Discrete Applied Mathematics 157 (2009) 402–405

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Note

On a new code, $[2^n - 1, n, 2^{n-1}]$

M. Basu [a,*], Md.M. Rahaman [a], S. Bagchi [b]

[a] Department of Mathematics, University of Kalyani, Kalyani-741235, India
[b] Department of Mathematics, National Institute of Technology, Durgapur-713209, India

ARTICLE INFO

Article history:
Received 18 February 2008
Received in revised form 17 June 2008
Accepted 18 June 2008
Available online 5 August 2008

Keywords:
Linear code
Support
Design
Parity sectioned reduction
Sectioned code
Non-uniform error correction

ABSTRACT

A binary linear code in F_2^n with dimension k and minimum distance d is called an $[n, k, d]$ code. A t-(n, m, λ) design D is a set X of n points together with a collection of m-subsets of X (called a block) such that every t-subset of X is contained in exactly λ blocks. A constant length code which corrects different numbers of errors in different code words is called a non-uniform error correcting code. Parity sectioned reduction of a linear code gives a non-uniform error correcting code. In this paper a new code, $[2^n - 1, n, 2^{n-1}]$, is developed. The error correcting capability of this code is $2^{n-2} - 1 = e$. It is shown that this code holds a 2-$(2^n - 1, 2^{n-1}, 2^{n-2})$ design. Also the parity sectioned reduction code after deleting the same g $(\leq e)$ positions of each code word of this code holds a 1-$(2^n - 1 - g, 2^{n-1} - j, {}^gC_j .2^{n-1-g})$ design for $n \geq 3, g = 1, 2, \ldots, e$ and $j = 0, 1, \ldots, g$.

1. Introduction

It is important to define a new code that can be encoded or decoded efficiently with error correcting ability.

A generator matrix for the $[n, k, d]$ linear code C over F_2^n is a $k \times n$ matrix G whose rows are linearly independent of $C = \mathbf{RS}(G)$, the row space of G.

In this paper, the systematic generator matrix for a new code, $[2^n - 1, n, 2^{n-1}]$, is defined. The different properties of this code are stated and proved.

Let P_n be a matrix of order $2^{n-1} \times n$. The rows of P_n are all binary code words of length n except the $\bar{0}$ code word.

In this paper, a systematic generator matrix of the new code is designed via $G_n = [P_n]^t$. Now we consider the square matrix C_n^* of order $2^n - 1$ whose rows are all the code words generated by G_n except the $\bar{0}$ code word.

For example,

$$P_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad G_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}, \quad C_3^* = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

* Corresponding author. Tel.: +91 9433186058; fax: +91 3325828282.
E-mail addresses: manjusri_basu@yahoo.com (M. Basu), meeza_maths@rediffmail.com (Md.M. Rahaman), satya.bagchi@nitdgp.ac.in (S. Bagchi).

0166-218X/$ – see front matter
doi:10.1016/j.dam.2008.06.029

$$P_4 = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 1&1&0&0\\ 1&0&1&0\\ 1&0&0&1\\ 0&1&1&0\\ 0&1&0&1\\ 0&0&1&1\\ 1&1&1&0\\ 1&1&0&1\\ 1&0&1&1\\ 0&1&1&1\\ 1&1&1&1 \end{pmatrix}, \qquad G_4 = \begin{pmatrix} 1&0&0&0&1&1&1&0&0&0&1&1&1&0&1\\ 0&1&0&0&1&0&0&1&1&0&1&1&0&1&1\\ 0&0&1&0&0&1&0&1&0&1&1&0&1&1&1\\ 0&0&0&1&0&0&1&0&1&1&0&1&1&1&1 \end{pmatrix}$$

