PROCEEDINGS
OF THE INSTITUTION OF ELECTRICAL ENGINEERS
Electronics

Maximum distance bounds for linear anticodes

Abdullah A. Hashim, B.Sc.(Eng.), M.Sc., Ph.D., D.I.C.

Indexing terms: Anticodes, Data links

Abstract

A mathematical analysis of linear anticodes is given in which a lower bound on the minimum of maximum-Hamming distance δ is obtained by the application of a systematic procedure for the generation of such anticodes. For the binary anticodes, the asymptotic form of this bound is established.

1 Introduction

A linear-block (m, k, δ) anticode over a Galois field $GF(q)$ forms an array of 2^k rows and m columns, in which each of the m columns is some linear combination (modulo-q) of the first k, $(k \leqslant m)$, columns of the array.[2] The anticode has a maximum distance δ if the distance between any two rows of the anticode array is less than or equal to δ, and since any linear anticode forms an algebraic group over $GF(q)$, then δ is equal to the maximum weight w_{max} of the rows of the array.[3] An anticode is good if it exhibits the least δ for given m and k; and said to be nonrepetitive if no two columns of the anticode array are identical.

Farrell[1,2] was the first to introduce the concept of anticodes. He suggested that for every good nonrepetitive (m, k, δ) anticode, there exists an (n, k, d) good, or nearly good, nonrepetitive linear code which can be constructed simply by deleting the given anticode array from the appropriate m-sequence code array.

The m-sequence code array is a $q^k \times q^k - 1$ matrix in which the first k columns are the information columns, and each of the remaining $q^k - k - 1$ columns is some distinct, linear combination (modulo-q) of the information columns.[1] The array can be partitioned into two parts, with one part consisting of the codewords of a linear nonrepetitive (n, k, d) code, and the other the corresponding (m, k, δ) anticode words. This implies that

$$m + n = q^k - 1$$

Since the m-sequence codes are equidistance codes[3] of distance equal to q^{k-1}, it follows that

$$d + \delta = q^{k-1}$$

The object behind this paper is the formulation of a mathematical description of linear anticodes from which a systematic procedure for the generation of anticodes is established. This leads to an asymptotic bound on δ/m for given k/m.

2 Matrix description of linear anticodes*

Since an (m, k, δ) linear anticode forms an algebraic group under modulo-q addition[1] (q being the number of symbols per sign), then an (m, k, δ) linear anticode forms a subspace U of the vector space U_m over $GF(q)$. If a set of the basis vectors of the subspace U are considered as the rows of a $(k \times m)$ matrix J, then matrix J is called the generator matrix of the anticode U. The reduced-echelon form of the matrix J has the form[3]

$$J = I_k b \tag{1}$$

*Since linear anticodes form algebraic groups, their matrix description is similar to that of group codes. The reader is referred to References 3 and 4.

Paper 7583 E, first received 28th February 1974 and in revised form 16th September 1975

Dr. Hashim was formerly with the Imperial College of Science & Technology, University of London, Exhibition Road, London SW7, England, and is now with the Department of Electronic & Communications Engineering, The Polytechnic of North London, London N7 8DB, England

The matrix I_k is the identity matrix of order k, and b is an arbitrary $k \times (m - k)$ matrix. The null space U' of U is a subspace of the vector space U_m,[3] noting that repeated rows in the anticode array result in all-zero rows in the standard echelon-form-generator matrix, which can then be deleted. A set of basis vectors from the null space U' of the subspace U can be considered as the rows of a $(m - k) \times m$ matrix L, the L matrix is called the generator matrix of the null space U' or the parity-check matrix of U. The reduced echelon form of L has the form[3]

$$L = -b^T I_{m-k} \tag{2}$$

where the matrix $-b^T$ is the transpose of the arbitrary matrix $-b$, and I_{m-k} is the identity matrix of the order $(m - k)$. The parity-check matrix of an anticode can itself be a generator matrix which generates the dual anticode of the anticode generated by J.

It is convenient here to introduce the term 'quasilinear independence'. The r-tuple vectors $r_1, r_2, \ldots, r_i$ over $GF(q)$ are quasilinearly independent if the vectors, formed by modulo-q addition of the scalar products $(\alpha_1 r_1 + \alpha_2 r_2 + \ldots + \alpha_i r_i)$, are all nonzero vectors, where α_j may be any one of the nonzero elements of $GF(q)$.

