ring $\mathrm{GR}(4^2)$ of $\mathbb{Z}_4$.
- Linear and additive codes; restrictions on the parameters
- Constructions

Distance-regular graphs

- A connected regular graph is called distance regular if every bipartite subgraph generated (as parts) by two cocentered spheres of different radius is biregular.
- In other words, a distance-regular graph is a regular graph G for which there exist integers b_i, c_i, $i = 0, \dots, d$ such that for any two vertices x, y in G and distance $i = d(x, y)$, there are exactly c_i neighbors of y in $G_{i-1}(x)$ and b_i neighbors of y in $G_{i+1}(x)$, where $G_i(x)$ is the set of vertices y of G with $d(x, y) = i$
[Brouwer et al. Distance Regular Graphs. p. 434].

Distance-regular graphs

- A connected regular graph is called distance regular if every bipartite subgraph generated (as parts) by two cocentered spheres of different radius is biregular.
- In other words, a distance-regular graph is a regular graph G for which there exist integers b_i, c_i, $i = 0, ..., d$ such that for any two vertices x, y in G and distance $i = d(x, y)$, there are exactly c_i neighbors of y in $G_{i-1}(x)$ and b_i neighbors of y in $G_{i+1}(x)$, where $G_i(x)$ is the set of vertices y of G with $d(x, y) = i$
  [Brouwer et al. Distance Regular Graphs. p. 434].

Perfect codes

- A set of vertices of a graph or any other discrete metric space is called an e-perfect code (perfect e-error-correction code), or simply a perfect code, if the vertex set is partitioned into the radius-e balls centered in the code vertices.
- The codes of cardinality 1 and the 0-perfect codes are called trivial perfect codes.

Perfect codes

- A set of vertices of a graph or any other discrete metric space is called an e-perfect code (perfect e-error-correction code), or simply a perfect code, if the vertex set is partitioned into the radius-e balls centered in the code vertices.
- The codes of cardinality 1 and the 0-perfect codes are called trivial perfect codes.

Perfect codes in Distance-gerular graphs

- The perfect codes in distance regular graphs are objects that are highly interesting from the point of view of both coding theory and algebraic combinatorics.
- On one hand, these codes are error correcting codes that attain the sphere-packing bound ("perfect" means "extremely good").
- On the other hand, they possess algebraic properties that are connected with the algebraic properties of the distance regular graph; a perfect code is a some kind of divisor [Cvetkovic et al. Spectra of Graphs: Theory and Application. 1980. Chapter 4] of the graph.

Perfect codes in Distance-gerular graphs

- The perfect codes in distance regular graphs are objects that are highly interesting from the point of view of both coding theory and algebraic combinatorics.
- On one hand, these codes are error correcting codes that attain the sphere-packing bound ("perfect" means "extremely good").
- On the other hand, they possess algebraic properties that are connected with the algebraic properties of the distance regular graph; a perfect code is a some kind of divisor [Cvetkovic et al. Spectra of Graphs: Theory and Application. 1980. Chapter 4] of the graph.

Perfect codes in Distance-gerular graphs

- The perfect codes in distance regular graphs are objects that are highly interesting from the point of view of both coding theory and algebraic combinatorics.
- On one hand, these codes are error correcting codes that attain the sphere-packing bound ("perfect" means "extremely good").
- On the other hand, they possess algebraic properties that are connected with the algebraic properties of the distance regular graph; a perfect code is a some kind of divisor [Cvetkovic et al. Spectra of Graphs: Theory and Application. 1980. Chapter 4] of the graph.

- It may safely be said that the most important class of distance regular graphs, for coding theory, is the Hamming graphs.
- The Hamming graph $H(n, q)$ is the Cartesian product of n copies of the complete graph K_q of order q.
- It is usual to consider the n-tuples ($=$ words of length n) over the Galois field $\mathrm{GF}(q)$ as the vertices of $H(n, q)$.
- The n-tuples form a vector space over $\mathrm{GF}(q)$.
- A subspace is called a linear code. A linear code can be defined by a basis (generator matrix) or by a basis of the dual subspace (check matrix).

- It may safely be said that the most important class of distance regular graphs, for coding theory, is the Hamming graphs.
- The Hamming graph $H(n, q)$ is the Cartesian product of n copies of the complete graph K_q of order q.
- It is usual to consider the n-tuples (= words of length n) over the Galois field GF(q) as the vertices of $H(n, q)$.
- The n-tuples form a vector space over GF(q).
- A subspace is called a linear code. A linear code can be defined by a basis (generator matrix) or by a basis of the dual subspace (check matrix).

- It may safely be said that the most important class of distance regular graphs, for coding theory, is the Hamming graphs.
- The Hamming graph $H(n, q)$ is the Cartesian product of n copies of the complete graph K_q of order q.
- It is usual to consider the n-tuples (= words of length n) over the Galois field $\mathrm{GF}(q)$ as the vertices of $H(n, q)$.
- The n-tuples form a vector space over $\mathrm{GF}(q)$.
- A subspace is called a linear code. A linear code can be defined by a basis (generator matrix) or by a basis of the dual subspace (check matrix).

- It may safely be said that the most important class of distance regular graphs, for coding theory, is the Hamming graphs.
- The Hamming graph $H(n, q)$ is the Cartesian product of n copies of the complete graph K_q of order q.
- It is usual to consider the n-tuples ($=$ words of length n) over the Galois field $\mathrm{GF}(q)$ as the vertices of $H(n, q)$.
- The n-tuples form a vector space over $\mathrm{GF}(q)$.
- A subspace is called a linear code. A linear code can be defined by a basis (generator matrix) or by a basis of the dual subspace (check matrix).

- It may safely be said that the most important class of distance regular graphs, for coding theory, is the Hamming graphs.
- The Hamming graph $H(n, q)$ is the Cartesian product of n copies of the complete graph K_q of order q.
- It is usual to consider the n-tuples ($=$ words of length n) over the Galois field $\mathrm{GF}(q)$ as the vertices of $H(n, q)$.
- The n-tuples form a vector space over $\mathrm{GF}(q)$.
- A subspace is called a linear code. A linear code can be defined by a basis (generator matrix) or by a basis of the dual subspace (check matrix).

