On Shortened Finite Geometry Codes*

C. L. CHEN

Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801

A general method of shortening a linear block code is introduced. Application of this shortening method to finite geometry codes produces a new class of majority-logic decodable codes.

INTRODUCTION

The class of finite geometry codes [Rudolph (1964, 1967), Weldon (1967, 1968), Goethals and Delsarte (1968), Peterson and Weldon (1972)] consisting of Euclidean geometry codes and projective geometry codes forms a class of multiple-error-correcting codes that are majority-logic decodable. Being majority-logic decodable codes, finite geometry codes can be simply implemented with high speed. The decoding complexity of these codes has been further reduced by a recently developed scheme (Chen, 1972). Thus these codes are attractive for error-control systems. However, the code length and code dimension of finite geometry codes are rather sparsely distributed. Very often this hinders the adoption of finite geometry codes in practical application.

One way to circumvent this situation is to shorten finite geometry codes. In this paper, we shall first present a general method of shortening linear block codes. The shortening of a code here has a more general meaning than in Berlekamp's (1968) book. The minimum distance of the shortened codes is at least as large as the original codes. The number of parity check digits will be reduced, however. Next, the general method of shortening linear block codes will be applied to finite geometry codes. The shortened finite geometry codes will preserve the nice features of being majority-logic decodable.

* This work was supported by the National Science Foundation under Grant No. GK-24879; auxiliary support was provided by the Joint Services Electronics Program (U.S. Army, U.S. Navy, and U.S. Air Force) under Contract DAAB-07-67-C-0199.

© 1972 by Academic Press, Inc.
Shortening a code by deleting some of its information digits is a common way of modifying a code (Berlekamp, Chap. 14, 1968). Let \((n, k)\) code denote a linear block code of length \(n\) with \(k\) information digits. Then the code can be shortened by deleting \(l\) information digits. The shortened code forms an \((n - l, k - l)\) code with the same number of parity check digits as the original code. The minimum distance of the shortened code is at least as large as the original code.

After having observed that the shortened code consists of the set of vectors of the original code which are zero on the deleted positions, we propose a more general way of shortening a code. It merely consists of selecting those vectors of the original code which have zeros on \(l\) given positions, and which obviously form a linear subspace. Deleting the \(l\)-chosen positions gives the shortened code. If these positions are carefully chosen, usually less than \(l\) information digits have to be deleted, giving a shortened code with less parity check digits than the original code. A way to achieve this is presented in the following theorem, for which we shall need the following definition.

**Definition 1.** A subcode \(C'\) of a code \(C\) is said to have *effective length* \(l\), if any vector of \(C'\) has all its nonzero elements confined in certain \(l\) fixed positions. Accordingly, a shortened code is a subcode of the original code, with a smaller effective length.

**Theorem 1.** If the dual code \(\bar{C}\) of an \((n, k)\) code \(C\) contains a subcode of effective length \(l\) and dimension \(l - k_0\), then \(C\) contains a subcode of dimension \(k - k_0\) and effective length \(n - l\), that is a shortened \((n - l, k - k_0)\) code.

*Proof.* Let \(G\) and \(H\) be the generator matrices of \(C\) and \(\bar{C}\), respectively. In addition, let \(H_0\) be the generator matrix of the subcode of \(\bar{C}\) with effective length \(l\) and dimension \(l - k_0\). Then \(H_0\) is a submatrix of \(H\). Let \(G_0\) be the submatrix of \(G\) such that every row vector in \(G_0\) has some nonzero elements at the \(l\) given positions corresponding to the nonzero columns of \(H_0\). The row rank of \(G_0\) is equal to \(k_0\). Deleting \(G_0\) from \(G\), we have a matrix that generates a subcode of \(C\) with effective length \(n - l\) and dimension \(k - k_0\). This subcode is the dual code generated by the matrix obtained from \(H\) by deleting the \(l\) given columns corresponding to the nonzero columns of \(H_0\). Q.E.D.
The relationship between the subcodes and the original codes can be depicted as follows:

\[ H : \]

\[ G : \]

The shaded areas in \( G \) and \( H \) represent the shortened code and the dual of the shortened code, respectively, in Theorem 1. \([0]\) represents an all zeros matrix. It should be mentioned that the \( l \) given positions are not necessarily in a consecutive order.

