C. M. Melas
E. Gorog

A Note on Extending Certain Codes to Correct Error Bursts in Longer Messages

Given a burst-correcting code for short messages, it would seem practical and would be desirable to derive efficient codes for correcting the same types of bursts in longer messages. This note presents a simple method of constructing such codes, and supplies a geometric interpretation of the method. The Fire burst correcting codes[1] are a special case of the class of codes presented here.

Description of method

Let $E(x)$ be an error polynomial as defined by Peterson and Brown.[2] We will define the error pattern polynomial as $P(x) = E(x)/x^r$, where x^r is a term of $E(x)$ chosen to minimize the degree of $P(x)$. This definition in effect normalizes the error polynomial with respect to block length. Thus, for single errors, $P(x) = 1$; for double adjacent errors, $P(x) = 1 + x$; etc. The set of all error patterns corresponding to a burst of length b is composed of all polynomials of degree $b - 1$ with a constant "1" term.

For the cyclic code defined by a generating polynomial $G(x)$ to correct a set, S, of error pattern polynomials in a message of length n, a necessary and sufficient condition is that, for any two polynomials $P_i(x)$ and $P_j(x)$ in S,

$$P_i(x) + x^k P_j(x) \not\equiv 0 \bmod G(x), \tag{1}$$

and

$$P_i(x) + x^{\lambda n} P_i(x) \equiv 0 \bmod G(x), \tag{2}$$

where $P_i(x) \not\equiv 0$ and k and λ are arbitrary integers.

Condition (1) follows immediately from the fact (stated in Ref. 2) that each correctable error polynomial must give a different remainder when divided by $G(x)$. Thus the condition for any two error polynomials,

$$E_i(x) + E_j(x) \not\equiv 0 \bmod G(x), \tag{3}$$

becomes

$$x^{r_1} P_i(x) + x^{r_2} P_j(x) \not\equiv 0 \bmod G(x); \tag{4}$$

and (1) is derived by dividing Eq. (4) by x^{r_1}. Equation (2) expresses the fact that the code is cyclic of period n, for any error pattern polynomial $P_i(x)$.

Consider now the generating polynomial $F(x)$ of a code correcting any *one* of the error patterns in S, in a message of length d. Since this is a single-pattern correcting code, inequality (1) does not apply, and Eq. (2) becomes

$$P_i(x) + x^{\mu d} P_i(x) \equiv 0 \bmod F(x), \tag{5}$$

where $P_i(x) \not\equiv 0$ and $\mu = 1, 2, \cdots$. The product polynomial $G(x)\ F(x)$ will generate a code correcting the set, S, of error patterns. Clearly, (1) implies that

$$P_i(x) + x^k P_j(x) \not\equiv 0 \bmod G(x)F(x). \tag{6}$$

Furthermore, if d and n are relatively prime, we can write, from Eqs. (2) and (5),

$$P_i(x) + x^{\mu d n} P_i(x) \equiv 0 \bmod G(x)F(x), \tag{7}$$

where $\mu = 1, 2, \cdots$, in which

$$P_i(x) \not\equiv 0 \bmod G(x) \text{ and } \bmod F(x). \tag{8}$$

Thus, (6), (7), and (8) define a code correcting the set, S, of error patterns in a message of length nd generated by $G(x)\ F(x)$.

