(Submitted as a "short paper" to the 1976 IEEE International Symposium on Information Theory)

A Class of Maximum Distance Separable Codes over GF(p) Encodable Using Only Addition and Subtraction

James L. Massey
Freimann Professor of Electrical Engineering
University of Notre Dame
Notre Dame, Indiana 46556

ABSTRACT

The m-stage c-box is defined to be the circuit consisting of the cascade of m identical sub-circuits, each of which contains a unit delay whose output is the sub-circuit output and which output is multiplied by the constant c and added to the sub-circuit input to form the input to the delay cell. It is shown that when a polynomial $b(x) = b_{n-1} x^{n-1} + \ldots + b_1 x + b_0$ is shifted into an m-stage c-box, the delay cell contents after n shifts form the polynomial a(x) given by $a(x) = b(x+c) \bmod x^m$.

The (n,k) constancyclic code over GF(p) with n = p and generated by $g(x) = (x-c)^{n-k}$ is known to be maximum distance separable. The information polynomial i(x) in a systematic encoding is encoded as $x^{n-k}\, i(x) - r(x)$, where r(x) is the remainder when $x^{n-k}\, i(x)$ is divided by g(x). It is shown that r(x) can be obtained by first shifting $x^{n-k}\, i(x)$ n times into an (n-k)-stage c-box and then shifting the result n-k times into an (n-k)-stage (-c)-box. When c = 1 (or -1) the encoder thus uses only additions and subtractions in GF(p), i.e., no scalar multiplications are needed in the encoding circuit for these maximum distance separable codes.

in fact, for $c = 1$, the contents $(a_0, a_1, \dots a_{m-1})$ after N-shifts will just be the first m entries in the N-th row of Pascal's triangle.

The usefulness of the k-stage c-box is the fact, as given by (1), that it can be used to translate the indeterminate of a polynomial by the amount c. Note that when $c = +1$ or $c = -1$, then the m-stage c-box uses no scalar multiplications in F, but only additions or subtractions, respectively.

Massey, Costello and Justesen [1] showed that, for every prime p, the (n,k) constacyclic code of length $n = p$ over $F = GF(p)$ generated by $g(x) = (x-c)^{n-k}$ is maximum distance separable (MDS), i.e., its minimum distance satisfies $d = n - k + 1$. They gave a simple decoding procedure for these MDS codes, but gave no simple systematic encoding circuit. We now show how these MDS codes can be systematically encoded using an (n-k)-stage c-box and an (n-k)-stage (-c)-box.

The information polynomial $i(x) = i_{k-1} x^{k-1} + \dots + i_1 x + i_0$ in a systematic encoding must be encoded into $x^{n-k}\, i(x) - r(x)$ where $r(x)$ is the remainder when $x^{n-k}\, i(x)$ is divided by $g(x) = (x-c)^{n-k}$. It remains to find a circuit which forms $r(x)$. By Euclid's division algorithm,

$$x^{n-k}\, i(x) = (x-c)^{n-k}\, Q(x) + r(x). \qquad (3)$$

From (3), it follows that

$$(x+c)^{n-k}\, i(x+c) = x^{n-k}\, Q(x+c) + r(x+c)$$

and hence that

$$(x+c)^{n-k}\, i(x+c) = r(x+c) \bmod x^{n-k}. \qquad (4)$$

From (4), it follows that we can obtain $r(x+c)$ as the contents of an (n-k)-stage c-box after n shifts with the input $x^{n-k}\, i(x)$. But then $r(x)$ itself can be obtained as the contents of an (n-k)-stage (-c)-box in n-k shifts with the input $r(x+c)$. When $c = 1$ (in which case the constacyclic code is a cyclic code) or

A Class of Maximum Distance Separable Codes over GF(p) Encodable Using Only Addition and Subtraction

James L. Massey
Freimann Professor of Electrical Engineering
University of Notre Dame
Notre Dame, Indiana 46556

SUMMARY

Consider the circuit shown in Figure 1 which is a cascade of identical sub-circuits and which we shall call an m-stage c-box. The constant c may be any element in an arbitrary field F. When the polynomial $b(x) = b_{n-1} x^{n-1} + \ldots$

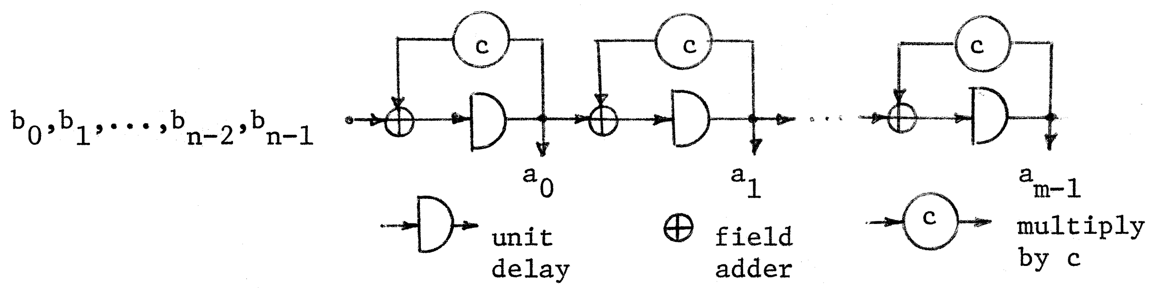

Fig. 1: The m-stage c-box.

$+ b_1 x + b_0$ with coefficients in F is read into the m-stage c-box, with higher order coefficients leading as shown in Figure 1, then the contents $a(x) = a_{m-1} x^{m-1} + \ldots + a_1 x + a_0$ after n shifts (i.e., just after b_0 has been shifted in from the input) is given by

$$a(x) \equiv b(x + c) \bmod x^m. \tag{1}$$

Equation (1) can be verified by observing that when the input sequence is 1,0,0,... then, after N shifts,

$$a_i = \binom{N-1}{i} c^{N-1-i} ; \tag{2}$$

$c = -1$ (in which case the constacyclic code is a negacyclic code), we see that only addition and subtraction, without scalar multiplication, is required in the encoding circuit. These codes look particularly interesting when p is a prime of the form $p = 2^s - 1$ since then the addition and subtraction in GF(p) are just the usual one's complement operations.

REFERENCE

[1] J. L. Massey, D. J. Costello, Jr., and J. Justesen, "Polynomial Weights and Code Constructions," IEEE Trans. Info. Th., Vol. IT-19, pp. 101-110, January 1973.