Aperiodic and odd correlations of some p-ary sequences from Galois rings

Ling, San; Özbudak, Ferruh

2006

Ling, S., & Özbudak, F. (2006). Aperiodic and odd correlations of some p-ary sequences from Galois rings. IEICE transactions on fundamentals of electronics, communications and computer sciences, E89A(9), 2258–2263.

https://hdl.handle.net/10356/94339

https://doi.org/10.1093/ietfec/e89-a.9.2258

PAPER Special Section on Sequence Design and its Application in Communications

Aperiodic and Odd Correlations of Some p-Ary Sequences from Galois Rings

San LING[†*a)], *Nonmember and* Ferruh ÖZBUDAK[††**b)], *Member*

SUMMARY We obtain an upper bound for the maximum aperiodic and odd correlations of the recently derived p-ary sequences from Galois rings [1]. We use the upper bound on hybrid sums over Galois rings [5], the Vinogradov method [4] and the methods of [5] and [6].

key words: *CDMA sequences, aperiodic correlation, odd correlation, hybrid sums*

1. Introduction

Recently using trace codes over Galois rings of characteristic p^2 and the generalized Nechaev-Gray map, p-ary sequence families of length $p(p^m-1)$ are constructed ([1], see also [2]). They compare favorably with certain known p-ary sequences of length p^m-1. Even in the case $p=2$, one of the families is slightly larger than the family $Q(D)$ of [3, Sect. 8.8], while they share the same bound for the maximum non-trivial (periodic) correlation.

The aperiodic and odd correlations, like periodic correlations, are also relevant for code-division multiple access (CDMA) applications [3]. In this paper we obtain bounds for the aperiodic and (generalized) odd correlations of these sequence families. Using the Vinogradov method [4], hybrid exponential sums and the methods of [5] and [6] we obtain our bounds.

We fix some notation throughout the paper. We assume that m is an integer with $m \geq 2$ throughout the paper. Let $\mathrm{GR}(p^2,m)$ be a Galois ring of characteristic p^2 with cardinality p^{2m}, $n=p^m-1$, $L=np$, $q=p^m$, β a primitive $(q-1)$-th root of unity in $\mathrm{GR}(p^2,m)$, and $\Gamma=\{0\}\cup\{\beta^i : 0\leq i\leq n-1\}$ be the Teichmüller set in $\mathrm{GR}(p^2,m)$. Let $\rho:\mathrm{GR}(p^2,m)\to\mathbb{F}_{p^m}$ be the reduction modulo p map. We extend ρ to the polynomial map $\rho:\mathrm{GR}(p^2,m)[x]\to\mathbb{F}_{p^m}[x]$ by its action on the coefficients. Let Tr be the trace map from $\mathrm{GR}(p^2,m)$ onto $\mathbb{Z}_{p^2}$. We consider the family $\mathcal{F}_D$ of [1, Theorem 3.12] (or equivalently the family $\mathcal{F}_{m,D}$ of [2, Theorem 4]). Let $S(D)$ be the set consisting of the polynomials $f(x)=f_0x+f_1x+\cdots+f_lx^l\in\mathrm{GR}(p^2,m)[x]$ of weighted degree (cf. [7]) at most D such that for $0\leq i\leq l$ with $p\mid i$ we have $f_i=0$. Let $\epsilon\in\mathrm{GR}(p^2,m)$ such that $\mathrm{Tr}(\epsilon)=1$. Let $\overline{S(D)}$ be the set of polynomials $\{f(x)+u\epsilon : f(x)\in S(D),\ u\in\mathbb{Z}_{p^2}\}$.

Recall that $r_1:\mathbb{Z}_{p^2}\to\mathbb{F}_p$ is the map sending $\alpha_0+p\alpha_1$ with $0\leq\alpha_0,\alpha_1\leq p-1$ to α_1. For $f\in\overline{S(D)}$ and $t\geq 0$, the t-th term of the sequence $\{s_f(t)\}_{t=0}^{\infty}$ of complex numbers is (cf. [1])

$$s_f(t):=e^{\frac{2\pi i}{p}r_1((1-p)^t\mathrm{Tr}(f(\beta^t)))}.$$

Here we recall the family $\mathcal{F}_D$ as a family of sequences of complex numbers ([1, Theorem 3.12]). Let P_D^1 be the subset of $\overline{S(D)}$ consisting of $f(x)+u\epsilon$ such that $f(x)\in S(D)$, $\rho(f(x))\neq 0$ and the sequence $\{\mathrm{Tr}(f(\beta^i))\}_{i=0}^{\infty}$ in $\mathbb{Z}_{p^2}$ has period p^m-1. For $f(x)+u\epsilon$, $g(x)+v\epsilon\in P_D^1$, we say they are *related* if there exist $0\leq k\leq p-1$ and $0\leq t\leq L-1$ such that