Perfect codes in Hamming graphs

- For the Hamming graphs $H(n, q)$, the study of possible parameters of perfect codes is completed only if q is a prime power [Zinoviev, Leontiev, 1973 and Tietavainen, 1973].
  - 1-perfect codes in $H(\frac{q^m-1}{q-1}, q)$ (the Hamming codes and the codes with parameters of Hamming codes)

$$\text{check matrix: } \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix};$$

  - 3-perfect binary Golay code in $H(23, 2)$;
  - 2-perfect ternary Golay code in $H(11, 3)$;
  - binary repetition code in $H(2e+1, 2)$: $\{000...0, 111...1\}$
- If q is not a prime power (6, 10, 12, 14, 15, ...), the problem of existence 1-perfect and (for some q) 2-perfect codes is open.

Perfect codes in Hamming graphs

- For the Hamming graphs $H(n, q)$, the study of possible parameters of perfect codes is completed only if q is a prime power [Zinoviev, Leontiev, 1973 and Tietavainen, 1973].
  - 1-perfect codes in $H(\frac{q^m-1}{q-1}, q)$ (the Hamming codes and the codes with parameters of Hamming codes)

    check matrix: $\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$;
  - 3-perfect binary Golay code in $H(23, 2)$;
  - 2-perfect ternary Golay code in $H(11, 3)$;
  - binary repetition code in $H(2e+1, 2)$: $\{000...0, 111...1\}$
- If q is not a prime power (6, 10, 12, 14, 15, ...), the problem of existence 1-perfect and (for some q) 2-perfect codes is open.

Perfect codes in Hamming graphs

- For the Hamming graphs $H(n, q)$, the study of possible parameters of perfect codes is completed only if q is a prime power [Zinoviev, Leontiev, 1973 and Tietavainen, 1973].
  - 1-perfect codes in $H(\frac{q^m-1}{q-1}, q)$ (the Hamming codes and the codes with parameters of Hamming codes)

    check matrix: $\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$;

  - 3-perfect binary Golay code in $H(23, 2)$;
  - 2-perfect ternary Golay code in $H(11, 3)$;
  - binary repetition code in $H(2e+1, 2)$: $\{000...0, 111...1\}$
- If q is not a prime power (6, 10, 12, 14, 15, . . .), the problem of existence 1-perfect and (for some q) 2-perfect codes is open.

Perfect codes in Hamming graphs

- For the Hamming graphs $H(n, q)$, the study of possible parameters of perfect codes is completed only if q is a prime power [Zinoviev, Leontiev, 1973 and Tietavainen, 1973].
  - 1-perfect codes in $H(\frac{q^m-1}{q-1}, q)$ (the Hamming codes and the codes with parameters of Hamming codes)

    check matrix: $\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$;

  - 3-perfect binary Golay code in $H(23, 2)$;
  - 2-perfect ternary Golay code in $H(11, 3)$;
  - binary repetition code in $H(2e+1, 2)$: $\{000...0, 111...1\}$
- If q is not a prime power (6, 10, 12, 14, 15, ...), the problem of existence 1-perfect and (for some q) 2-perfect codes is open.

Perfect codes in Hamming graphs

- For the Hamming graphs $H(n, q)$, the study of possible parameters of perfect codes is completed only if q is a prime power [Zinoviev, Leontiev, 1973 and Tietavainen, 1973].
  - 1-perfect codes in $H(\frac{q^m-1}{q-1}, q)$ (the Hamming codes and the codes with parameters of Hamming codes)

$$\text{check matrix: } \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix};$$

  - 3-perfect binary Golay code in $H(23, 2)$;
  - 2-perfect ternary Golay code in $H(11, 3)$;
  - binary repetition code in $H(2e+1, 2)$: $\{000...0, 111...1\}$
- If q is not a prime power (6, 10, 12, 14, 15, ...), the problem of existence 1-perfect and (for some q) 2-perfect codes is open.

Perfect codes in Hamming graphs

- For the Hamming graphs $H(n, q)$, the study of possible parameters of perfect codes is completed only if q is a prime power [Zinoviev, Leontiev, 1973 and Tietavainen, 1973].
  - 1-perfect codes in $H(\frac{q^m-1}{q-1}, q)$ (the Hamming codes and the codes with parameters of Hamming codes)

$$\text{check matrix:} \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix};$$

  - 3-perfect binary Golay code in $H(23, 2)$;
  - 2-perfect ternary Golay code in $H(11, 3)$;
  - binary repetition code in $H(2e+1, 2)$: $\{000...0, 111...1\}$
- If q is not a prime power (6, 10, 12, 14, 15, . . .), the problem of existence 1-perfect and (for some q) 2-perfect codes is open.

Correspondence

Notes on Digital Coding*

The consideration of message coding as a means for approaching the theoretical capacity of a communication channel, while reducing the probability of errors, has suggested the interesting number theoretical problem of devising lossless binary (or other) coding schemes serving to insure the reception of a correct, but reduced, message when an upper limit to the number of transmission errors is postulated.

An example of lossless binary coding is treated by Shannon[1] who considers the case of blocks of seven symbols, one or none of which can be in error. The solution of this case can be extended to blocks of 2^n-1-binary symbols, and, more generally, when coding schemes based on the prime number p are employed, to blocks of $p^n-1/p-1$ symbols which are transmitted, and received with complete equivocation of one or no symbol, each block comprising n redundant symbols designed to remove the equivocation. When encoding the message, the n redundant symbols x_m are determined in terms of the message symbols Y_k from the congruent relations

$$E_m \equiv X_m + \sum_{k=1}^{k=(p^n-1)/(p-1)-n} a_{mk} Y_k \equiv 0 \pmod{p}.$$

In the decoding process, the E's are recalculated with the received symbols, and their ensemble forms a number on the base p which determines univocally the mistransmitted symbol and its correction.

