Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 296–300*

On the reconstruction of Preparata-like codes [1]

Anastasia Vasil'eva vasilan@math.nsc.ru
Sobolev Institute of Mathematics,
Novosibirsk State University, Novosibirsk, RUSSIA

Abstract. We study the Fourier transform of Preparata-like codes and perfect codes containing Preparata-like codes. We try to reconstruct these codes by theirs vertices belonging to two concentric spheres.

1 Introduction

We study codes in the *n-dimensional binary Hamming space*, or hypercube, consisting from the set Q_n of all binary n-tuples (words), with component-wise modulo-2 addition and the Hamming metric. The *support* $\mathrm{supp}(\alpha)$ of the word α is the set of its nonzero positions; the cardinality of the support of a word α is its *Hamming weight* $\mathrm{wt}(\alpha)$. The *Hamming distance* $\rho(\alpha, \beta)$ between words α and β is the Hamming weight of $\alpha + \beta$.

A set $C \subseteq Q^n$ of M words with mutual distance at least d is called a *binary (n, M, d) code*, i.e., a code of length n, size M, and distance d. A code is called *perfect (with distance 3)* if the balls of radius 1 centered in the code words do not intersect and cover all Q_n. It is straightforward from the definition that the minimal distance between codewords is 3. Perfect codes of length n exist for every n of form $n = 2^t - 1$ and do not exist for any other n. In the half of the cases, namely, when t is even, there are Preparata-like codes (in what follows, we will call them as Preparata codes) of length $n = 2^t - 1$, which are defined as the codes of distance 5 and size $2^{n+1}/(n + 1)^2$. Every Preparata code P is included in a unique perfect code [3]; we denote it as $C(P)$.

A vertex partition $(D_0, \ldots, D_r)$ is called a perfect coloring (or equitable partition, or regular partition, or partition design) if for every $i, j \in \{0, \ldots, r\}$ there is 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.

It is well known that the eigenvalues of the graph of n-dimensional hypercube are equal to $n - 2i$, $i = 0, 1, \ldots, n$. The corresponding eigenfunctions satisfy the equation

$$\sum_{\mathbf{y}\in N(\mathbf{x})} f(\mathbf{y}) = (n - 2i)f(\mathbf{x}), \quad i = 0, 1, \ldots, n, \tag{1}$$

[1] The work was funded by the Russian science foundation (grant 14-11-00555)

where $\mathbf{x}$ is an arbitrary vertex of the hypercube and $N(\mathbf{x})$ is the set of all neighbors of $\mathbf{x}$.

Consider an orthogonal basis of a space of all real functions over the hypercube:

$$\left\{ f^{\mathbf{a}} : \mathbf{Q}^n \to \mathbf{R} \ : \ f^{\mathbf{a}}(\mathbf{x}) = (-1)^{\langle \mathbf{a}, \mathbf{x} \rangle}, \ \ \mathbf{a} \in \mathbf{Q}^n \right\}.$$

A function $f^{\mathbf{a}}$, $\mathbf{a} \in \mathbf{Q}^n$, is the eigenfunction with the eigenvalue $n - 2wt(\mathbf{a})$. So, the set of functions

$$\{ f^{\mathbf{a}} : \mathbf{Q}^n \to \mathbf{R} \ : \ \mathbf{a} \in W_i \} \tag{2}$$

forms the basis of the eigensubspace V_i with the eigenvalue $\lambda = n - 2i$, $i = 0, 1, \ldots, n$. This subspace consists of all functions such that their Fourier coefficients can be nonzero only on the i-th level of the hypercube. The subspace V_0 is 1-dimensional and consists of constant functions.

