[16] J. Salz and S. B. Weinstein, "Fourier transform communication system," in *Proc. ACM Symp. Probl. Optimiz. Data Commun. Syst.*, Pine Mountain, GA, Oct. 1969, pp. 99–128.
[17] D. V. Sarwate, "An upper bound on the aperiodic autocorrelation function for a maximal-length sequence," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 685–687, July 1984.
[18] S. B. Weinstein and P. M. Ebert, "Data transmission by frequency-division multiplexing using the discrete Fourier transform," *IEEE Trans. Commun. Technol.*, vol. COM-19, pp. 628–634, 1971.
[19] M. S. Zimmerman and A. L. Kirsch, "The AN/GSC-10 (KATHRYN) variable rate data modem for HF radio," *IEEE Trans. Commun. Technol.*, vol. COM-15, pp. 197–205, 1967.

On the Linear Complexity of Hall's Sextic Residue Sequences

Jeong-Heon Kim and Hong-Yeop Song, *Member, IEEE*

***Abstract*—In this correspondence, the characteristic polynomial and hence the linear complexity of Hall's sextic residue sequences are determined.**

***Index Terms*—Characteristic polynomial, Hall's sextic residue sequences, linear complexity.**

I. Introduction

Periodic balanced binary sequences with optimal autocorrelation play an important role in many applications, including spread-spectrum communications, due to their apparent randomness property and ease of generation [12]. They are equivalent to cyclic Hadamard difference sets [1], [6], and every *known* example of such sequences has period that is either i) a prime congruent to $3 \bmod 4$, or ii) a product of twin primes, or iii) $2^n - 1$ for some integer n [4], [7], [13], [1].

For cryptographic applications, e.g., stream ciphers, one prefers such sequences with larger linear complexity. The linear complexity L of a periodic binary sequence is the number of stages of the shortest linear feedback shift register (LFSR) that will produce it with appropriate connection and initial condition [6]. The basic idea is that the sequence can completely be identified by some unwanted (or hostile) users if $2L$ terms are observed.

So far, the linear complexity of known examples of balanced binary sequences with optimal autocorrelation has been determined except for one case. Those with periods of type iii) above are the easiest examples because they are either m-sequences or sums of a few decimated m-sequences. For those of type ii), the result is further generalized so that the linear complexity of larger classes of sequences including twin-prime sequences have been determined [2]. For type i), there are Legendre sequences with period of every such prime and Hall's sextic residue sequences with period of such prime p that can also be written as $4u^2+27$ for some u. The linear complexity of Legendre sequences has been determined earlier by Turyn [14] and recently rediscovered by Ding *et al.* [3], and further, their explicit trace representation was determined [5], [11]. This correspondence determines the linear complexity and characteristic polynomial of Hall's sextic residue sequences.

Let $p = 4u^2 + 27 = 6f + 1$ be a prime and g be a primitive root modulo p. All the nonzero elements of the integers $\bmod p$ can be partitioned into six residue classes C_l, $l = 0, 1, 2, \ldots, 5$, as

$$C_l = \{g^{6i+l} | i = 0, 1, \ldots, f-1\}. \tag{1}$$

Hall's sextic residue sequence of period p is defined as

$$s_t = \begin{cases} 1, & \text{if } t \in C_0 \cup C_1 \cup C_3 \\ 0, & \text{otherwise} \end{cases}$$

where $t = 0, 1, \ldots, p-1$, and g is (and, always can be) selected such that $3 \in C_1$ [8].

II. Linear Complexity of Hall's Sextic Residue Sequences

If a binary sequence $\{s_t\}$ of period p has linear complexity L, then there exist constants $c_0 = 1, c_1, c_2, \ldots, c_{L-1}, c_L = 1 \in \mathrm{GF}(2)$ such that

$$s_i = c_{L-1}s_{i-1} + c_{L-2}s_{i-2} + \cdots + c_0 s_{i-L}, \qquad \text{for all } L \le i < p.$$

The polynomial $c(x) = x^L + c_{L-1}x^{L-1} + \cdots + c_0$ is called the characteristic polynomial of the sequence.