$$g(x)+v\epsilon-kp=(1-p)^t\left(f(\beta^t x)+u\epsilon\right). \tag{1}$$

Equation (1) gives an equivalence relation on P_D^1 and let $\widetilde{P}_D^1$ be a full set of representatives of the equivalence classes in P_D^1. Let $S(D)_1=\{b(x)\in\Gamma[x] : pb(x)\in S(D)\}$. Let P_D^2 be the subset of $\overline{S(D)}$ consisting of $pf(x)+u\epsilon$ such that $f(x)\in S(D)_1$, the sequence $\{\mathrm{Tr}(pf(\beta^i))\}_{i=0}^{\infty}$ in $\mathbb{Z}_{p^2}$ has period p^m-1, and $u\in\mathbb{Z}_{p^2}\setminus p\mathbb{Z}_{p^2}$. For $pf(x)+u\epsilon$, $pg(x)+v\epsilon\in P_D^2$, we say they are *related* if there exists $0\leq t\leq L-1$ such that

$$pg(x)+v\epsilon=(1-p)^t\left(pf(\beta^t x)+u\epsilon\right). \tag{2}$$

Similarly Eq. (2) gives an equivalence relation on P_D^2 and let $\widetilde{P}_D^2$ be a full set of representatives of the equivalence classes in P_D^2. The family $\mathcal{F}_D$ of sequences of complex numbers is $\mathcal{F}_D=\left\{\{s_f(t)\}_{t=0}^{\infty} : f\in\widetilde{P}_D^1\cup\widetilde{P}_D^2\right\}$.

2. Aperiodic and Odd Correlations

In this section we give our bounds for the aperiodic and (generalized) odd correlations of the p-ary sequence families of [1].

We first define some constants.

Definition 2.1. For $w=e^{\frac{2\pi i}{p^2}}$, $\theta=1/w$ and $0\leq l\leq p-1$, let a_{1+lp} be the complex number given by

Manuscript received December 8, 2005.
Final manuscript received April 2, 2006.

[†]The author is with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Block 5 Level 3, 1 Nanyang Walk, Singapore 637616, Republic of Singapore.
[††]The author is with the Department of Mathematics, Middle East Technical University, İnönü Bulvarı, 06531, Ankara, Turkey.

[*]The research of this author is partially supported by NTU Research Grant No. M48110000.
[**]The research of this author is partially supported by the Turkish Academy of Sciences in the framework of Young Scientists Award Programme (F.Ö./TÜBA-GEBIP/2003-13).

a) E-mail: lingsan@ntu.edu.sg
b) E-mail: ozbudak@metu.edu.tr

DOI: 10.1093/ietfec/e89-a.9.2258

$$a_{1+lp} = \frac{1}{p}\left\{1 + \theta^{1+lp} + \theta^{2(1+lp)} + \cdots + \theta^{(p-1)(1+lp)}\right\}.$$

These constants are used in the following lemma.

Lemma 2.2. *For $x \in \mathbb{Z}_{p^2}$ we have*

$$e^{\frac{2\pi i}{p} r_1(x)} = \sum_{l=0}^{p-1} a_{1+lp}\, e^{\frac{2\pi i}{p^2}(1+lp)x}.$$

Proof. Assume that $c_u \in \mathbb{C}$ for $0 \le u \le p^2-1$ such that

$$e^{\frac{2\pi i}{p} r_1(x)} = \sum_{u=0}^{p^2-1} c_u e^{\frac{2\pi i}{p^2} ux} \text{ for each } x \in \mathbb{Z}_{p^2}.$$

This is equivalent to the system

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{p^2-1} \\ 1 & w^2 & w^4 & \cdots & w^{2(p^2-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{p^2-1} & w^{2(p^2-1)} & \cdots & w^{(p^2-1)(p^2-1)} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{p^2-1} \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \\ w^p \\ \vdots \\ w^p \\ \vdots \\ \vdots \\ w^{p(p-1)} \\ \vdots \\ w^{p(p-1)} \end{bmatrix}.$$

Since the square matrix above is a Vandermonde matrix, taking its inverse we obtain

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{p^2-1} \end{bmatrix} = \frac{1}{p^2} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \theta & \theta^2 & \cdots & \theta^{p^2-1} \\ 1 & \theta^2 & \theta^4 & \cdots & \theta^{2(p^2-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \theta^{p^2-1} & \theta^{2(p^2-1)} & \cdots & \theta^{(p^2-1)(p^2-1)} \end{bmatrix} \begin{bmatrix} 1 \\ \vdots \\ 1 \\ w^p \\ \vdots \\ w^p \\ \vdots \\ \vdots \\ w^{p(p-1)} \\ \vdots \\ w^{p(p-1)} \end{bmatrix}.$$

