Some Properties of Nonbinary Error-Correcting Codes*

C. Y. LEE†

Summary—An error-correcting code may be thought of as a subset S_0 of points belonging to a set S in which a metric is defined such that the distance between every pair of distinct points of S_0 is larger than some given number. In Hamming's original formulation, S was taken to be the set of all 2^n n-bit binary numbers and the distance between a pair of binary numbers s and t was taken to be the number of bits of s which do not agree with the corresponding bits of t. In this note we shall take S to be the set of all n-tuples in which each coordinate of an n-tuple can assume one of k integral values: 0, 1, . . . , $k - 1$, with $k \geqq 2$. Properties of these nonbinary codes will be discussed.

An error-correcting code may be thought of as a subset S_0 of points belonging to a set S in which a metric is defined such that the distance between every pair of distinct points of S_0 is larger than some given number. In Hamming's original formulation,[1] S was taken to be the set of all 2^n n-bit binary numbers and the distance between a pair of binary numbers s and t was taken to be the number of bits of s which do not agree with the corresponding bits of t. In this note we shall take S to be the set of all n-tuples in which each coordinate of an n-tuple can assume one of k integral values: $0, 1, \cdots, k - 1$, with $k \geqq 2$. These k values have the usual ordering and addition modulo k is assumed defined. For instance, if $k = 7$, then $4 + 6 = 3$ and $4 - 5 = 6$ (mod 7). In our case a metric can rather naturally be assigned to S and a result of Hamming[1] can be extended directly to group codes when each of the coordinates assumes one of a prime number of values (*i.e.*, k is prime). This extension is implied, but not proved, in a recent paper by Ulrich.[2] A method is also given for constructing certain single and double error-correcting group codes for arbitrary k. For nongroup codes, we extend several inequalities on code size obtained for binary codes by Plotkin.[3] Finally, we obtain all close-packed double error correcting codes for $k = 3$.

From here on, an n-tuple is called a *word* of length n and each coordinate of an n-tuple (word) is called a *letter*. The set of all words of length n in which each letter can assume one of k integral values $0, 1, \cdots, k - 1$ is designated by $S_k(n)$. $S_k(n)$ has k^n members. Any subset of $S_k(n)$ is called a *code*.

Consider the k values of each letter as points placed along a circle such that the circle is divided into k arcs of equal length. Let the distance between two letters x and y be the smallest number of arcs separating x and y. Let the distance between two words be the sum of the distances between their letters. Such a distance function is called a (*circular*) *metric* for $S_k(n)$. More precisely, if $s = (s_1, s_2, \cdots, s_n)$ and $t = (t_1, t_2, \cdots, t_n)$ are two words of $S_k(n)$, then ρ is the circular metric if

$$\rho(s, t) = \sum_{i=1}^{n} \rho(s_i, t_i)$$

where

$$\rho(s_i, t_i) = \text{Min}\ \{s_i - t_i, t_i - s_i\} \qquad (\text{mod } k).$$

The characteristics of a circular metric are exhibited by certain physical devices such as circular print wheels or ring counters.

As illustration let us observe several examples of ternary ($k = 3$) codes where each letter can take on one of three values 0, 1 and 2. The code C consisting of the following three 3-letter words in $S = S_3(3)$

0 0 0
1 1 1
2 2 2

is a ternary single error-correcting code. Should one of the words, say 111, be sent and a wrong word, say 121, be received, an encoding device could be instrumented to correct this single error since 121 is of a distance at least two away from the other words of the code.

We note that each member c of the code C has exactly six neighboring words in S with distance one away. These six words together with c form a closed ball of radius one about c. Since there can be not more than $3^3/(6 + 1)$, or less than 4 isolated balls of radius one in S, it follows that there can be not more than three words in any 3-letter ternary single error-correcting code. Thus we say the code C is *full* in S or the biggest possible in S.

We also note that S is an abelian group under addition modulo k and that the code C is a subgroup of S. C is therefore said to be a *group code* in S.

