REPORT R-438 OCTOBER 1969

CSL COORDINATED SCIENCE LABORATORY

ERROR CORRECTION IN HIGH SPEED ARITHMETIC

ROBERT T. CHIEN
SEJUNE HONG

UNIVERSITY OF ILLINOIS - URBANA, ILLINOIS

ERROR CORRECTION IN HIGH SPEED ARITHMETIC

Robert T. Chien
&
SeJune Hong

Coordinated Science Laboratory
University of Illinois
Urbana, Illinois

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

ERROR CORRECTION IN HIGH SPEED ARITHMETIC[*]

Robert T. Chien
SeJune Hong
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois

[*] This work was supported principally by the National Science Foundation under Grant GK-2339 and, in part, by the Joint Services Electronics Program under Contract DAAB-07-67-C-0199.

List of Symbols

E	Single iterative error
A	Generator of the arithmetic code
B	Number of codewords
m	Block length
r	Number of blocks
$\pm$	The polarity of error
k	The position of error
d	The number of erroneous digits
e_i	The distribution of error
S	Syndrome
$h(x)$	Hamming weight of x

Number of pages: 23

Number of tables: 3

Proposed running head: Arith. Codes for Iter. Error

ABSTRACT

The errors due to a faulty high speed multiplier are shown to be iterative in nature. These errors are analyzed in various aspects. The arithmetic coding technique is suggested for the improvement of high speed multiplier reliability. Through a number theoretic investigation, a large class of arithmetic codes for single iterative error correction are developed. The codes are shown to have near-optimal rates and to render a simple decoding method. The implementation of these codes seems highly practical.

I. INTRODUCTION

General Background

A great deal of research has been done on the improvement of speed and reliability of computers. The fast arithmetic units, especially high speed multiplier and divider schemes, contribute significantly to the overall performance of digital computers. For reliability, the employment of signal redundancy via error detecting or correcting codes seems to be a promising approach (Avizienis, 1965) although other techniques, such as hardware redundancy, are also helpful.

Recent developments in carry-save adders and iterative adders speed up addition and subtraction. Recoding techniques, employing minimal-non-zero representation of operands, have been well adopted for speeding up the multiplication and division. Practical schemes for high speed multiplication such as the one proposed by MacSorley (1961) have been implemented in many computers.

In a high speed arithmetic unit, the multiplier is divided into blocks of two (or more) bits each and each block is multiplied to the multiplicant to form partial sums. The partial sums are appropriately shifted and added in a multi-input parallel adder with minimum carry provisions. The longer the blocks, the faster the multiplication, but the complexity of hardware increases sharply with the size of blocks. The speed of such a multiplier has been analyzed by Freeman (1967).

Arithmetic Codes

The objective of this study is to find an arithmetic coding scheme to improve the reliability of the high speed multiplier. Arithmetic codes are designed to detect or correct errors in digital computations. One such error may change many output digits by propagations. Single error correcting codes are summarized in Peterson (1965), and multiple independent error correcting codes have been studied by Barrows (1966), Mandelbaum (1967), Chang and Tsao-Wu (1968) and Chien, Hong, and Preparata (1968, 1969). Burst error correcting arithmetic codes have been investigated by Stein (1962), Chien (1964), and Mandelbaum (1965).

Arithmetic codes are of the form AN, where A is a fixed integer called the generator. N is an integer in the interval (0, B-1), and B is the number of code words. If the code length is n, B is the smallest integer such that $AB>2^n$. In the binary case, A is obviously an odd number. The error correcting capability of ordinary AN codes depends on the minimum distance of the code, which in turn depends on the generator A. A corrupted signal (correct signal plus error) modulo A is called the syndrome of the error which is the same as the error modulo A. Syndrome of an error, usually denoted as S, then leads to the correct decision of the error through the decoding algorithms.

The error pattern expected in high speed multiplier is quite different from either the multiple independent errors or the burst errors. The iterative errors we expect from the high speed multiplier scheme are multiple equally spaced errors. A number theoretic investigation will be used in analyzing these errors, synthesizing codes for such errors, and demonstrating an easy implementation and high efficiency of such codes.

Definition of Iterative Error

If a faulty circuit occurs in the high speed multiplier, the resulting error pattern in the output will be of the following special form. First, since partial products are shifted by multiples of block length, the erroneous digit in each block will occupy the same relative position.

Hence, it is called the Iterative Error. Second, since a faulty circuit (stuck on 0 or 1) contributes to either carry or borrow type mistakes but not both, the entire erroneous digits will be of the same polarity. Now let m = the length of a block in bits, r = the number of blocks, and let E be a single interative error.

