REPORT R-417 MAY, 1969

CSL COORDINATED SCIENCE LABORATORY

SOME RESULTS IN THE THEORY OF ARITHMETIC CODES

R.T. CHIEN
S.J. HONG
F.P. PREPARATA

UNIVERSITY OF ILLINOIS – URBANA, ILLINOIS

SOME RESULTS IN THE THEORY OF ARITHMETIC CODES

R. T. Chien, S. J. Hong and F. P. Preparata
Coordinated Science Laboratory
University of Illinois, Urbana

This work was supported by the National Science Foundation under Grant GK-1690 and GK-2339. Auxiliary support was by the Joint Services Electronics Program (U.S. Army, U.S. Navy, and U.S. Air Force) under Contract DAAB 07-67-C-0199.

List of Symbols

A	Generator of Arithmetic Code
B	number of code words
e(B)	exponent of 2 modulo B
φ(B)	Euler function of B
W	Sum of local orbital weights
w	local orbital weight
dm	minimum distance

Number of pages	28
Number of Tables	2
Running Head	"Arithmetic Codes"

Abstract

This paper presents a simple number-theoretic investigation of the structure of binary arithmetic AN codes. The range (0, B-1) of represented integers is related to the code length n through $2^n-1 = AB$. The analysis is based on the partition of the integers $1 \leq N \leq B-1$ into orbits, which are analogous to cosets of the multiplicative subgroup of the powers of 2 modulo B. It is shown how the code minimum weight is related to the members of the orbit. The properties of sets of prime powers are used in developing a simple search strategy for codes. An important consequence of the presented analysis is the construction of codes of moderate distance and high rate, thereby filling the spectrum between the two known extremes of the single-error correcting Brown codes and of the maximum-sequence-like codes of Barrows and Mandelbaum. A list of codes of length ≤ 36 is finally presented.

I. Introduction

Arithmetic Codes, first proposed by Diamond (1955) have been the subject of continuing investigation over the past years. Single-error-correcting arithmetic codes have been investigated by Brown (1960), Peterson (1961), and Bernstein (1962). Burst-error-correcting arithmetic codes have been studied by Henderson (1961), Mandelbaum (1965), Stein (1962), and Chien (1964). In the case of multiple-error-correction only partial results are known. Results have been reported by Bernstein (1962), Barrows (1966), Mandelbaum (1967), Chang and Tsao-Wu (1968) and Chien, Hong and Preparata (1968). A survey of early results was given by Massey (1964). Use of arithmetic codes for improving computer reliability has been proposed by Avizienis (1965).

The purpose of this paper is to present new results on the determination of the minimum distance of arithmetic codes. Analytical as well as computational results are presented.

II. Background and preliminary results.

The codewords of an arithmetic code have the form AN. A is a fixed integer called the generator and N is a generic integer in the interval (0, M-1). Clearly M is the number of code words as defined by Peterson (1961).

The arithmetic weight (just "weight" hereafter) of an integer I is defined as the least number of nonzero (± 1) digits required to represent the number I in the modified binary form to be described later. The error correcting capabilities of the code depend solely upon the arithmetic weight

of the code words. Although a generalization into any radix system is easy, our discussion will be confined to the most practical binary case only. The distance between the two codes words AN_1 and AN_2 is the weight of $|AN_1 - AN_2|$ and it is easily recognized as the weight of some third code word. Hence, the minimum distance of the code is merely the minimum of the weights of all the nonzero code words. An error pattern E is called t-fold if the weight of E is t, and the code can correct errors up to t if and only if the minimum distance of the code is larger than 2t.

We now recall the representation of an integer b in Nonadjacent Form (NAF). The sequence $q_0 q_1 \cdots q_n$ is said to be the NAF representation of the integer b if

$$b = \sum_{i=0}^{n} q_i 2^i \qquad \text{and} \qquad \begin{cases} q_i = -1,0,1 \ (i=0,1,\ldots,n) \\ q_i q_{i+1} = 0 \end{cases}$$

One way to obtain b in NAF is to expand b in a binary representation and apply a conversion algorithm due to Reitwiesner (1960). The algorithm terminates and the NAF representation is proved by Bernstein (1962). The NAF algorithms are related to techniques for speeding up arithmetic processes and therefore have been the object of extensive studies in the latter context. (See, for instance, Wilson and Ledley (1961), Robertson (1958)(1967), Metze (1962) and MacSorley (1961). The following variation is particularly useful for our purpose. Consider the fraction $\frac{a}{B}$ where both a and B are positive integers. $0 < a < B$ and B is odd. The digits q_i of $\frac{a}{B}$ in NAF and the residues of each step of the expansion are recursively

given by the following algorithm.

1. - Set $r_{-1} = a/2$.

2. - Compute r_i and q_i according to the rules:

(1) $$2r_i = q_{i+1}B + r_{i+1}$$

(2) $$q_{i+1} = \begin{cases} 1 & \text{if } \frac{2B}{3} > r_i \geq \frac{B}{3} \\ 0 & \text{if } \frac{B}{3} > r_i \geq -\frac{B}{3} \\ -1 & \text{if } \frac{-B}{3} > r_i \geq -\frac{2B}{3} \end{cases} \qquad i = -1,0,1,2,\ldots$$

The following theorem establishes the validity of the given conversion algorithm.

Theorem 1: With the application of the Direct NAF Conversion Algorithm:

(3) $$q_i q_{i+1} = 0$$

(4) $$\frac{2B}{3} > r_i \geq -\frac{2B}{3}$$

for $i = 0,1,2,\ldots$.

Proof: For the case $i = 0$, if $q_0 = 0$ (3) and (4) are automatically satisfied. If $q_0 = 1$ then $B > a > \frac{2B}{3}$, and $0 > r_0 = a - B > \frac{2B}{3} - B = -\frac{B}{3}$, and $q_1 = 0$ as required; also r_0 satisfies (4). If $q_i = 0$, (3) is satisfied and, by the algorithm, $\frac{B}{3} > r_{i-1} \geq -\frac{B}{3}$,(4) is satisfied also. If $q_i \neq 0$ we may assume $q_i = 1$. (The case of $q_i = -1$ can be proved by a parallel argument.)

$q_i = 1$ implies $\frac{2B}{3} > r_{i-1} \geq \frac{B}{3}$ and $\frac{4B}{3} > 2r_{i-1} \geq \frac{2B}{3}$. As $2r_{i-1} = q_i B + r_i$, $\frac{B}{3} > r_i \geq -\frac{B}{3}$. Consequently, $q_{i+1} = 0$ and both (3) and (4) are satisfied. $\frac{2B}{3} - B \leq r_i < \frac{4B}{3} - B$ or equivalently $-\frac{B}{3} \leq r_i \leq \frac{B}{3}$. Hence $q_{i+1} = 0$, $|r| \leq \frac{2B}{3}$, and the theorem follows from mathematical induction on i.

It is further observed that when the integers are considered modulo B, one may write,

$$(5) \qquad q_{i+1} \begin{cases} \neq 0 & \text{if } \frac{2B}{3} > r_i \geq \frac{B}{3} \pmod{B} \\ = 0 & \text{if } B \geq r_i \geq \frac{2B}{3} \text{ or } \frac{B}{3} > r_i \geq 0, \pmod{B}. \end{cases}$$

Also, $r_i \equiv 2^i r_o$ modulo B. Denoting by e(B) the exponent of 2 modulo B, that is e(B) is the least integer for which $2^{e(B)} \equiv 1$, then $r_i \equiv 2^{e(B)} r_i \equiv$ $\equiv r_{i+e(B)}$. It also follows that $q_{i+e(B)} = q_i$ for $i \geq 1$, namely the expansion

$$\frac{a}{B} = q_0 . q_1 q_2 \cdots$$

is periodic with period e(B) for $i \geq 1$; $q_1 q_2 \cdots q_{e(B)}$ is termed the B-<u>period</u> of a/B, and its <u>weight</u> is defined as the number of nonzero q_i's it contains ($1 \leq a \leq B-1$).

