Improvement on Varshamor-Gilbert lower bound on minimum hamming distance of linear codes

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

Indexing terms: *Codes*

Abstract

An improvement on the Varshamov–Gilbert lower bound on the minimum Hamming distance d of linear bloc codes is proposed. The improved bound is based on the assumption that, for an (n, k) block code, the number o distinct vectors resulting from the linear combination of every $(d-2)$ columns of the parity-check matrix is muc less than the total number of vectors generated from such linear combinations. An expression for the larges possible number of distinct vectors obtainable for any (n, k) group code can therefore be introduced and shown t be a function of the weight distribution of the code.

List of symbols

(n, k, d) = a linear block code of length n digits and k message digits, having a minimum Hamming distance d, and being capable of correcting $t = (d-1)/2$ random errors or less

V_n = a vector space of dimension n

V = a subspace of the vector space V_n, used to indicate the linear (n, k) code

$[G]$ = generator matrix of an (n, k) code

$[H]$ = parity-check matrix of group code

$\binom{n}{i}$ = number of combinations of i out of n

$\{X_i\}$ = the set $X_1, X_2, \ldots, X_n$ (n is given in the text)

$[H^T]$ = transpose of the matrix $[H]$

$\in$ = membership, $v \in \{V\}$, v is an element of set $\{V\}$

C = membership, $\{U\} C \{V\}$, $\{U\}$ is a subset of $\{V\}$

$q.l.c.$ = quasilinear combinations

$\{V | v \in q.l.c.\binom{n}{j}(q-1)^j\}$ = set of all $\binom{n}{j}(q-1)^j$ vectors resulting from the quasilinear^j combinations of j n-tuple vectors over the Galois field of q elements $GF(q)$; q is a prime number

1 Introduction

A lower bound on d is defined, for arbitrary values of n and k, as the largest value of d associated with any code which can be shown to exist, having the value of n and d.

The Varshamov–Gilbert lower bound was proposed by Varshamov[1] and is a refinement of a bound proposed by Gilbert.[2] The same bound was also found by Sacks[3] from a consideration of the characteristics of the parity-check matrix $[H]$ of the code. Sacks suggested a systematic procedure for constructing an (n, k) code with r-parity-check symbols and minimum distance d. This procedure guaranteed the required independence of the $[H]$ matrix columns of the constructed code if the integer r was sufficiently large so that it satisfied the following inequality:

$$\sum_{i=0}^{d-2} \binom{n}{i} (q-1)^i \leqslant q^r \tag{1}$$

The smallest integer r that satisfies the above inequality is known as the Varshamov–Gilbert lower bound on d.

The object of this paper is to introduce a possible improvement on the above bound by showing that the number of distinct vectors, resulting from the linear combination of all $d-2$ columns of the $[H]$ matrix, are much less than the summation of eqn. 1.

An expression for the largest possible number of these distinct vectors [for any (n, k) group codes] is proposed, and a tighter bound is therefore obtained.

2 Improved bound

It is convenient here to redefine[4] 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 addition over $GF(q)$ 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 linear combinations ($q.l.c.$) of the above vectors may have $(q-1)$ combinational sums, each sum resulting in a nonzero r-tuple vecto over $GF(q)$.

The numerical value of the Varshamov–Gilbert bound, given by eqn. 1, may be rewritten as follows:

$$1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{d-3}(q-1)^{d-3} + \binom{n}{d-2}(q-1)^{d-2} = q^{n-k} \tag{2}$$

We may say, therefore, that since $q^{n-1} - 1$ represents the total number of the quasilinear combinations of one, two, ..., and $(d-2)$ columns of the $[H]$ matrix, the bound assumes that all the vectors resulting from these combinations are distinct.

Now let us consider a codeword vector $\boldsymbol{v}$ of weight d, which has nonzero elements at the positions $p_1, p_2, \ldots, p_d$. It follows that the addition over $GF(q)$ of the scalar products of these nonzero elements with the corresponding $p_1, p_2, \ldots$, and p_d columns of the $[H]$ matrix, results in a zero vector.[5] Let the set of these d scalar products, say $\{C\}$, be divided into two subsets $\{A\}$ and $\{B\}$. Moreover, let the addition over $GF(q)$ of the members of subset $\{A\}$ results in an r-tuple vector $\boldsymbol{a}$ and similarly the members of a subset $\{B\}$ result in vector $\boldsymbol{b}$. Then

