ISSN 0032-9460, Problems of Information Transmission, 2012, Vol. 48, No. 1, pp. 46–54. © Pleiades Publishing, Inc., 2012.
Original Russian Text © V.N. Potapov, 2012, published in Problemy Peredachi Informatsii, 2012, Vol. 48, No. 1, pp. 54–63.

Cardinality Spectra of Components of Correlation Immune Functions, Bent Functions, Perfect Colorings, and Codes[1]

V. N. Potapov

Sobolev Institute of Mathematics,
Siberian Branch, Russian Academy of Sciences, Novosibirsk
Novosibirsk State University
vpotapov@math.nsc.ru

Received April 15, 2011; in final form, November 2, 2011

Abstract—We study cardinalities of components of perfect codes and colorings, correlation immune functions, and bent function (sets of ones of these functions). Based on results of Kasami and Tokura, we show that for any of these combinatorial objects the component cardinality in the interval from 2^k to 2^{k+1} can only take values of the form $2^{k+1} - 2^p$, where $p \in \{0, \dots, k\}$ and 2^k is the minimum component cardinality for a combinatorial object with the same parameters. For bent functions, we prove existence of components of any cardinality in this spectrum. For perfect colorings with certain parameters and for correlation immune functions, we find components of some of the above-given cardinalities.

DOI: 10.1134/S003294601201005X

1. INTRODUCTION

Denote by E^n the set of ordered binary tuples (vertices) of length n. The n-dimensional Boolean cube E^n is naturally equipped with a vector space structure over the field $GF(2)$. Introduce the operation $[x, y] = (x_1y_1, \dots, x_ny_n)$ and the inner product $\langle x, y\rangle = x_1y_1 \oplus \dots \oplus x_ny_n$ for vectors $x, y \in E^n$. The number of ones in a tuple $y \in E^n$ is called the *weight* of the tuple and is denoted by $\mathrm{wt}(y)$. A *face of dimension* $n - \mathrm{wt}(y)$ is the set $E^n_y(z) = \{x \in E^n : [x, y] = [z, y]\}$.

Let $S \subset E^n$; by χ^S we denote the characteristic function of S. The cardinality of S will be referred to as the *weight* of χ^S. A function χ^S is said to be *correlation immune of order* $n - m$ if for any m-face $E^n_y(z)$ all intersections $E^n_y(z) \cap S$ are of the same cardinality. A set $S \subset E^n$ and its characteristic function χ^S is referred to as a *bitrade of order* $n - m$ if for any m-face $E^n_y(z)$ the cardinality of the intersection $E^n_y(z) \cap S$ is even (possibly, zero). Note that a correlation immune function of order $n - m$ is a bitrade of order $n - m - 1$.

The *Hamming distance* between tuples $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$ is the number of positions in which x and y differ; i.e., $d(x, y) = \mathrm{wt}(x \oplus y)$. The set of vertices that are at distance at most d form a vertex x is called a *ball* of radius d centered at x. A *sphere* of radius 1 centered at x is the set $F(x) = \{y \in E^n : d(x, y) = 1\}$.

A *perfect k-coloring* of a Boolean n-cube is a map $\mathrm{Col}\colon E^n \to \{1, \dots, k\}$ satisfying the following condition: the cardinality of the intersection $|\operatorname{Col}^{-1}(i) \cap F(x)|$ depends only on colors i and on $\mathrm{Col}(x)$, but not on the vertex $x \in E^n$. Each perfect coloring corresponds to a parameter matrix

[1] Supported in part by the Russian Foundation for Basic Research, project nos. 10-01-00616 and 11-01-00997, and Federal Target Program "Research and Educational Personnel of Innovation Russia" for 2009–2013, government contract no. 02.740.11.0362.

$A = \{a_{ij}\}$, where a_{ij} is the number of vertices of color j in a sphere of radius 1 centered at a vertex of color i. In what follows, we consider two-colorings only; moreover, we assume for convenience that the set of colors is $\{1, 0\}$. In this case Col is a Boolean function, and $\mathrm{Col} = \chi^S$, where S is the set of vertices of color 1.

It is known (see, e.g., [1,2]) that a perfect coloring of a Boolean n-cube with parameter matrix $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ is a correlation immune function of order $\dfrac{b+c}{2} - 1$.

