necessary and sufficient conditions in (24) derived in the previous sections also hold when carrier phase delays are considered—that is, $|\boldsymbol{R}|$ is maximized when

$$\sum_{\ell=1}^{L} g_{\ell i} g_{\ell j} \boldsymbol{\Theta}_{\ell i} \boldsymbol{X}_{\ell} \boldsymbol{\Theta}_{\ell j}^{\top} + \boldsymbol{W}_{ij} = \frac{E_{ij}}{N} \boldsymbol{I}_N, \qquad 1 \le i, j \le B. \quad (51)$$

And as before, it is possible that no such set of $\boldsymbol{X}_\ell$ exists, in which case, our results provide an upper/lower bound on sum capacity/TSC.

VI. Conclusion

The overall structure of collaborative but geographically dispersed bases is interesting in light of the proliferation of consumer wireless systems like 802.11 and the amount of dark fiber available from past fiber (over)deployments. In this correspondence, we considered an abstraction of such systems as multiple collaborating base stations and uniform channels between users and bases and derived bounds on sum capacity and TSC via structural properties of the received covariance matrix. We also showed that as compared to single-base systems, where maximizing sum capacity and minimizing TSC are equivalent problems, in multibase systems TSC and sum capacity optimization can lead to different results.

Acknowledgment

The authors wish to thank the Associate Editor, Giuseppe Caire, and the three anonymous reviewers for their constructive comments on an earlier version of the correspondence.

References

[1] P. Anigstein and V. Anantharam, "Ensuring convergence of the MMSE iteration for interference avoidance to the global optimum," *IEEE Trans. Inform. Theory*, vol. 49, pp. 873–885, Apr. 2003.

[2] A. Goldsmith, S. Jafar, and G. J. Foschini, "Exploring optimal multicellular multiple antenna systems," in *Proc. 2002 IEEE Vehicular Technology Conf.—VTC'02 Fall*, vol. 1, Vancouver, BC, Canada, Sept. 2002, pp. 261–265.

[3] S. V. Hanly and P. A. Whiting, "Information-theoretic capacity of multireceiver networks," *Telecommun. Syst.*, vol. 1, no. 1, pp. 1–42, 1993.

[4] R. A. Horn and C. A. Johnson, *Topics in Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1991.

[5] G. N. Karystinos and D. A. Pados, "New bounds on the total squared correlation and optimum design of DS-CDMA binary signature sets," *IEEE Trans. Commun.*, vol. 51, pp. 48–51, Jan. 2003.

[6] H. J. Landau and H. O. Pollack, "Prolate spheroidal wave functions, fourier analysis and uncertainty—III: The dimension of the space of essentially time- and band-limited signals," *Bell Syst. Tech. J.*, vol. 41, no. 4, pp. 1295–1335, July 1962.

[7] O. Popescu, C. Rose, and D. C. Popescu, "Maximizing the determinant for a special class of block-partitioned matrices," *Math. Probl. in Eng.*, vol. 2004, no. 1, pp. 49–62, May 2004.

[8] C. Rose, "CDMA codeword optimization: Interference avoidance and convergence via class warfare," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2368–2382, Sept. 2001.

[9] C. Rose, S. Ulukus, and R. Yates, "Wireless systems and interference avoidance," *IEEE Trans. Wireless Commun.*, vol. 1, pp. 415–428, July 2002.

[10] D. N. C. Tse and S. Hanly, "Multiaccess fading channels. Part I: Polymatroid structure, optimal resource allocation, and throughput capacities," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2796–2815, Nov. 1998.

[11] S. Ulukus and R. D. Yates, "Iterative construction of optimum signature sequence sets in synchronous CDMA systems," *IEEE Trans. Inform. Theory*, vol. 47, pp. 1989–1998, July 2001.

[12] P. Viswanath and V. Anantharam, "Optimal sequences and sum capacity of synchronous CDMA systems," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1984–1991, Sept. 1999.

[13] ——, "Optimal sequences for CDMA under colored noise: A Schur-saddle function property," *IEEE Trans. Inform. Theory*, vol. 48, pp. 1295–1318, June 2002.

[14] W. Yu, W. Rhee, S. Boyd, and J. M. Cioffi, "Iterative water-filling for Gaussian vector multiple-access channels," *IEEE Trans. Inform. Theory*, vol. 50, pp. 145–152, Jan. 2004.

