On the connection between correlation-immune functions and perfect 2-colorings of the Boolean $n$-cube

Vladimir N. Potapov

Sobolev Institute of Mathematics, Novosibirsk State University, Novosibirsk

Abstract

A coloring of the Boolean $n$-cube is called perfect if, for every vertex $x$, the collection of the colors of the neighbors of $x$ depends only on the color of $x$. A Boolean function is called correlation-immune of degree $n-m$ if it takes the value 1 the same number of times for each $m$-face of the Boolean $n$-cube. In the present paper it is proven that each Boolean function $\chi^S$ ($S \subset E^n$) satisfies the inequality

$$\text{nei}(S) + 2(\text{cor}(S) + 1)(1 - \rho(S)) \leq n,$$

where $\text{cor}(S)$ is the maximum degree of the correlation immunity of $\chi^S$, $\text{nei}(S) = \frac{1}{|S|} \sum_{x \in S} |B(x) \cap S| - 1$ is the average number of neighbors in the set $S$ for vertices in $S$, and $\rho(S) = |S|/2^n$ is the density of the set $S$. Moreover, the function $\chi^S$ is a perfect coloring if and only if we obtain an equality in the above formula.

Keywords: hypercube, perfect coloring, perfect code, correlation-immune function.

Let $E^n = \{0,1\}^n$ be the $n$-dimensional Boolean cube ($n$-cube). Define the operation $[x,y] = (x_1y_1, \ldots, x_ny_n)$ and the inner product $\langle x, y \rangle = x_1y_1 \oplus \cdots \oplus x_ny_n$ for vectors $x, y \in E^n$. The number of unities in a vector $y \in E^n$ is called the weight of $y$ and is denoted by $\text{wt}(y) = \langle y, 1 \rangle$. The sets $E^n_y(z) = \{x \in E^n : [x, y] = [z, y]\}$, where $\text{wt}(y) = m$, are called $(n-m)$-faces.

Let $S \subset E^n$ and let $\chi^S$ be the characteristic function of $S$. The function $\chi^S$ is said to be correlation-immune of order $n-m$ if, for all $m$-faces $E^n_y(z)$, the intersections $E^n_y(z) \cap S$ have the same cardinality. The maximum order of the correlation immunity of the function $\chi^S$ is denoted by $\text{cor}(S)$, $\text{cor}(S) = \max\{n-m\}$. The number $\rho(S) = |S|/2^n$ is the density of the function $\chi^S$. We will always assume that $\rho(S) \leq 1/2$, since otherwise we may consider $E^n \setminus S$ instead of $S$. If $\rho(S) = 1/2$ then the correlation immune function $\chi^S$ is called balanced.

The Hamming distance $d(x, y)$ between two vectors $x, y \in \Sigma^n$ is the number of positions at which they differ. The unit ball $\{y \in E^n : d(x, y) \leq 1\}$ is denoted by $B(x)$. Define the

*The work is supported by RFBR (grants 10-01-00424, 10-01-00616)
neighbors number \( \text{nei}(S) \) to be the average number of neighbors in the set \( S \) for vertices in \( S \), i.e., \( \text{nei}(S) = \frac{1}{|S|} \sum_{x \in S} |B(x) \cap S| - 1 \).

A mapping \( \text{Col} : E^n \to \{1, \ldots, k\} \) is called a perfect coloring with matrix of parameters \( A = \{a_{ij}\} \) if, for all \( i, j \), for every vertex of color \( i \), the number of its neighbors of color \( j \) is equal to \( a_{ij} \). In what follows we will only consider colorings in two colors. Moreover, for convenience we will assume that the set of colors is \( \{0, 1\} \). In this case the function \( \text{Col} \) is Boolean and \( \text{Col} = \chi^S \), where \( S \) is the set of 1-colored vertices.

A perfect code \( C \subset E^n \) can be defined as a perfect coloring with matrix of parameters \( A = \begin{pmatrix} 0 & n \\ 1 & n - 1 \end{pmatrix} \). Colorings with such parameters exist only if \( n = 2^m - 1 \) (\( m \) is integer).

A list of accessible parameters and corresponding constructions of perfect colorings can be found in [1] and [2].

It is well known (see [3]) that a perfect coloring of the \( n \)-cube with matrix of parameters \( \begin{pmatrix} n - b & b \\ c & n - c \end{pmatrix} \) is a correlation-immune function of degree \( b + c - 1 \). Therefore, if the vertices of some set \( S \) are regularly distributed on balls then the vertices of the set are uniformly distributed on faces. It is of interest to clarify the possibility of the reverse implication.

