Binary Codes with Specified Minimum Distance*

MORRIS PLOTKIN†

Summary—Two n-digit sequences, called "points," of binary digits are said to be at distance d if exactly d corresponding digits are unlike in the two sequences. The construction of sets of points, called codes, in which some specified minimum distance is maintained between pairs of points is of interest in the design of self-checking systems for computing with or transmitting binary digits, the minimum distance being the minimum number of digital errors required to produce an undetected error in the system output. Previous work in the field had established general upper bounds for the number of n-digit points in codes of minimum distance d with certain properties. This paper gives new results in the field in the form of theorems which permit systematic construction of codes for given n, d; for some n, d, the codes contain the greatest possible numbers of points.

BY the use of redundancy, it is possible to encode messages for transmission in such a way that errors in transmission may be corrected, provided they are not too dense. For the special case of transmission by means of binary digits, with fixed-length words, this paper investigates the relationships among word length, number of words in the code and number of errors in a word that can be corrected. The best codes known, with respect to these relationships but not to mechanizability, are given in Table I.

TABLE I

$d = 8$	.	.	.	.	.	.	.	.	2	2	2	2	4	4	8	16	32
	$A(n, d)$						2	2	2	2	4	4	8	16	32	
$d = 6$	.	.	.	.	.	.	2	2	2	4	6*	12*	24*			
				2	2	2	4	6*	12*	24*						
$d = 4$	.	.	2	2	4	8	16									2^{11}
		2	2	4	8	16									2^{11}	
$d = 2$	.	2	4	8	16	32	64	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	2^{13}	2^{14}	2^{15}
	2	4	8	16	32	64	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	2^{13}	2^{14}	2^{15}	2^{16}
			.				.				.					.
			.				.				.					.
			$4 \equiv n$				$8 \equiv n$				$12 \equiv n$					$16 \equiv n$

* These values differ from the corresponding values of $B(n, d)$.

In this paper, n-digit binary numbers are regarded as points in an n-dimensional space. The word "point" denotes a binary number, or more accurately, a sequence of binary digits, since the ordinary arithmetical properties of binary numbers are not utilized.[1] Two n-digit points are said to be "at distance d" if they differ in exactly d corresponding digits. For example, the points

1011101000

and

0111001001

are at distance 4, the first, second, fifth, and last digits being different for the two points. A set of n-digit points is called a "code of minimum distance d" if each point is at distance at least d from every other point of the set. The 6-digit points

000000 010101

111000 101101

100110 110011

011110 001011

form a code of minimum distance 3, as may be verified by comparing them pairwise. It is convenient to regard a set consisting of a single point as a code of minimum distance d for every positive integer d.

Clearly, for every ordered pair (n, d) of positive integers there is some maximal number $A(n, d)$[2] of n-digit points which might be selected to give a code of minimum distance d. The code exhibited above demonstrates that $A(6, 3) \geq 8$. It will be seen later than there does not exist a set of nine 6-digit points at a distance 3 or greater pairwise. The $A(n, d)$ notation describes this situation by the equation

$$A(6, 3) = 8.$$

Both the present paper and one by Hamming[1] are concerned primarily with properties of the function $A(n, d)$. [Hamming's paper would not be very different if he had used $A(n, d)$ instead of his $B(n, d)$.] Interest is attached to this function by reason of its connection with coding schemes for correction of errors in systems employing binary symbols for handling information. Consider a system for computing or transmitting n-digit binary numbers, and having the property that noise or system malfunction will affect at most x of the n-digits in any output number. There can be selected $A(n, 2x + 1)$ but no more n-digit numbers which form a code of minimum distance $2x + 1$. If the system can be designed or its operation programmed in such a manner that correct—*i.e.*, error free—operation will give rise to outputs consisting exclusively of numbers in the code, then the correct outputs will always be deducible from the actual output. There will always be exactly one code number at distance x or less from an output number. For example,

* Received by the PGIT, November 20, 1959. The work leading to this paper was sponsored by the Burroughs Corp.

† Auerbach Electronics Corp., Philadelphia, Pa.