Following this line of thought we observe that the code D consisting of the following nine words in the set $T = S_3(4)$ of all 4-letter ternary words is again a single error-correcting code:

0 0 0 0
1 1 1 0
2 2 2 0
0 1 2 1
1 2 0 1
2 0 1 1
0 2 1 2
1 0 2 2
2 1 0 2

* Manuscript received by the PGIT, January 6, 1958.

† Bell Telephone Labs., Inc., Whippany, N. J.

[1] R. W. Hamming, "Error detecting and error-correcting codes," *Bell. Sys. Tech. J.*, vol. 29, pp. 147–160; January, 1950.

[2] W. Ulrich, "Non-binary error correction codes," *Bell Sys. Tech. J.*, vol. 36, pp. 1341–1388; November, 1957.

[3] M. Plotkin, "Binary Codes with Specified Minimum Distance," Moore School of Elec. Eng., University of Pennsylvania, Philadelphia, Pa.; 1952.

Since $3^4/(8 + 1)$ is exactly 9, it follows that no 4-letter single error-correcting code can have more than nine members. Also, D is a subgroup of T under addition modulo 3. Therefore D is a full group code.

There is an additional property of the code D which is not shared by the code C. Each member d of D belongs to a ball of radius 1 about d consisting of nine members of T. If we take the union of all these balls over all members of D, we find that this union is exactly T and not smaller. We say the code D is *close-packed* in T.

I. Theorems

We shall state and discuss several results which will be proved in Section III.

As given previously, let $S_k(n)$ be the set of all words of length n in which each letter can assume one of k integral values $0, 1, \cdots, k - 1$. A subset S_0 of $S_k(n)$ is said to be a single error-correcting code if the distance between every pair of distinct members of S_0 is 3 or greater, and in general, a subset S_0 of $S_k(n)$ is said to be an e-error-correcting code if the distance between every pair of distinct members of S_0 is $2e + 1$ or greater. For given k and n, we shall let $a_k(n, d)$ denote the size (the number of elements) of the largest e-error-correcting code in $S_k(n)$ and we shall let $b_k(n, d)$ denote the size of the largest e-error-correcting group code in $S_k(n)$ where $d = 2e + 1$. Then

Theorem 1

Let k be an odd prime. If $2n + 1$ is not a power of k, then

$$b_k(n + 1, 3) = kb_k(n, 3).$$

If $2n + 1$ is a power of k, then any group code with $b_k(n, 3)$ members is close-packed, and

$$b_k(n + 1, 3) = b_k(n, 3).$$

For $k = 2$, this is essentially Hamming's result.[4]

Single error-correcting group codes in which k is prime are completely characterized by Theorem 1. In the case k is not prime, Theorem 1 fails but we have

Theorem 2

Let m be some given positive integer and let C denote a single error-correcting group code.

1) For all odd k, $k > 2$, there is an $(m + r)$-letter code C such that C is close-packed and C has k^r members where $r = \frac{1}{2}(k^m - 2m - 1)$.

2) For k even, $k > 2$, there is an $(m + r)$-letter code C with $k^r/2$ members where $r = \frac{1}{2}(k^m - 2^m)$.

Theorems 1 and 2 indicate the behavior of single error-correcting group codes, but much less is known about double error-correcting codes. From (ii) of Theorem 2, we may show

Corollary 1: Let k be even, $k > 2$. For a given m, let $r = \frac{1}{2}(k^m - 2^m)$. Then an $(m + 2r)$-letter double error-correcting group code with $k^r/2$ members can be constructed.

An example of such a double error-correcting code is as follows. Let $k = 6$, $m = 1$. Then, $r = \frac{1}{2}(k^m - 2^m) = 2$. By the corollary, a 5-letter double error-correcting group code having 18 members can be constructed. Such a code is

00000
02402
04204
11311
13113
15515
20220
22022
24424
31531
33333
35135
40440
42242
44044
51151
53553
55355.

So far we have been concerned with group codes. A more difficult problem is to construct full codes which may or may not be group codes. Plotkin gave[3] several interesting bounds on the number of points in nongroup, full binary codes. Extending his proofs, we may show the following two theorems.