Hence for $0 \le u \le p^2-1$ we have

$$\begin{aligned} c_u &= \frac{1}{p^2}\Big\{\left(1 + \theta^u + \cdots + \theta^{u(p^2-1)}\right) \\ &\quad + w^p\left(\theta^{up} + \theta^{u(p+1)} + \cdots + \theta^{u(2p-1)}\right) \\ &\quad + \cdots + w^{(p-1)p}\left(\theta^{(p-1)up} + \theta^{(p-1)up+u} + \cdots \right. \\ &\quad \left. + \theta^{(p-1)up+(p-1)u}\right)\Big\} \\ &= \frac{1}{p^2}\Big\{\left(1 + \theta^u + \cdots + \theta^{u(p^2-1)}\right) \\ &\quad + \theta^{(u-1)p}\left(1 + \theta^u + \cdots + \theta^{u(p^2-1)}\right) \\ &\quad + \cdots + \theta^{(u-1)(p-1)p}\left(1 + \theta^u + \cdots + \theta^{u(p^2-1)}\right)\Big\} \\ &= \frac{1}{p^2}\left(1 + \theta^u + \cdots + \theta^{u(p^2-1)}\right) \\ &\quad \cdot \left\{1 + \left(\theta^{(u-1)p}\right) + \cdots + \left(\theta^{(u-1)p}\right)^{p-1}\right\}. \end{aligned}$$

Note that

$$\begin{aligned} &1 + \left(\theta^{(u-1)p}\right) + \cdots + \left(\theta^{(u-1)p}\right)^{p-1} \\ &= \begin{cases} 0 & \text{if } u \not\equiv 1 \mod p, \\ p & \text{if } u \equiv 1 \mod p. \end{cases} \end{aligned}$$

Therefore $c_u = a_u$ for $u = 1 + lp$ with $0 \le l \le p-1$ and $c_u = 0$ otherwise. This completes the proof. □

Using Lemma 2.2 we obtain that for $t \ge 0$

$$s_f(t) = \sum_{l=0}^{p-1} a_{1+lp}\, e^{\frac{2\pi i}{p^2}[1+(l-t)p]\mathrm{Tr}(f(\beta^t))}. \tag{3}$$

For $k \ge 0$, let χ_k^L be the map on $\{0, 1, \ldots, L-1\}$ and χ_k^Γ be the multiplicative character of the cyclic group $\Gamma \setminus \{0\}$ defined as

$$\chi_k^L(t) = e^{\frac{2\pi i}{np} kt}, \quad t \in \{0, 1, \ldots, L-1\},$$

and

$$\chi_k^\Gamma(\beta^t) = e^{\frac{2\pi i}{n} kt}, \quad t \in \{0, 1, \ldots, n-1\}.$$

The character χ_k^Γ is extended to Γ by $\chi_k^\Gamma(0) = 0$.

For $f_1, f_2 \in \overline{S(D)}$ and $k \ge 0$, the sum $S_k(f_1, f_2)$ is given by

$$S_k(f_1, f_2) := \sum_{t=0}^{L-1} \chi_k^L(t) s_{f_1}(t) s_{f_2}(t). \tag{4}$$

Let $\alpha = e^{\frac{2\pi i}{p}}$. Using (3) and decomposing the sum (4) into p parts consisting of the ranges $0+ln, 1+ln, \ldots, n-1+ln$ with $0 \le l \le p-1$, we obtain the following lemma.

Lemma 2.3. *We have*

$$\begin{aligned} S_k(f_1, f_2) &= \sum_{t=0}^{n-1} \chi_{k+kn}^L(t) \sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1} C_k(l_1, l_2) \\ &\quad \cdot e^{\frac{2\pi i}{p^2}\{(1+l_1 p)\mathrm{Tr}(f_1(\beta^t)) + (1+l_2 p)\mathrm{Tr}(f_2(\beta^t))\}}, \end{aligned}$$

where $C_k(l_1, l_2)$ is the complex number

$$C_k(l_1, l_2) = \sum_{l=0}^{p-1} \alpha^{kl} a_{1+(l_1-l)p} a_{1+(l_2-l)p}.$$

Proof. For $0 \le t \le L-1$, using (3) we have

$$s_{f_1}(t)s_{f_2}(t) = \sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1} a_{1+l_1p}a_{1+l_2p} \cdot e^{\frac{2\pi i}{p^2}\{[1+(l_1-t)p]\mathrm{Tr}(f_1(\beta^t))+[1+(l_2-t)p]\mathrm{Tr}(f_2(\beta^t))\}}.$$

Note that

$$S_k(f_1,f_2) = \sum_{l=0}^{p-1}\sum_{t=0}^{n-1} \chi_k^L(t+ln)s_{f_1}(t+ln)s_{f_2}(t+ln).$$

