Asian Journal of Information Technology 6 (3): 385-387, 2007

A New Set of (7, 3) Ternary Linear Codes

Partha Pratim Dey, Kaniz Fatima and Mohua Hossain
Department of Computer Science and Engineering, North South University, Bangladesh

Abstract: In this study a set of ternary linear codes is developed and their error-correction capacity is explored. The relative advantage of certain codes over the other codes of the set is also discussed.

Key words: Linear code, error-correcting code, generator matrix, parity check matrix

INTRODUCTION

Let p be a prime number, n- a positive integer and F_p^n -n dimensional row vector space with canonical basis over the finite field F_p so that a typical element $x \in F_p^n$ has the shape $x = (x_1,...,x_n)$, $x \in F_p, i = 1,...,n$. A k- dimensional subspace C of F_p^n is called is called a p- ary linear [n,k] code. The vectors of are called code-words, and sometimes more briefly words. The parameter is called the length of a codeword and is called the dimension of the code. In this study we will explore a new set of ary, also known as ternary, linear codes and their error-correction capacity. A linear error-correcting code is a linear code for which it is sometimes possible to detect and correct errors that occur during transmission of the code-words. Specifically, a code is error correcting if the code possesses properties which allow to detect and correct up to errors. For basic acquaintance with the theory of these codes, please consult (Pless,1982; Van Lint, 1982). Some applications of error correcting codes include correction of errors that occur in information transmitted via the internet, data stored in a computer and music encoded on a computer disk.

Let $W = F_3^k$ and $V = F_3^n$ with $k < n$ and let G be a $K \times n$ matrix over of full row rank. Then $C = \{v \in V \mid v = wG$ for some $w \in W\}$ is a subspace of V of dimension K . Hence the vectors in C form the code-words in an [n,k] linear code in V with 3^k code-words. The matrix G is called a generator matrix for C. For this G, we can find an $(n-k) \times n$ matrix H of full row rank over F_3 with $HG^t = 0$, where G^t denotes the transpose of G, Since $HG^t = 0$, then $HG^t w^t = 0$ for all $w \in W$. Hence $H(wG)^t = 0$ for all $w \in W$,or, equivalently $Hc^t = 0$, for all $c \in C$. And since H has full row rank $Hc^t = 0$, if and only if $c \in C$. Thus H, can be used to identify code-words in C . The matrix H is called a parity check matrix for C. Note that $HG^t = 0$ implies $GH^t = 0$, so the columns of H^t, that is the rows of H, are in the null-space of G. Thus to determine H from G, we must only find a basis for the null-space of G and place these basis vectors as rows in H. Note that for (7, 3) a ternary linear code C, G is cogredient to the block matrix $[I_3 \mid A]$ where I_3 is the 3×3 identity matrix and A is the 3×4 matrix over F_3. The corresponding H is then given by $H = [A^t \mid 2I_4]$ where I_4 is the 4×4 identity matrix. Let G_7 be the following 3×7 matrix

$$\begin{bmatrix} 1 & 0 & 0 & \alpha & \beta & \alpha & \gamma \\ 0 & 1 & 0 & \alpha & \alpha & \beta & \gamma \\ 0 & 0 & 1 & \beta & \alpha & \alpha & \gamma \end{bmatrix}$$

where $\alpha, \beta, \gamma \in GF(3)$, $\alpha \# \beta$ and $\alpha, \beta \# 0$. Needless to say that $GF(3) = \{0, \alpha, \beta\}$.

ERROR-CORRECTION WITH PARITY CHECK MATRIX

We discuss a couple of theorems in this section. The theorems are not unknown, but their proofs have been modified to suit our purpose.

Theorem (1) let H be a parity check matrix of a p-ary [n,k] linear code C. Then the minimum number of dependent columns of H is greater than or equal to w (C) the minimum of weights of the nonzero words of C.

Proof. Let be the minimum number of dependent columns of H. Then by definition of dependence there exist S columns C_{i1}, C_{i2},.....C_{is} of H and s elements $\alpha_1,...,\alpha_s \in F_p$, not all equal zero, such that $\alpha_1 C_{i_1} + ... + \alpha_s C_{i_s} = 0$. We now observe that none of these $\alpha_1,...,\alpha_s$ is zero. Assume without loss, that $\alpha_1 = 0$. Then $\alpha_1 C_{i_1} + ... + \alpha_s C_{i_s} = 0$ becomes $\alpha_2 C_{i_2} + ... + \alpha_s C_{i_s} = 0$. As is the minimum number of dependent columns of H, the column vectors $C_{i_2},...,C_{i_s}$ are independent over F_p . Then equation $\alpha_2 C_{i_2} + ... + \alpha_s C_{i_s} = 0$ implies that $\alpha_2 = ... = \alpha_s = 0$. This is a contradiction as from dependence of $C_{i_1}, C_{i_2},..., C_{i_s}$ we know that $\alpha_1,...,\alpha_s$ can't be all zero. Hence

