Adding Two Information Symbols to Certain Nonbinary BCH Codes and Some Applications

By JACK KEIL WOLF

(Manuscript received March 20, 1969)

This paper is a compendium of results based on a simple observation: two information symbols can be appended to certain nonbinary BCH codes without affecting the guaranteed minimum distance of these codes. We give two formulations which achieve this result; the second yields information regarding the weights of coset *leaders for the original BCH codes.*

Single-error-correcting Reed-Solomon codes with the added information symbols yield perfect codes for the Hamming metric. We use these lengthened Reed-Solomon codes as building blocks for perfect single-error-correcting codes in another metric.

I. INTRODUCTION

This paper is a compendium of results based upon a simple observation: two information symbols can be appended to the code words of certain BCH codes without weakening the error correction capability of these codes.

We define a class of BCH codes called "maximally redundant codes" in Section II; for codes in this class a simple method is given for appending two columns to the check matrix which does not increase the number of check symbols for the code nor decrease the error correction capability of these codes. Section III gives the parameters for lengthened Reed-Solomon codes and shows that such codes are perfect for single error correction. Section IV discusses a general decoding algorithm for the lengthened codes and shows that these codes are invariant under certain permutation operations.

Section V discusses a method for constructing the lengthened codes from cosets of the original code. We use this approach in Section VI to determine the lower bounds on the number of high weight cosets

for the original BCH codes. Section VII defines a new metric and gives a procedure for constructing some perfect codes in this metric. These codes are based upon the lengthened Reed-Solomon codes. The appendix shows that a necessary and sufficient condition for the nonzero elements of $GF(p)$ to be partitioned into mutually exclusive and exhaustive four element subsets of the form

$$\{x, \beta x, -x, -\beta x\}, \qquad \beta, x \in GF(p)$$

is that there exists an integer t such that

$$\beta^{2t} \equiv -1 (\text{mod } p).$$

II. BCH CODES

BCH codes are random-error-correcting codes for symbols from $GF(q)$ where q is a prime (in which case q is replaced by p) or a power of a prime.[1-3] Let α be an element of $GF(q^m)$ and let the order of α be n. That is, $\alpha^n = 1$ and $\alpha^i \neq 1$ for $i < n$. The check matrix of a BCH code with designed distance d can then be given as

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha^{m_0} & (\alpha^{m_0})^2 & \cdots & (\alpha^{m_0})^{n-1} \\ 1 & \alpha^{m_0+1} & (\alpha^{m_0+1})^2 & \cdots & (\alpha^{m_0+1})^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{m_0+d-2} & (\alpha^{m_0+d-2})^2 & \cdots & (\alpha^{m_0+d-2})^{n-1} \end{bmatrix}.$$

The code words are all n-vectors, $\mathbf{C}$, with entries from $GF(q)$ which satisfy the equation

$$\mathbf{HC} = \mathbf{O}.$$

(Unless stated to the contrary, all vectors are column vectors.)

The proof that such codes have minimum distance at least d follows from demonstrating that all sets of $d - 1$ or fewer columns of $\mathbf{H}$ are linearly independent over $GF(q)$. Actually, the proof shows more than this: it shows that all sets of $d - 1$ or fewer columns of $\mathbf{H}$ are linearly independent over any extension field of $GF(q)$. To establish this linear independence let us consider the columns $j_1, j_2, \cdots, j_{d-1}$ and the determinant of the corresponding $(d - 1)$ by $(d - 1)$ array of symbols from $GF(q^m)$. Then,

$$\det \begin{vmatrix} (\alpha^{m_0})^{j_1} & (\alpha^{m_0})^{j_2} & \cdots & (\alpha^{m_0})^{j_{d-1}} \\ (\alpha^{m_0+1})^{j_1} & (\alpha^{m_0+1})^{j_2} & \cdots & (\alpha^{m_0+1})^{j_{d-1}} \\ \vdots & \vdots & \cdots & \vdots \\ (\alpha^{m_0+d-2})^{j_1} & (\alpha^{m_0+d-2})^{j_2} & \cdots & (\alpha^{m_0+d-2})^{j_{d-1}} \end{vmatrix}$$

$$= \alpha^{m_0(j_1+j_2+\cdots+j_{d-1})} \det \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \cdots & \alpha^{j_{d-1}} \\ \vdots & \vdots & \cdots & \vdots \\ (\alpha^{j_1})^{d-2} & (\alpha^{j_2})^{d-2} & \cdots & (\alpha^{j_{d-1}})^{d-2} \end{vmatrix}.$$

The latter determinant is a Vander Monde determinant and is known to be nonzero if $\alpha^{j_i} \neq \alpha^{j_k}$ for $i \neq k$. Since the elements of the matrices in question are elements from $GF(q^m)$, the nonvanishing of the determinant ensures that any set of $d-1$ columns of the check matrix are linearly independent over $GF(q^m)$. The special case of $m = 1$ defines a subset of BCH codes called Reed-Solomon codes.[4]

The number of check symbols in the code is upper bounded by $m(d-1)$ since these are the number of rows in the check matrix after each symbol from $GF(q^m)$ is replaced by an m-vector with elements from $GF(q)$. The reason that $m(d-1)$ is merely an upper bound is that the number of check symbols is equal to the number of linearly independent rows in the check matrix [when expressed in terms of elements from $GF(q)$]; in general this number can be less than $m(d-1)$. In this paper, codes for which the number of check symbols is equal to $m(d-1)$ are called "maximally redundant" BCH codes. Binary codes (codes for which $q = 2$) are examples of nonmaximally redundant codes while Reed-Solomon codes (codes for which $m = 1$) are examples of maximally redundant codes.