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

[2] This definition for $A(n, d)$ is not the same as Hamming's definition for his $B(n, d)$, in that a somewhat less restrictive class of codes is used here. $B(n, d) \leq A(n, d)$ for all n, d. $B(n, d)$ is always a power of 2; $A(n, d)$ need not be. The departure is for convenience only and does not constitute a significant innovation.

if $x = 1$ and $n = 6$, there could be used the code exhibited above to demonstrate that $A(6, 3) \geq 8$, since $d = 3 = 2x + 1$. An output of, for example, 101001 in such a system could be "corrected" to 101101, that being the code number at distance 1 or less from the actual output.

Following is a summary of Hamming's results, which are utilized in the present paper:[3]

$$A(n, 1) = 2^n,$$

$$A(n, 2) = 2^{n-1},$$

$$A(n + 1, 2k) = A(n, 2k - 1),$$

$$A(n, 2k - 1) \leq \frac{2^n}{1 + C(n, 1) + \cdots + C(n, k - 1)}$$

where

$$C(n, h) = \frac{n!}{h!\,(n - h)!}.$$

Except for the unimportant difference between $A(n, d)$ and $B(n, d)$, all definitions and results to this point are due to Hamming.

Definition: By the sum $a * b$ of two n-digit points a, b is meant that n-digit point whose jth digit is zero / unity according as the jth digits of a, b are the same / different.

For example,

if a is 1011101000

and b is 0111001001

then $a * b$ is 1100100001.

For any a, $a * a$ is the origin or null-point $00 \cdots 0$, denoted throughout by o.

Definition: $|a| = m$ means that exactly m of the digits of the point a are 1. In this notation, the distance between two n-digit points a, b is $|a * b|$.

It is clear that addition as defined above is associative: that $(a * b) * c = a * (b * c)$. If K is a code of n-digit points a, b, c, $\cdots$ of minimum distance d, then so is the code denoted by $K * x$ consisting of the points $a * x$, $b * x$, $c * x$, $\cdots$ where x is any n-digit point. For pairwise distances are preserved, since

$$|\,(a * x) * (b * x)\,| = |\,(a * b) * (x * x)\,|$$
$$= |\,(a * b) * 0\,| = |\,a * b\,|.$$

Theorem 1: If $2d > n$, then $A(n, d) \leq 2m \leq 2d/(2d - n)$, m an integer.

Proof: Let K be any code consisting of A n-digit points of minimum distance d. Let h be any point in K. Consider the code $K * h$, as defined by the notation of the preceding paragraph. Since $h * h = o$, o will be a member of $K * h$. By the minimum distance property it follows that the other $A - 1$ members of $K * h$ each have at least d digits equal to 1, so that the sum of $|k * h|$ over all k in K is at least $(A - 1)d$. This is true for each of the A possible choices of h. Letting h also run through all possible values we find that the total number N of 1's in the A^2 possible sums of two points $k * h$ for h, k both in K, must satisfy

$$A(A - 1)d \leq N = \sum |h * k|,$$

the sum over all ordered pairs (h, k).

Next, we obtain another inequality on N by considering corresponding digits of each point in K. Suppose x points in K have for their first digit 1 and the other $A - x$ have for their first digit 0. In the A^2 sums $k * h$, exactly $2x(A - x)$ will have for their first digit 1. If y, z, $\cdots$ are defined in similar manner for the second digits, third digits, $\cdots$ of the points in K, the same number $N = \sum |h * k|$ is seen to be expressible as

$$N = 2x(A - x) + 2y(A - y) + 2z(A - z) + \cdots .$$

Case 1): $A = 2m$. Each of the terms

$$2x(A - x),\ 2y(A - y),\ \text{etc.},$$

is at most $A^2/2$. Since there are n such terms,

$$N \leq nA^2/2.$$

Combining this inequality with $A(A - 1)d \leq N$,

$$2(A - 1)\,d \leq An$$

and

$$(2\,d - n)A \leq 2\,d.$$

Since $2d > n$ by hypothesis,

$$A = 2m \leq \frac{2\,d}{2\,d - n}.$$

Case 2): $A = 2m - 1$. Each of the terms

$$2x(A - x),\ 2y(A - y),\ \text{etc.},$$

is at most $(A^2 - 1)/2$. Continuing as in Case 1), it may be seen that

$$A = 2m - 1 < 2m \leq \frac{2\,d}{2\,d - n}.$$

Corollary: $A(n, n) = 2$. By the above theorem, $A(n, n) \leq 2$, and the pair $00\cdots0$, $11\cdots1$ constitute an example showing $A(n, n) \geq 2$.