In passing from n to $n+1$, the matrix with n rows and $p^n-1/p-1$ columns formed with the coefficients of the X's and Y's in the expression above is repeated p times horizontally, while an $(n+1)$ st row added, consisting of $p^n-1/p-1$ zeroes, followed by as many one's etc. up to $p-1$; an added column of n zeroes with a one for the lowest term completes the new matrix for $n+1$.

If we except the trivial case of blocks of $2S+1$ binary symbols, of which any group comprising up to S symbols can be received in error which equal probability, it does not appear that a search for lossless coding schemes, in which the number of errors is limited but larger than one, can be systematized so as to yield a family of solutions. A necessary but not sufficient condition for the existence of such a lossless coding scheme in the binary system is the existence of three or more first numbers of a line of Pascal's triangle which add up to an exact power of 2. A limited search has revealed two such cases; namely, that of the first three numbers of the 90th line, which add up to 2^{12} and that of the first four numbers of the 23rd line, which add up to 2^{11}. The first case does not correspond to a lossless coding scheme, for, were such a scheme to exist, we could designate by r the number of E_m ensembles corresponding to one error and having an odd number of 1's and by $90-r$ the remaining (even) ensembles. The odd ensembles corresponding to two transmission errors could be formed by re-entering term by term all the conbinations of one even and one odd ensemble corresponding each to one error, and would number $r(90-r)$. We should have $r+r(90-r)=2^{11}$, which is impossible for integral values of r.

On the other side, the second case can be coded so as to yield 12 sure symbols, and the a_{mk} matrix of this case is given in Table I. A second matrix is also given, which is that of the only other lossless coding scheme encountered (in addition to the general class mentioned above) in which blocks of eleven ternary symbols are transmitted with no more than 2 errors, and out of which six sure symbols can be obtained.

It must be mentioned that the use of the ternary coding scheme just mentioned will always result in a power loss, whereas the coding scheme for 23 binary symbols and a maximum of three transmission errors yields a power saving of $1\frac{1}{2}$ db for vanishing probabilities of errors. The saving realized with the coding scheme for blocks of 2^n-1 binary symbols approaches 3 db for increasing n's and decreasing probabilities of error, but a loss is always encountered when $n=3$.

MARCEL J. E. GOLAY
Signal Corps Engineering Laboratories
Fort Monmouth, N. J

TABLE I

	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}	Y_{12}
X_1	1	0	0	1	1	1	0	0	0	1	1	1
X_2	1	0	1	0	1	1	0	1	1	0	0	1
X_3	1	0	1	1	0	1	1	0	1	0	1	0
X_4	1	0	1	1	1	0	1	1	0	1	0	0
X_5	1	1	0	0	1	1	1	0	1	1	0	0
X_6	1	1	0	1	0	1	1	1	0	0	0	1
X_7	1	1	0	1	1	0	0	1	1	0	1	0
X_8	1	1	1	0	0	1	0	1	0	1	1	0
X_9	1	1	1	0	1	0	1	0	0	0	1	1
X_{10}	1	1	1	1	0	0	0	0	1	1	0	1
X_{11}	0	1	1	1	1	1	1	1	1	1	1	1

	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6
X_1	1	1	1	2	2	0
X_2	1	1	2	1	0	2
X_3	1	2	1	0	1	2
X_4	1	2	0	1	2	1
X_5	1	0	2	2	1	1

* Received by the Institute, February 23, 1949.

[1] C. E. Shannon, "A mathematical theory of communication," *Bell Sys. Tech. Jour.*, vol. 27, p. 418; July, 1948.

The Doob graphs

- The Doob graph $D(m, n)$ is a distance regular graph of diameter $2m + n$ with the same parameters as the Hamming graph $H(2m + n, 4)$.
- The Doob graph $D(m, n)$ is the Cartesian product of m copies of the Shrikhande graph Sh and n copies of the full graph $K = K_4$ of order 4.

The Doob graphs

- The Doob graph $D(m, n)$ is a distance regular graph of diameter $2m + n$ with the same parameters as the Hamming graph $H(2m + n, 4)$.
- The Doob graph $D(m, n)$ is the Cartesian product of m copies of the Shrikhande graph Sh and n copies of the full graph $K = K_4$ of order 4.

Perfect codes in Doob graphs

- As noted in [Koolen, Munemasa, 2000], nontrivial e-perfect codes in $D(m,n)$ can only exist when $e=1$ and $2m+n=(4^\mu-1)/3$ for some integer μ (with exactly the same proof as for $H(2m+n,4)$).
- Koolen and Munemasa constructed 1-perfect codes in the Doob graphs of diameter 5 (i.e., $D(1,3)$ and $D(2,1)$).
- In the current work:
- Restrictions on the parameters of linear 1-perfect codes in $D(m,n)$
- Construction of linear codes in $D(m,n)$ with the structure of $(\mathrm{GR}(4^2))^m \times (\mathrm{GF}(2^2))^n$.
- Construction of linear codes in $D(m,n'+n'')$ with the structure of $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$.

Perfect codes in Doob graphs

- As noted in [Koolen, Munemasa, 2000], nontrivial e-perfect codes in $D(m,n)$ can only exist when $e = 1$ and $2m + n = (4^\mu - 1)/3$ for some integer μ (with exactly the same proof as for $H(2m + n, 4)$).
- Koolen and Munemasa constructed 1-perfect codes in the Doob graphs of diameter 5 (i.e., $D(1,3)$ and $D(2,1)$).
- In the current work:
- Restrictions on the parameters of linear 1-perfect codes in $D(m,n)$
- Construction of linear codes in $D(m,n)$ with the structure of $(\mathrm{GR}(4^2))^m \times (\mathrm{GF}(2^2))^n$.
- Construction of linear codes in $D(m, n' + n'')$ with the structure of $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$.

Perfect codes in Doob graphs

- As noted in [Koolen, Munemasa, 2000], nontrivial *e*-perfect codes in $D(m, n)$ can only exist when $e = 1$ and $2m + n = (4^{\mu} - 1)/3$ for some integer μ (with exactly the same proof as for $H(2m + n, 4)$).
- Koolen and Munemasa constructed 1-perfect codes in the Doob graphs of diameter 5 (i.e., $D(1, 3)$ and $D(2, 1)$).
- In the current work:
- Restrictions on the parameters of linear 1-perfect codes in $D(m, n)$
- Construction of linear codes in $D(m, n)$ with the structure of $(\mathrm{GR}(4^2))^m \times (\mathrm{GF}(2^2))^n$.
- Construction of linear codes in $D(m, n' + n'')$ with the structure of $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$.

