XVIII. Communications Systems Research: Combinatorial Communication

TELECOMMUNICATIONS DIVISION

A. Cross-Correlations of Reverse Maximal-Length Shift Register Sequences,

T. A. Dowling[1] *and R. McEliece*

1. Introduction

Maximal-length binary shift register sequences with uniformly low cross-correlations are used for synchronization in spread spectrum communication systems (Ref. 1). In this article, a result on exponential sums in finite fields is applied to bound the cross-correlation of a maximal-length sequence with any phase shift of the reverse sequence. The result can also be applied to bound the non-zero weights of a certain $(2^k - 1, 2k)$ cyclic code.

2. A Bound on Cross-Correlations

If $a = (a_0, a_1, \cdots, a_{n-1})$ and $b = (b_0, b_1, \cdots, b_{n-1})$ are two sequences of length n over $GF\,(2)$, the cross-correlation function $C\,(\tau)$ with respect to a and b is defined by

$$C\,(\tau) = \sum_{i=0}^{n-1} s\,(a_i)\,s\,(b_{i+\tau})$$

where the subscripts are reduced modulo n and $s\,(x) = (-1)^x, x \in GF\,(2)$.

Consider the case where a is a maximal-length shift register sequence of length $2^k - 1$ and b is the reverse sequence, i.e., $b_i = a_{2^k-2-i}$, $i = 0, 1, \cdots, 2^k - 2$. Regard a as a non-null code word of the $(2^k - 1, k)$ cyclic code A generated by linear recursion (Ref. 2) by a primitive polynomial $f\,(x)$ of degree k over $GF\,(2)$. Then, the elements of a may be characterized by the Mattson–Solomon polynomial

$$g_a\,(x) = \mathrm{Tr}\,(cx)$$

where $c \in GF\,(2^k)$ and

$$\mathrm{Tr}\,(x) = \sum_{i=0}^{k-1} x^{2^i}$$

is the trace of $GF\,(2^k)\,/\,GF\,(2)$. The polynomial $g_a\,(x)$ satisfies $g_a\,(\alpha^i) = a_i, i = 0, 1, \cdots, 2^k - 2$, where α is a root of $f\,(x)$. With no loss of generality, a is assumed to be phase-shifted so that $c = 1$. Then,

$$b_i = \mathrm{Tr}\,(\alpha^{-(i+1)})$$

Thus,

$$C\,(\tau) = \sum_{i=0}^{2^k-2} (-1)^{\mathrm{Tr}\,(\alpha^i + \alpha^{-(\tau+1+i)})}$$

since $\mathrm{Tr}\,(x + y) = \mathrm{Tr}\,(x) + \mathrm{Tr}\,(y)$ for $x, y \in GF\,(2^k)$.

[1] NASA Summer Faculty Fellow, Dept. of Statistics, Univ. of No. Carolina.

Now, a result on exponential sums in finite fields is applied. This result was first proved by A. Weil (Ref. 3) and later, using different methods, by L. Carlitz and S. Uchiyama (Ref. 4). Let $K = GF(q)$, where $q = p^k$, and let $\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{k-1}}$; then, for any $c \in K$,

$$\left| \sum_{\substack{x \epsilon k \\ x \neq 0}} \exp\left[\frac{2\pi i \,\mathrm{Tr}(x + cx^{-1})}{p}\right] \right| \leqq 2q^{1/2} \qquad (1)$$

Setting $p = 2$ and $c = \alpha^{-(\tau+1)}$ and expressing x as α^i, Eq. (1) becomes

$$|C(\tau)| \leqq 2^{(k+2)/2} \qquad (2)$$

Calculations indicate that this bound is tight. It can be shown that $C(\tau) \equiv -1 \pmod 4$ for any τ. The extremal values, both maximum and minimum, satisfying Eq. (2) and this condition are attained for the cases computed ($k \leqq 8$).

3. Application to Coding Theory

The bound given by Eq. (1) can also be applied to bound the non-zero weights of the $(2^k - 1, 2k)$ cyclic code generated by $f(x) f^*(x)$ by linear recursion, where $f^*(x) = x^k f(1/x)$ is the reciprocal polynomial of $f(x)$. The Mattson–Solomon polynomial for this code is $g_a(x) = \mathrm{Tr}(cx) + \mathrm{Tr}(dx^{-1})$, where $c, d \in GF(2^k)$. If $w(c, d)$ denotes the weight of the code word with this polynomial, then $w(c, d) = w(1, cd)$ if $c \neq 0$, since the pairs (c, d) and $(1, cd)$ correspond to different cyclic shifts of the same code word. Hence, we can take $c = 1$ if $c \neq 0$. Then,

$$w(1, d) = \frac{2^k - 1 - \rho(d)}{2} \qquad (3)$$

where

$$\rho(d) = \sum_{\substack{x \in GF(2^k) \\ x \neq 0}} (-1)^{\mathrm{Tr}(x + dx^{-1})}$$

Thus, by Eq. (1), $|\rho(d)| \leqq 2^{(k+2)/2}$. Since $w(0, d) = 2^{k-1}$ if $d \neq 0$, we have, using Eq. (3),

$$2^{k-1} - 2^{k/2} - 1/2 \leqq w \leqq 2^{k-1} + 2^{k/2} - 1/2$$

where w is the weight of any non-zero code word of A.

References

1. Gold, R., "Optimal Binary Sequences for Spread Spectrum Multiplexing," (Correspondence), *IEEE Trans. Inform. Theory*, Vol. IT-13, pp. 619–621, 1967.
2. Mattson, H. F., and Solomon, G., "A New Treatment of Bose-Chaudhuri Codes," *J. Soc. Ind. Appl. Math.*, Vol. 9, pp. 654–669, 1961.
3. Weil, A., "On Some Exponential Sums," *Proc. Nat. Acad. Sci. U.S.A.*, Vol. 34, pp. 204–207, 1948.
4. Carlitz, L., and Uchiyama, S., "Bounds for Exponential Sums," *Duke Math. J.*, Vol. 24, pp. 37–41, 1957.