Let \( d_0 \) be the minimum weight of a vector in the null space \( H \) of an \((n, k)\) code. The vector generates a \((d_0, 1)\) code or subspace. If we delete from the \((n, k)\) code all vectors except those containing 0's elements in the \( d_0 \) positions corresponding to the nonzero elements of the minimum weight vector in \( H \), then we have a shortened \((n - d_0, k - d_0 + 1)\) code which has one less parity check digit than the original code. Thus we have the following corollary which has been discovered by Goethals (1971).

**Corollary.** Let \( d_0 \) be the minimum weight of a vector in the null space of an \((n, k)\) code, then a shortened \((n - d_0, k - d_0 + 1)\) code can be constructed that has a minimum distance at least as large as the original code.

**APPLICATION TO FINITE GEOMETRY CODES**

Let \( EG(m, p^s) \) and \( PG(m, p^s) \) denote the \( m \)-dimensional Euclidean geometry and projective geometry, respectively, over the finite field \( GF(p^s) \). Euclidean geometry (\( EG \)) codes and projective geometry (\( PG \)) codes can be defined as follows.

**Definition 2.** An \( r \)-th order \( EG \) code over \( GF(p) \) of length \( n = p^{ms} \) associated with \( EG(m, p^s) \) is the largest code that contains the incidence matrix of all \( r \)-flats of \( EG(m, p^s) \) in its null space.
DEFINITION 3. An $r$-th order $PG$ coder over $GF(p)$ of length $n = (p^{(m+1)r} - 1)/(p^r - 1)$ associated with $PG(m, p^s)$ is the largest code that contains in its null space the incidence matrix of all $r$-flats of $PG(m, p^s)$.

Note that an $r$-th order $EG$ code can be made cyclic by deleting an overall parity check digit.

It is well-known that $EG(m, p^s)$ can be obtained from $PG(m, p^s)$ by deleting the points of a $PG(m - 1, p^s)$ that is contained in the $PG(m, p^s)$ (CarMichael, Chap. XI, 1956). Furthermore, a vector corresponding to an $r$-flat can be obtained from a linear combination of the vectors corresponding to some $(r-1)$-flats. Thus, the null space of an $(r-1)$-th order geometry code contains the null space of an $r$-th order code as a subspace. This is equivalent to saying that an $(r-1)$-th order code is a subcode of an $r$-th order code associated with the same geometry.

Consider an $r$-th order $PG$ code associated with $PG(m, p^s)$. The null space $A$ contains as a subspace $B$ the null space of an $r$-th order $PG$ code associated with $PG(m - 1, p^s)$. Deleting from space $A$ those vectors in $B$ and those positions associated with $PG(m - 1, p^s)$, we have a shortened code that has the same code length as an $r$-th order $EG$ code associated with $EG(m, p^s)$. In fact, it can be shown (Delsarte et al., 1970) that the shortened code is equivalent to the $EG$ code. We write this result as follows.

THEOREM 2. An $r$-th order $EG$ code associated with $EG(m, p^s)$ can be obtained from an $r$-th order $PG$ code associated with $PG(m, p^s)$ by deleting a subgeometry $PG(m - 1, p^s)$ of $PG(m, p^s)$ and those vectors that contain nonzero elements in the positions corresponding to the deleted $PG(m - 1, p^s)$.

The $BCH$ bound on minimum distance $d_{BCH}$ of an $r$-th order $PG$ code associated with $PG(m, p^s)$ is equal to $d_{BCH} = (p^{s(m-r+1)} - 1)/(p^s - 1) + 1$. According to Theorem 2 the minimum distance of an $r$-th order $EG$ code associated with $EG(m, p^s)$ is at least as large as $d_{BCH} = (p^{s(m-r+1)} - 1)/(p^s - 1) + 1$. It has been shown [e.g., Kasami et al., 1968; Weldon and Peterson, 1972] that $d_{BCH}$ of an $r$-th order $EG$ code is equal to $d_{BCH} = p^{s(m-r-2)} + p^{s(m-r-1)} + 1$ which is greater than $[p^{s(m-r+1)} - 1]/(p^s - 1) + 1$.

