A CLASS OF A(N + C) CODES AND ITS PROPERTIES

T. R. N. RAO, IEEE FELLOW

and

KASEM VATHANVIT, STUDENT MEMBER IEEE

Center for Advanced Computer Studies
University of Southwestern Louisiana
Lafayette, Louisiana 70504-4330

ABSTRACT

We discuss here a new class of arithmetic codes, called A(N + C) codes where A and C are constant positive integers, N is information to be coded. A(N + C) codes are a special case of AN + B arithmetic codes which were first studied by Brown. AN codes are linear and cannot be used to detect unidirectional multiple errors. A(N + C) codes are non-linear and are useful for detecting and/or correcting symmetric errors, arithmetic errors and unidirectional errors. Furthermore, A(N + C) codes can be constructed to provide constant-weight, self-complementing and cyclic-code properties. It is apparent that the codes with these properties have, in some sense, broader capabilities of error detection and error correction.

1. INTRODUCTION

The class of arithmetic codes known as AN codes [3,4,9-14] have been extensively studied. Brown [3] has discussed a special class of AN + B codes which are self-complementing, i.e. for every code word X, its complement X' is also a code word. By a suitable selection, B to be equal to AC we obtain A(N + C) class of codes which has capability to detect/correct symmetric errors, asymmetric errors, arithmetic errors, and unidirectional errors. For that reason these codes may find a broader range of application. For background, definitions on error types, weight, distance metrics and for notation used in the paper, the reader may refer to [2,9,10].

2. CONSTRUCTION OF A(N + C) CODES

In this section we discuss the class of arithmetic codes, namely, A(N + C) codes, which have the following properties; constant-weight, self-complementing and cyclic-code.

The arithmetic codes we consider are of the form A(N + C) where A,N and C are all integers. A is called the generator, N is a number to be coded and C is a constant. The arithmetic codes have the property that A(N1 + C) + A(N2 + C) = A(N3 + C) + AC for N3 = N1 + N2. The sum obtained is a multiple of A, and therefore can be used to check for errors.

Before going to the construction method for A(N + C) codes, we begin with the concepts of constant-weight codes, self-complementing codes and cyclic-codes. All code representations discussed here are binary (i.e. radix r = 2) and the code (or block) length is n.

A constant weight code is sometimes called an m/n code. It is a code with each codeword containing exactly m 1's (i.e., Hamming weight m). The constant weight codes have an advantage in that they detect any number of unidirectional errors (see references [1,2]).

A self-complementing code [3,10] is a code with the property that the complement of a codeword is also a codeword. These codes have the advantage of simpler implementation logic for complementation and subtract operation. For example, the binary 3N code for $0 \leq N \leq 5$ has codewords 0000, 0011, 0110, 1001, 1100 and 1111 and is clearly self-complementing.

A cyclic code [7,9,10,13] is a code with the property that any cyclic shift of a codeword is also a codeword. Besides having a nice mathematical structure, the algebraic cyclic codes are easy to encode and decode using linear feedback shift registers [13]. The example of 3N code given before also serves as an example of a cyclic code. The necessary and sufficient condition for AN code to be cyclic is that A divides 2^n-1.

The exponent of r modulo B, for relatively prime r and B, is the least positive integer i, such that $r^i \equiv 1 (\mathrm{mod}\ B)$. We denote this by $e_r(B)$. Since the radix r is 2, we can drop the subscript for simplicity and write e(B) to denote the exponent of 2 modulo B.

First, we start with A of the form

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

for an appropriate prime p. Then we try to derive conditions for the code to have self-complementing, constant-weight and cyclic-code properties.

2.1 Self-Complementing Code

If X is an n-bit number (or word) its complement X' is defined to be 2^n-1-X. Also for a base b of

CH2146-9/85/0000/0293$01.00 © 1985 IEEE

the system, the complement of N here is defined as b-1-N. In this notation the base b is different from radix which is 2. As an example, we have binary coded decimal number system where base is 10 and the radix is 2. For two codewords $A(N_1 + C)$ and $A(N_2 + C)$ to be complements we have the following

$$N_2 = b-1-N_1$$

and $A(N_1 + C) + A(N_2 + C) = 2^n-1.$

The above yields for C the condition

$$A(b-1) + 2C = 2 -1$$

or $$C = \frac{2^n-1-A(b-1)}{2A} \qquad (2)$$

The equation(2) holds iff A is odd and b is even. For the special case when $A = (2^{e(p)}-1)/p$ and $n = e(p)$, the above condition for c simplifies

$$C = (p-b+1)/2 \qquad (3)$$

2.2 Cyclic and Constant-Weight Properties

Before we can consider the other properties of A(N + C) codes, it is important to note that the codewords are n-tuples, i.e. these are selected multiples of A and N has the maximum possible range $0 \leq N < (2^n-1)/A$. Since our interest is in $C \neq 0$ with self-complementary property, the range is indeed smaller. The number of multiples of A which are n-tuples (i.e. less than 2^n) are exactly p + 1. Also since we need only b codewords among them, we select the range for N, $0 \leq N \leq b-1$. Therefore the codewords are AC, A(1+C), and A(b-1+C). Let us illustrate this by means of the following.

