A Note on Cyclic Permutation Error-Correcting Codes

PETER G. NEUMANN

Bell Telephone Laboratories, Inc., Murray Hill, New Jersey

Error-correcting codes with \( n \) binary digits per code word are considered, in which the distances are fairly large (roughly \( n/2 \)) and the number of code words relatively small (roughly \( 2n \)). In particular, cyclic permutation codes, in which half of the code words are cyclic permutations of one another and the others are their complements, are shown to be related to difference sets. Consequently, the existence or nonexistence of certain optimal and near-optimal codes is established in terms of corresponding difference sets, for which various existence theorems and construction procedures are known. Despite the simplicity of their encoding and decoding procedures, those codes with large \( n \) seem undesirable for transmission applications (since their rate is asymptotically zero). Nevertheless, these codes seem interesting for switching circuit applications, e.g., in the design of load-sharing matrix switches.

I. INTRODUCTION

This note presents several results on the relationship between difference sets and certain error-correcting codes, each code being obtained from the cyclic permutations of one of its code words. Upon application of these results, the existence or nonexistence of various optimal and near-optimal codes is established.

There are two motivations for the codes described here. One is that simple encoders and maximum-likelihood error-correcting decoders can be designed for arbitrary cyclic permutation codes: these are discussed elsewhere (Neumann, 1962a). The second motivation is that these codes may be used in the logical design of switching circuits, e.g., load-sharing matrix switches (Takahasi and Goto, 1959; Chien, 1959, 1960; Neumann, 1962b).

An error-correcting binary code is designated by \( A(n, d; N) \), where \( N \) is the number of code words, \( n \) is the number of binary digits in each word, and \( d \) is the distance of the code, i.e., the minimum distance between code words (the distance between code words is defined as
usual as the number of respective positions in which the code words differ). If \( d = 2e + 1 \), the code is \( e \)-error correcting, while if \( d = 2e + 2 \), the code is \( e \)-error correcting and \( (e + 1) \)-error detecting. (For a comprehensive presentation of error-correcting codes, see Peterson (1961).)

A cyclic permutation code \( P'(n, d'; 2n) \) is defined as a code in which \( n \) of its code words are the cyclic permutations of one another and the other \( n \) code words are the binary complements of the first \( n \) code words. A cyclic permutation code \( P(n, d; 2n + 2) \) is obtained from \( P'(n, d'; 2n) \) by including the all-zero code word 0 and the all-one word 1. Any code word other than 0 or 1 thus generates the code by cyclic permutation and complementation. As a consequence of the relatively small number of code words (2\( n \) or 2\( n + 2 \)), the rate of transmission is asymptotically zero for large \( n \), behaving as \( (1/n) (1 + \log_2 n) \). The distances, on the
other hand, are seen to be fairly large, being of the order of \( n/2 \). If the distance \( d \) is odd, it is well known that a parity digit may be added to increase \( d \) by one; the code resulting from the addition of an even parity check digit is indicated by \( P^*(n + 1, d + 1; 2n + 2) \), \( d \) odd. As an example, a cyclic permutation code \( P(7, 3; 16) \) is given in Table I. (It is in fact the well-known Hamming code in disguise.) The corresponding code \( P^*(8, 4; 16) \) is also indicated. This example is considered in detail at the end of Section II.

There are four cases which are considered here, namely \( n = 4m - 1 \), \( 4m \), \( 4m + 1 \), and \( 4m + 2 \). Given \( n = 4m - 1 \) and \( N = 8m \), the code distance in any code \( A(4m - 1, d; 8m) \) can be at most \( 2m - 1 \). A code \( P(4m - 1, 2m - 1; 8m) \), if it exists, is then optimal in the sense that no other code \( A(4m - 1, 2m - 1; N) \) with this \( n \) and \( d \) can contain more than \( N = 8m \) code words (Plotkin, 1960). Bose and Shrikhande (1959) have shown that codes \( A(4m - 1, 2m - 1; 8m) \) and \( A(4m, 2m; 8m) \) exist if and only if a Hadamard matrix \( H_{4m} \) exists, or equivalently, if and only if a certain symmetrical balanced block design exists (see below). No \( m \) is known for which a Hadamard matrix \( H_{4m} \) cannot exist, although no such matrices have been found for certain cases, e.g., \( m = 29 \) and 39. Whereas codes \( A(4m - 1, 2m - 1; 8m) \) thus exist for possibly all \( m \), codes \( P(4m - 1, 2m - 1; 8m) \) exist for many \( m \), but not, for example, for \( m = 7, 10, 13, 14 \). The existence of these codes is discussed in Section III.

