SOME RESULTS IN
THE THEORY OF
ARITHMETIC CODES

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

UNIVERSITY OF ILLINOIS – URBANA, ILLINOIS

"THIS DOCUMENT HAS BEEN APPROVED FOR PUBLIC RELEASE AND SALE; ITS DISTRIBUTION IS UNLIMITED."
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.

Reproduction in whole or in part is permitted for any purpose of the United States Government.

This document has been approved for public release and sale; its distribution is unlimited.
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 \(\leq 36\) 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 \( q_0q_1...q_n \) is said to be the NAF representation of the integer \( b \) if

\[
b = \sum_{i=0}^{n} q_i 2^i \quad \text{and} \quad \begin{cases} q_i = -1, 0, 1 \quad (i = 0, 1, ..., n) \\ q_i q_{i+1} = 0 \end{cases}
\]

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:

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

\[
q_{i+1} = \begin{cases} 
1 & \text{if } \frac{2B}{3} > r_i \geq \frac{B}{3} \\
0 & \text{if } \frac{B}{3} > r_i \geq -\frac{B}{3} \\
-1 & \text{if } -\frac{B}{3} > r_i \geq -\frac{2B}{3} 
\end{cases}
\]

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

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

\[q_i q_{i+1} = 0\]

\[\frac{2B}{3} > r_i \geq -\frac{2B}{3}\]

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 \( q_{i+1} = 0 \),
\( |r_i| \leq \frac{2B}{3} \), and the theorem follows from mathematical induction on \( i \).

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

\[
q_{i+1} = \begin{cases} 
\neq 0 & \text{if } \frac{2B}{3} > r_i \geq \frac{B}{3} \pmod{B} \\
0 & \text{if } B \geq r_i \geq \frac{2B}{3} \text{ or } \frac{B}{3} > r_i \geq 0, \pmod{B}.
\end{cases}
\]

Also, \( r_i \equiv 2^i r_0 \pmod{B} \). 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 \( r_i \equiv 2^{e(B)} r_i \equiv r_{i+e(B)} \). It also follows that \( q_{i+e(B)} = q_i \) for \( i \geq 1 \), namely the expansion

\[
\frac{a}{B} = q_0.q_1q_2 \ldots
\]

is periodic with period \( e(B) \) for \( i \geq 1 \); \( q_1q_2 \ldots q_{e(B)} \) is termed the \( B \)-period of \( a/B \), and its weight 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

\[
A = \frac{2^{e(B)} - 1}{B}, \quad M = B
\]
If \( N \) is modulo \( B \), then \( AN \) is modulo \( 2^{e(B)} - 1 \). The generic code word then becomes

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

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

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

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 \( B = \prod_{i=1}^{n} p_i^{a_i} \) 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.,

\[ F \triangleq \{f_j\} = \{f_0, f_1, \ldots, f_{e(B)} - 1\} \text{ where } f_j = 2^j \mod B. \]

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 \( \zeta \), and \( F \) is the
subgroup generated by 2. F partitions $\zeta$ 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 $bf(B_1) \equiv b$, 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

\[
(6) \quad w_B(a) = \frac{e(B)}{e(B_1)} w_{B_1}(a)
\]

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

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

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

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

Obviously $\text{LCM}[e_i] = e \left( \frac{n}{p_i} \right)$. We now factor $\text{LCM}[e_i]$ as

$$
\text{LCM}[e_i] = \left( \frac{n}{p_i} \right)^{s_i} K
$$

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

\begin{equation}
S = S(p_1, p_2, \ldots, p_n) = \prod_{i=1}^{n} p_i^{s_i+1},
\end{equation}

the saturation product of the given set of $n$ primes. ($S$ was called Kernel 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.

**Theorem 4:** 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 $g(S)$.

**Proof:** 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

\begin{equation}
g(B) = \frac{\varphi(B)}{e(B)} = \frac{\prod_{i=1}^{n} p_i^{s_i+\beta_i}}{\prod_{i=1}^{n} p_i^{s_i+1}} = \frac{\prod_{i=1}^{n} (p_i^{\alpha_i} - 1)}{\prod_{i=1}^{n} (p_i^{s_i} - K)} = \frac{\varphi(S)}{e(S)} = g(S)
\end{equation}

Q.E.D.

