Lecture 3: Hamming codes. Reed-Muller codes.

Invited lecturer: Grigory Kabatiansky

g.kabatyansky@skoltech.ru

Teaching Assistant: Stanislav Kruglik

stanislav.kruglik@skolkovotech.ru

February 2, 2018

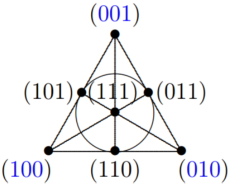
Outline

Outline

Hamming code and Fano plane

The Hamming Code and the projective plane of order the $PG(2,2)$ (Fano plane) are closely related.

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \; G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \quad \leftrightarrow$$



Extended binary Hamming code

The extended binary Hamming code is the code obtained from binary hamming code by adding a check bit. In the PCM we add additional row and column. PCM is presented below.

$$\bar{H} = \left[\begin{array}{ccc|c} & & & 0 \\ & H & & \vdots \\ & & & 0 \\ \hline 1 & \cdots & 1 & 1 \end{array}\right]$$

Because we add addition parity check bit our code distance is increased by one, so the parameters of code are the following: $n = 2^m$,$k = 2^m - m - 1$, $d = 4$.

PCM **H** of non-binary Hamming code has the property that its columns are made up of precisely one nonzero vector from each vector subspace of dimension 1 of $\mathbb{F}_q^m$.

$$H_m^q = \left.\boxed{\begin{array}{cccccc} 0 & 0 & 0 & & 0 & 1 \\ 0 & 0 & 0 & & 1 & * \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & & * & * \\ 0 & 0 & 1 & & * & * \\ 0 & 1 & * & & * & * \\ 1 & * & * & & * & * \end{array}}\right\} m$$

The parameters of the resulting code are as follows. $n = \frac{q^m-1}{q-1}$, $k = n - m$ and $|\mathcal{C}| = \frac{q^n}{1+n(q-1)}$. The code is also perfect.

Open problem

Are there perfect codes with $d = 3$ if $q \neq p^m$, where p is a prime number?

Dual code to binary Hamming code

The dual of a code $\mathcal{C}$ is denoted by $\mathcal{C}^\perp$. For a linear code $\mathcal{C}$ with parity check matrix $\mathbf{H}$, $\mathcal{C}^\perp$ is the linear code with generator matrix $\mathbf{H}$.

The dual of the Hamming code is a linear code with parameters $[2^m - 1, m]$ with a generator matrix whose rows are all the nonzero m-bit vectors. This is the Simplex code. If we include the zero column, we obtain the Hadamard code $[2^m, m]$. We note that the Hadamard code is the most redundant linear code in which no two codeword symbols are equal in every codeword. Its distance is equal to $n/2$

Outline

Definition

Let us consider a boolean function (Zhegalkin polynomial) from m variables with degree no more than s. The coefficients correspond to information bits. A value of this polynomial in all points of m-dimensional Boolean cube is a codeword (evaluation code). This code is called a $RM(m, s)$ code. The parameters of this code are the following: $n = 2^m$, $k = \sum_{i=0}^{s} \binom{m}{i}$.

Plotkin construction

Let us introduce some notation

- U – linear $[n, k_U, d_U]$ code;
- V – linear $[n, k_V, d_V]$ code;

Plotkin construction

$$\mathcal{C} = U \triangle V = (U, U + V) = \{(u, u + v) : u \in U, v \in V\}.$$

Properties: linear, $n(\mathcal{C}) = 2n$, $k(\mathcal{C}) = k_U + k_V$.
$d(\mathcal{C}) = \min\{d_V, 2d_U\}$

Code distance

Lemma

$RM(s, m) = RM(m-1, s) \triangle RM(m-1, s-1).$

Proof.

$$f(x_1, x_2, \ldots, x_m) = Q(x_1, x_2, \ldots, x_{m-1}) + x_m P(x_1, x_2, \ldots, x_{m-1}),$$

where $\deg Q \leq s$ and $\deg P \leq s-1$. $\square$

Code distance

Lemma

$$d(RM(m,s)) = 2^{m-s}.$$

Proof.

By induction. Base

$$d(RM(m,1)) = 2^{m-1}.$$

Thus,

$$\begin{aligned} d(RM(m,s)) &= \min\{d(RM(m-1,s)), 2d(RM(m-1,s-1))\} \\ &= 2^{m-s}. \end{aligned}$$

$\square$

Outline

Problem 1

Show that in binary linear code either all words have even weight or half of them have odd weight

Problem 2

Prove that if U-linear $[n, k_U, d_U]$ code and V-linear $[n, k_V, d_V]$ code then $d(U \triangle V) = min(d_V, 2d_U)$

Problem 3

Construct a finite field $\mathbb{F}_2^8$ over modulo of polynomial $\phi(x) = x^3 + x^2 + 1$ and find the values of $\alpha^4 + \alpha^2$ and $(\alpha^4)^2$

Thank you for your attention!