Corollary: $A(4m - 1, 2m) \leq 4m$ and $A(4m - 2, 2m) \leq 2m$.

Theorem 2: $A(n, d) \leq 2A(n - 1, d)$.

Proof: Let K be a code of $A(n, d)$ n-digit points of minimum distance d. Separate the points of K into two sets according to their first digit. At least one of the two sets will contain one-half or more of the points. Deletion of the first digit in each point of that set leaves a code of minimum distance d containing at least

$$\frac{A(n, d)}{2}$$

$(n - 1)$-digit points. This proves the theorem.

[3] Hamming's proofs that the relations hold for $B(n, d)$ are valid without change for $A(n, d)$.

Corollary: Since $A(4m-1, 2m) \leq 4m$, we have

$$A(4m, 2m) \leq 8m.$$

Also, if $A(4m, 2m) = 8m$, then $A(4m-1, 2m) = 4m$ and

$$A(4m-2, 2m) = 2m.$$

Theorem 3: If $4m-1$ is a prime, then $A(4m, 2m) = 8m$.

Proof: Since we have shown $A(4m, 2m) \leq 8m$, it is sufficient to construct a code of $8m$ $4m \equiv$ digit points of minimum distance $2m$.[4] One such construction is included in the Appendix.

Theorem 4: $A(2n, 2d) \geq A(n, 2d)\, A(n, d)$.

Proof: For this proof only the symbol $\frown$ denoting concatenation of two sets of symbols is introduced. Its meaning is illustrated by the example:

If a is 1011

and b is 00111,

then $\widehat{ab}$ is 101100111.

Clearly, $|\widehat{ab}| = |a| + |b|$ for any a, b.

Let L be a code of minimum distance d containing $A(n, d)$ n-digit points, and M a code of minimum distance $2d$ containing $A(n, 2d)$ n-digit points. From these will be constructed a code K of minimum distance $2d$, containing $A(n, d)A(n, 2d)$ points. This will prove the theorem.

Define K as the set of all points $u = \widehat{(aa)} * \widehat{(bo)}$ for a in L and b in M, o being the n-digit null point. The points u will of course be $2n$-digit points. There are $A(n, d)$ $A(n, 2d)$ distinct pairs a, b. If it can be shown that two distinct pairs a_1, b_1 and a_2, b_2 give rise to points u_1, u_2, in K at a distance at least $2d$, the theorem is proved.

$$\begin{aligned} u_1 * u_2 &= \widehat{(a_1 a_1} * \widehat{b_1 o)} * \widehat{(a_2 a_2} * \widehat{b_2 o)} \\ &= \widehat{(a_1 a_1} * \widehat{a_2 a_2)} * \widehat{(b_1 o} * \widehat{b_2 o)} \\ &= \{\widehat{(a_1 * a_2)}\ (a_1 * a_2)\} * \{\widehat{(b_1 * b_2)}\ o\}. \end{aligned}$$

For a_1, b_1 and a_2, b_2 distinct pairs, three cases may occur.

1) $a_1 = a_2$, $b_1 \neq b_2$. In this case

$$\begin{aligned} |\, u_1 * u_2 \,| &= |\, \widehat{o\ o} * \{\widehat{(b_1 * b_2)}\ o\} \,| \\ &= |\, \widehat{(b_1 * b_2)}\ o \,| = |\, b_1 * b_2 \,|. \end{aligned}$$

But, by hypothesis, b_1, b_2 are members of code M of minimum distance $2d$, so that in this case $|u_1 * u_2| \geq 2d$.

2) $a_1 \neq a_2$, $b_1 = b_2$. In this case

$$\begin{aligned} |\, u_1 * u_2 \,| &= |\, \{\widehat{(a_1 * a_2)}\ (a_1 * a_2)\} * \{\widehat{o\ o}\} \,| \\ &= |\, \widehat{(a_1 * a_2)}\ (a_1 * a_2) \,| \\ &= 2\,|\, a_1 * a_2 \,| \end{aligned}$$

and since $|a_1 * a_2| \geq d$ by hypothesis, again $|u_1 * u_2| \geq 2d$.