Theorem 3[5]

For all pairs d, n such that $3d > 2n$,

$$a_3(n, d) \leqq 3d/(3d - 2n).$$

Some examples of this theorem are $a_3(4, 3) \leqq 9$, which we already know, $a_3(7, 5) \leqq 15$ and $a_3(10, 7) \leqq 21$.

Theorem 4

For all k,

$$a_k(2n, 2d) \geqq a_k(n, d)a_k(n, 2d).$$

As an example, we know $a_3(11, 10) = 3$, by Theorem 3 and from the next section, we shall see that $a_3(11, 5) = 3$.[6] Therefore, by this theorem, we have $a_3(22, 10) \geqq 3^7$.

The proofs of these two theorems will be left to the reader.

II. Some Remarks on Close-Packed Codes

In the binary case, Golay showed[6] that there is a close-packed, 23-letter, triple error-correcting code having 2^{12} members. It can be shown trivially that there is a close-packed, 5-letter, double error-correcting binary code having two members. Shapiro showed[7] (unpublished) that there can be no close-packed double-error correcting, binary code[8] for $n \neq 5$ and $n \neq 90$. Moreover,

[4] If $2n + 1$ is replaced by $n + 1$, then the case $k = 2$ is exactly Hamming's result.

[5] The following extension to arbitrary k is probably true: $a_k(n, d) \leqq 4d/(4d - kn)$ when $4d > kn$ for k even, $a_k(n, d) \leqq 4kd/(4kd - (k^2 - 1)n)$ when $4kd > (k^2 - 1)n$ for k odd.

[6] M. J. E. Golay, "Notes on digital coding," Proc. IRE, vol. 37, p. 657; June, 1949.

[7] After this paper was submitted, the author learned that the unpublished material referred to will appear in a forthcoming paper by H. S. Shapiro and D. L. Slotnick, "On the mathematical theory of error-correcting codes," *IBM J. Res.*

[8] S. P. Lloyd, "Binary block coding" *Bell Sys. Tech. J.*, vol. 36, pp. 517–535; March, 1957. It is shown here that there is no close-packed code for $n = 90$.

he showed that there are at most a finite number of close-packed, e-error-correcting, binary codes over all n for $e \geqq 2$. We shall add a few facts here concerning k-valued, close-packed codes.

It follows from Theorems 1 and 2 that for each odd k, there is an infinite number of k-valued, close-packed, single error-correcting codes over all n, and it is clear that there can be no nontrivial close-packed, single error-correcting code for k even, $k > 2$. Let us consider next double error-correcting codes. The cases $k = 3$ and $k = 4$ are special and will be looked at first.

For $k = 3$, a closed ball of radius 2 about any point of $S_3(n)$ has exactly $2n^2 + 1$ members. Therefore, a necessary condition for a 3-valued, double error-correcting code to be close-packed is that $2n^2 + 1$ be a power of 3. That is, the diophantine equation

$$2n^2 + 1 = 3^x$$

be solvable in positive integral x and n. By chance this equation has been completely solved by Nagell,[9] presumably in no way connected with error correcting codes. The only possible solutions of this equation are

$$\begin{cases} n = 1 \\ x = 1 \end{cases} \quad \begin{cases} n = 2 \\ x = 2 \end{cases} \quad \begin{cases} n = 11 \\ x = \ \ 5. \end{cases}$$

The first two solutions are trivially sufficient, and each code has just one member. We therefore have

Remark 1: The only possible,[10] nontrivial, 3-valued close-packed, double error-correcting code is when $n = 11$.

For $k = 4$, we note that if we encode each value in binary so that the single letter 0 in the $k = 4$ system is encoded into the 2-letter binary word 00, 1 into 01, 2 into 11 and 3 into 10, then the circular metric in the $k = 4$ system is preserved in the corresponding binary system. Hence, every code in $S_4(n)$ is equivalent to a code in $S_2(2n)$. Therefore every close-packed code in $S_4(n)$ corresponds to a close-packed code in $S_2(2n)$. Since from previous discussion we know that there is no close-packed code in $S_2(2n)$, it follows that

Remark 2: There is no 4-valued, close-packed, double error-correcting code.

