Partial reconstruction of perfect binary codes *

Anastasia Yu. Vasil'eva

This paper continues the research published in [1, 2, 3, 4]. It was shown in [1] that a perfect code is uniquely determined by its vertices in the middle levels of a hypercube, and the concerned formula was obtained in [2] and [3]. In [4] it was proved that the vertices in the h-th level, $h \leq (n-1)/2$, of the code of length n uniquely determine all code vertices in the lower levels. In this paper we derive the reconstruction formula. As in [3, 4], centered functions, which are the generalization of perfect codes, are the subject of the consideration. The question on reconstruction of perfect binary codes was also investigated in [5], where a way to reach a formula was specified.

We are planning the following. Let us introduce vector F^j of 0-centered function f values at all vertices of the j-th level of the hypercube and an auxiliary vector U^j of the same dimension, $j \leq (n+1)/2$. Suppose that the vector F^h is known. Our main goal is to find an expression of the vector F^j presentation for any $j \leq h$, using the vector $F^h, h \leq (n+1)/2$, (Theorem 2). Three steps are undertaken. First, we express the vector F^j in terms of the vector U^j. Second, we define the vector U^j using the vector U^h. Third, we determine the vector U^h in terms of the vector F^h. The first step consists of combinatorial calculations (Lemmas 1, 2, 3 and 4). The second containing Lemma 5 is obvious. The last step is accomplished using the theory of association schemes (Lemma 6).

Section 1 contains essential definitions and facts on centered functions and the theory of association schemes. In section 2 we present technical combinatorial Lemmas 1, 2 and 3. Section 3 includes lemmas corresponding to the three above mentioned steps and the main theorem.

1 Definitions and essential facts

We denote n-dimensional vector space over $GF(2)$ by E^n and call it a hypercube. Let us consider Hamming metric in E^n, i. e. Hamming distance $\rho(\mathbf{x}, \mathbf{y})$ between vertices $\mathbf{x}$ and $\mathbf{y}$ of the hypercube is equal to the number of positions where the vertices differ. Hamming weight $wt(\mathbf{x})$ of vertex $\mathbf{x}$ is equal to the number of nonzero positions of $\mathbf{x}$. Define a partial ordering on E^n: $\mathbf{x} \preceq \mathbf{y}$ if $x_i \leq y_i,\ i = 1, \ldots, n$, where $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$.

Denote by W_r a set of all vertices with weight r and call it the r-th level of the hypercube. We use a special symbol for the middle level: $A = W_{(n+1)/2}$. The Johnson distance $g(\mathbf{x}, \mathbf{y})$ between vertices $\mathbf{x}, \mathbf{y} \in W_h,\ h = 0, \ldots, n,$ is a half of the Hamming distance between them.

A *perfect binary single-error-correcting code* C (briefly a *perfect code*) of length n is a subset of E^n such that the set of all balls of radius 1 with centers in C forms a partition of the hypercube.

A *ϑ-centered function* $f : E^n \to \mathbf{R}$ is a function such that the sum of its values in a ball of the radius 1 equals to ϑ. It is easy to see that the characteristic function of a perfect code

*This work is supported by Russian Foundation for Basic Research under the grant ° 00-01-00822

is 1-centered. An arbitrary function is ϑ-centered if and only if this function is the sum of a 0-centered function and the constant ϑ-centered function. Hence, without loss of generality we can consider only 0-centered functions.

Let $f : E^n \to \mathbf{R}$ be a 0-centered function. We can prove

Proposition 1. *A function $f : E^n \to \mathbf{R}$ is 0-centered if and only if f is a linear combination of functions*

$$f^{\mathbf{a}}(\mathbf{x}) = (-1)^{\langle \mathbf{a},\mathbf{x} \rangle}, \;\; \mathbf{x} \in A.$$

Moreover, if a function $\varphi : A \to \mathbf{R}$ is defined by a formula

$$\varphi(\mathbf{a}) = \sum_{\mathbf{x} \succeq \mathbf{a}} f(\mathbf{x}), \tag{1}$$

then the following statement is true.

Proposition 2. *Let $f : E^n \to \mathbf{R}$ be a 0-centered function and $\mathbf{x} \in E^n$. Then*

$$f(\mathbf{x}) = \frac{1}{2^{(n-1)/2}} \sum_{\mathbf{a} \in A} (-1)^{\langle \mathbf{a},\mathbf{x} \rangle} \varphi(\mathbf{a}). \tag{2}$$

The function φ is referred to as the Fourier transformation of the function f.

