$$\max_{0\le t<s} W_{a^s}(hq^t) < (\mu+1)b + r_j. \tag{26}$$

To finish the proof, we examine the largest value of $\tilde{D}^{(t)}$ (max) such that $h < h_0$. This is given by $(\gamma, \gamma, \cdots, \gamma, q-\sigma_j-1)$. But this equals $B - q^j$ because [1] shows that $B = (\gamma, \gamma, \cdots, \gamma, q-\sigma_j, 0, \cdots, 0)$; hence,

$$\begin{aligned}\tilde{D}^{(t)}(\max) &= B - q^j \\ &= (\mu+1)b - (q^j - r_j).\end{aligned} \tag{27}$$

By (4), $(q^j - r_j)$ is positive. Therefore

$$\tilde{D}^{(t)}(\max) < (\mu+1)b. \tag{28}$$

Q.E.D.

Lemmas 1, 2, and 3 establish Theorem 9A.

Theorem 9A: For h_0 given by (9) when $Q_0 = 0$,

$$\max_{0\le t<s} W_{a^s}(h_0 q^t) = (\mu+1)b + r_j.$$

Further, for any $h < h_0$ and divisible by b,

$$\max_{0\le t<s} W_{a^s}(hq^t) < (\mu+1)b.$$

A. Brinton Cooper, III
Army Materiel Sys. Anal. Agency
Aberdeen Proving Ground, Md. 21005
Willis C. Gore
Johns Hopkins University
Baltimore, Md. 21218

Reference

[1] C. L. Chen and S. Lin, "Further results on polynomial codes," *Inform. and Control*, vol. 15, pp. 38–60, 1969.

The Equivalence of Rank Permutation Codes to a New Class of Binary Codes

***Abstract*—An equivalence between the rank permutation codes and a new class of binary codes has been observed. A binary code may be generated by direct transformation of a permutation code. The binary codes are usually nonlinear and may be decoded by the inverse transformation and rank correlation of the equivalent permutation.**

The codewords of a rank permutation code[1] are each one of the permutations of the n digits $(1, 2, \cdots, n)$. A permutation code is a subgroup of the $n!$ permutations in the symmetric permutation group, S_n. It was shown[1] that when suitable weight and distance measurements are used, permutation codes have many of the characteristics of binary codes. It is shown here that this similarity of behavior may be explained by the fact that each permutation code is equivalent to a binary code and that the weight and distance of the permutation codewords are the Hamming weight and distance of the equivalent binary codewords. Thus, there is a class of binary codes that may be generated by the use of permutation codes.

TABLE I

Permutation	m_{12}	m_{13}	m_{14}	m_{23}	m_{24}	m_{34}	Weight
1234	0	0	0	0	0	0	0
1243	0	0	0	0	0	1	1
1324	0	0	0	1	0	0	1
1342	0	0	0	0	1	1	2
1423	0	0	0	1	1	0	2
1432	0	0	0	1	1	1	3
2134	1	0	0	0	0	0	1
2143	1	0	0	0	0	1	2
2314	0	1	0	1	0	0	2
2341	0	0	1	0	1	1	3
2413	0	1	0	1	1	0	3
2431	0	0	1	1	1	1	4
3124	1	1	0	0	0	0	2
3142	1	0	1	0	0	1	3
3214	1	1	0	1	0	0	3
3241	1	0	1	0	1	1	4
3412	0	1	1	1	1	0	4
3421	0	1	1	1	1	1	5
4123	1	1	1	0	0	0	3
4132	1	1	1	0	0	1	4
4213	1	1	1	1	0	0	4
4231	1	1	1	0	1	1	5
4312	1	1	1	1	1	0	5
4321	1	1	1	1	1	1	6

It was shown[1] that if the digits of the permutation codeword are $(x_1, x_2, \cdots, x_n)$ then the weight of the codeword is

$$w = \sum_{i=2}^{n} \sum_{i=1}^{i-1} m_{ij}$$

where

$$m_{ij} = \begin{cases} 1 & x_i > x_j \\ 0 & x_i < x_j. \end{cases}$$

The equivalent binary codeword is formed simply by taking the $n(n-1)/2$ m_{ij} values in sequence, or

$$(m_{12}, m_{13}, \cdots, m_{1n}, m_{23}, \cdots, m_{2n}, \cdots, m_{n-1,n}).$$

That each permutation generates a unique binary sequence is evident from the fact that no two digits in a permutation are the same, and that therefore changing one permutation into another requires a transposition of digits and a consequent change in the m_{ij} values.