3) $a_1 \neq a_2$, $b_1 \neq b_2$. In this case we write

$$\begin{aligned} |\, u_1 * u_2 \,| &= |\, \{\widehat{(a_1 * a_2) * (b_1 * b_2)}\}\ \{(a_1 * a_2) * o\} \,| \\ &= |\, (a_1 * a_2) * (b_1 * b_2) \,| + |\, a_1 * a_2 \,|. \end{aligned}$$

For any x, y, $|x * y| \geq |x| - |y|$, or

$$|\, x * y \,| + |\, y \,| \geq x.$$

Therefore, $|u_1 * u_2| \geq |b_1 * b_2| \geq 2d$.

Theorem 5: If $A(4m, 2m) = 8m$ holds for $m = x$, then it also holds for $m = 2x$.

Proof: $A(8m, 4m) \geq A(4m, 4m)A(4m, 2m) = 2A(4m, 2m)$. Also, $A(8m, 4m) \leq 16m$ by the corollary to Theorem 2. Therefore, $A(4m, 2m) = 8m$ implies $A(8m, 4m) = 16m$, which was to be proved.

Theorems 3 and 5 together prove that $A(4m, 2m) = 8m$ holds for a number of values of m. In $m \leq 20$, the values which are not reached are 7, 9, 13, 14, and 19. I know of no m for which I can show $A(4m, 2m) \neq 8m$. This suggests the conjecture $A(4m, 2m)$, $= 8m$ for all m.

From Theorems 1 to 5, in conjunction with Hamming's results, there may be deduced for a number of n, d the exact value of $A(n, d)$. With few exceptions, these n, d lie in the region $2d > n$. This is the region in which $A(n, d) \leq 4d$ and one would expect it for that reason to be the least interesting region from the point of view of practical applications. The known values of $A(n, d)$ for $d \leq 8$, $n \leq 16$ are shown in Table I. Corresponding values of $B(n, d)$ are given in Table II. The bottom two rows, $d = 1$ and $d = 2$, are given by Hamming; and values for n, d = 3, 3; 4, 4; 7, 3; 8, 4; 15, 3; 16, 4 are special cases of Golay's formula.[5] No single method can be

TABLE II

$d = 8$	.	.	.	.	.	.	.	.	.	2	2	2	2	4	4	8	16	32
$B(n, d)$									2	2	2	2	4	4	8	16	32	
$d = 6$	.	.	.	.	.	.	.	2	2	2	4	4	8	16				
						2	2	2	4	4	8	16						
$d = 4$	.	.	.	2	2	4	8	16	16	32	64	2^7	2^8	2^9	2^{10}	2^{11}		
			2	2	4	8	16	16	32	64	2^7	2^8	2^9	2^{10}	2^{11}	2^{11}		
$d = 2$	.	.	2	4	8	16	32	64	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	2^{13}	2^{14}	2^{15}	
	2	4	8	16	32	64	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	2^{13}	2^{14}	2^{15}	2^{16}		
			.				.				.				.			
			.				.				.				.			
			$4 \equiv n$				$8 \equiv n$				$12 \equiv n$				$16 \equiv n$			

[4] Since the original writing of this report, the author has learned that such codes are a special case of a more general class that may be constructed by methods given by R. E. A. C. Paley, "On Orthogonal Matrices," *J. Math. and Phys.*, vol. 12, pp. 311–320; 1933. By virtue of Paley's work, Theorem 3 may be stated not only for $4m-1$ prime, but for $4m-1$ of the form $2^k(p^h+1)$, p an odd prime and h, k integers.

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

prescribed for finding the values given for different n, d. To illustrate the procedures it will be shown that $A(13, 8) = 4$.

Because $8 - 1 = 7$ is a prime, $A(8, 4) = 16$ by $A(4m, 2m) = 8m$. This in turn implies that $A(8m, 4m) = 16m$, or $A(16, 8) = 32$.

$$A(13, 8) \geq \frac{A(14, 8)}{2} \geq \frac{A(15, 8)}{4} \geq \frac{A(16, 8)}{8} = 4$$

by Theorem 2. By Theorem 1,

$$A(13, 8) \leq 2m \leq \frac{16}{16 - 13}, \quad \text{or} \quad A(13, 8) \leqq 4.$$

Combining the two inequalities, $A(13, 8) = 4$.