The following theorem was proved in [4].

Theorem 1. *Let f be an arbitrary 0-centered function, $j \leq h \leq (n+1)/2$, and $\mathbf{x} \in W_j$. Then the value of the function f at the vertex $\mathbf{x}$ is uniquely determined by the values $f(\mathbf{z}), \mathbf{z} \in W_h$.*

From the proof of this theorem it was not clear how to obtain the corresponding formula. Another approach is suggested in the paper.

Some concepts and statements of the theory of association schemes are useful to remind.

By $E_k(x; h)$ denote the Eberlein polynomial:

$$E_k(x;h) = E_k(x;h,n) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{h-x}{k-j} \binom{n-h-x}{k-j}.$$

The Johnson association scheme is a set of all vertices of the h-th level W_h with relations $R_i, 0 \leq i \leq h$, such that

$$(\mathbf{x}, \mathbf{y}) \in R_i \Longleftrightarrow g(\mathbf{x}, \mathbf{y}) = i.$$

These relations can be described by their incidence matrices D_i^h, i.e. square (0,1)-matrices of size $|W_h| \times |W_h|$, rows and columns of which correspond to the vertices of W_h and the elements are

$$(D_i^h)_{\mathbf{x},\mathbf{y}} = \begin{cases} 1, & \text{if } \; g(\mathbf{x}, \mathbf{y}) = i, \\ 0, & \text{otherwise.} \end{cases}$$

The set of incidence matrices $D_i^h, \; i = 0, \ldots, h,$ forms a basis of a vector space which is an algebra called the Bose-Mesner algebra of the scheme. This algebra has another basis which consists of primitive idempotents $J_i^h, \; i = 0, \ldots, h,$ such that

$$\sum_{i=0}^{h} J_i^h = E; \qquad (J_i^h)^2 = J_i; \qquad J_i^h J_j^h = 0; \qquad 0 \leq i, j \leq h, \;\; i \neq j.$$

From these properties follows

Proposition 3. *Let the matrix P be invertible and be a linear combination of association scheme idempotents, i.e. there exist nonzero coefficients $\alpha_i \in \mathbf{R}$, $i = 0, \ldots, h$, such that $P = \sum_{i=0}^{h} \alpha_i J_i$. Then $P^{-1} = \sum_{i=0}^{h} \alpha_i^{-1} J_i$.*

The following interdependence between two mentioned bases of Bose-Mesner algebra holds:

$$D_k^h = \sum_{i=0}^{h} E_k(i;h) J_i^h, \tag{3}$$

$$J_i^h = \frac{1}{|W_h|} \sum_{k=0}^{h} q_i(k;h) D_k^h, \tag{4}$$

where

$$q_i(j;h) = \frac{\mu_i}{v_j} E_j(i;h),$$

$$\mu_i = \frac{n-2i+1}{n-i+1} \binom{n}{i}, \qquad v_j = \binom{h}{j} \binom{n-h}{j}.$$

2 Preliminary lemmas

In this section we are going to prove some technical lemmas. Let us introduce some notation. Throughout the paper $f : E^n \to \mathbf{R}$ denotes a 0-centered function. Let $\mathbf{x} \in W_j$. Denote

$$u(\mathbf{x}) = \sum_{\mathbf{a} \in A,\ \mathbf{a} \succeq \mathbf{x}} \varphi(\mathbf{a}); \tag{5}$$

$$\sigma_l(\mathbf{x}) = \sum_{\mathbf{a} \in A,\ \langle \mathbf{a}, \mathbf{x} \rangle = l} \varphi(\mathbf{a}); \tag{6}$$

$$d_m(\mathbf{x}) = \sum_{\mathbf{y} \in W_m,\ \mathbf{y} \preceq \mathbf{x}} u(\mathbf{y}). \tag{7}$$

We will use the following vectors:
Φ is the vector of the values for φ at all vertices belonging to the middle level $A = W_{(n+1)/2}$;
F^j is the vector of the values for f at all vertices belonging to the j-th level W_j, $j = 0, \ldots, h$;
U^j is the vector of the values for u at all vertices belonging to the j-th level W_j, $j = 0, \ldots, h$.

Our main goal is to find the expression of the vector F^j for any $j \le h$ over the vector F^h. Now we are ready to carry out our threestep plan (see introductory comments).