Hereafter we shall consider arithmetic codes for which

$$A = \frac{2^{e(B)} - 1}{B}, \qquad M = B$$

If N is modulo B, then AN is modulo $2^{e(B)}-1$. The generic code word then becomes

$$AN = N\,\frac{2^{e(B)}-1}{B} = \frac{N}{B}(2^{e(B)}-1) = \sum_{j=0}^{e(B)} q_j 2^{e(B)-j} - q_0$$

If $q_0 = 0$, the weight of AN is clearly the weight of the B-period of N/B. If $q_0 = 1$, notice that

$$AN \equiv A(N-B) = (\frac{N}{B}-1)(2^{e(B)}-1) = (q_0-1) + \sum_{j=1}^{e(B)} q_j 2^{e(B)-j} - (q_0-1)$$

i.e., the weight of AN equals in all cases the weight of the B-period of N/B. The preceding discussion proves the following Lemma:

Lemma 1. - The minimum distance $d_m(B)$ of the code generated by $A = (2^{e(B)-1})/B$ is the minimum of the weights of the B-periods of j/B, $(j = 1,2,\ldots,B-1)$.

We now investigate the dependence of the weights of the B-periods of $j/B (j = 1,\ldots,B-1)$ upon the number theoretic properties of B.

Let $B = \prod_{i=1}^{n} p_i^{\alpha_i}$ and consider the integers in the interval $I_B = [1,B-1]$. Consider now the sequence of the powers of 2 modulo B, i.e., $F \triangleq \{f_j\} = (f_0,f_1,\ldots,f_{e(B)-1})$ where $f_j = 2^j \bmod B$. Then for any integer $a \in I_B$, the sequence $\{af_j\}$ is called the B-orbit of a. To characterize the orbit we distinguish whether a is or is not relatively prime to B. In the former case there are $\varphi(B)$ such integers, where $\varphi(\ )$ is the Euler function. These integers form a multiplicative group ζ, and F is the

subgroup generated by 2. F partitions ζ into cosets, called the local B-orbits.

Consider now an integer $b \in I_B$, relatively prime only to a proper divisor B_1 of B. We have that $b = kB_2$, where $B_1B_2 = B$, and $bf_{e(B_1)} \equiv b$, i.e., the B-orbit of b is periodic with period $e(B_1)$ and is the concatenation of $e(B)/e(B_1)$ copies of $(q_0B_2,\ldots,q_{e(B_1)-1}B_2)$ where $(q_0,\ldots,q_{e(B_1)-1})$ is a local B_1-orbit. The B-orbits of all such b's are called the transferred B-orbits, originated by local B_1-orbits, for proper divisors B_1 of B. This completely describes the orbit structure of B.

It is easily recognized from the definition of B-period of a/B and relation (5) that the weight of the B-period equals the number of integers in the orbit of a belonging to the semiclosed interval $[B/3, 2B/3)$, hereafter denoted as the middle third of B. Since $g \in [B_1/3, 2B_1/3)$ implies $gB_2 \in [B/3, 2B/3)$, $(B_1B_2=B)$ then the number $w_B(a)$ of middle-third elements of the (transferred) B-orbit of a is given by

$$w_B(a) = \frac{e(B)}{e(B_1)} w_{B_1}(a) \tag{6}$$

where $w_{B_1}(a)$ is the number of middle-third elements in the B_1-orbit of a. The number of middle-third elements in the B-orbit of a is conveniently designated as the weight of the B-orbit of a. This is summarized by the following fundamental Theorem.

Theorem 2. - The minimum distance $d_m(B)$ of the code generated by $A = (2^{e(B)}-1)/B$ is the minimum of the weights of the local and transferred B-orbits.

When B is a prime and has either 2 or -2 as its primitive root, we have Barrows-Mandelbaum (1966, 1967) codes. Then $e(B) = B-1$, and there is a single local B-orbit of length B-1, i.e., containing all the positive integers less than B. Hence the B-orbital weight $w_B(j)$ is constant for all $1 \leq j \leq B-1$ and is given by $[(B+1)/3]$. This coincides with the expression for the code minimum distance as found by Barrows.* As is well-known, the rate R(B) of these codes,

$$R(B) = \frac{\log_2 B}{B-1}$$

is rather poor. Hence the Barrows-Mandelbaum codes are characterized by large distance and low rate. Indeed, they correspond to the maximal length sequence polynomial codes (Peterson, 1961). On the other hand, the single error correcting arithmetic codes (Brown, 1960 and Peterson, 1961) correspond to the other extreme case, i.e., the Hamming codes, which have good rate but can correct only one error. Our primary aim is to produce codes that lie between these two extremes, thus achieving reasonable rate and minimum distance at the same time.

---

*If $B = p^r$, (p has 2 as its primitive root), $dm(p^r) = p^{r-2}\left[\frac{p(p-1)}{3}\right]$

III. Search Strategy for Codes

A prime p is called 2-regular (see Chien, 1964) if the exponent of 2 modulo p^2 is different from the exponent of 2 modulo p. There are only two non-2-regular primes less than 10^6, namely 1093 and 3511 (Riesel, 1964). Our attention is confined to 2-regular primes in the sequel, with practically no loss of generality. First, we recall a well-known theorem on the exponent of 2 modulo B, when B is a composite number.

Theorem 3 Let $B = \prod_{i=1}^{n} p_i^{\alpha_i}$ ($\alpha_i \geq 1$ for all i, $2 \nmid B$)[1] and let $e_i = e(p_i)$. The exponent of 2 modulo B, e(B), is given by

$$e(B) = \underset{i}{\text{LCM}} \left[e_i \cdot p_i^{\alpha_i - 1} \right] \tag{7}$$

Since LCM [a,b,c] = LCM [a,LCM[b,c]] and LCM [ab,cd] = ac LCM [b,d] if (a,b) = 1,[2] (c,d) = 1 and (a,c) = 1, one can rewrite Eq. (7) as

$$e(B) = \text{LCM} \left[\prod_{i=1}^{n} p_i^{\alpha_i - 1}, \underset{i}{\text{LCM}} [e_i] \right] \tag{8}$$

Obviously $\underset{i}{\text{LCM}} [e_i] = e \left(\prod_{i=1}^{n} p_i \right)$. We now factor $\underset{i}{\text{LCM}} [e_i]$ as

$$\underset{i}{\text{LCM}} [e_i] = \left(\prod_{i=1}^{n} p_i^{s_i} \right) K \tag{9}$$

where $s_i > 0$ and K is not divisible by and p_i for all i. Thus,

---

[1] a|b denotes "a divides b" and a $\nmid$ b denotes "a does not divide b".
[2] (a,b) denotes the greatest common divisor of a and b.

$$e(B) = \prod_{i=1}^{n} p_i^{\max(\alpha_i - 1, s_i)} \cdot K \tag{10}$$

Given n distinct primes, $p_1, p_2, \ldots,$ and p_n, the exponents s_i's and K are entirely defined by Eq. (9). We call

$$S = S(p_1, p_2, \ldots, p_n) = \prod_{i=1}^{n} p_i^{s_i+1} , \tag{11}$$

the <u>saturation product</u> of the given set of n primes. (S was called <u>Kernel</u> in Chien, 1964). We first remark that $e(S) = K \prod_{i=1}^{n} p_i^{s_i} = e(B)$ for any $B = \prod_{i=1}^{n} p_i^{\alpha_i}$ $(\alpha_i \geq 1)$ that divides S. An additional property of S with reference to its multiples is given by the following theorem.

<u>Theorem 4</u>: If $B = \prod_{i=1}^{n} p_i^{\alpha_i}$ $(\alpha_i \geq 1)$ is a multiple of the saturation product $S(p_1, p_2, \ldots, p_n)$, then i) $e(B) = e(S)\frac{B}{S}$ and ii) the number g(B) of distinct local B-orbits equals g(S).

<u>Proof</u>: Property i) is apparent from Eq. (10). For ii), let $B = \prod_{i=1}^{n} p_i^{s_i+1+\beta_i}$ $(\beta_i \geq 0)$, then

$$g(B) = \frac{\varphi(B)}{e(B)} = \frac{\prod_{i=1}^{n} p_i^{s_i+\beta_i} (p_i - 1)}{\prod_{i=1}^{n} p_i^{s_i+\beta_i} \cdot K} = \frac{\prod_{i=1}^{n} (p_i - 1)}{K} = \frac{\varphi(S)}{e(S)} = g(S) \tag{12}$$

Q.E.D.