It is known that the reciprocal characteristic polynomial $c^*(x)$ of the sequence $\{s_t\}$ is given by [10]

$$\begin{aligned} c^*(x) &= c_0 x^L + c_1 x^{L-1} + \cdots + c_{L-1}x + 1 \\ &= (x^p - 1)/\gcd(x^p - 1, S(x)) \end{aligned}$$

where

$$S(x) = s_0 + s_1 x + \cdots + s_{p-1}x^{p-1}.$$

The linear complexity of $\{s_t\}$ is given by

$$L = p - \deg[\gcd(x^p - 1, S(x))].$$

For Hall's sextic residue sequence of period p, the corresponding $S(x)$ is given by

$$S(x) = C_0(x) + C_1(x) + C_3(x)$$

where, since $3 \in C_1$

$$C_l(x) = \sum_{i \in C_l} x^i = \sum_{i=0}^{f-1} x^{3^l g^{6i}}. \tag{2}$$

Then the linear complexity of Hall's sextic residue sequence of period p is given by

$$L = p - |\{j : S(\beta^j) = 0, 0 \le j \le p-1\}| \tag{3}$$

where β is a primitive pth root of unity over GF (2^n) that is the splitting field of $x^p - 1$.

Manuscript received April 25, 2000; revised December 6, 2000. This work was supported by the University Research Program supported by the Ministry of Information and Communication in Korea in the Program Year 1999.

The authors are with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul 120-749, Korea (e-mail: heon@yonsei.ac.kr; hysong@yonsei.ac.kr).

Communicated by A. M. Klapper, Associate Editor for Sequences.
Publisher Item Identifier S 0018-9448(01)04487-X.

To determine the linear complexity of Hall's sextic residue sequences, we need the following lemma.

Lemma 1: Let $p = 4u^2 + 27 = 6f + 1$ be a prime and β be a primitive pth root of unity.

P1. $|C_l| = (p-1)/6$, $aC_l = C_l$ for any $a \in C_0$ and $C_l(\beta) = C_0(\beta^{3^l})$.

P2. $C_l(\beta^a) = C_l(\beta)$ for any $a \in C_0$.

P3. $C_l(\beta^i) = C_l(\beta^j)$ if i and j are in the same residue class.

P4. If $2 \in C_0$, then $C_l(\beta) = 0$ or 1.

P5. $\sum_{l=0}^{5} C_l(\beta) = 1$.

P6. $-1 \in C_3$.

P7. If $p = 7 \bmod 8$ then $S(\beta)S(\beta^{-1}) = 0$. If $p = 3 \bmod 8$ then $S(\beta)S(\beta^{-1}) = 1$.

P8. If $p = 7 \bmod 8$ then $2 \in C_0$. If $p = 3 \bmod 8$ then $2 \in C_3$.

Proof: P1 follows from definitions (1) and (2). If $a \in C_0$, then $a = g^{6i}$ for some integer i. Then

$$C_l(\beta^a) = \sum_{j=0}^{f-1} (\beta^{g^{6i}})^{3^l g^{6j}} = \sum_{j=0}^{f-1} \beta^{3^l g^{6(i+j)}} = C_l(\beta)$$

which is P2. P3 is obtained by P2. If $2 \in C_0$, then $C_l(\beta)^2 = C_l(\beta^2) = C_l(\beta)$ by P2. Thus, if $2 \in C_0$, $C_l(\beta) = 0$ or 1. P5 is proven by

$$\sum_{l=0}^{5} C_l(\beta) = \sum_{l=0}^{5} \sum_{i=0}^{f-1} \beta^{3^l g^{6i}} = \sum_{j=1}^{p-1} \beta^j = 1.$$

Since $3f = (p-1)/2 = 2u^2 + 13$, f must be odd. Then P6 follows from the fact that

$$-1 = g^{(p-1)/2} = g^{(6f)/2} = g^{6(f-1)/2+3}.$$

For P7, we note that Hall's sextic residue sequence of period p induces a cyclic Hadamard difference set with parameters $v = p$, $k = (p-1)/2$, and $\lambda = (p-3)/4$ [1]. Therefore, we have

$$S(x)S(x^{-1}) = u^2 + 7 + (u^2 + 6) \sum_{i=0}^{p-1} x^i \pmod{x^p - 1}.$$

P7 is obtained by substituting β into x. P8 can be proved by observing that 2 is a cubic residue $\bmod p$ for any rational prime p [9]. □

Lemma 2: Let $p = 4u^2 + 27 = 7 \bmod 8$ and β be a primitive pth root of unity. Then one of $C_0(\beta) + C_3(\beta)$, $C_1(\beta) + C_4(\beta)$, and $C_2(\beta) + C_5(\beta)$ is 1 and the others must be 0.

