AN ITERATIVE APPROACH FOR THE CORRECTION OF ITERATIVE ERRORS

Robert T. Chien, et al.

Illinois University
Urbana, Illinois

November 1969
AN ITERATIVE APPROACH FOR THE CORRECTION OF ITERATIVE ERRORS

ROBERT T. CHIEN
SE JUNE HONG

UNIVERSITY OF ILLINOIS - URBANA, ILLINOIS

"THIS DOCUMENT HAS BEEN APPROVED FOR PUBLIC RELEASE AND SALE; ITS DISTRIBUTION IS UNLIMITED"
AN ITERATIVE APPROACH FOR THE
CORRECTION OF ITERATIVE ERRORS

by

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

This work was supported 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,
and in part by the National Science Foundation under Grant No. GK-2339.

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.
Other CSL Reports in Information Science include:


For copies of these reports please complete this form and send to
Professor R. T. Chien
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois 61801

My name and address is

________________________________________
________________________________________
________________________________________
AN ITERATIVE APPROACH FOR THE
CORRECTION OF ITERATIVE ERRORS

Robert I. Chien
Se June 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.
ABSTRACT

The errors most likely to occur in a high-speed multiplier are called the iterative errors. An arithmetic coding technique for the correction of such error patterns is proposed. We present a class of codes and show its error correcting ability. The unique feature of this code is an iterative decoding method.
I INTRODUCTION

The high-speed multiplier schemes such as the one proposed by MacSorley [1] have been well investigated and implemented in many computers. In such a multiplier scheme, the multiplier is divided into blocks of two (or more) bits each and each block is multiplied to the multiplicand to form partial products. The partial products are then appropriately shifted and added in a multi-input parallel adder with minimum carry provisions. The expected error pattern is quite different from either the multiple independent errors or the burst errors. These errors are shown to be iterative in nature and of the following special form. We let \( m \) = the length of a block in bits, \( r \) = the number of blocks, and let \( \mathbf{E} \) be a single iterative error.

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

A large class of arithmetic codes for the correction of such errors has been developed by Chien and Hong [2,3]. It has been shown that this class of codes has an easy implementation scheme and a nearly optimal rate. We propose a different class of arithmetic codes here, which is based on the concept of an iterative decoding method for the iterative errors.

Arithmetic codes are designed to detect or correct errors in digital computations. One such error may change many output digits by propagation. Single error correcting codes are summarized in Peterson [4], and multiple independent error correcting codes have been studied by Barrows [5], Mandelbaum [6], Chang and Tsao-Wu [7] and Chien, Hong, and Preparata [8,9]. Burst error correcting arithmetic codes have been investigated by Stein [10], Chien [11], and Mandelbaum [12].
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.

II. DERIVATION OF THE CODE

It follows from the definition that to correct the error one must correctly determine the polarity of the error, the position of the error (t), and the distribution of the erroneous digits, i.e., the set of e_i's. The class of codes dealt with in this work is for the cases when the number of blocks, r, is two to the same power, i.e., r = 2^t1 for some t_1 > 1. Note that the length of the code is m2^t0, and 2^m1 - 1 is now divisible by 2^m2^t0 + 1 for all 0 ≤ i ≤ t_1.

The Polarity of Error

Let t_0 be some integer less than t_1. Consider the positive error modulo 2^m2^t0 - 1. Clearly,

\[ E = E' = \sum_{i=0}^{t_1-1} c_i 2^{m1i} = \sum_{i=0}^{t_0-1} 2^{m1i} \mod 2^{m2^t0} - 1 \]
where $0 \leq i \leq 2^{t_1-t_0}$ for all $0 \leq i \leq 2^{t_0-1}$. Thus, each $f_i$ can have at the most $(t_1-t_0)$ 1's in its binary form. If $t_1-t_0 < \frac{1}{2^m}$, the whole residue $2^{t_0-1}$ must have less than $(2^m-1)$ 1's.

**Lemma 1** Given $t_0 > t_1 - \frac{1}{2^m}$

$$S = E \mod 2^{m2^{t_0}-1}$$

has less than $(2^m-1)$ 1's if and only if the polarity of error is positive.

**Proof** We must show that when the polarity is negative, $S$ has greater than $(2^m-1)$ 1's. Let $E' = -E'$ and $S' = E' \mod 2^{m2^{t_0}-1}$. We know that $S'$ has less than $(2^m-1)$ 1's. Therefore,

$$S = 2^{m2^{t_0}-1} - S'$$

and the number of ones in $S$ is greater than $m2^{t_0} - (m2^{t_0}-1) = m2^{t_0-1}$. We mention here that $S = 0$ only if $E = 0$, i.e., no error.