A *perfect code* with distance 3 is a subset of a Boolean n-cube that intersects each ball of radius 1 in exactly one vertex. A subset $C \subset E^n$ that intersects each ball of radius 1 in exactly t vertices is called a *t-fold perfect code.* It is easily seen that the characteristic function of a t-fold perfect code $C \subset E^n$ id a perfect coloring χ^C with a parameter matrix of the form $A = \begin{pmatrix} t-1 & n-t+1 \\ t & n-t \end{pmatrix}$.

The distance between Boolean functions f and g is defined as $d(f, g) = |\{x \in E^n : f(x) \neq g(x)\}|$. Boolean functions in E^n for an even n that are at the maximal distance from the set of affine functions are called bent functions.

Let $S_1 \subset E^n$, and let a function χ^{S_1} be a perfect coloring, correlation immune function, or bent function. We call a set $S_1 \setminus S_2$ a *component* of the perfect coloring (correlation immune function, bent function) χ^{S_1} if there exists a perfect coloring (correlation immune function, bent function) χ^{S_2} with the same parameters (in the case of a correlation immune function, with the same order and weight). The component $S_2 \setminus S_1$ of the function χ^{S_2} will be called the *alternative* to the component $S_1 \setminus S_2$. The union of two alternative components, i.e., the symmetric difference $S_1 \triangle S_2$, will be referred to as a *double component.*

The question on the cardinality spectrum for components of perfect codes was posed in [3]. Cardinalities of components of perfect codes or cardinalities of intersections of perfect codes were considered in [4–9]; the minimal cardinality of a component of a perfect code has been known for long, as well as the minimal cardinality of a component of a bent function (see also [10]). However, the problem of existence of components of *intermediate* cardinality between the minimum and twice the minimum cardinality remained little studied. Below we consider the question of existence of components of an intermediate cardinality for perfect codes and colorings and for correlation immune and bent functions. Based on results of [11], we find necessary conditions on the cardinality of intermediate components, which are sufficient in many cases.

2. ALGEBRAIC DEGREE OF PERFECT COLORINGS AND CORRELATION IMMUNE FUNCTIONS

Each Boolean function $f\colon E^n \to E$ can be represented as a *Zhegalkin polynomial* (in *algebraic normal form*)

$$f(x_1, \ldots, x_n) = \bigoplus_{y \in E^n} G[f](y) x_1^{y_1} \ldots x_n^{y_n},$$

where a^0 =1, $a^1 = a$, and $G[f]\colon E^n \to E$ is a Boolean function.

The *algebraic degree* of a Boolean function f is the largest degree of a term in its Zhegalkin polynomial; i.e., $\deg f = \max\limits_{G[f](y)=1} \mathrm{wt}(y)$. By the algebraic degree of a set $S \subset E^n$, we call the algebraic degree of its characteristic function.

The following fact is known.

Proposition 1 [2,12]. *For any Boolean function f, we have*

$$G[f](y) = \bigoplus_{\substack{x \in E^n \\ [x,y]=x}} f(x).$$

Since $f(x) = \bigoplus\limits_{\substack{y \in E^n \\ [x,y]=y}} G[f](y)$, for any Boolean function f we have $G[G[f]] = f$.

Proposition 1 immediately implies the following result.

Proposition 2. *A Boolean function $f\colon E^n \to E$ is a bitrade of order $n - m$ if and only if $\deg f \leq m - 1$.*

Let $S_1, S_2 \subset E^n$, and let correlation immune functions χ^{S_1} and χ^{S_2} have the same order $n - m$ and the same weight. Clearly, S_1 is a bitrade of order $n - m - 1$, and the component $S_1 \triangle S_2$ is a bitrade of order $n - m$. Thus, Proposition 2 implies the following fact.

Proposition 3. *Let $f\colon E^n \to E$ be a correlation immune function of order $n - m$. Then*

(a) $\deg f \leq m$ (*Siegenthaler inequality*);

(b) *The algebraic degree of a double component of the correlation immune function f is at most $m - 1$.*

Remark 1. If a correlation immune function f of order $n - m$ has an even number of ones in each m-face, then f is a bitrade of order $n - m$. Then from Proposition 2 we have $\deg f \leq m - 1$.

Since a perfect coloring with parameter matrix

$$\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix} \tag{1}$$

is a correlation immune function of order $\dfrac{b+c}{2} - 1$ (see, e.g., [1, 2]), Proposition 3 implies the following statement.