For any code C we denote by $f_C^{(h)}$ the orthogonal projection of the characteristic function χ_C onto the eigensubspace V_h. So, χ_C can be uniquely represented as the sum

$$\chi_C = f_C^0 + f_C^1 + \ldots + f_C^n.$$

The matrix A with elements $a_{\mathbf{xy}} = f^{\mathbf{x}}(\mathbf{y})$, $\mathbf{x}, \mathbf{y} \in \mathbf{Q}^n$, defines the orthogonal transform that is called Fourier transform. Let us denote by $A_{(n)}^{ij}$ the submatrix of A with rows corresponding to the vertices from W_i and columns corresponding to the vertices of W_j. Mentioned conditions can be expressed in terms of submatrices of matrix A of the Fourier transform.

It was shown in [1] that under some condition any function from V_i is uniquely determined by its values on W_i. Analogously, under some condition any function from $V_i \times V_j$ is uniquely determined by its values on $W_i \cup W_j$ [2].

Let us denote by $K_i(t, N)$, $i = 0, \ldots, N$, the Krawtchouk polynomial:

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

2 Fourier transform of Preparata codes

It is known that each Preparata code P induces a perfect coloring D by distances from the code P. The coloring D has four colors $D_0 = P, D_1, D_2, D_3$, moreover, $D_3 = C(P) \setminus P$. The parameter matrix of the coloring D is

$$S = \begin{bmatrix} 0 & n & 0 & 0 \\ 1 & 0 & n-1 & 0 \\ 0 & 2 & n-3 & 1 \\ 0 & 0 & n & 0 \end{bmatrix}.$$

Since the eigenvalues of S are

$$n, -1, -1 \pm \sqrt{n+1},$$

then the characteristic function of each color belongs to the subspace

$$V_0 \times V_k \times V_{(n+1)/2} \times V_h, \qquad k = \frac{n+1}{2} - \frac{\sqrt{n+1}}{2}, \quad h = \frac{n+1}{2} + \frac{\sqrt{n+1}}{2}.$$

Then the characteristic function of the color $D_i, i = 0, 1, 2, 3$, is represented as a sum of four eigenfunctions:

$$\chi_{D_i} = f^{(0)}_{D_i} + f^{(k)}_{D_i} + f^{((n+1)/2)}_{D_i} + f^{(h)}_{D_i}.$$

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

Lemma 1 *Let P be a Preparata code and $C(P)$ be the perfect code which contains P. Then*

$$f^{((n+1)/2)}_P = \frac{2}{n+1} f^{((n+1)/2)}_{C(P)}.$$

Proof. It is well-known that for any perfect code C holds $\chi_C - 1/(n+1) \in V_{(n+1)/2}$, i.e.

$$\chi_C = 1/(n+1) + f^{((n+1)/2)}_C.$$

In particular, it is true for the perfect code which contains the Preparata code P. As far as $D_3 = C(P) \setminus P$ and $\chi_{C(P)} = \chi_P + \chi_{D_3}$ then

$$f^{(k)}_P + f^{(k)}_{D_3} = 0,$$

$$f^{(h)}_P + f^{(h)}_{D_3} = 0,$$

$$f^{(((n+1)/2)}_P + f^{(((n+1)/2))}_{D_3} = f^{(((n+1)/2)}_{C(P)}. \tag{3}$$

The set D_2 is, on the one hand, the set of all vertices at distance 2 from the code P, on the other hand, the set of all vertices at distance 1 from the set $D_3 = C(P) \setminus P$. Then first,

$$\chi_{D_2}(\mathbf{x}) = \sum_{1 \le i < j \le n} \chi_P(\mathbf{x} + \mathbf{e^i} + \mathbf{e^j}),$$

and second,

$$\chi_{D_2}(\mathbf{x}) = \sum_{i=1}^{n} \chi_{D_3}(\mathbf{x} + \mathbf{e^i}).$$