The binary codeword $(b_1, b_2, \cdots, b_{n(n-1)/2})$ has a Hamming weight given by the number of 1's in the sequence, which is, in turn, equal to w. An interchange of the two digits x_i and x_j differing by 1, which either increases or decreases the weight w of the permutation by 1, will also change the value of m_{ij} and, hence, change the weight of the binary sequence by the same amount. The codewords in a rank permutation code are thus completely equivalent to a set of binary codewords of length $n(n-1)/2$ digits.

The inverse transformation from a binary sequence to a permutation can be performed by using the expression

$$x_i = 1 + \sum_{j=1}^{i-1} (1 - m_{ij}) + \sum_{j=i+1}^{n} m_{ij}.$$

This transformation is also unique for any binary sequence that will result in a legitimate permutation. Since $2^{n(n-1)/2} > n!$ for all n, there will always be some binary sequences that do not transform into legitimate permutations. These sequences

Manuscript received December 19, 1969. This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, Pasadena, under Contract NAS 7-100, sponsored by the National Aeronautics and Space Administration.

[1] H. D. Chadwick and L. Kurz, "Rank permutation group codes based on Kendall's correlation statistic," *IEEE Trans. Information Theory*, vol. IT-15, pp. 306–315, March 1969.

produce permutations with at least one digit appearing more than once.

An example of the transformation is shown for $n = 4$ in Table I. The weight distribution of the codewords is shown by Chadwick and Kurz in an appendix.[1] A binary sequence that does not appear in the table is (000010), which transforms back into the permutation (1333). The permutation code (1234), (3142), (2413), (4321) that has a minimum permutation code distance of 3 becomes the linear binary code (000000), (101001), (010110), (111111) with minimum Hamming distance of 3, but the permutation code (1234), (2341), (3412), (4123) becomes the nonlinear weight 3 code (000000), (001011), (011110), (111000). The code (1234), (4213), (3241) becomes the nonlinear code (000000), (111100), (101011) with minimum weight 4. Decoding of such binary codes may be performed by transforming the received binary word into its equivalent permutation and using the correlation properties of permutations described.[1]

The equivalence of these binary codes to the permutation codes offers a simple explanation of the properties of the permutation codes, while at the same time giving rise to an interesting class of binary codes.

HENRY D. CHADWICK
Jet Propulsion Lab.
Pasadena, Calif. 91103
IRVING S. REED
University of Southern California
Los Angeles, Calif. 90007

On Permutation Decoding of Binary Cyclic Double-Error-Correcting Codes of Certain Lengths

INTRODUCTION

Let $\mathcal{U}$ represent an $(n, k, 2)$ binary cyclic code [1], [2] generated by

$$g(X) = \frac{1 + X^n}{h(X)}$$

where n is odd and $h(X)$ has degree k. Suppose

$$R(X) = V(X) + E(X)$$

where $V(X)$ belongs to $\mathcal{U}$ and $E(X)$ has weight 2 or less.

Suppose also that

$$R_{i\beta}(X) = (X^{\beta}R^{2^i}(X) \text{ modulo } 1 + X^n) \text{ modulo } g(X)$$

where $\beta = 0, 1, 2, \cdots, n-1$ and $i = 0, 1, 2, \cdots, q$, where q is such that $nc = 2^q - 1$, c being the smallest integer possible.

It is known that under appropriate restrictions on the rate k/n, the consideration of $R_{0\beta}(X)$, $R_{1\beta}(X)$, $\cdots$ will yield $E(X)$. The decoding procedure based on this fact is called permutation decoding [3].