Proof: If $p = 7 \bmod 8$ then $2 \in C_0$. Then from P4 and P5 in Lemma 1, either one of $C_0(\beta)+C_3(\beta)$, $C_1(\beta)+C_4(\beta)$, and $C_2(\beta)+C_5(\beta)$ is 1 or all three of them are 1. From P1 in Lemma 1, we have

$$C_1(\beta) + C_4(\beta) = C_0(\beta^3) + C_3(\beta^3) \tag{4}$$

$$C_2(\beta) + C_5(\beta) = C_0\left(\beta^{3^2}\right) + C_3\left(\beta^{3^2}\right). \tag{5}$$

Suppose that all of them are 1. Then from (4) and (5), $C_0(\beta^i) + C_3(\beta^i) = 1$ for all $i = 1, \ldots, p-1$. It also means that $C_1(\beta^i)+C_4(\beta^i)=1$ for all $i=1, \ldots, p-1$, which is impossible since the degree of $C_1(x)+C_4(x)+1$ is less than $p-1$. □

Theorem 1: Let $p = 6f + 1 = 7 \bmod 8$. Then there exists a primitive pth root β of unity such that $S(\beta) = 1$, and for such β, we have $S(\beta^j) = 0$ for all $j \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5$.

Proof: Let γ be a primitive pth root of unity. Then

$$\begin{aligned}\sum_{i=1}^{p-1} S(\gamma^i) &= \sum_{i=1}^{p-1} C_0(\gamma^i) + \sum_{i=1}^{p-1} C_1(\gamma^i) + \sum_{i=1}^{p-1} C_3(\gamma^i) \\ &= \sum_{j=0}^{5} C_0\left(\gamma^{3^j}\right) + \sum_{j=0}^{5} C_1\left(\gamma^{3^j}\right) + \sum_{j=0}^{5} C_3\left(\gamma^{3^j}\right) \\ &= \sum_{j=0}^{5} C_0\left(\gamma^{3^j}\right) = \sum_{k=0}^{p-2} \gamma^{g^k} = 1.\end{aligned}$$

Thus, there exists at least one i such that $S(\gamma^i) = 1$. Then $\beta = \gamma^i$ is what we want.

Now we will show that $S(\beta^j) = 0$ for all $j \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5$. From P3 in Lemma 1, it suffices to show that $S(\beta^{3^i}) = 0$ for $i = 1, \ldots, 5$. Since

$$S(\beta) = C_0(\beta) + C_1(\beta) + C_3(\beta) = 1$$

we have

$$S(\beta^{-1}) = S(\beta^{3^3}) = C_3(\beta) + C_4(\beta) + C_0(\beta) = 0$$

from P7 in Lemma 1. Then we have $C_1(\beta) + C_4(\beta) = 1$ and hence, from Lemma 2

$$C_0(\beta) + C_3(\beta) = C_2(\beta) + C_5(\beta) = 0.$$

Thus, we have $C_1(\beta) = 1$ and $C_4(\beta) = 0$. Furthermore,

$$S(\beta^3) = C_1(\beta) + C_2(\beta) + C_4(\beta) = C_2(\beta) + 1$$

$$S(\beta^{-3}) = S\left(\beta^{3^4}\right) = C_4(\beta) + C_5(\beta) + C_1(\beta) = C_5(\beta) + 1.$$

Thus, $S(\beta^3) = S(\beta^{3^4}) = 0$ since $S(\beta^3)S(\beta^{-3}) = 0$. Similarly, $S(\beta^{3^2}) = S(\beta^{3^5}) = 0$. □