$$\boldsymbol{a} + \boldsymbol{b} = 0 \tag{3}$$

This equality indicates that $\boldsymbol{a}$ is the inverse vector of $\boldsymbol{b}$ and vice versa. If the subset $\{A\}$ has two members, then the vector $\boldsymbol{a}$ must be a vector in the set of vectors resulting from the quasilinear combination of every two columns of the $[H]$ matrix (denoted by $\{v|v \in q.l.c.\binom{n}{2}(q-1)2\}$), and, since the inverse of a vector $\boldsymbol{a}$ is equal to the scalar product $[(q-1)\boldsymbol{a}]$, it follows that the vector $\boldsymbol{b}$ is one of the vectors resulting from the quasilinear combinations of every two columns of $[H]$, i.e. $\boldsymbol{b} \in \{\boldsymbol{v}|\boldsymbol{v} \in q.l.c.\binom{n}{2}(q-1)^2\}$. However, the vector $\boldsymbol{b}$ is in the set $\{\boldsymbol{v}|\boldsymbol{v} \in q.l.c.\binom{n}{d-2}(q-1)^{d-2}\}$, which suggests that vector $\boldsymbol{b}$ is not distinct. Similarly, all the multiples of vector $\boldsymbol{b}$, $g.\boldsymbol{b}$, where g is any nonzero element of $GF(q)$, are in the set $\{\boldsymbol{v}|\boldsymbol{v} \in q.l.c.\binom{n}{d-2}(q-1)^{d-2}\}$, and since $g.\boldsymbol{a} + g.\boldsymbol{b} = 0$, according to the above argument, the $(q-1)$ multiples of vector $\boldsymbol{b}$ are not distinct.

Since set $\{C\}$ has d members, it can be divided, in two subsets $\{A\}$ and $\{B\}$ of two members and $(d-2)$ members, respectively, in many ways. The number of these combinations is equal to $\binom{d}{2}$. Consequently, the corresponding number of nondistinct vectors in the set $\{\boldsymbol{v}|\boldsymbol{v} \in q.l.c.\binom{n}{d-2}(q-1)^{d-2}\}$, for every codeword of weight d, is given by

$$\binom{d}{2}(q-1).$$

... a nondistinct vector in one of the sets $\{v|v\in q.l.c.\binom{n}{d-2}(q-1)^{d-2}\}$, $\{v|v\in q.l.c.\binom{n}{d-3}(q-1)^{d-3}\}$, …, $\{v|v\in q.l.c.\binom{n}{(d+1)/2}\cdot(q-1)^{(d+1)/2}\}$. The total number of these nondistinct vectors, for every codeword of weight d, is given by

$$(q-1)\sum_{i=2}^{\lceil\frac{d-1}{2}\rceil}\binom{d}{i} \qquad (4)$$

In general, every codeword of weight w, where $d \leqslant w \leqslant d-2+t$, $t=\left\lceil\frac{d-1}{2}\right\rceil$, suggests the existence of

$$(q-1)\sum_{i=w-d+2}^{t}\binom{w}{i} \qquad (5)$$

nondistinct vectors in the sets $\{v|v\in q.l.c.\binom{n}{d-2}(q-1)^{d-2}\}$, $\{v|v\in q.l.c.\binom{n}{d-3}\cdot(q-1)^{d-3}\}$, …, $\{v|v\in q.l.c.\binom{n}{(d+1)/2}(q-1)^{(d+1)/2}\}$. Since the linear combinations of every t column of the $[H]$ matrix give unique nonzero vectors in the vector space V_r,[5,6] no two codewords of weight w (where $d\leqslant w\leqslant t+d-2$) suggest the same nondistinct vectors.

The total number of these vectors may be computed as follows: Let the minimum number of codewords in an (n, k, d) linear code of weight w be $f(w)$; then the whole computation of these nondistinct vectors may be tabulated as in Table 1.

The total summation is then given by

$$(q-1)\sum_{w=d}^{d-2+t}f(w)\sum_{i=w-d+2}^{t}\binom{w}{i} \qquad (6)$$

The subtraction of the total number of nondistinct vectors of eqn. 7, from the summation of eqn. 1, results in an improved Varshamov–Gilbert lower bound on the minimum Hamming distance d. The improved bound is thus given by

$$\sum_{i=0}^{d-2}\binom{n}{i}(q-1)^i-(q-1)\sum_{w=d}^{d-2+t}f(w)\sum_{i=w-d+2}^{t}\binom{w}{i}=q^r \qquad (7)$$

The numerical evaluation for this improved bound requires the determination of the lowest possible value of $f(w)$, where $w=d$, $d+1$, …, $(d-2+t)$, in terms of the code parameters n, k and d.

3 Weight distribution of linear binary codes

The 2^k codewords of an (n, k) binary block code can be tabulated as the rows of an $2^k\times n$ matrix; this matrix is referred to as the code array.