Corollary 1. *Let $f\colon E^n \to E$ be a perfect coloring with parameter matrix* (1)*. Then*

(a) $\deg f \leq n - \dfrac{b+c}{2} + 1$*;*

(b) *The algebraic degree of a double component of the perfect coloring f is at most $n - \dfrac{b+c}{2}$.*

A perfect code of length n (for $n \neq 3$) is not only a correlation immune function of order $\dfrac{n-1}{2}$ but also a bitrade of order $\dfrac{n-1}{2}$, since it intersects faces of dimension $\dfrac{n+1}{2}$ in an even number of vertices (see, e.g., [3]). Proposition 3 yields the following result.

Corollary 2. *Let $C \subset E^n$ be a perfect code. Then*

(a) $\deg(\chi^C) \leq \dfrac{n-1}{2}$ $n \neq 3$;

(b) *The algebraic degree of a double component of the perfect code C is at most $\dfrac{n-1}{2}$.*

Boolean functions $f\colon E^n \to E$ can be regarded as elements of a Boolean cube of dimension 2^n. The set of bitrades of order $n - m - 1$ (Boolean functions of algebraic degree at most m) is called the Reed–Muller code of type $\mathcal{R}(m, n)$ in E^{2^n}. In [13], the weight spectrum of Reed–Muller codes is considered; in particular, the following statements are given.

Proposition 4 [13, ch. 13, Theorems 3 and 5]. *For any non-identically zero Boolean function $f = \chi^S$, one has*

$$|S| \geq 2^{n - \deg f}.$$

If $|S| = 2^{n-\deg f}$, then S is a linear code.

Hereinafter, by a *linear code* we mean an arbitrary affine subset of a Boolean cube E^n considered as a vector space over $GF(2)$.

Proposition 5 [11; 13, ch. 15, Theorem 10]. *Let* $f = \chi^S$ *be a Boolean function in* E^n *with* $\deg f \geq 2$ *and* $2^{n-\deg f+1} > |S|$. *Then*

$$|S| = 2^{n-\deg f+1} - 2^{n-\deg f+1-p},$$

where

$$p \in \{1, \dots, \mu\}, \quad \mu = \max\{(n - \deg f + 2)/2, \min\{n - \deg f, \deg f\}\}.$$

Note that in [11, 14] there are listed (up to affine transformations) all Boolean functions in E^n corresponding to vertices of the code $\mathcal{R}(m,n)$ in E^{2^n} with weights up to 2.5 times the minimum nonzero weight 2^{n-m}.

Using Propositions 2–5, we prove the following result.

Proposition 6. *Let a subset* $S \subset E^n$ *be a component of a correlation immune function of order* $n - m$ *with* $2^{n-m+1} > |S|$. *Then*

$$|S| = 2^{n-m+1} - 2^p, \quad \textit{where} \quad p \in \{0, \dots, n-m\}.$$

Moreover, a component of cardinality 2^{n-m} *is a linear code.*

Proof. Since the cardinality of a component is half the cardinality of a double component, from Propositions 3 and 5 we get the desired constraints on component cardinalities. Proposition 4 implies that the double component $A = S \cup S'$, $|A| = 2^{n-m+1}$, of a correlation immune function of order $n - m$ is a linear code. Then A intersects any face of the n-cube in either the empty set or a set of cardinality 2^t, where t is an integer. Moreover, a nonempty intersection of A with an $(m+1)$-face has cardinality of at least 4. Then the component S is a bitrade of order $n - m - 1$. Now Propositions 2 and 4 yield the result. △

Remark 2. A component of a correlation immune function f of order $n-m$ has algebraic degree of at most $2 \deg f$. Therefore, for $m < \frac{n}{2}$ the component cardinality is even.

Here are consequences of Proposition 6 and Corollaries 1 and 2.

Corollary 3. *Let* f *be a perfect coloring with parameter matrix* $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$. *Let* $S \subset E^n$ *be a component of* f, *and let* $2^{\frac{b+c}{2}} > |S|$. *Then*

$$|S| = 2^{\frac{b+c}{2}} - 2^p, \quad \textit{where} \quad p \in \Bigl\{0, \dots, \frac{b+c}{2} - 1\Bigr\}.$$

Moreover, a component of cardinality $2^{\frac{b+c}{2}-1}$ *is a linear code.*

Corollary 4. *Let* $S \subset E^n$ *be a component of a perfect code* $C \subset E^n$, *and let* $2^{\frac{n+1}{2}} > |S|$. *Then*

$$|S| = 2^{\frac{n+1}{2}} - 2^p, \quad \textit{where} \quad p \in \Bigl\{1, \dots, \frac{n-1}{2}\Bigr\}.$$