Frequency Hopping Sequences With Optimal Partial Autocorrelation Properties

Yu-Chang Eun, Seok-Yong Jin, Yun-Pyo Hong, and Hong-Yeop Song, *Member, IEEE*

***Abstract*—We classify some p^k-ary (p prime, k integer) generalized m-sequences and generalized Gordon–Mills–Welch (GMW) sequences of period $p^{2k} - 1$ over a residue class ring $R = \mathrm{GF}(p)[\xi]/(\xi^k)$ having optimal partial Hamming autocorrelation properties. In frequency hopping (FH) spread-spectrum systems, these sequences are useful for synchronizing process. Suppose, for example, that a transmitting p^k-ary FH patterns of period $p^{2k} - 1$ are correlated at a receiver. Usually, the length of a correlation window, denoted by L, is shorter than the pattern's overall period. In that case, the maximum value of the out-of-phase Hamming autocorrelation is lower-bounded by $\lceil \frac{L}{p^k+1} \rceil$ but the classified sequences achieve this bound with equality for any positive integer L.**

***Index Terms*—Finite rings, frequency hopping, generalized Gordon–Mills–Welch (GGMW) sequences, Hamming correlation, partial autocorrelation.**

I. Introduction

In frequency hopping multiple-access (FHMA) spread-spectrum systems employing orthogonal modulation, we have to use a set of frequency hopping patterns to minimize the maximum of Hamming out-of-phase autocorrelation and cross correlation to effectively discriminate between their own signals and reduce multiple-access interference (MAI). Specific methods to generate such sets originate from the properties of m-sequences, Reed–Solomon codes, or combinatorial methods used in the ring of integers $\bmod p$ for appropriate prime p [1], [2]. For example, an optimal family of frequency hopping (FH) sequences having p^k (p is a prime and k is a positive integer) symbols can be easily constructed from m-sequence over a Galois field $\mathrm{GF}(p)$ [3] or from a generalized m-sequence (GM) or a generalized Gordon–Mills–Welch (GGMW) sequence over a polynomial residue class ring [4], [5]. Such sequences have optimal periodic autocorrelation functions. However, usually the length of a correlation window is shorter than the period of the chosen FH sequence due to the limited synchronization time or hardware complexity. Moreover, the window length may vary from time to time depending on the channel conditions. In that case, the partial Hamming autocorrelation,

Manuscript received January 13, 2004; revised May 20, 2004. This work was supported under Grant (R01-2003-000-10330-0) from the Basic Research Program of the Korea Science and Engineering Foundation. The material in this correspondence was presented at the IEEE International Symposium on Information Theory, Chicago, IL, June/July 2004

The authors are with Department of Electrical and Electronic Engineering, Yonsei University, 134 Shinchon-dong Seodaemun-gu, Seoul, Korea (e-mail: yc.eun@coding.yonsei.ac.kr; sy.jin@coding.yonsei.ac.kr; yp.hong@coding.yonsei.ac.kr; hy.song@coding.yonsei.ac.kr).

Communicated by K. G. Paterson, Associate Editor for Sequences.
Digital Object Identifier 10.1109/TIT.2004.834792

rather than the full-period Hamming autocorrelation, will play a major role in determining the synchronization performance.

The partial Hamming correlation function between two sequences $X = \{x(j)\}$ and $Y = \{y(j)\}$, for a period N and the correlation window length L starting at t, is defined as follows:

$$H_{XY}(\tau; t \mid L) = \sum_{j=t}^{t+L-1} h[x(j), y(j+\tau)], \qquad 0 \le \tau < N \tag{1}$$

where $h[x, y]$ is a binary Hamming function determined as $h[x, y] = 1$ if $x = y$ and $h[x, y] = 0$ if $x \neq y$. If $t = 0$ and $L = N$, (1) represents the conventional periodic Hamming correlation function $H_{XY}(\tau)$ as defined in [3]. Then the maximum of the partial Hamming autocorrelation function (HAF) along with window length L is defined as

$$H(X \mid L) = \max_{0<\tau<N,\ 0\le t<N} \{H_{XX}(\tau; t \mid L)\}. \tag{2}$$

In this correspondence, we classify GM and GGMW sequences having optimal partial Hamming autocorrelation properties irrespective of the length of the correlation window. The optimality of the partial Hamming autocorrelation property can be extended from the optimal criteria as presented in [3].

Definition 1: Let S be the set of all sequences of length N over a given alphabet A. We say that a sequence $X(\in S)$ is *strictly optimal* if $H(X \mid L) \le H(X' \mid L)$ for all $L \le N$ and all $X' \in S$.

II. Generalized Maximal Length and GMW Sequences

Let R be a polynomial residue class ring defined by $R = \mathrm{GF}(p)[\xi]/(w(\xi)^k)$, where $w(\xi)$ is an irreducible polynomial of degree m over $\mathrm{GF}(p)$, $m \ge 1$. From this point, we will consider only the case where $m = 1$ or $R = \mathrm{GF}(p)[\xi]/(\xi^k)$. In that case, any element $b \in R$ can be expressed via the *ideal basis representation*

$$b = b_0 + b_1\xi + \cdots + b_{k-1}\xi^{k-1} \tag{3}$$

where $b_i \in \mathrm{GF}(p)$. Thus, R can be written as

$$R = \mathrm{GF}(p) + \xi\,\mathrm{GF}(p) + \cdots + \xi^{k-1}\,\mathrm{GF}(p). \tag{4}$$

The Galois extension ring of R denoted as $\mathrm{GR}(R, r)$ is defined as $R[x]/(f(x))$ where $f(x)$ is a basic monic irreducible polynomial of degree r over R. This $f(x)$ can be selected from the monic irreducible polynomials over $\mathrm{GF}(p)$ since $\mathrm{GF}(p)$ is a subring of R and any irreducible polynomial defined over the subring $\mathrm{GF}(p)$ is obviously irreducible over R [5]. Similarly to (3) and (4), any element $\beta(\in \mathrm{GR}(R, r))$ and $\mathrm{GR}(R, r)$ can be expressed as

$$\beta = \beta_0 + \beta_1\xi + \cdots + \beta_{k-1}\xi^{k-1}$$
$$\mathrm{GR}(R, r) = \mathrm{GF}(p^r) + \xi\,\mathrm{GF}(p^r) + \cdots + \xi^{k-1}\,\mathrm{GF}(p^r)$$

where $\beta_i \in \mathrm{GF}, (p^r)$.