Definition 1 $E = \pm 2^k \sum_{i=0}^{r-1} e_i 2^{mi}$, where $0 \leq k < m$ and $e_i = 0$ or 1 for all i.

Of course, if $e_i = 0$ for all i, there exists no error. It is also feasible to extend the definition to cover multiple such error patterns occuring at the same time; for instance, a double iterative error would be $E = \pm 2^{k_1} \sum_{i=0}^{r-1} e_i 2^{mi} \pm 2^{k_2} \sum_{i=0}^{r-1} f_i 2^{mi}$, where $0 < k_1 < k_2 < m$, $e_i = 0$ or 1 and $f_i = 0$ or 1 for all i. Obviously any code that corrects all single iterative errors will detect all double iterative errors and vice versa. The following code for the detection of single iterative errors is well known.

Theorem 1 The code with generator A, a divisor of $2^m - 1$ and $A > r$ detects all single iteration errors in r blocks of length m.

Proof It must be shown that $E \not\equiv 0 \bmod A$ for any error. Note that $2^{mi} \equiv 1 \bmod A$ for all i. Now, suppose $E \equiv \pm 2^k \sum_{i=0}^{r-1} e_i 2^{mi} \equiv 0 \bmod A$. Since 2 and A are relatively prime, we have $\sum_{i=0}^{r-1} e_i \equiv 0 \bmod A$. But $0 < \sum_{i=0}^{r-1} e_i \leq r < A$ and hence a contradiction. Q.E.D.

Example Let $m = 6$. The generators of single iterative error detecting codes are:

$A = 3$	if	$r<3$	$A = 21$	if	$7 \leq r < 21$
$A = 7$	if	$3 \leq r < 7$	$A = 63$	if	$21 \leq r < 63$

II. PRELIMINARY DISCUSSIONS

It follows from the definition that, to correct any single iterative error, one must correctly determine the polarity of the error, the position of the error, k, and the set of e_i's called the distribution of the error. For convenience, we introduce three notations, E_0,E_1 and E_2, respectively defined as

$$E_0 = E = \pm 2^k \sum_{i=0}^{r-1} e_i 2^{mi} \tag{1}$$

$$E_1 = 2^k \sum_{i=0}^{r-1} e_i 2^{mi} \tag{2}$$

and

$$E_2 = \sum_{i=0}^{r-1} e_i 2^{mi} \tag{3}$$

One can easily verify the relation, $E_0 = \pm E_1 = 2^k E_2$, representing the error in the order of decreasing complexity. The three different aspects of error analyzed in this chapter will serve as a basis for the forthcoming derivation of error correcting codes.

<u>Polarity of Error, ±</u>

First, let us consider the case for integers $m = 2n + 1$ and $r \leq 2(2^n-1)$ for some $n \geq 1$. We will find a simple method with which the polarity can be uniquely determined. The same method will be used for the general case later.

<u>Lemma 1</u> Let $m = 2n+1$ and $r \leq 2(2^n-1)$ for some $n \geq 1$, then $S \equiv E_0 \bmod 2^m-1$ has less than or equal to n1's if and only if the polarity of error is positive.

Proof Let $S' \equiv E_2 \equiv \sum_{i=0}^{r-1} e_i 2^{mi} \bmod 2^m-1$. Since e_i's are either 0 or 1, we have $0 \leq S \leq 2(2^n-1) < 2^m-1$. The maximum number of 1's S can have is therefore n.

Now $S'' \equiv E_1 \equiv 2^k E_2 \bmod 2^m-1$ is merely a cyclic shift of S' modulo 2^m-1, which does not affect the number of 1's in S'. Thus, if $E_0 = E_1$, S has less than or equal to n 1's. But if $E_0 = -E_1$, $-S' \equiv 2^m-1-S'$ which can not have less than $2n+1-n = n+1$ 1's. Q.E.D.

With the above discussion in mind, consider now a general case where there is no obvious relationship between m and r. Let ℓ be an integer less than r, then $r = s\ell + t$ where $s \geq 1$ and $0 \leq t < \ell$. Clearly,

$$E_2 = \sum_{i=0}^{r-1} e_i 2^{mi} \equiv \sum_{i=0}^{\ell-1} f_i 2^{mi} \bmod 2^{m\ell}-1 \qquad (4)$$

where $0 \leq f_i \leq s + 1$ for all $0 \leq i < t$ and $0 \leq f_i \leq s$ for all $t \leq i < \ell$.