Moreover, a component of cardinality $2^{\frac{n-1}{2}}$ *is a linear code.*

3. COMPONENTS OF PERFECT COLORINGS AND CORRELATION IMMUNE FUNCTIONS

The minimum cardinality ($2^{\frac{n-1}{2}}$) of a component of a perfect code of length n is well known; linearity of the minimal component was proved by Avgustinovich [15]. Components of the minimum possible cardinality are contained in any linear code (Hamming code). For perfect colorings, components of the minimum cardinality were constructed in [16]. Also, it was proved there that a component of the minimum cardinality is a linear code, and a family of perfect colorings that contain components of the minimum cardinality $2^{\frac{b+c}{2}-1}$ was presented.

In [3], all possible cardinalities of intersections of linear perfect codes were found. In particular, it was shown that linear perfect codes may intersect in a quarter of their vertices. One easily computes that the cardinality of a perfect code in E^7 is 2^4, which is twice the minimum cardinality of a component. Thus, for $n = 7$, two linear codes intersecting in a quarter of vertices generate a component of cardinality 1.5 as large as the minimum. For $n > 7$, components of perfect codes (of length n) of an intermediate cardinality between $2^{\frac{n-1}{2}}$ and $2^{\frac{n+1}{2}}$ are not known. Moreover, one can show that there are no components of intermediate cardinalities in perfect codes (for $n > 7$) of rank (dimension of the affine hull) greater by at most two than that of a linear code. Indeed, in [17] it is proved that all perfect codes of such ranks can be obtained by the Phelps construction (see [18]) from quaternary MDS codes, and in [19] it is proved that in this construction components of quaternary codes are in a one-to-one correspondence with components of perfect codes. In [20] it is shown that quaternary MDS codes have no components of the required cardinality. Below we construct 2-fold perfect codes with components of an intermediate cardinality between the minimum and twice the minimum cardinality.

Let Q_q be a nonempty set of a finite cardinality q. An *MDS code with distance* $d+1$ is a subset $M \subset Q_q^n$ that intersects every d-face of the q-ary n-cube Q_q^n in exactly one vertex. If every d-face contains exactly t elements of M, then M is said to be a *t-fold MDS* code. Thus, the notion of a multifold MDS code is equivalent to the notion of a Boolean-valued correlation immune function defined on the q-ary hypercube. Below we consider only MDS codes with distance 2, which are sometimes called trivial, since they exist for any space dimension n and any alphabet cardinality $q > 1$.

The following fact is known.

Proposition 7 [20]. *For any $t \geq 3$ and $p \in \{0, \ldots, t-1\}$ there exists a 2-fold MDS code $B_t^p \subset Q_4^t$ with a component of cardinality $2^t - 2^p$.*

The construction designed in [18] relates MDS codes with perfect codes. In [16], a generalization of that construction was proposed, which allows one to construct perfect colorings with parameter matrix

$$\begin{pmatrix} 0 & k(2^s-1) \\ k & k(2^s-2) \end{pmatrix}. \tag{2}$$

Let us briefly repeat the construction. Let $m = 2^{s-2}$ and $n = (2^s-1)k$, $s \geq 2$. Fix $\widetilde{R} \subset E^{m-1}$, a linear perfect code (Hamming code). Let

$$r \in E^{k(m-1)}, \quad \widetilde{r} = \left(\bigoplus_{i=1}^{k} r_i, \ldots, \bigoplus_{i=k(m-2)+1}^{k(m-1)} r_i \right), \quad R = \{r \in E^{k(m-1)} : \widetilde{r} \in \widetilde{R}\}.$$

For any $r \in R$, fix an MDS code $M_r \subset Q_4^{km}$ (with distance 2). Denote

$$\begin{array}{llll}
C_0^0 = \{0000, 1111\}, & C_1^0 = \{1001, 0110\}, & C_2^0 = \{0101, 1010\}, & C_3^0 = \{0011, 1100\}, \\
C_0^1 = \{0001, 1110\}, & C_1^1 = \{1000, 0111\}, & C_2^1 = \{0100, 1011\}, & C_3^1 = \{0010, 1101\}, \\
C_0 = \{000\ \ , 111\ \ \}, & C_1 = \{100\ \ , 011\ \ \}, & C_2 = \{010\ \ , 101\ \ \}, & C_3 = \{001\ \ , 110\ \ \}.
\end{array}$$

Define the set $P \subset E^n$, where $n = (2^s-1)k$, by

$$P = \bigcup_{r \in R} \bigcup_{\alpha \in M_r} Q_{\alpha,r}, \quad Q_{\alpha,r} = C_{\alpha_1}^{r_1} \times C_{\alpha_2}^{r_2} \times \ldots \times C_{\alpha_{k(m-1)}}^{r_{k(m-1)}} \times C_{\alpha_{k(m-1)+1}} \times \ldots \times C_{\alpha_{km}}. \tag{3}$$

Proposition 8 [16]. *Let a set $P \subset E^n$ be given by* (3). *Then χ^P is a perfect coloring with parameter matrix* (2).

