01 Jan 1971

Maximum-Distance Linear Codes

Gary K. Maki

James H. Tracey
Missouri University of Science and Technology

Recommended Citation

G. K. Maki and J. H. Tracey, "Maximum-Distance Linear Codes," *IEEE Transactions on Information Theory*, vol. 17, no. 5, p. 632, Institute of Electrical and Electronics Engineers, Jan 1971.
The definitive version is available at https://doi.org/10.1109/TIT.1971.1054680

by the recipe given in [4] are

$$(12) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \quad (23) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 & 0 \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & 0 & 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

$$(34) = \begin{pmatrix} -\frac{1}{3} & \frac{2\sqrt{2}}{3} & 0 & 0 & 0 \\ \frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \quad (45) = \begin{pmatrix} 1 & 0 & & 0 & 0 \\ 0 & -\frac{1}{2} & 0 & \frac{\sqrt{3}}{2} & 0 \\ 0 & 0 & -\frac{1}{2} & 0 & \frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{\sqrt{3}}{2} & 0 & \frac{1}{2} \end{pmatrix}.$$

The group of order 120 of 5×5 orthogonal matrices isomorphic with S_5 that is obtained by closure of these 4 matrices under multiplication is denoted by G_{120}.

Now $\overrightarrow{X_1}$ of Fig. 1 is left invariant by (12), (23), and (45) above. It is left invariant, therefore, by the subgroup of G_{120} generated by these matrices. This subgroup is of order 12, and is comprised of the matrices I, (12), (23), (13), (123), (132), (45), (12)(45), (23)(45), (13)(45), (123)(45), (132)(45). Here, for example, since in S_5 and (123) = (12)(23,) by the matrix (123) is meant the matrix product of the matrix (12) displayed above by the 5×5 matrix (23) similarly displayed. The matrices (14), (15), (24), (25), (34), (35), (24)(35), (14)(35), (14)(25) lie one per coset in the decomposition of G_{120} according to this subgroup. These 9 matrices send $\overrightarrow{X_1}$ into the remaining columns of Fig. 1.

It follows that χ is a group code and the demonstration is complete.

David Slepian
Bell Telephone Lab., Inc.
Murray Hill, N.J. 07974

References

[1] D. Slepian, "Group codes for the Gaussian channel," *Bell Syst. Tech. J.*, vol. 47, Apr. 1968, pp. 575–602.
[2] ——, "A class of binary signaling alphabets," *Bell Syst. Tech. J.*, vol. 35, Jan. 1956, pp. 203–234.
[3] a. M. Hall, *Theory of Groups*. New York: Macmillan, 1959, p. 44.
b. W. Burnside, *Theory of Groups*. New York: Dover, 1955, corollary II, p. 47.
[4] G. de B. Robinson, *Representation Theory of the Symmetric Group*. Toronto: Univ. Toronto Press, 1961.

Maximum-Distance Linear Codes

***Abstract*—Described here is a linear code that has a maximum distance between codewords of k for a code of order 2^k. Since the minimum–maximum distance is k for a code of order 2^k, a class of minimum–maximum distance codes results. For an (n,k) linear code, $k \leq n \leq k + k/2$ for k even and $k \leq n \leq k + (k - 1)/2$ for k odd. Maximum-distance codes are found useful in encoding the states of sequential circuits.**

Coding theory traditionally appears interested in minimum-distance linear codes. Maximum-distance codes are of interest in the encoding of asynchronous sequential circuits in that minimizing the distance between codewords reduces the hardware in the resulting circuit. Described here is a linear code where the maximum distance is k for a group of order 2^k.

Consider the n-tuples encoded with the variables $x_1,x_2,\cdots,x_k,x_{k+1},\cdots,x_n$. The variables $x_1,x_2,\cdots,x_k$ can be considered as information bits and $x_{k+1},\cdots,x_n$ as check or parity bits. A *parity set* is defined here as a set of variables $\{x_{l_1},x_{l_2},\cdots,x_{l_p},x_\xi\}$, where $\{x_{l_1}, x_{l_2},\cdots,x_{l_p}\} \in \{x_1,x_2,\cdots,x_k\}$, p is an even number, and $x_{l_1} \oplus x_{l_2} \oplus \cdots \oplus x_{l_p} = x_\xi$; $x_{l_1},x_{l_2},\cdots,x_{l_p}$ are called the independent variables and x_ξ is called the dependent variable of the parity set.

The code is constructed so that each x_i, $i = 1,2,\cdots,k$, is in no more than one parity set, and each x_i, $i = k + 1,\cdots,n$, is the dependent variable of some parity set. An example of an (n,k) code is given by the following generator matrix for a (9,7) code.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

The parity sets are $\{x_1,x_2,x_8\}$ and $\{x_3,x_4,x_5,x_6,x_9\}$. Variable x_7 is not in any parity set.

It should be clear that this encoding procedure produces a linear code of order 2^k.[1] The proof to show that the maximum distance is k follows these lines. Just as the minimum weight of a linear code is equal to the minimum distance,[1] the maximum weight is equal to the maximum distance. The maximum weight of a parity set $\{x_{l_1},x_{l_2},\cdots,x_{l_p},x_\xi\}$ is p since, by the closure property of the code, there exists a case where $x_{l_1} = x_{l_2} = \cdots = x_{l_p} = 1$; and since p is even, $x_\xi = 0$. In other words, the maximum weight of a parity set is equal to the number of independent variables in the parity set.

Let the code consist of m parity sets, in which there are $k - q$ independent variables and a set of q variables (independent) not in any parity set. Since each parity set consists of a disjoint set of variables, the maximum weight of the parity sets is the sum of the maximum weights of the parity sets. Since there are $k - q$ independent variables in the parity sets, the maximum weight of the parity sets is $k - q$. One of the codewords of maximum weight is where $x_1 = x_2 = \cdots = x_k = 1$ and here the weight is $k - q$ (the weight of the parity sets) plus q (the weight of the variables not in parity sets). Therefore the maximum weight is k.

The minimum–maximum distance is k for a linear code of order 2^k. (This is easily seen when $k = n$.) Therefore, the linear code here produces a code of minimum–maximum distance.

Since the smallest nonempty parity set consists of 3 variables, the maximum number of parity sets is $k/2$ for k even and $(k - 1)/2$ for k odd. Therefore the largest n-tuples is where $n = k + k/2$ for k even and $n = k + (k - 1)/2$ for k odd. For a maximum-distance k code, $k \leq n \leq k + k/2$ (or $k + (k - 1)/2$).

Details relative to this code's relationship to encoding asynchronous sequential circuits can be found in Maki.[2]

Gary K. Maki
Univ. Idaho
Moscow, Ida. 83843
James H. Tracey
Univ. Missouri
Rolla, Mo. 65403

Manuscript received February 1, 1971. This research was supported in part by the National Science Foundation under Grants GK-5907 and GK-2017.

[1] W. W. Peterson, *Error-Correcting Codes*. Cambridge, Mass.: M.I.T. Press, 1961.
[2] G. K. Maki, "State assignments for non-normal asynchronous sequential circuits," Ph.D. dissertation, Univ. Missouri, Rolla, 1969.