The Hamming weight of an integer I is defined as the number of 1's in the binary expression of I. Let w(x) be the maximum Hamming weight of I for all $0 \leq I \leq x$. Notice that w(x) is a non-decreasing function of x.

<u>Lemma 2</u> $w(x) = [\log_2(x+1)]$,*

<u>Proof</u> Clearly $w(x) = n$ if $2^n-1 \leq x < 2^{n+1}-1$ for some $n \geq 1$. Thus $n \leq \log_2(x+1) < n+1$ and $n = [\log_2(x+1)] = w(x)$. Q.E.D.

Define M(x) as the Hamming weight of x mod $2^{m\ell}-1$. $M(x) = M(2^k x)$ for any k, because 2^k amounts to a cyclic shift of 1's and 0's modulo $2^{m\ell}-1$. Rewriting Eq. (4), we get $0 \leq M(E_1) = M(E_2) \leq w(s+1)t + w(s)(\ell-t)$ and hence

$$M(E_1)_{max} = w(s)\ell + \{w(s+1) - w(s)\}t \qquad (5)$$

*[a] denotes the integer part of a

Theorem 2 Given m and r, if $\ell < r$ satisfies the condition, $M(E_1)_{max} < \frac{1}{2} m\ell$, then $M(E_0) < \frac{1}{2} m\ell$ if and only if the polarity of error is positive.

Proof If $E_0 = E_1$, the theorem follows from the hypothesis. If $E_0 = -E_1$, then $M(-E_1) = m\ell - M(E_1) \geq m\ell - M(E_1)_{max} > \frac{1}{2} m\ell$. Q.E.D.

The condition $M(E_1)_{max} < \frac{1}{2} m\ell$ is not as involved as it might seem. In fact, lemma 1 is a special case of this theorem. We know that $s = [\frac{r}{\ell}]$ and $t \equiv r \bmod \ell$. Also by lemma 2, $w(s+1) - w(s) = 1$ if and only if $s = 2^n-2$ for some $n > 1$. It is equal to zero otherwise. Given these facts, the table of maximum r's (r_{max}) for which ℓ satisfies the condition, is not difficult. Note that $M(E_1)_{max}$ is a non-decreasing function of r and hence ℓ and r_{max} are mutually non-decreasing functions of each other. From Table 1, one finds the smallest ℓ that satisfies the condition $M(E_1)_{max} < \frac{1}{2} m\ell$ via the first $r_{max} \geq r$ in the row of given m. The reason for the smallest ℓ is to maximize the rate of the code (see the section III).

Position of Error, k

We begin with the assumption that the number of error digits, $d = \sum_{i=0}^{r-1} e_i$ is given as well as $E_1 \bmod 2^m-1$. Let $S \equiv E_1 \equiv 2^k d \bmod 2^m-1$. We now derive a condition on r such that given d ($d \leq r$, necessarily) k can be uniquely decided from S.

Define T to be the smallest integer such that $2^x T \equiv T \bmod 2^m-1$ for any integer x in the range $0 < x < m$. Then, there must exist a least positive integer, y, such that x=y satisfies the above relation for T.

Table 1. r_{max} for m and ℓ

m ℓ	1	2	3	4	5	6	7
3	2	4	7	9	12	14	17
4	2	5	8	11	14	17	20
5	6	12	19	25	32	38	45
6	6	13	20	27	34	41	48
7	14	28	43	57	72	86	101
8	14	29	44	59	74	89	104
9	30	60	91	121	152	182	213
10	30	61	92	123	154	185	216
11	62	124	187	249	312	374	437
12	62	125	188	251	314	377	440
13	126	252	379	505	632	758	885
14	126	253	380	507	634	761	888
15	254	508	763	1017	1272	1526	1781
16	254	509	764	1019	1274	1529	1784

<u>Lemma 3</u> y is the largest divisor, x_0, of m ($x_0 < m$) and $T = (2^m-1)/(2^{x_0}-1)$.

<u>Proof</u> By the division algorithm, $m = ay+b$ where $0 < a$ and $0 \leq b < y$. Now, $2^mT \equiv 2^{ay+b}T \equiv 2^bT \equiv T \bmod 2^m-1$. This implies that $b = 0$ and $m = ay$, for y is the least positive integer for the above relation to hold. Therefore, 2^y-1 divides 2^m-1 and

$$T \equiv 0 \bmod \frac{2^m-1}{2^y-1} .$$

Clearly $T = (2^m-1)/(2^{x_0}-1)$ is the minimum when x_0 is the largest divisor of m ($x_0 < m$). We must now show that $y = x_0$ for this T. First, $(2^{x_0}-1)T \equiv 0 \bmod 2^m-1$. Suppose $y < x_0$, then

$$T = \frac{2^m-1}{2^{x_0}-1} \equiv 0 \bmod \frac{2^m-1}{2^y-1}$$

which is a contradiction because $y < x_0$ implies that $(2^m-1)/(2^{x_0}-1) < (2^m-1)/(2^y-1)$. Q.E.D.