Perfect codes in Doob graphs

- As noted in [Koolen, Munemasa, 2000], nontrivial e-perfect codes in $D(m, n)$ can only exist when $e = 1$ and $2m + n = (4^\mu - 1)/3$ for some integer μ (with exactly the same proof as for $H(2m + n, 4)$).
- Koolen and Munemasa constructed 1-perfect codes in the Doob graphs of diameter 5 (i.e., $D(1, 3)$ and $D(2, 1)$).
- In the current work:
- Restrictions on the parameters of linear 1-perfect codes in $D(m, n)$
- Construction of linear codes in $D(m, n)$ with the structure of $(\mathrm{GR}(4^2))^m \times (\mathrm{GF}(2^2))^n$.
- Construction of linear codes in $D(m, n' + n'')$ with the structure of $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$.

Perfect codes in Doob graphs

- As noted in [Koolen, Munemasa, 2000], nontrivial e-perfect codes in $D(m,n)$ can only exist when $e=1$ and $2m+n=(4^{\mu}-1)/3$ for some integer μ (with exactly the same proof as for $H(2m+n,4)$).
- Koolen and Munemasa constructed 1-perfect codes in the Doob graphs of diameter 5 (i.e., $D(1,3)$ and $D(2,1)$).
- In the current work:
- Restrictions on the parameters of linear 1-perfect codes in $D(m,n)$
- Construction of linear codes in $D(m,n)$ with the structure of $(\mathrm{GR}(4^2))^m \times (\mathrm{GF}(2^2))^n$.
- Construction of linear codes in $D(m,n'+n'')$ with the structure of $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$.

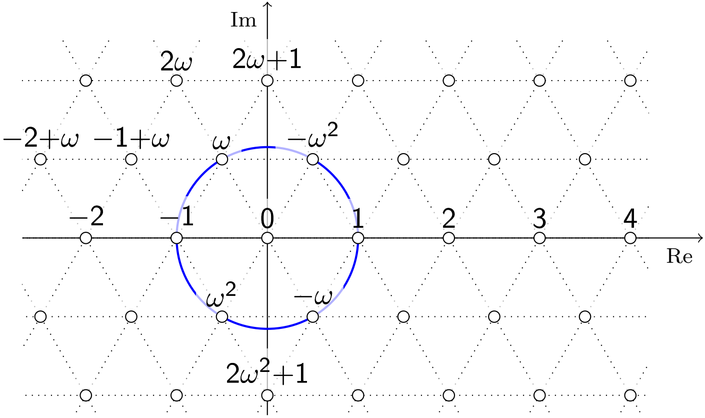
Perfect codes in Doob graphs

- As noted in [Koolen, Munemasa, 2000], nontrivial e-perfect codes in $D(m,n)$ can only exist when $e=1$ and $2m+n=(4^{\mu}-1)/3$ for some integer μ (with exactly the same proof as for $H(2m+n,4)$).
- Koolen and Munemasa constructed 1-perfect codes in the Doob graphs of diameter 5 (i.e., $D(1,3)$ and $D(2,1)$).
- <u>In the current work:</u>
- Restrictions on the parameters of linear 1-perfect codes in $D(m,n)$
- Construction of linear codes in $D(m,n)$ with the structure of $(\mathrm{GR}(4^2))^m \times (\mathrm{GF}(2^2))^n$.
- Construction of linear codes in $D(m,n'+n'')$ with the structure of $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$.

Eisenstein integers

- The Eisenstein integers $\mathbb{E}$ are the complex numbers of the form

$$z = a + b\omega, \qquad \omega = \frac{-1 + i\sqrt{3}}{2} = e^{2\pi i/3}, \quad a, b \in \mathbb{Z}.$$



Eisenstein integers modulo 2 or 4

- Given $p \in \mathbb{E} \backslash \{0\}$, we denote by $\mathbb{E}_p$ the ring $\mathbb{E}/p\mathbb{E}$ of residue classes of $\mathbb{E}$ modulo p.
- We are interested in: $\mathbb{E}_2 \simeq \mathrm{GF}(2^2)$ and $\mathbb{E}_4 \simeq \mathrm{GR}(4^2)$
- Each of 16 elements of $\mathbb{E}_4$ can be uniquely represented in the form $2a + b$ where $a, b \in \{0, 1, \omega, \omega^2\}$.
- $\mathcal{E} = \{-\omega^2, \omega, -1, \omega^2, -\omega, 1\}$ is the set of units.
- The elements of $\mathbb{E}_4$ are partitioned into $0\mathcal{E}$, $\mathcal{E}$, $2\mathcal{E}$, and $\psi\mathcal{E}$ where $\psi = 2 + \omega$.

Eisenstein integers modulo 2 or 4

- Given $p \in \mathbb{E} \backslash \{0\}$, we denote by $\mathbb{E}_p$ the ring $\mathbb{E}/p\mathbb{E}$ of residue classes of $\mathbb{E}$ modulo p.
- We are interested in: $\mathbb{E}_2 \simeq \mathrm{GF}(2^2)$ and $\mathbb{E}_4 \simeq \mathrm{GR}(4^2)$
- Each of 16 elements of $\mathbb{E}_4$ can be uniquely represented in the form $2a + b$ where $a, b \in \{0, 1, \omega, \omega^2\}$.
- $\mathcal{E} = \{-\omega^2, \omega, -1, \omega^2, -\omega, 1\}$ is the set of units.
- The elements of $\mathbb{E}_4$ are partitioned into $0\mathcal{E}$, $\mathcal{E}$, $2\mathcal{E}$, and $\psi\mathcal{E}$ where $\psi = 2 + \omega$.

