On a Sequence Conjectured to Have Ideal 2-level Autocorrelation Function

Anchung Chang Peter Gaal Solomon W. Golomb[1] Guang Gong P. Vijay Kumar
Communication Sciences Institute
University of Southern California
Los Angeles, CA 90089-2565 USA
Email kumar@aditya.usc.edu

Abstract — **In a recent paper, No, Golomb, Gong, Lee and Gaal conjectured that a certain family of sequences having a convenient trace description possesses the ideal autocorrelation property.**

More recent numerical results obtained by the authors of the present paper indicate that the linear cyclic code generated by the terms of the ideal autocorrelation sequence has the same 5-level weight distribution as does the dual of the triple-error correcting primitive BCH code.

It is shown that the conjectured autocorrelation sequences are balanced. It is proven that the dual of the cyclic code generated by the sequences has a minimal distance of at least 7. Also, a divisibility result is given concerning the weights of the cyclic code.

I. Introduction

For any integer $k \geq 1$ let $\mathbf{F}_{2^k}$ denote the finite field of 2^k elements. Let $m \geq 2$ be an integer and $n = 2m+1$. Let $T : \mathbf{F}_{2^n} \to \mathbf{F}_2$ denote the trace function given by

$$T(x) = \sum_{i=0}^{n-1} x^{2^i}, \quad x \in \mathbf{F}_{2^n}.$$

Let α be a primitive element of $\mathbf{F}_{2^n}$ and set $r = 2^{m+1}+1$. Based upon extensive numerical evidence, it has been conjectured by No, Golomb, Gong, Lee and Gaal [3] that the sequence

$$s(t) = T(\alpha^t + \alpha^{rt} + \alpha^{r^2 t})$$

has the ideal autocorrelation function, i.e.,

$$\sum_{t=0}^{2^n-2} (-1)^{s(t+\tau)+s(t)} = \begin{cases} 2^n-1 & \text{if } \tau = 0 \\ -1 & \text{else}. \end{cases}$$

This conjecture has been verified by computer to hold for all odd n, $5 \leq n \leq 23$.

Let $\mathcal{F}$ denote the family of 2^n+1 sequences

$$\mathcal{F} = \left\{T(\alpha^{rt} + \alpha^{r^2 t} + \alpha^{t+i}) \mid 0 \leq i \leq 2^n-2\right\} \bigcup \left\{T(\alpha^{rt} + \alpha^{r^2 t})\right\} \bigcup \{T(\alpha^t)\}.$$

More recent numerical results (for n odd, $5 \leq n \leq 19$) obtained by the authors suggest that the family of sequences $\mathcal{F}$ has the same correlation properties as the well-known family of Gold sequences.

Let $\mathcal{C}$ denote the $[2^n-1, 3n]$ binary cyclic code given by

$$\mathcal{C} = \left\{(T(a\alpha^t + b\alpha^{rt} + c\alpha^{r^2 t})) \mid a, b, c \in \mathbf{F}_{2^n}\right\}.$$

Here, our numerical results (for n odd, $5 \leq n \leq 15$) suggest that this code has the same weight distribution as does the dual of the triple-error correcting primitive BCH code of the same length.

II. Analytic Results

Our first result is that $s(t)$ has the balance property, i.e.,

$$\sum_{t=0}^{2^n-2} (-1)^{s(t)} = -1,$$

which is a necessary condition for the sequence to have the ideal autocorrelation property. This was shown by proving that the function

$$f(x) = x + x^r + x^{r^2}$$

is a permutation polynomial.

The second result concerns the cyclic code $\mathcal{C}$. It is shown that the dual of this code has minimum distance ≥ 7. This was done by using a result from [4], which states that the minimum distance of a linear cyclic code is equal to the rank of a matrix constructed by using the Discrete Fourier Transform. The bound on the minimal distance is supplied by a lower bound on the rank of this matrix.

The third result is that the Hamming weight of each codeword in $\mathcal{C}$ is divisible by 2^m. This was obtained by applying a theorem of McEliece's [1, 2], which connects the divisibility of the codeword weights with the smallest number of nonzeros of $\mathcal{C}$ whose product is 1. Finding this number was done by solving an equivalent nontrivial tiling problem.

Acknowledgements

The authors would like to acknowledge useful discussions with Kenneth Shum and Lloyd Welch.

References

[1] R. J. McEliece, "On periodic sequences from $GF(q)$," *J. Combin. Theory*, vol. 10, no. 1, pp. 80-91, Jan. 1971.

[2] F. J. McWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1979.

[3] J-S. No, S. W. Golomb, G. Gong, H-K. Lee and P. Gaal, "New Binary Pseudorandom Seqeucnes of Period $2^n - 1$ with Ideal Autocorrelation," to appear in the March 1998 issue of the *IEEE Trans. Inform. Theory.*

[4] Thomas Schaub, *A Linear Complexity Approach to Cyclic Codes,* Ph. D. Dissertation, 1988. Swiss Federal Institute of Technology Zuerich.

[1] The work was supported in part by the National Science Foundation under Grant Number NCR-9612864.

0-7803-5000-6/98/$10.00 © 1998 IEEE.