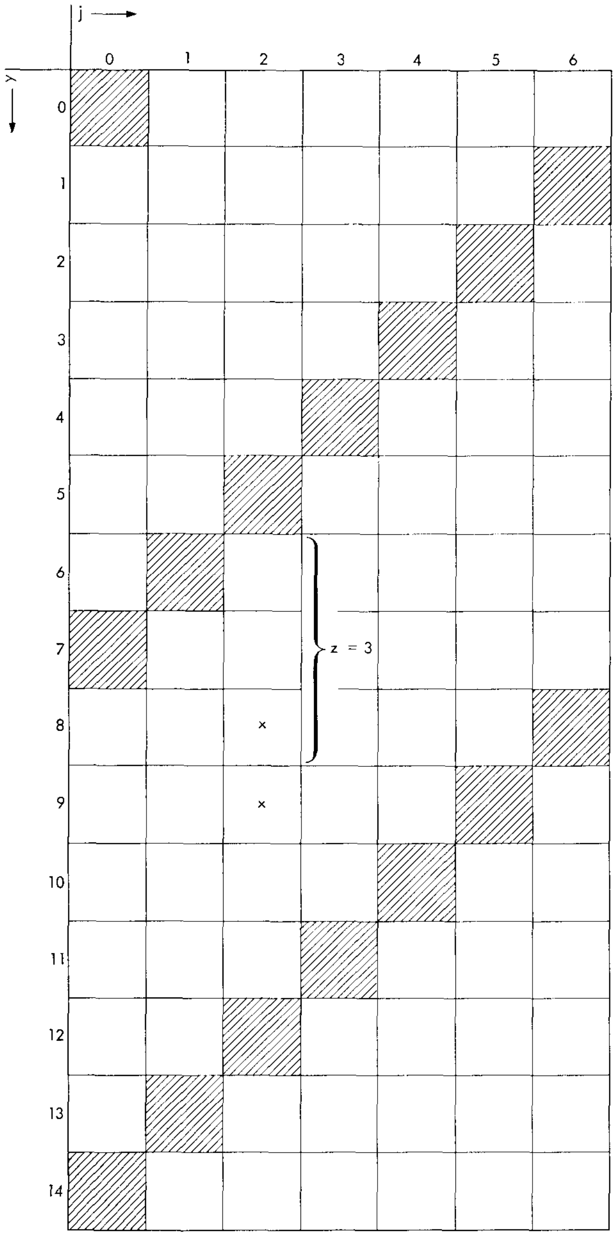
The following theorem can then be stated: If $G(x)$ is the generating polynomial of a code correcting a set, S, of error patterns in a message of length n; and if $F(x)$ is the generating polynomial of a code correcting an arbitrary pattern of that set, and only that pattern, in a message of length d, prime with respect to n, then the polynomial $G(x)\ F(x)$ generates a code correcting the set, S, in a message of length nd.

For example:

$$G(x) = (x^2 + x + 1)(x^4 + x + 1)$$

generates a code correcting a 3-bit burst in a 15-bit message.[3]

Figure 1 **Geometric interpretation of the method for constructing the codes.**



$$G(x)F(x) = (x^2 + x + 1)(x^4 + x + 1)(x^3 + x + 1)$$

generates a code correcting the same burst in a 105-bit message.

In Fire codes, a special case of these codes,

$$G(x) = 1 + x^{2b-1}$$

generates a polynomial correcting a burst of length b. To correct bursts of length b, $F(x)$ must be of degree b or greater. It cannot be equal to any of the burst pattern polynomials of degree $b - 1$, and $G(x)$ should be at least of degree $2b - 1$: otherwise there can always be two pattern polynomials $P_i(x)$ and $P_j(x)$ which will not satisfy (1). The degree of $G(x)$ $F(x)$, and thus the number of parity bits, must always equal at least $3b - 1$.

Geometric interpretation

Consider an array of dn bits, making up a code word of a cyclic burst-correcting code of normal length n. If the bits are arranged in d columns of n bits each, the code will determine the type of burst, and its location within a horizontal band (see Fig. 1). If a_{jy} is the first bit of the array in error, its y coordinate—i.e., the distance to the first bit of the n-cycle,—is determined by the code.

Assume now that the same array is also a code word of a single pattern-correcting code normally of length d. The array is composed of n cycles of this code. The position of the burst within d bits can now be determined. If n and d are relatively prime, the j coordinate of the first bit in error, a_{jy}, can also be determined. Let z be the distance of the first bit in error from any first bit of the d cycle. Obviously if $g \equiv z \bmod d$, $j = 0$, because the first bits of the d and the n cycles coincide in the first column. In the next column ($j = 1$), the start of the n cycle occurs x bits after that of the d cycle where $k \equiv n \bmod d$. Thus, for that value of x, only $g \equiv (z - k) \bmod d$.

In general, we have $y \equiv z - nj$, or $j \equiv (z - y/k) \bmod d$. In the example given in the Figure, $d = 7$, $n = 15$, and $k \equiv 15 \bmod 7 = 1$. Thus $j \equiv (z - y) \bmod 7$, and the shaded squares in the figure indicate the first bit of each of the d cycles, always shifted by 1 bit. Example: If a $1 + x$ error occurs in the message, on the squares marked x in the Figure, then the polynomial $G(x)$ will determine the type and y position. In this example, $y = 8$; the $F(x)$ polynomial will yield $z = 3$; and the corresponding j coordinate will be $j \equiv (3 - 8) \bmod 7 = 2$.

References

1. P. Fire, "A Class of Multiple-Error Correcting Binary Codes for Non-Independent Errors," Technical Report No. 55, April 24, 1959, Stanford Electronics Laboratory, Stanford California.
2. D. T. Brown and W. W. Peterson, "Cyclic Codes for Error Detection," *Proc. IRE*, **49**, 228-235 (1961).
3. C. M. Melas, "A New Group of Codes for Correction of Dependent Errors in Data Transmission," *IBM Journal* **4**, 58-65 (1960).

Received September 28, 1962