Eisenstein integers modulo 2 or 4

- Given $p \in \mathbb{E}\backslash\{0\}$, we denote by $\mathbb{E}_p$ the ring $\mathbb{E}/p\mathbb{E}$ of residue classes of $\mathbb{E}$ modulo p.
- We are interested in: $\mathbb{E}_2 \simeq \mathrm{GF}(2^2)$ and $\mathbb{E}_4 \simeq \mathrm{GR}(4^2)$
- Each of 16 elements of $\mathbb{E}_4$ can be uniquely represented in the form $2a + b$ where $a, b \in \{0, 1, \omega, \omega^2\}$.
- $\mathcal{E} = \{-\omega^2, \omega, -1, \omega^2, -\omega, 1\}$ is the set of units.
- The elements of $\mathbb{E}_4$ are partitioned into $0\mathcal{E}$, $\mathcal{E}$, $2\mathcal{E}$, and $\psi\mathcal{E}$ where $\psi = 2 + \omega$.

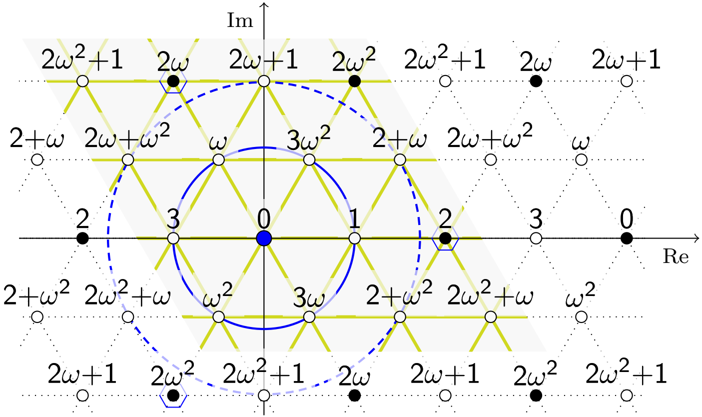
Eisenstein integers modulo 2 or 4

- Given $p \in \mathbb{E} \backslash \{0\}$, we denote by $\mathbb{E}_p$ the ring $\mathbb{E}/p\mathbb{E}$ of residue classes of $\mathbb{E}$ modulo p.
- We are interested in: $\mathbb{E}_2 \simeq \mathrm{GF}(2^2)$ and $\mathbb{E}_4 \simeq \mathrm{GR}(4^2)$
- Each of 16 elements of $\mathbb{E}_4$ can be uniquely represented in the form $2a + b$ where $a, b \in \{0, 1, \omega, \omega^2\}$.
- $\mathcal{E} = \{-\omega^2, \omega, -1, \omega^2, -\omega, 1\}$ is the set of units.
- The elements of $\mathbb{E}_4$ are partitioned into $0\mathcal{E}$, $\mathcal{E}$, $2\mathcal{E}$, and $\psi\mathcal{E}$ where $\psi = 2 + \omega$.

Eisenstein integers modulo 2 or 4

- Given $p \in \mathbb{E}\backslash\{0\}$, we denote by $\mathbb{E}_p$ the ring $\mathbb{E}/p\mathbb{E}$ of residue classes of $\mathbb{E}$ modulo p.
- We are interested in: $\mathbb{E}_2 \simeq \mathrm{GF}(2^2)$ and $\mathbb{E}_4 \simeq \mathrm{GR}(4^2)$
- Each of 16 elements of $\mathbb{E}_4$ can be uniquely represented in the form $2a + b$ where $a, b \in \{0, 1, \omega, \omega^2\}$.
- $\mathcal{E} = \{-\omega^2, \omega, -1, \omega^2, -\omega, 1\}$ is the set of units.
- The elements of $\mathbb{E}_4$ are partitioned into $0\mathcal{E}$, $\mathcal{E}$, $2\mathcal{E}$, and $\psi\mathcal{E}$ where $\psi = 2 + \omega$.

The Shrikhande graph



- The Shrikhande graph is the Cayley graph of $\mathbb{E}_4$ with the generating set $\mathcal{E}$.

The full graph. Doob graphs as modules. Linear codes.

- Similarly, the vertices of $K = K_4$ can be treated as the elements 0, 1, ω, ω^2 of $\mathbb{E}_2 \simeq \mathrm{GF}(2^2)$.
- Then, the vertices of $D(m, n)$ are the elements of $\mathbb{E}_4^m \times \mathbb{E}_2^n$, which is a module over the ring $\mathbb{E}_4$.
- A sumbodule of $\mathbb{E}_4^m \times \mathbb{E}_2^n$ is then a linear code in $D(m, n)$.
- Any weight-1 word (i.e., adjacent to $\overline{0}$) has an element of $\mathcal{E}$ in the first m coordinates or an element of $\{1, \omega, \omega^2\}$ in the last n coordinates.

The full graph. Doob graphs as modules. Linear codes.

- Similarly, the vertices of $K = K_4$ can be treated as the elements 0, 1, ω, ω^2 of $\mathbb{E}_2 \simeq \mathrm{GF}(2^2)$.
- Then, the vertices of $D(m,n)$ are the elements of $\mathbb{E}_4^m \times \mathbb{E}_2^n$, which is a module over the ring $\mathbb{E}_4$.
- A sumbodule of $\mathbb{E}_4^m \times \mathbb{E}_2^n$ is then a linear code in $D(m,n)$.
- Any weight-1 word (i.e., adjacent to $\overline{0}$) has an element of $\mathcal{E}$ in the first m coordinates or an element of $\{1, \omega, \omega^2\}$ in the last n coordinates.

The full graph. Doob graphs as modules. Linear codes.

- Similarly, the vertices of $K = K_4$ can be treated as the elements 0, 1, ω, ω^2 of $\mathbb{E}_2 \simeq \mathrm{GF}(2^2)$.
- Then, the vertices of $D(m,n)$ are the elements of $\mathbb{E}_4^m \times \mathbb{E}_2^n$, which is a module over the ring $\mathbb{E}_4$.
- A sumbodule of $\mathbb{E}_4^m \times \mathbb{E}_2^n$ is then a linear code in $D(m,n)$.
- Any weight-1 word (i.e., adjacent to $\overline{0}$) has an element of $\mathcal{E}$ in the first m coordinates or an element of $\{1, \omega, \omega^2\}$ in the last n coordinates.