Hereafter, by the statement that $R_{i_1\beta}(X)$, $R_{i_2\beta}(X)$, $\cdots$, $R_{i_r\beta}(X)$ will suffice, we mean that the consideration of these $R_{i\beta}(X)$ will yield $E(X)$. Also, when we say that permutation decoding is not possible for a certain code, we mean that the consideration of $R_{0\beta}(X)$, $R_{1\beta}(X)$, $\cdots$, $R_{q\beta}(X)$ will not yield $E(X)$.

The object of the present note is to give an analysis of codes $\mathcal{U}$ of certain specified lengths from the point of view of permutation decoding. Specifically, we relate the particular $R_{i\beta}(X)$, to be considered, to the rate k/n.

Manuscript received December 2, 1969. This work was supported in part by the National Research Council of Canada under Grant A-3371.

In this connection, a brief description of how the bounds on k, which will be given later, are arrived at follows. These bounds are obtained by the consideration of cyclotomic cosets. We arrange the numbers $0, 1, 2, \cdots, j, \cdots, n-1$ in a row. Below this now we arrange $j/2$ below which we have $j/4$ and so on. All numbers are computed modulo n. Suppose, for example, we want to know the bound on k so that every $E(X)$ can be obtained by considering just $R_{0\beta}(X)$ and $R_{1\beta}(X)$. Then we consider the first two rows from the top. We examine the last column and note down the two numbers in that column and their complements. By the complement of a number b we mean the number $n - b$. Next we move to the last but one column and note down from this column every number and its complement that are already not covered by the examination of the last column. We continue the process column after column until all the numbers $0, 1, \cdots, n-1$ have been noted down. The number of the column at which we stop the examination is the upper bound on $k + 1$. For example, if $n = 63$ and we want to consider just $R_{0\beta}(X)$ and $R_{1\beta}(X)$, then we stop the examination at the 42nd column so that $k \leq 41$. Generally if we wish to consider $R_{0\beta}R_{r\beta}, \cdots, R_{r\beta}$, then we consider the first $r + 1$ rows and examine all the $r + 1$ numbers in each column. The validity of the method is based on the theory of permutation decoding [3]. We may also remark that the data, to be presented later, were obtained by implementing the above-mentioned procedure on a digital computer.

It is clear that whether or not a code exists for a given rate is not pertinent in the derivation of the bounds on k. Thus, for example, when we say that if in $(17, k, 2)$ codes $k \leq 11$, $R_{0\beta}(X)$, and $R_{1\beta}(X)$ will suffice, we mean that any $(17, k, 2)$ existent code with $k \leq 11$ can be decoded with $R_{0\beta}(X)$ and $R_{1\beta}(X)$; we do not mean that codes for all $k \leq 11$ exist.

Hereafter, by R_i we mean $R_{i\beta}(X)$.

Since it is known [3] that every $(n, k, 2)$ code with $k/n < 1/2$ can be decoded with just R_0, we shall consider here only cases with $k/n \geq 1/2$.

Now we give the actual results.

(17, k, 2) Codes

We find that if $k \leq 11$, R_0 and R_1 will suffice. If $k \leq 13$, R_0, R_1, and R_3 will suffice. If $k > 13$, permutation decoding is not possible. The relevant BCH [4]–[6] codes are (17, 9, 2) and can be decoded with R_0 and R_1.

(21, k, 2) Codes

For these codes we find that if $k \leq 13$, R_0 and R_1 will suffice. The consideration of further R_i does not improve the value of k. In other words if $k > 13$, permutation decoding is not possible.

We note that the relevant BCH codes are (21, 12, 2) and therefore require just R_0 and R_1.

(23, k, 2) Codes

The analysis of these codes is summarized in Table I. We find that the relevant BCH codes, which are (23, 12, 2), can be permutation decoded with R_0 and R_1.

(31, k, 2) Codes

From Table II, which contains the summary of results, we find that the relevant BCH codes, which are (31, 21, 2), can be permutation decoded with R_0, R_1, and R_2.

(45, k, 2) Codes

We find that for $k \leq 29$, R_0 and R_1 will suffice. For $k > 29$, permutation decoding is not possible.

To decode the relevant BCH codes, which are (45, 29, 2), we require R_0 and R_1.

(47, k, 2) Codes

The relevant BCH codes are (47, 24, 2). We find from Table III that they are decodable with R_0 and R_1.