Criterion for perfect 2-coloring of the q-ary n-cube

V. N. Potapov

Seminar of Sobolev Institute of Mathematics

December 6, 2012

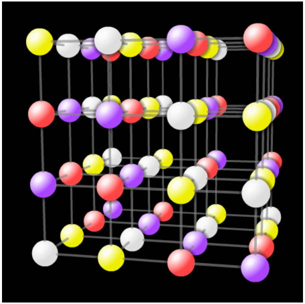
Let Z_q be the set $\{0, \ldots, q-1\}$. The set Z_q^n of n-tuples over Z_q is called q-ary n-dimensional cube (hypercube). The Hamming distance $d(x, y)$ between two n-tuples $x, y \in Z_q^n$ is the number of positions at which they differ.

Definition

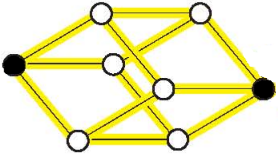
A correlation immune function of order $n-m$ is a function $f : Z_q^n \to U$ whose each value is uniformly distributed on all m-dimensional faces.

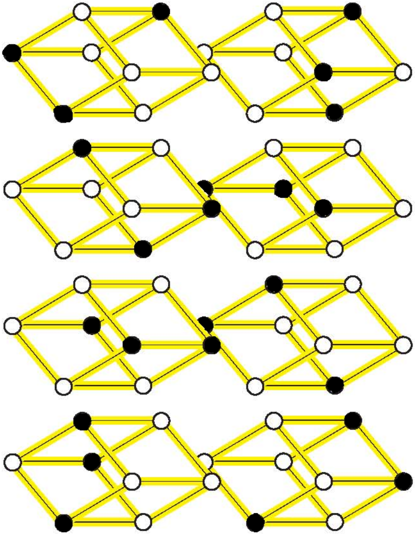
For any function f we denote the maximum order of its correlation immunity by $\mathrm{cor}(f) = \max\{n-m\}$.

Latin cube



Perfect 1-error correcting binary code.





Definition

The density of the Boolean valued function $f : Z_q^n \to Z_2$ is equal to $\rho(f) = \frac{|\{x \in Z_q^n \mid f(x)=1\}|}{q^n}$.

Theorem (Friedman, 1992, Bierbrauer, 1995)

The inequality $q(\mathrm{cor}(f) + 1) \leq \frac{n(q-1)}{1-\rho(f)}$ holds for every function $f : Z_q^n \to Z_2$.

Definition

Define the number $a(\chi^C)$ to be the average number of neighbors in a set $C \subseteq Z_q^n$ for n-tuples in the complement of C, i. e. $a(\chi^C) = \frac{1}{q^n - |C|} \sum_{x \notin C} |\{y \in C \mid d(x,y) = 1\}|$.

$$a(f) \leq \frac{q^n \rho(f) n(q-1)}{q^n(1-\rho(f))}$$

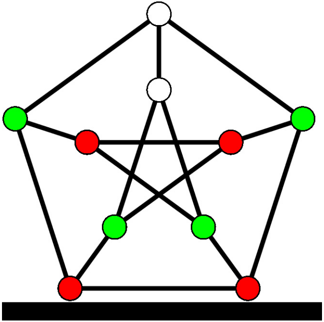
Theorem

The inequality $\rho(f)q(\mathrm{cor}(f) + 1) \leq a(f)$ holds for every function $f : Z_q^n \to Z_2$.

Let $S(x)$ be a sphere $S(x) = \{y \in Z_q^n : d(x, y) = 1\}$, where d is Hamming distance.

Definition

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 x of color i, the number of its neighbors of color j is equal to $p_{ij} = |Col^{-1}(j) \cap S(x)|$.



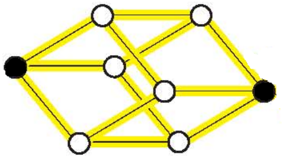
$$\begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 1 \end{pmatrix}$$

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.

Proposition

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 $P = \begin{pmatrix} n(q-1)-1 & 1 \\ n(q-1) & 0 \end{pmatrix}$.

1-Perfect codes there exists only if $n = \frac{q^j - 1}{q-1}$.



Theorem (Tarannikov, 2002)

Let f be a perfect 2-coloring with the matrix of parameters $P = \begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ Then $\mathrm{cor}(f) = \frac{c+b}{q} - 1$.

Theorem (Fon-Der-Flaass, 2007)

Let $f : Z_2^n \to Z_2$ be a Boolean function, $0 < \rho(f) < 1/2$. Than the inequality $\mathrm{cor}(f) \leq \frac{2n}{3} - 1$ holds and if $\mathrm{cor}(f) = \frac{2n}{3} - 1$ than f is a perfect 2-coloring.

Theorem (Delsarte, 1972, Pulatov, 1976, Ostergard, Pottonen, Phelps, 2010)

Boolean function f is a characteristic function of an 1-perfect code if and only if $\mathrm{cor}(f) = \frac{n-1}{2}$ and $\rho(f) = \frac{1}{n+1}$.

Theorem (Potapov, 2010)

Boolean function f is a perfect 2-coloring with the parameter $p_{11} = 0$ if and only if $\rho(f) = 1 - \frac{n}{2(\mathrm{cor}(f)+1)}$.

Theorem

Boolean-valued function $f : Z_q^n \rightarrow Z_2$ is a perfect 2-coloring if and only if the equation $\rho(f)q(\mathrm{cor}(f)+1) = a(f)$ holds.

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 $\langle x, z \rangle = x_1 z_1 + \cdots + x_n z_n$.

Proposition

The characters of the group $Z_q \times \cdots \times Z_q$ form an orthonormal basis of $\mathbb{V}$.

Let M be the adjacency matrix of the hypercube Z_q^n.
This means that $Mf(x) = \sum_{y, d(x,y)=1} f(y)$.

Proposition

The characters are eigenvectors of M with eigenvalue $((n - wt(z))(q-1) - wt(z))$, where $wt(z)$ is the number of nonzero coordinates of z.

Proposition

(a) Let f be a perfect 2-coloring with the matrix of parameters P. 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 $z \in Z_q^n$ such that $wt(z) \neq 0, s$ then f is a perfect 2-coloring.

Proposition

(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 $0 < wt(z) \leq m$.

Let $f : Z_q^n \to Z_2$ then

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

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

$$(Mf, f) = (n(q-1) - a(f))\rho(f).$$