The full graph. Doob graphs as modules. Linear codes.

- Similarly, the vertices of $K = K_4$ can be treated as the elements 0, 1, ω, ω^2 of $\mathbb{E}_2 \simeq \mathrm{GF}(2^2)$.
- Then, the vertices of $D(m, n)$ are the elements of $\mathbb{E}_4^m \times \mathbb{E}_2^n$, which is a module over the ring $\mathbb{E}_4$.
- A sumbodule of $\mathbb{E}_4^m \times \mathbb{E}_2^n$ is then a linear code in $D(m, n)$.
- Any weight-1 word (i.e., adjacent to $\overline{0}$) has an element of $\mathcal{E}$ in the first m coordinates or an element of $\{1, \omega, \omega^2\}$ in the last n coordinates.

Doob graphs as modules over $\mathbb{Z}_4$. Additive codes.

- $\mathbb{E}_4$ itself is a module over $\mathbb{Z}_4$; its elements are represented by the pairs from $\mathbb{Z}_4^2$, in the basis $(\omega, 1)$.
- Similarly, $\mathbb{E}_2 \longrightarrow \mathbb{Z}_2^2$.
- Alternatively, the vertices of K_4 can be represented by elements of $\mathbb{Z}_4$.
- Then, the vertices of $D(m, n' + n'')$ are the elements of the module $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ over the ring $\mathbb{Z}_4$.
- A sumbodule C of $M = (\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ is then an additive code of type $(n', n'', m; \Gamma, \Delta)$ in $D(m, n' + n'')$. Where $M/C \simeq \mathbb{Z}_2^\Gamma \times \mathbb{Z}_4^\Delta$.
- Any weight-1 words has values from $\{01, 10, 11, 03, 30, 33\}$ in a pair from the first $2m$ coordinates or values from $\{01, 10, 11\}$ in a pair from the next $2n'$ coordinates or an element of $\{1, 2, 3\}$ in the last n'' coordinates.

Doob graphs as modules over $\mathbb{Z}_4$. Additive codes.

- $\mathbb{E}_4$ itself is a module over $\mathbb{Z}_4$; its elements are represented by the pairs from $\mathbb{Z}_4^2$, in the basis $(\omega, 1)$.
- Similarly, $\mathbb{E}_2 \longrightarrow \mathbb{Z}_2^2$.
- Alternatively, the vertices of K_4 can be represented by elements of $\mathbb{Z}_4$.
- Then, the vertices of $D(m, n' + n'')$ are the elements of the module $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ over the ring $\mathbb{Z}_4$.
- A sumbodule C of $M = (\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ is then an additive code of type $(n', n'', m; \Gamma, \Delta)$ in $D(m, n' + n'')$. Where $M/C \simeq \mathbb{Z}_2^\Gamma \times \mathbb{Z}_4^\Delta$.
- Any weight-1 words has values from $\{01, 10, 11, 03, 30, 33\}$ in a pair from the first $2m$ coordinates or values from $\{01, 10, 11\}$ in a pair from the next $2n'$ coordinates or an element of $\{1, 2, 3\}$ in the last n'' coordinates.

Doob graphs as modules over $\mathbb{Z}_4$. Additive codes.

- $\mathbb{E}_4$ itself is a module over $\mathbb{Z}_4$; its elements are represented by the pairs from $\mathbb{Z}_4^2$, in the basis $(\omega, 1)$.
- Similarly, $\mathbb{E}_2 \longrightarrow \mathbb{Z}_2^2$.
- Alternatively, the vertices of K_4 can be represented by elements of $\mathbb{Z}_4$.
- Then, the vertices of $D(m, n' + n'')$ are the elements of the module $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ over the ring $\mathbb{Z}_4$.
- A sumbodule C of $M = (\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ is then an additive code of type $(n', n'', m; \Gamma, \Delta)$ in $D(m, n' + n'')$. Where $M/C \simeq \mathbb{Z}_2^\Gamma \times \mathbb{Z}_4^\Delta$.
- Any weight-1 words has values from $\{01, 10, 11, 03, 30, 33\}$ in a pair from the first $2m$ coordinates or values from $\{01, 10, 11\}$ in a pair from the next $2n'$ coordinates or an element of $\{1, 2, 3\}$ in the last n'' coordinates.

Doob graphs as modules over $\mathbb{Z}_4$. Additive codes.

- $\mathbb{E}_4$ itself is a module over $\mathbb{Z}_4$; its elements are represented by the pairs from $\mathbb{Z}_4^2$, in the basis $(\omega, 1)$.
- Similarly, $\mathbb{E}_2 \longrightarrow \mathbb{Z}_2^2$.
- Alternatively, the vertices of K_4 can be represented by elements of $\mathbb{Z}_4$.
- Then, the vertices of $D(m, n' + n'')$ are the elements of the module $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ over the ring $\mathbb{Z}_4$.
- A sumbodule C of $M = (\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ is then an additive code of type $(n', n'', m; \Gamma, \Delta)$ in $D(m, n' + n'')$. Where $M/C \simeq \mathbb{Z}_2^\Gamma \times \mathbb{Z}_4^\Delta$.
- Any weight-1 words has values from $\{01, 10, 11, 03, 30, 33\}$ in a pair from the first $2m$ coordinates or values from $\{01, 10, 11\}$ in a pair from the next $2n'$ coordinates or an element of $\{1, 2, 3\}$ in the last n'' coordinates.

Doob graphs as modules over $\mathbb{Z}_4$. Additive codes.

