[4] S. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Select. Aareas Commun.*, vol. 16, pp. 1451–1458, Oct. 1998.
[5] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1456–1467, Sept. 1999.
[6] G. Ganesan and P. Stoica, "Space-time block codes: A maximum SNR approach," *IEEE Trans. Inform. Theory*, vol. 47, pp. 1650–1656, May 2001.
[7] O. Tirkkonen and A. Hottinen, "Square-matrix embeddable space-time block codes for complex signal constellations," *IEEE Trans. Inform. Theory*, vol. 48, pp. 384–395, Feb. 2002.
[8] W. Su and X.-G Xu, "On space-time block codes from complex orthogonal designs," *Wireless Personal Commun.*, vol. 25, no. 1, pp. 1–26, Apr. 2003.
[9] W. Su and X.-G. Xia, "Quasiorthogonal space-time block codes with full diversity," in *Proc. IEEE GLOBECOM'02*, vol. 2, 2002, pp. 1098–1102.
[10] B. M. Hochwald and W. Sweldens, "Differential unitary space-time modulation," *IEEE Trans. Commun.*, vol. 48, pp. 2041–2052, Dec. 2000.
[11] A. Shokrollahi, B. Hassibi, B. M. Hochwald, and W. Sweldens, "Representation theory for high-rate multiple-antenna code design," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2335–2367, Sept. 2001.
[12] B. Hassibi and B. M. Hochwald, "Cayley differential unitary space-time codes," *IEEE Trans. Inform. Theory*, vol. 48, pp. 1485–1503, June 2002.
[13] X.-B. Liang and X.-G. Xia, "Unitary signal constellations for differential space-time modulation with two transmit antennas: Parametric codes, optimal designs and bounds," *IEEE Trans. Inform. Theory*, vol. 48, pp. 2291–2322, Aug. 2002.
[14] Q. Yan and R. Blum, "Robust space-time block coding for rapid fading channels," in *Proc. IEEE GLOBECOM*, vol. 1, 2001, pp. 460–464.
[15] S. Zummo and S. Al-Semari, "Space-time coded QPSK for rapid fading channels," *Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Communications (PIMRC)*, vol. 1, pp. 504–508, 2000.
[16] W. Firmanto, B. Vucetic, and J. Yuan, "Space-time TCM with improved performance on fast fading channels," *IEEE Commun. Letters*, vol. 5, pp. 154–156, Apr. 2001.
[17] H. Bölcskei and A. Paulraj, "Performance of space-time codes in the presence of spatial fading correlation," in *Proc. Asilomar Conf. Signals, Systems and Computers*, vol. 1, 2000, pp. 687–693.
[18] M. P. Fitz, J. Grimm, and S. Siwamogsatham, "A new view of performance analysis techniques in correlated Rayleigh fading," in *Proc. IEEE Wireless Communications and Networking Conf. (WCNC)*, Sept. 1999, pp. 139–144.
[19] S. Siwamogsatham, M. P. Fitz, and J. Grimm, "A new view of performance analysis of transmit diversity schemes in correlated Rayleigh fading," *IEEE Trans. Inform. Theory*, vol. 48, pp. 950–956, Apr. 2002.
[20] S. Siwamogsatham and M. P. Fitz, "Robust space-time codes for correlated Rayleigh fading channels," *IEEE Trans. Signal Processing*, vol. 50, pp. 2408–2416, Oct. 2002.
[21] Z. Safar and K. J. R. Liu, "Performance analysis of space-time codes over correlated Rayleigh fading channels," in *Proc. IEEE Int. Conf. Communications*, vol. 5, Anchorage, AK, May 2003, pp. 3185–3189.
[22] H. El Gamal, "On the robustness of space-time coding," *IEEE Trans. Signal Processing*, vol. 50, pp. 2417–2428, Oct. 2002.
[23] K. Leeuwin-Boulle and J. C. Belfiore, "The cutoff rate of time correlated fading channels," *IEEE Trans. Inform. Theory*, vol. 39, pp. 612–617, Mar. 1993.
[24] E. Baccarelli, "Performance bounds and cutoff rates for data channels affected by correlated randomly time-variant multipath fading," *IEEE Trans. Commun.*, vol. 46, pp. 1258–1261, Oct. 1998.
[25] O. Y. Takeshita and D. J. Constello Jr, "New classes of algebraic interleavers for turbo-codes," in *Proc. IEEE Int. Symp. Information Theory*, MIT, Cambridge, MA, 1998, p. 419.
[26] W. C. Jakes, *Microwave Mobile Communications*. New York: Wiley, 1974.
[27] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1991.

New Family of p-ary Sequences With Optimal Correlation Property and Large Linear Span

Ji-Woong Jang, Young-Sik Kim, Jong-Seon No, *Member, IEEE*, and Tor Helleseth, *Fellow, IEEE*

***Abstract*—For an odd prime p and integers n, m, and k such that $n = (2m+1)k$, a new family of p-ary sequences of period $p^n - 1$ with optimal correlation property is constructed using the p-ary Helleseth–Gong sequences with ideal autocorrelation, where the size of the sequence family is p^n. That is, the maximum nontrivial correlation value $R_{\max}$ of all pairs of distinct sequences in the family does not exceed $p^{\frac{n}{2}} + 1$, which means the family has optimal correlation in terms of Welch's lower bound. The symbol distribution of the sequences in the family is enumerated. It is also shown that the linear span of the sequences in the family is $(m+2)n$ except for the m-sequence in the family.**

***Index Terms*—Family of sequences, optimal correlation, p-ary sequences.**

I. Introduction

In the wireless communication systems employing code-division multiple-access (CDMA) scheme, a signature sequence is assigned to each user, which makes it possible to distinguish his signal from those of the other users. In design of sequences for CDMA system, the most important properties of the sequences are low periodic correlation between all pairs of distinct sequences and large family size. For an odd prime p, families of p-ary sequences of period $p^n - 1$ with optimal correlation property have been found, where the optimality of correlation values means that maximum magnitude of out-of-phase autocorrelation and cross-correlation values of any pairs of sequences of period $p^n - 1$ in the family is upper-bounded by $R_{\max} = p^{\frac{n}{2}} + 1$. Sidelnikov constructed a family of p-ary sequences with optimal correlation property and a family of prime-phase sequences with optimal correlation property was introduced by Kumar and Moreno [3]. By extending the alphabet size, Liu and Komo [7] constructed p-ary Kasami sequences. The family of p-ary bent sequences also has the optimal correlation property. Using the p-ary bent functions given by Kumar and Moreno, a family of balanced p-ary sequences with optimal correlation property was constructed by Moriuchi and Imamura [9]. The known families of p-ary sequences of period $p^n - 1$ with optimal correlation property are listed in Table I. The family size of the sequences due to Sidelnikov and to Kumar and Moreno are larger than that of the others in Table I. But the linear span of the sequences due to Sidelnikov and to Kumar and Moreno are much smaller than those of the others.