For $0 \le t \le n-1$, $0 \le l \le p-1$, and $i = 1, 2$ we have

$$e^{\frac{2\pi i}{p^2}\{[1+(l_1-t-ln)p]\mathrm{Tr}(f_i(\beta^t))\}} = e^{\frac{2\pi i}{p^2}\{[1+(l+l_1-t)p]\mathrm{Tr}(f_i(\beta^t))\}}$$

and $\chi_k^L(t+ln) = \chi_k^L(t)\alpha^{kl}$. Therefore

$$\begin{aligned} S_k(f_1,f_2) &= \sum_{t=0}^{n-1}\chi_k^L(t)\sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1} a_{1+l_1p}a_{1+l_2p} \\ &\quad \times \sum_{l=0}^{p-1}\alpha^{kl}e^{\frac{2\pi i}{p^2}\{[1+(l_1+l-t)p]\mathrm{Tr}(f_1(\beta^t))+[1+(l_2+l-t)p]\mathrm{Tr}(f_2(\beta^t))\}} \\ &= \sum_{t=0}^{n-1}\chi_k^L(t)\sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1} a_{1+l_1p}a_{1+l_2p} \\ &\quad \times \sum_{l=0}^{p-1}\alpha^{k(l+t)}e^{\frac{2\pi i}{p^2}\{[1+(l_1+l)p]\mathrm{Tr}(f_1(\beta^t))+[1+(l_2+l)p]\mathrm{Tr}(f_2(\beta^t))\}}. \end{aligned}$$

We observe that $\chi_k^L(t)\alpha^{kt} = \chi_{k+kn}^L(t)$. Therefore

$$\begin{aligned} S_k(f_1,f_2) &= \sum_{t=0}^{n-1}\chi_{k+kn}^L(t) \\ &\quad \times \sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1} e^{\frac{2\pi i}{p^2}\{[1+l_1p]\mathrm{Tr}(f_1(\beta^t))+[1+l_2p]\mathrm{Tr}(f_2(\beta^t))\}} \\ &\quad \times \sum_{l=0}^{p-1}\alpha^{kl}a_{1+(l_1-l)p}a_{1+(l_2-l)p}. \end{aligned}$$

As $\sum_{l=0}^{p-1}\alpha^{kl}a_{1+(l_1-l)p}a_{1+(l_2-l)} = C_k(l_1,l_2)$, this completes the proof. □

The following properties of $C_k(l_1,l_2)$ follow from its definition:

(P1): For $k = k_0 + k_1p$, we have $C_k(l_1,l_2) = C_{k_0}(l_1,l_2)$.

(P2): $C_k(l_1+1, l_2+1) = \alpha^k C_k(l_1,l_2)$.

Example 2.4. *In Tables 1 and 2 we give the values of $C_k(l_1,l_2)$ in the cases $p = 2$ and $p = 3$.*

For integers h, k, let $\delta(h,k)$ be the complex number

$$\delta(h,k) = \sum_{t=0}^{h-1} e^{\frac{2\pi i}{np}kt}.$$

For the partial-period correlation of the sequences s_{f_1} and s_{f_2}, the function $\Delta_{f_1,f_2}(h)$ is given by

Table 1 The values of $C_k(l_1,l_2)$ for $p = 2$.

$C_k(l_1,l_2)$	(0,0)	(0,1)	(1,0)	(1,1)
0	0	1	1	0
1	$-w$	0	0	w

Table 2 The values of $C_k(l_1,l_2)$ for $p = 3$.

$C_k(l_1,l_2)$	(0,0)	(0,1)	(0,2)
0	$\frac{1}{3(-2w^3-1)}$	$\frac{1}{3(w^3+2)}$	$\frac{1}{3(w^3+2)}$
1	$-w^4-w$	0	0
2	$\frac{1}{3(-w^3-2w^2)}$	$\frac{1}{3(-w^3-2w^2)}$	$\frac{1}{3(-w^3+w^2)}$
$C_k(l_1,l_2)$	(1,0)	(1,1)	(1,2)
0	$\frac{1}{3(w^3+2)}$	$\frac{1}{3(-2w^3-1)}$	$\frac{1}{3(w^3+2)}$
1	0	w	0
2	$\frac{1}{3(-w^3-2w^2)}$	$\frac{1}{3(2w^3+w^2)}$	$\frac{1}{3(2w^3+w^2)}$
$C_k(l_1,l_2)$	(2,0)	(2,1)	(2,2)
0	$\frac{1}{3(w^3+2)}$	$\frac{1}{3(w^3+2)}$	$\frac{1}{3(-2w^3-1)}$
1	0	0	w^4
2	$\frac{1}{3(-w^3+w^2)}$	$\frac{1}{3(2w^3+w^2)}$	$\frac{1}{3(-w^3+w^2)}$

$$\Delta_{f_1,f_2}(h) := \frac{1}{L}\sum_{k=0}^{L-1}\bar{\delta}(h,k)S_k(f_1,f_2), \tag{5}$$

where $\bar{\delta}(h,k)$ is the complex conjugate of $\delta(h,k)$.

