Discrete Mathematics 312 (2012) 1269–1272

Contents lists available at SciVerse ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Note

On perfect 2-colorings of the q-ary n-cube[☆]

Vladimir N. Potapov

Sobolev Institute of Mathematics, 4 Acad. Koptug avenue, 630090, Novosibirsk, Russia
Novosibirsk State University, 2 Pirogova st., 630090, Novosibirsk, Russia

ARTICLE INFO

Article history:
Received 8 July 2011
Received in revised form 29 November 2011
Accepted 6 December 2011
Available online 9 January 2012

Keywords:
Hypercube
Perfect coloring
Perfect code
MDS code
Equitable partition
Orthogonal array

ABSTRACT

A coloring of a q-ary n-dimensional cube (hypercube) is called perfect if, for every n-tuple x, the collection of the colors of the neighbors of x depends only on the color of x. A Boolean-valued function is called correlation-immune of degree $n-m$ if it takes value 1 the same number of times for each m-dimensional face of the hypercube. Let $f = \chi^S$ be a characteristic function of a subset S of hypercube. In the present paper we prove the inequality $\rho(S)q(\mathrm{cor}(f)+1) \le \alpha(S)$, where $\mathrm{cor}(f)$ is the maximum degree of the correlation immunity of f, $\alpha(S)$ is the average number of neighbors in the set S for n-tuples in the complement of a set S, and $\rho(S) = |S|/q^n$ is the density of the set S. Moreover, the function f is a perfect coloring if and only if we have an equality in the formula above. Also, we find a new lower bound for the cardinality of components of a perfect coloring and a 1-perfect code in the case $q > 2$.

1. Introduction

Let Z_q be the set $\{0, \ldots, q-1\}$. The set Z_q^n of n-tuples over Z_q is called q-ary n-dimensional cube (hypercube). The *Hamming distance* $d(x, y)$ between two n-tuples $x, y \in Z_q^n$ is the number of positions at which they differ. If $d(x, y) = 1$, we call x and y *neighbors*. Define the number $\alpha(S)$ to be the average number of neighbors in a set $S \subseteq Z_q^n$ for n-tuples in the complement of S, i.e. $\alpha(S) = \frac{1}{q^n-|S|}\sum_{x\notin S} |\{y \in S \mid d(x, y) = 1\}|$.

A mapping Col: $Z_q^n \to \{0, \ldots, k\}$ is called a *perfect coloring* with the matrix of parameters $P = \{p_{ij}\}$ if, for all i, j, for every n-tuple of color i, the number of its neighbors of color j is equal to p_{ij}. Other terms used for this notion in the literature are "equitable partition", "partition design" and "distributive coloring". In what follows we will only consider colorings in two colors (2-coloring). Moreover, for convenience we will assume that the set of colors is $\{0, 1\}$. In this case the Boolean-valued function Col is a characteristic function of the set of n-tuples colored by 1.

A *1-perfect code* (one-error-correcting code) $C \subset Z_q^n$ can be defined as the set of units of a perfect coloring with the matrix of parameters $P = \begin{pmatrix} n(q-1)-1 & 1 \\ n(q-1) & 0 \end{pmatrix}$. The entry 0 in the Southeast says that no two codewords are neighbors, hence the minimum distance is at least 2; the entries in the first row show that each vector outside of the code is at distance 1 from exactly one codeword. If q is the power of a prime number then a coloring with such parameters exists only if $n = \frac{q^m-1}{q-1}$ (m is an integer). For $q = 2$ a list of achievable parameters and corresponding constructions of perfect 2-colorings can be found in [3,4].

Let U be a finite set. A *correlation immune* function of order $n-m$ is a function $f : Z_q^n \to U$ whose each value is uniformly distributed on all m-dimensional faces. For any function f we denote the maximum order of its correlation immunity by

☆ The work is supported by RFBR (grants 10-01-00424, 10-01-00616) and Federal Target Grant "Scientific and educational personnel of innovation Russia" for 2009–2013 (government contract No. 02.740.11.0362).

E-mail address: vpotapov@math.nsc.ru.