In this correspondence, for an odd prime p and integers n, m, and k such that $n = (2m+1)k$, a new family of p-ary sequences of period $p^n - 1$ with optimal correlation property is constructed using the p-ary Helleseth–Gong sequences with ideal autocorrelation, where the size of the sequence family is p^n. That is, the maximum nontrivial correlation value $R_{\max}$ of all pairs of distinct sequences in the family does not exceed $p^{\frac{n}{2}} + 1$, which means the family has optimal correlation with respect to Welch's lower bound. The symbol distribution of the

Manuscript received January 9, 2003; revised February 18, 2004. This work was supported in part by the Korean Ministry of Information and Communications and the Norwegian Research Council.

J.-W. Jang, Y.-S. Kim, and J.-S. No are with the School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-742, Korea (e-mail: jsno@snu.ac.kr).

T. Helleseth is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (e-mail: Tor.Helleseth@ii.uib.no).

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

Digital Object Identifier 10.1109/TIT.2004.831837

TABLE I
FAMILIES OF p-ARY SEQUENCES OF PERIOD $p^n - 1$ WITH OPTIMAL CORRELATION PROPERTY $R_{\max} = p^{\frac{n}{2}} + 1$

Family	n	Family size	Linear span	Balance
New sequences	$(2m+1)k$	p^n	$n, (m+2)n$	no
Sidelnikov	even or odd	p^n	$n, 2n$	no
Kumar and Moreno	$(2m+1)k$	p^n	$n, 2n$	no
Kasami	even, $2m$	p^m	$\frac{3}{2}n$	no
Bent sequences	even, $2m$	p^m	*	yes
Moriuchi *et al.*	even, $2m$	p^m	*	yes

* The linear span of the bent sequences and the sequences by Moriuchi et al. is much larger than that of the others.

sequences in the family is enumerated. It is also shown that the linear span of the sequences in the family is $(m+2)n$ except for the m-sequence in the family.

II. PRELIMINARIES

Let $\boldsymbol{S}$ be the family of M p-ary sequences of period $N = p^n - 1$ for an odd prime p given by

$$\boldsymbol{S} = \{s_i(t) \mid 0 \le i \le M-1, 0 \le t \le N-1\}.$$

The correlation function of the sequences $s_i(t)$ and $s_j(t)$ in $\boldsymbol{S}$ is written as

$$R_{i,j}(\tau) = \sum_{t=0}^{N-1} \omega^{s_i(t+\tau) - s_j(t)}$$

where ω is a complex pth root of unity, $0 \le i,j \le M-1$, and $0 \le \tau \le N-1$. The maximum magnitude $R_{\max}$ of the correlation values is defined as

$$R_{\max} = \max_{0 \le i,j \le M-1, 0 \le \tau \le N-1} |R_{i,j}(\tau)|$$

where the maximization excludes the case of in-phase ($i=j$ and $\tau = 0$) autocorrelation. A family of p-ary sequences of period $p^n - 1$ is said to have optimal correlation property if $R_{\max}$ does not exceed $p^{\frac{n}{2}} + 1$.

Let z be an integer and V_z^n the n-dimensional vector space over the set of integers modulo z, J_z. Let $\omega_z = e^{j\frac{2\pi}{z}}$, $j = \sqrt{-1}$. Let $f(\underline{x})$ be a function from V_z^n to J_z. The Fourier transform of the function $f(\underline{x})$ is defined as

$$F(\underline{\lambda}) = \frac{1}{\sqrt{z^n}} \sum_{\underline{x} \in V_z^n} \omega_z^{f(\underline{x}) - \underline{\lambda} \cdot \underline{x}^T}, \qquad \underline{\lambda} \in V_z^n$$

where $\underline{x}^T$ denotes the transpose of $\underline{x}$.

Definition 1 (Kumar, Scholtz, and Welch [4]): A function $f(\underline{x})$ from V_z^n to J_z is said to be a generalized bent function if the Fourier coefficients $F(\underline{\lambda})$ of $f(\underline{x})$ all have unit magnitude for any $\underline{\lambda} \in V_z^n$. □

In this correspondence, we assume that the integer z is an odd prime p. Thus, V_p^n is the n-dimensional vector space over the finite field F_p with p elements and $f(\underline{x})$ is a function from V_p^n to F_p.

Olsen, Scholtz, and Welch introduced the *trace transform* for a function from F_{2^n} to F_2. Their definition can be generalized as follows.

Definition 2 (Olsen, Scholtz, and Welch [10]): Let $f(x)$ be a function from F_{p^n} to F_p. Then the *trace transform* of $f(x)$ and its inverse transform are defined by

$$F(\lambda) = \frac{1}{\sqrt{p^n}} \sum_{x \in F_{p^n}} \omega^{f(x) - \mathrm{tr}_1^n(\lambda x)}, \qquad \lambda \in F_{p^n}$$

$$\omega^{f(x)} = \frac{1}{\sqrt{p^n}} \sum_{\lambda \in F_{p^n}} F(\lambda) \omega^{\mathrm{tr}_1^n(\lambda x)}, \qquad x \in F_{p^n}. \qquad \square$$

The elements x and λ in F_{p^n} can be related to the elements $\underline{x}$ and $\underline{\lambda}$ in V_p^n as follows:

$$x = \sum_{i=1}^{n} x_i \alpha_i \Rightarrow \underline{x} = (x_1, x_2, x_3, \ldots, x_n)$$

$$\lambda = \sum_{i=1}^{n} \lambda_i \alpha_i \Rightarrow \underline{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n)$$

where x_i and λ_i are in F_p and $\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n\}$ is a basis of F_{p^n} over F_p. By replacing x in F_{p^n} by $\underline{x}$ in V_p^n, the function $f(x)$ from F_{p^n} to F_p makes the corresponding function $f(\underline{x})$ from V_p^n to F_p. It is known that the set of the trace transform values of the function $f(x)$ is the same as that of the Fourier coefficients of the corresponding function $f(\underline{x})$. Therefore, the function $f(x)$ is a generalized bent function from F_{p^n} to F_p if and only if the corresponding function $f(\underline{x})$ is a generalized bent function from V_p^n to F_p.