In [21], a generalization of the construction from [18] was proposed, which makes it possible to construct multifold perfect codes using multifold MDS codes. Similarly, let us use 2-fold MDS codes instead of 1-fold codes in the construction from [16]. Consider the set

$$S_{p,m,k} = \bigcup_{r \in R} \bigcup_{\alpha \in B^p_{km}} Q_{\alpha,r}, \quad Q_{\alpha,r} = C^{r_1}_{\alpha_1} \times C^{r_2}_{\alpha_2} \times \ldots \times C^{r_{k(m-1)}}_{\alpha_{k(m-1)}} \times C_{\alpha_{k(m-1)+1}} \times \ldots \times C_{\alpha_{km}}, \tag{4}$$

where B^p_{km} is a 2-fold MDS code defined in Proposition 7.

Theorem 1. *Let $p \in \{0, \ldots, km-1\}$, and let the set $S_{p,m,k} \subset E^n$ be given by* (4). *Then*

(a) $\chi^{S_{p,m,k}}$ *is a perfect coloring with parameter matrix*

$$\begin{pmatrix} k & k(2^s-2) \\ 2k & k(2^s-3) \end{pmatrix}, \tag{5}$$

where $n = (2^s-1)k$ and $m = 2^{s-2}$, $s \geq 2$, $k \geq 1$, $km \geq 3$;

(b) *The perfect coloring $\chi^{S_{p,m,k}}$ has a component of cardinality $(2^{km} - 2^p)2^{km}$.*

The proof of claim (a) of Theorem 1 is quite similar to that of Proposition 8 [16, Theorem 2]. Claim (b) follows from Proposition 7.

As is stated above, for perfect colorings there is an estimate for their correlation immunity that depends on parameters of the coloring only. In particular, the function $\chi^{S_{p,m,k}}$ is correlation immune of order $2km-1$. Let $f\colon E^n \to E$ be a correlation immune function of order i. Then the function $g\colon E^{n+n'} \to E$ given by $g(x,y) = f(x) \oplus y_1 \oplus \ldots \oplus y_{n'}$ is correlation immune of order $i+n'$. Thus, Theorem 1 in the case of $m = 1$ yields the following result.

Corollary 5. *Let $n = 3k + n'$ and $r = 2k + n' - 1$, $k \geq 3$. For any $p \in \{0, \ldots, k-1\}$ there exists a correlation immune function $g\colon E^{n+n'} \to E$ of order r having a component of cardinality $(2^k - 2^p)2^{k+n'}$.*

4. COMPONENTS OF BENT FUNCTIONS AND MOBILE SETS

The set of functions $a\colon E^n \to \mathbb{Q}$ can be considered as a 2^n-dimensional vector space $\mathbb{V}$ over $\mathbb{Q}$. It is known that functions of the form $f^v(u) = (-1)^{\langle u,v \rangle}$, $v \in E^n$, form an orthogonal basis of $\mathbb{V}$. The *Fourier transform* of a function a is a function $\widehat{a}$ whose values

$$\widehat{a}(v) = \sum_{u \in E^n} a(u)(-1)^{\langle u,v \rangle}$$

are inner products of the vectors a and f^v in $\mathbb{V}$. Introduce the notation σ_f for the function $\sigma_f(x) = (-1)^{f(x)}$. The numbers $\widehat{\sigma}_f(v)$, $v \in E^n$, are called *Walsh–Hadamard coefficients* of the Boolean function f.

Correlation immune functions and perfect colorings can be described in terms of the Walsh–Hadamard coefficients.