For $n > 2d$, although they do not provide exact values of $A(n, d)$, Theorems 1 to 5 may be useful in obtaining bounds. Again, the method chosen will be different for different n, d. For purposes of illustration the case $n = 26$, $d = 6$ is discussed.

$$A(26, 6) = A(25, 5) \leq \frac{2^{25}}{1 + 25 + (1/2)(25)(24)} = \frac{128}{163} \cdot 2^{17},$$

$$A(26, 6) \geqq A(13, 6)A(13, 3) \geqq A(12, 6)A(14, 4) \geq 24A(7, 4)A(7, 2),$$

and

$$A(26, 6) \geq (24)(8)(64) = 3 \cdot 2^{12}.$$

This tells us that

$$3 \cdot 2^{12} \leq A(26, 6) \leq \frac{128}{163} \cdot 2^{17}.$$

Further, it tells us how to construct a code of 3.2^{12} points for $n = 26$, $d = 6$, because all theorems of this paper bounding $A(n, d)$ from below are constructive in nature. In order to construct such a code the inequalities leading to $A(26, 6) \geq 3.2^{12}$ are retraced.

First let K_1 be the code of 8 points for $n = 4$, $d = 2$, consisting of all 4-digit points which have an even number of 1's among their digits. From K_1 and the two point code 1111,0000, there may be constructed by the method of Theorem 4 a code K_2 of $(8)(2) = 16$ points with $n = 8$, $d = 4$. If the sixteen points of K_2 are separated into two sets according to whether the last digit is 0 or 1, at least one of the sets will have eight or more points and deletion of the last digit will give a code K_3 of at least eight members with $n = 7$, $d = 4$. We have now got as far as $A(7, 4) = 8$ in retracing the inequalities. Next we take K_4 as the code of 64 points consisting of all 7-digit points with an even number of 1's among their digits. K_4 exemplifies $A(7, 2) = 64$. From K_3 and K_4 there may be constructed by the method of Theorem 4 a code K_5 of $A(7, 2)A(7, 4) = 2^9$ points, with $n = 14$ and $d = 4$. By merely suppressing the last digit of K_5 we get a code K_6 with the same number 2^9 of points, $n = 13$, $d = 3$.

Since $4 \cdot 3 - 1 = 11$ is a prime, the method of Theorem 3 permits construction of a code K_7 exemplifying $A(12, 6) = 24$. By the possibly wasteful process of adding an 0 at the end of each point of K_7 there may be constructed K_8, a code of 24 points with $n = 13$, $d = 6$. Finally from K_6 and K_8 there may be obtained, again by the method of Theorem 4, our desired code for $n = 26$, $d = 6$, with at least $24 \cdot 2^9 = 3 \cdot 2^{12}$ points.

Appendix

Proof That $A(4m, 2m) = 8m$ If $4m - 1$ is a Prime

In this proof of congruences are modulo $4m - 1$ if not otherwise noted. The first and greater part of the proof consists of constructing a set $a_1, a_2, \cdots, a_{4m-1}$ of $(4m - 1)$-digit points satisfying

$$| a_i | = 2m \quad \text{and} \quad | a_j * a_k | = 2m, \qquad k \neq j$$

and

$$j, k = 1, 2, \cdots, 4m - 1.$$

After that the rest is simple.

It is a well-known theorem in elementary number theory that every odd prime p has a primitive root r: an integer such that each of $r, r^2, r^3, \cdots, r^{p-1}$ is congruent to a different one of $1, 2, 3, \cdots, p - 1$. Let r be a primitive root of the prime $4m - 1$.

An integer $x \not\equiv 0$ modulo p is called a quadratic residue of a prime p if there exists another integer y satisfying $y^2 \equiv x$ modulo p. If there exists no y satisfying $y^2 \equiv x$ modulo p then x is called a quadratic nonresidue of p. It is known from elementary number theory that exactly half of the integers $1, 2, \cdots, p - 1$ are quadratic residues and half are quadratic nonresidues and that -1 is a quadratic nonresidue of all prines of the form $4m - 1$.