Proposition 2.5. *We have*

$$\begin{aligned} \Delta_{f_1,f_2}(h) &= \frac{1}{L}\sum_{k_0=0}^{p-1}\sum_{\substack{k_1=0\\ p\nmid k_1}}^{L-1}\bar{\delta}(h,k_1-k_0n)\sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1}C_{k_0}(l_1,l_2) \\ &\quad \times \sum_{t=0}^{n-1}\chi_{k_1/p}^{\Gamma}(\beta^t)e^{\frac{2\pi i}{p^2}\{(1+l_1p)\mathrm{Tr}(f_1(\beta^t))+(1+l_2p)\mathrm{Tr}(f_2(\beta^t))\}}. \end{aligned}$$

Proof. By decomposing the range $\{0,1,\ldots,L-1\}$ into p smaller ones we obtain

$$\Delta_{f_1,f_2}(h) = \frac{1}{L}\sum_{k_0=0}^{p-1}\sum_{\substack{k=0\\ p\nmid(k-k_0)}}^{L-1}\bar{\delta}(h,k)S_k(f_1,f_2).$$

Note that $\chi_{k+kn}^L(t) = \chi_{k+k_0n}^L(t)$ if $k \equiv k_0 \mod p$. Then using Lemma 2.3 we obtain

$$\begin{aligned} \Delta_{f_1,f_2}(h) &= \frac{1}{L}\sum_{k_0=0}^{p-1}\sum_{\substack{k=0\\ p\nmid(k-k_0)}}^{L-1}\bar{\delta}(h,k)\sum_{t=0}^{n-1}\chi_{k+k_0n}^L(t)\sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1}C_k(l_1,l_2) \\ &\quad \times e^{\frac{2\pi i}{p^2}\{(1+l_1p)\mathrm{Tr}(f_1(\beta^t))+(1+l_2p)\mathrm{Tr}(f_2(\beta^t))\}} \\ &= \frac{1}{L}\sum_{k_0=0}^{p-1}\sum_{\substack{k_1=0\\ p\nmid k_1}}^{L-1}\bar{\delta}(h,k_1-k_0n)\sum_{t=0}^{n-1}\chi_{k_1}^L(t)\sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1}C_{k_1-k_0n}(l_1,l_2) \\ &\quad \times e^{\frac{2\pi i}{p^2}\{(1+l_1p)\mathrm{Tr}(f_1(\beta^t))+(1+l_2p)\mathrm{Tr}(f_2(\beta^t))\}}. \end{aligned}$$

For $0 \le k_1 \le L-1$ with $p \mid k_1$, we observe that $\chi_{k_1}^L(t) = \chi_{k_1/p}^{\Gamma}(\beta^t)$. Moreover using the property (P1) of $C_k(l_1,l_2)$ we

obtain

$$\Delta_{f_1,f_2}(h) = \frac{1}{L}\sum_{k_0=0}^{p-1}\sum_{\substack{k_1=0\\ p\nmid k_1}}^{L-1}\bar{\delta}(h,k_1-k_0n)\sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1}C_{k_0}(l_1,l_2)$$
$$\times\sum_{t=0}^{n-1}\chi^{\Gamma}_{k_1/p}(\beta^t)e^{\frac{2\pi i}{p^2}\{(1+l_1p)\mathrm{Tr}(f_1(\beta^t))+(1+l_2p)\mathrm{Tr}(f_2(\beta^t))\}}.$$

□

Definition 2.6. For $0 \le k_0 \le p-1$, let R_{k_0} be the nonnegative integer defined as

$$R_{k_0} = \sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1}|C_{k_0}(l_1,l_2)|,$$

where $|C_{k_0}(l_1,l_2)|$ is the absolute value. Moreover let R be the nonnegative integer

$$R = \max\{R_{k_0} : 0 \le k_0 \le p-1\}.$$

Example 2.7. *For $p = 2$, we have*

$$R_0 = R_1 = R = 2.$$

For $p = 3$, we have

$$R_0 = 3\sqrt{3},\ R_1 = 3,\ R_2 = 3\sqrt{3},$$
$$\text{and } R = 3\sqrt{3} = 5.19615\ldots.$$

Recall that $\alpha = e^{\frac{2\pi i}{p}}$.