Proposition 9 (see [2, 12]). *A Boolean function $f = \chi^S$ is correlation immune of order m if and only if $\widehat{\sigma}_f(v) = 0$ for any $v \in E^n$ such that $0 < \mathrm{wt}(v) \leq m$.*

Proposition 10 [22]. (a) *Let f be a perfect coloring with parameter matrix $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$. Then $\widehat{\sigma}_f(v) = 0$ for any $v \in E^n$ with $\mathrm{wt}(v) \neq 0, \dfrac{b+c}{2}$.*

(b) *Let a Boolean function f be such that $\widehat{\sigma}_f(v) = 0$ for any $v \in E^n$ with $\mathrm{wt}(v) \neq 0, k$. Then f is a perfect coloring.*

Let $f\colon E^n \to E$ be a Boolean function, and let $w \in E^n$. By

$$\mathrm{wt}(f_w) = |\{x \in E^n \mid f(x) = 1,\ [x, 1 \oplus w] = x\}|$$

we denote the number of ones of a subfunction obtained by substituting 0 in all arguments x_i of f such that $w_i = 1$.

Proposition 11 ([23]; see also [2]). *For any Boolean function $f\colon E^n \to E$, one has*

$$\sum_{\substack{v \in E^n \\ [v,w]=v}} \widehat{\sigma}_f(v) = 2^n - 2^{\mathrm{wt}(w)+1}\,\mathrm{wt}(f_w) \qquad (\textit{Sarkar identity}).$$

From the Sarkar identity, one easily obtains the following fact.

Proposition 12. *Let f be a Boolean function, and let $\widehat{\sigma}_f(v) \equiv 0 \pmod{2^k}$ for any $v \in E^n$. Then* $\deg f \le n - k + 1$.

Proof. Let $\deg f > n-k+1$. Consider a nonzero term of the maximum degree in the Zhegalkin polynomial of f. Let $G[f](y) = 1$ and $\mathrm{wt}(y) = \deg f$. Then $\mathrm{wt}(f_{y\oplus 1}) \equiv 1 \pmod 2$. For the Sarkar identity, we have

$$\sum_{\substack{v \in E^n \\ [v,y\oplus 1]=v}} \widehat{\sigma}_f(v) = 2^n - 2^{n-\mathrm{wt}(y)+1}\,\mathrm{wt}(f_{y\oplus 1}) \equiv 1 \pmod{2^{n-\mathrm{wt}(y)+2}} \not\equiv 0 \pmod{2^k}. \quad \triangle$$

The Sarkar identity and Proposition 9 imply the following result (see, e.g., [2]).

Proposition 13. *Let $f\colon E^n \to E$ be a correlation immune function of order m, $m \le n-1$. Then $\widehat{\sigma}_f(v) \equiv 0 \pmod{2^{m+1}}$ for any $v \in E^n$.*

Note that Proposition 3 (a) can be proved independently using Propositions 12 and 13.

Paper [7] uses the notion of a *shifting set* in E^n, which is a union of two codes C_1 and C_2 with distance 3 having the same neighborhood. Define a function $h\colon E^n \to \mathbb{Q}$ by $h = \chi^{C_1} - \chi^{C_2}$. It is seen from the definition that the sum of values of h over any ball of radius 1 is 0, i.e., the function h is 0-*centered*. The following fact is known.

Proposition 14 [24]. *Let $h\colon E^n \to \mathbb{Q}$ be a 0-centered function. Then $\widehat{h}(v) = 0$ if $\mathrm{wt}(v) \ne \dfrac{n+1}{2}$.*

In particular, this proposition implies that shifting sets can be contained in Boolean cubes of odd dimensions only.

Proposition 15. *Any shifting set $C \subset E^n$ is a bitrade of order $\dfrac{n-1}{2}$.*

Proof. By the definition, a shifting set C is a union of codes C_1 and C_2 with distance 3, and $h = \chi^{C_1} - \chi^{C_2}$ is a 0-centered function. The subspace of $\mathbb{V}$ generated by all functions f^v with $\mathrm{wt}(v) \le m$ contains characteristic functions of all faces of dimensions at least $n-m$. Then Proposition 14 implies that the inner product (h, χ^F) is zero for any face G of dimension $\dfrac{n+1}{2}$. Hence, $|C_1 \cap G| = |C_2 \cap G|$, and $|C \cap G|$is even. $\triangle$

From Propositions 2, 4, 5 and 15, we get the following result.

Corollary 6. *Let $S \subset E^n$ be a shifting set, and let $2^{\frac{n+3}{2}} > |S|$. Then*

$$|S| = 2^{\frac{n+3}{2}} - 2^p, \quad \textit{where} \quad p \in \Big\{1, \ldots, \frac{n+1}{2}\Big\}.$$

Moreover, a shifting set of cardinality $2^{\frac{n+1}{2}}n$ is a linear code.