Theorem 2: Hall's sextic residue sequence of period $p = 4u^2 + 27$ has the following reciprocal characteristic polynomial $c^*(x)$:

$$c^*(x) = \begin{cases} (x-1) \prod_{i \in C_0} (x - \beta^i), & \text{if } p \equiv 7 \bmod 8 \\ x^p - 1, & \text{if } p \equiv 3 \bmod 8 \end{cases}$$

where β is a primitive pth root of unity such that $S(\beta) = 1$. The linear complexity L is given by

$$L = \begin{cases} 1 + \dfrac{p-1}{6}, & \text{if } p \equiv 7 \bmod 8 \\ p, & \text{if } p \equiv 3 \bmod 8. \end{cases}$$

Proof: If $p \equiv 7 \bmod 8$, by Theorem 1 $S(\beta^a) = 1$ for $a \in C_0$ and $S(\beta^b) = 0$ for $b \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5$. Also $S(1) = [(p-1)/2 \bmod 2] = 1$. Thus, $c^*(x)$ is given by

$$c^*(x) = \frac{(x^p - 1)}{\gcd(x^p - 1, S(x))} = (x-1) \prod_{i \in C_0} (x - \beta^i)$$

which is over GF (2) since $2C_0 = C_0$. The linear complexity L is $1 + (p-1)/6$.

If $p \equiv 3 \bmod 8$, by P7 in Lemma 1 we have $S(\beta^j)S((\beta^j)^{-1}) = 1$ for $j = 1, \ldots, p-1$. That is, $S(\beta^j) \neq 0$ for $j = 1, \ldots, p-1$. Also $S(1) = [(p-1)/2 \bmod 2] = 1$ because $p = 3 \bmod 8$. Thus, $\gcd(x^p - 1, S(x)) = 1$ and hence $c^*(x) = x^p - 1$ and $L = p$. □

REFERENCES

[1] L. D. Baumert, *Cyclic Difference Sets*. New York: Springer-Verlag, 1971.

[2] C. Ding, "Linear complexity of generalized cyclotomic binary sequences of order 2," *Finite Fields Their Applic.*, vol. 3, pp. 159–174, 1997.

[3] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of Legendre sequences," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1276–1278, May 1998.

[4] J.-H. Kim and H.-Y. Song, "Existence of cyclic Hadamard difference sets and its relation to binary sequences with ideal autocorrelation," *J. Commun. and Networks*, vol. 1, no. 1, pp. 14–18, Mar. 1999.

[5] J.-H. Kim, M. Shin, and H.-Y. Song, "Trace representation of Legendre sequences," *Des., Codes Cryptogr.*, to be published.

[6] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA: Holden-Day, 1967. Revised edition: Laguna Hills, CA: Aegean Park, 1982.

[7] S. W. Golomb and H.-Y. Song, "A conjecture on the existence of cyclic Hadamard difference sets," *J. Statist. Planning and Infer.*, vol. 62, pp. 39–41, 1997.

[8] M. Hall, Jr., "A survey of difference sets," *Proc. Amer. Math. Soc.*, vol. 7, pp. 975–986, 1956.

[9] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed. New York: Springer-Verlag, 1990.

[10] R. Lidl and H. Neiderreiter, "Finite fields," in *Encyclop. Math. Its Applic.*. Reading, MA: Addison-Wesley, 1983, vol. 20.

[11] J.-S. No, H.-K. Lee, H. Chung, H.-Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," *IEEE Trans. Inform. Theory*, vol. 42, pp. 2254–2255, Nov. 1996.

[12] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*. Rockville: Comput. Sci., 1985. Revised edition: New York: McGraw-Hill, 1994.

[13] H.-Y. Song and S. W. Golomb, "On the existence of cyclic Hadamard difference sets," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1266–1268, July 1994.

[14] R. Turyn, "The linear generation of the Legendre sequences," *J. Soc. Ind. Appl. Math.*, vol. 12, no. 1, pp. 115–117, 1964.