Consider the code array of an (n, k) binary block code, arranged as follows:

*$\left\lceil\frac{x}{2}\right\rceil$ means the largest integer, smaller than or equal to $x/2$, i.e. $\left\lceil\frac{d-1}{2}\right\rceil=t$, the number of random errors the code can correct

Table 1

COMPUTATION OF NONDISTINCT VECTORS

Codeword weight w	Minimum number of codewords of weight w $f(w)$	Number of nondistinct vectors in the linear combinations of $(d-2)$ columns of the $[H]$ matrix, corresponding to subsets $\{A\}$ and $\{B\}$ of 'i' members and $(w-i)$ members, respectively $i=$	2 3 4 . . . t
d	$f(d)$	$(q-1)f(d)$	$\left[\binom{d}{2}+\binom{d}{3}+\binom{d}{4}+\ldots+\binom{d}{t}\right]+$
$d+1$	$f(d+1)$	$(q-1)f(d+1)$	$\left[\binom{d}{3}+\binom{d}{4}+\ldots+\binom{d+1}{t}\right]+$
$d+2$	$f(d+2)$	$(q-1)f(d+2)$	$\left[\binom{d}{4}+\ldots+\binom{d+2}{t}\right]+$
.			.
.			.

... codewords of the upper half of the array are tabulat[ed in a] sequence that corresponds to the decimal value (from 2^{k-1} … 2^k-1) of the k binary information digits of each codeword. Th[e code]words of the lower half of the array are tabulated in a sequen[ce that] corresponds to the decimal value, from 0 up to $(2^{k-1}-1)$, o[f the] information digits.

If all zero elements of the first k columns of this array are re[placed] by $+1$ s and the 1 elements by -1 s, then the resulting column[s are] the k functions of Rademacher.[7] Walsh functions are usually d[efined] by products of Rademacher functions.[7] This definition, ho[wever,] does not yield the Walsh functions ordered by the number o[f sign] changes as does the difference equation.† Rademacher fun[ctions] correspond to the functions Wal$(1,\theta)$, Wal$(3,\theta)$, Wal$(7,\theta)$ e[tc. It] should be noted that the result of multiplying together two [Walsh] functions, when transformed by replacing all the positive elemen[ts by] 0 s and the negative element by 1 s, is identical to that produce[d by] similarly transforming the original functions and performing a si[mple] modulo-2 addition.[7,8] Since all the redundant digits of any (linear code are a consequence of the mudulo-2 addition of som[e of] the k information digits, it follows that all the n columns of the a[rray] array are Walsh functions. Every Walsh function has equal numbe[r of] 1 s and 0 s, and hence the columns of any code array will have e[qual] 1 s and 0 s; therefore, the total number of 1 s in the array is equa[l to] $(n.2^{k-1})$. Since there are 2^k-1 nonzero codewords in V, the ave[rage] weight of codewords in V is given by‡

$$W_{ave}=\frac{n.2^{k-1}}{2^k-1}$$

Now, consider an (n, k) linear code V of minimum Hamming dista[nce] d equal to average weight W_{ave}. Since the minimum Hamming dista[nce] d of any (n, k) linear code is equal to the minimum weight;[5] i.e. in [the] case of the code under consideration (V) $d=W_{min}=W_{ave}$, it follo[ws] that as d tends to W_{ave} the maximum weight of the codewords o[f V] will be equal to the minimum weight. Therefore, the code V is [an] equidistant code with all its 2^k-1 nonzero codewords of weig[ht] W_{ave}, where $W_{ave}=n.2^{k-1}/(2^k-1)$. For large values of k, W_{ave} ten[ds] to n/2.

On the other hand, consider an (n, k) linear block code V [of] minimum Hamming distance equal to unity. Such a code has n[o] redundant digits and therefore its weight distribution is binomial.

For other linear block codes of minimum Hamming distance d where $1\leqslant d\leqslant\frac{n}{2}$, the weight distribution would lie between th[e] distributions of equidistance and unit-distance codes. Moreover, th[e] characteristics of the weight distribution of such codes may be deter[mined] as follows: Consider the sequency§ of the 2^k Walsh functions

†The Walsh functions Wal(j,θ) may be defined by the following difference equation:[7]

$$\text{Wal}(2j+p,\theta)=(-1)^{[j/2]+p}\{\text{Wal}[j,2(\theta+\tfrac{1}{4})]+(-1)^{j+p}\text{Wal}[j,2(\theta-\tfrac{1}{4})]\}$$

$p=0$ or 1; $j=0,1,2,\ldots$; Wal$(0,\theta)=1$ for $-\frac{1}{2}<\theta<\frac{1}{2}$; Wal$(0,\theta)=0$ for $\theta<-\frac{1}{2},\theta>+\frac{1}{2}$

‡the same results may be obtained by using Pless[9] identities; see also Peterson,[5] p. 70

§The sequency of Wal(i,θ) is defined as the largest number of adjacent 1 s or 0 s occurring in the given Wal(i,θ), while the integer i is called the normalised sequency of the function Wal(i,θ).