Q.E.D.

**Intermediate Error Pattern**

Using the same notation as $E = \pm E'$, or

$$E' = 2^k \sum_{i=0}^{t_1-1} e_i 2^{mi}$$

we now define an intermediate error pattern as

$$E_j = E' \mod 2^{m2^{t_0}-1}$$
for all \( t_0 \leq j \leq t_1 \). Clearly, \( \mathcal{E}_{t_1} = \mathcal{E}' \); and from Eq. (2) we have

\[
\mathcal{E}_j = 2^k \sum_{i=0}^{t_1-j-1} a_i 2^m i
\]

(4)

where \( 0 \leq a_i \leq 2^{t_1-j} \) and \( 0 \leq k < m \). Also, note that \( \mathcal{E}_j = \mathcal{E}_{j+1} \mod 2^{m+1} \) for all \( j < t_1 \).

Consider an intermediate error pattern, \( \mathcal{E}_j \), given in an ordinary binary form. Each \( a_i \) becomes a burst of length at most \( t_1-j \) with at least \( m \cdot (t_1-j) \) 0's in between. These bursts can be uniquely recognized if \( t_1-j < \frac{1}{2} m \), i.e., if \( j > t_1 - \frac{1}{2} m \). Let \( k_j \) be the maximum integer such that \( 2^k a_i \leq 2^{t_1-j} \) for all \( i \), for the given \( \mathcal{E}_j \) of Eq. (4). Clearly, \( k_j \geq 0 \).

Now denote by \( \mathcal{E}_j \) the following equation which is numerically the same as \( \mathcal{E}_j \):

\[
\mathcal{E}_j = 2^{(k-k_j)} \sum_{i=0}^{t_1-j-1} (a_i 2^k) 2^m i
\]

(5)

Lemma 2 If \( t_0 > t_1 - \frac{1}{2} m \), \( \mathcal{E}_j \) can be uniquely determined from the binary pattern of \( \mathcal{E}_j \), for all \( t_0 \leq j \leq t_1 - 1 \).

Proof \( t_0 > t_1 - \frac{1}{2} m \) implies \( j > t_1 - \frac{1}{2} m \) for all given \( j \)'s. Thus, the bursts of \( a_i \)'s are uniquely recognized for all \( j \). Now mark the position of \( \left\lfloor \frac{m+\star j}{2} \right\rfloor \) th bit after the longest burst and each \( m \) th bit positions thereafter,

\[\star\]The term, "burst", denotes a binary pattern beginning and ending with 1's. A single 1 is considered as a burst of length one. A cyclic connection between \( m+1 \) th bit and the first bit is assumed.

\[\star\star\]\( \left\lfloor x \right\rfloor \) denotes the least integer greater than or equal to \( x \).
cyclically around the entire length of $2^m$ bits. These marks fall among the 0's separating the bursts. Let the position of the smallest marked bit be $k'$, we have

$$2^k \sum_{i=0}^{2^j-1} (a_i 2^{k-k'}) \cdot 2^m \equiv E_j \mod 2^m - 1$$

Now, change $k'$ until $(a_i 2^{k-k'}) \leq 2^{t_1-j}$ for all $i$, for the first time. By the definition of $k_j$, $k' = k - k_j$ and $k-k' = k_j$ for Eq. (5). We mention here that any time $(a_i 2^j)$ becomes an odd number, $k_j = 0$ and the position of the error, $k = (k-k_j)$.

Q.E.D.

Suppose a binary pattern of $E_j$ is given and $(k-k_j)$ and $(a_i 2^j)$'s are all decided according to lemma 2. We let

$$E_{j+1} = 2^{(k-k_j)} \sum_{i=0}^{2^{j+1}-1} b_i 2^{m_i}$$

where $0 \leq b'_{i+2} j \leq 2^{t_1-j-1}$ and $b_i + b_{i+2} j = (a_i 2^j)$ for all $i$.

**Lemma 3** Let $E_{j+1} = 2^2 \sum_{i=0}^{2^{j+1}-1} b_i 2^{m_i}$. $0 \leq b_i \leq 2^{t_1-j-k_j}$ for all $0 \leq i \leq 2^{j+1}$.

**Proof** From Eq. (4), we know that $0 \leq b_i \leq 2^{t_1-j-1}$ for all $i$. Also, from the definition of $E_j$, $a_i = b_i + b_{i+2} j$ for all $0 \leq i \leq 2^{j-1}$. Now, since $(a_i 2^j) \leq 2^{t_1-j}$, $(b_i + b_{i+2} j) \leq 2^{t_1-j-k_j}$ regardless of $k_j$.