0012-365X/$ – see front matter
doi:10.1016/j.disc.2011.12.004

$\mathrm{cor}(f)$. An *orthogonal array* ($OA(N,k,u,t)$) of strength t with N rows, k columns ($k \geq t$) and based on u symbols is an $N \times k$ array with elements from U, $|U| = u$, such that every $N \times t$ subarray contains each of the u^t possible t-tuples equally often as a row (say λ times). N must be a multiple of u^t and $\lambda = N/u^t$ is the index of the array. The definition of correlation immune (of order t) function f is equivalent to the following property: the array whose rows are the vectors of $f^{-1}(a)$ for each $a \in U$ is an orthogonal array of strength t. In [5] it is established that for each unbalanced Boolean function $f = \chi^S$ ($S \subset Z_2^n$) the inequality $\mathrm{cor}(f) \leq \frac{2n}{3} - 1$ holds. Moreover, in the case of the equality $\mathrm{cor}(f) = \frac{2n}{3} - 1$, the function f is a perfect 2-coloring. Similarly, if for any set $S \subset Z_2^n$ the Friedman inequality (see [6]) $\rho(S) \geq 1 - \frac{n}{2(\mathrm{cor}(f)+1)}$ becomes an equality then the function χ^S is a perfect 2-coloring (see [11]). Consequently, in the extremal cases, regular distributions on balls follow from uniform distributions on faces. The main result of the present paper is the following theorem:

Theorem 1. (a) *For each Boolean-valued function $f = \chi^S$, where $S \subset Z_q^n$, the inequality $\rho(S)q(\mathrm{cor}(f) + 1) \leq \alpha(S)$ holds.*
(b) *A Boolean-valued function $f = \chi^S$ is a perfect 2-coloring if and only if $\rho(S)q(\mathrm{cor}(f) + 1) = \alpha(S)$.*

2. Criterion for perfect 2-coloring

In the proof of the theorem we employ the idea from [1].

We consider Z_q as the cyclic group on the set $\{0, \ldots, q-1\}$. We may impose the structure of the group $Z_q \times \cdots \times Z_q$ on the hypercube. Consider the vector space $\mathbb{V}$ of complex-valued functions on Z_q^n with the scalar product $(f,g) = \frac{1}{q^n}\sum_{x\in Z_q^n} f(x)\overline{g(x)}$. For every $z \in Z_q^n$ define a *character* $\phi_z(x) = \xi^{\langle x,z\rangle}$, where $\xi = e^{2\pi i/q}$ is a primitive complex qth root of unity and $\langle x,z\rangle = x_1z_1 + \cdots + x_nz_n$. Here all arithmetic operations are performed on complex numbers. As is generally known, the characters of the group $Z_q \times \cdots \times Z_q$ form an orthonormal basis of $\mathbb{V}$. It is sufficient to verify that $\xi^k\overline{\xi^k} = 1$ and $\sum_{j=0}^{q-1} \xi^{kj} = 0$ as $k \neq 0 \bmod q$.

Let M be the adjacency matrix of the hypercube Z_q^n. This means that $Mf(x) = \sum_{y,d(x,y)=1} f(y)$. It is well known that the characters are eigenvectors of M. Indeed, we have

$$M\phi_z(x) = \sum_{y,d(x,y)=1} \xi^{\langle y-x,z\rangle+\langle x,z\rangle} = \xi^{\langle x,z\rangle}\sum_{j=1}^{n}\sum_{k\neq 0}\xi^{kz_j} = ((n - wt(z))(q-1) - wt(z))\phi_z(x),$$

where $wt(z)$ is the number of nonzero coordinates of z.

Consider a perfect coloring $f \in \mathbb{V}, f(Z_q^n) = \{0, 1\}$ with the matrix of parameters

$$A = \begin{pmatrix} n(q-1) - b & b \\ c & n(q-1) - c \end{pmatrix}.$$

The vector $(-b, c)$ is an eigenvector of A with the eigenvalue $n(q-1) - c - b$. The definition of a perfect 2-coloring implies that the function $(b+c)f - b$ is the eigenvector of the matrix M. Moreover, the converse is true: every two-valued eigenvector of M generates a perfect coloring (see [5]).

Proposition 1 (*See [3]*).
(a) *Let f be a perfect 2-coloring with the matrix of parameters A. Then $s = \frac{c+b}{q}$ is an integer and $(f, \phi_z) = 0$ for every n-tuple $z \in Z_q^n$ such that $wt(z) \neq 0, s$.*
(b) *Let $f: Z_q^n \to \{0, 1\}$ be a Boolean-valued function. If $(f, \phi_z) = 0$ for every n-tuple $z \in \{0, \ldots, q-1\}^n$ such that $wt(z) \neq 0, s$ then f is a perfect 2-coloring.*

Proposition 2 (*See [1]*).
(a) *If $f \in \mathbb{V}$ is a correlation-immune function of order m then $(f, \phi_z) = 0$ for every n-tuple $z \in Z_q^n$ such that $0 < wt(z) \leq m$.*
(b) *A Boolean-valued function $f \in \mathbb{V}$ is correlation-immune of order m if $(f, \phi_z) = 0$ for every n-tuple $z \in Z_q^n$ such that $0 < wt(z) \leq m$.*

Corollary 1. *Let f be a perfect 2-coloring with the matrix of parameters A. Then $\mathrm{cor}(f) = \frac{c+b}{q} - 1$.*

For 1-perfect codes the last statement was proved in [2].