- $\mathbb{E}_4$ itself is a module over $\mathbb{Z}_4$; its elements are represented by the pairs from $\mathbb{Z}_4^2$, in the basis $(\omega, 1)$.
- Similarly, $\mathbb{E}_2 \longrightarrow \mathbb{Z}_2^2$.
- Alternatively, the vertices of K_4 can be represented by elements of $\mathbb{Z}_4$.
- Then, the vertices of $D(m, n' + n'')$ are the elements of the module $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ over the ring $\mathbb{Z}_4$.
- A sumbodule C of $M = (\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ is then an additive code of type $(n', n'', m; \Gamma, \Delta)$ in $D(m, n' + n'')$. Where $M/C \simeq \mathbb{Z}_2^\Gamma \times \mathbb{Z}_4^\Delta$.
- Any weight-1 words has values from $\{01, 10, 11, 03, 30, 33\}$ in a pair from the first $2m$ coordinates or values from $\{01, 10, 11\}$ in a pair from the next $2n'$ coordinates or an element of $\{1, 2, 3\}$ in the last n'' coordinates.

Doob graphs as modules over $\mathbb{Z}_4$. Additive codes.

- $\mathbb{E}_4$ itself is a module over $\mathbb{Z}_4$; its elements are represented by the pairs from $\mathbb{Z}_4^2$, in the basis $(\omega, 1)$.
- Similarly, $\mathbb{E}_2 \longrightarrow \mathbb{Z}_2^2$.
- Alternatively, the vertices of K_4 can be represented by elements of $\mathbb{Z}_4$.
- Then, the vertices of $D(m, n' + n'')$ are the elements of the module $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ over the ring $\mathbb{Z}_4$.
- A sumbodule C of $M = (\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ is then an additive code of type $(n', n'', m; \Gamma, \Delta)$ in $D(m, n' + n'')$. Where $M/C \simeq \mathbb{Z}_2^\Gamma \times \mathbb{Z}_4^\Delta$.
- Any weight-1 words has values from $\{01, 10, 11, 03, 30, 33\}$ in a pair from the first $2m$ coordinates or values from $\{01, 10, 11\}$ in a pair from the next $2n'$ coordinates or an element of $\{1, 2, 3\}$ in the last n'' coordinates.

Parameters of additive 1-perfect codes.

Theorem

Assume there is an additive 1*-perfect code* C *of type* $(n', n'', m; \Gamma, \Delta)$ *in* $D(m, n' + n'')$*. Then* $n'' \neq 1$*,* Γ *is even,*

$$2m + n' + n'' = (2^{\Gamma+2\Delta} - 1)/3, \quad (1)$$

$$3n' + n'' = 2^{\Gamma+\Delta} - 1, \quad (2)$$

$$n'' \leq 2^{\Delta} - 1 \quad (3)$$

- The number of elements in the factor-group is the number of weight$\leq$ 1 words. (1) follows. Then Γ is even.
- The number of order-2 elements in the factor-group is the number of weight-1 words of order-2. (2) follows.
- There are at least n'' weight-1 words of order 2 that are multiples of 2. (3) follows.
- $n'' \neq 1$ follows from the fact that a projective space cannot be partitioned into one point and several lines.

Parameters of additive 1-perfect codes.

Theorem

Assume there is an additive 1*-perfect code* C *of type* $(n', n'', m; \Gamma, \Delta)$ *in* $D(m, n'+n'')$*. Then* $n'' \neq 1$*,* Γ *is even,*

$$\begin{aligned} 2m + n' + n'' &= (2^{\Gamma+2\Delta} - 1)/3, && (1) \\ 3n' + n'' &= 2^{\Gamma+\Delta} - 1, && (2) \\ n'' &\leq 2^{\Delta} - 1 && (3) \end{aligned}$$

- The number of elements in the factor-group is the number of weight≤ 1 words. (1) follows. Then Γ is even.
- The number of order-2 elements in the factor-group is the number of weight-1 words of order-2. (2) follows.
- There are at least n'' weight-1 words of order 2 that are multiples of 2. (3) follows.
- $n'' \neq 1$ follows from the fact that a projective space cannot be partitioned into one point and several lines.

Parameters of additive 1-perfect codes.

Theorem

Assume there is an additive 1*-perfect code* C *of type* $(n', n'', m; \Gamma, \Delta)$ *in* $D(m, n' + n'')$*. Then* $n'' \neq 1$*,* Γ *is even,*

$$
\begin{aligned}
2m + n' + n'' &= (2^{\Gamma+2\Delta} - 1)/3, && (1)\\
3n' + n'' &= 2^{\Gamma+\Delta} - 1, && (2)\\
n'' &\leq 2^{\Delta} - 1 && (3)
\end{aligned}
$$

- The number of elements in the factor-group is the number of weight$\leq$ 1 words. (1) follows. Then Γ is even.
- The number of order-2 elements in the factor-group is the number of weight-1 words of order-2. (2) follows.
- There are at least n'' weight-1 words of order 2 that are multiples of 2. (3) follows.
- $n'' \neq 1$ follows from the fact that a projective space cannot be partitioned into one point and several lines.

Parameters of additive 1-perfect codes.

Theorem

Assume there is an additive 1*-perfect code* C *of type* $(n', n'', m; \Gamma, \Delta)$ *in* $D(m, n' + n'')$*. Then* $n'' \neq 1$*,* Γ *is even,*

$$\begin{aligned} 2m + n' + n'' &= (2^{\Gamma+2\Delta} - 1)/3, && (1) \\ 3n' + n'' &= 2^{\Gamma+\Delta} - 1, && (2) \\ n'' &\leq 2^{\Delta} - 1 && (3) \end{aligned}$$

- The number of elements in the factor-group is the number of weight$\leq$ 1 words. (1) follows. Then Γ is even.
- The number of order-2 elements in the factor-group is the number of weight-1 words of order-2. (2) follows.
- There are at least n'' weight-1 words of order 2 that are multiples of 2. (3) follows.
- $n'' \neq 1$ follows from the fact that a projective space cannot be partitioned into one point and several lines.

Construction of linear codes using check matrices

A check matrix of a linear code in $D(m, n)$ consists of two parts:

$$A = A_{\gamma,\delta} = A^*|A'$$

with elements from $\mathbb{E}_4$ and $\mathbb{E}_2$, respectively. We define the multiplication Az^{T} for $z = (x|y)$ as

$$A^* x^{\mathrm{T}} + 2A' y^{\mathrm{T}}$$

(here, the result of the multiplication by 2 is considered as a column-vector over $\mathbb{E}_4$).

