İstanbul Üniv. Fen Fak. Mat Der. 59 (2000), 167-175

Constructing Codes Using A_H

N. AYGÖR, H. ÖZDAĞ

Abstract: In this study, we obtained code by the contraction of the incidence matrix of a symmetric block design with parameters (v,k,λ). We give a new definition of dot product and we prove some theorems by using this definition. By this way the construction method has been given for Hamming codes.

1. Introduction

In this work we consider difference set with parameters (v,k,λ) and obtain incidence matrix A of the design that is a development of these difference set in $(Z_v, +)$. When $|H| = h$ and $H < Z_v$, by contracted the incidence matrix A of the symmetric design, we have obtained A_H. We study some new theorems of the linear code generated by A_H which contracted of A and we also show this linear code is perfect code hence a Hamming code.

Definition 1.1 :

Let G be a group of order v, written multiplicatively. A (v,k,λ)-difference set in G is a set D consisting of k group elements with the property that the list of differences

$$xy^{-1} \quad \text{with} \quad x, y \in D$$

contains every non-identity element exactly λ times.(To avoid trivialities, we insist that $k > \lambda$.)

Definition 1.2 :

Let $\boldsymbol{D}$ be a (v,k,λ)-difference set in a group G. Define an incidence structure D, called the development of $\boldsymbol{D}$, as follows: the points are the elements of G and the blocks are the left translates of $\boldsymbol{D}$,

$$g\boldsymbol{D} = \{ gx \mid x \in \boldsymbol{D} \} \quad \text{for all } g \in G.$$

Definition 1.3 :

Suppose that $\boldsymbol{D}$ is a (v,k,λ)-difference set in an abelian group G. Let D be the development of $\boldsymbol{D}$ and let A be the incidence matrix of D. We can contract A by any subgroup H of G. Let G be a group of order v and let H be the subgroup of order h in G. $w = [\, G : H \,]$ is the number of different cosets of G in H. The contracted matrix A_H has size w and satisfies the equations

$$A_H A_H^T = nI + h\lambda J \text{ and}$$

$$A_H J = J A_H = kJ$$

(where J the matrix with every entry 1, of appropriate size.)

2. Calculation of Dimension of C_H and C_H^{ext}

Definition 2.1 :

The code generated by rows of A_H is called as C_H-code. The extended of C_H is given as follows:

$$B_H = \begin{bmatrix} & & & & 1 \\ & & & & 1 \\ & & A_H & & \cdot \\ & & & & \cdot \\ & & & & \cdot \\ & & & & 1 \\ h\lambda & h\lambda & \cdots & h\lambda & k \end{bmatrix}.$$

$(w+1)\times(w+1)$

The code generated by rows of B_H is said as C_H^{ext}.

Definition 2.2 :

If $\bar{x} = (x_1, x_2, \ldots, x_w, x_{w+1})$ $\bar{y} = (y_1, y_2, \ldots, y_w, y_{w+1})$ for $\bar{x}, \bar{y} \in C_H^{ext}$ then $\mu(\bar{x}, \bar{y}) = (x_1y_1 + x_2y_2 + \ldots + x_wy_w - h\lambda\, x_{w+1}y_{w+1})$.

Theorem 2.3 : If $p \mid k$ and $p \mid n$ then C_H-code contracted with H is self-orthogonal.

Proof: Since $p \mid n$, $p \mid k$ and $n = k - \lambda$ then $p \mid \lambda$. Therefore $nI + h\lambda J$ is $0 \ mod\ p$. Then from the equality $A_H A_H^T = nI + h\lambda J$ we deduce that scalar product of two rows of A_H always equals to 0.

Theorem 2.4 : Let $p \mid n$ and $p \mid k$. Then C_H^{ext}-code is self-orthogonal with respect to μ.

Proof:

i. Let a_i be a row of B_H for $i < w+1$.

Hence $(a_i, a_i) = n + h\lambda - h\lambda.1 = n$ because of $A_H A_H^T = nI + h\lambda J$.

Therefore since $p \mid n$, $(\bar{x}, \bar{y}) \equiv 0 \ (mod\ p)$.

ii. Let a_i and a_j be two rows, of B_H for j, $i < w+1$ $(i \neq j)$.