Now let us consider $EG$ codes only. The null space of an $r$-th order code associated with $EG(m, p^s)$ contains as a subspace the null space of an $r$-th order code associated with $EG(m_0, p^s)$, where $r \leq m_0 < m$. Thus, a shortened $EG$ code can be formed by deleting the digits corresponding to $EG(m_0, p^s)$ and deleting those code vectors that have nonzero elements in the positions corresponding to the deleted $EG(m_0, p^s)$. Let $(n, k)$ code denote the $r$-th order code associated with $EG(m, p^s)$, and $(n_0, k_0)$ code
denote the \( r \)-th order code associated with \( EG(m_0, p^n) \). Then the shortened code is an \((n - n_0, k - k_0)\) code which has \((n_0 - k_0)\) less number of parity check digits than the \((n, k)\) code. Furthermore, the number of parity check equations orthogonal on the digits corresponding to a certain flat for the shortened code is the same as that for the original \((n, k)\) code, with each of the parity check equations containing less number of digits. Thus, the shortened code can be majority-logic decoded in a similar way as the original code with the same guaranteed correctable error patterns. The following theorem is a summary of the above results.

**Theorem 3.** If an \( r \)-th order code associated with \( EG(m, p^n) \) is an \((n, k)\) code and an \( r \)-th order code associated with \( EG(m_0, p^n) \) is an \((n_0, k_0)\) code, where \( r \leq m_0 < m \), then a shortened \((n - n_0, k - k_0)\) code that is majority-logic decodable can be constructed.

For an example, the second order \( EG \) code associated with \( EG(4, 2^2) \) is a \((256, 127)\) code with \( d = 24 \), and the second order \( EG \) code associated with \( EG(3, 2^2) \) is a \((64, 48)\) code. A shortened \((192, 79)\) code with \( d \geq 24 \) can be obtained from these two \( EG \) codes.

A similar result on \( PG \) codes can be obtained as follows.

**Theorem 4.** If an \( r \)-th order code associated with \( PG(m, p^n) \) is an \((n, k)\) code and an \( r \)-th order code associated with \( PG(m_0, p^n) \) is an \((n_0, k_0)\) code, where \( r \leq m_0 < m \), then a shortened \((n - n_0, k - k_0)\) majority-logic decodable code can be constructed.

Note that for the case \( m_0 = m - 1 \), the above theorem reduces to Theorem 2.

For \( s = 1, p = 2 \), finite geometry codes reduces to Reed–Muller (RM) codes. The results above applied to Reed–Muller codes have been studied by Chen and Lin (1970).

An \( r \)-th order RM code of length \( 2^m \) has \( K = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r} \) information digits with a minimum distance \( d = 2^{m-r} \). According to Theorem 3 a shortened code can be constructed from the \( r \)-th order RM code with the following parameters:

- code length = \( 2^n - 2^{m_0} \), \( r \leq m_0 \leq m \)
- number of information digits = \( \sum_r^r \left[ \binom{m}{r} - \binom{m_0}{r} \right] \)
- minimum distance = \( d \)

Note that the number of parity check digits for the shortened code is reduced by \( 2^{m_0} - \sum_r^r \binom{m_0}{r} \).
Conclusions

A general method of shortening a linear block code has been introduced in this paper. This method may be considered a generalization of Goethals (1971), and Chen and Lin (1970). The application of this method to finite geometry codes has been presented. The shortened finite geometry codes form a new class of majority-logic decodable codes.

It would be interesting to know how the minimum distance of a code would be affected by shortening.

Acknowledgment

The author wishes to thank the reviewer for valuable comments.

Received: July 1, 1971

References