Let us now consider appending two columns to the check matrix, $\mathbf{H}$, to form the new check matrix, $\mathbf{H}'$,

$$\mathbf{H}' = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \mathbf{H}.$$

It is now easy to see that any $(d-1)$ columns of $\mathbf{H}'$ are linearly independent over $GF(q^m)$. [Determinants formed from $(d-1)$ columns, excluding the first two columns, are $(d-1)$ by $(d-1)$ Vander Monde. Determinants formed from $(d-1)$ columns, including one of the first two columns, are $(d-2)$ by $(d-2)$ Vander Monde after expansion about the column in question. Determinants formed from $(d-1)$

columns, including both the first and second column of $\mathbf{H}'$, are $(d-3)$ by $(d-3)$ Vander Monde after expansion.]

The number of symbols per block in the lengthened code is thus two more than the corresponding number for the BCH code. The number of check symbols may or may not be increased in accordance with whether or not the number of linearly independent rows remains the same after the addition of these two columns. One class of BCH codes for which the number of check symbols does not increase is the maximally redundant codes. This class includes all Reed-Solomon codes as well as other codes.

It is possible that in some cases more than two columns can be appended to the parity check matrix while preserving the designed distance of the code. No general results have been found, however, for such cases.* For example, if a column is appended which contains a single 1 in the $(l+1)$th position of the column vector, the resultant determinant after expansion and factoring is of the form

$$D_l = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_{d-2}} \\ \cdot & \cdot & \cdots & \cdot \\ (\alpha^{i_1})^{l-1} & (\alpha^{i_2})^{l-1} & \cdots & (\alpha^{i_{d-2}})^{l-1} \\ (\alpha^{i_1})^{l+1} & (\alpha^{i_2})^{l+1} & \cdots & (\alpha^{i_{d-2}})^{l+1} \\ \cdot & \cdot & \cdots & \cdot \\ (\alpha^{i_1})^{d-2} & (\alpha^{i_2})^{d-2} & \cdots & (\alpha^{i_{d-2}})^{d-2} \end{vmatrix}.$$

Such a determinant can be evaluated as

$$D_l = \prod_{i>k}^{d-2} (\alpha^{i_i} - \alpha^{i_k}) \text{ [sum of all products of } (d-2-l) \text{ distinct } \alpha^{i_i}].$$

The latter sum of products can be zero even if all the α^{i_i} are distinct.

III. LENGTHENED REED-SOLOMON CODES

The Reed-Solomon codes codes with symbols from $GF(q)$ are BCH codes formed by choosing the parameter $m = 1$. These codes have parameters

$$\text{block length} \qquad n = q - 1,$$

$$\text{check symbols per block } r = d - 1,$$

* An exception is $d = 4$ and q even where three columns can be appended to the parity check matrix. The appended columns are then the 3×3 identity matrix.

and correct any pattern of $[(d-1)/2]$ or fewer errors in a block of length n. Any t error-correcting linear code can have no fewer than $2t$ check symbols; this bound is achieved by the Reed-Solomon codes if d is an odd integer. This is not to say that the codes cannot be improved upon: in particular, the lengthened codes formed as described in Section II represent a minor improvement.

The lengthened code has parameters:

$$\text{block length} \qquad n' = q + 1,$$
$$\text{check symbols per block } r' = (d-1),$$

and corrects any pattern of $[(d-1)/2]$ or fewer errors in a block of length n' symbols. The lengthened codes are maximum distance separable (MDS) in that they have the maximum possible minimum distance for a given block length n', and code size $q^{(n'-r')}$. These codes complement the set of maximum distance separable codes given by Singleton.[5] The weight distributions of the code words of maximum distance separable codes are given by Berlekamp.[6] The case of single error-correcting lengthened Reed-Solomon codes (that is, $d = 3$) are of particular interest in that they are perfect codes. That is, bounded distance decoding results in the use of every syndrome. Specifically, there are q^2 distinct syndromes. There are $(q-1)$ different errors which can occur in any of the $(q+1)$ different positions resulting in $q^2 - 1$ different error patterns. The all zero error pattern (no errors) in addition to the $(q-1)(q+1) = q^2 - 1$ single error patterns use all q^2 syndromes.

IV. Decoding and Symmetry of Lengthened Maximally Redundant BCH Codes*

The columns of the parity check matrix are conveniently labeled:

$$\overleftarrow{\qquad\qquad n' \qquad\qquad}\overrightarrow{\qquad}$$

$$\mathbf{H}' = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 1 & \alpha & (\alpha)^2 & \cdots & (\alpha)^{n'-3} \\ 0 & 0 & 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n'-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & 1 & \alpha^{d-2} & (\alpha^{d-2})^2 & \cdots & (\alpha^{d-2})^{n'-3} \end{bmatrix}$$

$$\text{label} \quad 0 \quad \infty \quad 1 \quad \alpha \quad \alpha^2 \qquad\qquad \alpha^{n'-3}$$

* This section is based on suggestions from E. R. Berlekamp of Bell Telephone Laboratories.

where α is a primitive element of $GF(q^m)$ and m_o has been taken equal to zero. If the second column were omitted from this matrix, the resultant code would be an extension of a BCH code of designed distance $d - 1$. That is, the resultant code is obtained by appending an overall parity check digit to a BCH code of designed distance $d - 1$. The code with the second digit omitted (block length $n' - 1$) is called a "singly-lengthened" BCH code. The code of block length n' (which includes all digits) is called a "doubly-lengthened" BCH code.