For

$$\beta = \sum_{i=0}^{k-1} \beta_i \xi^i \in \mathrm{GR}(R, r)$$

let the mapping $\sigma^s\colon \beta \mapsto \sum_{i=0}^{k-1} {\beta_i}^{p^s} \xi^i$ denote a Frobenius automorphism of $\mathrm{GR}(R, r)$. If $s|r$, the trace function $\mathrm{Tr}_s^r(\cdot)$ from $\mathrm{GR}(R, r)$ into its subring $\mathrm{GR}(R, s)$ is calculated as

$$\begin{aligned}\mathrm{Tr}_s^r(\beta) &= \sum_{i=0}^{(r/s)-1} \sigma^{si}(\beta)\\ &= \sum_{i=0}^{(r/s)-1} \sum_{j=0}^{k-1} \beta_j^{p^{si}} \xi^j = \sum_{j=0}^{k-1} \mathrm{tr}_s^r(\beta_j)\xi^j\end{aligned} \tag{5}$$

where

$$\mathrm{tr}_s^r(v) = \sum_{i=0}^{(r/s)-1} v^{p^{si}}$$

is the field trace function from $\mathrm{GF}(p^r)$ to $\mathrm{GF}(p^s)$. The trace function defined in (5) has the following properties:

1) $\mathrm{Tr}_s^r(\beta) = \mathrm{Tr}_s^r(\sigma^{si}(\beta))$, $\forall i$ and $\forall \beta \in \mathrm{GR}(R, r)$;
2) $\mathrm{Tr}_s^r(b\beta + c\gamma) = b\mathrm{Tr}_s^r(\beta) + c\mathrm{Tr}_s^r(\gamma)$, $\forall\, b, c \in \mathrm{GR}(R, s)$ and $\forall \beta, \gamma \in \mathrm{GR}(R, r)$;
3) for any fixed $b \in \mathrm{GR}(R, s)$, the equation $\mathrm{Tr}_s^r(\beta) = b$ has exactly $p^{k(r-s)}$ solutions.

When α is a root of a primitive basic irreducible polynomial $f(x)$ over $R = \mathrm{GF}(p)[\xi]/(\xi^k)$ and the Galois extension ring is defined as $\mathrm{GR}(R, r) = R[x]/(f(x))$, every *GM* sequence $S^\nu = \{s^\nu(i)\}$ over R has the following unique trace representation [5]:

$$s^\nu(i) = \mathrm{Tr}_1^r(\nu\alpha^i), \qquad \nu \in \mathrm{GR}(R, r).$$

For $a = \sum_{i=0}^{k-1} a_i\xi^i \in \mathrm{GR}(R, s)$, let us define a permutation monomial

$$\Psi^d : a \mapsto \sum_{i=0}^{k-1} a_i^d \xi^i.$$

Then, every GGMW sequence [5], extended from a GMW sequence over a finite field [6], [7], can be represented as

$$s^\nu(i) = \mathrm{Tr}_1^s(\Psi^d[\mathrm{Tr}_s^r(\nu\alpha^i)]), \qquad \nu \in \mathrm{GR}(R, r)$$

where $s|r$ and $\gcd(d, p^s - 1) = 1$.

III. GM and GGMW Sequences With Optimal Partial Autocorrelation Property

For a frequency hopping sequence X of period N and a given correlation window of length $L\ (\le N)$, we derive a lower bound on the maximum out-of-phase autocorrelation value $H(X \mid L)$, defined in (2). We use the special case $H(X) = H(X \mid N)$. We start from the minimum bound on $H(X)$ presented in [3].

Lemma 1: For every sequence $X = \{x(j)\}$ of length N over an alphabet A of size $|A| = m$

$$H(X) \ge \overline{H}(X) \ge \frac{(N-b)(N+b-m)}{m(N-1)} \tag{6}$$

where b is the least nonnegative residue of N modulo m and $\overline{H}(X)$ is the average out-of-phase value of $H_{XX}(\tau)$.

Using the preceding lemma, we can derive the following lower bound on the partial HAF maxium.