The rate R(B) of the code generated by $(2^{e(B)}-1)/B$ is given by

$$R(B) = \frac{\log_2 B}{e(B)} = \frac{\sum_{i=1}^{n} \alpha_i \log_2 p_i}{\prod_{i=1}^{n} p_i^{\max(\alpha_i - 1, s_i)} \cdot K} , \quad (\alpha_i \geq 1) \tag{13}$$

For B ($B = \pi\, p_i^{\alpha_i} (\alpha_i \geq 1)$), a divisor of S, e(B) = e(S), that is, the denominator in Eq. (13) is constant, whence R(B) is maximized for B = S. For B, a multiple of S, with increasing α_i's the denominator of Eq. (13) grows faster than the numerator, whence R(B) is again maximized for B = S. We summarize this formally as a theorem.

Theorem 5: Given a set of odd primes, $p_1, p_2, \ldots, p_n$, $B = S(p_1, p_2, \ldots, p_n)$ generates the maximum rate code in the class of codes generated by $(2^{e(B)}-1)/B$, with $B = \prod_{i=1}^{n} p_i^{\alpha_i}$, $(\alpha_i \geq 1)$.

Theorems 4 and 5 provide general guidelines for the search for "good" arithmetic codes. Let us first consider the codes generated by multiples B of the saturation product S. Since $e(B) = e(S)\frac{B}{S}$ and g(B) = g(S), the weight of the local B orbits is expected to be B/S times as large as the one of the local S-orbits, yielding codes with large distance but low rate. We mention here that a large proportion of these codes (hereafter referred to as "extension codes" and further examined in Section 5) are characterized by the ratio dm(B)/e(B) = dm(S)/e(S).

Let us now consider the codes generated by divisors B of S (such that $B = \prod_{i=1}^{n} p_i^{\alpha_i}, (\alpha_i > 0)$). These codes have all the same length e(S) and increasing efficiency as B approaches S. We notice that as B approaches S, $d_m(B)$ is monotonically nonincreasing. In fact, from Theorem 2, the minimum distance $d_m(B)$ is the minimum of the weights of the local B-orbits and of the transferred B-orbits. The minimum of the weights of the latter set equals $d_m(B_1)$ for some proper divisor B_1 of B, whence

$$d_m(B) \leq d_m(B_1). \qquad (B_1 \text{ divides } B)$$

Since $R(B) > R(B_1)$, the previous relation suggests the possibility that we may gain rate without sacrificing minimum distance (i.e., when $d_m(B) = d_m(B_1)$). Therefore codes with high rate and large minimum distance are to be expected for values of $B = \prod_{i=1}^{n} p_i^{\alpha_i}$ corresponding to choices of $(\alpha_1,\alpha_2,\ldots,\alpha_n)$ close to $(s_1,s_2,\ldots,s_n)$ in the lattice of integers having $(s_1,s_2,\ldots,s_n)$ as its supremum (See table II). This remark provides the rationale underlying the search for codes.

This search requires the actual computation for given B of the minimum distance of the code generated by $(2^{e(B)}-1)/B$. The following remarks are quite useful in order to reduce the computational effort required.

Consider a given $B = \prod_{i=1}^{n} p_i^{\alpha_i}$ $(\alpha_i > 0)$, a divisor of the saturation product $S(p_1,p_2,\ldots,p_n)$. Let $w_{min}(B_j)$ be the minimum of the weights of the local B_j-orbits, where B_j is a divisor of B. Then, according to Theorem 2

$$d_m(B) = \min_{B_j | B} \left\{ w_{min}(B_j) \frac{e(B)}{e(B_j)} \right\}$$

where the minimization is over all divisors B_j of B. The problem therefore reduces to computing $w_{min}(B)$ for given B. The code length, e(B), and the number of distinct local B-orbits, g(B), are given by relations (7) and (12) respectively. One has to generate the local B-orbits and

check the weights in each orbit by counting those elements that are in the middle third of B. We now provide a useful theorem for the determination of $w_{min}(B)$.

First, consider a $B \neq 3$, and any r such that $(r,B) = 1$. Clearly if r is in the middle third of B, -r mod B also is in the middle third of B. On the basis of the following theorem the actual checking effort can be halved.

Theorem 6: The integers r and -r ($1 \leq r < B$, $(r,B) = 1$) belong to distinct B-orbits (having equal weight) if and only if $2^{e(B)/2} + 1 \equiv 0 \bmod B$. Otherwise, the B-orbit they belong to contains r and -r, e(B)/2 positions apart.

Proof: r and -r belong to the same orbit if and only if $-r \equiv r2^k$, $(0 \leq k < e(B))$, i.e., $r(2^k+1) \equiv 0 \bmod B$. Since $(r,B) = 1$, it must be $(2^k+1) \equiv 0$, or, equivalently $2^{2K}-1 \equiv 0 \bmod B$. It follows that e(B) divides 2k, or $k = j\frac{e(B)}{2}$, for some positive j, whence $k = e(B)/2$.

Q.E.D.

We now select the B's to be inspected according to the guidelines provided by theorem 5 and the ensueing discussion. Theorem 2 provides the basic search algorithm to find the minimum distance of the code to the chosen B. The minimum weight of the local B_j-orbits for all the divisors B_j's and B is checked according to theorems 1, 3 and 6. A computer search, programmed on the CDC-1604, produced thousands of codes of various lengths in a reasonable time. For each length and minimum distance the highest rate codes ($R > 1/3$) are presented in Table I.

In Table II, we present codes whose B's have the same prime divisors, to illustrate the point that, indeed, rate improvement is possible without sacrificing minimum distance for those B's that divide the corresponding saturation product.

TABLE I

List of Codes Discovered

Code Length	B	Minimum Distance	Rate (> 1/3)
10	11	4	0.400
12	39	4	0.500
14	43	4	0.429
15	151	4	0.533
18	133	5	0.444
18	667	4	0.556
20	123	6	0.350
20	451	5	0.450
20	3813	4	0.600
21	337	5	0.429
21	2359	4	0.571
22	267	6	0.409
22	15709	4	0.636
24	663	6	0.417
24	1989	5	0.458
24	46995	4	0.667
25	601	7	0.400
25	1801	5	0.440
25	55831	4	0.640
26	2731	4	0.462
28	1247	7	0.393
28	1695	6	0.393
28	24295	5	0.536
28	215265	4	0.643
29	2089	6	0.414
29	486737	4	0.655
30	1661	7	0.367
30	14949	6	0.467
30	71827	5	0.567
30	1649373	4	0.700
33	13788017	4	0.727
34	43691	4	0.471
35	2201	7	0.343
35	122921	6	0.486
35	279527	5	0.543
35	15610967	4	0.686
36	2071	9	0.333
36	24309	8	0.417
36	73815	7	0.472
36	959595	6	0.556
36	4740255	5	0.639
36	123818877	4	0.750

TABLE II

Comparison of Codes with Same Prime Components

Length	Minimum Distance	B	Better B
18	4	3.73	3^2.73
20	4	5.3.11	5^2.3.11
	4	5.3.31	5^2.3.31
21	3	7.127	7^2.127
30	6	3.11.151	3^2.11.151
	3	3.31.151.331	3^2.31.151.331