On the Achievability of the Cramér–Rao Bound for Poisson Distribution

Ron Aharoni and Delman Lee, *Member, IEEE*

***Abstract*—This correspondence examines the Cramér–Rao (CR) bound for data obtained in emission tomography. The likelihood function involved is the combined probability of independent Poisson random variables, the expectation of each being a linear function $\boldsymbol{c}_i^T\boldsymbol{\lambda}$ of the parameter vector $\boldsymbol{\lambda}$. We investigated the achievability of the CR bound in the interior and on the boundary of the domain of the problem. For the former, we found that the CR bound is achievable if and only if the vectors $\boldsymbol{c}_i$'s are obtained from a basis for $\mathbb{R}^N$, by repeating some vectors, multiplied by constant factors. A similar result holds for the boundary case. The practical implication of the achievability condition is that the CR bound is not attainable for typical emission tomographic systems.**

***Index Terms*—Achievability, constrained Cramér–Rao (CR) bound, emission tomography.**

I. INTRODUCTION

We wish to study the behavior of the Cramér–Rao (CR) bound in emission tomography. The case of transmission tomography was studied by [1], [2]. In emission tomography, one injects into the subject some photon-emitting substance and obtains a vector of measurements, $\boldsymbol{y} = (y_1, \ldots, y_P)^T \in \mathbb{N}^P$, of the photon emissions in P directions (called *projection lines*). $\mathbb{N}$ is the set of natural numbers including zero. The problem is to obtain a spatial map of the density of the injected material from the projection line measurements. The probability distribution which emerges is (see, e.g., [3]–[5])

$$p(\boldsymbol{y}|\boldsymbol{\lambda}) = \prod_{i=1}^{P} \frac{e^{-\langle \boldsymbol{c}_i, \boldsymbol{\lambda}\rangle}\langle \boldsymbol{c}_i, \boldsymbol{\lambda}\rangle^{y_i}}{y_i!} \tag{1}$$

where $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_N)^T$, and λ_i is the average number of photon emissions in the ith pixel detected by the system. The $P \times N$ matrix $C = (\boldsymbol{c}_1, \ldots, \boldsymbol{c}_P)^T$ is called the *projection matrix*. An element c_{ij} of the projection matrix is the ratio of the mean number of emissions detected at the ith projection line from the jth pixel to the total number of emissions detected at the ith projection line.

For the distribution in (1) to make mathematical sense, we only require $\langle \boldsymbol{c}_i, \boldsymbol{\lambda}\rangle \geqslant 0$ for all i, where $\boldsymbol{c}_i, \boldsymbol{\lambda} \in \mathbb{R}^N$. (Note that the limit of $\langle \boldsymbol{c}_i, \boldsymbol{\lambda}\rangle^{y_i}$ as $\langle \boldsymbol{c}_i, \boldsymbol{\lambda}\rangle \to 0$ is well defined. That is, $\langle \boldsymbol{c}_i, \boldsymbol{\lambda}\rangle^{y_i} \to 1$ for $y_i = 0$, and $\langle \boldsymbol{c}_i, \boldsymbol{\lambda}\rangle^{y_i} \to 0$ for $y_i > 0$. Thus, the product term in (1) can be regarded as the Kronecker delta function when $\langle \boldsymbol{c}_i, \boldsymbol{\lambda}\rangle = 0$.) For the distribution in (1) to reflect the physical situation in emission tomography, we have the following physical constraints: $\lambda_i \geqslant 0$ and $c_{ij} \geqslant 0$ for all i, j. We shall investigate the CR bound without the physical constraints for most part of the correspondence, and return to the implication of the physical constraints in Section III-C.

Manuscript received November 20, 1998; revised December 20, 2000. This work was performed while the authors were with the Image Processing Group, University of Pennsylvania, Philadelpha, and was supported by NIH under Grants HL 28438 and CA 54356.

R. Aharoni is with the Department of Mathematics, Technion–Israel Institute of Technology, 32000 Haifa, Israel (e-mail: ra@techunix.technion.ac.il).

D. Lee is with TAL Apparel Ltd., Kowloon, Hong Kong (e-mail: delman@ieee.org).

Communicated by T. E. Fuja, Associate Editor At Large.

Publisher Item Identifier S 0018-9448(01)04425-X.