For $k > 4$, a closed ball of radius 2 about any point of $S_k(n)$ has $2n^2 + 2n + 1$ members. Therefore, for k prime, a necessary condition for a k-valued, $k > 4$, double error-correcting code to be close-packed is that $2n^2 + 2n + 1$ be a power of k. In other words, the diophantine equation

$$2n^2 + 2n + 1 = k^x$$

be solvable in positive, integral n, x and prime k.

This equation is trivially solvable for $x = 1$. For $x > 1$, it can be shown that there is an infinite number of solutions. However, this equation has at most a finite number of solutions for fixed k (see below), and at most a finite number of solutions[11] for fixed $x \geqq 3$.

Some known solutions to this equation are

$$\begin{cases} n = 3 \\ k = 5 \\ x = 2 \end{cases} \quad \begin{cases} n = 119 \\ k = 13 \\ x = 4 \end{cases} \quad \begin{cases} n = 4059 \\ k = 5741 \\ x = 2. \end{cases}$$

There is no code which satisfies the first solution. It is not known, although somewhat doubtful, whether there are codes which satisfy the other two solutions.

Extending a proof given by Shapiro,[7] it can be shown that

Remark 3: There can be at most a finite number of close-packed, e-error-correcting codes for each k, k prime, $k \geqq 2e + 1$ and $e \geqq 2$.

III. Definitions and Proofs

Let $S_k(n)$ be the set of all n-tuples $(x_1, x_2, \cdots, x_n)$ where x_i takes on integral values $0, 1, \cdots, k - 1$, for $i = 1, 2, \cdots, n$. Each member of $S_k(n)$ is called a *k-valued word of length n* or a *word* if no confusion arises. Each coordinate of a word is called a letter.

Now let a metric ρ be assigned to $S_k(n)$. We introduce the term *proximity* $P(S)$ of any subset S of $S_k(n)$ to be

$$P(S) = \text{Min } \{\rho(x, y) | x, y \,\varepsilon\, S, x \neq y\}.$$

Let d be a positive integer. Any subset of $S_k(n)$ whose proximity is not less than d is said to be an *e-error-correcting code* where $e = (d - 1)/2$ if d is odd, and is said to be an *e-error-detecting code* where $e = d/2$ if d is even. We shall call either an e-error-correcting or detecting code a d-code.

A d-code in $S_k(n)$ is said to be *full* if there is no d-code in $S_k(n)$ with more elements. For given n, d and k, let $a_k(n, d)$ denote the number of elements contained in a full d-code. A d-code is said to be *close-packed* if d is odd and if the union of closed balls of radius $(d - 1)/2$ about all members of the code exhausts $S_k(n)$.

Next let an operation + (mod k) be defined on $S_k(n)$ such that if s and t are two members of $S_k(n)$, each letter of $s + t$ is the sum modulo k of the corresponding letters of s and t. $S_k(n)$ is an abelian group under + (mod k). Any d-code on $S_k(n)$ is said to be a *group code* if it is a subgroup of $S_k(n)$. A group code is *full* if there is no group code having more elements. The number of elements in a full group code is denoted by $b_k(n, d)$.

Since the order of a finite group is a multiple of the order of every one of its subgroups and since the order of $S_k(n)$ is k^n, it follows that

Lemma 1: If k is a prime, $b_k(n, d)$ is a power of k.

[9] T. Nagell, "Sur l' impossibilité de quelques équations à deux indéterminées," *Norsk Matematisk Forenings Skrifter*, series 1, no. 13; 1923.

[10] A code satisfying the third solution has been constructed by Golay, *op. cit.*

[11] For a proof of this, see E. Landan and A. Ostrowski, "On the diophantine equation $ay^2 + by + c = dx^n$," *Proc. London Math. Soc.*, ser. 2, vol. 19, pp. 276–280, 1921.