<u>Theorem 3</u> Given d and $S \equiv 2^kd \equiv E_1 \bmod 2^m-1$, k can be uniquely decided if and only if $r < T$.

<u>Proof</u> If $r \geq T$, there is an error with $d = T$, for which $2^{x_0}T \equiv 2^{2x_0}T \equiv 2^{3x_0}T \ldots \bmod 2^m-1$, which results in a multiple solution for k. However, if $r < T$, and $2^kd \equiv 2^{k'}d \bmod 2^m-1$, then $(2^{k-k'}-1)d \equiv 0 \bmod 2^m-1$ and $0 \leq k-k' < m$. Since $d \leq r < T$, $k-k' = 0$ by the definition of T. Furthermore, $2^kd \equiv 0 \bmod 2^m-1$ only when $d = 0$, i.e., when there is no error. Q.E.D.

Table 2. T for given m

m	T	m	T	m	T
3	$2^3-1 = 7$	8	$2^4+1 = 17$	13	$2^{13}-1 = 8191$
4	$2^2+1 = 5$	9	$2^6+2^3+1 = 73$	14	$2^7+1 = 129$
5	$2^5-1 = 31$	10	$2^5+1 = 33$	15	$2^{10}+2^5+1 = 1057$
6	$2^3+1 = 9$	11	$2^{11}-1 = 2047$	16	$2^8+1 = 257$
7	$2^7-1 = 127$	12	$2^6+1 = 65$		

Distribution and the Number of Error Digits, d

In the previous section we have assumed that d was known. Now, we derive a condition on r such that d and the set of e_i's, namely the distribution, can be uniquely decided. We begin with a lemma which can be proved easily.

Lemma 4 If $(m,r) = 1$, the mapping from the set, $\{2^{mi} | 0 \leq i \leq r-1\}$, to the set, $\{2^j | 0 \leq j \leq r-1\}$, defined by $2^{mi} \equiv 2^j \bmod 2^r-1$ is one to one and onto.

Theorem 4 Let $(m,r) = 1$, $E_1 \neq 0$ and $S \equiv E_1 \bmod 2^r-1$. $S = 0$ if and only if $e_i = 1$ for all i, and when $S \neq 0$, S has d 1's. Furthermore, E_1 can be uniquely decided given k and S.

Proof By lemma 4, each term 2^{mi} maps to $2^{mi \bmod r}$ in one to one correspondence, and 2^k amounts to a cyclic shift which does not alter the number of 1's in S. Now given k and $S \neq 0$, $2^{-k}S \bmod 2^r-1$ can be uniquely mapped back to E_2, digit by digit, from which we obtain $E_1 = 2^k E_2$. If $S = 0$, $E_1 = \sum_{i=0}^{r-1} 2^{mi}$. Q.E.D.

III. CORRECTION OF SINGLE ITERATIVE ERROR

Now we are ready to synthesize codes for single iterative error correction. First, the A_1-code is shown with its error correcting ability demonstrated by a simple decoding algorithm. We then present some variations of this code. The rate (efficiency) considerations and a comparison of these codes are given with examples.

A_1-Code

As it was mentioned earlier, a successful correction of error depends on the correct decoding of the polarity, position, and distribution of error. A_1-Code is designed to do all these in the above order. Thus, from the syndrome we decipher $E_0 \pm E_1 = \pm 2^k E_2$.

Generator of the A_1-code is defined as $A_1 = \text{LCM}[(2^{m\ell}-1),(2^r-1)]$, where $r < T$ given in lemma 3, $(r,m) = 1$ and ℓ is the smallest integer satisfying the condition given by theorem 2. When m is given, $r < T$ (one may use Table 2) and $(r,m) = 1$, one finds ℓ from Table 1. The number of codewords is $B = [\frac{2^{mr}}{A}] + 1 \approx \frac{2^{mr}}{A}$ for large mr.

Theorem 5 The A_1-codes correct all single iterative errors.

Proof (Decoding Algorithm) Let a corrupted output be $K = AN + E_0$ and let $h(x)$ denote the Hamming weight of the integer x. $A = A_1$ in this case.