Check matrices of linear 1-perfect codes

$$A_{0,2} = \left(\begin{array}{cccccccccccccc} 0 & 0 & 2 & 2 & 2\omega & 2\omega & 2\omega^2 & 2\omega^2 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \psi & 1 & \psi & 1 & \psi & 1 & \psi & 0 & 2 & 2\omega & 2\omega^2 & 1 & -\omega \\ \hline \end{array}\right.$$

$$\left.\begin{array}{ccccc|ccccc} 1 & 1 & \psi & \dots & \psi & 0 & 1 & 1 & 1 & 1 \\ 2\omega^2{+}1 & 2{+}\omega^2 & 0 & \dots & 2{+}\omega^2 & 1 & 0 & 1 & \omega & \omega^2 \\ \hline \end{array}\right)$$

$$A_{1,1} = \left(\begin{array}{cccccccc|ccccc} 1 & 1 & 1 & 1 & \psi & \psi & \psi & \psi & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 2 & 2\omega & 2\omega^2 & 0 & 2 & 2\omega & 2\omega^2 & 1 & 0 & 1 & \omega & \omega^2 \end{array}\right)$$

$$A_{0,1} = \left(\begin{array}{cc|c} 1 & \psi & 1 \\ \hline \end{array}\right)$$

Characterization of linear codes

Theorem (Theorem 2)

Linear 1*-perfect codes in* $D(m, n)$ *exist if and only if for some integer* $\gamma \geq 0$ *and* $\delta > 0$,

$$n = (4^{\gamma+\delta} - 1)/3 \qquad \textit{and} \qquad m = (4^{\gamma+2\delta} - 4^{\gamma+\delta})/6.$$

From linear codes to additive codes

- From linear 1-perfect codes we trivially get 1-perfect additive codes of type $(n, 0, m; 2\gamma, 2\delta)$.
- Then, we can obtain 1-perfect additive codes of type $(n - n''/3, n'', m - n''/3; 2\gamma, 2\delta)$ with nonzero n''. The idea is the following:
- Assume the same column h occurs in both $\mathbb{E}_4$ and $\mathbb{E}_2$ parts of the check matrix. Then, it "cover" the syndromes $h, \omega h, \omega^2 h, 3h, 3\omega h, 3\omega^2 h$ and $2h, 2\omega h, 2\omega^2 h$. Regrouping gives $h, 2h, 3h$, and $\omega h, 2\omega h, 3\omega h$, and $\omega^2 h, 2\omega^2 h, 3\omega^2 h$, which can be "covered" by three $\mathbb{Z}_4$ coordinates in the n''-part.

$$\left(\begin{array}{c|c} ..\ 1\ .. & ..\ 1\ .. \\ ..\ \omega^2\ .. & ..\ \omega^2\ .. \end{array}\right) \longrightarrow \left(\begin{array}{c|c} ..\ 1\,0\ .. & ..\ 1\,0\ .. \\ ..\ 0\,1\ .. & ..\ 0\,1\ .. \\ ..\ 0\,3\ .. & ..\ 0\,1\ .. \\ ..\ 1\,3\ .. & ..\ 1\,1\ .. \end{array}\right) \longrightarrow \left(\begin{array}{c|c|c} .. & .. & ..\ 0\ 1\ 3\ .. \\ .. & .. & ..\ 1\ 0\ 3\ .. \\ .. & .. & ..\ 3\ 0\ 1\ .. \\ .. & .. & ..\ 3\ 1\ 0\ .. \end{array}\right)$$

Additive codes

Theorem (Theorem 3)

Additive 1-perfect codes exist for all parameters that satisfy the conclusion of Theorem 1 with even Δ.

PROBLEM! Construct additive 1-perfect codes with odd δ

Additive codes, $\delta = 3$

Check matrix for an additive 1-perfect code of type $(0,7,7;0,3)$:

$$\left(\begin{array}{ccccccc|ccccccc} 12 & 22 & 03 & 32 & 03 & 13 & 11 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 03 & 30 & 23 & 11 & 33 & 30 & 02 & 0 & 1 & 0 & 3 & 3 & 3 & 2 \\ 22 & 03 & 32 & 03 & 13 & 11 & 12 & 0 & 0 & 1 & 2 & 3 & 1 & 1 \end{array}\right)$$

The columns of the matrix are considered as vectors over Z_4 that represent elements of the Galois ring $\mathrm{GR}(4^3)$. Let ξ be a primitive seventh root of 1 in $\mathrm{GR}(4^3)$. The first 14 columns of the matrix are divided into the pairs $\xi^i + 2\xi^{i+2}$, $\xi^{i+1} + 2\xi^{i+5}$, $i = 0, 1, \ldots, 6$; the last 7 columns are ξ^0, ξ^1, ..., ξ^6.

Non-linear codes

Theorem (Theorem 4)

Assume that positive integers m, n, μ satisfy

$$\begin{aligned} 2m + n &= (4^\mu - 1)/3, \\ m &\leq \begin{cases} (4^\mu - 2.5 \cdot 2^\mu + 1)/9 & \text{if } \mu \text{ is odd,} \\ (4^\mu - 2 \cdot 2^\mu + 1)/9 & \text{if } \mu \text{ is even.} \end{cases} \end{aligned} \tag{4}$$

Then there is a 1-perfect code in the Doob graph $D(m, n)$.

Problems

- For every value (m, n) satisfying $2m + n = (4^{\mu} - 1)/3$ and not covered by the constructions, construct a 1-perfect code in $D(m, n)$ or prove its nonexistence. In particular, do there exist 1-perfect codes in $D(6, 9)$, $D(9, 3)$, $D(10, 1)$?
- For every value (n', n'', m) satisfying (1)–(3) with odd $\Delta \geq 3$ (except the case $(0, 7, 7)$), construct an additive 1-perfect code of type $(n', n'', m; \Gamma, \Delta)$ in the $D(m, n' + n'')$ or prove its nonexistence. In particular, does there exist an additive 1-perfect code of type $(1, 4, 8; 0, 3)$ in $D(8, 5)$?
- Are the constructed non-additive codes (Theorem 4) propelinear?