Corollary 1:

$$H(X \mid L) \ge \frac{L}{N}\ \frac{(N-b)(N+b-m)}{m(N-1)}. \tag{7}$$

Proof: Let us derive the average out-of-phase value of $H_{XX}(\tau; t \mid L)$ as defined in (1)

$$\begin{aligned}\overline{H}(X \mid L) &= \frac{\sum_{\tau=1}^{N-1}\sum_{t=0}^{N-1} H_{XX}(\tau; t \mid L)}{(N-1)N}\\ &= \frac{\sum_{\tau=1}^{N-1}\ L\,H_{XX}(\tau; 0 \mid N)}{(N-1)N}\\ &= \frac{L}{N}\ \frac{\sum_{\tau=1}^{N-1} H_{XX}(\tau)}{(N-1)}\\ &= \frac{L}{N}\ \overline{H}(X).\end{aligned}$$

Then $H(X \mid L) \ge \overline{H}(X \mid L)$ and (6) yields the result. □

Now, we classify some *strictly optimal* GM or GGMW sequences which achieve the lower bound given in (7). First, let us choose a degree $2k$ primitive irreducible polynomial $f(x)$ over GF(p) as a primitive basic irreducible polynomial over $R = \mathrm{GF}(p)[\xi]/(\xi^k)$. Assume $f(\alpha) = 0$ and

$$\nu = \alpha^{e_0} + \alpha^{e_1}\xi + \cdots + \alpha^{e_{k-1}}\xi^{k-1} \in \mathrm{GR}(R, 2k).$$

Then

$$s^\nu(i) = \mathrm{Tr}_1^k\Big(\Psi^d[\mathrm{Tr}_k^{2k}(\nu\alpha^i)]\Big)$$

will be a p^k-ary sequence, of period $p^{2k}-1$, if all the α^{e_j}'s are linearly independent over GF(p) and $\gcd(d, p^k - 1) = 1$. In that case, the maximum out-of-phase value calculated for a given L is bounded using (7), as

$$H(S^\nu \,|L\,) \geq \left\lceil \frac{L}{p^k+1} \right\rceil. \tag{8}$$

Subsequently, the following theorem can be used to classify the *strictly optimal* GGMW sequences satisfying the equality in (8) for any positive integer L. Here L is at most $p^{2k}-1$, the period of S^ν.

Theorem 1: Let $f(x)$ be a degree $2k$ primitive polynomial over GF(p), $f(\alpha) = 0$, and $\gcd(d, p^k - 1) = 1$. A GGMW sequence $\{s^\nu(i)\}$

$$s^\nu(i) = \mathrm{Tr}_1^k\Big(\Psi^d[\mathrm{Tr}_k^{2k}(\nu\alpha^i)]\Big),$$
$$\nu = \alpha^{e_0} + \alpha^{e_1}\xi + \alpha^{e_2}\xi^2 + \cdots + \alpha^{e_{k-1}}\xi^{k-1}$$

is *strictly optimal* if and only if $\alpha^{e_0 d}, \alpha^{e_1 d}, \alpha^{e_2 d}, \ldots, \alpha^{e_{k-1} d}$ are linearly independent over GF(p) and $e_i \equiv e_j \pmod{p^k+1}$ for all $i, j,\ 0 \leq i, j \leq k-1$.

Proof: Since $\alpha^{(e_j - e_0)d} \in \mathrm{GF}(p^k)$ for all j if $e_j \equiv e_0 \pmod{p^k+1}$

$$s^\nu(i) - s^\nu(i+\tau) = \sum_{j=0}^{k-1} \mathrm{tr}_1^k\bigg(\alpha^{(e_j-e_0)d}\Big[(\mathrm{tr}_k^{2k}(\alpha^{i+e_0}))^d - (\mathrm{tr}_k^{2k}(\alpha^{i+\tau+e_0}))^d\Big]\bigg)\xi^j \tag{9}$$

for a GGMW sequence S^ν and a fixed nonzero τ. Then (9) will be equal to zero exactly when all ξ^j's coefficients are zero, or equivalently

$$\mathrm{tr}_1^k\bigg(\alpha^{(e_j-e_0)d}\Big[(\mathrm{tr}_k^{2k}(\alpha^{i+e_0}))^d - (\mathrm{tr}_k^{2k}(\alpha^{i+\tau+e_0}))^d\Big]\bigg) = 0 \tag{10}$$

for all $j,\ 0 \leq j \leq k-1$. Since all the $\alpha^{(e_j-e_0)d}$'s are linearly independent over GF(p) they form a basis for GF(p^k). Therefore, (10) occurs only if

$$(\mathrm{tr}_k^{2k}(\alpha^{i+e_0}))^d - (\mathrm{tr}_k^{2k}(\alpha^{i+\tau+e_0}))^d = 0 \tag{11}$$

as proven in [8]. However, since the given monomial is a simple permutation, the number of solutions for $0 \leq i \leq p^{2k}-2$ in (11) is the same for any value of d, namely, $d = 1$. Therefore,

$$\begin{aligned} &H_{S^\nu S^\nu}(\tau; t \mid L) \\ &= \Big|\{\, i | s^\nu(i) - s^\nu(i+\tau) = 0, t \leq i \leq t+L-1\}\Big| \\ &= \Big|\{\, i | \mathrm{tr}_k^{2k}\Big(\alpha^{i+e_0}(1-\alpha^\tau)\Big) = 0, t \leq i \leq t+L-1\}\Big|. \end{aligned} \tag{12}$$

To evaluate (12) with a window length L and a nonzero τ given, we need the following lemma as explained in [1].