Step 1) Let the initial syndrome be $S_0 \equiv K \equiv AN + E_0 \bmod A$. If $h(S_0 \bmod 2^{m\ell}-1) < \frac{1}{2} m\ell$, the polarity is positive and otherwise negative. (By theorem 2.) If $S_0 = 0$, there is no error. (By theorem 3)

Step 2) Let $S_1 = S_0$ if the polarity is positive and let $S_1 = A - S_0$ if the polarity is negative. In either case $S_1 \equiv E_1 \bmod A$.

Step 3) Let $S_2 \equiv S_1 \equiv E_1 \bmod 2^r-1$.

$h(S_2) = d$ or, if $S_2 = 0$, $d = r$ (By theorem 4)

Step 4) Let $S_3 \equiv S_1 \bmod 2^m-1$. Since 2^m-1 divides $2^{m\ell}-1$ for any $\ell \geq 1$, $S_3 \equiv S_1 \equiv E_1 \equiv 2^k d \bmod 2^m-1$. Starting with d from the previous step, form $2^i d \bmod 2^m-1$ (cyclic shift of d). When $2^{i'} d = S_3$, $k = i'$ (By theorem 3)

Step 5) Now $E_2 \equiv 2^{-k}S_2 \bmod 2^r-1$ (cyclic shift left).

If $S_2 = 0$, $E_2 = \sum_{i=0}^{r-1} 2^{mi}$.

If $S_2 \neq 0$, let

$$2^{-k}S_2 \bmod 2^r-1 = \sum_{i=0}^{r-1} a_i 2^i \quad (a_i = 0,1)$$

$$E_2 = \sum_{i=0}^{r-1} a_i 2^{(\frac{1}{m} i \bmod r)m} . \quad \text{(By theorem 4)} \qquad \text{Q.E.D.}$$

One of the many interesting aspects of this code is that the decoding is very simple, which is quite unusual for ordinary arithmetic codes. In fact, the decoding requires essentially three shift registers of length m,r and mr each, plus some basic combinatorial threshold elements and a few constant-divisor divider circuits.

A_2-Code

Suppose a faulty multiplier has its kth position stuck either on 0 or 1. Assuming all inputs occur with equal frequency, the probability that this fault will actually contribute to an error digit in any particular block is very close to one half. Therefore, the probability that the entire blocks will contain the error digits, i.e., $E_0 = \pm 2^k \sum_{i=0}^{r-1} 2^{mi}$, is $(1/2)^r$. Define this type of error as a solid error, then the probability of the occurrence of a solid error is less than 1% if $r \geq 7$, or less than 0.1% as $r \geq 10$. It is apparently desirable to have a code that corrects all but solid iterative errors if a higher rate is achieved.

A modified code for given m and r is defined by the generator $A_2 = [2^{m\lambda}-1), (2^r-1)]$, where λ is the same as the ℓ for the A_1-code with m and r-1. Obviously $A_1 = A_2$ whenever $\ell = \lambda$, i.e., for given m, no r_{max} in Table 1 equals r-1. For example, if m = 6 and r = 20, $\lambda = \ell = 3$; but if m = 6 and r = 21, $\ell = 4$ and $r = \ell-1 = 3$ (from Table 1). Hence, from now on, we assume that $r-1 = r_{max}$ for given m in Table 1 and $\lambda = \ell-1$, when the A_2-code is used.

<u>Theorem 6</u> The A_2-codes correct all but solid single iterative errors and detect solid error.

<u>Proof</u> Since for non-solid errors, d=r-1 is the maximum number of digits in error, given λ satisfies the condition for theorem 2. Thus $S_0 \neq 0$ and $S_2 = 0$ is the only case when the polarity is undecidable, but the solid error is detected. The rest of the cases follow the same decoding steps as the A_1-code. Q.E.D.

The A_2-codes are especially effective when the block length, m, is even. Notice that if m = 2n (for some $n \geq 2$), $T = \frac{2^{2n}-1}{2^n-1} = 2^n+1$. But (r,m) = 1 forces r to be odd < T, and so $r = 2^n-1$ is a likely candidate for the number of blocks. We mention here that $r = 2^n-1$ and m = 2n are relatively prime for most cases except when n = 6, 12, 18, 20 or 21, etc. The first column of Table 1 shows, and it is easy to prove that, for m = 2n and $\ell = 1$, $r_{max} = 2^n-2$, which makes $r = r_{max} + 1 = 2^n - 1$ be indeed suitable for A_2-codes.

