SOME NEW RESULTS ON BINARY LINEAR BLOCK CODES

Indexing term: Error-correction codes

Certain properties of the parity-check matrix H of (n, k) linear codes are used to establish a computerised search procedure for new binary linear codes. Of the new error-correcting codes found by this procedure, two codes were capable of correcting up to two errors, three codes up to three errors, four codes up to four errors and one code up to five errors. Two meet the lower bound given by Helgert and Stinaff, and seven codes exceed it. In addition, one meets the upper bound. Of the even-Hamming-distance versions of these codes, eight meet the upper bound, and the remaining two exceed the lower bound.

Introduction: A linear block (n, k, t) error-correcting code[2, 3] comprises q^k distinct codewords, q being the number of symbols per sign; for binary codes, $q = 2$, which form a subspace V of the vector space V_n over the field F of q elements. The basis vectors of the subspace V can be considered to be the rows of a matrix G, called the generator matrix of V. The basis vectors of the null space V' of the subspace V can be considered as the rows of the parity-check matrix H. Since V' is the row space of H and the null space of V, a vector v is in V if and only if it is orthogonal to every row of H. It follows that, for each codeword of Hamming weight ω, there is a linear-dependence relation between ω columns of H; conversely, for each linear-dependence relation involving ω columns of H, there is a codeword of weight ω.[2] In general, we can say that, if an (n, k) code V has a parity-check matrix H, V will correct all errors of weight t or less, if and only if every $2t$ columns from H are linearly independent.[2] The parity-check matrix may be viewed in a slightly different, but nevertheless useful way, as follows:

Let a subset U of n vectors in a vector space V_{n-k} be formed over a field F of q elements, and let U contain at least one set of the basis vectors of V_{n-k}. A parity-check matrix H can be produced so that its n columns are the vectors in U. The (n, k) linear code corresponding to this matrix will correct t random errors if and only if all linear combinations of every t vectors in U give unique nonzero vectors in V_{n-k}. That this statement is correct can be seen from the following argument:

Since the set U includes at least one set of the basis vectors of the vector space V_{n-k}, the parity-check matrix H, whose columns are the vectors of U, has a rank equal to its dimension. All the $n-k$ rows of H are thus linearly independent. Now consider $2t$ vectors of the set U. Let these $2t$ vectors form two sets U_1 and U_2 of t vectors each. The linear combination of all vectors of U_1 form a set S_1 of q^t unique vectors. Similarly, set S_2 corresponds to the linear combinations of all vectors of U_2. Since S_1 contains all the vectors that are the linear combinations of the vectors $(u_1, u_2, \ldots, u_t) \in U_1$, it follows that, if a vector s is in S_1, all vectors of the scalar product (as) are in S_1 also, where $a = 1, 2, \ldots, q-1$. This implies that the modulo-q addition of any vector in S_1 with any vector in S_2 is a nonzero vector, and therefore every $2t$ vectors of U are linearly independent. As a consequence, every $2t$ columns of the parity-check matrix H are linearly independent, and hence the corresponding (n, k) code can correct up to t random errors.

Computer search and results: Using the above characteristics of the parity-check matrix, a computer search was developed to find one code at a time for a given number of parity-check digits and a given error-correcting capability t. The computer search follows the following steps:

(a) read the given H matrix

(b) cross out the $(n-k)$-tuple vectors of the all t linear combinations of the columns of the H matrix

(c) take the vectors of the vector space V_{n-k} in turn, starting with the all-zero vector and ending with the all-one vector

(d) test each vector for uniqueness. If not unique, start again at step (c) with the next vector

(e) test for uniqueness of all t linear combinations of the vector with the columns of the H matrix. If any vector of the resultant linear combination is not unique, start again at step (c) with the next vector

(f) cross out the vector and all the t linear combinations of step (e)

(g) increase the size of the H matrix by one column by adding the vector to the H matrix

(h) continue the search, again starting from step (c), until all vectors in V_{n-k} have been tested.

Using the search, the following results have been obtained (Table 1):

For $t = 5$ and $m = n-k = 19$, and taking the 19th-order identity matrix as the starting matrix, a $(26, 7, 5)$ code was found. The best linear block code corresponding to the largest previously known value of k for $t = 5$ and $m = 19$ was $(25, 6, 5)$.[2]

For $t = 4$ and $m = 17$, 18, 19 and 22, the mth-order identity matrix is taken as the starting H matrix. The following codes were found: $(26, 9, 4)$, $(30, 12, 4)$, $(34, 15, 4)$ and $(47, 25, 4)$. For these values of t and m, the previously best known linear block codes were $(23, 6, 4)$, $(25, 7, 4)$, $(30, 11, 4)$ and $(46, 24, 4)$.[2]

For $t = 3$ and $m = 15$, the parity-check matrix of the Karlin[5] $(30, 16, 3)$ code, with a dummy parity digit, was used as a starting matrix. A $(34, 19, 3)$ code was found. The

largest previously known value of K for $t = 3$ and $m = 15$ is given by the (32, 17, 3) code.[4]