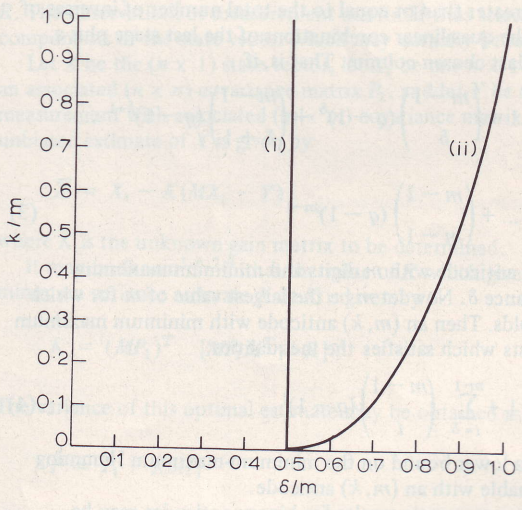

Fig. 1
Bounds on minimum maximum distance for linear anticodes

(i) Plotkin's average distance upper bound
(ii) Linear anticodes lower bound on S

matrix of an anticode can itself be a generator matrix which generates the dual anticode of the anticode generated by J.

Since there are $(q - 1)$ nonzero elements in $GF(q)$, the quasilinear combinations of the above vectors may have $(q - 1)^i$ combination sums, each sum resulting in a nonzero r-tuple vector over $GF(q)$. It follows that if the vectors are not quasilinearly independent over $GF(q)$ they must be linearly dependent over the field.

From the above we have the following

Theorem: for any (m, k) linear anticode U over $GF(q)$ which has a parity-check matrix $\boldsymbol{L}$, U will have a maximum distance δ or less if and only if every combination of $\delta + i, i = 1, 2, ..., m - \delta$, columns of $\boldsymbol{L}$ are quasilinearly independent.

Proof: suppose that some m-tuple vector $u, u \epsilon U$, has a weight of $\delta + 1, 1 \leqslant i \leqslant m - \delta$. Since U is a row space of $\boldsymbol{J}$, and U' is a row space of $\boldsymbol{L}$ and a null space of U, an m-tuple vector such as u is in U if and only if it is orthogonal to every row of $\boldsymbol{L}$. That is to say

$$u\boldsymbol{L}^T = 0$$

Since u has a weight of $\delta + i$, this specifies a linearly dependent set of $\delta + i$ columns of $\boldsymbol{L}$. Conversely, the modulo-q addition of $\delta + i$ columns of $\boldsymbol{L}$ is equal to the zero vector which contradicts the conditions of the theorem. Therefore, we conclude that for the condition of the theorem to be fulfilled there must be no m-tuple vector in U of weight greater than δ.

3 Systematic procedure of generating linear anticodes

Consideration of the above theorem suggests the following systematic procedure for the construction of an (m, k, δ) anticode over $GF(q)$ for given values of δ and $(m - k)$. The columns of the $\boldsymbol{L}$ matrix can be determined as follows. Start with the identity matrix of order $(m - k)$. The $(m - k + 1)$th column is chosen arbitrarily from the vector space U_{m-k} over $GF(q)$, subject only to the condition that the chosen column must not be the inverse of any of the vectors obtained from the quasilinear combinations of every $\delta + i, ..., (m - k - \delta)$ of the previously chosen columns. The inverse of a vector r over $GF(q)$ is that vector which when added (modulo-q) to r results in a zero vector. Similarly the jth column is chosen so that it is different from the inverse of any of the vectors obtained from the quasilinear combinations of every $\delta + i, i = 0, 1, ..., j - 1 - \delta$ of the previously chosen columns. This method of generation guarantees the required independence of columns specified in the theorem. As long as the set of all these inverse vectors does not include all the $(m - k)$-tuple vectors, another column can be added. This process of building up the $\boldsymbol{L}$-matrix will, therefore, continue until all the $(m - k)$-tuple vectors are exhausted. The anticode is the null space of this $(m - k) \times m$ matrix $\boldsymbol{L}$.