A_3-Code

Even though the discussion in this section can be applied to any m, we limit the scope to the even m cases. The objective is to remodify the modified codes so that the resultant code will correct all the single iterative errors including the solid error. Define the generator of remodified code as $A_3 = A_2 \cdot A'$, where A' is called the remodifier factor. Of course, it is desirable to have a smaller A' for a higher rate. We redefine A' as an integer such that the solid error $E = \sum_{i=0}^{r-1} 2^{mi} = \frac{2^{mr}-1}{2^m-1} \not\equiv 2^x(-E) \bmod A'$, for any x.

Theorem 7 The A_3-codes correct all single iterative errors.

Proof When a solid error is detected by the syndrome modulo A_2, the syndrome modulo A' uniquely reveals the polarity. Hence, all the decoding steps are applicable. Q.E.D.

The reason behind employing remodified A_3-code instead of the original A_1-code is to gain a higher rate if possible. This requires that $\log_2 A' < m^*$. Because, for given m and $r = r_{max} + 1$, $A_1 \approx 2^m A_2$ for most cases (see example 2). Finding such A' for arbitrary m may be very difficult. However, possible candidates are 7, 23...etc., i.e., those numbers x for which $y \not\equiv -2^j y \bmod x$ for any j and $y \not\equiv 0$. A simple test shows that 7 fails to be an A'; for a solid error of $m = 2n$ and $r = 2^n-1$, becomes 0 mod 7.

Lemma 5 $A' = 23$ is a remodifier for $m = 2n$ $(n = 3,4,5,7,8,9)$.

Proof First, $\log_2 23 < 5 < m$ given. Second, for any $y \not\equiv 0 \bmod 23$, $y \not\equiv 2^x y \bmod 23$ for any x, because $\{2^x \bmod 23 = \text{prime}\}$ forms two mutually complementary cosets. We now have to prove that $\sum_{i=0}^{r-1} 2^{mi} \not\equiv 0 \bmod 23$ for all the given m's.

Since $r = 2^n-1$, this sum becomes $(2^{mr}-1)/(2^m-1) = (2^{2n(2^n-1)}-1)/(2^{2n}-1)$. Since 23 is a factor of $2^{11}-1$, it is sufficient to show that 11 and $2n(2^n-1)$ are relatively prime for the given n's. But the smallest 2^n-1 divisible by 11 is when $n = 10$ which is larger than all the given n values. Q.E.D.

Lemma 6 Let p be a prime. If -2 (but not 2) is primitive modulo p, $(2^{rm}-1)/(2^m-1) \not\equiv 0 \bmod p$ and $\log_2 p < m$; then $A' = p$ is a remodifier for any m and r.

Proof Let $(2^{rm}-1)/(2^m-1) \equiv x \not\equiv 0 \bmod p$. It is well known that if e is the least positive integer to satisfy $2^e-1 \equiv 0 \bmod p$, e divides p-1, but since 2 is not a primitive root of p, e is a proper divisor of p-1. Suppose $x \equiv -2^y x \bmod p$ for some y. Let $y = ae+b$ with $a \geq 0$, $0 \leq b < e$. If $b = 0$, then $2^y \equiv 1 \bmod p$ and we arrive at a contradiction that $x \equiv -x \bmod p$. If $b \neq 0$, then $x \equiv -2^b x \bmod p$ or $2^b \equiv -1 \bmod p$. Thus $2^{2b} \equiv 1 \equiv (-2)^{2b} \bmod p$, but e divides 2b and so $e = 2b < p-1$. This is a contradiction on the hypothesis that -2 is a primitive root of p. Q.E.D.

Rate Comparison and Examples

Rate or efficiency of a code is defined as

$$R = \frac{\text{number of code words in bits}}{\text{code length}} \qquad (6)$$

We will first derive a sphere packing upper bound on the rate of single iterative error correcting codes. To correct all the errors, the syndrome of each distinct error pattern must also be distinct. This sets a lower bound on A, the generator. The total number of distinct single iterative errors is

$$2\cdot m\cdot(2^{r}-1) + 1 \tag{7}$$

For large m and r, this rapidly approaches $m2^{r+1}$. Hence $A \geq m2^{r+1}$, or the number of codewords is less than or equal to $2^{mr}/m2^{r+1}$. From Eq. (6)

$$R \leq \frac{\log_2(2^{mr}/m2^{r+1})}{mr} = 1 - \frac{1}{m} - \frac{1+\log_2 m}{mr} \tag{8}$$

This is a strict upper bound on the rate for large m and r. This shows that the upper bound approaches $1 - \frac{1}{m}$ for large r or 1 for large m and r.