It remains for us to specify the metric on $S_k(n)$. ρ is said to be the (*circular*) *metric* on $S_k(n)$ if for any pair of words $x = (x_1, x_2, \cdots, x_n)$, $y = (y_1, y_2, \cdots, y_n)$ of $S_k(n)$,

$$\rho(x, y) = \sum_{i=1}^{n} \rho(x_i y_i)$$

where

$$\rho(x_i y_i) = \text{Min}\,\{x_i - y_i, y_i - x_i\} \qquad (\text{mod } k).$$

The idea of the proofs for Theorems 1 and 2 runs as follows. We first show that a code can be constructed if a certain matrix can be found and then show how such a matrix can be obtained.

Definition 1: An m by r matrix $E(m, r)$ with entries a_{ij} is said to be *admissible* if when its columns are regarded as words of $S_k(m)$:

1) Every column is of distance more than one from the origin $(0, 0, \cdots, 0)$.
2) The sum or difference modulo k of any two columns shall be a word different from the origin.

For example, let $E_1(2, 3)$ and $E_2(2, 3)$ be matrices

$$E_1(2, 3) = \begin{bmatrix} 0 & 1 & 2 \\ 4 & 2 & 3 \end{bmatrix}, \qquad E_2(2, 3) = \begin{bmatrix} 0 & 1 & 4 \\ 3 & 2 & 3 \end{bmatrix}.$$

For $k = 5$, $E_1(2, 3)$ is not admissible since condition 1) is violated and $E_2(2, 3)$ is not admissible since condition 2) is violated.

Lemma 2: Let n be given and let m and r be any pair of positive integers such that $m + r = n$. Then for all odd k, an n-letter single error-correcting group code S having k^r members can be constructed if an admissible matrix $E(m, r)$ can be found.

Proof: Suppose $E(m, r)$ is found, the theorem will then be proved by construction. Denote by S the set of all n-letter words of the form.

$$(x_1 x_2 \cdots x_r y_1 y_2 \cdots y_m)$$

where $x_1 x_2 \cdots x_r$ are arbitrary but

$$y_i = \sum_{j=1}^{r} a_{ij} x_j (\text{mod } k), \qquad i = 1, 2, \cdots, m,$$

with $a_{ij} \,\varepsilon\, E(m, r)$. S has k^r members.

Let $s_1 = (x_1 x_2 \cdots x_r y_1 y_2 \cdots y_m)$ and $s_2 = (u_1 u_2 \cdots u_r v_1 v_2 \cdots v_m)$ be two distinct words of S. $\rho(s_1, s_2) \geqq 3$ if three or more of the x_j's are different from the corresponding u_j's. Otherwise, there are two cases.

Case 1: $x_j = u_j$ except for $j = s, t$, $s \neq t$ for which $x_s \neq u_s$, $x_t \neq u_t$.

Let us suppose that the letter distances $\rho(x_s, u_s)$ and $\rho(x_t, u_t)$ are each exactly 1, for otherwise $\rho(s_1, s_2)$ would be larger than 2. Therefore, in this case,

$$x_s - u_s = 1 \quad \text{or} \quad k - 1 \quad (\text{mod } k)$$

and

$$x_t - u_t = 1 \quad \text{or} \quad k - 1 \quad (\text{mod } k).$$

Since $E(m, r)$ is admissible, by condition 2 there exist p, q where $p \neq q$, $1 \leqq p, q \leqq m$ such that not both $a_{ps} + a_{pt}$ and $a_{qs} + a_{qt}$ are zero (mod k) and not both $a_{ps} - a_{pt}$ and $a_{qs} - a_{qt}$ are zero (mod k). We assert that either y_p is different from v_p or y_q is different from v_q. Suppose they are both identical, then

$$\begin{aligned} a_{ps}(x_s - u_s) + a_{pt}(x_t - u_t) &= 0 \\ a_{qs}(x_s - u_s) + a_{qt}(x_t - u_t) &= 0 \end{aligned} \quad (\text{mod } k)$$

contradicting condition 2 of admissibility of $E(m, r)$. Therefore $\rho(s_1, s_2) \geqq 3$.

Case 2: $x_j = u_j$ except for $j = s$ for which $x_s \neq u_s$.

By condition 1 of admissibility of $E(m, r)$, either there are two members a_{ps}, $a_{qs} \neq 0$ or there is one member a_{ts}, $1 < a_{ts} < k - 1$.