Corresponding Author: Partha Pratim Dey, Department of Computer Science and Engineering, North South University, Bangladesh

each of $\alpha_1,...,\alpha_s$ is nonzero. Let $v \in F_p^n$ such that i,...i, coordinates of V are, $\alpha_1,...,\alpha_s$ respectively and the other coordinates are zero. Then $Hv^t = \alpha_1 C_{i_1} + ... + \alpha_s C_{i_s} = 0$ and therefore is a word C of with weight s . Hence $s \geq w(C)$.

Theorem (2) let C be a P-ary $[n,k]$ -linear code and H be a parity-check matrix of C. If no two columns of H are dependent, then C can detect and correct 1 error. Proof. Throughout this proof, we let $e_m(\tau)$ denote an n-dimensional row vector of F_p^n whose mth coordinate is $\tau \in F_p$ and other coordinates are zero. Let C be the code-word that was sent and due to noise in the channel $r = c + e(\alpha)$ was received. Then $Hr^t = Hc^t + He_i(\alpha)^t = 0 + \alpha C_i = \alpha C_i$ where C_i is the ith column of H. The equation $Hr = \alpha C$ indicates that error vector is $e(\alpha)$ and one recovers codeword c from r as follows: $c = r - e(\alpha)$. On the other hand, contrary to our assumption if two columns C_i and C_j were dependent i.e. aC_i were equal to βC_j, then in earlier situation Hr^t would be equal to aC_i as well as βC_j and we would not know which of the two code-words: $c = r\text{-}e_i(\alpha)$ and $r\text{-}e_j(\alpha)$, was actually sent, making unique decoding impossible. But in our case, due to the assumption of independence of two columns of H, this ambiguity in recovering the transmitted word will not arise.

MAIN RESULTS

We begin this section with a theorem concerning the case $\gamma = \beta$.

Theorem (3) the last four coordinates of a word generated by:

$$G_\beta = \begin{bmatrix} 1 & 0 & 0 & \alpha & \beta & \alpha & \beta \\ 0 & 1 & 0 & \alpha & \alpha & \beta & \beta \\ 0 & 0 & 1 & \beta & \alpha & \alpha & \beta \end{bmatrix}$$

is:

A permutation of 1 zero and 3 α' s, or
A permutation of 1 zero and 3 β' s, or
A permutation of 2 zeros, 1α and 1β, or
A permutation of 2α' s and 2β' s.

Moreover the minimum weight of $C(G_\beta)$, the code generated by G_β is 4.

Proof. Let $x = (\alpha,\beta,\alpha,\beta)$,y = (α, α, α, β, β) and $z = (\beta,\alpha,\alpha,\beta)$. Then a code word which is one-span i.e., spanned by just one row vector of G with a nonzero coefficient from GF (3) should have one of $x, 2x, y, 2y, z$ or 2z for last four coordinates. As each of x, y, z contains 2α' s and 2β' = s, so will each of by virtue of the fact that 2α = β and 2β = α. As x, y, z, 2x, 2y and 2z are all distinct and each contains 2α' s and 2β' s, they constitute all the $\frac{4!}{2!2!} = 6$ permutations of 2α' s and 2β's. This also says that each word of $C(G_\beta)$ which is one span has weight 1+4 = 5.

Let us now consider the nonzero codewords which are two-spans i.e., the words which are spanned by 2 row vectors of G with nonzero coefficients from GF (3). There are 12 of them and each should have one $x+y, x+z, y+z, 2x+y, 2x+z, 2y+z$ of or their doubles as the last four coordinates. As:

$x+y = (\beta,0,0,\alpha), x+z = (0,0,\beta,\alpha), y+z = (0,\beta,0,\alpha),$

$2x+y = (0,\beta,\alpha,0), 2x+z = (\alpha,\beta,0,0),$

their doubles too will contain 2 zeros,1$\alpha$and 1β. Thus these 12 four digit vectors will constitute all the $\frac{4!}{2!} = 12$ permutations of 2 zeros, 1$\alpha$and 1β. Hence each codeword of $C(G_\beta)$ which is 2-span should have weight 2+2 = 4and the last four coordinates of each of these 12 codewords is a permutation of 2 zeros, 1α and 1β.