Let $n = ek$, where e and k are integers. A basis $\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_e\}$ of F_{p^n} over F_{p^k} is said to be *trace-orthogonal* if

$$\mathrm{tr}_k^n(\alpha_i \alpha_j) = \begin{cases} a_i, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases}$$

where $a_i \in F_{p^k}^*$. It is known that for any positive integer e and odd prime p, there exists a trace-orthogonal basis of F_{p^n} over F_{p^k} [12]. Suppose elements x and λ in F_{p^n} can be related to the elements $\underline{x}$ and $\underline{\lambda}$ in the e-dimensional vector space $V_{p^k}^e$ over F_{p^k} as follows:

$$x = \sum_{i=1}^{e} x_i \alpha_i \Rightarrow \underline{x} = (x_1, x_2, x_3, \ldots, x_e) \tag{1}$$

$$\lambda = \sum_{i=1}^{e} \lambda_i \alpha_i \Rightarrow \underline{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_e) \tag{2}$$

where x_i and λ_i are in F_{p^k}. Then, if we choose the basis to be trace-orthogonal, we have the relation

$$\mathrm{tr}_k^n(\lambda x) = \sum_{i=1}^{e} a_i \lambda_i x_i. \tag{3}$$

Let $\lambda_i' = a_i \lambda_i$ for $1 \le i \le e$ and $\underline{\lambda}' = (\lambda_1', \lambda_2', \lambda_3', \ldots, \lambda_e')$. Then the relation in (3) can be rewritten as

$$\mathrm{tr}_k^n(\lambda x) = \sum_{i=1}^{e} \lambda_i' x_i = \underline{\lambda}' \cdot \underline{x}^T.$$

Suppose that using (1) and (2), a function $f(x)$ from F_{p^n} to F_{p^k} is related to the corresponding function $f(\underline{x})$ from $V_{p^k}^e$ to F_{p^k}. Then the trace transform in Definition 2 can be modified into the trace transform defined in the intermediate field as follows.

Definition 3: Let $n = ek$. Let $f(\underline{x})$ be a function from $V_{p^k}^e$ to F_{p^k}. Then the trace transform of $\mathrm{tr}_1^k(f(\underline{x}))$ and its inverse transform are defined as

$$F_M(\underline{\lambda}) = \frac{1}{\sqrt{p^n}} \sum_{\underline{x} \in V_{p^k}^e} \omega^{\mathrm{tr}_1^k(f(\underline{x})) - \mathrm{tr}_1^k(\underline{\lambda} \cdot \underline{x}^T)}, \qquad \underline{\lambda} \in V_{p^k}^e$$

$$\omega^{\mathrm{tr}_1^k(f(\underline{x}))} = \frac{1}{\sqrt{p^n}} \sum_{\underline{\lambda} \in V_{p^k}^e} F_M(\underline{\lambda}) \omega^{\mathrm{tr}_1^k(\underline{\lambda} \cdot \underline{x}^T)}, \qquad \underline{x} \in V_{p^k}^e. \quad \square$$

It is clear that the trace transform of a function $\mathrm{tr}_1^k(f(\underline{x}))$ from $V_{p^k}^e$ to F_p is related to the trace transform $F(\lambda)$ of the corresponding function $\mathrm{tr}_1^k(f(x))$ from F_{p^n} to F_p as follows:

$$F(\lambda) = F_M(\underline{\lambda}').$$

That is, the set of the trace transform values of the function $\mathrm{tr}_1^k(f(\underline{x}))$ is the same as that of the corresponding function $\mathrm{tr}_1^k(f(x))$. Therefore, if the trace transform of the function $\mathrm{tr}_1^k(f(x))$ or $\mathrm{tr}_1^k(f(\underline{x}))$ only takes values of unit magnitude, the functions $\mathrm{tr}_1^k(f(x))$ and $\mathrm{tr}_1^k(f(\underline{x}))$ become generalized bent functions.

Let $Q(x)$ be a quadratic form from F_{p^n} to F_{p^k}. Using (1), the quadratic form $Q(x)$ can be expressed as

$$Q(\underline{x}) = \sum_{i=1}^{e} \sum_{j=1}^{e} b_{ij} x_i x_j \tag{4}$$

where $b_{ij} \in F_{p^k}$. It is known from Dickson [1] that for an odd integer ρ, any quadratic form with rank ρ can be transformed by linear transformations into a canonical form

$$Q(\underline{x}) = \sum_{i=1}^{\rho} r x_i^2 \tag{5}$$

where $\rho \leq e$ and $r = 1$ or a quadratic nonresidue in F_{p^k}. It is clear that $Q(x)$ and the corresponding function $Q(\underline{x})$ in (4) and (5) have the same rank. From Definition 3, we easily derive the following lemma.

Lemma 4: $\mathrm{tr}_1^k(Q(\underline{x}))$ is a quadratic p-ary bent function from $V_{p^k}^e$ to F_p if and only if the quadratic function $Q(\underline{x})$ from $V_{p^k}^e$ to F_{p^k} has full rank e.

Proof: It is straightforward from Deligne's theorem [3] that a p-ary quadratic function with full rank is a bent function.