If \( n = 4m + 1 \) and \( N = 8m + 4 \), then the distance \( d \) of an arbitrary code can be at most \( 2m \). However, whereas codes

\[
P(4m - 1, 2m - 1; 8m)
\]

exist for many values of \( m \), it is seen that no codes

\[
P(4m + 1, 2m; 8m + 4)
\]

exist. It is seen below, that codes \( P'(4m + 1, 2m; 8m + 2) \) do occasionally exist; for example, those for \( n = 5 \) and 13 are the only ones for \( n \leq 220 \), although they are not optimal. The existence of such codes is considered in Section IV. Codes \( P(4m + 1, 2m - 1; 8m + 4) \) are also mentioned, although they too are not optimal.

If \( n = 4m \) and \( N = 8m + 2 \), then \( d \) can be at most \( 2m - 1 \), although a code \( P(4m, 2m - 1; 8m + 2) \) apparently exists only for \( m = 1 \). An optimal code \( P'(4m, 2m; 8m) \) exists at least for \( m = 1 \), although as mentioned above there are many codes \( P^*(4m, 2m; 8m) \). The existence of the codes \( P' \) is also discussed in Section IV.
If \( n = 4m + 2, N = 8m + 6 \) then the code distance \( d \) can be at most \( 2m \). Codes \( P(4m + 2, 2m; 8m + 6) \) exist for most (if not all) \( m \); they are however far from optimal, and are not considered here.

II. DIFFERENCE SETS

In order to provide a mathematical basis for certain cyclic permutation codes, it is now desirable to introduce the notion of a difference set. It is seen that each difference set leads to a cyclic permutation code, and that the converse holds in several interesting cases.

A \((v, k, \lambda)\) difference set \( D_0 : d_1, d_2, \ldots, d_k \pmod{v} \) is a set of \( k \) distinct integers such that among the differences \( d_a - d_b \pmod{v} \) each integer \( 1, 2, \ldots, v - 1 \) occurs exactly \( \lambda \) times. It follows that each set \( D_i : d_1 + i, d_2 + i, \ldots, d_k + i \pmod{v} \) is a difference set with the same \( v, k \) and \( \lambda, i = 0, 1, 2, \ldots, v - 1 \). The corresponding cyclic incidence matrix \( A = [a_{ij}] \) has elements \( a_{ij} = 1 \) if the integer \( j \) is in the \( i \)th difference set \( d_1 + i, d_2 + i, \ldots, d_k + i \pmod{v} \), \( i, j = 0, \ldots, v - 1 \), and \( a_{ij} = 0 \) otherwise.

The complement of a difference set \((v, k, \lambda)\) is the set of integers \((\text{mod } v)\) which do not occur in the original difference set. The complement is seen to be a difference set \((v, v - k, v - 2\lambda + \lambda)\). The corresponding incidence matrix is the complement of the original incidence matrix, obtained by interchanging 0 and 1.

**Lemma 1.** Given the \((v, k, \lambda)\) difference sets \( D_i : d_1 + i, d_2 + i, \ldots, d_k + i \pmod{v}, i = 0, 1, \ldots, v - 1 \), each row in the cyclic incidence matrix \( A = \| a_{ij} \| \) is distance \( 2k - 2\lambda \) from every other row. The same result holds for the complementary incidence matrix \( \tilde{A} \).

**Proof:** A difference \( l = d_a - d_b \pmod{v} \) in \( D_0 \) corresponds to a coincidence of ones in the \( d_a \) column of the rows in the incidence matrix for \( D_0 \) and \( D_1 \), since \( d_a = l + d_b \pmod{v} \) is in \( D_0 \) and in \( D_1 \). Since each difference \( l \) occurs \( \lambda \) times in \( D_0 \), such a coincidence of ones between \( D_0 \) and each \( D_i \) occurs exactly \( \lambda \) times. Thus, since exactly \( k \) of the \( a_{ij} \) are one for each \( i \), the remaining \( k - \lambda \) ones among the \( a_{ij}(a_{0j}) \) for that \( i \)

---

1 For a survey of difference sets and a listing of all those for \( 3 \leq k \leq 50, k < v/2 \), see Hall (1956).

2 The incidence matrix is also the incidence matrix of a cyclic symmetrical \((v, k, \lambda)\) block design (Hall and Ryser, 1951) in which \( v \) elements are found among \( v \) sets of \( k \) elements each, such that each element occurs in \( k \) different sets and each pair of elements occurs in \( \lambda \) different sets. It follows that each set has exactly \( \lambda \) elements in common with any other set. Necessarily, \( \lambda(v - 1) = k(k - 1) \) must be satisfied, and hence \( \lambda \) is computable from \( v \) and \( k \) as \( k(k - 1)/(v - 1) \). It also follows that each two sets have exactly \( \lambda \) elements in common.
which do not coincide with ones in the $a_{ij}(a_{ij})$ must find $a_{ij} = 1$ ($a_{ij} = 1$). Hence any two rows in the incidence matrix differ in exactly $2k - 2\lambda$ positions, i.e., they are distance $2k - 2\lambda$ apart. The same result must therefore hold for the complementary incidence matrix, since distances are invariant under complementation.