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

\begin{equation}
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)
\end{equation}
For $B = \prod p_i^{\alpha_i}$ ($\alpha_i \geq 1$), 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 $\alpha_i$'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 $\left(2^{e(B)} - 1\right)/B$, 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 $d_m(B)/e(B) = d_m(S)/e(S)$.

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
Since \( R(B) > R(B_1) \), the previous relation suggests the possibility that we may gain rate without sacrificing minimum distance (i.e., when \( \text{d}_{m}(B) = \text{d}_{m}(B_1) \)). 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 \( (\alpha_1, \alpha_2, ..., \alpha_n) \) close to \( (s_1, s_2, ..., s_n) \) in the lattice of integers having \( (s_1, s_2, ..., s_n) \) 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 \( S(p_1, p_2, ..., p_n) \). 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

\[
\text{d}_{m}(B) = \min_{B_j | B} \left\{ \frac{w_{\min}(B_j) e(B_j)}{e(B)} \right\}
\]

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 $w_{\text{min}}(B)$.

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 $-r$ ($1 < r < B$, $(r, B) = 1$) belong to distinct $B$-orbits (having equal weight) if and only if $2^{e(B)/2} + 1 \equiv 0 \mod B$. 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., $r(2^k+1) \equiv 0 \mod B$. Since $(r, B) = 1$, it must be $(2^k+1) \equiv 0$, or, equivalently $2^{2k}-1 \equiv 0 \mod B$. It follows that $e(B)$ divides $2k$, or $k = \frac{j e(B)}{2}$, 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 ensuing 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>
<thead>
<tr>
<th>Code Length</th>
<th>B</th>
<th>Minimum Distance</th>
<th>Rate (&gt; 1/3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>11</td>
<td>4</td>
<td>0.400</td>
</tr>
<tr>
<td>12</td>
<td>39</td>
<td>4</td>
<td>0.500</td>
</tr>
<tr>
<td>14</td>
<td>43</td>
<td>5</td>
<td>0.533</td>
</tr>
<tr>
<td>15</td>
<td>151</td>
<td>5</td>
<td>0.444</td>
</tr>
<tr>
<td>18</td>
<td>133</td>
<td>6</td>
<td>0.556</td>
</tr>
<tr>
<td>18</td>
<td>667</td>
<td>6</td>
<td>0.350</td>
</tr>
<tr>
<td>20</td>
<td>123</td>
<td>5</td>
<td>0.450</td>
</tr>
<tr>
<td>20</td>
<td>451</td>
<td>5</td>
<td>0.600</td>
</tr>
<tr>
<td>20</td>
<td>3813</td>
<td>6</td>
<td>0.429</td>
</tr>
<tr>
<td>21</td>
<td>337</td>
<td>4</td>
<td>0.571</td>
</tr>
<tr>
<td>21</td>
<td>2359</td>
<td>5</td>
<td>0.409</td>
</tr>
<tr>
<td>22</td>
<td>267</td>
<td>6</td>
<td>0.636</td>
</tr>
<tr>
<td>22</td>
<td>15709</td>
<td>6</td>
<td>0.417</td>
</tr>
<tr>
<td>24</td>
<td>663</td>
<td>4</td>
<td>0.667</td>
</tr>
<tr>
<td>24</td>
<td>1989</td>
<td>5</td>
<td>0.458</td>
</tr>
<tr>
<td>24</td>
<td>46995</td>
<td>6</td>
<td>0.400</td>
</tr>
<tr>
<td>25</td>
<td>601</td>
<td>7</td>
<td>0.440</td>
</tr>
<tr>
<td>25</td>
<td>1801</td>
<td>5</td>
<td>0.640</td>
</tr>
<tr>
<td>25</td>
<td>55831</td>
<td>4</td>
<td>0.462</td>
</tr>
<tr>
<td>26</td>
<td>2731</td>
<td>4</td>
<td>0.393</td>
</tr>
<tr>
<td>28</td>
<td>1247</td>
<td>7</td>
<td>0.393</td>
</tr>
<tr>
<td>28</td>
<td>1695</td>
<td>6</td>
<td>0.536</td>
</tr>
<tr>
<td>28</td>
<td>24295</td>
<td>5</td>
<td>0.643</td>
</tr>
<tr>
<td>28</td>
<td>215265</td>
<td>6</td>
<td>0.414</td>
</tr>
<tr>
<td>29</td>
<td>2089</td>
<td>6</td>
<td>0.655</td>
</tr>
<tr>
<td>30</td>
<td>486737</td>
<td>7</td>
<td>0.367</td>
</tr>
<tr>
<td>30</td>
<td>1661</td>
<td>7</td>
<td>0.467</td>
</tr>
<tr>
<td>30</td>
<td>14949</td>
<td>6</td>
<td>0.567</td>
</tr>
<tr>
<td>30</td>
<td>71827</td>
<td>5</td>
<td>0.700</td>
</tr>
<tr>
<td>30</td>
<td>1649373</td>
<td>4</td>
<td>0.727</td>
</tr>
<tr>
<td>33</td>
<td>13788017</td>
<td>4</td>
<td>0.471</td>
</tr>
<tr>
<td>34</td>
<td>43691</td>
<td>4</td>
<td>0.343</td>
</tr>
<tr>
<td>35</td>
<td>2201</td>
<td>7</td>
<td>0.486</td>
</tr>
<tr>
<td>35</td>
<td>122921</td>
<td>6</td>
<td>0.543</td>
</tr>
<tr>
<td>35</td>
<td>279527</td>
<td>5</td>
<td>0.686</td>
</tr>
<tr>
<td>35</td>
<td>15610967</td>
<td>5</td>
<td>0.333</td>
</tr>
<tr>
<td>36</td>
<td>2071</td>
<td>9</td>
<td>0.417</td>
</tr>
<tr>
<td>36</td>
<td>24309</td>
<td>8</td>
<td>0.472</td>
</tr>
<tr>
<td>36</td>
<td>73815</td>
<td>7</td>
<td>0.556</td>
</tr>
<tr>
<td>36</td>
<td>959595</td>
<td>6</td>
<td>0.639</td>
</tr>
<tr>
<td>36</td>
<td>4740255</td>
<td>5</td>
<td>0.750</td>
</tr>
<tr>
<td>36</td>
<td>123818877</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>
TABLE II
Comparison of Codes with Same Prime Components