$$C_4^* = \begin{pmatrix} 1&0&0&0&1&1&1&0&0&0&1&1&1&0&1\\ 0&1&0&0&1&0&0&1&1&0&1&1&0&1&1\\ 0&0&1&0&0&1&0&1&0&1&1&0&1&1&1\\ 0&0&0&1&0&0&1&0&1&1&0&1&1&1&1\\ 1&1&0&0&0&1&1&1&1&0&0&0&1&1&0\\ 1&0&1&0&1&0&1&1&0&1&0&1&0&1&0\\ 1&0&0&1&1&1&0&0&1&1&1&0&0&1&0\\ 0&1&1&0&1&1&0&0&1&1&0&1&1&0&0\\ 0&1&0&1&1&0&1&1&0&1&1&0&1&0&0\\ 0&0&1&1&0&1&1&1&1&0&1&1&0&0&0\\ 1&1&1&0&0&0&1&0&1&1&1&0&0&0&1\\ 1&1&0&1&0&1&0&1&0&1&0&1&0&0&1\\ 1&0&1&1&1&0&0&1&1&0&0&0&1&0&1\\ 0&1&1&1&1&1&1&0&0&0&0&0&0&1&1\\ 1&1&1&1&0&0&0&0&0&0&1&1&1&1&0 \end{pmatrix}$$

and so on.

2. Definitions

1. *Support* [3]: Let $\bar{x}$ be a binary word of length n. The set of positions in which $\bar{x}$ has non-zero entries is called the support of $\bar{x}$.

2. *Design* [4]: Let C be a binary code of length n. Let S_w be the set of code words in C of weight w. We say that S_w holds a t-(n, w, λ) design if the supports of code words in S_w form the blocks of a t-(n, w, λ) design, and if for any t-set $T \subset \{1, 2, \ldots, n\}$ there are exactly λ code words of weight w in C with 1's in the positions given by T.

3. *Parity sectioned reduction* [1]: Let C be a binary e-error correcting (n, k) linear systematic code with parity check matrix $H_{n-k,n} = [A|I_{n-k}]$ and error range inequalities

$$\sum_{j=1}^{n} |x_j - c_{i,j}| \le e, \quad i = 1, 2, \ldots, 2^k.$$

By g-parity sectioned reduction of the code C, we mean the following operations on the parity check matrix $H_{n-k,n}$ and the error range inequalities:

1. Select some g $(\le e)$ parity check positions for sectioning; if the code is sectioned at the pth check position, then delete the pth column and row of I_{n-k}. A reduced matrix $H_{n-k-g,n-g} = [A' : I_{n-k-g}]$ is obtained.
2. In each code word of C, delete the g-parity check digits; in the error range inequalities, assign values from (0, 1) to the variables corresponding to these g positions.

3. Properties

Property 1. *The matrix C_n^* can be rearranged in a manner such that the transpose of this matrix is equal to itself.*

Property 2. *The Hamming weight (i.e. support) of each code word of C_n is 2^{n-1}.*

Property 3. *The code C_n is self-orthogonal for $n > 2$.*

Property 4. *The code C_n is not a dual code since the length of the code is odd for all values of n* [2].

Property 5. *The code C_n is not perfect.*

Property 6. *The code C_n is a $2^{n-2}-1$-error correcting code.*

Property 7. *The $(g+1)$ sets $\{C'_{nj} | j = 0, 1, \ldots, g\}$ of the g $(\leq 2^{n-2}-1 = e)$-parity sectioned reduction of C_n contain*

$$\binom{g}{j} .2^{k-g}$$

code words [1].

Property 8. *The $(g+1)$ sets of $\{C'_{nj} | j = 0, 1, \ldots, g\}$ of the g $(\leq 2^{n-2}-1 = e)$-parity sectioned reduction of C_n can correct up to $e-j$ errors* [1].

Property 9. *The g $(\leq 2^{n-2}-1 = e)$-parity sectioned reduction of C_n gives a code C'_n which is a non-uniform error correcting $(2^n-1-g, n)$ linear code* [1].

Theorem 1. *The minimum weighted code words of $[2^n-1, n, 2^{n-1}]$ hold a 2-$(2^n-1, 2^{n-1}, 2^{n-2})$ design, $n \geq 2$.*

Proof. Every code word of $[2^n-1, n, 2^{n-1}]$ has constant weight 2^{n-1} (Property 2).

Now C_n^* is the code word matrix of the $[2^n-1, n, 2^{n-1}]$ code C_n except the $\bar{0}$ code word. Without any loss of generality C_n^* is taken in such a manner that $C_n^* = C_n^{*t}$ (Property 1). Therefore, the ith row and ith column of C_n^* are identical.