To prove the converse, let $\mathrm{tr}_1^k(Q(\underline{x}))$ be a p-ary quadratic bent function, where $Q(\underline{x})$ has rank ρ, $\rho < e$. From Dickson [1, p. 157], $\mathrm{tr}_1^k(Q(\underline{x}))$ can be rewritten as

$$\mathrm{tr}_1^k(Q(\underline{x})) = \mathrm{tr}_1^k(Q(\underline{x}_1, \underline{x}_2)) = \mathrm{tr}_1^k\left(\sum_{i=1}^{\rho} a_i x_i^2\right) \tag{6}$$

where $a_i \in F_{p^k}^*$, $\underline{x}_1$ is a ρ-tuple vector on $V_{p^k}^{\rho}$, and $\underline{x}_2$ is an $(e-\rho)$-tuple vector on $V_{p^k}^{e-\rho}$. Then the trace transform of (6) is given as

$$\begin{aligned}
&Q_M(\underline{\lambda}) \\
&= \frac{1}{\sqrt{p^n}} \sum_{\underline{x} \in V_{p^k}^e} w^{\mathrm{tr}_1^k(Q(\underline{x})) - \mathrm{tr}_1^k(\underline{\lambda} \cdot \underline{x}^T)} \\
&= \frac{1}{\sqrt{p^n}} \sum_{\underline{x} \in V_{p^k}^e} w^{\mathrm{tr}_1^k(\sum_{i=1}^{\rho} a_i x_i^2) - \mathrm{tr}_1^k(\sum_{i=1}^{e} \lambda_i x_i)} \\
&= \frac{1}{\sqrt{p^n}} \sum_{\underline{x}_1 \in V_{p^k}^{\rho}} w^{\mathrm{tr}_1^k(\sum_{i=1}^{\rho} a_i x_i^2) - \mathrm{tr}_1^k(\underline{\lambda}_1 \cdot \underline{x}_1^T)} \sum_{\underline{x}_2 \in V_{p^k}^{e-\rho}} w^{-\mathrm{tr}_1^k(\underline{\lambda}_2 \cdot \underline{x}_2^T)} \\
&= \frac{1}{\sqrt{p^n}} \sum_{\underline{x}_2 \in V_{p^k}^{e-\rho}} w^{-\mathrm{tr}_1^k(\underline{\lambda}_2 \cdot \underline{x}_2^T)} \sum_{\underline{x}_1 \in V_{p^k}^{\rho}} w^{\mathrm{tr}_1^k(\sum_{i=1}^{\rho} a_i x_i^2) - \mathrm{tr}_1^k(\underline{\lambda}_1 \cdot \underline{x}_1^T)}.
\end{aligned} \tag{7}$$

Let

$$\mathrm{tr}_1^k(Q'(\underline{x}_1)) = \mathrm{tr}_1^k\left(\sum_{i=1}^{\rho} a_i x_i^2\right).$$

Then the inner summation in (7) is the trace transform of $\mathrm{tr}_1^k(Q'(\underline{x}_1))$. Clearly, $Q'(\underline{x}_1)$ has full rank on $V_{p^k}^{\rho}$ and thus $\mathrm{tr}_1^k(Q'(\underline{x}_1))$ is a bent function on $V_{p^k}^{\rho}$. Therefore, the inner summation of (7) is equal to $\pm\sqrt{p^{k\rho}}$. Thus, we can rewrite (7) as follows:

$$\begin{aligned}
Q_M(\underline{\lambda}) &= \pm \frac{\sqrt{p^{k\rho}}}{\sqrt{p^n}} \sum_{\underline{x}_2 \in V_{p^k}^{e-\rho}} w^{-\mathrm{tr}_1^k(\underline{\lambda}_2 \cdot \underline{x}_2^T)} \\
&= \begin{cases} 0, & \text{if } \underline{\lambda}_2 \neq \underline{0} \\ \pm\sqrt{p^{k(e-\rho)}}, & \text{if } \underline{\lambda}_2 = \underline{0}, \end{cases}
\end{aligned} \tag{8}$$

which means that $\mathrm{tr}_1^k(Q(\underline{x}))$ is not a bent function on $V_{p^k}^e$. Thus. every quadratic bent function has full rank. $\square$

Helleseth and Gong introduced new p-ary sequences with ideal autocorrelation, which are referred to as Helleseth–Gong (HG) sequences [2].

Theorem 5 (Helleseth and Gong [2]): Let α be a primitive element of F_{p^n}. Let $n = (2m+1)k$ and let s, $1 \leq s \leq 2m$ be an integer such that $\gcd(s, 2m+1) = 1$. Define $b_0 = 1$, $b_{is} = (-1)^i$, and $b_i = b_{2m+1-i}$ for $i = 1, 2, \ldots, m$. Let $u_0 = b_0/2 = (p+1)/2$ and $u_i = b_{2i}$ for $i = 1, 2, \ldots, m$ where all indexes of the b_i's are taken $\bmod 2m+1$ and $q = p^k$. Then the HG sequence of period $p^n - 1$ is given by

$$s(t) = \mathrm{tr}_1^n\left(\sum_{l=0}^{m} u_l \alpha^{\frac{q^{2l}+1}{2} t}\right). \tag{9}$$

The HG sequence has an ideal two-level autocorrelation. $\square$

We provide an example of HG sequence as follows.

Example 6: For $p = 3$, let $m = 2$, $k = 2$, and $n = (2m+1)k = 10$. Let $s = 2$ so $\gcd(s, 2m+1) = 1$. Then the parameters b_i and u_i are given as follows:

$$\begin{gathered}
b_0 = 1,\ b_1 = b_6 = (-1)^3 = -1,\ b_2 = (-1)^1 = -1 \\
b_3 = b_8 = (-1)^4 = 1,\ b_4 = (-1)^2 = 1 \\
u_0 = \frac{b_0}{2} = 2,\ u_1 = b_2 = 2,\ u_2 = b_4 = 1.
\end{gathered}$$

Thus, the HG sequence of period $3^{10} - 1$ is given as

$$s(t) = \mathrm{tr}_1^n(\alpha^t) + \mathrm{tr}_1^n(\alpha^{41t}) - \mathrm{tr}_1^n(\alpha^{3281t})$$

where α is a primitive element in $F_{3^{10}}$. $\square$

Let $h(x)$ be the HG polynomial defined by

$$h(x) = \sum_{l=0}^{m} u_l x^{\frac{q^{2l}+1}{2}}, \qquad x \in F_{p^n}.$$

Then the HG sequence in (9) can be rewritten as

$$s(t) = \mathrm{tr}_1^n(h(\alpha^t)), \quad 0 \leq t \leq p^n - 2.$$

We can construct a new p-ary sequence s_β for each $\beta \in F_{p^n}$ using the HG sequence as follows:

$$\begin{aligned}
s_\beta(t) &= \mathrm{tr}_1^n(\alpha^t) + \mathrm{tr}_1^n(h(\beta\alpha^{2t})) \\
&= \mathrm{tr}_1^n\left(\alpha^t + \sum_{l=0}^{m} u_l \beta^{\frac{q^{2l}+1}{2}} \alpha^{(q^{2l}+1)t}\right).
\end{aligned} \tag{10}$$

It is clear that the sequences in (10) have period $p^n - 1$.