Lemma 2: Let m-sequence $b(i)$ over GF(p^s), p prime, be defined as

$$b(i) = \mathrm{tr}_s^{rs}(\alpha^i)$$

where α is a primitive element of GF(p^{rs}), and let $T = (p^{rs} - 1)/(p^s - 1)$. Then every segment of T consecutive symbols from $b(i)$ contains exactly $(p^{(r-1)s} - 1)/(p^s - 1)$ zeros.

Applying Lemma 2, we observe that an m-sequence represented by $\mathrm{tr}_k^{2k}(\alpha^i)$ produces only one zero symbol in every segment of $p^k + 1$ consecutive indices i. Since $\mathrm{tr}_k^{2k}(\alpha^{i+e_0}(1-\alpha^\tau))$ is a cyclic-shifted version of $\mathrm{tr}_k^{2k}(\alpha^i)$ when $\tau \neq 0$, (12) becomes

$$H_{S^\nu S^\nu}(\tau; t \mid L) = \begin{cases} \frac{L}{p^k+1}, & \text{if } (p^k+1)|L \\ \left\lceil \frac{L}{p^k+1} \right\rceil \text{ or } \left\lceil \frac{L}{p^k+1} \right\rceil - 1, & \text{otherwise.} \end{cases}$$

This proves that

$$H(S^\nu \,|L\,) = \lceil L/(p^k+1) \rceil. \tag{13}$$

Conversely, assume that S^ν is *strictly optimal*. For $L = 1$ and an arbitrary but fixed τ, it is obvious that t^* exists such that

$$H_{S^\nu S^\nu}(\tau; t^* \,|\, 1) = 1$$

where $s^\nu(t^*) - s^\nu(t^* + \tau) = 0$. Since S^ν satisfies the bound (13) for any L, it yields

$$H_{S^\nu S^\nu}(\tau; t^* \,|\, L) = w$$

for $(w-1)(p^k+1) < L \leq w(p^k+1)$. This produces

$$s^\nu(t^*+i) - s^\nu(t^*+i+\tau) = \begin{cases} 0, & \text{if } i \equiv 0 \pmod{p^k+1} & \text{(14a)} \\ \text{nonzero}, & \text{otherwise.} & \text{(14b)} \end{cases}$$

Since (14a) indicates that

$$s^\nu(t^* + j(p^k+1)) - s^\nu(t^* + j(p^k+1) + \tau) = 0$$

for all $j,\ 0 \leq j < p^k - 1$, each ξ^l's coefficient of the equation must be zero as

$$\mathrm{tr}_1^k\bigg(\alpha^{j(p^k+1)d}\Big[(\mathrm{tr}_k^{2k}(\alpha^{t^*+e_l}))^d - (\mathrm{tr}_k^{2k}(\alpha^{t^*+e_l+\tau}))^d\Big]\bigg) = 0. \tag{15}$$

As j varies from 0 to $p^k - 2$, $\alpha^{j(p^k+1)d}$ passes through all the elements in GF(p^k). This indicates that the difference of two inner traces in (15) will be zero for the same reason as was applied to (10) to produce (11). Because of the permutation property of the given monomial, applying $d = 1$ to this equation will not change the solutions of e_l with t^* and τ fixed. This yields the following equation involving e_l:

$$\mathrm{tr}_k^{2k}\Big(\alpha^{t^*+e_l}(1-\alpha^\tau)\Big) = 0. \tag{16}$$

Since an m-sequence $\mathrm{tr}_k^{2k}(\alpha^e)$ produces only one zero symbol in every segment of p^k+1 consecutive indices e, we have $e_i \equiv e_j (\mathrm{mod}\, p^k+1)$ for all $i, j,\ 0 \leq i, j \leq k-1$ in (16).

Next, to show that $\alpha^{e_0 d}, \alpha^{e_1 d}, \alpha^{e_2 d}, \ldots, \alpha^{e_{k-1} d}$ are linearly independent, we assume the contrary. Then there exist $c_0, c_1, \ldots, c_{k-1}$ which are not all-zero in GF(p) satisfying

$$\sum_{l=0}^{k-1} c_l \alpha^{e_l d} = 0.$$

Assuming that $c_l \neq 0$ and $\gamma \in \mathrm{GF}(p^k)$, the following equation is obviously true:

$$\mathrm{tr}_1^k(\alpha^{(e_l-e_0)d}\gamma) = -\sum_{j=0, j\neq l}^{k-1} \frac{c_j}{c_l}\, \mathrm{tr}_1^k(\alpha^{(e_j-e_0)d}\gamma). \tag{17}$$

TABLE I

THREE 27-ARY GM SEQUENCES HAVING A PERIOD OF $3^6 - 1$

(e_0, e_1, e_2)	GM Sequences (Frequency Hopping Patterns)
$(0, 1, 2)$	0 0 0 9 3 1 0 0 18 15 5 1 0 9 12 13 4 1 18 6 2 9 3 10 21 7 20 15 23 25 26 $\cdots$
$(0, 17, 100)$	21 0 9 15 18 19 21 18 3 24 2 7 3 24 15 25 4 4 15 9 20 21 0 25 6 19 8 21 14 19 17 $\cdots$
$(0, 28, 56)$	24 3 6 15 24 22 21 6 18 18 5 1 24 15 0 25 4 13 9 15 14 21 18 4 3 4 20 3 26 1 2 $\cdots$