Example. Let p=11; then e(p)=10 and $A=(2^{10}-1)/11=93$. From (3) we obtain C=(p-b+1)/2 for the code to be self-complementing. For b=10, C=1 and for b=8, C=2 and so on. For b=10 we obtain 93(N+1) code, which is listed in Table 1 below.

Table 1

Code Words of 93(N + 1) Code

Decimal(N)	93(N + 1) Code
0	0001011101
1	0010111010
2	0100010111
3	0101110100
4	0111010001
5	1000101110
6	1010001011
7	1011101000
8	1101000101
9	1110100010

Let us consider 93(N + 1) code, and its error detection and correction capabilities.

For arithmetic errors, we first find the minimum arithmetic distance. The minimum arithmetic distance of the code is 4. From theory [10] we know the code can detect up to 3 arithmetic errors or it can both detect up to 2 arithmetic errors and correct 1 arithmetic error.

For unidirectional errors, we first find the minimum value of N(X,y) and N(Y,X). The minimum value of N(X,Y) and N(Y,X) is 2. From theory [6-9],the code can detect all unidirectional errors and correct 1 (symmetric or arithmetic) error.

This and some other A(N + C) codes for bases which are powers of two and ten can be found in Table 2 below.

Table 2

prime	code length	generator	constant	base
p	e(p)	A	C	b
11	10	93	2	8
			1	10
17	8	15	5	8
			4	10
			1	16
37	36	1857283155	15	8
			14	10
			11	16
			3	32
41	2C	25575	17	8
			16	10
			13	16
			5	32
67	66	1101298153654301589	30	8
			29	10
			26	16
			18	32
			2	64
113	28	2375535	53	8
			52	10
			49	16
			41	32
			25	64
			7	100
137	68	2154364271382137415	65	8
			64	10
			61	16
			53	32
			37	64
			19	100
			5	128

3. REMARKS AND CONCLUSION

The examples presented above illustrate that A(N+C) codes can be constructed to provide self-complementing, constant-weight and cyclic-code properties. The cyclic code property is an interesting property but is not important for arithmetic application. The Table 2 is generated by a computer search of all primes up to 137. The theory of A(N + C) has not been established as yet, but a few conjectures can be made by observation of the Table 2 as follows.

Conjecture 1. An A(N + C) code with $A = (2^{e(p)}-1)/p$ is a constant weight code iff e(p) is even and $C \geq 1$. For this case, the code weight is exactly one half of the code length e(p).

Conjecture 2. An A(N + C) code with $A = (2^{e(p)}-1)/p$ is a constant weight and cyclic iff the base b = p-1 and c = 1. The proofs do not appear to be difficult but we have not made a solid attempt as yet to prove them.

As far as the authors are aware these are the only class of codes known which provide arithmetic error correction and multiple unidirectional error detection. These codes are in that sense arithmetic analog of the single-error-correcting, all-unidirectional-error-detecting (SEC-AUED) codes presented by Bose and Rao [2].

REFERENCES

[1] Bose, B. and Pradhan, D. K., "Optimal Unidirectional Error Detecting/Correcting Codes," IEEE Trans. Comput., Vol. C-31, June 1982.

[2] Bose, B. and Rao, T. R. N., "Theory of Unidirectional Error Correcting/Detecting Codes," IEEE Trans. Comput., Vol. C-31, June 1982.

[3] Brown, D. T., "Error Detecting and Correcting Binary Codes for Arithmetic Operations," IRE Trans. Electron. Comput. EC-9, September 1960.

[4] Chen, R. T., Hong, S. J. and Preparata, F. P., "Some Results in the Theory of Arithmetic Codes," Inform. Control, Vol. 19, 1971.

[5] Constantin, S. D. and Rao, T. R. N., "On the Theory of Binary Asymmetric Codes," Inform. Contr., Vol. 40, January 1979.

[6] Hamming, R. W., "Error Detecting and Correcting Codes," Bell Syst. Tech. J., Vol. 29, April 1950.

[7] Lin, S. and Costello, D. J., Jr., Error Control Coding: Fundamentals and Applications, Prentice Hall 1983.

[8] Mandelbaum, D., "Arithmetic Codes with Large Distance," IEEE Trans. Information Theory, April 1967.

[9] Peterson, W. W. and Weldon, E. J., Error Correcting Codes, MIT Press, 1972.

[10] Rao, T. R. N., Error Coding for Arithmetic Processors, Academic Press, 1974.

[11] Shiozaki, A., "Single Asymmetric Error-correcting Cyclic AN Codes," Inform. Contr., Vol. 40, January 1979.

[12] Stone, H. S., Discrete Mathematical Structures and their Applications, Science Research Associates, 1973.

[13] Wakerly, J. F., Error Detecting Codes, Self-Checking Circuits and Applications, North-Holland, 1978.

[14] Wakerly, J. F., "Detection of Unidirectional Multiple Errors Using Low-cost Arithmetic Codes," IEEE Trans. Comput., Vol. C-24, February 1975.