For $t = 3$ and $m = 19$ and 20, starting with the mth-order identity matrix as the starting matrix, a (72, 53, 3) and a (86, 66, 3) code were found. The best codes corresponding to the largest known values of K for $t = 3$ and $m = 19$ and 20, respectively, were previously (70, 51, 3) and (83, 63, 3).[6]

Finally, for $t = 2$ and $m = 11$ and 13, and starting with the mth-order identity matrix as the H matrix, the following codes were found: (41, 30, 2) and (71, 58, 2). For these values of t and m, the previously best known linear block codes were (39, 28, 2)[7] and (70, 57, 2).[2]

Using the above search, ten new, good binary codes were found, plus the ten even-Hamming-distance versions of the newly found codes. Owing to the limitations of computer memory and time, the above results represent the limit of application of the search procedure.

A. A. HASHIM
A. G. CONSTANTINIDES

Department of Electrical Engineering
Imperial College of Science & Technology
Exhibition Road, London SW7 2BT, England

27th December 1973

References

1 HELGERT, H. J., and STINAFF, R. D.: 'Minimum-distance bounds for binary linear codes', *IEEE Trans.*, 1973, **IT-19**, pp. 344–356
2 PETERSON, W. W., and WELDON, E. J., JUN.: 'Error-correcting codes' (MIT 1972)
3 BERLEKAMP, E. R.: 'Algebraic coding theory' (McGraw–Hill, 1968)
4 GOPPA, V. D.: 'A new class of linear error-correcting codes', Probl. Peredaci Inf., 1970, **6**, pp. 24–30
5 KARLIN, M.: 'New binary coding results by circulants', *IEEE Trans.*, 1969, **IT-15**
6 HELGERT, H. J.: 'Srivastava codes', *ibid.*, 1972, **IT-18**, pp. 292–297
7 WAGNER, T. J.: 'A search technique for quasi-perfect codes', *Inf. & Control*, 1966, **9**, pp. 94–99

Table 1

n	k	d	d_L	d_U	The first K columns of H matrix in octal
26	7	11	11	11	1777, 76037, 316343, 526554, 653265, 1132671, 1255316
27	7	12	12	12	As above, with addition of overall-parity-check digit
26	9	9	8	10	377, 7417, 31463, 52525, 65252, 113152, 213630, 263723, 306136
27	9	10	9	10	As above, with addition of overall-parity-check digit
30	12	9	8	10	All columns of code (26, 9) plus 416246, 521055, 724616
31	12	10	9	10	As above, with addition of overall-parity-check digit
34	15	9	8	10	All columns of code (30, 12) plus 1023305, 1441516, 1777651
35	15	10	9	11	As above, with addition of overall-parity-check digit
47	25	9	8	12	All columns of code (30, 12) plus 1023305, 1347214, 2027151, 2457261, 3166444, 4055666, 4632577, 5251417, 7514712, 10057307, 11414574, 12345175, 17170103
48	25	10	9	12	As above, with addition of overall-parity-check digit
34	19	7	7	8	23642, 7504, 7211, 36422, 35044, 32111, 24223, 10447, 21117, 2236, 4475, 11172, 22364, 4750, 11721, 37777, 40343, 42507, 56016
35	19	8	8	8	As above, with addition of overall-parity-check digit
72	53	7	6	8	All columns of code (55, 38) plus 414510, 425201, 431744, 612665, 622311, 657104, 667425, 1014517, 1025230, 1031772, 1206630, 1236343, 1243167, 1273441, 1404303
73	53	8	7	8	As above, with addition overall-parity-check digit
86	66	7	6	8	All columns of code (72, 38) plus 2014523, 225217, 2031761, 2317101, 2327413, 2352645, 2362302, 2407003, 3106403, 3400062, 3431735, 3733415, 3776332
87	66	8	7	8	As above, with addition overall-parity-check digit
41	30	5	4	6	17, 63, 125, 152, 226, 253, 333, 355, 367, 427, 455, 511, 647, 1031, 1113, 1214, 1343, 1562, 1660, 1710, 1723, 2034, 2045, 2203, 2432, 2563, 3060, 3102, 3465, 3611
42	30	6	5	6	As above, with addition overall-parity-check digit
71	58	5	5	6	12543, 15172, 13115, 16445, 17131, 17440, 3220, 1750, 10347, 14270, 3066, 4267, 12220, 5110, 2444, 521, 14342, 13353, 15676, 2633, 4433, 5073, 12726, 5353, 12676, 2573, 11166, 12116, 5047, 12730, 5354, 10602, 4301, 15206, 6503, 12505, 16747, 17070, 3626, 1713, 5122, 2451, 11137, 11745, 14471, 16127, 777, 10064, 2025, 16012, 7005, 16510, 7244, 1661, 10423, 6071, 13327, 3374
72	58	6	5	6	As above, with addition of overall-parity-check digit

n = code length
k = number of information digits
d = Hamming distance
d_L = Helgert and Stinaff[1] lower bounds on minimum Hamming distance
d_U = Helgert and Stinaff[1] upper bounds on minimum Hamming distance