<table>
<thead>
<tr>
<th>Length</th>
<th>Minimum Distance</th>
<th>B</th>
<th>Better B</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>4</td>
<td>3.73</td>
<td>$3^2.73$</td>
</tr>
<tr>
<td>20</td>
<td>4</td>
<td>5.3.11</td>
<td>$5^2.3.11$</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>5.3.31</td>
<td>$5^2.3.31$</td>
</tr>
<tr>
<td>21</td>
<td>3</td>
<td>7.127</td>
<td>$7^2.127$</td>
</tr>
<tr>
<td>30</td>
<td>6</td>
<td>3.11.151</td>
<td>$3^2.11.151$</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>3.31.151.331</td>
<td>$3^2.31.151.331$</td>
</tr>
</tbody>
</table>
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 $Z(B) \triangleq \left[ \frac{B+1}{3} \right] = \sum_{B_i \subseteq B} W(B_i)$. 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 $B_0 \equiv (\alpha_1-1, \alpha_2-1, \ldots, \alpha_n-1)$. $B$ and $B_0$ clearly defines a unit-$n$-cube $C$, with $l.u.b. = B$ and $g.l.b. = B_0$. When a point $P \in C, P = (\alpha_1 - b_1, \alpha_2 - b_2, \ldots, \alpha_n - b_n)$ 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,

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

or, equivalently,

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

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 $h(P),$

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

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.

\[
Z(B) = \left[ \frac{B+1}{3} \right] = \left[ \frac{1}{3} \sum_{i=1}^{n} (3n_i + (-1)^\delta_i)^2 + 1 \right]
\]