For d odd, one decoding algorithm for the correction of $[(d - 1)/2]$ or fewer errors for the doubly lengthened BCH codes is:

(*i*) Ignore the last syndrome digit (the only equation involving the symbol in position labeled ∞) and decode as in Section 10.3 of Ref. 6 for extended BCH codes. Let D be the number of errors indicated by the decoding algorithm. If $D < (d - 1)/2$, decode all positions except the position labeled ∞ and then use the last parity check equation to decode the position labeled ∞.

(*ii*) If $D = (d - 1)/2$, assume that the digit in position ∞ is correct, modify the syndrome accordingly, and decode as in Ref. 6 using all digits in the modified syndrome.

The lengthened primitive BCH codes have interesting symmetry properties. Since the singly-lengthened primitive BCH code is an extension of a primitive BCH code with designed distance one less, it is invariant under the affine permutation group on $GF(q)$, as Theorem 10.37 of Ref. 6 shows.

One might hope that the doubly-lengthened BCH code would be invariant under the triply-transitive linear fractional group on $GF(q) \cup \infty$ (page 358 of Ref. 6). This is not really the case since the code is not invariant under the simple permutation $x \rightarrow 1/x$. The doubly-lengthened BCH code is invariant, however, under the multiply and permute operation of order two specified:

(*i*) Exchange digits at 0 and ∞.

(*ii*) Multiply digit at α^i by $\alpha^{-i(d-2)}$ and then move it to position α^{-i}.

This operation transforms the $\mathbf{H}'$ matrix into the same matrix with the rows listed in reverse order. Since this operation preserves Hamming weights, it ensures considerable symmetry.

V. ALTERNATIVE FORMULATION OF LENGTHENED MAXIMALLY REDUNDANT BCH CODES

We will now describe an alternative formulation of lengthened maxi-

mally redundant BCH codes which is more complicated than that described in Section III. However, its real utility is that it gives insight to the problem of determining the weight distribution of coset leaders for the (unlengthened) BCH codes (a subject discussed in Section V).

Consider an (unlengthened) maximally redundant BCH code [with symbols from $GF(q)$] with check matrix

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha^{m_0} & (\alpha^{m_0})^2 & \cdots & (\alpha^{m_0})^{n-1} \\ 1 & \alpha^{m_0+1} & (\alpha^{m_0+1})^2 & \cdots & (\alpha^{m_0+1})^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{m_0+d-2} & (\alpha^{m_0+d-2})^2 & \cdots & (\alpha^{m_0+d-2})^{n-1} \end{bmatrix},$$

where α is an element of $GF(q^m)$. Consider an n-vector $\mathbf{X}$ [with entries from $GF(q)$] such that

$$\mathbf{HX} = \begin{bmatrix} \sigma_1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \sigma_2 \end{bmatrix},$$

where σ_1 and σ_2 are elements from $GF(q^m)$. We now prove the following inequalities regarding the weight of $\mathbf{X}$, denoted $W(\mathbf{X})$.

Inequality 1: If $\sigma_1 = \sigma_2 = 0$, $W(\mathbf{X}) \geqq d$ for $\mathbf{X} \neq 0$.

Proof: The vectors $\mathbf{X}$ which satisfy $\mathbf{HX} = \mathbf{O}$ are the code words of the code with check matrix $\mathbf{H}$ and have minimum distance at least d. Thus the weight of any nonzero code word is greater than or equal to d.

Inequality 2: If $\sigma_1 = 0$ and $\sigma_2 \neq 0$ or if $\sigma_1 \neq 0$ and $\sigma_2 = 0$, then $W(\mathbf{X}) \geqq d - 1$.

Proof: We first note that $\mathbf{X} \neq 0$ since either σ_1 or σ_2 is nonzero. Next consider the case where $\sigma_1 \neq 0$ and $\sigma_2 = 0$ and form a new check matrix $\mathbf{H}_{(1)}$ obtained by deleting the first row of $\mathbf{H}$. Now $\mathbf{H}_{(1)}\mathbf{X} = 0$ so that $\mathbf{X}$ is a code word corresponding to the check matrix $\mathbf{H}_{(1)}$. But any $(d-2)$ columns of $\mathbf{H}_{(1)}$ form a $(d-2)$ by $(d-2)$ Vander Monde determinant

so that the weight of $\mathbf{X}$ is at least $(d-1)$. The proof for the case where $\sigma_1 = 0$ and $\sigma_2 \neq 0$ follows similarly by noticing that $\mathbf{X}$ is a code word in a code corresponding to a check matrix formed by deleting the last row of $\mathbf{H}$.

Inequality 3: If $\sigma_1 \neq 0$ and $\sigma_2 \neq 0$, then $W(\mathbf{X}) \geqq d-2$.

Proof: Again $\mathbf{X} \neq 0$ since both σ_1 and σ_2 are nonzero. Now consider a check matrix formed by deleting the first and last rows of $\mathbf{H}$. Since $\mathbf{X}$ is in the null space of this new check matrix, every such nonzero vector must have weight at least $(d-2)$.

The lengthened code is now formed of $(n+2)$-tuples of the form $\begin{bmatrix} -\sigma_1 \\ -\sigma_2 \\ \mathbf{X} \end{bmatrix}$.

From before we see that all such nonzero vectors must have weight at least d. It is easy to verify that the set of code words from a linear code and indeed that such a linear code is the null space of the check matrix

$$\mathbf{H}' = \begin{bmatrix} 1 & 0 & \\ 0 & 0 & \\ 0 & 0 & \mathbf{H} \\ \vdots & \vdots & \\ 0 & 1 & \end{bmatrix}.$$

VI. WEIGHTS OF COSETS OF MAXIMALLY REDUNDANT BCH CODES

In this section we digress from the main theme of this paper to present some results on another problem: determining the weights of cosets (that is, coset leaders) for maximally redundant BCH codes. It should be emphasized that this problem differs from the widely researched problem of determining the weights of the code words themselves.