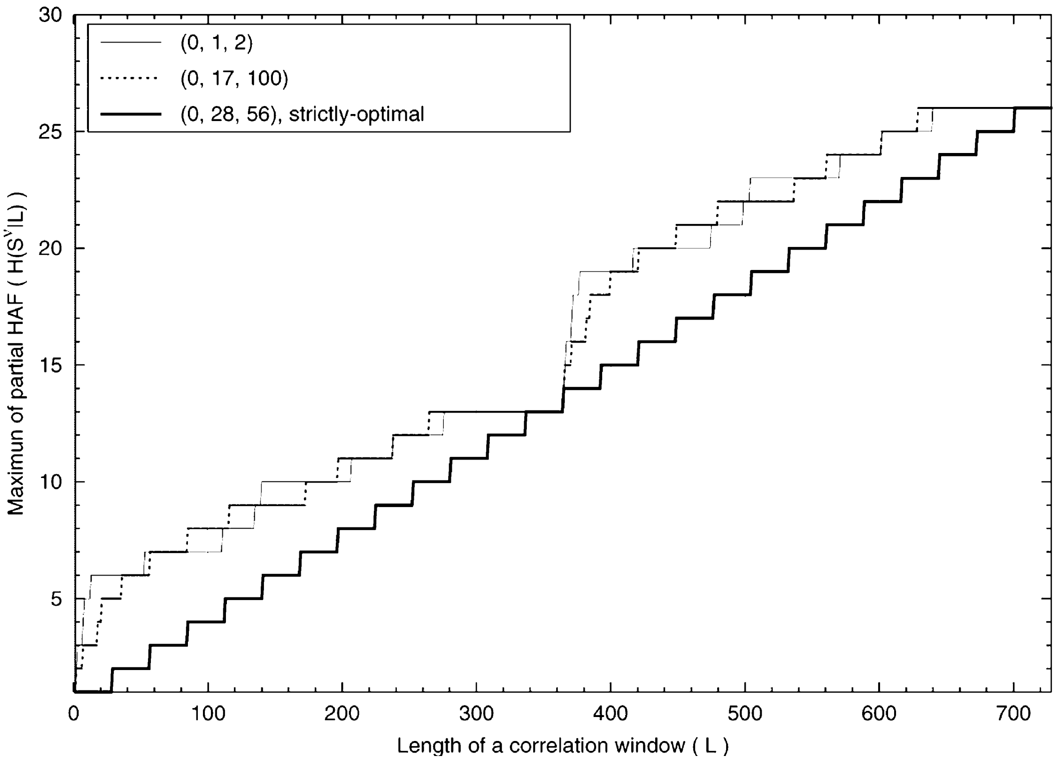

Fig. 1. $H(S^\nu|L)$ of three GM sequences represented by (e_0, e_1, e_2).

Applying (17) to (9), the trace term of ξ^l's coordinate can be described by a linear combination of the remaining trace terms. Since (9) is, in this case, related to the binary Hamming function of a GGMW sequence derived over GR(R', r) where $R' = \text{GF}(p)[\xi]/\xi^{k-1}$, zero occurs in (9) at least $p^{k+1} - 1$ times during one period. This demonstrates that S^ν is not optimal even in the case of full-period autocorrelation, which is a contradiction. □

For GM sequences, we can obtain a similar result.

Corollary 2: Let $f(x)$ be a degree $2k$ primitive polynomial over GF(p) and $f(\alpha) = 0$. A GM sequence $\{s^\nu(i)\}$,

$$s^\nu(i) = \text{Tr}_1^{2k}(\nu\alpha^i), \quad \nu = \alpha^{e_0} + \alpha^{e_1}\xi + \alpha^{e_2}\xi^2 + \cdots + \alpha^{e_{k-1}}\xi^{k-1}$$

is strictly optimal if and only if $\alpha^{e_0}, \alpha^{e_1}, \alpha^{e_2}, \ldots, \alpha^{e_{k-1}}$ are linearly independent over GF(p) and $e_i \equiv e_j (\text{mod} p^k + 1)$ for all $i, j,\ 0 \leq i, j \leq k - 1$.

Proof: Applying $d = 1$ in Theorem 1 yields this corollary. □

Example 1: In Table I, we represent three GM sequences over $R = \text{GF}(3)[\xi]/\xi^3$ where

$$s^\nu(i) = \text{Tr}_1^6(\nu\alpha^i), \qquad \nu = \alpha^{e_0} + \alpha^{e_1}\xi + \alpha^{e_2}\xi^2 \in \text{GR}(R, 6)$$

and α is a root of a primitive polynomial $x^6 + x + 2$ over GF(3). Although both sequences $(e_0, e_1, e_2) = (0, 1, 2)$ and $(e_0, e_1, e_2) = (0, 17, 100)$ have the optimal periodic Hamming autocorrelation properties they are *not strictly optimal* as shown in Fig. 1. However, any sequence satisfying Theorem 1 must be *strictly optimal*, for example, $(e_0, e_1, e_2) = (0, 28, 56)$ where any $e_a - e_b$ for $a \neq b$ is divisible by $28 = 3^3 + 1$, and $1, \alpha^{28}, \alpha^{2 \cdot 28}$ are linearly independent over GF(3).