Hence $\mu(a_i, a_j) = h\lambda - h\lambda = 0$

iii. $\mu(a_{w+1}, a_{w+1}) = w(h\lambda)^2 - h\lambda k^2$

$= h\lambda(w\, h\lambda - k^2)$

$= h\lambda(v\lambda - k^2)$

$= h\lambda(k^2 - k + \lambda - k^2) = -n\, h\lambda$

Since $p \mid n$, $\mu(\bar{x}, \bar{y}) = 0$.

vi. Let a_{w+1} be the last row of B_H for $i < w+1$, $j = w+1$.

Since $A_H J = kJ$, $\mu(a_i, a_{w+1}) = k\, h\lambda - k\, h\lambda = 0$.

Therefore C_H^{ext}-code is self-orthogonal.

Theorem 2.5 : Let the F_p-code be C_H which is generated by rows of contracting matrix A_H. If $p \mid n$, then $Dim\ C_H \leq \frac{1}{2}(w+1)$.

Proof: Suppose that $p \mid n$. If $p \mid k$ then C_H is self-orthogonal with respect to the ordinary dot product. Because $A_H\ A_H^T = nI + h\lambda J$.

Let a_i, a_j be two rows of A_H. If $i = j$ then $a_i, a_j = n + h\lambda$. Since $p \mid n$ and $p \mid k$ then $p \mid k - n$ and hence $p \mid \lambda$ because of $n = k - \lambda$.

Therefore $n + h\lambda \equiv 0\ (mod\ p)$.

Thus $a_i\ a_j \equiv 0\ (mod\ p)$. If $i \neq j$ then $a_i\ a_j \equiv 0\ (mod\ p)$, $a_i\ a_j = h\lambda$ and $p \mid \lambda$.

$Dim\ C_H^{ext} \leq \frac{1}{2}(w+1)$ because of C_H is self-orthogonal.

Suppose now, $p \mid n$ and $p \mid k$. Two rows of extended matrix C_H^{ext} are

$$\bar{x} = (x_1, x_2, \ldots, x_w, x_{w+1})$$
$$\bar{y} = (y_1, y_2, \ldots, y_w, y_{w+1}).$$

Hence dot product is $\mu(\bar{x}, \bar{y}) = (x_1y_1 + x_2y_2 + \ldots + x_wy_w - h\lambda\, x_{w+1}y_{w+1})$.
Therefore $\mu(\bar{x}, \bar{y}) \equiv 0\ (mod\ p)$.
Hence the extended F_p-code C_H^{ext} is self-orthogonal with respect to above dot product. Then $Dim\ C_H^{ext} \leq \frac{1}{2}(w+1)$.

If $p \mid k$ then we show that $Dim\ C_H^{ext} = Dim\ C_H$. The sum of the fist w columns of B_H, is

$$\begin{bmatrix} k \\ k \\ \cdot \\ \cdot \\ \cdot \\ wk\lambda \end{bmatrix} \text{ and final column is } \begin{bmatrix} 1 \\ 1 \\ \cdot \\ \cdot \\ \cdot \\ k \end{bmatrix}.$$

Since $p \mid k$ and $(p, k) = 1$ then the inverse of $k \ mod\ p$ exists. If we multiply the sum of first w columns by k^{-1} we get

$$whλ = vλ = (k^2 - k + λ)$$
$$= k^2 - n.$$

Since $p \mid n$, $whλ \equiv k^2 \ (mod\ p)$. Therefore the sum of the first w columns equals to

$$\begin{bmatrix} 1 \\ 1 \\ . \\ . \\ . \\ k \end{bmatrix}$$

Hence, the sum of the first w columns with respect to $mod\ p$ is equal to the final column.

Similarly, the sum of the first w rows of B_H is $[k \quad k \quad . \quad . \quad . \quad kw]$ and the last row is $[hλ \quad hλ \quad . \quad . \quad . \quad hλk]$.

The $hλk^{-1}$ times the sum of the first w rows is

$$[hλ \ hλ ... whλ k^{-1}].$$

Here the last element of this row is $whλk^{-1} = vλk^{-1}$

$$= (k^2 - k + λ) k^{-1}$$
$$= (k^2 - n) k^{-1} = k - nk^{-1}$$

and since $p \mid n$, we have $whλk^{-1} \equiv k \ (mod\ p)$.