The complete weight enumeration of the cosets is known only for a very few classes of codes.[6] This knowledge is crucial to determining the performance of codes using a complete decoding algorithm (that is, maximum likelihood decoding).

In this section we are not able to determine the complete weight enumeration for the codes under consideration. Rather we can only give lower bounds to the number of coset leaders whose weight exceeds

certain values. However, we believe that this knowledge is both new and useful.

Specifically we are concerned with the weights of coset leaders of maximally redundant primitive BCH codes. Our main result is:

$$[\text{Number of coset leaders of weight} \geqq d - j]$$
$$\geqq (q^m)^{j-1}[(j+1)q^m - j] - 1 \quad \text{for} \quad \begin{cases} j \geqq 1 \\ 2j < d. \end{cases}$$

This result shows that for a maximally redundant BCH code of minimum (designed) distance d, in addition to having as coset leaders all vectors of weight less than or equal to $[(d-1)/2]$, coset leaders exist for all weights up to and including $(d-1)$. The actual minimum distance of the code, d_{ACT}, may exceed the designed distance d. If $[(d_{ACT}-1)/2] < d-1$, the codes cannot be perfect codes and if $[(d_{ACT}-1)/2] < d-2$, the codes cannot be quasiperfect. For Reed-Solomon codes $d_{ACT} = d$ and the codes are not perfect for any d and not quasiperfect for $d > 3$.

Proof: Consider a coset leader $\mathbf{X}'$ corresponding to the syndrome, $\mathbf{S}$, where

$$\mathbf{HX}' = \mathbf{S} = \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_i \\ 0 \\ 0 \\ \vdots \\ 0 \\ \sigma_{i+1} \\ \sigma_{i+2} \\ \vdots \\ \sigma_j \end{bmatrix} \begin{matrix} \uparrow \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \downarrow \end{matrix} d-1 \quad \text{where} \quad \sigma_i \in GF(q^m) \qquad i = 0, 1, \cdots, j.$$

Consider a new check matrix obtained by deleting the first i rows and the last $(j-i)$ rows of $\mathbf{H}$. $\mathbf{X}'$ must be a vector in the null space of this new check matrix and will be nonzero unless $\sigma_1 = \sigma_2 = \cdots = \sigma_j = 0$.

Furthermore every such nonzero vector must have weight at least $d - j$ since any set of $d - 1 - j$ columns of this new check matrix forms a Vander Monde determinant. A counting problem remains: counting the number of distinct nonzero syndromes having a run of $d - 1 - j$ consecutive zeros. For $i = j$, there are $(q^m)^j - 1$ such patterns corresponding to the q^m different values for each σ_i (excluding $\sigma_1 = \sigma_2 = \cdots = \sigma_i = 0$). For each $i < j$, there are $(q^m - 1)(q^m)^{i-1}$ such patterns corresponding to the $(q^m - 1)$ distinct nonzero values for σ_{i+1} and the q^m distinct values for all other σ_k, $k \neq i + 1$. Counting in this fashion, if $2j < d$ we include each such pattern once and only once resulting in a total of

$$(q^m)^j - 1 + j(q^m - 1)(q^m)^{i-1} = (q^m)^{i-1}[(j + 1)q^m - j] - 1$$

such patterns.

The above proof not only yields a bound to the number of high weight coset leaders but also gives an easy way of recognizing their occurrence from their respective syndromes. Thus if one were to use bounded distance decoding (decoding only coset leaders of weight $\leqq [(d - 1)/2]$), many nondecodable cosets would be easily recognizable by the form of the syndrome.

A tighter bound can sometimes be obtained by noticing that the parity check matrix

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha^{m_0} & (\alpha^{m_0})^2 & \cdots & (\alpha^{m_0})^{n-1} \\ 1 & \alpha^{m_0+a} & (\alpha^{m_0+a})^2 & \cdots & (\alpha^{m_0+a})^{n-1} \\ 1 & \alpha^{m_0+2a} & (\alpha^{m_0+2a})^2 & \cdots & (\alpha^{m_0+2a})^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{m_0+(d-2)a} & (\alpha^{m_0+(d-2)a})^2 & \cdots & (\alpha^{m_0+(d-2)a})^{n-1} \end{bmatrix}$$

yields a code with a minimum distance of at least d if a and n are relatively prime. Thus the zeros in the syndrome that signify a high weight coset need not occur as a single burst but rather can occur with a fixed periodicity.

VII. SOME PERFECT SINGLE-ERROR-CORRECTING CODES FOR ANOTHER METRIC

In this section we use the lengthened Reed-Solomon codes to construct codes for a new metric. In particular, we consider the case where $q = p$, a prime, and we are interested in codes that correct errors of the form $\pm 1, \pm 2, \cdots, \pm T$ in a "single position" of a code word. In particular,

codes are given for $T = 1$ and $T = 2$. For $T = 1$, these codes are single-error-correcting Lee metric codes.[7]

The lengthened Reed-Solomon code used in the construction of these codes has a check matrix

$$\mathbf{H}' = \begin{bmatrix} \longleftarrow n' = p + 1 \longrightarrow \\ 1 & 0 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{p-2} \end{bmatrix}$$

where α is a primitive element from $GF(p)$. The null space of this matrix is a perfect single-error-correcting code for the Hamming metric. That is, it corrects any error $[\pm 1, \pm 2, \cdots, \pm(p - 1/2)]$ which occurs in any one position in a code word.