Definition 2.8. Let $B(p)$ be the constant depending on the prime number p defined as

$$B(p) = \max\left\{|1+\alpha^k+\cdots+\alpha^{kl}| : 1 \le k \le p-1,\ 0 \le l \le p-1\right\}.$$

Example 2.9. *We have*

$$B(2)=1,\ B(3)=1,\ B(5)=\sqrt{\frac{3+\sqrt{5}}{2}}=1.61803\ldots.$$

Now we state some important results from [5], [7] and [8].

Theorem 2.10 (Kumar-Helleseth-Calderbank). *For $f(x) \in \overline{S(D)} \setminus \mathrm{GR}(p^2,m)$, we have*

$$\left|\sum_{x\in\Gamma}e^{\frac{2\pi i}{p^2}\mathrm{Tr}(f(x))}\right| \le (D-1)q^{1/2}.$$

Theorem 2.11 (Shanbhag-Kumar-Helleseth). *For $f(x) \in \overline{S(D)} \setminus \mathrm{GR}(p^2,m)$ and $1 \le k \le n-1$ we have*

$$\left|\sum_{x\in\Gamma}\chi^{\Gamma}_k(x)e^{\frac{2\pi i}{p^2}\mathrm{Tr}(f(x))}\right| \le Dq^{1/2}.$$

Theorem 2.12 (Sarwate). *For $1 \le h \le L-1$ we have*

$$\sum_{k=0}^{L-1}|\bar{\delta}(h,k)| < \frac{2L}{\pi}\ln\left(\frac{4L}{\pi}\right).$$

Recall that the family $\mathcal{F}_D$ of sequences of complex numbers is constructed from the subset $\widetilde{P}_D^1 \cup \widetilde{P}_D^2$ of $\overline{S(D)}$. Using Theorems 2.10, 2.11 and 2.12 we obtain the following bound.

Proposition 2.13. *For $f_1(x), f_2(x) \in \widetilde{P}_D^1 \cup \widetilde{P}_D^2$ such that $(1+l_1p)f_1(x)+(1+l_2p)f_2(x) \notin \mathrm{GR}(p^2,m)$ for each $0 \le l_1, l_2 \le p-1$, we have*

$$|\Delta_{f_1,f_2}(h)| < \frac{R_0h+B(p)\sum_{k_0=1}^{p-1}R_{k_0}}{L}(D-1)q^{1/2}$$
$$+\frac{R_0h+B(p)\sum_{k_0=1}^{p-1}R_{k_0}}{L}+\frac{2R}{\pi}Dq^{1/2}\ln\frac{4L}{\pi}.$$

Proof. We consider the cases $k_1 = 0$ and $p \le k_1 < L-1$ with $p \mid k_1$ separately. For the case $k_1 = 0$, let

$$\Delta^{(1)}_{f_1,f_2}(h) := \frac{1}{L}\sum_{k_0=0}^{p-1}\bar{\delta}(h,-k_0n)\sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1}C_{k_0}(l_1,l_2)$$
$$\times\sum_{t=0}^{n-1}e^{\frac{2\pi i}{p^2}\{(1+l_1p)\mathrm{Tr}(f_1(\beta^t))+(1+l_2p)\mathrm{Tr}(f_2(\beta^t))\}}.$$

We also consider the subcases $k_0 = 0$ and $1 \le k_0 \le p-1$ in $\Delta^{(1)}_{f_1,f_2}(h)$ separately.

$$\Delta^{(1)}_{f_1,f_2}(h) = \frac{1}{L}\bar{\delta}(h,0)\sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1}C_0(l_1,l_2)$$
$$\cdot\sum_{t=0}^{n-1}e^{\frac{2\pi i}{p^2}\{(1+l_1p)\mathrm{Tr}(f_1(\beta^t))+(1+l_2p)\mathrm{Tr}(f_2(\beta^t))\}}$$
$$+\frac{1}{L}\sum_{k_0=1}^{p-1}\bar{\delta}(h,-k_0n)\sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1}C_{k_0}(l_1,l_2)$$
$$\cdot\sum_{t=0}^{n-1}e^{\frac{2\pi i}{p^2}\{(1+l_1p)\mathrm{Tr}(f_1(\beta^t))+(1+l_2p)\mathrm{Tr}(f_2(\beta^t))\}}.$$

Note that $|\bar{\delta}(h,0)| = h$. Also for $1 \le k_0 \le p-1$ we observe that $\delta(h,-k_0n) = 1+\alpha^{-k_0}+\alpha^{-2k_0}+\cdots+\alpha^{-(h-1)k_0}$ and hence $|\delta(h,-k_0n)| \le B(p)$. For $f(x) = (1+l_1p)f_1(x)+(1+l_2p)f_2(x)$ we have

$$\sum_{t=0}^{n-1}e^{\frac{2\pi i}{p^2}\{(1+l_1p)\mathrm{Tr}(f_1(\beta^t))+(1+l_2p)\mathrm{Tr}(f_2(\beta^t))\}} = \sum_{x\in\Gamma\setminus\{0\}}e^{\frac{2\pi i}{p^2}\mathrm{Tr}(f(x))}.$$