Q.E.D.
The $8$-Code

Define a class of integers, $\beta_j$, as the following. $\beta_j$ is a prime factor of $2^{m^2_j} + 1$, such that $x = m^2_j$ is the least positive solution for $2^x + 1 \equiv 0 \mod \beta_j$. $\beta_j$ is said to have order $n$ if

$$
2^{j+n_i} \sum_{i=0}^{j+n_i} e_i 2^{m_i} \not\equiv 0 \mod 2^{m^2_j} + 1 \implies 2^{j+n_i} \sum_{i=0}^{j+n_i} e_i 2^{m_i} \not\equiv 0 \mod \beta_j
$$

where $e_i = 1$ or $0$ for all $i$. An equivalent condition is

$$
2^{j-1} \sum_{i=0}^{j-1} a_i 2^{m_i} \not\equiv 0 \mod \beta_j
$$

(7)

where $|a_i| \leq 2^{n-1}$ for all $i$ and not all $a_i$'s are 0.

Finding the order of given $\beta_j$ seems to be a difficult number theory problem. But one can easily find the order by a computer programming. Table 1 shows a short list of $\beta_j$'s and the orders. It appears that all the $\beta_j$'s have order at least one.

<table>
<thead>
<tr>
<th>$m$</th>
<th>$j$</th>
<th>$\beta_j$</th>
<th>order</th>
<th>$m$</th>
<th>$j$</th>
<th>$\beta_j$</th>
<th>order</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>13</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>97</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>241</td>
<td>2</td>
<td>6</td>
<td>8</td>
<td>193</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>41</td>
<td>2</td>
<td>7</td>
<td>2</td>
<td>29</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>61681</td>
<td>8</td>
<td>7</td>
<td>2</td>
<td>113</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>241</td>
<td>8</td>
<td>7</td>
<td>4</td>
<td>1579031</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>673</td>
<td>2</td>
<td>7</td>
<td>8</td>
<td>5153</td>
<td>1</td>
</tr>
</tbody>
</table>
For a given $m$ and $r = 2^t$, the $B$-code is defined under the following assumptions. i) $t_1 > t_0 > t_1 - \frac{1}{2}m$ and $t_0 \geq 0$; ii) there exist $B_j$'s ($t_0 \leq j \leq t_1 - 2$) of order at least $t_1 - j + 2$ and $B_{t_1 - 1}$ of order 2. When such $B_j$'s exist we define the generator of the $B$-code as

$$A_B = (2^{m^2} - 1)B_{t_0} B_{t_0 + 1} \ldots B_{t_1 - 1}$$

We mention here that this generator divides $2^{mr} - 1$ and therefore resembles the form of the generators for ordinary multiple error correcting arithmetic codes [5-10].

III. ITERATIVE DECODING

The decoding is done by iteratively determining the intermediate error patterns. We first show how $e_{j+1}$ is obtained from given $e_j$ and present the complete decoding algorithm. An example follows for illustration.

**Lemma 4** Assume the order of $B_j$ is greater than or equal to $t_1 - j + 2$.

$e_{j+1} = e_j + 1 \mod B_j$ if and only if $e_{j+1} = e_j$ for all $t_0 \leq j \leq t_1 - 1$.

**Proof** We must show that $e_{j+1} = e_j \mod B_j$ implies $e_{j+1} = e_j$. Now,

$$e_{j+1} = 2^{k-j} \sum_{i=0}^{k-1} b_{i} 2^{j} 2^{m_1} = 2^{k-j} \sum_{i=0}^{k-1} b_{i} 2^{m_1} \mod B_j$$

or

$\sum_{i=0}^{k-1} (b_{i} 2^{j} - b_{i}') 2^{m_1} = 0 \mod B_j$
but

\[ 2^{m_l} = -2^m(i+2^j) \mod \beta_j \]

Thus

\[ \sum_{i=0}^{2^j-1} ((b_i - b_{i+2^j})2^j - (b'_i - b'_{i+2^j}))2^m = 0 \mod \beta_j \]

Since \(|(b_i - b_{i+2^j})| \leq 2^{t_1-j-k_j}\) by lemma 3 and \(|b'_i - b'_{i+2^j}| \leq 2^{t_1-j-1}\),

\[ |(b_i - b_{i+2^j})2^j - (b'_i - b'_{i+2^j})| \leq 2^{t_1-j} + 2^{t_1-j-1} \leq 2^{t_1-j+1} \]

for all \(j\). By the definition of \(\beta_j\),

\[ (b_i - b_{i+2^j})2^j - (b'_i - b'_{i+2^j}) = 0 \]

But

\[ (b_i + b_{i+2^j})2^j = a_i2^j = (b'_i + b'_{i+2^j}) \]

Therefore \(b'_i = b_i2^j\) for all \(0 \leq i \leq 2^{t_1-1}\).