IV. Concluding Remarks

Optimal families of FH sequences can be constructed from these classified GM and GGMW sequences by using the same method as presented in [5]. Then all the sequences in such a family have the same optimal partial Hamming autocorrelation properties. In this correspondence, we have only considered the case in which $w(\xi) = \xi$ for $R = \text{GF}(p)[\xi]/(w(\xi)^k)$. Therefore, further study should focus on a more general case when the degree of $w(\xi)$ is greater than one.

References

[1] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*. Rockville, MD: Computer Sci., 1985.

[2] D. V. Sarwate, "Reed-Solomon codes and the design of sequences for spread-spectrum multiple-access communications," in *Reed-Solomon Codes and their Applications*, S. B. Wicker and V. K. Bhargava, Eds. Piscataway, NJ: IEEE Press, 1994, pp. 175–204.

[3] A. Lempel and H. Greenberger, "Families of sequences with optimal Hamming correlation properities," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 90–94, Jan. 1974.

[4] P. V. Komo and S. C. Liu, "Maximal length sequences for frequency hopping," *IEEE J. Select. Areas Commun.*, vol. 8, pp. 819–822, Jun. 1990.

[5] P. Udaya and M. U. Siddiqi, “Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings,” *IEEE Trans. Inform. Theory*, vol. 44, pp. 1492–1503, July 1998.

[6] W. H. Mills, B. Gordon, and L. R. Welch, “Some new difference sets,” *Canadian J. Math.*, vol. 14, pp. 614–625, 1962.

[7] M. Antweiler and L. Bomer, “Complex optimal sequences over GF (p^M) with a two-level autocorrelation function and a linear span,” *IEEE Trans. Inform. Theory*, vol. 38, pp. 120–130, Jan. 1992.

[8] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Norwall, MA: Kluwer, 1987.

Compression Mappings on Primitive Sequences Over $Z/(p^e)$

Xuan Yong Zhu and Wen Feng Qi

***Abstract*—Let $Z/(p^e)$ be the integer residue ring with odd prime $p \geq 5$ and intetger $e \geq 2$. For a sequence $\underline{a}$ over $Z/(p^e)$, there is a unique p-adic expansion $\underline{a} = \underline{a}_0 + \underline{a}_1 \cdot p + \cdots + \underline{a}_{e-1} \cdot p^{e-1}$, where each $\underline{a}_i$ is a sequence over $\{0, 1, \ldots, p-1\}$, and can be regarded as a sequence over the finite field GF (p) naturally. Let $f(x)$ be a primitive polynomial over $Z/(p^e)$, and $G'(f(x), p^e)$ the set of all primitive sequences generated by $f(x)$ over $Z/(p^e)$. Set**

$$\varphi_{e-1}(x_0, \ldots, x_{e-1}) = x_{e-1}^k + \eta_{e-2,1}(x_0, x_1, \ldots, x_{e-2})$$
$$\psi_{e-1}(x_0, \ldots, x_{e-1}) = x_{e-1}^k + \eta_{e-2,2}(x_0, x_1, \ldots, x_{e-2})$$

where $\eta_{e-2,1}$ and $\eta_{e-2,2}$ are arbitrary functions of $e-1$ variables over GF (p) and $2 \leq k \leq p-1$. Then the compression mapping

$$\varphi_{e-1} : \begin{cases} G'(f(x), p^e) \rightarrow \text{GF}\,(p)^\infty \\ \underline{a} \rightarrow \varphi_{e-1}(\underline{a}_0, \ldots, \underline{a}_{e-1}) \end{cases}$$

is injective, that is, $\underline{a} = \underline{b}$ if and only if

$$\varphi_{e-1}(\underline{a}_0, \ldots, \underline{a}_{e-1}) = \varphi_{e-1}(\underline{b}_0, \ldots, \underline{b}_{e-1})$$

for $\underline{a}, \underline{b} \in G'(f(x), p^e)$. Furthermore, if $f(x)$ is a strongly primitive polynomial over $Z/(p^e)$, then

$$\varphi_{e-1}(\underline{a}_0, \ldots, \underline{a}_{e-1}) = \psi_{e-1}(\underline{b}_0, \ldots, \underline{b}_{e-1})$$

if and only if

$$\underline{a} = \underline{b} \text{ and } \varphi_{e-1}(x_0, \ldots, x_{e-1}) = \psi_{e-1}(x_0, \ldots, x_{e-1})$$

for $\underline{a}, \underline{b} \in G'(f(x), p^e)$.