At the end of this proof the last row with respect to $mod\ p$ equals to $hλk^{-1}$ times the sum of the first w rows. Thus A_H and B_H have the same F_p – rank

Therefore $Dim\ C_H^{ext} = \frac{1}{2}(w+1)$. Finally, we have $Dim\ C_H^{ext} \leq \frac{1}{2}(w+1)$.

3. Application

In this section we give an example to the theorem above.

Example 3.1: Let $\boldsymbol{D} = \{\bar{7},\bar{9},\bar{14},\bar{15},\bar{18}\} \subset (Z_{21},+)$ is a difference set with parameters (21, 5, 1). Blocks of symmetric design that is development of $\boldsymbol{D}$ are given as follows: For

$$\forall g \in G,\ g+\boldsymbol{D} = \{g+d \mid d \in \boldsymbol{D}\}$$

$$B_1 = \{\bar{7},\bar{9},\bar{14},\bar{15},\bar{18}\}$$

$$B_2 = \{\bar{8},\bar{10},\bar{15},\bar{16},\bar{19}\}$$

$$\vdots$$

$$B_{21} = \{\bar{6},\bar{8},\bar{13},\bar{14},\bar{17}\}\ .$$

Here the incidence matrix is

$$A = \begin{bmatrix}
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

We obtain the following matrix by contracted A_H with H

$$A_H = \begin{bmatrix}
2 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 2 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 2 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 2 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 2 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 2 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 2
\end{bmatrix}$$

When we reduced A_H to *mod* 2, $A_H = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$.

Therefore we get linear code

C_H = {0001011,1000101,1100010,0110001,1011000,0101100, 0010110, 1001110, 1101001, 0111010, 1010011,0100111, 0011101, 1110100, 1111111, 0000000}

which are generated by A_H . This code is with parameters (7, 16, 3) .

Now we show that this code is perfect . We know that (n, M, $2t$+1)-code is perfect if and only if the sphere-packing condition

$$M\left\{1+(q-1)n+(q-1)^2\binom{n}{2}+\ldots+(q-1)^t\binom{n}{t}\right\}=q^n$$

is satisfied .

Since d =3, then t =1 and

$$16\left\{\binom{7}{0}+(2-1)\binom{7}{1}\right\}=2^7 .$$

Follows from the fact that Hamming codes are the only perfect linear codes with these parameters.

4. Result

We prove some theorems with respect to our new definition of dot product and we show that the new codes which are obtained by contraction of long codewords are perfect code.

References

[1] ASSMUS, Jr. E. F. and KEY, J. D., *Hadamard Matrices and Their Design: A coding –Theoretic Approach.* Transactions of the American Mathematical Society, Volume 330, Number 1, 1992.

[2] BLAKE, I.F. and MULLIN, R.C., *The Mathematical theory of Coding*, Academic press, New York, 1975.

[3] CALDERBANK, A.R., *Covering Bounds for Codes*, Journal of Combinatorial Theory, Series A60, 1992, 117 –122.

[4] CAMERON, P.J. And LINT, J.H.V., *Graph Theory – Coding Theory and Block Designs*, Cambridge university Press, 1975.

[5] HEDAYAT, A. and WALLIS, W.D., *Hadamard Matrices and Their Applications*, Ann Statist. 6, 1978, 1184-1238.

[6] HILL, R., *A First Course in Coding Theory*, Clarendon Press, Oxford, 1986

[7] HUGHES, D.R. and PIPER, F.C., *Design Theory*, Cambridge University Press, 1985.

[8] JOHNSEN, E. C., *Skew-Hadamard Abelian Group Difference Sets*, Journal of Algebra 4, 1966, 388-402.

[9] LANDER, E.S., *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, 1983.

[10] SPENCE,E., *Hadamard Matrices from Relative Difference Sets*, Journal of Combinatorial Theory A 19, 1975, 287-300.

[11] TONCHEV, V.D., *Self-Orthogonal design and extremal Doubly Even Codes*, Journal of Combinatorial Theory, Series A 52, 1989, 191-205.

Author addresses :

Nilgün Aygör
Y.T.Ü. Fen – Edebiyat Fakültesi,
Matemetik Bölümü
Davutpaşa - İstanbul
e-mail : aygor@yildiz.edu.tr

Hülya Özdağ
Fen- Edebiyat Fakültesi
Matemetik Bölümü
Davutpaşa - İstanbul
ozdag@yildiz.edu.tr