NOTE ON ARITHMETIC CODES AND ARITHMETIC DISTANCE

By

William F. Hartman

Technical Report No. EE-705

November 1970

Department of

ELECTRICAL ENGINEERING

UNIVERSITY OF NOTRE DAME, NOTRE DAME, INDIANA

NOTE ON ARITHMETIC CODES AND ARITHMETIC DISTANCE

By

William F. Hartman

Technical Report No. EE-705

November 1970

Department of Electrical Engineering
University of Notre Dame, Notre Dame, Indiana

This work was supported by the National Aeronautics and Space Administration under NASA Grant NGL 15-004-026 in liaison with the Goddard Space Flight Center.

ABSTRACT

This report presents some observations on cyclic arithmetic codes and their distance-properties. The main result is the demonstration that modular arithmetic weight is invariant to cyclic shifts of codewords. As a consequence of this result, it is shown that the minimum distance of a cyclic arithmetic code can be found by a search of less than one-sixth of the codewords. This result also permits a simple proof of a result due to Goto and Fukumura for computation of arithmetic weighs in terms of the residue classes modulo B, the number of codewords.

I. INTRODUCTION

It will be assumed that the reader is familiar with the concepts of arithmetic weight and distance, denoted AW and AD respectively, as described by Massey (6). We shall also require the following three definitions, the first due to Reitweisner (7), and the other two due to Garcia (3).

<u>Definition 1</u> The <u>nonadjacent form</u> (NAF) of an integer I is the unique expression for I of the form $I = \sum_{i=0}^{n} a_i 2^i$ where $a_i \in \{-1,0,1\}$ and $a_i\, a_{i+1} = 0$, $i \geq 0$.

The arithmetic weight of I is the number of non-zero terms in the NAF for I. Note that AW(I) = AW(-I) since these two NAF differ only in the sign of their respective terms.

<u>Definition 2</u> The <u>modular arithmetic weight</u> of an integer I, relative to the modulus m, denoted MAW(I) is defined as:

$$\text{MAW}(I) = \min\,[\text{AW}(I),\ \text{AW}(m-I)].$$

<u>Example 1</u>: Let m = 31

$$\begin{aligned} \text{MAW}\,(21) &= \min\,[\text{AW}(21),\ \text{AW}(31-21)] \\ &= \min\,[\text{AW}(21),\ \text{AW}(10)] \\ &= \min\,[3,2] \\ &= 2 \end{aligned}$$

It should be noted that MAW does not necessarily satisfy the triangle inequality, as seen in the next example.

<u>Example 2</u>: Let m = 35

$$\text{MAW}\,(3+19) = \text{MAW}\,(22) = 3 \text{ but } \text{MAW}\,(3) = \text{MAW}\,(19) = 1$$

<u>Definition 3</u> The modular arithmetic distance (MAD) between integers I_1 and I_2 is:

$$\text{MAD}\,(I_1,I_2) = \text{MAW}\,(|I_1-I_2|)$$

MAD is not in general a true metric since the triangle inequality fails for certain modulo's.

Example 3: Let $m = 35$

MAD $(0,22)$ = MAW $(22) = 3$

But MAD $(0,3)$ = MAD $(3,22) = 1$

Garcia (3) has however shown that for modulo's of the form 2^n or 2^n-1 the triangle inequality does hold, and hence MAD is a true metric for these values of the modulus.

Definition 4 The arithmetic code with B codewords generated by the integer A is the set of integers $\{0, A, 2A, \ldots (B-1)A\}$.

It is customary to think of the codeword $A \cdot N$ as resulting from the encoding of the information digit N, and arithmetic codes are often called AN codes for this reason.

An AN code is said to be cyclic if the n-place cyclic shift of the radix two form of every codeword is the radix two form of a codeword, where n is defined by $AB = 2^n-1$. Some of the more convenient properties of cyclic arithmetic codes are: 1) The codewords are closed under addition modulo $m=2^n-1$ and, in fact, form an ideal in the ring of integers modulo 2^n-1. 2) If I is a codeword then 2^n-1-I is also a codeword. Also 3) the minimum MAW and the minimum AW of the nonzero codewords coincide.