In [3] it is established that for each unbalanced Boolean function \( \chi^S \) \( (S \subset E^n) \) the inequality \( \text{cor}(S) \leq \frac{2n}{3} - 1 \) holds. Moreover, in the case of the equality \( \text{cor}(S) = \frac{2n}{3} - 1 \), the function \( \chi^S \) is a perfect coloring. Similarly, if for any set \( S \subset E^n \) the Bierbrauer-Friedman inequality \( \rho(S) \geq 1 - \frac{n}{2(\text{cor}(S) + 1)} \) becomes an equality then the function \( \chi^S \) is a perfect 2-coloring (see [4]). Consequently, in the extremal cases, the regular distribution on balls follows from the uniform distribution on faces. In the present paper we prove the following theorem:

**Theorem 1.**

(a) For each Boolean function \( a = \chi^S \), where \( S \subset E^n \) and \( \rho(S) \leq 1/2 \), the inequality \( \text{nei}(S) + 2(\text{cor}(S) + 1)(1 - \rho(S)) \leq n \) holds.

(b) A Boolean function \( a = \chi^S \) is a perfect 2-coloring if and only if \( \text{nei}(S) + 2(\text{cor}(S) + 1)(1 - \rho(S)) = n \).

In the proof of the theorem we employ the idea from the papers [4] and [7]. Before proceeding to the proof we introduce some necessary concepts.

The set \( \mathbb{V} \) of all functions \( a : E^n \to \mathbb{Q} \) has the natural structure of an \( 2^n \)-dimensional vector space. It is well known that the functions \( f^v(u) = (-1)^{(u,v)} \), where \( v \in E^n \), constitute a Fourier orthogonal basis of the space \( \mathbb{V} \). The Fourier transform \( \hat{a} \) of a function \( a \) is determined by the equality

\[
\hat{a}(v) = \sum_{u \in E^n} a(u)(-1)^{(u,v)}. 
\]

Obviously, the function \( \hat{a} \) is the inner product of the vectors \( a \) and \( f^v \) in \( \mathbb{V} \). Since \( \langle f^v, f^v \rangle = 2^n \) for every vertex \( v \in E^n \), we have the equalities

\[
a(u) = \frac{1}{2^n} \sum_{v \in E^n} \hat{a}(v)(-1)^{(u,v)},
\]

(1)
\[ 2^n \sum_{u \in E^n} a^2(u) = \sum_{v \in E^n} \hat{a}^2(v). \quad (2) \]

We need the following well-known statements.

**Proposition 1.** ([2], [8]) A Boolean function \( a = \chi_S \) is correlation immune of degree \( m \) if and only if \( \hat{a}(v) = 0 \) for every \( v \in E^n \) such that \( 0 < \text{wt}(v) \leq m \).

**Proposition 2.** ([1])

(a) Let \( a = \chi_S \) be a perfect coloring with matrix of parameters \( \left( \begin{array}{cc} n - b & b \\ c & n - c \end{array} \right) \).

Then \( \hat{a}(v) = 0 \) for every \( v \in E^n \) such that \( \text{wt}(v) \neq 0, \frac{b+c}{2} \).

(b) Let \( a = \chi_S \) be a Boolean function. If \( \hat{a}(v) = 0 \) for every vertex \( v \in E^n \) such that \( \text{wt}(v) \neq 0, k \) then \( a \) is a perfect coloring.

**Corollary 1.** Let \( a = \chi_S \) be a perfect coloring with matrix of parameters \( \left( \begin{array}{cc} n - b & b \\ c & n - c \end{array} \right) \).

Then \( \text{cor}(S) = \frac{b+c}{2} - 1 \).

Put \( a'(v) = \hat{a}(v)/|S| \). From (2) we obtain

\[ \sum_{v \in E^n} (a'(v))^2 = \frac{2^n}{|S|^2} \sum_{u \in E^n} a^2(u) = \frac{2^n}{|S|}. \quad (3) \]

Given a Boolean function \( a = \chi_S \), the weight distribution \( (B_0(a), \ldots, B_n(a)) \) is determined by

\[ B_i(a) = \frac{1}{|S|} |\{v, u \in S \mid \text{wt}(u + v) = i\}|. \]

 Obviously, \( B_1(a) = \text{nei}(S) \), where \( a = \chi_S \).