Lemma 1. *Let $\mathbf{x} \in W_j$ and $m \le j$. Then*

$$d_m(\mathbf{x}) = \frac{1}{\binom{(n+1)/2 - m}{j-m}} \sum_{l=m}^{j} \binom{l}{m} \sum_{\mathbf{z} \in W_j,\ \langle \mathbf{x}, \mathbf{z} \rangle = l} u(\mathbf{z}). \tag{8}$$

Proof. It easy to see that for any vertex $\mathbf{y} \in W_m,\ m \le j$,

$$u(\mathbf{y}) = \frac{1}{\binom{(n+1)/2-m}{j-m}} \sum_{\mathbf{z}\in W_j,\ \mathbf{z}\succeq\mathbf{y}} u(\mathbf{z}).$$

Hence, according to (7),

$$d_m(\mathbf{x}) = \sum_{\mathbf{y}\in W_m,\ \mathbf{y}\preceq\mathbf{x}} \frac{1}{\binom{(n+1)/2-m}{j-m}} \sum_{\mathbf{z}\in W_j,\ \mathbf{z}\succeq\mathbf{y}} u(\mathbf{z}).$$

The number of entries of the summand $u(\mathbf{z})$ in this double sum depends only on the scalar product of vertices $\mathbf{x}, \mathbf{z} \in W_j$ and is equal to

$$|\{\mathbf{y} \in W_m : \mathbf{y} \preceq \mathbf{x},\ \mathbf{y} \preceq \mathbf{z}\}| = \binom{\langle \mathbf{x}, \mathbf{z}\rangle}{m}.$$

Hence formula (8) is true. $\bigtriangledown$

Lemma 2. *Let $\mathbf{x} \in W_j$ and $m \le j$. Then*

$$d_m(\mathbf{x}) = \sum_{t=m}^{j} \binom{t}{m} \sigma_t(\mathbf{x}). \tag{9}$$

Proof. The proof is similar to the proof of Lemma 1. By definitions (6) and (7) we have

$$d_m(\mathbf{x}) = \sum_{\mathbf{y}\in W_m,\ \mathbf{y}\preceq\mathbf{x}} \ \sum_{\mathbf{a}\in A,\ \mathbf{a}\succeq\mathbf{y}} \varphi(\mathbf{a}).$$

In the last sum the number of entries of the summand $\varphi(\mathbf{a})$ depends only on the scalar product of vertices $\mathbf{x} \in W_j$ and $\mathbf{a} \in A$. This number is equal to the binomial coefficient $\binom{\langle \mathbf{a}, \mathbf{x}\rangle}{m}$. Hence the formula (9) is true. $\bigtriangledown$

Lemma 3. *Let $\mathbf{x} \in W_j$ and $l \le j$. Then*

$$\sigma_l(\mathbf{x}) = \sum_{m=l}^{j} (-1)^{m+l} \binom{m}{l} d_m(\mathbf{x}). \tag{10}$$

Proof. From Lemma 2 for any $\mathbf{x} \in W_j$ we get the following matrix equation:

$$d(\mathbf{x}) = M^j \sigma(\mathbf{x}),$$

where

$$d(\mathbf{x}) = (d_0(\mathbf{x}), d_1(\mathbf{x}), \ldots, d_j(\mathbf{x}))^T,$$
$$\sigma(\mathbf{x}) = (\sigma_0(\mathbf{x}), \sigma_1(\mathbf{x}), \ldots, \sigma_j(\mathbf{x}))^T$$

and M^j is the triangular matrix of size $(j+1)\times(j+1)$ with elements $(M^j)_{kt} = \begin{pmatrix} t \\ k \end{pmatrix}$.

The vector $\sigma(\mathbf{x})$ is required. So it is necessary to invert the matrix M^j. The matrix $(M^j)^{-1}$ exists because M^j is a triangular matrix with nonzero diagonal. We can check directly that the matrix $(M^j)^{-1}$ consists of the elements $(M^j)_{kl} = (-1)^{k+l}\begin{pmatrix} l \\ k \end{pmatrix}$. In fact,

$$(M^j(M^j)^{-1})_{kl} = \sum_{t=k}^{l}(-1)^{t+l}\begin{pmatrix} l \\ t \end{pmatrix}\begin{pmatrix} t \\ k \end{pmatrix} = \begin{cases} 1, & \text{if } k=l, \\ 0, & \text{otherwise.} \end{cases}$$

The last equation is well known. Finally, $\sigma(\mathbf{x}) = (M^j)^{-1}d(\mathbf{x})$ and we get (10). $\triangledown$

3 Main result

The principal lemmas and the main theorem are included in this section. In Lemma 4 we present the vector F^j as a linear transformation of the vector U^j. This linear transformation is inverted in Lemma 6. In Lemma 5 we express the vector U^j in terms of the vector U^h. Our main goal is to find the expression of the vector F^j for any $j \le h$ in terms of the vector F^h.