In the rest of this report unless otherwise mentioned the modulus m will be 2^n-1 for the appropriate n.

II. OBSERVATIONS

Let $[a,b]$ denote the set of integers I such that $a \leq I \leq b$ and $(a,b]$ denote the set of integers I such that $a < I \leq b$. The set $W = (0,2^n-1]$ where $AB = 2^n-1$ is of considerable interest in the theory of cyclic AN codes. The lower third (L3) of W is defined to be the set $(0, \frac{2^n}{3}]$, the middle third (M3) as the set $(\frac{2^n}{3}, \frac{2^{n+1}-1}{3}]$ and the upper third (U3) as the set $(\frac{2^{n+1}-1}{3}, 2^n-1]$.

If $[a_n \, a_{n-1} \, . \, . \, . \, a_o]$ is the concatenation of the coefficients in the NAF of an integer $I \varepsilon W$ then:

$I \varepsilon L3$ if and only if $a_n = a_{n-1} = 0$

$I \varepsilon M3$ if and only if $a_n = 0$, $a_{n-1} = 1$

$I \varepsilon U3$ if and only if $a_n = 1$, $a_{n-1} = 0$

Five lemmas will be given that simplify the proofs of the subsequent theorems.

Lemma 1 For any integers I and J,

$$AW(I) - AW(J) \leq AW(I+J) \leq AW(I) + AW(J)$$

Proof: By the triangle inequality

$$AW(I+J) \leq AW(I) + AW(J)$$

again by the triangle inequality $AW(I) = AW(-J + (I+J) \leq AW(-J) + AW(I+J)$ or $AW(I) - AW(J) \leq AW(I+J)$

Lemma 2 For any integer I and any modulus m, MAW (I) = MAW (m-I).

Proof: Follows directly from the definition of modular arithmetic weight.

The next lemma shows that for an integer I in the lower third of W, the modular arithmetic and arithmetic weighs coincide.

Lemma 3 For $I \varepsilon L3$ then

$$MAW\ (I) = AW\ (I)$$

Proof: $AW(2^n - I) = AW(I) + 1$ since the NAF of I may be written $\sum_{i=o}^{n-2} a_i 2^i$ so that $2^n - \sum_{i=o}^{n-2} a_i 2^i$ is already the NAF for $2^n - I$.

thus $$\begin{aligned} AW(2^n - I - 1) &\geq AW(2^n - I) - AW(1) \\ &\geq AW(I) + 1 - 1 \\ &\geq AW(I). \end{aligned}$$

and hence $MAW(I) = \min [AW(I), AW(2^n - 1 - I)] = AW(I)$

The next two lemmas relate the arithmetic weight of I and the arithmetic weight of I-1 according to the endings of I in NAF. If $\sum_{i=o}^{n} a_i 2^i$ is the NAF of I, we shall often represent this NAF as the concatenation of its coefficients in descending order letting P represent +1, and N represent -1. For instance, I=3 has the NAF $2^2 - 2^o$ which we shall denote by PON. The notation $OP(ON)^i$ denotes the sequence in which OP is followed by i repetitions of the subsequence ON. It should be noted that the cases in the two lemmas are just shifts of each other.

Lemma 4 For an odd integer I,

$$AW(I) - 1 \leq AW(I-1) \leq AW(I).$$

Proof: The only possible endings for I in NAF are $OP(ON)^i$ or $OO(ON)^j$ where $i \geq 0$, $j \geq 1$.

Subtracting one results in NAF's with endings

$OO(PO)^i$ or $O(NO)(PO)^{j-1}$.

In the first case $AW(I-1) = AW(I) - 1$.

In the second case $AW(I-1) = AW(I)$.

Lemma 5 For an even integer I,

$$AW(I) \leq AW(I-1) \leq AW(I) + 1.$$

Proof: The possible endings in NAF for I are

$PO(NO)^i$ or $OO(NO)^i$ where $i \geq o$

Subtracting one results in the NAF's

$OP(OP)^i$ or $ON(OP)^i$.

In the first case $AW(I-1) = AW(I)$

In the second case $AW(I-1) = AW(I) + 1$.