Now consider the rate of A_1-code, for A_2 and A_3 codes are already improved versions of the former. At the worst case $[(2^{m\ell}-1), (2^{r}-1)] = (2^{m\ell}-1)\cdot(2^{r}-1)$. Hence, the rate is lower bounded as

$$R > \frac{mr-(m\ell+r)}{mr} = 1 - \frac{1}{m} - \frac{\ell}{r} \tag{9}$$

which is an encouraging result. Although ℓ is related to m and r, it clearly shows the tendency that the lower bound for fundamental code approaches $1 - \frac{1}{m}$ for large r and also approaches 1 for large m and r, which is exactly how the upper bound behaves. To be precise, let us estimate ℓ/r. Recall theorem 2 and Eq. (5). For large m we have $2w(s) \approx m$. But $w(s) \approx \log_2 [\frac{r}{\ell}] \approx \log_2 \frac{r}{\ell} \approx \frac{m}{2}$ and so $\ell \approx r\cdot 2^{-m/2}$. Thus, for large m, Eq. (9) becomes

$$R > - \frac{1}{m} - 2^{-m/2} \approx 1 - \frac{1}{m} \tag{10}$$

This demonstrates that indeed the A_1-code is nearly perfect. We formally state this as a theorem.

Theorem 8 The rate of the A_1-code assymtotically approaches the upper bound for large m.

Further comparison of the codes will be presented in the following two sets of examples. Some typical values for m and r are chosen. In Examples 1, we show A_1-codes with odd m's. Examples 2 compares the generators A_1, A_2, and A_3. In both cases, the approximate rate and the upper limit is presented for a verification of theorem 8, in Table 3.

Examples 1 A_1-Codes for m = odd

	(m,r)	ℓ	
a)	(3,2)	1	$A_1 = [(2^3-1),(2^2-1)] = (2^3-1)(2^2-1)$
b)	(5,18)	3	$A_1 = [(2^{15}-1),(2^{18}-1)]=(2^{15}-1)(2^{18}-1)/(2^3-1)$
c)	(7,13)	1	$A_1 = [(2^7-1), [2^{13}-1)] = (2^7-1)(2^{13}-1)$
d)	(9,58)	2	$A_1 = [(2^{18}-1),(2^{58}-1)]=(2^{18}-1)(2^{58}-1)/3$
e)	(11,62)	1	$A_1 = [(2^{11}-1),(2^{62}-1)] = (2^{11}-1)(2^{62}-1)$

Examples 2 Comparison of different codes for m = even. All the examples here have $\ell = 2$, $\lambda = 1$, $m = 2n$, $r = 2^n-1$.

f)	(6,7)	$\begin{cases} A_1 = [(2^{12}-1)(2^7-1)] = (2^{12}-1)(2^7-1) \\ A_2 = [(2^6-1)(2^7-1)] = (2^6-1)(2^7-1) \\ A_3 = (2^6-1)(2^7-1)\cdot 23 \end{cases}$
g)	(8,15)	$\begin{cases} A_1 = (2^{16}-1)(2^{15}-1) \\ A_2 = (2^8-1)(2^{15}-1) \\ A_3 = (2^8-1)(2^{15}-1)\cdot 23 \end{cases}$
h)	(10,31)	$\begin{cases} A_1 = (2^{20}-1)(2^{31}-1) \\ A_2 = (2^{10}-1)(2^{31}-1) \\ A_3 = (2^{10}-1)(2^{31}-1)\cdot 23 \end{cases}$
i)	(14,127)	$A_3 = (2^{14}-1)(2^{17}-1)\cdot 23$
j)	(16,255)	$A_3 = (2^{16}-1)(2^{255}-1)\cdot 23$
k)	(18,511)	$A_3 = (2^{18}-1)(2^{511}-1)\cdot 23$

Table 3.

Comparison of actual rates with the upper bound[1]

	A_1-Codes, odd m					A_3-Codes, even m			
	(m	r)	Rate	Upper Bound		(m	r)	Rate	Upper Bound
a	3	2	0.333	0.333 [2]	f	6	7	0.60	0.748
b	5	18	0.65	0.763	g	8	15	0.78	0.842
c	7	13	0.78	0.815	h	10	31	0.85	0.886
d	9	58	0.86	0.879	i	14	127	0.918	0.926
e	11	62	0.89	0.903	j	16	255	0.931	0.936
					k	18	511	0.943	0.945

[1] Calculated by Eq. (8) except for (m,r) = (3,2)

[2] For small m and r Eq. (7) is used for the bound $R \leq \dfrac{\log_2([\frac{2^{mr}}{A}]+1)}{mr}$

IV. CONCLUSION

The likely errors due to a faulty high speed multiplier are shown to be iterative in nature. These errors are analyzed in various aspects. An arithmetic coding technique to correct these iterative errors have been suggested for the improvement of reliability.