IV. Extension Codes

We begin this section by investigating the sum W(B) of the weights of the local B-orbit. To this end, we shall introduce some convenient nomenclature. Let $Z(B) \triangleq [\frac{B+1}{3}] = \sum_{B_1 | B} W(B_1)$. Next, since $B = \prod_{i=1}^{n} p_i^{\alpha_i}$ $(\alpha_i \geq 1)$, we represent B as an ordered n-tuple of exponents of p_i's, i.e., $B \equiv (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Thus B and all its divisors are represented as an n-dimensional lattice. If $B_1 | B$, $B_1 \equiv (\beta_1, \beta_2, \ldots, \beta_n)$ with $\beta_i \leq \alpha_i$ for all i, and we denote this as $B_1 \subseteq B$ ("B covers B_1"). Let $B_o \equiv (\alpha_1 - 1, \alpha_2 - 1, \ldots, \alpha_n - 1)$. B and B_o clearly defines a unit-n-cube C, with l.u.b. = B and g.l.b. = B_o. When a point $P \in C$, $P \equiv (\alpha_1 - b_1, \alpha_2 - b_2, \ldots, \alpha_n - b_n)$ and $b_i = 1$ or 0 for all i. Let $h(P) = \sum_{i=1}^{n} b_i$, i.e., the Hamming weight of the vector $(b_1, b_2, \ldots, b_n)$. Now,

$$Z(B) = [\frac{B+1}{3}] = \sum_{B_i \subseteq B} W(B_i),$$

or, equivalently,

$$W(B) = Z(B) - \sum_{B_i \subset B} W(B_i) .$$

Iterating this expression we see that the only points contributing to W(B), are the points in C, and they give positive or negative contribution to W(B) depending on whether they differ from B in even or odd number of coordinates, respectively. Therefore, from the definition of h(P),

$$W(B) = \sum_{P \in C} (-1)^{h(P)} Z(P) . \tag{14}$$

We now obtain a convenient expression for Z(P). First, assume that 3

does not divide B, so each p_i can be expressed as $p_i = 3n_i + (-1)^{\delta i}$ with $\delta_i = 0$ or 1.

$$Z(B) = \left[\frac{B+1}{3}\right] = \left[\frac{1}{3}\left(\prod_{i=1}^{n}(3n_i+(-1)^{\delta_i})^{\alpha_i} + 1\right)\right]$$

$$= \left[\frac{1}{3}\left(\prod_{i=1}^{n}\left(\sum_{j=0}^{\alpha_i}\binom{\alpha_i}{j}(3n_i)^{\alpha_i-j}(-1)^{\alpha_i j}\right) + 1\right)\right].$$

When the product is expanded, each term is divisible by three except $\prod_{i=1}^{n}(-1)^{\delta_i\alpha_i}$, whence

$$Z(B) = \frac{1}{3}\prod_{i=1}^{n}p_i^{\alpha_i} - \frac{1}{3}\prod_{i=1}^{n}(-1)^{\delta_i\alpha_i} + \left[\frac{\prod_{i=1}^{n}(-1)^{\delta_i\alpha_i}+1}{3}\right]$$

Since $\prod_{i=1}^{n}(-1)^{\delta_i\alpha_i} = \pm 1$, the third term clearly equals zero. Substituting α_i for $\alpha_i - b_i$, we obtain Z(P), as

$$Z(P) = \frac{B}{3}\prod_{i=1}^{n}\left(\frac{1}{p_i}\right)^{b_i} - \frac{1}{3}(-1)^{\sum_{i=1}^{n}\delta_i\alpha_i}\prod_{i=1}^{n}(-1)^{\delta_i\alpha_i} \tag{15}$$

From Eqs. (14) and (15),

$$W(B) = \frac{B}{3}\sum_{b_i}^{*}\left\{(-1)^{\sum_{i=1}^{n}b_i}\prod_{i=1}^{n}\left(\frac{1}{p_i}\right)^{b_i}\right\} - \frac{(-1)^{\sum_{i=1}^{n}\delta_i\alpha_i}}{3}\sum_{b_i}^{*}\left\{(-1)^{\sum_{i=1}^{n}b_i}\prod_{i=1}^{n}(-1)^{\delta_i b_i}\right\}$$

$$= \frac{B}{3}\sum_{b_i}^{*}\left\{\prod_{i=1}^{n}\left(\frac{-1}{p_i}\right)^{b_i}\right\} - \frac{(-1)^{\sum_{i=1}^{n}\delta_i\alpha_i}}{3}\cdot\sum_{b_i}^{*}\left\{\prod_{i=1}^{n}(-1)^{(1+\delta_i)b_i}\right\} \tag{16}$$

where $\sum_{b_i}^{*}$ means that the sum is over all the binary n-tuples $(b_1, b_2, \ldots, b_n)$.

We recognize now

$$\sum_{b_i}^{*} \{ \prod_{i=1}^{n} (\frac{-1}{P_i})^{b_i} \} = \prod_{i=1}^{n} (1 - \frac{1}{P_i})$$

and likewise

$$\sum_{b_i}^{*} \{ \prod_{i=1}^{n} ((-1)^{1+\delta_i})^{b_i} \} = \prod_{i=1}^{n} (1+(-1)^{1+\delta_i})$$

which is 2^n if and only if $\delta_i = 1$ for all i, and zero otherwise. Thus we obtain from Eq. (16),

$$W(B) = \frac{\varphi(B)}{3} - \frac{2^n}{3} (-1)^{\sum_{i=1}^{n} \alpha_i} \quad \text{if } \delta_i = 1 \text{ for all i and} \tag{17}$$

$$W(B) = \frac{\varphi(B)}{3} \quad \text{if some } \delta_i = 0. \tag{18}$$

Now assume that 3 divides B. We let $P_n = 3$ without loss of generality.

$$Z(P) = [\frac{1}{3}(3^{\alpha_n - b_n} \prod_{i=1}^{n-1} P_i^{\alpha_i - b_i} + 1)].$$

Clearly $Z(P) = 3^{\alpha_n - b_n - 1} \left\{ \prod_{i=1}^{n-1} P_i^{\alpha_i - b_i} \right\}$ for $P \in C$ and $\alpha_n \geq 2$, which in turn leads to $W(B) = \frac{\varphi(B)}{3}$. If now $\alpha_n = 1$, we partition C into D and D^c, such that if $P \in D$, $b_n = 0$ and if $P \in D^c$, $b_n = 1$. We have,

$$Z(P) \begin{cases} = \frac{1}{3} \prod_{i=1}^{n-1} p_i^{(\alpha_i - b_i)} - \frac{1}{3} \prod_{i=1}^{n-1} (-1)^{\delta_i (\alpha_i - b_i)} & \text{if } P \in D^c \\ = \prod_{i=1}^{n-1} p_i^{(\alpha_i - b_i)} & \text{if } P \in D \end{cases}$$

Rewriting Eq. (14) we get

$$W(B) = \sum_{P\in D^c} (-1)^{h(P)} Z(P) + \sum_{P\in D} (-1)^{h(P)} Z(P)$$

Note that D^c is a unit-(n-1)-cube, and since $\prod_{i=1}^{n-1} p_i^{\alpha_i}$ is not divisible by 3, the first sum is $(-1)^{b_n} W(\frac{B}{3}) = -W(\frac{B}{3})$ (since $b_n=1$ if $P\in D^c$) to which the relations (17) and (18) apply. The second term is given by

$$(-1)^{b_n} \sum_{b_i\neq b_n}^{*} \{ \prod_{i=1}^{n-1} p_i^{\alpha_i} \prod_{i=1}^{n-1} (\frac{-1}{P_i})^{b_i} \} = \varphi(\frac{B}{3})$$

Observing that $\varphi(\frac{B}{3}) = \frac{\varphi(B)}{2}$ for $\alpha_n = 1$, we readily obtain, for $\alpha_n=1 (P_n=3)$, and $\delta_i=1$ for all $i\neq n$,

$$W(B) = \frac{\varphi(B)}{2} - \frac{1}{3}\frac{\varphi(B)}{2} + \frac{(-1)^{\sum_{i=1}^{n-1}\alpha_i}}{3} 2^{n-1}$$

$$= \frac{\varphi(B)}{3} + \frac{2^{n-1}}{3}(-1)^{\sum_{i=1}^{n-1}\alpha_i}$$

$$= \frac{\varphi(B)}{3} - \frac{2^{n-1}}{3}(-1)^{\sum_{i=1}^{n}\alpha_i}$$

Summarizing these as a theorem, we have

Theorem 7: W(B), the sum of all the weights of distinct local B-orbits of $B = \prod_{i=1}^{n} p_i^{\alpha_i}$ ($\alpha_i \geq 1$):

i) $W(B) = \frac{\varphi(B)}{3} - \frac{2^n}{3}(-1)^{\sum_{i=1}^{n}\alpha_i}$ if $p_i = 3n_i - 1$ for all i

ii) $W(B) = \frac{\varphi(B)}{3} - \frac{2^{n-1}}{3}(-1)^{\sum_{i=1}^{n}\alpha_i}$ if $p_n = 3$, $\alpha_n = 1$ and $p_i = 3n_i - 1$ $\forall i \neq n$

iii) $W(B) = \frac{\varphi(B)}{3}$ otherwise.