III. New Construction of a Family of p-ary Sequences

Using the new p-ary sequence defined in (10), a family of p-ary sequences with family size p^n and optimal correlation property can be constructed as follows.

Theorem 7: Let $s_\beta(t)$ be the p-ary sequence defined in (10). Then the family of p-ary sequences given by

$$\boldsymbol{S} = \{s_\beta(t) \mid \beta \in F_{p^n},\ 0 \le t \le p^n - 2\}$$

has the optimal correlation property with $R_{\max} = p^{\frac{n}{2}} + 1$.

Proof: The cross-correlation function of two p-ary sequences $s_{\beta_i}(x)$ and $s_{\beta_j}(x)$ in $\boldsymbol{S}$ can be rewritten as

$$\begin{aligned} R_{ij}(\tau) + 1 &= \sum_{t=0}^{p^n-2} w^{s_{\beta_i}(t+\tau) - s_{\beta_j}(t)} + 1 \\ &= \sum_{x \in F_{p^n}} w^{\mathrm{tr}_1^n(cx + h(\beta_i c^2 x^2) - x - h(\beta_j x^2))} \end{aligned} \tag{11}$$

where $c = \alpha^\tau \in F_{p^n}^*$. Then the proof can be classified into the following three cases.

Case (i) $c = 1, \beta_i = \beta_j$:
It is clear that $R_{ij}(\tau) = p^n - 1$.

Case (ii) $c \neq 1, \beta_i c^2 = \beta_j$:
It is also clear that $R_{ij}(\tau) = -1$.

Case (iii) $\beta_i c^2 \neq \beta_j$:
The condition excludes the case of $\beta_i = \beta_j = 0$. We will prove it assuming $\beta_j \neq 0$; the proof in the case $\beta_i \neq 0$ is similar.

Since $\frac{n}{k}$ is an odd integer, it is clear that a quadratic nonresidue in F_{p^k} is also a quadratic nonresidue in F_{p^n}. Thus, β_i and β_j can be expressed as $\beta_i = r_i a_i^2$ and $\beta_j = r_j a_j^2$, where $a_i, a_j \in F_{p^n}$ and r_i and r_j are 1 or quadratic nonresidues in F_{p^k}. We assume that $\beta_j \neq 0$ and thus $a_j \neq 0$. Let $u = \frac{a_i}{a_j} c$ and $y = a_j x$. Then the cross-correlation function in (11) can be rewritten as

$$\begin{aligned} R_{ij}(\tau) + 1 &= \sum_{x \in F_{p^n}} w^{\mathrm{tr}_1^n(h(r_i a_i^2 c^2 x^2) - h(r_j a_j^2 x^2)) + \mathrm{tr}_1^n((c-1)x)} \\ &= \sum_{y \in F_{p^n}} w^{\mathrm{tr}_1^n(h(r_i u^2 y^2) - h(r_j y^2)) + \mathrm{tr}_1^n(\frac{c-1}{a_j} y)}. \end{aligned}$$

Using the property that for $r \in F_{p^k}$, $h(rx) = rh(x)$, we have

$$\begin{aligned} R_{ij}(\tau) + 1 &= \sum_{y \in F_{p^n}} w^{\mathrm{tr}_1^n(r_i h(u^2 y^2) - r_j h(y^2)) + \mathrm{tr}_1^n(\frac{c-1}{a_j} y)} \\ &= \sum_{y \in F_{p^n}} w^{\mathrm{tr}_1^k(\mathrm{tr}_k^n(r_i h(u^2 y^2) - r_j h(y^2))) + \mathrm{tr}_1^n(\frac{c-1}{a_j} y)}. \end{aligned} \tag{12}$$

Let $Q(y)$ be the quadratic function defined by

$$\begin{aligned} Q(y) &= \mathrm{tr}_k^n(r_i h(u^2 y^2) - r_j h(y^2)) \\ &= \mathrm{tr}_k^n\left(\sum_{l=0}^{m} u_l [r_i u^{q^{2l}+1} - r_j] y^{q^{2l}+1}\right) \\ &= r_j \mathrm{tr}_k^n\left(\sum_{l=0}^{m} u_l [\frac{r_i}{r_j} u^{q^{2l}+1} - 1] y^{q^{2l}+1}\right). \end{aligned}$$

Then (12) corresponds to the trace transform of the quadratic function $\mathrm{tr}_1^k(Q(y))$ from F_{p^n} to F_p as in Definition 2. If the quadratic function $\mathrm{tr}_1^k(Q(y))$ is a p-ary bent function, then we have $|R_{ij}(\tau) + 1| = p^{\frac{n}{2}}$. From Definition 3 and Lemma 4, if $Q(y)$ has full rank, then $\mathrm{tr}_1^k(Q(y))$ is bent. Thus, it is sufficient to show that $Q(y)$ has full rank $2m + 1$.

It is already known that the rank of the quadratic function $Q(y)$ is equal to ρ if $q^{2m+1-\rho}$ is the number of elements $z \in F_{p^n}$ satisfying $Q(y + z) = Q(y)$ for all $y \in F_{p^n}$. Let $a_l = u_l[\frac{r_i}{r_j} u^{q^{2l}+1} - 1]$. Then the condition

$$\mathrm{tr}_k^n\left(\sum_{l=0}^{m} a_l (y + z)^{q^{2l}+1}\right) = \mathrm{tr}_k^n\left(\sum_{l=0}^{m} a_l y^{q^{2l}+1}\right)$$

can be modified into

$$\mathrm{tr}_k^n\left(\sum_{l=0}^{m} a_l (y^{q^{2l}} z + y z^{q^{2l}}) + \sum_{l=0}^{m} a_l z^{q^{2l}+1}\right) = 0.$$