In the first instance,

$$\begin{aligned} y_p - v_p &= a_{ps}(x_s - u_s) \\ y_q - v_q &= a_{qs}(x_s - u_s) \end{aligned} \quad (\text{mod } k).$$

First, suppose $x_s - u_s = 2 \neq k - 1$ (mod k). Then, since k is odd, it is impossible for either $y_p - v_p = 0$ or $y_q - v_q = 0$ (mod k). Next, suppose $x_s - u_s = 1$ or $k - 1$ (mod k). Again it is impossible for either $y_p - v_p = 0$ or $y_q - v_q = 0$ (mod k). Therefore, $\rho(s_1, s_2) \geqq 3$.

In the second instance,

$$y_t - v_t = a_{ts}(x_s - u_s) \quad (\text{mod } k).$$

Again since k is odd, if $x_s - u_s = 2 \neq k - 1$ (mod k), $y_t - v_t \neq 0$ (mod k). If $x_s - u_s = 1$ or $k - 1$ (mod k), then $1 < y_t - v_t < k - 1$ implying $\rho(y_t, v_t) \geqq 2$ so that $\rho(s_1, s_2) \geqq 3$.

Thus, in either case, two distinct words of S are at a distance at least three apart. Since it can be checked that S is an abelian group, the proof follows.

In the case k is even, a slight modification in admissibility conditions is required.

Definition 2: An m by r matrix $E(m, r)$ is said to be *E-admissible* if $E(m, r)$ is admissible and

3) In every column j of $E(m, r)$, there is an element a_{ij} such that $2a_{ij} \neq 0$ (mod k).

Lemma 3: Let m, r be defined such that $m + r = n$ where n is given. Let k be even. Then an n-letter single error-correcting group code S having k^r members exists if an E-admissible matrix $E(m, r)$ can be found.

Proof: The only part of the proof which is different from the proof for Lemma 2 is in Case 2 where $x_j = u_j$ except for $j = s$ for which $x_s \neq u_s$. Consider again two subcases.

Case 2.1: There are at least two members a_{ps}, $a_{qs} \neq 0$ in $E(m, r)$ such that either $2a_{ps} \neq 0$ (mod k) or $2a_{qs} \neq 0$ (mod k) by E-admissibility of $E(m, r)$. Suppose $2a_{ps} \neq 0$ (mod k). Now

$$\begin{aligned} y_p - v_p &= a_{ps}(x_s - u_s) \\ y_q - v_q &= a_{qs}(x_s - u_s) \end{aligned} \quad (\text{mod } k).$$

First suppose $x_s - u_s = 2$ (mod k). Then since $2\,a_{ps} \not\equiv 0$ (mod k), $y_p - v_p \not\equiv 0$ (mod k). Next suppose $x_s - u_s = 1$ or $k - 1$ (mod k). Then $y_p - v_p \not\equiv 0$ and $y_q - v_q \not\equiv 0$ (mod k). Therefore $\rho(s_1, s_2) \geqq 3$.

Case 2.2: There is exactly one nonzero member a_{ts} in the set $\{a_{is} \mid i = 1, 2, \cdots, m\}$. By E-admissibility of $E(m, r)$, it follows that $1 < a_{ts} < k - 1$ and $2a_{ts} \not\equiv 0$ (mod k). Now

$$y_t - v_t = a_{ts}(x_s - u_s) \quad (\text{mod } k).$$

If $x_s - u_s = 2$ (mod k), since $2a_{ts} \not\equiv 0$ (mod k), it follows that $y_t - v_t \not\equiv 0$ (mod k). If $x_s - u_s = 1$ or $k - 1$ (mod k), then $1 < y_t - v_t < k - 1$. In either case $\rho(s_1, s_2) \geqq 3$. This concludes the proof.

Lemma 4: A code S, whenever constructable by application of Lemma 2, is close-packed (hence full) if $2n + 1$ is a power of k.

Proof: Each word s in S is contained in a ball consisting of $2n + 1$ words of radius 1 about s and different words of S are contained in disjoint balls. Thus, there are $k^n/(2n + 1) = k^r$ balls the union of which exhausts the set S.