Consider the case where it is required only to correct an error of the form ± 1. Also consider the new check matrix

$$\mathbf{H}'' = \left[\mathbf{H}' \quad 2\mathbf{H}' \quad 3\mathbf{H}' \quad \cdots \quad \left(\frac{p-1}{2}\right)\mathbf{H}' \right], \qquad \longleftarrow n'' = \left(\frac{p-1}{2}\right)n' = \frac{p^2-1}{2} \longrightarrow$$

To show that the null space of $\mathbf{H}''$ will correct any single error of the form ± 1, we need only show that all columns of $\mathbf{H}''$ are distinct from each other after multiplication by ± 1. This follows immediately from noticing that all pairs of columns of $\mathbf{H}'$ are linearly independent over $GF(p)$.

We prove the code is perfect by noting that $2n'' + 1 = p^2$ syndromes are needed to correct a ± 1 error in each of the n'' positions (plus the all zero error pattern). But since $\mathbf{H}''$ has two rows, there are exactly p^2 syndromes; every syndrome is used to correct the required error patterns.

The above code has the same block length, number of check symbols, and error corrections capability as Berlekamp's perfect megacyclic single-error-correcting Lee metric codes.[6]

The form chosen for $\mathbf{H}'$ with the first row consisting of all ones and a single zero makes the decoding algorithm easy. Let

$$\mathbf{S} = \begin{bmatrix} \sigma_1 \\ \sigma_2 \end{bmatrix} \quad \text{where} \quad -\frac{(p-1)}{2} \leqq \sigma_i \leqq \frac{p-1}{2} \; i = 1, 2.$$

The algorithm is as follows.

(*i*) If $\sigma_1 = 0$, the error is in position $2 + (|\sigma_2| - 1)n'$ and has value sgn (σ_2).

(*ii*) If $\sigma_2 = 0$, the error is in position $1 + (|\sigma_1| - 1)n'$ and has value sgn (σ_1).

(*iii*) If $\sigma_1 \neq 0$ and $\sigma_2 \neq 0$, let x be the solution to the congruence $\sigma_1\alpha^x \equiv \sigma_2 \bmod (p)$. The error is then in position $(x + 3) + (|\sigma_1| - 1)n'$ and has value sgn (σ_1).

As an example, consider the code for $p = 5$ with $\alpha = 2$, a primitive root. Then

$$\mathbf{H}' = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 4 & 3 \end{bmatrix}$$

and

$$\mathbf{H}'' = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 2 & 0 & 2 & 2 & 2 & 2 \\ 0 & 1 & 1 & 2 & 4 & 3 & 0 & 2 & 2 & 4 & 3 & 1 \end{bmatrix}.$$

Consider an error pattern resulting in the syndrome $\begin{bmatrix} -2 \\ 2 \end{bmatrix}$. Solving for x [in accordance with (*iii*) above] we have

$$(-2)2^x \equiv 2 \bmod (5)$$

$$2^x \equiv -1 \bmod 5,$$

which has the solution $x = 2$. Thus we have an error in position

$$(x + 3) + (|\sigma_1| - 1)n' = (2 + 3) + (|-2| - 1)\,6 = 11$$

having the value -1.

A more interesting case arises when one desires to correct a single error of magnitude $+1$, -1, $+2$, or -2. We give a construction procedure which results in perfect codes for the case where the prime p is such that there exists a least positive integer t which satisfies the congruence

$$2^{2t} \equiv -1 \bmod p.$$

Form the multiplicative subgroup

$$1\ 2\ 4\ 8 \cdots 2^{2t} \equiv -1 \qquad 2^{2t+1} \equiv -2 \cdots 2^{4t-1}.$$

Let $a_0 = 1$, and consider the coset table:

a_0	$2a_0$	$4a_0$	$8a_0$	$\cdots$	$2^{2t}a_0 \equiv -a_0$	$a_0 2^{2t+1} \equiv -2a_0$	$\cdots$ $(2^{4t-1})a_0$
a_1	$2a_1$	$4a_1$	$8a_1$	$\cdots$	$-a_1$	$-2a_1$	$\cdots$ $(2^{4t-1})a_1$
a_2	$2a_2$	$4a_2$	$8a_2$	$\cdots$	$-a_2$	$-2a_2$	$\cdots$ $(2^{4t-1})a_2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots\ \vdots$	$\vdots$	$\vdots$	$\vdots\ \vdots$ $\vdots$
a_{l-1}	$2a_{l-1}$	$4a_{l-1}$	$8a_{l-1}$	$\cdots$	$-a_{l-1}$	$-2a_{l-1}$	$\cdots$ $(2^{4t-1})a_{l-1}$

where $4tl = p - 1$.

Now again begin with the check matrix for the lengthened Reed-Solomon single error-correcting code

$$\mathbf{H}' = \begin{bmatrix} \overleftarrow{\qquad n' = p+1 \qquad}\overrightarrow{\qquad} \\ 1 & 0 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{p-2} \end{bmatrix},$$

and form the new check matrix

$$\mathbf{H}''' = [a_0\mathbf{H}' \quad 2^2a_0\mathbf{H}' \quad 2^4a_0\mathbf{H}' \quad \cdots \quad 2^{2(t-1)}a_0\mathbf{H}' \quad a_1\mathbf{H}' \quad 2^2a_1\mathbf{H}' \quad \cdots$$
$$\cdot 2^{2(t-1)}a_1\mathbf{H}' \quad \cdots \quad a_{l-1}\mathbf{H}' \quad 2^2a_{l-1}\mathbf{H}' \quad \cdots \quad 2^{2(t-1)}a_{l-1}\mathbf{H}'].$$

The block length of this code, n''', is

$$n''' = ltn' = \frac{(p-1)}{4}n' = \frac{p^2-1}{4}.$$

In order for the code to correct all single errors of the form ± 1, ± 2, we would require $4n''' + 1 = p^2$ syndromes. Since the code has two check symbols, it has exactly p^2 syndromes available for error correction. Thus the code will be a perfect code if we can prove that its error correction capability is as asserted.