The MacWilliams transform of a weight distribution \( (B_0(a), \ldots, B_n(a)) \) is the array \( (B'_0(a), \ldots, B'_n(a)) \), where \( B'_k(a) = \frac{1}{|S|} \sum_{i=0}^{n} B_i(a) P_k(i) \) and \( P_k \) are the Kravchuk polynomials.

In [8] the following equalities are proven:

\[ B_k(a) = \frac{|S|}{2^n} \sum_{i=0}^{n} B'_i(a) P_k(i), \quad (4) \]

\[ B'_k(a) = \sum_{\text{wt}(v)=k} (a'(v))^2. \quad (5) \]

From (3) and (5) we obtain the following:

**Corollary 2.** If \( \overline{0} \in S \) and \( a = \chi_S \) then

(a) \( B'_k(a) \geq 0 \) for \( i = 0, \ldots, n \);

(b) \( B'_k(a) = 0 \iff a'(v) = 0 \) for every vector \( v \in E^n \) with weight \( \text{wt}(v) = k \);

(c) \( B'_0(a) = 1 \);

(d) \( \sum_{i=0}^{n} B'_k(a) = 2^n / |S| \).
Propositions 1, 2 and Corollary 2 (b) imply the following well-known statements (see [3] and [7]).

**Corollary 3.** If $0 \in S$ and $a = \chi^S$ then $B_k'(a) = 0$ for $0 < k \leq \text{cor}(S)$.

**Corollary 4.** Let $0 \in S$, $a = \chi^S$, and let $B_k'(a) = 0$ for $i \neq 0, k$. Then $\chi^S$ is a perfect coloring.

**Proof of the theorem.** Without lost of generality we suppose that $0 \in S$. Put $t = \text{cor}(S)$. From (4), Corollary 2 (c), and Corollary 3 we obtain the equality

\[ \text{nei}(S)/\rho(S) = P_1(0) + \sum_{i=t+1}^{n} B_k'(a)P_1(i). \]

Since $P_1(i) = n - 2i$ (see [7] or [8]), we have

\[ \text{nei}(S)/\rho(S) \leq n + \sum_{i=t+1}^{n} B_k'(a)(n - 2i). \]

Corollary 2 (a), (d) implies $\sum_{i=0}^{n} B_k'(a) = 1/\rho(S)$ and $B_k'(a) \geq 0$. Hence,

\[ \text{nei}(S) \leq \rho(S)n + (n - 2(t + 1))(1 - \rho(S)). \]

Moreover, the equality

\[ \text{nei}(S) = \rho(S)n + (n - 2(t + 1))(1 - \rho(S)) \] (6)

holds if and only if $B_k'(a) = 0$ for $i \geq t + 2$. Then from Corollary 4 (b) we conclude that $\chi^S$ is a perfect coloring.

Each perfect 2-coloring satisfies (6), which is a consequence of Proposition 2 (b) and Corollary 3 (b). △

For perfect codes, a similar theorem was previously proven in [7]. Namely, if $\text{cor}(S) = \text{cor}(H)$ and $\rho(S) = \rho(H)$, where $S, H \subset E^n$ and $H$ is a perfect code, then $S$ is also a perfect code.

**References**

1. D.G. Fon-Der-Flaass, *Perfect 2-colorings of a hypercube*, Siberian Math. J. 48:4 (2007), 740–745.

2. D.G. Fon-Der-Flaass, *Perfect 2-colorings of the 12-cube that attain the bounds on correlation immunity*, (Russian) Sib. Elektron. Mat. Izv. 4 (2007), 292–295.

3. D.G. Fon-Der-Flaass, *A bound of correlation immunity*, Siberian Electronic Mathematical Reports, 4 (2007), 133–135.
4. J. Friedman, *On the bit extraction problem*, Proc. 33rd IEEE Symposium on Foundations of Computer Science (1992), 314-319.

5. J. Bierbrauer, *Bounds on orthogonal arrays and resilient functions*, Journal of Combinatorial Designs, 3 (1995), 179-183.

6. V.N. Potapov, *On perfect colorings of Boolean n-cube and correlation immune functions with small density*, (Russian) Sib. Elektron. Mat. Izv. 7 (2010), 372–382.

7. P.R.J. Oстergard, O. Pottonen, and 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.

8. F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.