For a 2-design, ${}^{2^{n-1}}C_2$ combinations of columns of C_n^* are to be considered or, in other words, for a 2-design, ${}^{2^{n-1}}C_2$ combinations of rows of C_n^* are to be considered.

Now we choose any two rows of C_n^*, i.e. any two distinct code words C_i, C_j (say), $i, j = 1, 2, \ldots, 2^n-1$ and $i \neq j$, of $[2^n-1, n, 2^{n-1}]$.

We have [3]

$$\begin{aligned} d &= \min\{d(C_i, C_j) | i, j = 1, 2, \ldots, 2^n-1\} \\ &= \min\{w(C_i) | i = 1, 2, \ldots, 2^n-1\} \\ &= 2^{n-1}. \end{aligned}$$

Therefore, the number of columns of C_i and C_j which contain $(0, 1)^t$ and $(1, 0)^t$ is equal to 2^{n-1}, i.e. there are in total 2^{n-1} 1's in the columns of the form $(0, 1)^t$ and $(1, 0)^t$ of the code words C_i and C_j.

Again the total of 1's of the code words C_i and C_j is $2.2^{n-1} = 2^n$.

So the remaining number of 1's which are of the form $(1, 1)^t$ in C_i and C_j is $2^n - 2^{n-1} = 2^{n-1}$.

Hence the number of columns $(1, 1)^t$ is $2^{n-1}/2 = 2^{n-2}$.

Therefore, the minimum weighted code word of $[2^n-1, n, 2^{n-1}]$ holds a 2-$(2^n-1, 2^{n-1}, 2^{n-2})$ design, $n \geq 2$. □

Theorem 2. *The minimum weighted code words of $[2^n-1, n, 2^{n-1}]$ do not hold a 3-design.*

Proof. We have

$$G_n = \begin{pmatrix} 1 & 0 & \cdots & 0 & \vdots & 1 & \cdots \\ 0 & 1 & \cdots & 0 & \vdots & 1 & \cdots \\ 0 & 0 & \cdots & 0 & \vdots & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \vdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & \vdots & 0 & \cdots \end{pmatrix}.$$

First we choose the first three columns from C_n^*; then we get at least one row which contains three consecutive 1's, since the sum of the first three rows is a row of C_n^*.

Now we choose the first, second and $(n+1)$th columns of C_n^*; then it is proved that we do not get any row which contains three consecutive 1's. □

Theorem 3. *The minimum weighted code words of $(g+1)$ sets $\{C'_{nj} | j = 0, 1, \ldots, g\}$ of the g $(\leq 2^{n-2}-1)$-parity sectioned reduction of C_n hold a 1-$(2^n-1-g, 2^{n-1}-j, {}^gC_j .2^{n-1-g})$ design for $n \geq 3$.*

Proof. Let C_n be the $[2^n - 1, n, 2^{n-1}]$ code. Then, the length of a g $(\leq 2^{n-2} - 1)$-parity sectioned reduction code is $2^n - 1 - g$.

It is obvious that the weight of the parity sectioned reduction code C'_{nj} is 2^{n-1-j}.

The total number of code words of the code C'_{nj} is ${}^{g}C_j\, 2^{n-g}$ and the number of 1's in each column of the code words of C'_{nj} is ${}^{g}C_j\, 2^{n-g}/2 = {}^{g}C_j\, 2^{n-g-1}$.

Hence the theorem. □

Note: By Theorem 2, it can be stated that the minimum weighted code word of $(g + 1)$ sets $\{C'_{nj} | j = 0, 1, \ldots, g\}$ of the g $(\leq 2^{n-2} - 1)$-parity sectioned reduction of C_n^* does not hold a 2-design.

Acknowledgements

The authors thank the referee for his/her valuable comments. The second author thanks C.S.I.R. for financial support of his research work.

References

[1] M.A. Bernard, B.D. Sharma, Linear codes with non-uniform error correcting capability, Designs, Codes and Cryptography 10 (1997) 315–323.
[2] San Ling, Chaoping Xing, A first course of coding theory, National University of Singapore, 2004.
[3] V.S. Pless, W.C. Huffman, Handbook of Coding Theory, vol. II, North-Holland, 1998.
[4] S. Roman, Coding and Information Theory, Springer, 1991.