ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 6, No. 3, 2011, *pp.* 173-176

T-Wise Balanced Designs from Binary Hamming Codes

Manjusri Basu[1] and Satya Bagchi[2]

[1] Department of Mathematics, University of Kalyani, Kalyani, W.B, India, Pin-741235,

[2] Department of Mathematics, National Institute of Technology, Durgapur, Burdwan, W.B, India, Pin-713209

(*Received October 16, 2010, accepted December 21, 2010*)

Abstract. In this paper we show that the binary Hamming codes $(2^r-1, 2^{2^r-r-1}-2, 3)$ satisfy (2^r-r-2) - $(2^{2^r-r-1}-1, \{3,4,...,2^r-4\}, 1)$ designs, where $r \geq 3$, a positive integer. For different values of r most of the t-wise balanced designs obtained from our constructions appear to be new.

Keywords: Hamming code, t-wise balanced design, Steiner system.

1. Introduction

A linear code C defined over the field F_2 with dimension k and length n is an $[n,k]$ linear code over F_2. If C has minimum distance d then C is an $[n,k,d]$ linear code over the field F_2 [2].

Two codes are called equivalent if they differ only in the order of the symbols [4].

A generator matrix of the $[n,k,d]$ linear code C over F_2^n is a $k*n$ matrix G whose rows are linearly independent of $C = RS(G)$ the row space of G. The generator matrix G of a linear code $C = RS(G)$ can be written in a standard form: $G = [I_k \mid A^t]$ where the parity check matrix $H = [A \mid I_{n-k}]$, I_s is an identity matrix of order s [4]

The binary Hamming single-error-correcting codes are an important family of codes which are easy to encode and decode. A binary Hamming code $H_r = [2^r-1, 2^r-r-1, 3]$ has parity check matrix H whose 2^r-1 columns consist of all nonzero binary vectors of length r, each used once.

Let X be a v-set (i.e. a set with v elements), whose elements are called points. A t-design is a collection of distinct k-subsets (called blocks) of X with the property that any t-subset of X is contained in exactly λ blocks. We call this a $t-(v,k,\lambda)$ design. $2-(v,k,\lambda)$ design is called pair wise balanced design or balanced incomplete block design. A Steiner system is a t-design with $\lambda = 1$, and a $t-(v,k,1)$ design is usually denoted by $S(t,k,v)$ [1,5,6] .

A t-wise balanced design (tBD) of type $t-(v,k,\lambda)$ is a pair (X,B) where X is a v-set and B is a collection of subsets of X (blocks) with the property that the size of every block is in the set K and every t-element subset of X is contained in exactly λ blocks. If $\lambda = 1$, the notation $S(t,K,v)$ often used and the design is a t-wise Steiner system. If K is a set of positive integers strictly between t and v, then the tBD is proper [3].

2. Some Theorems

Theorem 2.1: The minimum distance of a linear code is the minimum weight of the nonzero codewords.

Theorem 2.2: Any binary Hamming code $H_r = [2^r-1, 2^r-r-1, 3]$ is equivalent to any binary

[1] Corresponding author. *E-mail address*: manjusri_basu@yahoo.com.
[2] *E-mail address*: satya5050@gmail.com

code $[2^r-1, 2^r-r-1, 3]$, $r \geq 3$.

Theorem 2.3: Adding all code words of the generator matrix of the binary Hamming code gives 1 (i.e. all 1 code word).

Theorem 2.4: If we interchange two or more columns of a standard generator matrix of a code C and apply some row operations then we get a standard generator matrix of a code C' which is equivalent to the code C.

Theorem 2.5: If a code $C=[n,k,d]$ holds t-wise balanced design then any equivalent code $C=[n,k,d]$ of C holds the same t-wise balanced design.

Theorem 2.6: The weights of the Hamming code $H_r=[2^r-1, 2^r-r-1, 3]$, $r \geq 3$ are $3,4,\ldots,2^r-4$ excluding all **0** and all **1** codes.

3. New Theorems

Theorem 3.1: The binary Hamming codewords excluding **0** and **1** codes satisfy the t-wise balanced designs (2^r-r-2) - $(2^{2^r-r-1}-2, \{3,4,\ldots,2^r-4\}, 1)$, where $r \geq 3$

Proof: The dimension of the Hamming code $H_r=[2^r-1, 2^r-r-1, 3]$ is 2^r-r-1. Let H_r^* represent the codes H_r excluding 0 and 1. Hence the number of codewords of H_r^* is $2^{2^r-r-1}-2$. The weights of H_r^* are $3,4,\ldots,2^r-4$ (Theorem 2.6). Hence $v=2^{2^r-r-1}-2$ and $K=3,4,\ldots,2^r-4$.

We consider the Hamming code $H_r=[2^r-1, 2^r-r-1, 3]$ The generator matrix

$$G=[I \mid A] \tag{1}$$

of H_r is of the order $(2^r-r-1)\times(2^r-1)$ where I is the identity matrix of order 2^r-r-1.

Let us choose 2^r-r-2 columns out of 2^r-1 columns of G.

Two cases arise:

Case I: All 2^r-r-2 columns are in I.

We obtain corresponding codewords by linear combinations of rows of these columns. And we have exactly one codeword of length 2^r-r-2 with 2^r-r-2 consecutive **1**.

Case II: At least one column of 2^r-r-2 columns is not in I.

Step I. Select a column of the selected columns which is not in I. If there is no such column then goto Step IV.

Step II. Interchange the selected column with any non-selected column in I.

Step III. Goto Step I.

Step IV. All selected 2^r-r-2 columns are among first 2^r-r-1 columns of G', transformed matrix of the generator matrix $G(Eq.(1))$.

Now by row operations G' can be written in standard form $G''=[I \mid A']$. From this standard generator matrix G'', we obtain the codewords C'' equivalent to H_r (Theorem 2.4). Thus by case I we have exactly one codeword of length 2^r-r-2 with 2^r-r-2 consecutive 1. Hence C'' holds t-wise balanced design 2^r-r-2 - $(2^{2^r-r-1}-2, \{3,4,\ldots,2^r-4\}, 1)$.

Therefore the code H_r^* equivalent to C'' holds t-wise balanced design 2^r-r-2 - $(2^{2^r-r-1}-2, \{3,4,\ldots,2^r-4\}, 1)$ (Theorem 2.5). This completes the proof.

Thus H_r^* is 2^r-r-2-wise Steiner system $S(2^r-r-2, \{3,4,\ldots,2^r-4\}, 2^{2^r-r-1}-2)$.

Lemma: The H_r^* is not proper t-wise balanced design.