Raising the first term to the $q^{2m+1-2l}$ power, we have

$$\mathrm{tr}_k^n\left(y\left[\sum_{l=0}^{m} a_l^{q^{2m+1-2l}} z^{q^{2m+1-2l}} + \sum_{l=0}^{m} a_l z^{q^{2l}}\right] + \sum_{l=0}^{m} a_l z^{q^{2l}+1}\right) = 0$$

which is equivalent to

$$\sum_{l=0}^{m} a_l^{q^{2m+1-2l}} z^{q^{2m+1-2l}} + \sum_{l=0}^{m} a_l z^{q^{2l}} = 0 \tag{13}$$

and

$$\mathrm{tr}_k^n\left(\sum_{l=0}^{m} a_l z^{q^{2l}+1}\right) = 0.$$

Equations (13) can be rewritten as

$$\sum_{l=0}^{m} u_l \left\{ \left(\frac{r_i}{r_j} u^{(q^{2l}+1) q^{2m+1-2l}} - 1\right) z^{q^{2m+1-2l}} + \left(\frac{r_i}{r_j} u^{(q^{2l}+1)} - 1\right) z^{q^{2l}} \right\} = 0$$

and thus we have

$$\sum_{l=0}^{2m} b_l \left(\frac{r_i}{r_j} u^{(q^{2l}+1)} - 1\right) z^{q^{2l}} = 0$$

where $u_0 = \frac{b_0}{2}$ and $u_l = b_{2l} = b_{2m+1-2l}$. To prove that the rank of $Q(y)$ is $\rho = 2m + 1$, we have to show that the equation

$$\sum_{l=0}^{2m} b_l \left(\frac{r_i}{r_j} \left(\frac{a_i}{a_j} c\right)^{q^{2l}+1} - 1\right) z^{q^{2l}} = 0$$

has $z = 0$ as its only solution for any $\frac{r_i}{r_j}(\frac{a_i}{a_j} c)^2 \neq 1$. This is already proved in [2]. From the condition, it is clear that

$$\frac{r_i}{r_j}\left(\frac{a_i}{a_j} c\right)^2 = \frac{b_i c^2}{b_j} \neq 1$$

and thus we have proved the theorem. □

Clearly, the sequence in (10) becomes a p-ary m-sequence when $\beta = 0$. For $\beta \neq 0$, (10) can be transformed into the form

$$s_i^\gamma(t) = \mathrm{tr}_1^n\left(\alpha^{t+i} + \gamma \sum_{l=0}^{m} u_l \alpha^{(q^{2l}+1)t}\right) \tag{14}$$

where $0 \le i \le \frac{p^n-1}{2} - 1$ and γ is 1 or a quadratic nonresidue in F_{p^k}. Then the family of p-ary sequences defined in Theorem 7 can be rewritten as

$$\boldsymbol{S} = \left\{ s_i^\gamma(t) \mid 0 \le i \le \frac{p^n - 1}{2} - 1,\ 0 \le t \le p^n - 2 \right\} \bigcup \left\{ \mathrm{tr}_1^n(\alpha^t) \right\}. \tag{15}$$

Let W be a subset of V_p^n and $g(\underline{x})$ a function from W to F_p. Then we define the notation

$$w_c = |\{\underline{x} \mid g(\underline{x}) = c,\ \underline{x} \in W\}|, \qquad c \in F_p.$$

Then the symbol distribution of $g(\underline{x})$ is defined as the ordered p-tuple $(w_0, w_1, w_2, \ldots, w_{p-1})$. It is interesting to find the symbol distribution of the sequences in the family given in (15). Using the result in Section II, it is easy to derive that the quadratic part of the sequence in (14) can be transformed into the quadratic form

$$f(\underline{x}) = a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2 \tag{16}$$

mapping from $V_p^n \backslash \{\underline{0}\}$ to F_p. It is clear that the quadratic form in (14) is bent and thus $f(\underline{x})$ has full rank, that is, $a_i \in F_p^*$.

Let $\chi(x)$ denote the quadratic character of x defined by

$$\chi(x) = \begin{cases} +1, & \text{if } x \text{ is a quadratic residue} \\ 0, & \text{if } x = 0 \\ -1, & \text{if } x \text{ is a quadratic nonresidue.} \end{cases}$$

Dickson [1] derived the number of solutions in V_p^n to quadratic equations over F_p.

Theorem 8 (Dickson [1, pp. 47–48]): Let p be an odd prime and $n = (2m+1)k = 2h$ be an even integer. Then the number of solutions $(x_1, x_2, \ldots, x_n)$ in V_p^n of the quadratic equation

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2 = c$$

where $a_j \in F_p^*$ and $c \in F_p$, is given by

$$v_c = \begin{cases} p^{2h-1} + \nu(p^h - p^{h-1}), & \text{if } c = 0 \\ p^{2h-1} - \nu p^{h-1}, & \text{if } c \neq 0 \end{cases} \tag{17}$$

where $\nu = \chi((-1)^h a_1 a_2 \cdots a_n)$. □

Theorem 9 (Dickson [1, pp. 47–48]): Let p be an odd prime and $n = (2m+1)k = 2h+1$ be an odd integer. Then the number of solutions $(x_1, x_2, \ldots, x_n)$ in V_p^n to the quadratic equation

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2 = c$$

where $a_j \in F_p^*$ and $c \in F_p$, is given as

$$v_c = p^{2h} + \eta p^h \tag{18}$$

where $\eta = \chi((-1)^h a_1 a_2 \cdots a_n c)$. □

It is clear that the new sequence family includes one p-ary m-sequence, which has the symbol distribution

$$(p^{n-1} - 1, p^{n-1}, p^{n-1}, \ldots, p^{n-1}).$$

We denote this distribution by $D_\infty = 1$. The distribution of D_c for the new sequence family defined in (15) is given in the following theorem.

Theorem 10: Let D_c be the number of sequences with symbol distribution $(v_c - 1, v_{c+1}, \ldots, v_{p-1}, v_0, v_1, \ldots, v_{c-1})$ in the sequence family in (15). Then

$$D_c = \begin{cases} 1, & \text{if } c = \infty \\ \frac{v_c - 1}{2}, & \text{if } c = 0 \\ \frac{v_c}{2}, & \text{if } c \in F_p^* \end{cases}$$

where v_c is defined in (17) and (18).