The numbers $r^2, r^4, \cdots, r^{4m-2}$ are all quadratic residue of $4m - 1$, for clearly $y = r^k$ satisfies $y^2 \equiv r^{2k}$ for $k = 1, 2, \cdots, 2m - 1$. Therefore, $r, r^3, \cdots, r^{4m-3}$ must be quadratic nonresidues of $4m - 1$. The numbers $-r^2, -r^4, \cdots, -r^{4m-2}$ are also quadratic nonresidues, for if there were a w satisfying $w^2 \equiv -r^{2k}$ there would be a y—namely, the y satisfying $w = yr^k$—which satisfies $y^2 \equiv -1$, and this is known to be impossible modulo $4m - 1$. The numbers $r, r^3, \cdots, r^{4m-3}$ are, therefore, each congruent to a different one of $-r^2, -r^4, \cdots, -r^{4m-2}$, each set containing one member congruent to each of the nonresidues among $1, 2, 3, \cdots, 4m - 2$.

I shall construct the $a_1, a_2, \cdots, a_{4m-1}$ in terms of their binary digits. To that end, I first define a binary digit z_i for all integral i by:

$z_i = 1$ if i is a quadratic residue of $4m - 1$; *i.e.*, if i is congruent to one of $r^2, r^4, r^6, \cdots, r^{4m-2}$.
$z_i = 0$ if i is a quadratic nonresidue of $4m - 1$; *i.e.*, if i is congruent to one of $r, r^3, \cdots, r^{4m-3}$.
$z_i = 1$ if $i \equiv 0$.

The z_i so defined have the property, as is easily verified, that $z_i = z_{ir^2}$ for every i. It follows that $z_i = z_{ir^2} = z_{ir^4} = z_{ir^6} = \cdots$ etc., for every i. Also, since $r^2, r^4, r^6, \cdots, r^{4m-2}$ are congruent to $-r, -r^3, \cdots, -r^{4m-3}$ in some order the above equations may be expressed

$$z_i = z_{-ir} = z_{-ir^3} = z_{-ir^5} = \cdots \text{ etc., or}$$

$$z_{-i} = z_{ir} = z_{ir^3} = z_{ir^5} = \cdots \text{ etc., for every } i.$$

These equations may all be combined into

$$z_{ir^k} = \begin{cases} z_i, & k \text{ even} \\ z_{-i}, & k \text{ odd} \end{cases}$$

for any i and k.

The a_i are now defined. Let a_1 be the $(4m - 1)$-digit point whose ith digit is z_i, $i = 1, 2, \cdots, 4m - 1$. For $j = 2, 3, \cdots, 4m - 1$, a_j is obtained by cyclic permutation of the digits of a_1: let z_{j+i-1} be the ith digit of a_j. Consider the digits of a_1. The last one is z_{4m-1}, which is 1 because $4m - 1 \equiv 0$. Of the others, half of the subscripts are residues and half are nonresidues; *i.e.*, half the digits are 1's and half 0's. Therefore, $2m$ of the digits are 1's, and $2m - 1$ 0's; $|a_1| = 2m$. But since a_j is obtained by permuting the digits of a_1, we have

$$|a_j| = 2m, \qquad j = 1, 2, \cdots, 4m - 1.$$

This is one of the two conditions we shall require on the a_j, the other being

$$|a_j * a_k| = 2m \quad \text{if} \quad j \neq k.$$

We now verify that the second condition is also met.

Let

$$s_{j,k} = |a_j * a_k|, \qquad i, j = 1, 2, \cdots, 4m - 1.$$

I wish to show $s_{ik} = 2m$ for all $j \neq k$. By the cyclic construction of the a_j, it is clear that $|a_j * a_k| = |a_1 * a_{k-j+1}|$ if $k > j$. It is, therefore, sufficient to prove $s_{1,k} = 2m$, $k = 2, 3, \cdots, 4m - 1$; or $s_{1,u+1} = 2m$, $u = 1, 2, \cdots, 4m - 2$.

$s_{1,u+1} = |a_1 * a_{u+1}|$ is investigated directly by comparison of corresponding digits of a_1 and a_{u+1}. These are, in order, the pairs z_1, z_{u+1}; z_2, z_{u+2}; $\cdots$; z_{4m-1}, z_u. $s_{1,u+1}$ is the number of pairs z_j, z_{u+j} for which $z_j \neq z_{u+j}$. It is convenient to rearrange the pairs as follows (*I* utilize $z_{4m-1} = z_0$, $z_{4m-1-u} = z_{-u}$, etc.):

$$z_0, z_u; z_u, z_{2u}; \cdots; z_{-u}, z_0.$$

This rearrangement will always be possible because the first elements of the pairs are the same for both sets, $0, u, 2u, \cdots$, running through the values $1, 2, 3, \cdots$ for $u = 1, 2, \cdots, 4m - 2$.