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

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

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

\[
Z(P) = \frac{B}{3} \sum_{i=1}^{n} \left( \frac{1}{p_i} \right) b_i - \frac{1}{3} \sum_{i=1}^{n} (-1)^\delta_i b_i + \frac{1}{3} \sum_{i=1}^{n} \delta_i b_i
\]

From Eqs. (14) and (15),

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

\[
= \frac{B}{3} \sum_{b_i} \left\{ \prod_{i=1}^{n} \left( \frac{1}{p_i} \right) b_i \right\} - \frac{1}{3} \sum_{b_i} (-1)^i \prod_{i=1}^{n} (-1)^\delta_i b_i
\]

where \( \sum* \) means that the sum is over all the binary n-tuples \( (b_1, b_2, \ldots, b_n) \).
We recognize now
\[
\sum^* \left\{ \prod_{i=1}^n \left( \frac{-1}{p_i^{b_i}} \right) \right\} = \prod_{i=1}^n \left( 1 - \frac{1}{p_i^{b_i}} \right)
\]
and likewise
\[
\sum^* \left\{ \prod_{i=1}^n \left( (-1)^{i+\delta_i} b_i \right) \right\} = \prod_{i=1}^n \left( 1 + (-1)^{i+\delta_i} \right)
\]
which is \(2^n\) if and only if \(\delta_i = 1\) for all \(i\), and zero otherwise. Thus we obtain from Eq. (16),

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

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

Now assume that 3 divides \(B\). We let \(P_n = 3\) without loss of generality.

\[
Z(P) = \left[ \frac{1}{3} \left( N^b \prod_{i=1}^{n-1} \frac{\alpha_i - b_i}{P_i} + 1 \right) \right].
\]

Clearly \(Z(P) = 3^{n-1} \frac{\alpha_i - b_i}{P_i} \prod_{i=1}^{n-1} \alpha_i - b_i \) for \(P \in C\) and \(\alpha_i \geq 2\), which in turn leads to \(W(B) = \frac{\varphi(B)}{3}\). If now \(\alpha_i = 1\), 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,

\[
Z(P) \begin{cases} 
= \frac{1}{3} \prod_{i=1}^{n-1} \frac{\alpha_i - b_i}{P_i} \quad - \frac{1}{3} \prod_{i=1}^{n-1} \left( -1 \right)^{\delta_i (\alpha_i - b_i)} \quad \text{if} \quad P \in D^c \\
= \prod_{i=1}^{n-1} \frac{\alpha_i - b_i}{P_i} \quad \text{if} \quad P \in D \\
= \prod_{i=1}^{n-1} \frac{\alpha_i - b_i}{P_i} \quad \text{if} \quad P \in D \end{cases}
\]
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 \( \prod_{i=1}^{n-1} p_i \) is not divisible by 3, the first sum is \( (-1)^n \frac{W(B)}{3} = -W(B) \) (since \( b_n = 1 \) if \( P \in D^c \)) to which the relations (17) and (18) apply. The second term is given by

\[ (-1)^n \sum_{b \neq b_n} \prod_{i=1}^{n-1} \frac{b_i}{p_i} = \varphi \left( \frac{B}{3} \right) \]

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

\[ W(B) = \frac{\varphi(B)}{2} \frac{1}{3} \frac{\varphi(B)}{2} + \frac{(-1)^n}{3} 2^{n-1} \]

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

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

Summarizing these as a theorem, we have

**Theorem 7:** \( W(B) \), the sum of all the weights of distinct local B-orbits of \( B = \prod_{i=1}^{n} p_i \) (\( \alpha_i \geq 1 \)): 
i) \( W(B) = \frac{\varphi(B)}{3} - \frac{2}{3} \sum_{i=1}^{n} \alpha_i \) if \( p_i = 3n_i - 1 \) for all \( i \)

ii) \( W(B) = \frac{\varphi(B)}{3} - \frac{2}{3} \sum_{i=1}^{n} \alpha_i \) if \( p_n = 3, \alpha_i = 1 \) 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 saturated 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:

Property 1: If \( T = \prod_{i=1}^{n} p_i^{\alpha_i} \) is saturated with respect to \( p_1, p_2, \ldots, p_m \), then

