On the reconstruction of Preparata-like codes

Anastasia Yu. Vasil'eva

Sobolev Institute of Mathematics,
Novosibirsk, RUSSIA

ACCT-2016

Notations

$\mathbf{Q}^n = \{0,1\}^n$ – n-dimensional binary Hamming space, with component-wise modulo-2 addition and the Hamming metric.
$wt(\alpha) = \sum_{i=1}^{n} |\alpha_i|$ – the Hamming weight of the vector α
$\rho(\alpha, \beta) = wt(\beta - \alpha)$ – the Hamming distance between words α and β.
$W_i = \{\beta \in \mathbf{Q}^n \ : \ wt(\beta) = i\}$

Hypercube

The graph of n-dimensional binary hypercube

vertices: $\mathbf{Q}^n$,
edges: (α, β), if $\rho(\alpha, \beta) = 1$.

Adjacency matrix

$2^n \times 2^n$,

$$D_{\alpha,\beta} = \begin{cases} 1, & \rho(\alpha, \beta) = 1 \\ 0, & other \end{cases}$$

Eigenvalues

$n - 2i, \ i = 0, 1, \ldots, n.$

Eigenfunctions

$V = \{f : \mathbf{Q}^n \longrightarrow \mathbb{C}\}$
$f \leftrightarrow (f(0,\ldots,0), f(0,\ldots,0,1),\ldots,f(1,\ldots,1))^T$

Eigensubspace V_i

The eigenvalue: $n-2i$. The orthogonal basis:
$B_i = \{f^{\mathbf{a}} : \mathbf{Q}^n \to \mathbf{R} \ : \ \mathbf{a} \in W_i\}$, where $f^{\mathbf{a}}(\mathbf{x}) = (-1)^{\langle \mathbf{a},\mathbf{x}\rangle}$

$V_0 = \{f \equiv const\}$
An orthogonal basis of V:
$B_0 \bigcup B_1 \bigcup \ldots \bigcup B_n$.

The orthogonal projection

For any set $C \in \mathbf{Q}^n$ we denote by $f_C^{(h)}$ the orthogonal projection of the characteristic function χ_C onto the eigensubspace V_h,
$\chi_C = f_C^{(0)} + f_C^{(1)} + \ldots + f_C^{(n)}$.

Fourier transform

The matrix

$a_{\mathbf{xy}} = f^{\mathbf{x}}(\mathbf{y}) = (-1)^{\langle \mathbf{x},\mathbf{y} \rangle}, \ \mathbf{x}, \mathbf{y} \in \mathbf{Q}^n$,
$A = (a_{\mathbf{xy}})$ defines the orthogonal transform that is called Fourier transform.

Let us denote by $A^{ij}_{(n)}$ the submatrix of $A = A_{(n)}$ with rows corresponding to the vertices from W_i and columns corresponding to the vertices of W_j.

Perfect codes: definition

$n = 2^t - 1$

Definition

The code $C \subseteq \mathbf{Q}^n$ is perfect if the balls of radius 1 centered in the code words do not intersect and cover all Q^n.

The code distance is equal to 3.
Perfect codes of length n exist for every n of form $n = 2^t - 1$ and do not exist for any other n.

The characteristic function

$\chi_C = f_C^{(0)} + f_C^{((n+1)/2)}$

Reconstruction of Perfect Binary Codes

$n = 2^t - 1$ is odd

$$|W_{(n-1)/2}| = |W_{(n+1)/2}| = max_{i=0,1,\ldots,n}|W_i|$$

Reconstruction

$$C \bigcap W_{(n+1)/2} \rightarrowtail C$$

Preparata codes: definition

$n = 4^t - 1$

Definition

A code is Preparata-like (or shortly, Preparata code), if
the length is $n = 4^t - 1$
the code distance is 5
the cardinality $2^{n+1}/(n+1)^2$.

$P \subseteq C(P)$

Every Preparata code P is contained in a unique perfect code $C(P)$.

Perfect colorings: definition

Definition

A vertex partition $(D_0, \dots, D_r)$ is called a perfect coloring (or equitable partition, or regular partition, or partition design) if for every $i, j \in \{0, \dots, r\}$ there exists an integer s_{ij} such that every vertex from D_i has exactly s_{ij} neighbors from D_j.

The matrix $S = (s_{ij})$ is called the parameter matrix of the coloring.

Preparata code: coloring

A Preparata code P induces a perfect coloring D by distances:
$D_0 = P, D_1, D_2, D_3 = C(P) \setminus P$

The parameter matrix: $S = \begin{bmatrix} 0 & n & 0 & 0 \\ 1 & 0 & n-1 & 0 \\ 0 & 2 & n-3 & 1 \\ 0 & 0 & n & 0 \end{bmatrix}$

with the eigenvalues $n, -1, -1 \pm \sqrt{n+1}$

The characteristic function of the color $D_i, i = 0, 1, 2, 3,$

$\chi_{D_i} = f_{D_i}^{(0)} + f_{D_i}^{(k)} + f_{D_i}^{((n+1)/2)} + f_{D_i}^{(h)}$
$k = \frac{n+1}{2} - \frac{\sqrt{n+1}}{2}, \quad h = \frac{n+1}{2} + \frac{\sqrt{n+1}}{2}.$

It is easy to see that $f_P^{(0)} = \frac{2}{(n+1)^2}$.

Results

Lemma

Let P be an arbitrary Preparata code and $C(P)$ be the perfect code which contains P. Then

$$f_P^{((n+1)/2)} = \frac{2}{n+1} f_{C(P)}^{((n+1)/2)}.$$

Results

For a Preparata code P define the function $F_P = \chi_P - \frac{2}{n+1}\chi_{C(P)}$ with the following values:

$$F_P(\mathbf{x}) = \begin{cases} \frac{n-1}{n+1}, & \mathbf{x} \in P \\ -\frac{2}{n+1}, & \mathbf{x} \in C(P) \setminus P \\ 0, & \mathbf{x} \notin C(P) \end{cases}$$

This function is antipodal, i.e. $F_P(\mathbf{x}) = F_P(\mathbf{1} + \mathbf{x})$, because the codes P and $C(P)$ are antipodal.

Results

Theorem

Let P be a Preparata code. Then

$$F_P \in V_k \times V_h, \qquad k = \frac{n+1}{2} - \frac{\sqrt{n+1}}{2}, \quad h = \frac{n+1}{2} + \frac{\sqrt{n+1}}{2}$$

.

Krawtchouk polynomials

Definition

The Krawtchouk polynomial:

$$K_i(l, N) = \sum_{j=0}^{i} (-1)^j \binom{l}{j} \binom{N-l}{i-j} \quad i = 0, \ldots, N.$$

$$(1-t)^l (1+t)^{N-l} = \sum_{m=0}^{N} K_m(l; N) t^m,$$

Results

Theorem

Let P be a Preparata code. If

$$K_i(i, 2i + \sqrt{n+1}) \neq 0, \quad i = 0, \dots, k,$$

then the pair of codes P and $C(P)$ is uniquely determined by the sets $P \cap (W_{k-1} \cup W_k)$ and $C(P) \cap (W_{k-1} \cup W_k)$.

Notes

The value $K_i(i, 2i + \sqrt{n+1})$ is equal to the coefficient at t^i of the polynomial $(1 - t^2)^i (1 + t)^{\sqrt{n+1}}$.

$K_i(i, 2i + \sqrt{n+1}) \neq 0$ for all $i = 0, \dots, k$, for small n, for $n = 15$ and $n = 63$.

The author hopes that it is true for all $n = 4^m - 1$.

Thank you for your attention!