Lemma 5: Let m, r be defined such that

$$k^m \geqq 2n + 1, \qquad k^{m-1} < 2n + 1$$

and

$$r = n - m.$$

An admissible matrix $E(m, r)$ having rm members exist for all *odd* k.

Proof: The lemma will be proved by construction. Let us consider, for each j, $j = 1, 2, \cdots, r$, the m-tuple $(a_{1j}, a_{2j}, \cdots, a_{mj})$ as a member of $S_k(m)$. Let S be a subset of $S_k(m)$ consisting of all members of $S_k(m)$ except the closed ball of radius 1 about $(0, 0, \cdots, 0)$. Define an equivalence relation $\sim$ on S such that if $s_1, s_2, \epsilon S$, $s_1 \sim s_2$ if $s_1 = s_2$ or $s_1 = s^{-1}_2$. Then any set of representatives (one from each equivalence class) has $(k^m - 2m - 1)/2$ words. Since

$$\frac{k^m - 2m - 1}{2} \geqq n - m = r,$$

choose r of these words arbitrarily to form a set of letters with rm members. Since this set of letters satisfies the two conditions of Def. 1, it is an admissible matrix and the proof follows.

Proof of Theorem 1: Define m such that

$$k^m \geqq 2n + 1 \quad \text{and} \quad k^{m-1} < 2n + 1.$$

Set $r = n - m$. Then by Lemmas 2 and 5, an n-letter group code S having k^r words exists.

Suppose first $2n + 1 = k^m$. Then by Lemma 4, S is close-packed so that $b_k(n, 3) = k^r$. Since

$$b_k(n + 1, 3) \leqq \frac{k^{n+1}}{2n + 3} < \frac{k^{n+1}}{2n + 1} = k^{r+1},$$

it follows by Lemma 1 that

$$b_k(n + 1, 3) = b_k(n, 3).$$

Next suppose $k^m > 2n + 1$ and $k^{m-1} < 2n + 1$. Should n be increased by 1, we still have

$$k^m \geqq 2n + 3 \quad \text{and} \quad k^{m-1} < 2n + 3,$$

so that m remains unchanged. Thus r is increased by 1, implying an $(n + 1)$-letter code having k^{r+1} words exists. Now

$$b_k(n + 1, 3) \leqq \frac{k^{n+1}}{2n + 3} = \frac{k^{r+2}k^{m-1}}{2n + 3} < k^{r+2}.$$

Therefore, it follows by Lemma 1 that $b_k(n + 1, 3) = k^{r+1}$, or

$$b_k(n + 1, 3) = kb_k(n, 3).$$

Lemma 6: Let k be even. For a given m, an E-admissible matrix having at least

$$m(\tfrac{1}{2}(k^m - 2^m - 2m))$$

members can be constructed.

Proof: Let us again consider, for each j, $j = 1, 2, \cdots, r$, the m-tuple $(a_{1j}, a_{2j}, \cdots, a_{mj})$ as a member of $S_k(m)$. Let S be the subset of $S_k(m)$ consisting of all members of $S_k(m)$ except 1) the closed ball of radius 1 about $(0, 0, \cdots, 0)$ and 2) all members s of $S_k(m)$ such that $s = s^{-1}$.

Again define an equivalence relation $\sim$ on S such that if $s_1, s_2, \epsilon S$, $s_1 \sim s_2$ if $s_1 = s_2$ or $s_1 = s^{-1}_2$. Then any set of representatives (one from each equivalence class) has $\frac{1}{2}\,(k^m - 2^m - 2m)$ members since there are exactly $2^m + 2m$ members of $S_k(m)$ which are not in S. The set of letters which make up members of S is then the E-admissible matrix in question.

Proof of Theorem 2, 1): Theorem 2, 1) follows from Lemmas 2 and 5.

Lemma 7: Let k be even. For some given n, let $b_k(n, 2)$ be the size of the largest code in which the distance between every pair of points is not less than 2 (*i.e.*, a single error-detecting code). Then $b_k(n, 2) = k^n/2$.

