Hadamard Transforms of Three-Term Sequences

Guang Gong and Solomon W. Golomb

The Communication Sciences Institute
University of Southern California
Electrical Engineering-Systems, EEB#500
Los Angeles, California 90089-2565

Abstract: Certain three-term sequences of period $2^n - 1$ are conjectured to have the two-level autocorrelation property. In this note, a formula involving Hadamard transforms of three-term sequences is presented. Its validity has been verified by computer on the range of $5 \le n \le 23$.

Index terms: Hadamard transform, two-level autocorrelation sequences, m-sequences.

I. Conjecture

Let $n = 2m + 1$, $q = 1 + 2^m$, and α be a primitive element of $GF(2^n)$. Let $f(x) = Tr(x + x^q + x^{q^2})$ and $A = \{a_i\}$ where $a_i = f(\alpha^i)$. In reference [1], the sequence A is conjectured to have a two-level autocorrelation for all $n > 1$ and this conjecture has been verified for $3 \le n \le 23$. In this note, we present an interesting formula for the Hadamard transform of the sequence A or, equivalently, for the function $f(x)$. The Hadamard transform of $f(x)$ is defined by

$$\hat{f}(\lambda) = \sum_{x \in GF(2^n)} (-1)^{f(x) + Tr(\lambda x)}, \quad \lambda \in GF(2^n). \tag{1}$$

Conjecture. For $n \ge 5$, the Hadamard transform $\hat{f}(\lambda)$, $\lambda \in GF(2^n)$, of $f(x)$ is 3-valued with the values 0, $\pm 2^{m+1}$. Specially,

$$\hat{f}(\lambda) = 0 \qquad \Leftrightarrow Tr(\lambda^t) = 0,$$

$$\hat{f}(\lambda) = \pm 2^{m+1} \Leftrightarrow Tr(\lambda^t) = 1$$

where $t = \frac{2}{3}(2^{2l} - 1) + 1$ for $m = 2l$ or $2l + 1$ where $l \ge 1$.

The result has been verified by computer on the range of $5 \le n \le 23$.

II. Discussion

From $3t = 2(2^{2l} - 1) + 3 = 2^{2l+1} + 1$, which is relatively prime to $2^n - 1$, we have gcd(t, $2^n - 1$) = 1. Therefore, the Hadamard transform of $f(x)$ is determined by the m-sequence $\{Tr(\alpha^{it})\}_{i \ge 0}$. This is similar to the case of Gold sequences [2], as follows. Let $g(x) = Tr(x^{1+2^k})$ where $(k, n) = 1$. The Hadamard transform of $g(x)$ is

$$\hat{g}(\lambda) = \sum_{x \in GF(2^n)} (-1)^{g(x)+Tr(\lambda x)}, \ \lambda \in GF(2^n).$$

From reference [2], $\hat{g}(\lambda)$ is 3-valued with values 0, $\pm 2^{m+1}$, and

$$\hat{g}(\lambda) = 0 \quad \Leftrightarrow Tr(\lambda) = 0,$$

$$\hat{g}(\lambda) = \pm 2^{m+1} \Leftrightarrow Tr(\lambda) = 1.$$

I.e, the Hadamard transform of $g(x)$ is determined by the m-sequence $\{Tr(\alpha^i)\}_{i \ge 0}$. Thus we see that the three-term function $f(x)$ behaves like the monomial (one-term) function $Tr(x^{1+2^k})$ with respect to the Hadamard transform.

References

[1] J.S. No, S.W. Golomb, G. Gong, H.K. Lee, and P. Gaal, "New binary pseudorandom sequences of period 2^n - 1 with ideal autocorrelation," *IEEE Trans. on Inform. Theory*, vol. 44, No. 2, March 1998, pp.814-817.

[2] R. Gold, ``Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. on Inform. Theory*, vol. IT, January 1968, pp.154-156.