Moreover $f(x) \in \overline{S(D)} \setminus \mathrm{GR}(p^2,m)$ and $\left|e^{\frac{2\pi i}{p^2}\mathrm{Tr}(f(0))}\right| \le 1$. Therefore using Theorem 2.10 we get

$$\left|\sum_{t=0}^{n-1}e^{\frac{2\pi i}{p^2}\{(1+l_1p)\mathrm{Tr}(f_1(\beta^t))+(1+l_2p)\mathrm{Tr}(f_2(\beta^t))\}}\right| \le (D-1)q^{1/2}+1.$$

Recall that for $0 \le k_0 \le p-1$, $\sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1}|C_{k_0}(l_1,l_2)| = R_{k_0}$. Therefore

$$\left|\Delta^{(1)}_{f_1,f_2}(h)\right| \le \left(\frac{hR_0}{L}+\frac{B(p)\sum_{k_0=1}^{p-1}R_{k_0}}{L}\right)\left((D-1)q^{1/2}+1\right). \quad (6)$$

Next we consider the remaining case where $p \le k_1 < L-1$ with $p \mid k_1$ and we let

$$\Delta^{(2)}_{f_1,f_2}(h) := \frac{1}{L}\sum_{k_0=0}^{p-1}\sum_{\substack{k_1=p\\ p|k_1}}^{L-1}\bar{\delta}(h,k_1-k_0n)\sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1}C_{k_0}(l_1,l_2)$$
$$\times\sum_{t=0}^{n-1}\chi^{\Gamma}_{k_1/p}(\beta^t)e^{\frac{2\pi i}{p^m}\{(1+l_1p)\mathrm{Tr}(f_1(\beta^t))+(1+l_2p)\mathrm{Tr}(f_2(\beta^t))\}}.$$

Using Theorem 2.11 for $f(x)=(1+l_1p)f_1(x)+(1+l_2p)f_2(x)$ and noting that $\chi^{\Gamma}_{k_1/p}(0)=0$, we get

$$\left|\sum_{t=0}^{n-1}\chi^{\Gamma}_{k_1/p}(\beta^t)e^{\frac{2\pi i}{p^m}\{(1+l_1p)\mathrm{Tr}(f_1(\beta^t))+(1+l_2p)\mathrm{Tr}(f_2(\beta^t))\}}\right|\le Dq^{1/2}.$$

Note that $\sum_{l_1=0}^{p-1}\sum_{l_2=0}^{p-1}|C_{k_0}(l_1,l_2)|\le R$ for each $0\le k_0\le p-1$. Moreover

$$\sum_{k_0=0}^{p-1}\sum_{\substack{k_1=p\\ p|k_1}}^{L-1}|\bar{\delta}(h,k_1-k_0n)|<\sum_{k=0}^{L-1}|\bar{\delta}(h,k)|,$$

since the set of summands in the right hand side strictly includes the set of summands in the left hand side and there exists an extra nonzero summand in the right hand side. Therefore

$$\left|\Delta^{(2)}_{f_1,f_2}(h)\right|<\frac{RDq^{1/2}}{L}\sum_{k=0}^{L-1}|\bar{\delta}(h,k)|.$$

Using Theorem 2.12 we get

$$\left|\Delta^{(2)}_{f_1,f_2}(h)\right|<\frac{2R}{\pi}Dq^{1/2}\ln\frac{4L}{\pi}. \tag{7}$$

As $\Delta_{f_1,f_2}(h)=\Delta^{(1)}_{f_1,f_2}(h)+\Delta^{(1)}_{f_1,f_2}(h)$, using (6) and (7) we complete the proof. □

Remark 2.14. We observe that the bound of Proposition 2.13 holds also if there exist $0\le l_1,l_2\le p-1$ such that $(1+l_1p)f_1(x)+(1+l_2p)f_2(x)\in \mathrm{GR}(p^2,m)$. Indeed for such $0\le l_1,l_2\le p-1$, let $u=(1+l_1p)f_1(x)+(1+l_2p)f_2(x)\in \mathrm{GR}(p^2,m)$ and $R_{(l_1,l_2)}(h)$ be the contribution corresponding to (l_1,l_2) in $\Delta_{f_1,f_2}(h)$. We have $R_{(l_1,l_2)}(h)=R^{(1)}_{(l_1,l_2)}(h)+R^{(2)}_{(l_1,l_2)}(h)$, where