Finally we investigate the eight codewords which are 3-spans i.e. the words which are spanned by all three row vectors of G with nonzero coefficients from GF (3). Each of them should have one of $x+y+z$, $x+2y+2z, 2x+2y+z, 2x+y+2z$ or their doubles as the last four coordinates. Note that $x+2y+2z, 2x+2y+z, 2x+y+2z$ and $2x+y+2z = (\alpha,\alpha,0,\alpha)$. As each has 3$\alpha'$ s and 1 zero, they constitute all the $\frac{4!}{3!1!} = 4$ permutations of 3α's and 1 zero. On the other hand, the remaining four 3-spans, being doubles of these four, constitute all the $\frac{4!}{3!1!} = 4$ permutations of 3β' s and 1 zero. Hence each codeword of C (G_β) which is 3-span has weight 3+3 = 6 and the last 4 coordinates of each of these eight codewords is a permutation of zero and s or a permutation of 1 zero and 3β' s. Thus the minimum weight of C (G_β) is 4.

Corrolary (4) the code generated by G_γ, denoted by C (G_γ), is a 1-error correcting ternary linear code for any $\gamma \in$ GF (3).

Proof. As minimum weight C (G_β) of is 4 the minimum weight of C (G_α) and C (G_0) is greater than or equal to 3. Hence for any $\gamma \in$ GF (3), the minimum weight of C (G_γ) is greater than or equal to 3. Thus by Theorem (1), theminimum number of dependent columns of parity check matrix H of C (G_γ) is greater than or equal to 3. So any two columns of H are independent. Hence by Theorem (2), can detect and correct 1 error.

Let us now prove a theorem that sheds light on an advantage that code C (G_β) possesses over C (G_α) and C (G_0).

Theorem (5) if one of the last four digits of a word of C (G_β) gets altered during transmission, the corruption of the word can immediately be felt and known from the look of the last four digits. But it may not be true for C (G_γ) if $\gamma = \alpha$ or $\gamma = 0$.

Proof let be a codeword of type (α) of Theorem (3) i.e. the last four coordinates of c is a permutation of 1 zero and 3 alphas. Suppose is sent and during transmission the zero digit of the last four digits of gets altered. Then the received vector r should have 4 nonzero digits, which are either all alpha or alphas and beta, at the tail. As this r is not a codeword of type (d) of Theorem (3), containing 2 alphas and 2 betas, and these are the only words in C (G_β) whose last four digits are nonzero, one immediately sees that this is not a codeword at all. On the other hand, if one of the alphas is altered, then r should have either 1 zero, 1 beta and 2 alphas or 2 zeros and 2 alphas. From the look of the last four digits, one immediately sees that this r is not a word, as by Theorem (3) (a) and (b), if one of the last four digits of a word is zero, then the remaining three should be identical, and by Theorem (3) (a), if two of the last four digits are zero, then the other two digits are alpha and beta. Thus if one of the last four digits of a type (α) word is altered, one immediately realizes that the word has undergone corruption. Almost identical arguments work for a codeword of type (b).

Suppose now a codeword of type (c) is sent. Of the last four digits of say a zero digit is altered during transmission. Then one of the last four digits of r is zero and the other three digits are nonzero. But these three nonzero digits are not same. Hence the fact that the received vector r is not a word immediately comes to notice. On the other hand, if a nonzero digit of the last four digits of is altered, then r should have either 3 zeros and a nonzero digit or 2 zero and 2 identical nonzero digits. One then immediately knows that the transmitted word has undergone corruption, as by Theorem (3) (c), at most of the last four digits of a codeword can be zero and when 2 of the last four digits of a codeword are zero, the other two are distinct.

Finally suppose a codeword is of type (d) i.e. the last four digits of are a permutation of 2 alphas and 2 betas. Say c is sent and during transmission a digit is corrupted. The received vector r is then either a vector one of whose last four digits is zero, but the other 3 digits are nonzero and non identical contrary to Theorem (3) (a) and (b) or is a vector each of whose last four digits is an alpha or beta and the number of alphas and betas is not equal, as opposed to Theorem (3) (d). One immediately notices that such an r is not a codeword, hence r has undergone corruption.

REFERENCES

Pless, V., 1982. Introduction to the Theory of Error-Correcting Codes, John Wiley and Sons, Inc.

Van Lint, J.H., 1982. Introduction to Coding Theory, Springer-Verlag New York Inc.