4 Bounds on δ

In the worst possible case for an arbitrary choice of columns of the $\boldsymbol{L}$ matrix, the inverses of all the vectors of the quasilinear combinations might be distinct. Since the inverse vectors of the quasilinear combinations of the mth stage include all these vectors in the previous stages, then to ensure success in the face of this worst case, the number of q^{m-k} vectors of the vector space U_{m-k} need only be greater than or equal to the total number of inverses of all vectors of the quasilinear combinations of the last stage plus a vector for the last chosen column. That is, if

$$q^{m-k} \geqslant 1 + \binom{m-1}{\delta}(q-1)^{\delta} + \binom{m-1}{\delta+1}(q-1)^{\delta+1} ...$$

$$... + \binom{m-1}{m-1}(q-1)^{m-1} \tag{3}$$

there exists an anticode with m digits and minimum-maximum Hamming distance δ. Now let m be the largest value of m for which inequality[3] holds. Then an (m, k) anticode with minimum maximum distance δ exists which satisfies the inequalities:

$$q^{m-k} \leqslant 1 + \sum_{i=\delta}^{m-1} \binom{m-1}{i}(q-1)^i \tag{4}$$

This provides a lower bound on the minimum-maximum Hamming distance attainable with an (m, k) anticode.

For large m, asymptotic results for binary anticodes may be obtained using the following inequalities:

$$\sum_{i=\lambda n}^{n} \binom{n}{i} \leqslant (\lambda)^{-\lambda n}(\mu)^{-\mu n} \tag{5}$$

providing $\lambda > \frac{1}{2}$, where $\mu = 1 - \lambda$. (See Reference 3, p. 468)

Inequality 4 becomes

$$2^{m-k} - 1 \leqslant (\delta/m)^{-\delta}\left(\frac{m-\delta}{m}\right)^{-(m-\delta)} \tag{6}$$

Taking the logarithm of both sides, assuming $2^{m-k} \gg 1$, and dividing by m we obtain

$$1 - \frac{k}{m} \leqslant -\frac{\delta}{m}\log_2\left(\frac{\delta}{m}\right) - \left(1 - \frac{\delta}{m}\right)\log_2\left(1 - \frac{\delta}{m}\right) \tag{7}$$

This lower bound is plotted in Fig. 1. Note that the shape of this bound is the mirror image of Varsharmov and Gilbert's[5] lower bound for linear block codes of maximum-minimum distance d, where d is replaced by δ and m by n.

An upper bound on the minimum maximum distance of anticodes may be established by using the Plotkin[6] principle of 'average distance'. That is, the minimum weight of a codeword in an (n, k) linear code is at most as large as the average weight of the code. Because of similarities between linear codes and linear anticodes, it follows that the Plotkin[6] average distance bound is also true for linear anticodes, and that it is true to say that the maximum weight of an anticode word in an (m, k) linear anticode is never smaller than the average weight of the anticode.

Consider the array of an (m, k) linear anticode over $GF(q)$. Since each field element appears q^{k-1} times in each column,[3,4] the number of nonzero elements in each column is $(q - 1)q^{k-1}$, and since there are m columns, the sum of the weights of all anticodewords in the anticode is $m(q - 1)q^{k-1}$. Also, since there are $q^k - 1$ nonzero anticode words, it follows that the average weight of an (m, k) anticode over $GF(q)$ is $mq^{k-1}(q - 1)/(q^{k-1})$. This is also found by Farrell* in unpublished work. The asymptotic form of the Plotkin bound on δ for linear anticodes is given by

$$\delta \leqslant m/q \tag{8}$$

For the binary case, this bound is plotted in Fig. 1.

5 Remarks

Using the properties of the parity-check matrix $\boldsymbol{L}$ for linear anticodes established above, a computerised search procedure for new binary linear anticodes may be established following the steps of the suggested procedure. Such a computer search for new anticodes will be limited to some values of $(m - k)$ less than 15. Work in this direction is under way, and it is hoped that some of the new anticodes thus generated in turn lead to new codes.

6 Acknowledgments

The author wishes to acknowledge A.G. Constantinides of the Department of Electrical Engineering, Imperial College of Science & Technology, for his support, guidance and encouragement. He also gratefully acknowledges helpful discussions with his colleague P.M. Buckley.

7 References

1 FARRELL, P.G.: 'Coding for noisy data links'. Ph.D. thesis, University of Cambridge, 1969
2 FARRELL, P.G.: 'Linear binary anticodes', *Electron. Lett.*, 1970, **6**, pp. 419–421
3 PETERSON, W.W., and WELDON, E.J., Ja.: 'Error-correcting codes' (MIT Press, 1972)
4 BERLEKAMP, E.R.: 'Algebraic coding theory' (McGraw-Hill, 1968)
5 GILBERT, E.N.: 'A comparison of signalling alphabets', *Bell Syst. Tech. J.*, 1952, **31**, pp. 504–522
6 PLOTKIN, M.: 'Binary codes with specified minimum distance'. *IRE Trans.*, 1960, **IT-6**, pp. 445–450

*Personal communication