Q.E.D.

**Theorem 9** The \(\beta\)-codes, when exist, correct all single iterative errors.

**Proof** Let the initial syndrome be \(S_0 = A_B N + E \equiv E \mod A_B\).

Step 1) If \(h(S \mod 2^{m2^t_0} - 1) < m2^{t_0-1}\), the polarity is positive, and otherwise negative. (By lemma 1.) If positive \(S_1 = S_0\), and if negative \(S_1 = A_B - S_0\). In either case \(S_1 \equiv E' \mod A_B\).

Step 2) \(E_{t_0} \equiv E' \equiv S_1 \mod 2^{m2^t_0} - 1\). However, the \(E_{t_0}\) obtained now is in binary pattern. Iteratively follow the next step for \(t_0 \leq t_1 - 2\).
Step 3) From the binary $E_j$, find $E_j$ by lemma 2. Using $S_1 = E_j \mod 8$, find $E_{j+1}$ uniquely from $E_j$ by lemma 4.

Step 4) Let $E_{t_1^{-1}} = \sum_{i=0}^{t_1-1} a_i 2^{mi}$. i) If $S_1 = 0 \mod \beta_{t_1-1}$, then $a_1 = 0$ or 2 for all $i$ and $k = k'$. ii) If $S_1 = 0 \mod \beta_{t_1-1}$ and $a_1 = 0$ or 2 for all $i$, then $k = k' + 1$. iii) If $S_1 = 0 \mod \beta_{t_1-1}$ and $a_1 = 0$, 1, or 2 for all $i$, then $k = k'$.

Step 5) Let $E = E_{t_1^{-1}} = \sum_{i=0}^{t_1-1} a_i 2^{mi}$

Let $E' = \sum_{i=0}^{t_1-1} e_i 2^{mi}$

where $0 \leq e_i \leq 1$ for all $i$ and $e_i + e_{i+1} \mod 2^i = a_i 2^{k_i - k}$ for all $i$.

By the same arguments as lemma 4, $E'_{t_1} = E_{t_1}$ if and only if $E'_{t_1} = E_{t_1} \mod 2^1$.

Q.E.D.

Example Let $m = 6$. Table 1 gives $\beta_1 = 241$ with order 8 and $\beta_2 = 673$ with order 2. Let $t_1 = 2$, i.e., $r = 8$. $t_0 = 1$ satisfies the condition for $\beta$-code, thus

$$A_\beta = (2^{12} - 1) \cdot 241 \cdot 673$$

the rate of which is approximately 0.4. Suppose the error is $(e_0, e_1, \ldots, e_7) = (10110101)$, $k = 3$ and of positive polarity. $E'_{t_1} = E' \mod 2^{12} - 1$ becomes the following binary pattern with the marks, $\uparrow$.

(\begin{array}{c}
\hline
\hline
\end{array})
IV. CONCLUSION

The $\beta$-codes are based on an interesting decoding method, namely, an iterative decoding for the iterative errors. From the syndrome of an iterative error, intermediate error patterns are iteratively decoded, each time doubling the length of the pattern. Although some searching and matching operations are necessary at each step, the unusual feature of this decoding technique may be desired for some applications.

The $\beta$-codes of high rate do not seem to exist for small $m$'s. However, for large $m$, it is very probable that such $\beta_j$'s exist. The rate of the $\beta$-code is generally less than the rate of the codes described in [3]. Again, for large $m$, the rate of $\beta$-code is likely to improve.
The decoder design, a theory of a simple method to find the order of \( \beta \), and a proof of existence of \( \beta \)-codes for large \( m \) are interesting problems for further research. Also, the iterative decoding concept may find a useful application in the polynomial codes.

V. REFERENCES


### AN ITERATIVE APPROACH FOR THE CORRECTION OF ITERATIVE ERRORS

The errors most likely to occur in a high-speed multiplier are called the iterative errors. An arithmetic coding technique for correction of such error patterns is proposed. We present a class of codes and show its error correcting ability. The unique feature of this code is an iterative decoding method.

#### Abstract

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

November, 1969

13

12

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

DD FORM 1473
Computer Reliability
Error Correcting Codes
Computer Arithmetic