***Index Terms*—Compressing mapping, integer residue ring, linear recurring sequence, primitive sequence.**

I. Introduction

Suppose p is a prime and $R_e = Z/(p^e)$ is the integer residue ring modulo p^e, which can be also represented as $\{0, 1, \ldots, p^e - 1\}$. In this correspondence, given positive integer $m \geq 2$, we always consider $a (\bmod\, m)$ as an element in $\{0, 1, \ldots, m-1\}$.

Manuscript received June 9, 2003; revised May 13, 2004. This work was supported by the Foundation for the Author of National Excellent Doctoral Dissertation of P. R. China under Grant 200060 and by the National Natural Science Foundation of China under Grant 60373092.

The authors are with Department of Applied Mathematics, Zhengzhou Information Engineering University, Zhengzhou, 450002, China (e-mail: xuanyong.zhu@263.net; wenfeng.qi@263.net).

Communicated by K. G. Paterson, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2004.834791

Let $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ be a monic polynomial with degree $n \geq 1$ over R_e. A sequence $\underline{a} = (a(t))_{t \geq 0}$ over R_e satisfying the recursion

$$a(i+n) = -[c_0 a(i) + c_1 a(i+1) + \cdots + c_{n-1} a(i+n-1)] (\bmod\, p^e)$$

for $i = 0, 1, 2, \ldots$, is called a linear recurring sequence of degree n over R_e, generated by $f(x)$. $G(f(x), p^e)$ denotes the set of all sequences over R_e generated by $f(x)$. Reference [8] is a good introduction on linear recurring sequences over R_e.

Let $\underline{a} = (a(t))_{t \geq 0}$ and $\underline{b} = (b(t))_{t \geq 0}$ be sequences over R_e and $c \in R_e$. Define $\underline{a} + \underline{b} = (a(t) + b(t))_{t \geq 0}$, $c\underline{a} = (c \cdot a(t))_{t \geq 0}$, $\underline{a} \cdot \underline{b} = (a(t) \cdot b(t))_{t \geq 0}$, and the shift operator of sequence $x^k \underline{a} = (a(t+k))_{t \geq 0}$ for $k = 0, 1, 2, \ldots$. So we have

$$G(f(x), p^e) = \{\underline{a} \in R_e^\infty \mid f(x)\underline{a} = \underline{0}\}.$$

Especially, we set

$$G'(f(x), p^e) = \{\underline{a} \in G(f(x), p^e) \mid \underline{a} \not\equiv \underline{0} (\bmod\, p)\}.$$

If $f(0) \not\equiv 0 (\bmod\, p)$, then there always exists a positive integer P such that $f(x)$ divides $x^P - 1$ over $Z/(p^e)$. The least such P is called the period of $f(x)$ over $Z/(p^e)$ and denoted by $\text{per}\,(f(x), p^e)$, which is upper-bounded by $p^{e-1}(p^n - 1)$, where $n = \deg f(x)$.

Definition 1: Let $f(x)$ be a monic polynomial of degree n over $Z/(p^e)$, then $f(x)$ is called a primitive polynomial if $\text{per}(f(x), p^e) = p^{e-1}(p^n - 1)$ (see [3], [7], and [19]).

Let $f(x)$ be a primitive polynomial of degree n over $Z/(p^e)$, then $f(x) (\bmod\, p^i)$ is also a primitive polynomial over $Z/(p^i)$, whose period is

$$\text{per}(f(x), p^i) = p^{i-1}(p^n - 1), \qquad i = 1, 2, \ldots, e-1.$$

In particular, $f(x) (\bmod\, p)$ is a primitive polynomial over the prime field GF (p), see [11]. Thus, we have

$$x^{p^{i-1}T} \equiv 1 + p^i h_i(x) (\bmod\, f(x)) \tag{1}$$

for $i = 1, 2, \ldots, e-1$, where $T = p^n - 1$ and $h_i(x)$ is a polynomial over $Z/(p^e)$ of degree less than n satisfying $h_i(x) \not\equiv 0 (\bmod\, p)$. Clearly, $h_i(x)$ is coprime with $f(x) (\bmod\, p)$ over $Z/(p)$. Furthermore, we have [1], [7]

1) if $p = 2$, then $h_2(x) = \cdots = h_{e-1}(x) \not\equiv 0 (\bmod\, 2)$ and $h_2(x) = h_1(x) + h_1(x)^2 (\bmod\, f(x))$;
2) if $p \geq 3$, then $h_1(x) = h_2(x) = \cdots = h_{e-1}(x) \not\equiv 0 (\bmod\, p)$.

For the primitive polynomial $f(x)$ over $Z/(p^e)$, we always set

$$h(x) = h_1(x) (\bmod\, p) \tag{2}$$

where $h_1(x)$ is defined by (1). We call $f(x)$ a strongly primitive polynomial over $Z/(p^e)$, if $\deg h(x) \geq 1$ for the case of $p \geq 3$ or $p = e = 2$, and $\deg h_2(x) \geq 1$ for the case of $p = 2$ and $e \geq 3$. Obviously, we have $\deg f(x) \geq 2$ for the strongly primitive polynomial $f(x)$ over $Z/(p^e)$ with $e \geq 2$ (see [15]).