**Lemma 2.** Each row in $A$ is distance $v - (2k - 2\lambda)$ from any row in $\bar{A}$ other than its own complement, from which it is distance $v$.

**Proof:** Any row is obviously distance $v$ from its complement. Lemma 2 therefore follows from Lemma 1.

Each row of the incidence matrix or of its complement is now interpreted as a code word $a_i = a_i^0 a_i^1 \cdots a_i^{v-1}$, where for convenience $a_i^j = a_{ij}$. The distance of the resulting code follows from Lemmas 1 and 2 and is given by the following theorem.

**Theorem 1.** Given a $(v, k, \lambda)$ difference set, the distance $d'$ of the corresponding code $P'(v, d'; 2v)$ is the smaller of $2k - 2\lambda$ and $v - 2k + 2\lambda$.

The distance $d$ of the code $P(v, d; 2v + 2)$ is the smallest of $\lceil \lambda \rceil, v - k, 2k - 2\lambda$ and $v - 2k + 2\lambda$.

As an example, consider the difference set $0, 1, 2, 4$ (mod $7$) with $v = 7, k = 4, \lambda = 2$. Each difference occurs twice ($1 - 0 = 2 - 1 = 1, 2 - 0 = 4 - 2 = 2$, etc.). The corresponding cyclic incidence matrix for the difference sets $i, 1 + i, 2 + i, 4 + i$ (mod $7$), $i = 0, 1, \cdots, 6$, is the $7 \times 7$ matrix in the upper lefthand corner of Table I, and has distance $2k - 2\lambda = 4$. Since $v - 2k + 2\lambda = 3$, the code word $a_0 = 1101001$ corresponding to the difference set $0, 1, 2, 4$ (mod $7$) thus generates the code $P(7, 3; 16)$ of Table I.

Similarly, the complementary difference set $3, 5, 6$ (mod $7$) with $v = 7, k = 3, \lambda = 1$ generates the same code; the corresponding code word $00010111$ is $a_0$. Furthermore, since the reversal of any difference set, i.e., the set $v - d_1, v - d_2, \cdots, v - d_6$ (mod $v$), is also a difference set with the same $(v, k, \lambda)$, the code word $0010111$ or $1101000$ may be used to generate a code $P(7, 3; 16)$ which is the reversal of that in Table I, i.e., with the digits with $j = 0, 1, \cdots, 6$ considered in the reverse order.

### III. CYCLIC PERMUTATION CODES $P(4m - 1, 2m - 1; 8m)$

There are various classes of cyclic permutation codes

$$P(4m - 1, 2m - 1; 8m)$$

cited in the literature (Plotkin, 1960; Golomb, 1955) or derivable from known results (Brauer, 1953; Hall, 1956). However, the following
Theorem shows that the code words in each such code correspond to difference sets, and hence that the codes may be obtained by exhausting the difference sets.

**Lemma 3.** Given a \( v \) by \( v \) cyclic incidence matrix in which each row (with \( k \) ones) is distance \( 2\mu \) from every other row, any row corresponds to a difference set \( (v, k, k - \mu) \).

**Proof:** This is the converse of Lemma 1. If any two rows of the cyclic incidence matrix differ in exactly \( 2\mu \) positions, they must both have ones in \( (2k - 2\mu)/2 = k - \mu \) positions. Hence each difference \( l = d_\alpha - d_\beta \) in the set of integers for which \( a_\alpha \) is one occurs \( k - \mu \) times, and the set is a difference set \( (v, k, k - \mu) \). Note that \( \mu \) must be \( \lfloor v(v - k)/(v - 1) \rfloor \).

**Theorem 2.** A code word other than 0 and 1 in any code \( P(4m - 1, 2m - 1; 8m) \) corresponds to a difference set \( (4m - 1, 2m, m) \) or its complement \( (4m - 1, 2m - 1, m - 1) \).