Proof: From the balance property of a p-ary m-sequence, it is clear that $D_\infty = 1$. Since $\gcd(q^{2l} + 1, p^n - 1) = 2$ for all l, the period of the quadratic part in (14) is $\frac{p^n - 1}{2}$. As i varies over $0 \leq i \leq p^n - 2$ in (14), the $\frac{p^n - 1}{2}$ different sequences of period $p^n - 1$ can be generated, where each sequence occurs exactly twice. Using (16) and the transformation of the linear part $\mathrm{tr}_1^n(\alpha^{t+i})$, $s_i^\gamma(t)$ in (14) can be transformed into the function from $V_p^n \backslash \{\underline{0}\}$ to F_p given by

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2 + d_1 x_1 + d_2 x_2 + \cdots + d_n x_n \tag{19}$$

where $a_i \in F_p^*$ and $d_i \in F_p$. As i varies over $0 \leq i \leq p^n - 2$, every $(d_1, d_2, d_3, \ldots, d_n)$ in V_p^n occurs exactly once except for $\underline{0}$. We can modify (19) into

$$a_1 \left(x_1 + \frac{d_1}{2a_1}\right)^2 + a_2 \left(x_2 + \frac{d_2}{2a_2}\right)^2 + \cdots + a_n \left(x_n + \frac{d_n}{2a_n}\right)^2 - c$$

and putting $x_i' = x_i + \frac{d_i}{2a_i}$, we have

$$a_1 {x_1'}^2 + a_2 {x_2'}^2 + \cdots + a_n {x_n'}^2 - c \tag{20}$$

where

$$c = \frac{d_1^2}{4a_1} + \frac{d_2^2}{4a_2} + \cdots + \frac{d_n^2}{4a_n}$$

is in F_p. From (17) and (18), the symbol distribution of $f(\underline{x})$ in (16) is given as $(v_0 - 1, v_1, v_2, \ldots, v_{p-1})$, where excluding $\underline{x} = \underline{0}$ makes $v_0 - 1$ instead of v_0. Then for a fixed c in F_p, the symbol distribution of (20) is given as

$$(v_c - 1, v_{c+1}, \ldots, v_{p-1}, v_0, v_1, \ldots, v_{c-1}) \tag{21}$$

where for $\underline{x} = \underline{0}$, (19) takes the value 0 and thus excluding $\underline{x} = \underline{0}$ in (19) makes $v_c - 1$ instead of v_c.

In order to find the number of sequences with the symbol distribution in (21) in the sequence family defined in (15), we have to find the number of solutions $(d_1, d_2, d_3, \ldots, d_n)$ in $V_p^n \backslash \{\underline{0}\}$ satisfying the quadratic equation

$$\frac{d_1^2}{4a_1} + \frac{d_2^2}{4a_2} + \cdots + \frac{d_n^2}{4a_n} = c$$

as i varies over $0 \leq i \leq p^n - 2$. In fact, this corresponds to $2D_c$ because each sequence occurs exactly twice as i varies over $0 \leq i \leq p^n - 2$, which is already calculated in (17) and (18). We have to exclude the solution $\underline{0}$ for $c = 0$ because $(d_1, d_2, d_3, \ldots, d_n)$ is in $V_p^n \backslash \{\underline{0}\}$. Thus, we have $D_0 = \frac{v_0 - 1}{2}$ and $D_c = \frac{v_c}{2}$ for $c \in F_p^*$. □

Kumar and Moreno [3] calculated the correlation distribution of the sequences in their sequence family by finding the correlation values of two sequences in the family, which corresponds to Fourier coefficients of the quadratic forms with full rank. In their paper, the correlation distribution was derived by using the full rank property of the quadratic function. Therefore, the correlation distribution of the sequences in the new family defined in Theorem 7 is the same as that of the sequence family by Kumar and Moreno.

The linear span of the new p-ary sequences $s_\beta(t)$ in Theorem 7 is derived as in the following theorem.

Theorem 11: The linear span of the sequence $s_\beta(t)$ defined in Theorem 7 is equal to $(m+2)n$.

Proof: For $d_i = q^{2i} + 1, 0 \leq i \leq m$ in (10), $\gcd(d_i, p^n - 1) = 2$. It is clear that α^{d_i} does not belong to any subfield of F_{p^n}. Thus, the coset of α^2 in F_{p^n} has size n and so does that of each element α^{d_i}. Therefore, the linear span of $s_\beta(x)$ is $(m+2)n$. □

REFERENCES

[1] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*. New York: Dover, 1958.

[2] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation function," *IEEE Trans. Inform. Theory*, vol. 48, pp. 2868–2872, Nov. 2002.

[3] P. V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inform. Theory*, vol. 37, pp. 603–616, May 1991.

[4] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *J. Combin. Theory*, ser. A, vol. 40, pp. 90–107, 1985.

[5] A. Lempel and M. Cohn, "Maximal families of bent sequences," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 865–868, Nov. 1982.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, ser. Encyclopedia of Mathematics and Its Applications. Reading, MA: Addison-Wesley, 1983, vol. 20.

[7] S.-C. Liu and J. F. Komo, "Nonbinary Kasami sequences over GF(p)," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1409–1412, July 1992.
[8] F. J. McWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
[9] T. Moriuchi and K. Imamura, "Balanced nonbinary sequences with good periodic correlation properties obtained from modified Kumar–Moreno sequences," *IEEE Trans. Inform. Theory*, vol. 41, pp. 572–576, Mar. 1995.
[10] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 858–864, Nov. 1982.
[11] O. S. Rothaus, "On bent functions," *J. Combin. Theory*, ser. A, vol. 20, pp. 300–305, 1976.
[12] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields," *SIAM J. Comput.*, vol. 9, no. 4, pp. 758–767, Nov. 1980.
[13] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*. Rockville, MD: Computer Sci., 1985, vol. 1.
[14] L. R. Welch, "Lower bounds on the maximal cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 396–399, May 1976.