The third case of above theorem is of particular interest. Most odd numbers are in this category and this is the case when we can easily determine the minimum distance for B's that are divisible by the saturation product, S, as will be shown in the sequel.

First we extend the concept of saturation with respect to a subset of the prime factors of a number T. Relabelling the indices when necessary $T = \prod_{i=1}^{n} p_i^{\alpha_i}$ is said to be <u>saturated</u> with respect to the primes $p_1, p_2, \ldots, p_m$ if $\alpha_i \geq s_i + 1$ for $i = 1,2,\ldots m$ and $1 \leq \alpha_i \leq s_i$ for $i = m + 1,\ldots,n$. From (9) and (10) we readily obtain the following properties:

<u>Property 1</u>: If $T = \prod_{i=1}^{n} p_i^{\alpha_i}$ is saturated with respect to $P_1, P_2, \ldots,$ and P_m, then i) $e(T \cdot \prod_{i=1}^{m} p_i^{\beta_i}) = e(T) \prod_{i=1}^{m} p_i^{\beta_i}$ and ii) $g(T \cdot \prod_{i=1}^{m} p_i^{\beta_i}) = g(T)$

Consider a T saturated with respect to P_1. For both T and p_1T, the number of local orbits is $g(T) = g(p_1 \cdot T) = \varphi(T)/e(T)$. Consider an element b of a local T-orbit. Then $b2^{je(T)} \equiv \gamma_j T + b \bmod p_1 T$, where $0 \leq \gamma_j < p_1$ for every j. The fact that $e(P_1T) = P_1 e(T)$ is the smallest positive integer solution for $2^x \equiv 1 \bmod p_1 T$, shows that $\gamma_i \neq \gamma_j$ if $i \not\equiv j \bmod p_1$. Therefore to each element b of a local T-orbit there

correspond p_1 elements of the form $b + jT$ in a local p_1T-orbit. This yields:

Property 2: If T is saturated with respect to P_1, to any local T-orbit with members $\{b_0, b_1, \ldots, b_{e-1}\}$, there corresponds a unique local P_1T-orbit with members $\{b_i+nT \mid 0 \leq i < e(T),\ 0 \leq n < P_1\}$.

Now label the weights of all the distinct local T-orbits as $w_i(T)$ for all $1 \leq i \leq g(T)$. When T is partially saturated in terms of $P_1 = 3$, $w_i(P_1T) = e(T)$ for all i, by Property 2. If $P_1 = 3n_1+(-1)^{\delta}$ ($\delta = 1$ or 0), the number ℓ contributes to the weight of local P_1T-orbit only if $n_1T + \frac{T}{3}(-1)^{\delta} \leq \ell < 2n_1T + \frac{2T}{3}(-1)^{\delta}$. Therefore $w_i(P_1T) = n_1e(T) + (-1)^{\delta} w_i(T) = \frac{e(P_1T)}{3} + (-1)^{\delta}\{w_i(T) - \frac{e(T)}{3}\}$ for every i. When $T = \prod_{i=1}^{n} p_i^{\alpha_i}$ is saturated with respect to $P_1, P_2, \ldots, P_m$, one can apply the previous result repeatedly and obtain,

Theorem 8: Let $T = \prod_{i=1}^{n} p_i^{\alpha_i}$ be partially saturated with respect to $P_1, P_2, \ldots, P_m$ ($m \leq n$) and let $w_i(T)$ be known for all $1 \leq i \leq g(T)$. Then for $B = T \cdot \prod_{i=1}^{m} p_i^{\beta_i}$ the weights of local B-orbits become for every i

(19) $w_i(B) = \frac{e(B)}{3}$ if 3 is one of the p_i's saturated

(20) $w_i(B) = \frac{e(B)}{3} + (-1)^{\sum_{i=1}^{m} \delta_i \beta_i}\{w_i(T) - \frac{e(T)}{3}\}$ if $p_i = 3n_i+(-1)^{\delta_i}$ for all i

$\delta_i = 1$ or 0.

Now we can easily find the minimum weight of all the local B-orbits. For Eq. (19), it is trivial, and for Eq. (20), $w_{min}(B)$ results from $w_{min}(T)$ or $w_{max}(T)$ depending upon whether $\sum_{i=1}^{m} \delta_i \beta_i$ is even or odd,

respectively. Thus the knowledge of $w_{min}(T)$ and $w_{max}(T)$ is sufficient to find the minimum local orbital weights beyond the (partial) saturation product, without actually generating the local orbits and checking their weights.

Consider now $T = \prod_{i=1}^{n} p_i^{\alpha_i}$ saturated with respect to $p_1, p_2, \ldots, p_m$ $(1 \leq m \leq n)$, and assume that, for every $i \leq m$ either, $p_i = 3n_i + 1$ or $p_i = 3$ if 3^2 divides T (this falls in case iii) of theorem 7). Let $B = T \cdot \prod_{i=1}^{m} p_i^{\beta_i}$ and let $d_m(T)$ be known. We can now prove the following conclusive theorem:

Theorem 9: Let $T = \prod_{i=1}^{n} P_i^{\alpha_i}$ be saturated with respect to $P_1, P_2, \ldots, P_m$ $(1 \leq m \leq n)$, where for all $1 \leq i \leq m$, $P_i = 3n_i+1$ or 3 if 3^2 divides T. Then for $B = T \cdot \prod_{i=1}^{m} p_i^{\beta_i}$, $d_m(B) = dm(T) \prod_{i=1}^{m} p_i^{\beta_i}$.

Proof: We must show that for every divisor B_j of B that does not divide T, there exist a divisor T_j of T such that $w_{min}(B_j) \geq w_{min}(T_j)\frac{e(B_j)}{e(T_j)}$. Any such B_j can be expressed (perhaps relabelling the indices each time) as $B_j = \prod_{i=1}^{k} p_i^{\alpha_i+a_i} \cdot \prod_{i=k+1}^{n} p_i^{\gamma_i}$ where $1 \leq k \leq m$, $1 \leq a_i \leq \beta_i$ and $\gamma_i \leq \alpha_i$ for all i. Let $T_j = \prod_{i=1}^{k} p_i^{\alpha_i} \cdot \prod_{i=k+1}^{n} p_i^{\gamma_i}$. Obviously T_j is a divisor of T and hence $dm(T) \leq w_{min}(T_j)\frac{e(T)}{e(T_j)}$. First, notice that any such B_j and T_j also belongs to the case iii) of theorem 7. Therefore,

$$w_{min}(T_j) \leq w_{avg}(T_j) = \frac{W(T_j)}{g(T_j)} = \frac{e(T_j)}{3} \leq w_{max}(T_j)$$

Notice also that T_j is saturated with respect to $P_1, P_2, \ldots, P_k$, whence by theorem 8, we have

i) If 3 is one of the saturated primes

$$w_{min}(B_j) = \frac{e(B_j)}{3} = \frac{e(T_j)}{3} \prod_{i=1}^{k} p_i^{a_i} \geq w_{min}(T_j) \prod_{i=1}^{k} p_i^{a_i}$$

ii) Otherwise ($\delta_i = 0$ for all $1 \leq i \leq k$)

$$w_{min}(B_j) = \frac{e(B_j)}{3} + w_{min}(T_j) - \frac{e(T_j)}{3} \geq w_{min}(T_j) \prod_{i=1}^{k} p_i^{a_i} .$$

Hence for both cases $w_{min}(B_j) \geq w_{min}(T_j) \frac{e(B_j)}{e(T_j)}$.