**Proof:** Since 0 and 1 are in the code, there are \( 4m - 1 \) code words \( a_\alpha \), with \( 2m \) ones, and \( 4m - 1 \) complementary code words \( \bar{a}_\beta \), with \( 2m - 1 \) ones. The distance between any two \( a_\alpha \), as is the distance between any two \( \bar{a}_\beta \). Suppose that the distance between \( a_\alpha \) and \( a_\beta \) is \( 2m + 2\epsilon \), for some nonnegative integer \( \epsilon \); then the distance between \( a_\alpha \) and \( \bar{a}_\beta \) must be \( 4m - 1 - 2m - 2\epsilon = 2m - 1 - 2\epsilon \). It follows that \( \epsilon \) must be zero, and hence all code words \( a_\alpha \) are exactly distance \( 2m \) from one another. Therefore Lemma 3 applies, and each code word corresponds to a difference set \( (4m - 1, 2m, m) \) or \( (4m - 1, 2m - 1, m - 1) \), depending on whether it has \( 2m \) or \( 2m - 1 \) ones. (Note incidentally that the code words 0 and 1 correspond to difference sets \( (4m - 1, 0, 0) \) and \( (4m - 1, 4m - 1, 4m - 1) \), respectively.) Conversely, given either difference set, with \( k = 2m \) or \( k = 2m - 1 \), it follows that \( 2k - 2\lambda \) is \( 2m \) in either case. The smallest of \( 2k - 2\lambda \), \( v - 2k + 2\lambda \), \( k \) and \( v - k \) is therefore \( 2m - 1 \), which by Theorem 1 is the distance of the code.

A summary of known results which lead to cyclic permutation codes \( P(4m - 1, 2m - 1; 8m) \) is provided in Table II. \( Q \) in the table denotes the existence of a quadratic residue code (Plotkin, 1960) arising from the difference set \( (4m - 1, 2m - 1, m - 1) \) of quadratic residues of any prime \( 4m - 1 \). The names of Hopf, Schur, Gilman, Coxeter, Todd and Paley, all referred to in Brauer (1953), are connected with independent observations of the corresponding Hadamard matrix, the first two dating
TABLE II

VARIOUS CYCLIC PERMUTATION CODES $P(4m - 1, 2m - 1; 8m)$

<table>
<thead>
<tr>
<th>$m$</th>
<th>$n = 4m - 1$</th>
<th>$d = 2m - 1$</th>
<th>$N_q$</th>
<th>$N = 8m$</th>
<th>Cyclic permutation codes $P(n, d; N)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>1</td>
<td>8</td>
<td>8</td>
<td>$Q \leftrightarrow R \leftrightarrow T$</td>
</tr>
<tr>
<td>2</td>
<td>7</td>
<td>3</td>
<td>16</td>
<td>16</td>
<td>$Q \leftrightarrow R$</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>5</td>
<td>16</td>
<td>24</td>
<td>$Q$</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>7</td>
<td>32</td>
<td>32</td>
<td>$R \leftrightarrow T$</td>
</tr>
<tr>
<td>5</td>
<td>19</td>
<td>9</td>
<td>32</td>
<td>40</td>
<td>$Q$</td>
</tr>
<tr>
<td>6</td>
<td>23</td>
<td>11</td>
<td>32</td>
<td>48</td>
<td>$Q$</td>
</tr>
<tr>
<td>7</td>
<td>27</td>
<td>13</td>
<td>32</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>31</td>
<td>15</td>
<td>64</td>
<td>64</td>
<td>$Q \ast R \leftrightarrow S$</td>
</tr>
<tr>
<td>9</td>
<td>35</td>
<td>17</td>
<td>64</td>
<td>72</td>
<td>$T$</td>
</tr>
<tr>
<td>10</td>
<td>39</td>
<td>19</td>
<td>64</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>43</td>
<td>21</td>
<td>64</td>
<td>88</td>
<td>$Q \ast S$</td>
</tr>
<tr>
<td>12</td>
<td>47</td>
<td>23</td>
<td>64</td>
<td>96</td>
<td>$Q$</td>
</tr>
<tr>
<td>13</td>
<td>51</td>
<td>25</td>
<td>64</td>
<td>104</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>55</td>
<td>27</td>
<td>64</td>
<td>112</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>59</td>
<td>29</td>
<td>64</td>
<td>120</td>
<td>$Q$</td>
</tr>
<tr>
<td>16</td>
<td>63</td>
<td>31</td>
<td>128</td>
<td>128</td>
<td>$R \ast U$</td>
</tr>
<tr>
<td>32</td>
<td>127</td>
<td>63</td>
<td>256</td>
<td>256</td>
<td>$Q \ast R \leftrightarrow S$</td>
</tr>
<tr>
<td>64</td>
<td>255</td>
<td>127</td>
<td>512</td>
<td>512</td>
<td>$R (\ast U?)$</td>
</tr>
</tbody>
</table>

$N_q$ is given for the corresponding best group code $B(n, d; N_q)$. $Q$ denotes a quadratic residue code, $R$ denotes a recursive code, $S$ denotes a sextic residue code, $T$ denotes a twin-prime code, and $U$ denotes another code. An asterisk indicates the existence of nonisomorphic codes, while an arrow indicates an isomorphism.

back to 1920. Only the first two such codes ($m = 3, 7$) are group ("linear") codes. As an example, the quadratic residues of 7 form the difference set $1, 2, 4$ (mod 7), which leads to the reversal of the code of Table I; similarly the quadratic residues of 7 and zero form the difference set $0, 1, 2, 4$ (mod 7), which leads to the code of Table I.