Proof: We must prove that any column of $\mathbf{H}'''$, when multiplied by $+1$, -1, $+2$, or -2, is distinct from any other column of $\mathbf{H}'''$ when multiplied by $+1$, -1, $+2$, or -2. If the two columns in question come from two distinct columns of $\mathbf{H}'$, then this is certainly the case since the columns of $\mathbf{H}'$ are linearly independent over $GF(p)$. Let the pair of columns in question be derived from the same column of $\mathbf{H}'$, say $\mathbf{h}$. One such column is of the form $2^{2(l_1)}\ a_{j_1}\mathbf{h}$ and the other is of the form $2^{2(l_2)}\ a_{j_2}\mathbf{h}$ where $(0 < l_1, l_2 \leqq t-1)$ and $(0 \leqq j_1, j_2 \leqq l-1)$. Now let z be any member of one of the cosets. Then $-z$, $+2z$, and $-2z$ are also members of that coset; so we need only consider the case $j_1 = j_2$. But

$$\begin{aligned} (1)(2^{2l_1}) &= 2^{2l_1} & (1)(2^{2l_2}) &= 2^{2l_2} \\ (2)(2^{2l_1}) &= 2^{2l_1+1} & (2)(2^{2l_2}) &= 2^{2l_2+1} \\ (-1)(2^{2l_1}) &= 2^{2(l_1+t)} & (-1)(2^{2l_2}) &= 2^{2(l_2+t)} \\ (-2)(2^{2l_1}) &= 2^{2(l_1+t)+1} & (-2)(2^{2l_2}) &= 2^{2(l_2+t)+1}, \end{aligned}$$

and no term in the left four equations can equal a term in the right four equations for $l_1 \neq l_2$, $0 \leqq l_1, l_2 \leqq t-1$. Thus the assertion is proved.

As an example, let $p = 13$ where 2 is a primitive element of order

$4t = 12$. Thus $t = 3$ and $l = 1$. The matrix $\mathbf{H}'$ can be taken as

$$\mathbf{H}' = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 4 & 8 & 3 & 6 & 12 & 11 & 9 & 5 & 10 & 7 \end{bmatrix}$$

and $\mathbf{H}'''$ is

$$\mathbf{H}''' = [\mathbf{H}' \quad 4\mathbf{H}' \quad 3\mathbf{H}'].$$

As a second example let $p = 17$. The coset table is

$$\begin{array}{cccccccccc} 1 & 2 & 4 & 8 & 16 \equiv -1 & 15 & 13 & 9 \\ 3 & 6 & 12 & 7 & 14 & 11 & 5 & 10 \end{array}.$$

The check matrix $\mathbf{H}'''$ is

$$\mathbf{H}''' = [\mathbf{H}' \quad 4\mathbf{H}' \quad 3\mathbf{H}' \quad 12\mathbf{H}'] \quad \begin{matrix} \longleftarrow 72 \longrightarrow \uparrow \\ 2 \\ \downarrow \end{matrix}$$

where $\mathbf{H}'$ is a two row by 18 column check matric formed in the manner described. Berlekamp has given a code for $p = 17$ with block length 72 with Lee distance 5 that requires four check symbols.[6] The above code requires only two check symbols but corrects only a small subset of the class of errors correctable by Berlekamp's code. Wyner has found several classes of codes which correct two errors per block, each error of the form ± 1.[8] One such class has a block length of p and requires three check symbols.

In the proof we have given a decomposition of the integers $1, 2, \cdots, p - 2, p - 1 = 4m$ into disjoint sets $S_1 S_2 \cdots S_m$ each containing four elements, such that the elements of each set are of the form x, $2x$, $-x$, and $-2x \pmod{p}$. A sufficient condition for this decomposition was that there exists a least positive integer t such that $2^{2t} \equiv -1 \pmod{p}$. The appendix shows that this condition is necessary for this decomposition.

In particular we consider the following question in the appendix: For which primes p and elements β from $GF(p)$ is it possible to partition the nonzero field elements $(1, 2, \cdots, p - 1)$ into four element subsets, S_i, such that $S_i = \{x_i, \beta x_i, -x_i - \beta x_i\} \pmod{p}$, where each nonzero field element occurs in one and only one subset? We show that the answer is: Such a partition can be achieved if and only if there exists a least positive integer t such that $\beta^{2t} \equiv -1 \pmod{p}$. Stein has considered

a more general version of this problem.[9] The results in the appendix were proved independently of Stein.

VIII. ACKNOWLEDGMENTS

The comments and suggestion of E. Berklekamp, R. Graham, J. MacWilliams, and A. Wyner are gratefully acknowledged.

APPENDIX

On a Partitioning of the Nonzero Elements of GF(p)

By R. L. Graham and J. K. Wolf

A.1 *Introduction*

The problem we consider is: For which primes, p, and elements, β, from $GF(p)$ is it possible to partition the nonzero field elements of $GF(p)$ into mutually exclusive and exhaustive four element subsets, S_i, such that

$$S_i = \{x_i, \beta x_i, -x_i, -\beta x_i\}, \pmod p?$$

A necessary condition for the existence of such a partition is that

$$\beta \neq \begin{cases} \pm 1 \\ 0 \end{cases} \mod p;$$

otherwise the subsets would not contain four distinct elements.

We will show that a necessary and sufficient condition for this partition is that there exists a t such that $\beta^{2^t} \equiv -1 \pmod p$. Further we will show that for a prime of the form $p = 8k + 5$ such a partition always exists for $\beta = 2$.