Q.E.D.

V. Conclusion

The reported research, contributes in filling the spectrum of arithmetic codes between the two extreme cases of single-error-correcting Brown Codes and the maximal-sequence-like Barrows-Mandelbaum Codes. The direct conversion algorithm and the study of orbits are shown to be valuable tools in analyzing the structure of such codes. The underlying structure reveals a number of interesting aspects of the multiple error correcting arithmetic codes. The analysis indicates where "good" codes are to be expected and how to calculate their minimum distance. A class of large-minimum-distance codes is also presented, whose rate is higher than that of the Barrows-Mandelbaum codes.

The decoding problem essentially remains unsolved even though some preliminary results have recently been presented (Laste and Tsao-Wu, 1969). However, further research based on the orbit structure of B seems to be very promising.

References

Avzienis, A., "A Study of the Effictiveness of Fault-Detecting Codes for Binary Arithmetic," Technical Report No. 32-711, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, September, 1965.

Barrows, J. T. Jr., "A New Method for Constructing Multiple Error Correcting Linear Residue Codes," Report R-277, Coordinated Science Laboratory, University of Illinois, Urbana, Illinois, January, 1966.

Bernstein, A. J., "Theory of Computational Error Correcting Codes for Arithmetic Units," Thesis, Columbia University, New York, N.Y., 1962.

Bernstein, A. J. and Kim, W. H. (1962), "Linear Codes for Single Error Correction in Symmetric and Asymmetric Computational Processes," IRE Trans. Vol. IT-8, pp. 29-34.

Brown, D. T., (1960), "Error Detecting and Correcting Binary Codes for Arithmetic Operations," IRE Trans. Vol. EC-9, pp. 333-337.

Chang, S. H. and Tsao-Wu, N. T., (1968), "Discussion on Arithmetic Codes with Large Distance," IEEE PGIT-14, pp. 174-175.

Chien, R. T., (1964), "Linear Residue Codes for Burst Error Correction," IEEE Trans. on Information Theory, Vol. IT-10, pp. 127-133.

Chien, R. T., Hong, S. J. and Preparata, F. P., "Some Contribution to the Theory of Arithmetic Codes," Proceedings of the First Annual Hawaii International Conference on Systems Sciences, January, 1968.

Diamond, J. M., (1955), "Checking Codes for Digital Computers," Proceedings of IRE, Vol. 43, pp. 487-488.

Henderson, D. S., "Residue-Class Error Checking Codes," Presented at the 16th National Meeting of the ACM, September, 1961.

Laste, E. R. and Tsao-Wu, N. T., (1969), "The Decoding of Arithmetic Cyclic Codes by Permutation of Residue," Proceedings of Princeton Conference on Information Sciences and Systems.

MacSorley, O. L., (1961), "High-Speed-Arithmetic in Binary Computers," Proceedings of IRE. pp. 67-91.

Mandelbaum, D., (1965), "Arithmetic Error Detecting Codes for Communication Links Involving Computers," IEEE Trans. on Communication Technology, Vol. Com. 13, pp. 165-171.

Mandelbaum, D., (1967), "Arithmetic Codes with Large Distance," IEEE Trans. on Information Theory, Vol. IT-13, No. 2.

Massey, (1964), "Survey of Residue Coding for Arithmetic Errors," International Computation Center Bulletin, UNESCO, Rome, Italy.

Metze, G., (1962), "A Class of Binary Divisions Yielding Minimally Represented Quotients," IRE Trans. on Electronic Computers.

Peterson, W. W., "Error Correcting Codes," John Wiley & Sons, Inc., New York, N. Y., 1961, Chapter 13.

Reitwiesner, G. H., "Binary Arithmetic," in Advances in Computers, Vol. 1, edited by F. L. Alt, Academic Press, New York, N.Y., 1960, pp. 232-308.

Riesel, H., (1964), "Note on the Congruence $a^{p-1} \equiv 1 \bmod p^2$," Mathematics of Computation, 18, pp. 149-150.

Robertson, T. E., (1967), "The Correspondence Between Methods of Digital Division and Multiplier Recoding Procedures," Report No. 252, Department of Computer Sciences, University of Illinois, Urbana, Illinois.

Robertson, J. R., (1958), "A New Class of Digital Division Methods," IRE Transactions on Electronic Computers.

Stein, J. J., (1962), "Prime Residue Error Correcting Codes," IEEE Trans. on Information Theory, Vol. IT-9, p. 170.

Wilson, J. B. and Ledley, R. S., (1961), "An Algorithm for Rapid Binary Division," IRE Transaction on Electronic Computers.

Distribution List as of April 1, 1969

Dr A.A. Dougal
Asst Director (Research)
Ofc of Defense Res & Eng
Department of Defense
Washington, D.C. 20301

Office of Deputy Director
(Research and Information, Rm 3D1037)
Department of Defense
The Pentagon
Washington, D.C. 20301

Director, Advanced Research Projects
Agency
Department of Defense
Washington, D.C. 20301

Director for Materials Sciences
Advanced Research Projects Agency
Department of Defense
Washington, D.C. 20301

Headquarters
Defense Communications Agency (340)
Washington, D.C. 20305

Defense Documentation Center
Attn: DDC-TCA
Cameron Station
Alexandria, Virginia 22314 (50 Copies)

Director
National Security Agency
Attn: TDL
Fort George G. Meade, Maryland 20755

Weapons Systems Evaluation Group
Attn: Colonel Blaine O. Vogt
400 Army-Navy Drive
Arlington, Virginia 22202

Central Intelligence Agency
Attn: OCR/DD Publications
Washington, D.C. 20505

Hq USAF (AFRDD)
The Pentagon
Washington, D.C. 20330

Hq USAF (AFRDDG)
The Pentagon
Washington, D.C. 20330

Hq USAF (AFRDSD)
The Pentagon
Washington, D.C. 20330

Colonel E.P. Gaines, Jr.
ACDA/FO
1901 Pennsylvania Ave N.W.
Washington, D.C. 20451

Lt Col R.B. Kalisch (SREE)
Chief, Electronics Division
Directorate of Engineering Sciences
Air Force Office of Scientific Research
Arlington, Virginia 22209

Dr I.R. Mirman
AFSC (SCT)
Andrews Air Force Base, Maryland 20331

AFSC (SCTSE)
Andrews Air Force Base, Maryland 20331

Mr Morton M. Pavane, Chief
AFSC Scientific and Technical Liaison Office
26 Federal Plaza, Suite 1313
New York, New York 10007

Rome Air Development Center
Attn: Documents Library (EMTLD)
Griffiss Air Force Base, New York 13440

Mr H.E. Webb (EMMIIS)
Rome Air Development Center
Griffiss Air Force Base, New York 13440

Dr L.M. Hollingsworth
AFCRL (CRN)
L.G. Hanscom Field
Bedford, Massachusetts 01730

AFCRL (CRMPLR), Stop 29
AFCRL Research Library
L.G. Hanscom Field
Bedford, Massachusetts 01730

Hq ESD (ESTI)
L.G. Hanscom Field
Bedford, Massachusetts 01730 (2 copies)

Professor J. J. D'Azzo
Dept of Electrical Engineering
Air Force Institute of Technology
Wright-Patterson AFB, Ohio 45433

Dr H.V. Noble (CAVT)
Air Force Avionics Laboratory
Wright-Patterson AFB, Ohio 45433

Director
Air Force Avionics Laboratory
Wright-Patterson AFB, Ohio 45433

AFAL (AVTA/R.D. Larson
Wright-Patterson AFB, Ohio 45433

Director of Faculty Research
Department of the Air Force
U.S. Air Force Academy
Colorado Springs, Colorado 80840

Academy Library (DFSLB)
USAF Academy
Colorado Springs, Colorado 80840

Director
Aerospace Mechanics Division
Frank J. Seiler Research Laboratory (OAR)
USAF Academy
Colorado Springs Colorado 80840

Director, USAF PROJECT RAND
Via: Air Force Liaison Office
The RAND Corporation
Attn: Library D
1700 Main Street
Santa Monica, California 90045