$R$ denotes the existence of a recursive code arising from the difference set corresponding to the maximal sequence of any primitive irreducible polynomial of degree $r$ over $GF(2)$ (Golomb, 1955; Green and San Soucie, 1958). A recursive code $P(2^r - 1, 2^{r-1} - 1; 2^{r+1})$ exists for each $r \geq 2$ ($m = 2^{r-2}$), each one being a group code. The codes for $m = 1$ and 2 ($r = 2$ and 3) are isomorphic to the above-mentioned corresponding quadratic residue codes. As an example, the polynomial equation

---

3 These difference sets correspond to hyperplanes of finite Desarguesian projective geometries (Hall, 1956).
\[ x^3 + x^2 + 1 = 0 \] for \( r = 3 \) corresponds to the maximal sequence \( 1110100 \) (i.e., \( a_0^3 + a_0^2 + a_0^0 \equiv 0 \pmod{2} \), etc.), to the difference set \( 0, 1, 2, 4 \pmod{7} \), and hence to the code of Table I.

Incidentally, successive multiplication of a difference set may be used to exhaust all primitive irreducible polynomials of any degree \( r \), given any one. For \( r = 5 \), for example, there are six such polynomials (in general, there are \( \varphi(2^r - 1)/r \) such polynomials of degree \( r \), where \( \varphi(n) \) is Euler's Phi-function; Zierler, 1955). The difference set \( (31, 16, 8) \)
\[ D_a : 0, 1, 2, 3, 4, 6, 7, 8, 12, 14, 16, 17, 19, 24, 25, 28 \pmod{31} \]

corresponds to the polynomial \( x^5 + x^4 + x^3 + x^2 + 1 \). Multiplication of each element of \( D_a \) by \( 3 \pmod{31} \) yields the difference set \( D_b \) corresponding to \( x^5 + x^4 + x^2 + 1 \), and another multiplication by 3 yields \( D_c \) corresponding to \( x^5 + x^4 + x^2 + x + 1 \). Subsequent multiplication by 3 cycles through the reversals of these three difference sets and hence yields the three remaining primitive irreducible polynomials of degree 5 (i.e., \( x^5 + x^3 + x^2 + x + 1 \), etc.).

For arbitrary \( r \), multiplication by some suitable integer often gives all \( \varphi(2^r - 1)/r \) polynomials (e.g., when \( 2^r - 1 \) is a prime, and when \( 2^r - 1 = 15 \) or 63), but otherwise always seems to give half of them, the other half being obtained by reversal. (Notice that no primitive irreducible polynomial can be its own reversal whenever \( r > 2 \).) For \( r = 5 \), a transformation \( x \rightarrow x^8 \) can also be performed directly upon the polynomials. Thus \( x^4 + x^3 + x^2 + 1 \) becomes \( x^{15} + x^{12} + x^9 + x^6 + 1 \), whose irreducible factorization is \( (x^5 + x^2 + 1)(x^{10} + x^5 + x^4 + x^2 + 1) \). The first factor is the desired polynomial. In general, however, this transformation and reduction of the polynomials seems harder to evaluate than the difference set approach.

\( S \) in Table II denotes a sextic residue code arising from the sextic residue difference sets of Hall (1956), occurring for primes \( n = v = 4t^2 + 27 \). These codes add no new values of \( 4m - 1 \), but are apparently distinct from the quadratic residue codes for the same \( n \); they are also apparently isomorphic to recursive codes whenever \( n = 2^r - 1 \).

\( T \) denotes a twin-prime code arising from difference sets for which \( v = pq = p(p + 2) \), where \( p \) and \( q = p + 2 \) are twin primes (Brauer, 1953). They may be constructed from the quadratic residues of the

---

1 Any \( 2r \) consecutive digits in the (maximal) sequence corresponding to the difference set \( (4m - 1, 2m, m) \) may be used to determine the polynomial. The determination is simplest when the occurrence of \( r - 1 \) successive zeros is used as a starting point; each successive digit in either direction then determines the presence or absence of one term of the polynomial.
individual primes. Incidentally, Stanton and Sprott (1958) have shown
the existence of difference sets over ordered pairs whenever \( v = p^a q^b \)
with \( q^b = p^a + 2 \) (twin prime powers). However, whenever \( a \) or \( b \) is
greater than one, elements of the Galois field \( GF(p^a) \) or \( GF(q^b) \) are
involved, which prevent a difference-preserving one-dimensionalization of
the resulting difference set. Consequently a cyclic incidence matrix and
corresponding code do not arise, although a noncyclic matrix may be
constructed.