1) \( e(T \cdot \prod_{i=1}^{m} p_i^{\beta_i}) = e(T) \prod_{i=1}^{m} p_i^{\beta_i} \) and
2) \( g(T \cdot \prod_{i=1}^{m} p_i^{\beta_i}) = g(T) \prod_{i=1}^{m} p_i^{\beta_i} \)

Consider a \( T \) saturated with respect to \( p_1 \). For both \( T \) and \( p_1 T \), the number of local orbits is \( g(T) = g(p_1 T) = \varphi(T)/e(T) \). Consider an element \( b \) of a local \( T \)-orbit. Then \( b2^j e(T) \equiv \gamma_j T + b \mod p_1 T \), where \( 0 \leq \gamma_j < p_1 \) for every \( j \). The fact that \( e(p_1 T) = p_1 e(T) \) is the smallest positive integer solution for \( 2^x \equiv 1 \mod p_1 T \), shows that \( \gamma_i \neq \gamma_j \) if \( i \neq j \mod p_1 \). 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 $\{b_i + nT | 0 \leq i < e(T), 0 \leq n < P_1\}$.

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 $\ell$ 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

$T = \prod_{i=1}^{n} p_i$ is saturated with respect to $P_1, P_2, \ldots, P_m$, one can apply the
previous result repeatedly and obtain,

**Theorem 8:** Let $T = \prod_{i=1}^{n} p_i$ 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 $B = T \cdot \prod_{i=1}^{m} P_{1i}$ 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) \[ w_i(B) = \frac{e(B)}{3} + (-1)^{\sum_{j=1}^{m} \delta_i \beta_i} \left\{ w_i(T) - \frac{e(T)}{3} \right\} \] if $p_i = 3n_1 + (-1)^{\delta_i}$ 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 $w_{\text{min}}(T)$ and $w_{\text{max}}(T)$ 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 $B = T \cdot \prod_{i=1}^{m} p_i^{\beta_i}$, $d_m(B) = d_m(T) \prod_{i=1}^{m} p_i^{\beta_i}$.

**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 $w_{\text{min}}(B_j) \geq w_{\text{min}}(T_j \cdot \frac{e(B_j)}{e(T_j)})$. Any such $B_j$ can be expressed (perhaps relabelling the indices each time) as $B_j = \prod_{i=k+1}^{n} p_i^{\alpha_i+a_i} \cdot \prod_{i=1}^{k} p_i^{\gamma_i}$ where $1 \leq k \leq m$, $1 \leq a_i \leq \beta_i$ and $\gamma_i \leq \alpha_i$ for all $i$. Let $T_j = \prod_{i=k+1}^{n} p_i^{\alpha_i} \cdot \prod_{i=1}^{k} p_i^{\gamma_i}$. Obviously $T_j$ is a divisor of $T$ and hence $d_m(T) \leq w_{\text{min}}(T_j \cdot \frac{e(T_j)}{e(T_j)})$. First, notice that any such $B_j$ and $T_j$ also belongs to the case iii) of theorem 7. Therefore,

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

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

\[
\omega_{\min}(B_j) = \frac{e(B_j)}{3} = \frac{e(T_j)}{3} \prod_{i=1}^{k} p_i \geq \omega_{\min}(T_j) \prod_{i=1}^{k} p_i
\]

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

\[
\omega_{\min}(B_j) = \frac{e(B_j)}{3} + \omega_{\min}(T_j) - \frac{e(T_j)}{3} \geq \omega_{\min}(T_j) \prod_{i=1}^{k} p_i
\]

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

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


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


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


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 Brooklyn
55 Johnson Street
Brooklyn, N.Y. 11201
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 \(\leq 36\) is finally presented.
<table>
<thead>
<tr>
<th>KEY WORDS</th>
<th>LINK A</th>
<th>LINK B</th>
<th>LINK C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ROLE WT</td>
<td>ROLE WT</td>
<td>ROLE WT</td>
</tr>
<tr>
<td>Arithmetic Codes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Distance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orbits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exponents</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extension Codes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rate</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>