A.2 *Proof of Assertion*

First notice that a necessary condition for this partition to exist is that $p = 4m + 1$ for some $m \geqq 1$, since $p - 1$ must be divisible by four. A second necessary condition is that

$$\beta \neq \begin{cases} 1 \\ 0 \\ -1 \end{cases} \pmod p.$$

Let r be a primitive root of p so that $r^{2m} \equiv -1 \pmod p$. Define α as the smallest positive integer such that $r^\alpha \equiv \beta \pmod p$. By assumption

$\beta \not\equiv -1 \pmod{p}$, so that $\alpha \not\equiv 2m$. The subset S_i must then consist of the four elements

$$S_i = \{r^{y_i}, r^{y_i+\alpha}, r^{y_i+2m}, r^{y_i+2m+\alpha}\}$$

so that an equivalent problem is to decompose the additive group $Z_{p-1} = \{0, 1, 2, \cdots, p-2 = 4m-1\}$ into mutually exclusive and exhaustive subsets of the form $S_i' = \{y_i, y_i + \alpha, y_i + 2m, y_i + 2m + \alpha\} \bmod (4m)$].

This problem can be viewed geometrically as that of covering the vertices of a regular $4m$-gon placed on a circle by translates of the pattern $\{0, \alpha, 2m, \alpha + 2m\}$. This pattern is symmetric modulo $2m$, so the problem reduces to covering the vertices of a regular $2m$-gon placed on a circle by translates of the pattern $\{0, \alpha\}$. This pattern $\{0, \alpha\}$ can be viewed as a chord spanning α vertices. For example, for $m = 6$ and $\alpha = 5$, this covering is shown in Fig. 1 while for $m = 6$ and $\alpha = 4$, no such covering is possible.

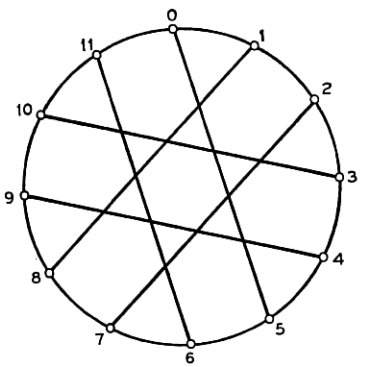

Fig. 1 — A covering for $m = 6$ and $\alpha = 5$.

In terms of sets, the problem now is to decompose the additive group Z_{2m} into m mutually exclusive and exhaustive two-element subsets, S_i'', of the form $S_i'' = \{y_i, y_i + \alpha\} \pmod{2m}$.

In the following, we denote by $[2m, \alpha]$ a covering of the $2m$-gon by chords spanning α vertices. Letting $2m = 2^\gamma(2v + 1)$ we now prove the following theorem.

Theorem 1: *A* $[2m, \alpha]$ *covering exists if and only if* $2^\gamma \nmid \alpha$. *We prove this theorem by first proving the following lemmas.*

Lemma 1: *A* $[2m, \alpha]$ *covering exists if* $*(2m, \alpha) = 1$.

* (x, y) = greatest common divisor of x and y.

Proof: Let $S_i'' = \{2(i-1)\alpha, (2i-1)\alpha\} \pmod{2m}$, $i = 1, 2, \cdots, m$. Then the subset S_i'' is of the proper form and it remains to show that each element of Z_{2m} appears in one and only one subset. Assume that an element of Z_{2m} appears in more than one subset. Then for $0 \leqq i \leqq j \leqq 2m-1$,

$$i\alpha \not\equiv j\alpha \pmod{2m}$$

or

$$(j-i)\alpha \not\equiv 0 \bmod 2m.$$

But by assumption $(2m, \alpha) = 1$ so $2m$ and α have no common factors. Thus $2m \mid (j-i)$ which is impossible since $(j-i) < 2m$. We have then shown that no element of Z_{2m} appears in more than one subset. But there are $2m$ elements in the m subsets so that each element of Z_{2m} must appear once and only once in those subsets.

The decomposition used in the proof of Lemma 1 can also be viewed as taking alternate edges of the regular star of step size α. For example, the covering in Fig. 1 can be viewed as taking alternate edges of a star of step size α. In Fig. 2, this star is shown for $m = 6$ and $\alpha = 5$ with the alternate edges as solid lines.

Lemma 2: *A* $[x, \alpha]$ *covering exists if and only if a* $[kx, k\alpha]$ *covering exists, where* $k \geqq 1$.

Proof: If a $[x, \alpha]$ covering exists, a $[kx, k\alpha]$ covering can be obtained by simply interleaving the $[x, \alpha]$ covering k times. If a $[kx, k\alpha]$ covering exists, the chords must span exactly $k\alpha$ vertices. Thus deleting all

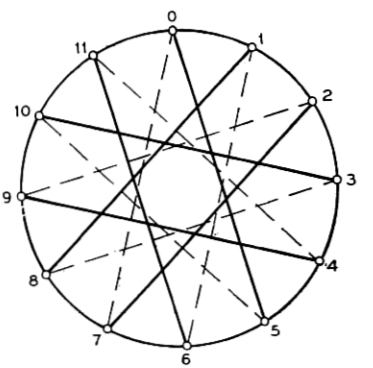

Fig. 2 — A star of step size 5 for $m = 6$.

vertices except those congruent to zero modulo k, we have a $[x, \alpha]$ covering.

Lemma 3: *A $[x, \alpha]$ covering does not exist for x odd.*

Proof: The covering problem is that of partitioning the integers $\{0, 1, \ldots, x-1\}$ into two element subsets. For this to be possible two must divide x.