Hq SAMSO (SMTTA/Lt Nelson)
AF Unit Post Office
Los Angeles, California 90045

Det 6, Hq OAR
Air Force Unit Post Office
Los Angeles, California 90045

AUL3T-9663
Maxwell AFB, Alabama 36112

AFETR Technical Library
(ETV,MU-135)
Patrick AFB,Florida 32925

ADTC (ADBPS-12)
Eglin AFB, Florida 32542

Mr B.R. Locke
Technical Adviser, Requirements
USAF Security Service
Kelly Air Force Base, Texas 78241

Hq AMD (AMR)
Brooks AFB, Texas 78235

USAFSAM (SMKOR)
Brooks AFB, Texas 78235

Commanding General
Attn: STEWS-RE-L, Technical Library
White Sands Missile Range
New Mexico 88002 (2 copies)

Hq AEDC (AETS)
Attn: Library/Documents
Arnold AFS, Tennessee 37389

European Office of Aerospace Research
APO New York 09667

Phsical & Engineering Sciences Division
U.S. Army Research Office
3045 Columbia Pike
Arlington, Virginia 22204

Commanding General
U.S. Army Security Agency
Attn: IARD-T
Arlington Hall Station
Arlington, Virginia 22212

Commanding General
U.S. Army Materiel Command
Attn: AMCRD-TP
Washington, D.C. 20315

Technical Director (SMUFA-A2000-107-1)
Frankford Arsenal
Philadelphia, Pennsylvania 19137

Redstone Scientific Information Center
Attn: Chief, Document Section
U.S. Army Missile Command
Redstone Arsenal, Alabama 35809

Commanding General
U.S. Army Missile Command
Attn: AMSMI-REX
Redstone Arsenal, Alabama 35809

Commanding General
U.S. Army Strategic Communications Command
Attn: SCC-CG-SAE
Fort Huachuca, Arizona 85613

Commanding Officer
Army Materials and Mechanics Res. Center
Attn: Dr N. Priest
Watertown Arsenal
Watertown, Massachusetts 02172

Commandant
U.S. Army Air Defense School
Attn: Missile Science Division, C&S Dept
P.O. Box 9390
Fort Bliss, Texas 79916

Commandant
U.S. Army Command & General Staff College
Attn: Acquisitions, Library Division
Fort Leavenworth, Kansas 66027

Commanding Officer
U.S. Army Electronics R&D Activity
White Sands Missile Range, New Mexico 88002

Mr Norman J. Field, AMSEL-RD-S
Chief, Office of Science & Technology
Research and Development Directorate
U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Commanding Officer
Harry Diamond Laboratories
Attn: Dr Berthold Altman (AMXDO-TI)
Connecticut Avenue and Van Ness St N.W.
Washington, D.C. 20438

Director
Walter Reed Army Institute of Research
Walter Reed Army Medical Center
Washington, D.C. 20012

Commanding Officer (AMXRD-BAT)
U.S. Army Ballistics Research Laboratory
Aberdeen Proving Ground
Aberdeen, Maryland 21005

Technical Director
U.S. Army Limited War Laboratory
Aberdeen Proving Ground
Aberdeen, Maryland 21005

Commanding Officer
Human Engineering Laboratories
Aberdeen Proving Ground
Aberdeen, Maryland 21005

U.S. Army Munitions Command
Attn: Science & Technology Br. Bldg 59
Picatinny Arsenal, SMUPA-VA6
Dover, New Jersey 07801

U.S. Army Mobility Equipment Research
and Development Center
Attn: Technical Document Center, Bldg 315
Fort Belvoir, Virginia 22060

Director
U.S. Army Engineer Geodesy,
Intelligence & Mapping
Research and Development Agency
Fort Belvoir, Virginia 22060

Dr Herman Robl
Deputy Chief Scientist
U.S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

Richard O. Ulsh (CRDARD-IPO)
U.S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

Mr Robert O. Parker, AMSEL-RD-S
Executive Secretary, JSTAC
U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Commanding General
U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703
Attention:AMSEL-SC
RD-GF
RD-MT
XL-D
XL-E
XL-C
XL-S (Dr R. Buser)
HL-CT-DD
HL-CT-R
HL-CT-L (Dr W.S. McAfee)
HL-CT-O
HL-CT-I
HL-CT-A
NL-D
NL-A
NL-P
NL-P-2 (Mr D. Haratz)
NL-R (Mr R. Kulinyi)
NL-S
KL-D
KL-E
KL-S (Dr H. Jacobs)
KL-SM (Drs Schiel/Hieslmair)
KL-T
VL-D
VL-F (Mr R.J. Niemela)
WL-D
1 copy to each symbol listed individually addressed

Dr A.D. Schnitzler, AMSEL-HL-NVII
Night Vision Laboratory, USAECOM
Fort Belvoir, Virginia 22060

Dr G.M. Janney, AMSEL-HL-NVOR
Night Vison Laboratory,USAECOM
Fort Belvoir, Virginia 22060

Atmospheric Sciences Office
Atmospheric Sciences Laboratory
White Sands Missile Range
New Mexico 88002

Missile Electronic Warfare,
Technical Area, AMSEL-WT-MI
White Sands Missile Range
New Mexico 88002

Project Manager
Commcn Positioning & Navigation Systems
Attn: Harold H. Bahr (AMCPM-NS-TM), Bldg 439
U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Director, Electronic Programs
Attn: Code 427
Department of the Navy
Washington, D.C. 20360

Commander
U.S. Naval Security Group Command
Attn: G43
3801 Nebraska Avenue
Washington, D.C. 20390

Director
Naval Research Laboratory
Washington, D.C. 20390
Attn: Code 2027 6 copies
Dr W.C. Hall, Code 7000 1 copy
Dr A. Brodizinsky, Sup.Elec Div. 1 copy

Dr G.M.R. Winkler
Director, Time Service Division
U.S. Naval Observatory
Washington, D.C. 20390

Naval Air Systems Command
AIR 03
Washington, D.C. 20360 2 copies

Naval Ship Systems Command
Ship 031
Washington, D.C. 20360

Naval ship Systems Command
Ship 035
Washington, D.C. 20360

U.S. Naval Weapons Laboratory
Dahlgren, Virginia 22448

Naval Electronic Systems Command
ELEX 03, Room 2046 Munitions Building
Department of the Navy
Washington, D.C. 20360 (2 copies)

Commander
Naval Electronics Laboratory Center
Attn: Library
San Diego, California 92152 (2 copies)

Deputy Director and Chief Scientist
Office of Naval Research Branch Office
1030 Est Gree Street
Pasadena, California 91101

Library (Code2124)
Technical Report Section
Naval Postgraduate School
Monterey, California 93940

Glen A. Myers (Code 52Mv)
Assoc Professor of Elec. Engineering
Naval Postgraduate School
Monterey, California 93940

Commanding Officer and Director
U.S. Naval Underwater Sound Laboratory
Fort Trumbull
New London, Connecticut 06840

Commanding Officer
Naval Avionics Facility
Indianapolis, Indiana 46241

Dr H. Harrison, Code RRE
Chief, Electrophysics Branch
National Aeronautics & Space Admin.
Washington, D.C. 20546

NASA Lewis Research Center
Attn: Library
21000 Brookpark Road
Cleveland, Ohio 44135

Los Alamos Scientific Laboratory
Attn: Report Library
P.O. Box 1663
Los Alamos, New Mexico 87544

Federal Aviation Administration
Attn: Admin Stds Div (MS-110)
800 Independence Ave S.W.
Washington, D.C. 20590

Head, Technical Services Division
Naval Investigative Service Headquarters
4420 North Fairfax Drive
Arlington, Virginia 22203

Commander
U.S. Naval Ordnance Laboratory
Attn: Librarian
White Oak, Maryland 21502 (2 copies)

Commanding Officer
Office of Naval Research Branch Office
Box 39 FPO
New York, New York 09510

Commanding Officer
Office of Naval Research Branch Office
219 South Dearborn Street
Chicago, Illinois 60604

Commanding Officer
Office of Naval Research Branch Office
495 Summer Street
Boston, Massachusetts 02210