The Most Significant Bit of Maximum-Length Sequences Over $\mathbb{Z}_{2^l}$: Autocorrelation and Imbalance

Patrick Solé, *Member, IEEE,* and Dmitrii Zinoviev

***Abstract*—The imbalance and the autocorrelation of the binary sequences in the title are explored by combining the local Weil bound with spectral analysis. Recent estimates on these quantities are improved by a factor of order $2^{l/2}$, for large l.**

***Index Terms*—Autocorrelation, Galois rings, maximum-length sequences over rings, most significant bit.**

I. Introduction

Maximum-length (ML) sequences over the rings $\mathbb{Z}_{2^l}$ were introduced by Dai [1], motivated by cryptographic applications. Using the 2-adic expansion in the local ring $\mathbb{Z}_{2^l}$, various binary sequences can be defined from a given ML sequence over $\mathbb{Z}_{2^l}$. Of particular interest, from the nonlinearity viewpoint, is the most significant bit [6]. In a cryptographic usage such as, for instance, a key in a one-time-pad system, such a deterministic sequence should look as random as possible. It should be as *balanced* as possible the frequency of each of the two symbols 0, 1 should be close to $1/2$. It should be *uncorrelated* with itself: low inner products with its successive shifts.

Recently some estimates were given for the autocorrelation and the imbalance of the binary sequences in the title [4], using the Galois rings character sum estimates of [7]. The aim of this note is, still using [7], to sharpen the autocorrelation and imbalance estimate of [4] by a factor exponential in l. Our approach uses the Discrete Fourier Transform techniques of [8], [9].

Manuscript received July 30, 2003; revised February 11, 2004. The material in this correspondence was presented in part at the Kodierungtheorie, Oberwolfach, Germany, December 2003.

P. Solé is with the CNRS-I3S, ESSI, 06 903 Sophia Antipolis, France (e-mail: ps@essi.fr).

D. Zinoviev is with the CNRS-I3S, ESSI, 06 903 Sophia Antipolis, France, and with the Institute for Problems of Information Transmission, Russian Academy of Sciences, GSP-4, Moscow, 101447, Russia (e-mail: zinoviev@essi.fr, zinov@iitp.ru).

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

Digital Object Identifier 10.1109/TIT.2004.831858

II. Preliminaries

Let $R = \mathrm{GR}(2^l, m)$ denote the Galois ring of characteristic 2^l with 2^{lm} elements. Let ξ be an element in $\mathrm{GR}(2^l, m)$ that generates the Teichmüller set $\mathcal{T}$ of $\mathrm{GR}(2^l, m)$. Specifically, let $\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}$ and $\mathcal{T}^* = \{1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}$. The 2-adic expansion of $x \in \mathrm{GR}(2^l, m)$ is given by

$$x = x_0 + 2x_1 + \cdots + 2^{l-1}x_{l-1}$$

where $x_0, x_1, \ldots, x_{l-1} \in \mathcal{T}$. The Frobenius operator F is defined for such an x as

$$F(x_0 + 2x_1 + \cdots + 2^{l-1}x_{l-1}) = x_0^2 + 2x_1^2 + \cdots + 2^{l-1}x_{l-1}^2$$

and the trace Tr, from $\mathrm{GR}(2^l, m)$ down to $\mathbb{Z}_{2^l}$, as

$$\mathrm{Tr}(x) := \sum_{j=0}^{m-1} F^j(x).$$

We also define another trace tr from $\mathbb{F}_{2^m}$ down to $\mathbb{F}_2$ as

$$\mathrm{tr}(x) := \sum_{j=0}^{m-1} x^{2^j}.$$

Throughout this note, we let $n = 2^m$ and $R^* = R \setminus 2R$. Let $\gamma = \xi(1 + 2\lambda) \in R$, where $\xi \in \mathcal{T}$ and $\lambda \in R^*$. Assume $1 + 2\lambda$ is of order 2^{l-1}. Since ξ is of order $2^m - 1$ then γ is an element of order $N = 2^{l-1}(2^m - 1)$. Following [4, Lemma 2], we define the sequence

$$S_{l,m} := \left\{ (\mathrm{Tr}(\alpha\gamma^t))_{t=0}^{N-1} \mid \alpha \in R^* \right\}. \tag{1}$$

Let $\mathrm{MSB} : \mathbb{Z}_{2^l}^n \to \mathbb{Z}_2^n$ be the most significant bit (MSB) map, i.e.,

$$\mathrm{MSB}(x_0 + 2x_1 + \cdots + 2^{l-1}x_{l-1}) := x_{l-1}.$$

III. Imbalance and Autocorrelation Properties

Let l be a positive integer (without loss of generality we assume that $l \geq 4$) and $\omega = e^{2\pi i/2^l}$ be a primitive 2^lth root of 1 in $\mathbb{C}$. Let ψ_k be the additive character of $\mathbb{Z}_{2^l}$ such that

$$\psi_k(x) = \omega^{kx}.$$

Let $\mu : \mathbb{Z}_{2^l} \to \{\pm 1\}$ be the mapping $\mu(t) = (-1)^c$, where c is the most significant bit of $t \in \mathbb{Z}_{2^l}$, i.e., it maps $0, 1, \ldots, 2^{l-1} - 1$ to $+1$ and $2^{l-1}, 2^{l-1} + 1, \ldots, 2^l - 1$ to -1. Our goal is to express this map as a linear combination of characters. Recall the Fourier transformation formula on $\mathbb{Z}_{2^l}$

$$\mu = \sum_{j=0}^{2^l-1} \mu_j \psi_j, \qquad \text{where } \mu_j = \frac{1}{2^l} \sum_{x=0}^{2^l-1} \mu(x)\psi_j(-x). \tag{2}$$

For all $\beta \in R = \mathrm{GR}(2^l, m)$, we denote by Ψ_β the character

$$\Psi_\beta : R \to \mathbb{C}^*, \quad x \mapsto \omega^{\mathrm{Tr}(\beta x)}.$$

Note that for the previously defined ψ_k and Ψ_β we have

$$\psi_k(\mathrm{Tr}(\beta x)) = \Psi_{\beta k}(x). \tag{3}$$

The following lemma follows from [7].

Lemma 3.1: For all $\lambda \in R$, $\lambda \neq 0$, we have

$$\left| \sum_{x \in \mathcal{T}} \Psi_\lambda(x) \right| \leq (2^{l-1} - 1)\sqrt{2^m}.$$

Proof: We restate [7, Theorem 1] for the special Galois ring of concern here. Let $f(X)$ denote a polynomial in $R[X]$ and let

$$f(x) = F_0(x) + 2F_1(x) + \cdots + 2^{l-1}F_{l-1}(x)$$