Let us introduce a square matrix B^j, $j \le (n+1)/2$, of size $\begin{pmatrix} n \\ j \end{pmatrix} \times \begin{pmatrix} n \\ j \end{pmatrix}$. Its rows and columns correspond to vertices of the j-th level W_j of the hypercube and its elements are uniquely determined by the scalar products of vertices $\mathbf{x}, \mathbf{z} \in W_j$, i.e. the row corresponds to the vertex $\mathbf{x}$ and the column corresponds to the vertex $\mathbf{z}$, then the element $(B^j)_{xz}$ in this row and this column is defined as

$$(B^j)_{xz} = \beta^j(\langle \mathbf{x}, \mathbf{z}\rangle), \qquad \text{where} \tag{11}$$

$$\beta^j(t) = \frac{1}{2^{(n-1)/2}}\sum_{l=0}^{t}\sum_{m=l}^{t}(-1)^m \frac{\begin{pmatrix} t \\ m \end{pmatrix}\begin{pmatrix} m \\ l \end{pmatrix}}{\begin{pmatrix} (n+1)/2-m \\ j-m \end{pmatrix}}. \tag{12}$$

Note that the martix B^j is a linear combination of the incidence matrices of the Johnson association scheme: $B^j = \sum_{t=0}^{j}\beta^j(t)D^j_{j-t}$.

Lemma 4. *Let $j \le (n+1)/2$. Then*

$$F^j = B^j U^j. \tag{13}$$

Proof. Let $\mathbf{x}$ be a vertex of weight j. From (2) and (6) we have

$$f(\mathbf{x}) = \frac{1}{2^{(n-1)/2}}\sum_{\mathbf{a}\in A}(-1)^{\langle \mathbf{a},\mathbf{x}\rangle}\varphi(\mathbf{a}) = \frac{1}{2^{(n-1)/2}}\sum_{l=0}^{j}(-1)^l\sigma_l(\mathbf{x}).$$

From Lemma 2 it follows that

$$f(\mathbf{x}) = \frac{1}{2^{(n-1)/2}}\sum_{l=0}^{j}\sum_{m=l}^{j}(-1)^m d_m(\mathbf{x})\begin{pmatrix} m \\ l \end{pmatrix}.$$

Using lemma 1 we get

$$f(\mathbf{x}) = \frac{1}{2^{(n-1)/2}} \sum_{l=0}^{j} \sum_{m=l}^{j} (-1)^m \frac{\binom{m}{l}}{\binom{(n+1)/2 - m}{j-m}} \sum_{t=m}^{j} \binom{t}{m} \sum_{\mathbf{z} \in W_j,\ \langle \mathbf{x}, \mathbf{z} \rangle = t} u(\mathbf{z}).$$

After changing the order of the summation we get:

$$f(\mathbf{x}) = \frac{1}{2^{(n-1)/2}} \sum_{t=0}^{j} \left(\sum_{\mathbf{z} \in W_j,\ \langle \mathbf{x}, \mathbf{z} \rangle = t} u(\mathbf{z}) \right) \sum_{l=0}^{t} \sum_{m=l}^{t} (-1)^m \frac{\binom{m}{l}\binom{t}{m}}{\binom{(n+1)/2 - m}{j-m}} =$$

$$= \sum_{\mathbf{z} \in W_j} u(\mathbf{z}) \beta^j(\langle \mathbf{x}, \mathbf{z} \rangle).$$

This expression gives us (13). $\bigtriangledown$

Denote by L^{jh}, $j \leq h \leq (n+1)/2$, a matrix of size $\binom{n}{j} \times \binom{n}{h}$, which rows correspond to the vertices of the j-th level W_j of the hypercube and columns correspond to the vertices of the h-th level W_h of the hypercube. If $\mathbf{y} \in W_j$ and $\mathbf{x} \in W_h$, then the element $(L^{jh})_{\mathbf{y},\mathbf{x}}$ in the corresponding row and column is

$$(L^{jh})_{\mathbf{y},\mathbf{x}} = \begin{cases} \binom{h}{j}^{-1}, & \text{if } \mathbf{y} \preceq \mathbf{x}, \\ 0, & \text{otherwise.} \end{cases} \tag{14}$$

Lemma 5. *Let $j \leq h \leq (n+1)/2$. Then*

$$U^j = L^{jh} U^h. \tag{15}$$

This lemma is easy, so its proof is omitted.