\( U \) in Table II denotes the nongroup code arising from a difference set
\((63, 31, 15)\) given by Hall (1956) which he notes is distinct from the
projective geometry. Other nongroup codes may also exist for additional
nonprimes \( 2^r - 1 \), e.g., 255.

In addition to showing the existence of various codes \( Q, R, S, T, \) and
\( U \), Table II shows which codes are isomorphic (\( \leftrightarrow \)) and which are not
(\( * \)).

The above cases of cyclic permutation codes \( P(4m - 1, 2m - 1; 8m) \)
are the only ones known to the author. A study by Hall (1956) shows
no other cases for \( 4m \leq 100 \). Application of Theorem 2.1 of Hall (1956)
together with the concept of a multiplier of the difference set and of a
necessary condition of Chowla and Ryser (see Hall, 1956) shows no
other cases for \( 4m \leq 120 \). This theorem and the necessary condition
may be used to exhaust all cyclic permutation codes

\[ P(4m - 1, 2m - 1; 8m), \]

by virtue of the author's Theorem 2. Similarly each difference set
\((4m - 1, 2m, m)\) may be used to construct an optimal code

\[ P_i(4m - 1, 2m; 4m) \]

from the cyclic permutations of \( a_0 \) and the all-zero code word 0.

IV. OTHER CYCLIC PERMUTATION CODES

**Theorem 3.** A code word in any code \( P'(4m + 1, 2m; 8m + 2) \) corre-
sponds to a difference set with \( v = \binom{l + 1}{2} + 1 = 4m + 1 \), \( k = l^2 \),
\( \lambda = \binom{l}{2} \), or its complement with \( k = (l + 1)^2 \), \( \lambda = \binom{l + 2}{2} \).
That is, such a code exists only if \( m = \binom{l + 1}{2} \).

**Proof:** There are \( 4m + 1 \) code words \( a \), containing \( k \) ones, the dis-
tance between each two of which must be at least \( 2m \); this is also the
case for the complementary code words $\bar{a}_i$ with $4m + 1 - k$ ones. Suppose that the distance between $a_\alpha$ and $a_\beta$ is $2m + 2\epsilon$; then the distance between $a_\alpha$ and $\bar{a}_\beta$ is $4m + 1 - 2m - 2\epsilon = 2m + 1 - 2\epsilon$. Hence $\epsilon$ must be zero, and all of the code words $a_\alpha$ must be distance $2m$ apart. By Lemma 3, each code word $a_\alpha$ corresponds to a difference set $(4m + 1, k, k - m)$, while its complement $\bar{a}_i$ with $4m + 1 - k$ ones corresponds to the complementary difference set $(4m + 1, v - k, v - k - m)$.

It remains to determine what $k$ must be. By Lemma 1 it is required that $2k - 2\lambda = 2m$. Applying the relation $\lambda = k(k - 1)/(v - 1)$, it follows that $k - m = k(k - 1)/4m$ must be satisfied, or equivalently $k^2 - (4m + 1)k + 4m^2 = 0$. The roots $k = \frac{1}{2} (4m + 1 \pm \sqrt{8m + 1})$ of this equation must be integral, which implies that $8m + 1$ must be the square $(2l + 1)^2$ of some odd integer. It follows that

$$v = 4m + 1 = 2l^2 + 2l + 1 = 4 \binom{l + 1}{2} + 1,$$

whence

$$m = \binom{l + 1}{2}.$$

The two solutions for $k$ yield

$$k = l^2, \quad \lambda = \frac{(l^2 - l)}{2} = \binom{l}{2},$$

and

$$k = (l + 1)^2, \quad \lambda = \frac{(l^2 + 3l + 2)}{2} = \binom{l + 2}{2}.$$

For $l = 1$ and $l = 2$, difference sets and codes of the form of Theorem 3 do exist: for $l = 1$, a difference set $(v, k, \lambda) = (5, 1, 0)$ leads to the code $P'(5, 2; 10)$; for $l = 2$, the difference set $0, 1, 3, 9 \pmod{13}$ with $(v, k, \lambda) = (13, 4, 1)$ leads to the code $P'(13, 6; 26)$. The former code has a value of $N$ six less than the optimal code $A(5, 2; 16)$, while the latter has a value of $N$ six less than the best known code $A(13, 6; 32)$, constructed by Stevens and Bouricius (1959). For $l = 3, 4, 5, 6, 7$, and hence $4m + 1 < 145$, the results of Hall (1956) show that no such difference sets, e.g., $(25, 9, 3), (41, 16, 6)$, etc., can exist, and hence no code $P'(4m + 1, 2m; 8m + 2)$ can exist for the corresponding $m = \ldots$
6, 10, 15, 21, 28. For \( l = 8, 9 \), and hence \( 4m + 1 < 221 \), the author has shown that no such difference sets can exist. The codes in this particular class are therefore considerably rarer than those of the previous section.