Lemma 4: *Let $2m = dM$ and $\alpha = dA$, where $(A, M) = 1$. Then a $[2m, \alpha]$ covering exists if and only if M is even.*

Proof: From Lemma 2, a $[2m, \alpha] = [dM, dA]$ covering exists if and only if a $[M, A]$ covering exists. But from Lemma 3, a $[M, A]$ covering will not exist if M is odd. If M is even, since $(A, M) = 1$, Lemma 1 insures the existence of a $[M, A]$ covering.

Proof of Theorem 1: Let $2m = 2^\gamma(2v+1) = dM$ and $\alpha = dA$ where $(A, M) = 1$. If $2^\gamma \mid \alpha$, then $2^\gamma \mid d$ and M will be odd. By Lemma 4, a $[2m, \alpha]$ covering will not exist if M is odd. Conversely, assume that $2^\gamma \nmid \alpha$. Then $2 \mid M$ and M is even and by Lemma 4, a $[2m, \alpha]$ covering exists. Q.E.D.

Using Theorem 1 we now prove the main result, which is given as Theorem 2.

Theorem 2: *The nonzero elements of $GF(p)$ can be partitioned into mutually exclusive and exhaustive 4 element subsets, S_i, such that $S_i = \{x_i, \beta x_i, -x_i, -\beta x_i\} \pmod p$ if and only if there exists a positive interger t such that $\beta^{2t} \equiv -1 \pmod p$.*

Proof of Theorem 2: From Theorem 1, such a partition is possible if and only if $2^\gamma \nmid \alpha$. Let us first assume the existence of a positive integer t such that $\beta^{2t} \equiv -1 \pmod p$. But $r^\alpha \equiv \beta \pmod p$ so that $r^{\alpha 2t} \equiv -1 \pmod p$. Since $r^\delta \equiv -1 \pmod p$ implies

$$\delta = \frac{p-1}{2} + l(p-1) = (2l+1)\left(\frac{p-1}{2}\right) = (2l+1)(2m),$$

for some l, then $\alpha 2t = (2l+1)(2m) = (2l+1)(2v+1)2^\gamma$. Thus $\alpha t = 2^{\gamma-1}(2l+1)(2v+1)$ and $2^\gamma \nmid \alpha$.

Next assume that $2^\gamma \nmid \alpha$. There exists a y such that $r^{\alpha y} \equiv \beta^y \equiv -1 \pmod p$ if and only if

$$\alpha y = \left(\frac{p-1}{2}\right)(2q+1) = 2m(2q+1) = 2^\gamma(2v+1)(2q+1)$$

for some q. But $2^\gamma \nmid \alpha$, so y must have an even factor, that is $2 \mid y$. Thus y can be written as $y = 2t$ and $\beta^{2t} \equiv -1 \pmod{p}$. Further notice that the condition

$$\beta \neq \begin{cases} +1 \\ 0 \\ -1 \end{cases} \pmod{p}$$

is subsumed by the condition $\beta^{2t} \equiv -1 \pmod{p}$. Q.E.D.

A.3 *A Special Set of Primes with the Desired Partition*

Each of the two theorems in Section A.2 give a necessary and sufficient condition for the desired partition. Either condition, however, requires some calculation to discover whether p admits such a partition. The following discussion yields an easily recognizable class of primes, p, for which the partition will always be possible if $\beta = 2$.

The Legendre symbol (a/p) is defined as

$$(a/p) = \begin{cases} 1 & \text{if } x^2 = a \text{ has a solution in } GF(p) \text{ (that is, } a \text{ is a quadratic residue mod } p) \\ -1 & \text{if } x^2 = a \text{ does not have a solution in } GF(p) \text{ (that is, } a \text{ is a quadratic nonresidue mod } p) \\ 0 & \text{if } a = 0. \end{cases}$$

Lemma 5: A sufficient condition for the partition to exist is $(\beta/p) = -1$.

Proof: By Euler's criterion

$$a^{(p-1)/2} \equiv (a/p) \bmod p.$$

Since $p - 1 = 4m$, if $(\beta/p) = -1$ then $\beta^{2m} \equiv -1 \bmod p$, and the partition is possible for that β and p.

One can show (p. 172 of Ref. 6) that $(2/p) = -1$ if $p = 8k + 5$ for some k. Thus if $\beta = 2$ and the prime p is of the form $p = 8k + 5$ such a partition can be achieved.

REFERENCES

1. Bose, R. C., and Ray-Chaudhuri, D. K., "On a Class of Error Correcting Binary Group Codes," Inform. and Control, *3*, No. 1 (March 1960), pp. 68–79.
2. Bose, R. C., and Ray-Chaudhuri, D. K., "Further Results on Error Correcting Binary Group Codes," Inform. and Control, *3*, No. 3 (September 1960), pp. 279–390.
3. Hocquenghem, A., "Codes correcteurs d'erreurs," Chiffres, *2*, (September 1959), pp. 147–156.

4. Reed, I. S., and Solomon, G., "Polynomial Codes over Certain Finite Fields," J.S.I.A.M., *8*, No. 2 (June 1960), pp. 300–304.
5. Singleton, R., "Maximum Distance Q-Nary Codes," IEEE Trans. Inform. Theory, *IT-10*, No. 2 (April 1964), pp. 116–118.
6. Berlekamp, E. R., *Algebraic Coding Theory*, New York: McGraw-Hill, 1968.
7. Lee, C. Y., "Some Properties of Nonbinary Error-Correcting Codes," IRE Trans. Inform. Theory, *IT-4*, No. 2 (June 1958), pp. 77–82.
8. Wyner, A. D., unpublished work.
9. Stein, S. K., "Factoring by Subsets," Pacific J. Math., *22*, No. 3 (September 1967), pp. 523–541.