Using these equations and the definition of eigenfunction, we get the equations for the eigenfunctions. First,

$$f_{D_2}^{((n+1)/2)}(\mathbf{x}) = \sum_{1\le i<j\le n} f_P^{((n+1)/2)}(\mathbf{x}+\mathbf{e^i}+\mathbf{e^j}) =$$

$$\frac{1}{2}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} f_P^{((n+1)/2)}((\mathbf{x}+\mathbf{e^j})+\mathbf{e^i}) - nf_P^{((n+1)/2)}(\mathbf{x})\right) =$$

$$\frac{1}{2}\left(\sum_{j=1}^{n}(-f_P^{((n+1)/2)}(\mathbf{x}+\mathbf{e^j}) - nf_P^{((n+1)/2)}(\mathbf{x})\right) =$$

$$\frac{1}{2}\left(f_P^{((n+1)/2)}(\mathbf{x}) - nf_P^{((n+1)/2)}(\mathbf{x})\right) = -\frac{n-1}{2}f_P^{((n+1)/2)}(\mathbf{x}).$$

Second,

$$f_{D_2}^{((n+1)/2)}(\mathbf{x}) = \sum_{i=1}^{n} f_{D_3}^{((n+1)/2)}(\mathbf{x}+\mathbf{e^i}) = -f_{D_3}^{((n+1)/2)}(\mathbf{x}).$$

Comparing two expressions for $f_{D_2}^{((n+1)/2)}$ we have that

$$\frac{n-1}{2}f_P^{((n+1)/2)} = f_{D_3}^{((n+1)/2)}.$$

Now using 3 we finally get that

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

Lemma is proved.

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.

Lemma 1 implies the following

Theorem 1 *Let P be a Preparata code. Then*

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

.

We try to use Theorem 1 to reconstructing a Preparata code by its subset.

Theorem 2 *Let P be a Preparata code. If*

$$K_i(i, 2i + \sqrt{n+1}) \neq 0, \quad i = 0, \dots, k, \tag{4}$$

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

Proof. Any function $f \in V_k \times V_h$ is uniquely determined by its values $\{f(\mathbf{x}) \ : \ \mathbf{x} \in W_k \cup W_h\}$ if and only if the matrix

$$\begin{bmatrix} A^{kk}_{(n)} & A^{kh}_{(n)} \\ A^{hk}_{(n)} & A^{hh}_{(n)} \end{bmatrix}$$

is invertible [2]. It is easy to see that

$$\begin{bmatrix} A^{kk}_{(n)} & A^{kh}_{(n)} \\ A^{hk}_{(n)} & A^{hh}_{(n)} \end{bmatrix} = A^{kk}_{(n+1)}.$$

The eigenvalues of $A^{kk}_{(n+1)}$ are

$$\lambda_j(k, n+1) = (-2)^j K_{k-j}(k-j, n+1-2j), \quad j = 0, \dots, k$$

Substitution $i = k - j$ implies that $A^{kk}_{(n+1)}$ is invertible if and only if $K_i(i, 2i + \sqrt{n+1}) \neq 0$ for all $i = 0, \dots, k$. Theorem is proved.

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

The values $K_i(i, 2i + \sqrt{n+1}) \neq 0$ for all $i = 0, \dots, k$, are nonzero for small n, more exactly, for $n = 15$ and $n = 63$. The author hopes to prove these inequalities for all $n = 4^m - 1$.

References

[1] A.Yu. Vasil'eva, On reconstruction of generalized centered functions, *Proc. of Ninth Int. Workshop on Algebraic and Combinatorial Coding Theory 19-25 June, 2004*, Kranevo, Bulgaria. P. 384-389.

[2] A. Yu. Vasil'eva, On reconstructive sets of vertices in the Boolean cube, *Diskretn. Anal. Issled. Oper.*, 19:1 (2012), P. 316.

[3] G. V. Zaitsev, V. A. Zinoviev, and N. V. Semakov. Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error-correcting codes. In P. N. Petrov and F. Csaki, editors, *Proc. 2nd Int. Symp. Information Theory, Tsahkadsor, Armenia, USSR, 1971*, P. 257–264, Budapest, Hungary, 1973. Akademiai Kiado.