Aaron D. Wyner*

A Note on a Class of Binary Cyclic Codes Which Correct Solid-Burst Errors

In a recent paper[1], Melas and Gorog discussed a technique for extending the length of certain shortened cyclic codes to correct the same class of error patterns (for example, "burst" error patterns). In this note a similar result is stated for unshortened cyclic codes,[2] and the technique is employed to generate a class of binary cyclic codes which correct solid-burst errors.

Definition

Let $G(X)$ by a polynomial over $GF(q)$. The *cyclic code generated by* $G(X)$ is the set of multiples of $G(X)$ modulo $X^n - 1$, where n is the smallest integer for which $G(X)$ divides $X^n - 1$; n is the *length* of the code.

If the code is to correct the class of error polynomials $\mathcal{E}$ it is necessary and sufficient that for $E_1(X)$ and $E_2(X) \epsilon \mathcal{E}$,

$$E_1(X) \equiv E_2(X) \quad \text{modulo} \quad G(X)$$

which implies that

$$E_1(X) \equiv E_2(X) \quad \text{modulo} \quad X^n - 1. \tag{1}$$

Usually, the class of errors to be corrected may be written in the form $X^r P(X)$, where $P(X)$ belongs to some set of error "patterns" $\mathcal{S}$, that is $\mathcal{E}(\mathcal{S}) = \{X^r P(X) : P(X) \epsilon \mathcal{S}, r = 1, 2, 3, \cdots\}$. If condition (1) is satisfied for $\mathcal{E}(\mathcal{S})$ we say that the code corrects the patterns $\mathcal{S}$.

Theorem

Let $g(X)$ generate a cyclic code over $GF(q)$ of length n_1, which corrects the error patterns $\mathcal{S}$. Let $f(X)$ generate a cyclic code over $GF(q)$ of length n_2 which corrects each of the classes of error patterns $\mathcal{S}_i = \{P_i(X), 0\}$ for *every* $P_i(X) \epsilon \mathcal{S}$. Further say that $\mathcal{S}$ has the property that for $P_i(X)$, $P_j(X) \epsilon \mathcal{S}$,

A. $X^r P_i(X) - P_j(X) \equiv 0 \bmod X^{n_1} - 1 \Leftrightarrow n_1 \mid r$ and $P_i(X) = P_j(X)$

B. $X^r P_i(X) - P_i(X) \equiv 0 \bmod X^{n_2} - 1 \Leftrightarrow n_2 \mid r$.

In other words, no member of $\mathcal{S}$ is a cyclic shift of another member of $\mathcal{S}$ when the cycle length is n_1, and no member of $\mathcal{S}$ is a cyclic shift of itself when the cycle length is n_1 or n_2 (except, of course, when the shift length r is a multiple of n_1 or n_2). Then the code generated by l.c.m. $(g(X), f(X))$ corrects the class of error patterns $\mathcal{S}$ with code length l.c.m.(n_1, n_2).

We now apply this technique to obtain a class of binary cyclic codes which correct solid-bursts.[3]

Let $P_i(X) = 1 + X + X^2 + \cdots + X^{i-1}$, and let $\mathcal{S} = \{0, P_i(X)\text{: i} = 0, 1, 2, \cdots b\}$, the class of solid bursts of length up to b.

Let $g(X) = X^c + 1$, so that $n_1 = c$. If $c \geq b + 1$, condition A is satisfied. Since $g(X)$ generates the trivial code with only the zero code word, $g(X)$ corrects the patterns $\mathcal{S}$.

Let $f(X)$ be an irreducible polynomial of degree r whose roots have order n_2. If $n_2 \geq b + 1$, condition B is satisfied. Further assume that $f(X)$ does not divide $X^c + 1$ so that $f(X)$ and $g(X)$ are relatively prime. We shall now demonstrate that the code generated by $f(X)$ corrects the class of patterns $\mathcal{S}_i = \{P_i(X), 0\}$. To do this we must show that if $X^r P_i(X) \equiv P_i(X)$ modulo $f(X)$, then r is a multiple of n_2 (so that these are, in fact, the same error patterns).

If $f(X)$ divides $(X^r + 1)P_i(X)$, then, since $f(X)$ is irreducible, $f(X)$ divides $P_i(X)$ or $X^r + 1$. If $f(X)$ divides $P_i(X) = X^{i-1} + X^{i-2} + \cdots + X + 1$, then $f(X)$ divides $X^i + 1$. By minimality of n_2, and since $i \leq b$, we have

* Now with Bell Telephone Laboratories, Inc., Murray Hill, N. J.

$n_2 \leq i \leq b$. But $n_2 \geq b + 1 > b$, hence $f(X)$ divides $X^r + 1$. This can be so only when r is a multiple of n_2.

Since all the hypotheses of the theorem are satisfied, we conclude that the cyclic code generated by $g(X)f(X) = (X^c + 1)f(X)$ corrects the class of solid-bursts of length up to b with code length l.c.m.(n_1, n_2).

Example

Say $b = 20$. Choose $g(X) = X^{21} + 1$, and $f(X) = X^5 + X^2 + 1$, a primitive polynomial with $n_2 = 31$ which is greater than $b + 1$. Hence the code generated by $(X^{21} + 1)(X^5 + X^2 + 1)$ corrects solid-bursts of length up to 20 with code length $31 \cdot 21 = 651$. The number of digits required is $21 + 5 = 26$.

Acknowledgments

The author wishes to acknowledge a number of very helpful conversations with Dr. R. T. Chien of the IBM Thomas J. Watson Research Center.

References and Footnotes

1. E. M. Melas and E. Gorog, "A Note on Extending Certain Codes to Correct Error Bursts in Longer Messages," *IBM Journal* 7, 151 (1963).
2. Definitions of "shortened" and "unshortened" are those of Peterson, *Error-Correcting Codes*, The MIT Press and John Wiley and Sons, Inc., New York, 1961 (Chapter 8).
3. The notion of solid bursts was introduced to the author by G. Schillinger in a private communication.

Received July 31, 1963