Proof of Theorem 1. We have the following equalities by the definitions and general properties of an orthonormal basis.

$$\sum_z |(f, \phi_z)|^2 = \frac{1}{q^n}\sum_{x\in Z_q^n} |f(x)|^2 = \rho(S). \tag{1}$$

$$(f, \phi_{\overline{0}}) = \frac{1}{q^n}\sum_{x\in Z_q^n} f(x) = \rho(S). \tag{2}$$

$$(Mf, f) = \frac{1}{q^n}\sum_{x\in Z_q^n}\sum_{y,d(x,y)=1} f(x)\overline{f(y)} = \mathrm{nei}(S)\rho(S), \tag{3}$$

where $\mathrm{nei}(S) = \frac{1}{|S|}\sum_{x\in S} |\{y \in S \mid d(x, y) = 1\}|$.

$$(Mf, f) = \sum_{z\in Z_q^n} (n(q-1) - wt(z)q)|(f, \phi_z)|^2. \quad (4)$$

From (1) to (4) and Proposition 2 we obtain the equality

$$\mathrm{nei}(S)\rho(S) = \rho(S)^2 n(q-1) + \sum_{z, wt(z)\geq \mathrm{cor}(f)+1} (n(q-1) - wt(z)q)|(f, \phi_z)|^2.$$

Since $\sum_{z,wt(z)\geq \mathrm{cor}(f)+1} |(f, \phi_z)|^2 = \rho(S) - \rho(S)^2$, we have

$$\mathrm{nei}(S)\rho(S) \leq \rho(S)^2 n(q-1) + (n(q-1) - (\mathrm{cor}(f) + 1)q)(\rho(S) - \rho(S)^2) \quad \text{and}$$
$$(\mathrm{cor}(f) + 1)q(1 - \rho(S)) \leq n(q-1) - \mathrm{nei}(S). \quad (5)$$

Substitute the set $Z_q^n \setminus S$ instead of the set S in the inequality (5). Since $\mathrm{cor}(\chi^S) = \mathrm{cor}(\chi^{Z_q^n\setminus S})$, $1 - \rho(Z_q^n \setminus S) = \rho(S)$ and $n(q-1) - \mathrm{nei}(Z_q^n \setminus S) = \alpha(S)$ we obtain (a) of the theorem.

Moreover, the equality

$$(\mathrm{cor}(f) + 1)q(1 - \rho(S)) = n(q-1) - \mathrm{nei}(S) \quad (6)$$

holds if and only if $(f, \phi_z) = 0$ for every n-tuple z such that $wt(z) \geq \mathrm{cor}(f) + 2$. Then from Proposition 1(b) we conclude that f is a perfect 2-coloring.

Any perfect 2-coloring satisfies (6), which is a consequence of Proposition 1(a) and Corollary 1. As mentioned above, equality (6) is equivalent to the equality (b) of the theorem. □

Since $\mathrm{nei}(S) \neq 0$, the inequality (5) implies the Bierbrauer–Friedman inequality (see [6,1])

$$\rho(S) \geq 1 - \frac{n(q-1)}{q(\mathrm{cor}(f) + 1)}.$$

For 1-perfect binary codes, a similar theorem was previously proved in [9]. Namely, if $\mathrm{cor}(S) = \mathrm{cor}(H)$ and $\rho(S) = \rho(H)$, where $S, H \subset Z_2^n$ and H is a 1-perfect code, then S is also a 1-perfect code.

3. Components of a perfect 2-coloring

By a *bitrade of order* $n - m$ we will mean a subset $B \subseteq Z_q^n$ such that the cardinality of intersections B and each m-dimensional face are even. For example, if q is even then $B \subseteq Z_q^n$ is a bitrade of order $n - 1$.