Definition 3. A matrix $E(m, r)$ is said to be *E′-admissible* if it satisfies condition 2 of Definition 1 and condition 3 of Definition 2.

Lemma 8: For a given m, there are at least $m(\frac{1}{2}(k^m - 2^m))$ members in an E'-admissible matrix.

Proof: The proof here is identical with the proof for Lemma 6 if we let the members of class 1 excluded from the set S in that proof be now included in S.

Proof of Theorem 2, 2) and Corollary 1: Let m be given and let $r = \frac{1}{2}(k^m - 2^m)$. Let S_r be an r-letter single error-detecting code with $k^r/2$ members as given by Lemma 7. By Lemma 8, for the pair m, r in question, an E'-admissible matrix $E(m, r)$ can be constructed. For each $x = (x_1, x_2, \cdots, x_r)$ in S_r, define y_i such that

$$y_i = \sum_{j=1}^{r} a_{ij}x_j \pmod{k}, \qquad i = 1, 2, \cdots, m,$$

where each a_{ij} belongs to the E'-admissible matrix $E(m, r)$. Let S_{m+r} be the set of all $(m + r)$-letter words

$$(x_1, x_2, \cdots, x_r, y_1, y_2, \cdots, y_m)$$

where $(x_1, x_2, \cdots, x_r)$ εS_r and the y_i's are given above. Then S_{m+r} is a code satisfying the conditions of Theorem 2, 2).

Next let S_{m+2r} be the set of all $(m + 2r)$-tuples

$$(x_1, x_2, \cdots, x_r, y_1, y_2, \cdots, y_m, x_1, x_2, \cdots, x_r)$$

where $(x_1, x_2, \cdots, x_r)$ εS_r and the y_i's are determined by the linear relations above. S_{m+2r} has $k^r/2$ members and as in the proof of Theorem 1, we may show that $\rho(s_1, s_2) \geqq 5$ for every pair s_1, s_2 εS_{m+2r}. Also, if s_1, s_2 εS_{m+2r}, then $s_1 + s_2$ εS_{m+2r}. Therefore S_{m+2r} is an $(m + 2r)$-letter double error-correcting group code with $k^r/2$ members, and the proof of Corollary 1 follows.

Acknowledgment

The writer is indebted to W. Ulrich and E. Wolman for helpful criticisms and discussions.

Correction

Paul E. Green, Jr., author of "The Output Signal-to-Noise Ratio of Correlation Detectors," which appeared on pages 10–18 of the March, 1957 issue of these Transactions, has requested the editors to make the following corrections to his paper.

In the first paragraph on page 12, the term u_i in the last line should be μ_i.

In (9) on the same page, $\mathrm{Re}([X(\omega)\ H(\omega)]^*[X(\omega)\ H(\omega)])$ should be $[X(\omega) \mid H(\omega) \mid^{2*} X(\omega)] + \mathrm{Re}([X(\omega)\ H(\omega)] * [X(\omega)\ H(\omega)])$.

The right side of (11) on page 13 should be preceded by $\mid I(\Delta)\mid^2$.

In (12), on the same page, multiply the first denominator integrand term $X^2(\omega)\ \mathrm{Re}^2[H(\omega)|$ by a factor of two, and in (13) $N_2(\omega)$ should be replaced by $N_2(\omega) + \Delta)$.

The fifth from the last line in column two of page 13 should read:

For the bandpass filter, the reciprocal $\cdots$. Insert after the last line: For the low-pass filter, the effective integration time is π/W_f.

The following should be added to footnote 8: By using integration limits of $-\infty$ and $+\infty$ instead of 0 and ∞, one obtains a different definition of W_f, sometimes used, which is the reciprocal of the effective integration time for both types of filter.

In (25) on page 15, h_j^2 in the second term should be replaced by h_j, and ξ^2 should be ξ_i^2.

On page 16, the first line after (35), the equation reference should be (28), not (27).

On page 17, in the equation following (41), replace 1/8 with 1/2. In the second paragraph of column one, the equation reference on the fourth line should be (25) instead of (3), and in (51), on the same page, the right side should be multiplied by $\mid I(\Delta) \mid^2$.