<u>Theorem 1</u> For $I \varepsilon W$ then

$$MAW(I) = AW(I)$$

if (i) $I \varepsilon L3$

(ii) $I \varepsilon M3$ and even

otherwise $MAW(I) = AW(2^n-1-I)$

<u>Proof</u> $I \varepsilon L3$ by Lemma 3 previously

$I \varepsilon U3$ by Lemmas 3 and 4 previously

$I \varepsilon M3$ and I even

$$AW(2^n-1) = AW(I)$$

$$AW(2^n-1-I) \leq AW(I) + 1$$

$$\therefore \quad MAW(I) = AW(I)$$

$I \varepsilon M3$ and I odd

$$AW(2^n-I) = AW(I)$$

$$AW(2^n-I-1) \quad AW(2^n-I)$$

$$AW(I)$$

$$\therefore \quad MAW(I) = AW(2^n-1-I)$$

<u>Definition 5</u> Let $I \varepsilon W$ and $T(I)$ be the integer whose radix two form is the n-place cyclic shift of the radix two form of I. Similarly, let $T^i(I)$ be the integer corresponding to the i-th cyclic shift. Note that $T(I) = 2I$ if $I \varepsilon (0,2^{n-1}-1]$ and $T(I) = 2I - 2^n+1$ if $I \varepsilon (2^{n-1}-1,\ 2^n-1]$.

The following theorem shows that modualr arithmetic weight is invariant to cyclic shifts.

Theorem 2 For $I \varepsilon W$ $MAW(I) = MAW\,[T(I)]$.

Proof $I \varepsilon (0,2^{n-1}-1]$

$I \varepsilon L3$ $T(I) \varepsilon L3$ or $T(I) \varepsilon M3$ and $T(I)$ even

$MAW(I) = AW(2I) = AW(I) = MAW(I)$

$I \varepsilon M3$ and I even $MAW(I) = AW(I)$

$T(I) \varepsilon U3$ and $MAW(2I) = AW(2^n-1-2I)$

but $AW(2^n-2I) = AW(I) -1$ since 2^n-2I ends in 00

$AW(2^n-2I-1) = AW(I) - 1 + 1 = MAW(I)$

$I \varepsilon M3$ and I odd $MAW(I) = AW(2^n-1-I)$

$T(I) \varepsilon U3$

$MAW(2I) = AW(2^n-1-2I)$

$AW(2^n-I) = AW(I)$

$AW(2^n-2I) = AW(I) -1$

and by lemmas 3 and 4

$AW(I) \leq AW(2^n-I-1) \leq AW(I) - 1$

$AW(I) \leq AW(2^n-2I-1) \leq AW(I) - 1$

and the equalities go together

$\therefore MAW(2I) = MAW(I)$

$I \varepsilon (2^{n-1}-1,\ 2^n-1]$

$MAW(I) = MAW(2^n-1-I)$

$MAW(T(I)) = MAW(2I-2^n+1) = MAW(2(2^n-1-I))$

but since from the previous parts of the theorems

$MAW(J) = MAW(2J)$ $J \varepsilon [0,2^{n-1})$

then $MAW(I) = MAW[T(I)]$.

Corollary 2 The minimum distance of a cyclic AN code is the minimum of the arithmetic weights of its non-zero odd codewords in the lower third.

Proof: It must be shown that the minimum of the arithmetic weighs of the non-zero codewords is attained by an odd codeword in L3. If I is an even codeword then I is one or more cyclic shifts of an odd codeword. The odd codewords in U3 and M3 are obtained by T(I') where I' is an even codeword.

The following development relates the arithmetic weight of integers in L3 to the cyclic group of the powers of 2 modulo B and the cosets of this cyclic group.

Definition 6 The NAF of I ε W is said to be cyclic nonadjacent if $a_{n-1}\, a_0 = 0$.

Example 4 Let I = 11

NAF of I = (PONON) is not cyclic nonadjacent if n=5 but is cyclic nonadjacent if n>5.

Note that any number in L3 or in M3 and even, automatically is cyclic nonadjacent.

Definition 7 For I ε L3, let Z(I) be the integer whose NAF if the n-place cyclic shift of the NAF for I. Similarly let $Z^i(I)$ be the i^{th} cyclic shift. Note that $Z^i(I)$ may be negative.