If u is a quadratic residue of $4m - 1$, then $u \equiv r^{2k}$ and we had seen that $z_{ir^{2k}} = z_i$. We may express the pairs $z_0, z_u; z_u, z_{2u}; z_{2u}, z_{3u}; \cdots; z_{-u}, z_0$ as $z_0, z_{r^{2k}}; z_{r^{2k}}, z_{2r^{2k}}; z_{2r^{2k}}, z_{3r^{2k}}; \cdots; z_{-r^{2k}}, z_0$; or finally as $z_0, z_1; z_1, z_2, z_2, z_3; \cdots, z_{-1}, z_0$. To summarize, $s_{1,u+1}$ is the number of pairs of adjacent elements z_j, z_{j+1} in a complete cycle $z_0, z_1, z_2, \cdots, z_{-1}, z_0$ for which $z_j \neq z_{j+1}$, if u is a quadratic residue of $4m - 1$.

If u is a quadratic nonresidue of $4m - 1$, then $u \equiv r^{2k-1}$ and we had seen that $z_{ir^{2k-1}} = z_{-1}$. In this case the pairs $z_0, z_u; z_u, z_{2u}; z_{2u}, z_{3u}; \cdots; z_{-u}, z_0$ may be expressed by $z_0, z_{r^{2k-1}}; z_{r^{2k-1}}, z_{2r^{2k-1}}; z_{2r^{2k-1}}, z_{3r^{2k-1}}; \cdots; z_{-r^{2k-1}}, z_0$; and finally by $z_0, z_{-1}; z_{-1}, z_{-2}; z_{-2}, z_{-3}; \cdots; z_1, z_0$. This time it is seen that $s_{1,u+1}$ is the number of pairs of adjacent elements z_j, z_{j-1} in a complete cycle $z_0, z_{-1}, z_{-2}, \cdots, z_1, z_0$ for which $z_j \neq z_{j-1}$, if u is a quadratic nonresidue of $4m - 1$.

But the two cycles, for u a residue and for u a nonresidue, give the same value of $s_{1,u+1}$, for one cycle is the other written backwards. It remains to find $s_{1,u+1} = s$, the distance $|a_j * a_k|$ for any distinct j, k. Consider the first digit of a_j, $j = 1, 2, \cdots, 4m - 1$. It will be z_j, which has been seen to take on the value 1 for $2m$ of the j and 0 for $2m - 1$ of the j. Exactly $2m(2m - 1)$ of the

$$\frac{(4m - 1)(4m - 2)}{2}$$

different $a_j * a_k$, $j \neq k$, will have 1 for the first digit. This is true also for the second, third, etc., digits by reason of the cyclic construction of the a_j. The total number of 1's in all the different $a_j * a_k$ is therefore $\sum_{j<k} |a_j * a_k| = (4m - 1)2m(2m - 1)$. But this sum is also

$$\frac{(4m - 1)(4m - 2)}{2}$$

because s was the distance between each pair and there are

$$\frac{(4m - 1)(4m - 2)}{2}$$

pairs a_j, a_k, $j \neq k$. Combining the two,

$$s = 2m = |a_j * a_k| \quad \text{for} \quad j \neq k;$$

$$j, k = k, 2, \cdots, 4m - 1.^6$$

Now that there have been constructed the a_j with the two desired properties $|a_j| = 2m$ and $|a_j * a_k| = 2m$ if $j \neq k$, it is easy to construct a code to demonstrate $A(4m, 2m) \geq 8m$.

[6] This implies that there are $2m$ alternations—1 followed by 0 or 0 followed by 1—in the sequence $z_0 z_1 z_2 \cdots z_{-1} z_0$. Since $z_1 = z_0 = 1$ and $z_{-1} = 0$, it follows that for primes of form $4m - 1$ the quadratic residues among $1, 2, \cdots, 4m - 2$ occur in exactly m blocks, as do the nonresidues.

For $j = 1, 2, \cdots, 4m - 1$, let b_i be the $4m$-digit point obtained by adding an 0 at the end of a_i. Because $|a_i| = 2m$ and $|a_i * a_k| = 2m$ for $j = k$ it is clear that $|b_i| = 2m$ and $|b_i * b_k| = 2m$ for $j = k$. I denote by e the $4m$-digit point whose digits are all 1; by o, as before, the $4m$-digit point whose digits are all 0.