Proposition 3. *Let $B \subseteq Z_q^n$ be a nonempty bitrade of order m, $m < n$. Then $|B| \geq 2^{m+1}$.*

Proof. Suppose that the statement is true for $n = k$. We will prove it for $n = k + 1$. Since $|B| \geq 2$, there exist two parallel k-dimensional faces F_1, F_2 such that the intersections $F_i \cap S$ are nonempty for $i = 1, 2$. It is clear that $F_i \cap S$ is a bitrade of order $m - 1$ in the $(n - 1)$-dimensional cube F_i. By induction hypothesis, $|F_i \cap B| \geq 2^m$ for $i = 1, 2$; consequently, $|B| \geq 2^{m+1}$. □

Suppose that the characteristic functions $f = \chi^{S_1}$ and $g = \chi^{S_2}$ are perfect 2-colorings (correlation-immune) with the same matrix of the parameters ($\mathrm{cor}(f) = \mathrm{cor}(g)$). A set $S_1 \triangle S_2$ is called *mobile* and sets $S_1 \setminus S_2$ and $S_2 \setminus S_1$ are called *components* of perfect 2-colorings (correlation-immune functions) χ^{S_1} and χ^{S_2}, respectively. It is clear, that a mobile set of correlation-immune function of order m is a bitrade of order m.

Corollary 2. (a) *Let f be a perfect 2-coloring with the matrix of parameters A. If $S \subset Z_q^n$ is a component of f then $|S| \geq 2^{\frac{c+b}{q}-1}$.*

(b) *Let $C \subset Z_p^n$ be a 1-perfect code. If $S \subset Z_q^n$ is a component of f then $|S| \geq 2^{\frac{n(q-1)+1}{q}-1}$.*

If $q = 2$ then the lower bound $|S| \geq 2^{\frac{n+1}{2}-1}$ for the cardinality of components of 1-perfect codes is achievable (see, for example, [11]). In the case $q > 2$, an upper bound for the cardinality of components of 1-perfect codes is obtained constructively (see [10,8]). If $q = p^r$ and p is a prime number then $|S| \geq p^{\frac{q^{m-1}-1}{q-1}(r(q-2)+1)}$ where $n = \frac{q^m-1}{q-1}$.

A set $S \subset Z_p^n$ is called *MDS code with distance* 2 if the intersection of S with each 1-dimensional face contains precisely one n-tuple. Obviously, a characteristic function of an MDS code is a perfect 2-coloring with the matrix of parameters $\begin{pmatrix} n(q-2) & n \\ n(q-1) & 0 \end{pmatrix}$. If $q \geq 4$ then the lower bound $|S| \geq 2^{n-1}$ for the cardinality of the components of MDS codes is achievable (see [7]).

References

[1] J. Bierbrauer, Bounds on orthogonal arrays and resilient functions, Journal of Combinatorial Designs 3 (1995) 179–183.
[2] P. Delsarte, Bounds for unrestricted codes by linear programming, Philips Research Reports 27 (1972) 272–289.
[3] D.G. Fon-Der-Flaass, Perfect 2-colorings of a hypercube, Siberian Mathematical Journal 48 (4) (2007) 740–745.
[4] D.G. Fon-Der-Flaass, Perfect 2-colorings of the 12-cube that attain the bounds on correlation immunity, Sibirskie Elektronnye Matematicheskie Izvestiya 4 (2007) 292–295 (Russian).
[5] D.G. Fon-Der-Flaass, A bound of correlation immunity, Siberian Electronic Mathematical Reports, 4, 2007, pp. 133–135.
[6] J. Friedman, On the bit extraction problem, in: Proc. 33rd IEEE Symposium on Foundations of Computer Science 1992, pp. 314–319.
[7] D.S. Krotov, V.N. Potapov, P.V. Sokolova, On reconstructing reducible n-ary quasigroups and switching subquasigroups, Quasigroups and Related Systems 16 (2008) 55–67.
[8] A.V. Los', Construction of perfect q-ary codes by switching of simple components, Problems of Information Transmission 42 (1) (2005) 30–37.
[9] P.R.J. Östergård, O. Pottonen, K.T. Phelps, The perfect binary one-error-correcting codes of length 15: part II-properties, IEEE Transactions on Information Theory 56 (2010) 2571–2582.
[10] K.T. Phelps, M. Villanueva, Ranks of q-ary 1-perfect codes, Design, Codes and Cryptography 27 (1–2) (2002) 139–144.
[11] V.N. Potapov, On perfect colorings of Boolean n-cube and correlation immune functions with small density, Sibirskie Elektronnye Matematicheskie Izvestiya 7 (2010) 372–382 (Russian).