It was shown that this class of codes are nearly optimal in rates. The A_1-codes form the basic scheme from which the modified A_2-codes and the remodified A_3-codes are derived. It is shown that the A_2-codes generally achieve higher rates than the A_1-codes, at the small expense of not being able to correct a specific solid error. The A_3-codes, on the other hand, correct all the single iterative errors with usually higher rates than the A_1-codes. The latter two codes are especially useful for even block length.

The decoding is shown to be very simple. The encoding consists of premultipling either the multiplicand or the multiplier by the fixed generator A. Also, possibly losing a few bits, we may drop the LCM in the generator so that $A = (2^{m\ell}-1)(2^r-1)$ which is very easy to multiply. One can also multiply $(2^{m\ell}-1)$ to the multiplicand and (2^r-1) to the multiplier to achieve a faster encoding time. The implementation of these codes seem to be very promising.

V. REFERENCES

Avizienis, A., 1965, "A Study of Effectiveness of Fault-Detecting Codes for Binary Arithmetic," Tech. Report No. 32-711, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California.

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

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

Chien, R. T., 1964, "Linear Residue Codes for Burst Error Correction," IEEE Trans. on Information Theory, Vol. IT 10.

Chien, R. T., Hong, S. J. and Preparata, F. P., 1969, "Some Results in the Theory of Arithmetic Codes," submitted for publication, Report R-417, Coordinated Science Laboratory, University of Illinois, Urbana, Illinois.

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

Freeman, H., 1967, "Calculation of Mean Shift for a Binary Multiplier Using 2,3, or 4 Bits at a Time," IEEE Trans., Vol. EC-16.

MacSorley, O. L., 1961, "High-Speed Arithmetic in Binary Computers," Proc. of IRE, Vol. 49, No. 1.

Mandelbaum, D., 1965, "Arithmetic Error Detecting Codes for Communication Links Involving Computers," IEEE Trans. on Communication Technology Vol. Com. 13.

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

Peterson, W. W., 1965, "Error Correcting Codes," The M.I.T. Press, Cambridge, Massachusetts, 3rd Ed.

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

Distribution List as of 1 October, 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 H. 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-MT
White Sands Missile Range
New Mexico 88002

Project Manager
Common 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

ERRATUM

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

DELETE

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

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

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

Dept of Electrical Engineering
Rice University
Houston, Texas 77001

Research Laboratories for the Eng. Sc.
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

Lehigh University
Dept of Electrical Engineering
Bethelem, Pennsylvania 18015

Commander Test Command (TCD-)
Defense Atomic Support Agency
Sandia Base
Albuquerque, New Mexico 87115

Materials Center Reading Room 13-2137
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

Professor James A. Cadzow
Department of Electrical Engineering
State University of New York at Buffalo
Buffalo, New York 14214

Director, Naval Research Laboratory
Attn: Library, Code 2029 (ONRL)
Washington, D.C. 20390

Commanding Officer (Code 2064)
Navy Underwater Sound Laboratory
Fort Trumbull
New London, Connecticut 06320

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

ERROR CORRECTION IN HIGH SPEED ARITHMETIC

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

5. AUTHOR(S) *(First name, middle initial, last name)*

CHIEN, Robert T. & HONG, SeJune

6. REPORT DATE October, 1969	7a. TOTAL NO. OF PAGES 23	7b. NO. OF REFS 12

8a. CONTRACT OR GRANT NO. DAAB-07-67-C-0199; also NSF Grant GK-2339.	9a. ORIGINATOR'S REPORT NUMBER(S) R-438
b. PROJECT NO.	
c.	9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*
d.	

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

The errors due to a faulty high speed multiplier are shown to be iterative in nature. These errors are analyzed in various aspects. The arithmetic coding technique is suggested for the improvement of high speed multiplier reliability. Through a number theoretic investigation, a large class of arithmetic codes for single iterative error correction are developed. The codes are shown to have near-optimal rates and to render a simple decoding method. The implementation of these codes seems highly practical.

14 KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT.
Computer Arithmetic						
Error Correcting Codes						
Computer Reliability						