Note that pairs of alternative components of 2-fold perfect codes constructed in Section 3, i.e., pairs of perfect colorings with parameter matrix $\begin{pmatrix} 1 & (2^s-2) \\ 2 & (2^s-3) \end{pmatrix}$, are shifting sets.

A Boolean function f is a *bent function* if and only if $\widehat{\sigma}_f(v) = \pm 2^{n/2}$ for any $v \in E^n$ and n is even (see, e.g., [25]).

Theorem 2. (a) *Let a set $S \subset E^n$ be a component of a bent function f, and let $2^{\frac{n}{2}} > |S|$. Then*

$$|S| = 2^{\frac{n}{2}} - 2^p, \quad \textit{where} \quad p \in \{0, \ldots, n/2 - 1\}.$$

Moreover, a component of cardinality $2^{\frac{n}{2}-1}$ is a linear code.

(b) *For any $p \in \{0, \ldots, n/2 - 1\}$ there exists a bent function $f\colon E^n \to E$ having a component of cardinality $2^{\frac{n}{2}} - 2^p$.*

Proof. Similarly to the proof of Proposition 12, one can easily get from the Sarkar identity that $\deg f \le n/2$ for any bent function f in E^n (see also [12]). Then (a) follows from Propositions 4 and 5. Let us construct a bent function with components of the required cardinalities. Let $x, y \in E^{n/2}$, and let λ be an arbitrary Boolean function in $E^{n/2}$. It is known (see, e.g., [12,25]) that the Boolean function $f(x,y) = \langle x, y\rangle \oplus \lambda(y)$ is a bent function. Then the functions

$$f^1(x,y) = \langle x, y\rangle \oplus y_1 \ldots y_{n/2},$$
$$f^2_p(x,y) = \langle x, y\rangle \oplus y_1 \ldots y_p x_{p+1} \ldots x_{n/2}$$

are bent functions; moreover,

$$\mathrm{wt}(f^1 \oplus f^2_p) = 2^p(2^{\frac{n}{2}-p+1} - 2).$$

Hence, the bent function f^1 has a component of cardinality $2^{\frac{n}{2}} - 2^p$. △

Properties of minimum-cardinality components of bent functions were considered in [10,26,27]. In particular, in [10] it is proved that a component of a bent function of cardinality $2^{\frac{n}{2}-1}$ is a linear code, and in [26] it is proved that if a bent function is affine on an affine set of dimension $n/2$, then this set is a double component.

REFERENCES

1. Fon-Der-Flaass, D.G., A Bound on Correlation Immunity, *Sib. Elektron. Mat. Izv.*, 2007, vol. 4, pp. 133–135.

2. Tarannikov, Yu.V., On Correlation-Immune and Stable Boolean Functions, *Mat. Vopr. Kibern.*, vol. 11, Moscow: Fizmatlit, 2002, pp. 91–148.

3. Etzion, T. and Vardy, A., On Perfect Codes and Tilings: Problems and Solutions, *SIAM J. Discrete Math.*, 1998, vol. 11, no. 2, pp. 205–223.

4. Avgustinovich, S.V., Heden, O, and Solov'eva, F.I., On Intersections of Perfect Binary Codes, *Bayreuth. Math. Schr.* 2005, no. 74, pp. 1–6.

5. Avgustinovich, S.V., Heden, O., and Solov'eva, F.I., On Intersection Problem for Perfect Binary Codes, *Des. Codes Cryptogr.*, 2006, vol. 39, no. 3, pp. 317–322.

6. Avgustinovich, S.V., Lobstein, A.C., and Solov'eva, F.I., Intersection Matrices for Partitions by Binary Perfect Codes, *IEEE Trans. Inform. Theory*, 2001, vol. 47, no. 4, pp. 1621–1624.

7. Vasil'ev, Yu.L., Avgustinovich, S.V., and Krotov, D.S., On Shifting Sets in the Binary Hypercube, *Diskretn. Anal. Issled. Oper.*, 2008, vol. 15, no. 3, pp. 11–21 [*J. Appl. Ind. Math.* (Engl. Transl.), 2009, vol. 3, no. 2, pp. 290–296].

8. Heden, O., Soloveva, F.I., and Mogilnykh, I.Yu., Intersections of Perfect Binary Codes, in *Proc. 2010 IEEE Region 8 Int. Conf. on Computational Technologies in Electrical and Electronics Engineering (SIBIRCON), Irkutsk Listvyanka, Russia, 2010.* Piscataway: IEEE, 2010, pp. 52–54.