**Theorem 4.** A code word in any code \( P'(4m, 2m; 8m) \) corresponds to a difference set with \( v = 4l^2, k = \binom{2l}{2}, \lambda = 2\binom{l}{2} \), or its complement. That is, such a code exists only if \( m = l^2 \).

**Proof:** The proof is similar to that of Theorem 3, the difference set being of the form \((4m, k, k - m)\). By Lemma 1, it follows that \( k - m = k(k - 1)/4m - 1 \) must be satisfied, whence \( k = 2m \pm \sqrt{m} \) must be integral, i.e., \( m = l^2 \).

Such a code \( P'(4, 2; 8) \) exists for \( m = l^2 = 1 \), but not for \( l = 2, 3, 4, 5 \). The author has not investigated the cases for \( l \geq 6 \), that for \( l = 6 \) being whether a difference set \((144, 66, 30)\) and a code \( P'(144, 72; 288) \) exist. Note that all cases satisfy a necessary existence condition of Chowla and Ryser (see Hall, 1956), namely, that \( k - \lambda = \lambda^2 \) be a square when \( v \) is even. All such codes are of course optimal.

For completeness, it might be added that if each code word in a code \( P'(4m + 2, 2m; 8m + 4) \) is to correspond to a difference set, similar analysis shows that \( 3m + 1 \) must be a square. If in addition the necessary condition of Chowla and Ryser is applied, it is seen that \( m \) must be the square of a binomial coefficient \( \binom{2l + 2}{l} \). The first few cases to be considered are thus as follows: \( l = 0, m = 1 \), for which a difference set \((6, 1, 0)\) exists, but results in the bad code \( P'(6, 2; 12) \); \( l = 1, m = 16 \), for which a difference set \((66, 26, 10)\) does not exist (by the results of Hall, 1956); \( l = 2, m = 225 \) and \( l = 3, m = 3136 \), which have not been investigated.

From Theorem 1 it is also possible to consider arbitrary difference sets and their resulting codes. The codes are in some cases nearly optimal. The difference set \((40, 13, 4)\), for example, leads to a code \( P'(40, 18; 80) \).

It is also possible to use cyclic incidence matrices which do not correspond to difference sets (and cyclic balanced block designs). Consider, for example, the quadratic residues of 13, \( Q_0 : 1, 3, 4, 9, 10, 12 \) \((v = 13, k = 6)\). Of the differences \( l = d_\alpha - d_\beta \), six \((l \in Q_0)\) occur two times each, and the remaining six \((l \in Q_0)\) occur three times each. In the corresponding cyclic incidence matrix, which corresponds to a partially balanced block design (Bose and Shimamoto, 1952), each row is distance
8( = 2k - 2\lambda_1 = 12 - 4) from each of six rows, and distance
6( = 2k - 2\lambda_2 = 12 - 6)
from each of the six others. Hence the minimum distance between one row of the matrix and a row of its complement is
5( = v - 2k + 2\lambda_{\text{min}} = 13 - 8),
and the code $P'(13, 5; 26)$ results. In fact, the all-zero and the all-one code words may be added without reducing the distance, yielding a code $P(13, 5; 28)$. This code is far from optimal, however, since there exists a code $A(13, 5; 64)$ (Stevens and Boucicou, 1959). In general, the quadratic residues of any prime $4m + 1$ lead to a cyclic permutation code $P(4m + 1, 2m - 1; 8m + 4)$ (Chien, 1959), although these codes are not optimal. Other similar codes are also not optimal. For $4m + 1 = 9$, for example, a code $P(9, 3; 20)$ results from the set of integers 0, 1, 2, 4 (mod 9), whose cyclic incidence matrix corresponds to a partially balanced block design (9, 4, "1½"). It is noted, however, that this code is optimal neither in $N$ nor in $d$, since codes $A(9, 3; 38)$ and $A(9, 4; 20)$ (due to Golay) exist. Note incidentally that a code $P(9, 4; 20)$ cannot exist, by virtue of Theorem 3, although a code $p(9, 4; 19)$ can be constructed (Stevens and Boucicou, 1959) by cyclically permuting 111010000 and 111100110, and adding 000000000.

V. RELATED CODES

In conclusion, it should be noted that the results of Theorems 1, 3, and 4 may be extended to arbitrary (noncyclic) symmetrical block designs having the desired $v$, $k$, and $\lambda$ (see for example, Connor, 1952); however the extensions are not nearly so powerful as Bose and Shrikhande's above-mentioned Theorem 1, showing the coexistence of $A(4m - 1, 2m - 1; 8m)$ and $A(4m, 2m; 8m)$, block designs, and Hadamard matrices.