The following lemma is central in the paper.

Lemma 6. *Let $h \leq (n+1)/2$. Then the matrix B^h is invertible and*

$$(B^h)^{-1} = \frac{1}{\binom{n}{h}} \sum_{k=0}^{h} \left(\sum_{i=0}^{h} \frac{q_i(k,h)}{\sum_{t=0}^{h} \beta^h(t) E_{h-t}(i;h)} \right) D_k^h, \tag{16}$$

where D_k^h, $k = 0, \ldots, h$, are the incidence matrices and $q_i(k;h)$, $E_j(i;h)$, $i,j,k = 0, \ldots, h$, are the parameters of the Johnson association scheme and the values $\beta^h(t), t = 0, \ldots, h$, are defined by (12).

Proof. Theorem 1 was proved in [4]. Moreover, it was proved that the vector F^h can be an arbitrary vector of the concerned dimension. Therefore, the linear transformation B^h is invertible. We get from Lemma 4 that all elements of the martix B^h depend only on the scalar products of the vertices of the h-th level W_h. So B^h is a sum (with coefficients) of the incidence matrices of the Johnson association scheme:

$$B^h = \sum_{t=0}^{h} \beta^h(t) D^h_{h-t}.$$

This allows using of the properties of the association scheme. First we change the basis of Bose-Mesner algebra (using (3)):

$$B^h = \sum_{i=0}^{h} \left(\sum_{t=0}^{h} \beta^h(t) E_{h-t}(i,h) \right) J^h_i.$$

Then we use the proposition 3:

$$(B^h)^{-1} = \sum_{i=0}^{h} \left(\sum_{t=0}^{h} \beta^h(t) E_{h-t}(i,h) \right)^{-1} J^h_i.$$

Third, we change (using (4)) the basis of Bose-Mesner algebra a second time and get the equation (16). $\bigtriangledown$

Now we are ready to formulate and prove the main theorem.

Theorem 2. *Let $f : E^n \to \mathbf{R}$ be an arbirtary 0-centered function and $j \le h \le (n+1)/2$. Then the vector F^j of the function f values over the j-th level of the hypercube is a linear transformation of the vector F^h of the function f values over the h-th level and*

$$F^j = B^j L^{jh} (B^h)^{-1} F^h, \tag{17}$$

where the matrices B^j, L^{jh}, $(B^h)^{-1}$ are defined by (11), (12), (14), (16).

Proof. The proof is a straightforward application of Lemmas 4, 6 and 5.

Remark 1. *Let C be a perfect code, χ be its characteristic function and all code vertices in the h-th level of the hypercube be known, $h \le (n+1)/2$. To reconstruct all code vertices in the j-th level $j \le h$, we apply Theorem 2 to the 0-centered function $\chi - 1/(n+1)$.*

References

[1] *Avgustinovich S.V.,* On a property of perfect binary codes, Discrete Analysis and Operation Research V.2. No. 1. 1995. P. 4-6. (in Russian)

[2] *Avgustinovich S.V., Vasil'eva A.Yu.* On reconstruction of centered function, Proc. Int. Conf. "Discrete Analysis and Operation Research", Novosibirsk, Russia. June, 26 - July, 1, 2000. P. 64 (in Russian)

[3] *Avgustinovich S.V.,Vasil'eva A.Yu.* Reconstruction of centered function by its values at two middle levels of hypercube, Discrete Analysis and Operation Research, submitted (in Russian).

[4] *Avgustinovich S.V., Vasil'eva A.Yu.* Testing sets for 1-perfect codes, Proc. of Int. conf. "General theory of infomation transfer and combinatorics", Germany, Bielefeld, November 4-9, 2002, submitted.

[5] *O. Heden,* On the reconstruction of perfect codes, Discrete Mathematics, V. 256. 2002. P. 479-485.