9. Soloveva, F.I. and Los', A.V., Intersections of q-ary Perfect Codes, *Sibirsk. Mat. Zh.*, 2008, vol. 49, no. 2, pp. 464–474 [*Sib. Math. J.* (Engl. Transl.), 2008, vol. 49, no. 2, pp. 375–382].

10. Kolomeec, N.A. and Pavlov, A.V., Properties of Bent Functions with Minimal Distance, *Prikl. Diskr. Mat.*, 2009, no. 4, pp. 5–20.

11. Kasami, T. and Tokura, N., On the Weight Structure of Reed–Muller Codes, *IEEE Trans. Inform. Theory*, 1970, vol. 16, no. 6, pp. 752–759.

12. Logachev, O.A., Sal'nikov, A.A., and Yashchenko, V.V., *Bulevy funktsii v teorii kodirovaniya i kriptologii* (Boolean Functions in Coding Theory and Cryptology), Moscow: MCCME, 2004.

13. MacWilliams, F.J. and Sloane, N.J.A., *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977. Translated under the title *Teoriya kodov, ispravlyayushchikh oshibki*, Moscow: Svyaz', 1979.

14. Kasami, T., Tokura, N., and Azumi, S., On the Weight Enumeration of Weights Less than $2.5d$ of Reed–Muller Codes, *Inform. and Control*, 1976, vol. 30, no. 4, pp. 380–395.

15. Avgustinovich, S.V., private communication (talk given at the Coding Theory seminar, Institute of Mathematics, Siberian Branch of the Russian Academy of Sciences), 2003.

16. Potapov, V.N., On Perfect Colorings of Boolean n-Cube and Correlation Immune Functions with Small Density, *Sib. Elektron. Mat. Izv.*, 2010, vol. 7, pp. 372–382.

17. Avgustinovich, S.V., Heden, O., and Solov'eva, F.I., The Classification of Some Perfect Codes, *Des. Codes Cryptogr.*, 2004, vol. 31, no. 3, pp. 313–318.

18. Phelps, K.T., A General Product Construction for Error Correcting Codes, *SIAM J. Algebr. Discrete Methods*, 1984, vol. 5, no. 2, pp. 224–228.

19. Krotov, D.S. and Potapov, V.N., On Switching Equivalence of n-ary Quasigroups of Order 4 and Perfect Binary Codes, *Probl. Peredachi Inf.*, 2010, vol. 46, no. 3, pp. 22–28 [*Probl. Inf. Trans.* (Engl. Transl.), 2010, vol. 46, no. 3, pp. 219–224].

20. Potapov, V.N., Latin Bitrade, ArXiv e-print `arXiv:1104.1295v1`, 2011.

21. Krotov, D.S. and Potapov, V.N., On Multifold MDS and Perfect Codes That Are Not Splittable into Onefold Codes, *Probl. Peredachi Inf.*, 2004, vol. 40, no. 1, pp. 6–14 [*Probl. Inf. Trans.* (Engl. Transl.), 2004, vol. 40, no. 1, pp. 5–12].

22. Fon-Der-Flaas, D.G., Perfect 2-Colorings of a Hypercube, *Sibirsk. Mat. Zh.*, 2007, vol. 48, no. 4, pp. 923–930 [*Sib. Math. J.* (Engl. Transl.), 2007, vol. 48, no. 4, pp. 740–745].

23. Sarkar, P., Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions, Cryptology ePrint Archive: Report 2000/049, 2000. Available at `http://eprint.iacr.org/2000/049`.

24. Avgustinovich, S.V. and Vasil'eva, A.Yu., Computation of a Centered Function from Its Values on the Middle Layers of the Boolean Cube, *Diskretn. Anal. Issled. Oper., Ser. 1*, 2003, vol. 10, no. 2, pp. 3–16.

25. Tokareva, N.N., Bent Functions: Results and Applications. A Survey, *Prikl. Diskr. Mat.*, 2009, no. 1, pp. 15–37.

26. Carlet, C., Boolean Functions for Cryptography and Error Correcting Codes, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Crama, Y. and Hammer, P.L., Eds., Cambridge: Cambridge Univ. Press, 2010, ch. 8, pp. 257–397.

27. Carlet, C., Two New Classes of Bent Functions, *Advances in Cryptology—EUROCRYPT'93. Proc. Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway*, Helleseth, T., Ed., Lect. Notes Comp. Sci., vol. 765, Berlin: Springer, 1994, pp. 77–101.