Wal$(1, \theta)$ up to Wal$(2, \theta)$ have a sequency equal to 2^{k-1}, while Wal$(3, \theta)$ up to Wal$(6, \theta)$ have a sequency equal to 2^{k-2}; in general Wal$(2^j - 1, \theta)$ up to Wal$(2^{j+1} - 2, \theta)$ have a sequency equal to 2^{k-j}. This implies that half of the group of the 2^k Walsh functions have a sequency $\leqslant 2$, one quarter of the functions of the group have a sequency $\leqslant 4$, and, in general, $(1/2^j)$ of the Walsh functions of the group have a sequency $\leqslant 2^j$; only one Walsh function has a sequency equal to 2^k. Since the code array of an (n, k) code may be arranged in such a way that each column of the array represents a Walsh function, and if the (n, k) code is nonrepetitive,|| then each row of the array forms part of a distinct Walsh function. This suggests that if n is not negligible compared with 2^k, then half of the rows of the (n, k) code array have a sequency $\leqslant 2$, one quarter of the rows have a sequency $\leqslant 4$, $(1/2^j)$ rows have a sequency of 2^j and two rows may have a sequency of n. Then, since the largest number of codewords has a weight equal to the average value, it follows that the weight distribution of an (n, k) nonrepetitive linear block code may have a maximum value at a point corresponding to the average weight of the code.

The proposed improvement on the Varshamov–Gilbert lower bound on d for linear block codes may be evaluated for codes, fulfilling the preceding assumptions, as follows:

(*a*) assume that the minimum number of codewords of weight (w) where $d \leqslant w < w_{ave}$ in an (n, k, d) linear code, is as low as zero

(*b*) the minimum number of codewords of average weight $f(w_{ave})$ tends to the average value of $f(w)$. The correctness of this statement can be seen from the fact that, since $f(w_{ave})$ is the maximum value for $f(w)$ (where $w = 1, 2, \ldots, n$) then the lowest value of $f(w_{ave})$ cannot be less than the average value of $f(w)$, i.e.

$$f(w_{ave}) \geqslant \frac{2^k - 1}{Z} \tag{9}$$

where Z is the total number of the nonzero $f(w)$, and, in general, $Z \leqslant n - d$. However, for an (n, k) code with even Hamming distance d, derived from an $(n-1, k)$ code with odd Hamming distance $(d-1)$ by annexing an overall parity-check digit $f(w)$ equal to zero for w odd, and therefore

$$Z \leqslant \left\lceil \frac{n-d}{2} \right\rceil$$

|| A code is nonrepetitive if no two columns of the code array are identical

4 Conclusions

Using eqns. 1, 7 and 9, the Varshamov–Gilbert bou its improvement may be evaluated. The improvement is foun significant for $n \leqslant 10$. However, as the code length increa numerical evaluation of the proposed improvement using th suggested bound on the lowest value of $f(w_{ave})$ is founc negligible. Nevertheless, the proposed improvement can be importance if a tighter bound on the lowest values of $f(w)$ $d \leqslant w \leqslant (d - 2 + t)$, is known.

5 Acknowledgment

The author wishes to thank A. G. Constantinides an Buckley of Imperial College of Science and Technology, Lonc the many useful discussions and help in connection with thi

6 References

1 VARSHAMOV, R.R.: 'Estimate of the number of signals in error-c codes', *Dokl. Akad. Nauk SSSR*, 1957, **117**, pp. 739–741

2 GILBERT, E.N.: 'A comparison of signalling alphabets', *Bell Syst.* 1952, **31**, pp. 504–522

3 SACKS, G.E.: 'Multiple error correction by means of parity chec *Trans.*, 1958, **IT-4**, pp. 145–147

4 HASHIM, A.A., 'Maximum distance bounds for linear anticodes', *Pr* 1976, **123**, (3), pp. 189–190

5 PETERSON, W.W., and WELDON, E.J. Jr.: 'Error correcting cod Press, Cambridge, 1972, 2nd edn.,)

6 HASHIM, A.A., and CONSTANTINIDES, A.G.: 'Some new re binary linear block codes', *Electron. Lett.*, 1974, **10**, pp. 31–33

7 HARMUTH, F.: 'Transmission of information by orthogonal f (Springer-Verlag Book Co., 1971)

8 HASHIM, A.A., and CONSTANTINIDES, A.G.: 'Class of linea codes', *Proc. IEE*, 1974, **121**, (7), pp. 555–558

9 PLESS, V.: 'Power moment identities on weight distributions correcting codes, *Inf. & Control*, 1963, **6**, pp. 147–152