I claim that the points e, o, b_i, $e * b_i$ form a code of $8m$ $4m$-digit points of minimum distance $2m$, demonstrating that $A(4m, 2m) \geq 8m$. Clearly there are $8m$ points in the code, each of $4m$ digits. Only the minimum distance requirement need be established. Since $|b_i| = 2m$ implies $|e * b_i| = 2m$, the zeros of b_i being the 1's of $e * b_i$ and conversely, it is clear that e, o are each at distance $2m$ from each of the remaining points. Also, $|b_i * b_k| = 2m$ for $j \neq k$ implies $|(e * b_i) * (e * b_k)| = 2m$ for $j \neq k$, the two distances being equal. It remains only to check $|b_i * (e * b_k)|$. But this is equal to $|e * (b_i * b_k)|$, and is equal to $2m$ or $4m$ because $|b_i * b_k| = 2m$ or 0 depending on whether $j \neq k$ or $j = k$.

This completes the proof that the code as constructed exemplifies $A(4m, 2m) \geq 8m$. The construction of such a code for given m is quite simple in practice, compared to the proof above that the code constructed fulfills the requirements. The case $m = 3$ is illustrated.

For $m = 3$, $4m - 1 = 11$. It is readily determined that 2 is a primitive root of 11, the numbers $2, 2^2, 2^3, \cdots, 2^{10}$ being congruent modulo 11 to 2, 4, 8, 5, 10, 9, 7, 3, 6, 1, respectively. The second, fourth, etc., of these are the residues: 4, 5, 9, 3, 1; the others 2, 8, 10, 7, 6, the non-residues. The definition of z_i requires that $z_i = 1$ for $i = 1, 3, 4, 5, 9$, and also for $i = 11$; $z_i = 0$ for $i = 2, 6, 7, 8, 10$. This gives us the a_i:

a_1: 1 0 1 1 1 0 0 0 1 0 1

a_2: 0 1 1 1 0 0 0 1 0 1 1

a_3: 1 1 1 0 0 0 1 0 1 1 0

.....

(etc., by cyclic permutation)

.....

a_{10}: 0 1 1 0 1 1 1 0 0 0 1

a_{11}: 1 1 0 1 1 1 0 0 0 1 0.

The desired code of $8m = 24$ points of $4m = 12$ digits each, of minimum distance $2m = 6$ is the following:

0:	000000 000000	e:	111111 111111
b_1:	101110 001010	$e * b_1$:	010001 110101
b_2:	011100 010110	$e * b_2$:	100011 101001
b_3:	111000 101100	$e * b_3$:	000111 010011
.....		.....	
.....		.....	
b_{10}:	011011 100010	$e * b_{10}$:	100100 011101
b_{11}:	110111 000100	$e * b_{11}$:	001000 111011.

On Decoding Linear Error-Correcting Codes—I*

NEAL ZIERLER†

Summary—A technique is described for finding simply computable numerical-valued functions of a received binary word whose value indicates where errors in transmission have occurred. Although it seems that a certain condition must usually be fulfilled for such functions to exist, or for our method to constitute an efficient procedure for finding them, there is, on the one hand, a strong tendency for "good" codes to satisfy the condition, while, on the other, it appears to be straightforward to construct codes which are good for a specified channel and also fulfill the condition. An advantage of the resulting decoding procedure is that it corrects and detects all possible errors; more precisely, if a word u is received and the coset $\bar{u}$ to which u belongs has a unique leader e, the procedure concludes that $u + e$ was sent, while if u has no unique leader, that fact, along with the weight of $\bar{u}$ (and sometimes a little more) can be indicated. The ideas and techniques are illustrated by the construction of decoding procedures for the perfect (23, 12) three-error-correcting code.

* Received by the PGIT, November 12, 1959. Operated with support from the U. S. Army, Navy and Air Force.

† Lincoln Lab., Mass. Inst. Tech., Lexington, Mass.

I. Introduction

THE type of decoding procedure with which this paper is concerned may be briefly described as follows (see also the Summary). Let V be the space of binary n-tuples; let A, the code, be a k-dimensional