Given any symmetrical block design $(v, k, \lambda)$, a code $D'(v, d'; 2v)$ may be obtained by taking the rows of the incidence matrix and of its complement as code words. As in Theorem 1, the distance $d'$ is the smaller of $2k - 2\lambda$ and $v - 2k + 2\lambda$.

Note that the formula $\lambda = k(k - 1)/(v - 1)$ results in $\lambda = 2\frac{1}{2}$, which, although it is not an integer, is indicative of the nature of the set. The corresponding cyclic block design is known as a symmetrical partially balanced block design with two associate classes.
With respect to codes $A(4m + 1, 2m; 8m + 2)$, Theorem 3 leads to the generalization that the only symmetrical block designs with $v = 4m + 1$ which may lead to such codes containing the complement of each code word are those with

$$v = 4 \left(\frac{l + 1}{2}\right) + 1, \quad k = l^2, \quad \lambda = \binom{l}{2},$$

or their complements. For $l = 3$, for example, a noncyclic design $(25, 9, 3)$ exists (due to Bhattacharya; see Connor, 1952) and leads to a code $D'(25, 12; 50)$, with the rows of the incidence matrix and their complements as the code words. Note, however, that there is no result analogous to Bose and Shrikhande's: although a code $A(9, 4; 18)$ exists, there is no corresponding symmetric block design $(9, k, \lambda)$.

With respect to codes $A(4m, 2m; 8m)$, Theorem 4 implies that the only symmetrical block designs with $v = 4m$ which may lead to codes $D'(4m, 2m; 8m)$ containing the complement of each code word are those with

$$v = 4l^2, \quad k = \binom{2l}{2}, \quad \lambda = 2 \binom{l}{2},$$

or their complements. For $l = 2$, for example, a noncyclic design $(16, 6, 2)$ exists and leads to a code $A(16, 8; 32)$ in which each code word has either 6 or 10 ones. Of course many other codes $A(4m, 2m; 8m)$ can be derived from Hadamard block designs with $v = 4m - 1$ by including the code words 0 and 1, and adding a parity digit.

VI. CONCLUSIONS

The author has discussed elsewhere simple encoders and decoders for cyclic permutation codes, operating on a maximum-likelihood principle rather than a parity-check basis (Neumann, 1962a). Their simplicity may serve to increase the utility of the optimal as well as the near-optimal cyclic permutation codes for moderate values of $n$. In addition, Green and San Soucie (1958) have discussed a parity-check encoder and decoder which are applicable for all of the recursive codes.

Although cyclic permutation codes are considered here in terms of transmission systems, they seem to have significant applications in the design of load-sharing matrix switches (Chien, 1960; Neumann, 1962b). In these applications the distance properties are so utilized that with only small excitations on the input drivers one output wire can be
selected while the net excitation on all others is effectively zero; the dis-
tance of the code permits a certain amount of variation in the driving
excitations. In terms of such an application, the cyclic permutation
structure should lend itself to ease of construction, inspection and
maintenance of the matrix switch.

Acknowledgment

The author wishes to thank T. H. Crowley and B. A. Tague for several stimu-
lating conversations and useful suggestions. He is also indebted to J. D. Rutledge
of IBM, who pointed out the work of Stevens and Bouricius (1959), reference to
which has been added to this paper.

Received: September 20, 1961

References

Bose, R. C., and Shimamoto, T., (1952), Classification and analysis of partially
balanced incomplete block designs with two associate classes. J. Am. Statist.
Assoc. 47, 151–184.

Bose, R. C., and Shrikhande, S. S., (1959), A note on a result in the theory of

225.

Chien, R. T., (1959), Orthogonal matrices, error-correcting codes and load-
sharing matrix switches, (Letter). IRE Trans. on Electronic Computers EC-8,
400.

Chien, R. T., (1960), A class of optimal noiseless load-sharing matrix switches

Connor, W. S., Jr., (1952), On the structure of balanced incomplete block designs.

Golomb, S. W., (1955), Sequences with randomness properties. Glenn L. Martin
Co., Final Report on Contract No. W36-039SC-54-36611, Baltimore, Mary-
land.

Green, J. H., Jr., and San Soucie, R. L., (1958), An error-correcting encoder and


495–502.

Neumann, P. G., (1962a), Encoding and decoding for cyclic permutation codes.
(To be published.)

Neumann, P. G., (1962b), On the logical design of noiseless load-sharing matrix
switches. Presented at the Princeton University Conference on Logical De-
sign Theory and Switching Circuits, Jan. 4, 1962. (To be published.)

Peterson, W. W., (1961), "Error-Correcting Codes." M.I.T. Press and Wiley,
New York.

Plotkin, M., (1960), Binary codes with specified minimum distance. IRE Trans.