Example 5 Let I = 11 and n = 6

I = OPONON = 11

$Z^1(I)$ = PONONO = 22

$Z^2(I)$ = ONONOP = -19

$Z^3(I)$ = NONOPO = -38

$Z^4(I)$ = ONOPON = -13

$Z^5(I)$ = NOPONO = -26

$Z^6(I)$ = I = 11

<u>Lemma 6</u> $Z^i(I) = T^i(I)$ if $Z^i > 0$, otherwise $Z^i(I) = T^i(I)-2^n+1$.

<u>Proof:</u> It suffices to show that $T^i(I)$ and $Z^i(I)$ are either the same integer or differ by exactly 2^n-1. But since cyclic shifting always doubles the integers with perhaps the addition or subtraction of 2^n-1, it follows that $T^i(I) \equiv Z^i(I) \bmod 2^n-1$ all i and also $o < T^i(I) < 2^n$ and $-2^n < Z^i(I) < 2^n$ so the conclusion follows.

The following theorem gives us - simple counting procedure to find the AW of an integer in L3.

<u>Theorem 3</u> For $I \varepsilon L3$

$$AW(I) = \#\{i : T^i(I) \varepsilon M3,\ i = 0,1\ldots N-1\}$$

<u>Proof:</u> AW(I) is just the number of non-zero terms in the NAF of I. But a_{n-1-i} is the leading term in the NAF of $Z^i(I)$ and hence is zero if and only if $|Z^i(I)| \varepsilon L3$ by lemma 6 this is equivalent to $T^i(I) \varepsilon L3$ or $(2^n-1) - T^i(I) \varepsilon L3$. But $2^n-1-T^i(I) \varepsilon L3$ is equivalent ot $T^i(I) \varepsilon U3$. Hence $a_{n-1-i} \neq o$ if and only if $T^i(I) \varepsilon M3$.

Let M3B the "middle third of B" be the set of integers I such that $AI \varepsilon M3$. It is readily checked that $M3B = (\frac{B}{3}, \frac{2B}{3}]$. We now have as a consequence the following corollary due originally to Goto and Fuhumura (4) and used by them to simplify the Barrows-Mandelbaum codes.

<u>Corollary 3</u> The minimum distance of a cyclic AN code is given by

$$\min_{\substack{L < B/3 \\ L \text{ odd}}} \#\{i : Z^i L \bmod B \varepsilon M3B,\ i = 0,1\ldots(n-1)\}$$

<u>Proof:</u> $AW(AI) = \#\{i : T^i(AI) \varepsilon M3\ i = 0,1..(n-1)\}$ but $\#\{i : T^i(AI) \varepsilon M3\}$ is the same as $\#\{i : 2^i(AI) \bmod AB \varepsilon M3\}$. And that is the same as $\#\{i : 2^i I \bmod B \varepsilon M3B\}$

This corollary shows that the minimum arithmetic weight of the non-zero codewords of a cyclic arithmetic code can be obtained without ever actually constructing the codewords but simply by considering integers modulo B.

REFERENCES

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

2. Chien, R.T., Hong, S.T. and Preparata, F.D. "Some Results in the Theory of Arithmetic Codes" Report R-417 Coordinated Science Laboratory, Urbana, Illinois, May, 1967.

3. Garcia, O.N. "Error Codes for Arithmetic and Logical Operations" Report D-69-03 Electrical Engineering Department, University of Maryland, College Park, Maryland, 1969.

4. Goto, M. and Fukumura, T. "The Distance of Arithmetic Codes", Memoirs of the Faculty of Engineering, Nagoya University Japan, pp. 474-482, 1968.

5. Mandelbaum, D. "Arithmetic Codes with Large Distances" IEEE Transactions on Information Theory, Vol. IT-13, pp. 237-242, April, 1967.

6. Massey, J.L. "Survey of Residue Coding for Arithmetic Errors" International Computation Center Bulletin Vol. 3 No. 4 October, 1964

7. Reitweisner, G.H. Advances in Computers Vol. I edited by F.L. Alt, Academic Press, New York, 1960.

8. Tsao-Wu, N.T. "Arithmetic Cyclic Codes" Communication Theory Group Report #10, Northeastern University, June, 1968.