Commander (ADL)
Naval Air Development Center
Johnsville, Warminster, Pa 18974

Commanding Officer
Naval Training Device Center
Orlando, Florida 32813

Commander (Code 753)
Naval Weapons Center
Attn: Technical Library
China Lake, California 93555

Commanding Officer
Naval Weapons Center
Corona Laboratories
Attn: Library
Corona, California 91720

Commander, U.S. Naval Missile Center
Point Mugu, California 93041

W.A. Eberspacher, Associate Head
Systems Integration Division
Code 5340A, Box 15
U.S. Naval Missile Center
Point Mugu, California 93041

Mr M. Zane Thornton, Chief
Network Engineering, Communications
and Operations Branch
Lister Hill National Center for
Biomedical Communications
8600 Rockville Pike
Bethesda, Maryland 20014

U.S. Post Office Department
Library - Room 1012
12th & Pennsylvania Ave, N.W.
Washington, D.C. 20260

Director
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

Mr Jerome Fox, Research Coordinator
Polytechnic Institute of Brooklyn
55 Johnson Street
Brooklyn, New York 11201

Director
Columbia Radiation Laboratory
Columbia University
538 West 120th Street
New York, New York 10027

Director
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois 61801

Director
Stanford Electronics Laboratories
Stanford University
Stanford, California 94305

Director
Microwave Physics Laboratory
Stanford University
Stanford, California 94305

Director, Electronics Research Laboratory
University of California
Berkeley, California 94720

Director
Electronic Sciences Laboratory
University of Southern California
Los Angeles, California 90007

Director
Electronics Research Center
The University of Texas at Austin
Austin Texas 78712

Division of Engineering and Applied Physics
210 Pierce Hall
Harvard University
Cambridge, Massachusetts 02138

Dr G.J. Murphy
The Technological Institute
Northwestern University
Evanston, Illinois 60201

Dr John C. Hancock, Head
School of Electrical Engineering
Purdue University
Lafayette, Indiana 47907

Dept of Electrical Engineering
Texas Technological College
Lubbock, Texas 79409

Aerospace Corporation
P.O. Box 95085
Los Angeles, California 90045
Attn: Library Acquisitions Group

Proffessor Nicholas George
California Inst of Technology
Pasadena, California 91109

Aeronautics Library
Graduat Aeronautical Laboratories
California Institute of Technology
1201 E. California Blvd
Pasadena, California 91109

The John Hoplins University
Applied Physics Laboratory
Attn: Document Librarian
8621 Georgia Avenue
Silver Spring, Maryland 20910

Raytheon Company
Attn: Librarian
Bedford, Massachusetts 01730

Raytheon Company
Research Division Library
28 Seyon Street
Waltham, Massachusetts 02154

Dr Sheldon J. Wells
Electronic Properties Information Center
Mail Station E-175
Hughes Aircraft Company
Culver City, California 90230

Dr Robert E. Fontana
Systems Research Laboratories Inc.
7001 Indian Ripple Road
Dayton, Ohio 45440

Nuclear Instrumentation Group
Bldg 29, Room 101
Lawrence Radiation Laboratory
University of California
Berkeley, California 94720

Sylvania Electronic Systems
Applied Research Laboratory
Attn: Documents Librarian
40 Sylvan Road
Waltham, Massachusetts 02154

Hollander Associates
P.O. Box 2276
Fullerton, California 92633

Illinois Institute of Technology
Dept of Electrical Engineering
Chicago, Illinois 60616

The University of Arizona
Dept of Electrical Engineering
Tucson, Arizona 85721

Utah State University
Dept Of Electrical Engineering
Logan, Utah 84321

Case Institute of Technology
Engineering Division
University Circle
Cleveland, Ohio 44106

Hunt Library
Carnegie-Mellon University
Schenley Park
Pittsburgh, Pennsylvania 15213

Dr Leo Youns
Stanford Research Institute
Menlo Park, California 94025

School of Engineering Sciences
Arizona State University
Tempe, Arizona 85281

Engineering & Mathmatical Sciences Library
University of California at Los Angeles
405 Hilgred Avenue
Los Angeles, California 90024

The Library
Government Publications Section
University of California
Santa Barbara, California 93106

Carnegie Institute of Technology
Electrical Engineering Department
Pittsburgh, Pennsylvania 15213

Professor Joseph E. Rowe
Chairman, Dept of Electrical Engineering
The University of Michigan
Ann Arbor, Michigan 48104

New York University
College of Engineering
New York, New York 10019

Syracuse University
Dept of Electrical Engineering
Syracuse, New York 13210

Yale University
Engineering Department
New Haven, Connecticut 06520

Airborne Instruments Laboratory
Deerpark, New York 11729

Raytheon Company
Attn: Librarian
Bedford, Massachusetts 01730

Lincoln Laboratory
Massachusetts Institute of Technology
Lexington, Massachusetts 02173

The University of Iowa
The University Libraries
Iowa City, Iowa 52240

Lenkurt Electric Co,Inc
1105 County Road
San Carlos, California 94070
Attn: Mr E.K. Peterson

Philco Ford Corporation
Communications & Electronics Div.
Union Meeting and Jolly Rods
Blue Bell, Pennsylvania 19422

Union Carbide Corporation
Electronic Division
P.O. Box 1209
Mountain View, California 94041

Electromagnetic Compatibility Analysis Center
(ECAC), Attn: ACLP
North Severn
Annapolis, Maryland 21402

Director
U. S. Army Advanced Materiel Concepts Agency
Washington, D.C. 20315

ADDENDUM

Dept of Electrical Engineering
Rice University
Houston, Texas 77001

Research Laboratories for the Eng. Sciences
School of Engineering & Applied Science
University of Virginia
Charlottesville, Virginia 22903

Dept of Electrical Engineering
College of Engineering & Technology
Ohio University
Athens, Ohio 45701

Project MAC
Document Room
Massachusetts Institute of Technology
545 Technology Square
Cambridge, Massachusetts 02139

ERRATUM

Mr Jerome Fox, Research Coordinator
Polytechnic Institute of Brroklyn
55 Johnson Street (should be 333 Jay Street)
Brooklyn, N.Y. 11201

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)*
University of Illinois
Coordinated Science Laboratory
Urbana, Illinois 61801

2a. REPORT SECURITY CLASSIFICATION
Unclassified

2b. GROUP

3. REPORT TITLE
SOME RESULTS IN THE THEORY OF ARITHMETIC CODES

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*

5. AUTHOR(S) *(First name, middle initial, last name)*
CHIEN, R. T., HONG, S. J., & PREPARATA, F. P.

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
May, 1969	28	23

8a. CONTRACT OR GRANT NO.
DAAB 07-67-C-0199; auxiliary support by NSF GK-2339 and GK-1690

b. PROJECT NO.

c.

d.

9a. ORIGINATOR'S REPORT NUMBER(S)
R-417

9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*

10. DISTRIBUTION STATEMENT
This document has been approved for public release and sale; its distribution is unlimited.

11. SUPPLEMENTARY NOTES

12. SPONSORING MILITARY ACTIVITY
Joint Services Electronics Program
thru U.S. Army Electronics Command
Fort Monmouth, New Jersey 07703

13. ABSTRACT

This paper presents a simple number-theoretic investigation of the structure of binary arithmetic AN codes. The range (0,B-1) of represented integers is related to the code length n through $2^n - 1 = AB$. The analysis is based on the partition of the integers $1 \leq N \leq B-1$ into orbits, which are analogous to cosets of the multiplicative subgroup of the powers of 2 modulo B. It is shown how the code minimum weight is related to the members of the orbit. The properties of sets of prime powers are used in developing a simple search strategy for codes. An important consequence of the presented analysis is the construction of codes of moderate distance and high rate, thereby filling the spectrum between the two known extremes of the single-error correcting Brown codes and of the maximum-sequence like codes of Barrows and Mandelbaum. A list of codes of length ≤ 36 is finally presented.

DD FORM 1 NOV 65 1473

Security Classification

14 KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Arithmetic Codes						
Minimum Distance						
Orbits						
Exponents						
Extension Codes						
Rate						