$$R^{(1)}_{(l_1,l_2)}(h)=\frac{1}{L}\sum_{k_0=0}^{p-1}\bar{\delta}(h,-k_0n)C_{k_0}(l_1,l_2)\sum_{t=0}^{n-1}e^{\frac{2\pi i}{p^m}\mathrm{Tr}(u)},$$

and

$$R^{(2)}_{(l_1,l_2)}(h)=\frac{1}{L}\sum_{k_0=0}^{p-1}\sum_{\substack{k_1=p\\ p|k_1}}^{L-1}\bar{\delta}(h,k_1-k_0n)C_{k_0}(l_1,l_2)$$
$$\cdot\sum_{t=0}^{n-1}\chi^{\Gamma}_{k_1/p}(\beta^t)e^{\frac{2\pi i}{p^m}\mathrm{Tr}(u)}.$$

As $\sum_{t=0}^{n-1}\chi^{\Gamma}_{k_1/p}(\beta^t)=0$ for each $p\le k_1\le L-1$ with $p|k_1$, we have $R^{(2)}_{(l_1,l_2)}(h)=0$. Moreover the main term of the bound of Proposition 2.13 is due to the term $\Delta^{(2)}_{f_1,f_2}(h)$ in the proof of Proposition 2.13. Hence the bound of Proposition 2.13 holds also if there exist $0\le l_1,l_2\le p-1$ such that $(1+l_1p)f_1(x)+(1+l_2p)f_2(x)\in \mathrm{GR}(p^2,m)$.

We recall that the aperiodic and the odd (generalized) correlation of the sequences s_{f_1} and s_{f_2} are

$$\theta^{a}_{f_1,f_2}(\tau)=\sum_{t=\max\{0,\tau\}}^{\min\{L-1,L-1-\tau\}}s_{f_1}(t+\tau)s_{f_2}(t),\quad\text{and}$$
$$\theta^{-}_{f_1,f_2}(j,\tau)=\sum_{t=0}^{L-\tau-1}s_{f_1}(t+\tau)s_{f_2}(t)+\alpha^j\sum_{t=L-\tau}^{L-1}s_{f_1}(t+\tau)s_{f_2}(t).$$

The Vinogradov method [4] implies that

$$\Delta_{f_1,f_2}(h)=\sum_{t=0}^{L-1}\delta_h(t)s_{f_1}(t)s_{f_2}(t), \tag{8}$$

where

$$\delta_h(t)=\begin{cases}1 & \text{if}\quad 0\le t<h\le L-1,\\ 0 & \text{otherwise}\end{cases}$$

is the indicator function of the partial period.

Using (8), Proposition 2.13 and Remark 2.14 we obtain the following theorem.

Theorem 2.15. *For $0\le\tau\le L-1$, $0\le j\le p-1$, and $f_1(x),f_2(x)\in\widetilde{P}^1_D\cup\widetilde{P}^2_D$ with $f_1\ne f_2$ or $\tau\ne 0$ we have*

$$|\theta^{a}_{f_1,f_2}(\tau)|<\left\{\frac{2R}{\pi}\ln\frac{4L}{\pi}+\frac{R_0(L-1)+B(p)\sum_{k_0=1}^{p-1}R_{k_0}}{L}\right\}Dq^{1/2}$$
$$-(q^{1/2}-1)\frac{R_0(L-1)+B(p)\sum_{k_0=1}^{p-1}R_{k_0}}{L}$$

and

$$|\theta^{-}_{f_1,f_2}(j,\tau)|<\left\{\frac{4R}{\pi}\ln\frac{4L}{\pi}+\frac{2R_0(L-1)+2B(p)\sum_{k_0=1}^{p-1}R_{k_0}}{L}\right\}Dq^{1/2}$$
$$-2(q^{1/2}-1)\frac{R_0(L-1)+B(p)\sum_{k_0=1}^{p-1}R_{k_0}}{L}$$

Proof. The proof follows from (8) and the application of Proposition 2.13 and Remark 2.14 with $h=L-1$. □

Remark 2.16. The bounds for the maximum aperiodic and odd correlations for $p=2$ and $p=3$ are comparable. Note that for the case $p=2$, the family $Q(D)$ of [3, Sect. 8.8] and the family $\mathcal{F}_D$ of [1, Theorem 3.12], which is slightly larger than $Q(D)$, also share the same upper bounds on the maximum aperiodic and odd correlations.

Remark 2.17. For the family $\mathcal{F}_D$, Welch's bound ([9], cf. [3, Theorem 9.2]) implies that if $0\le\tau\le L-1$, $f_1(x),f_2(x)\in\widetilde{P}^1_D\cup\widetilde{P}^2_D$ with $f_1\ne f_2$ or $\tau\ne 0$ we have

$$|\theta^a_{f_1,f_2}(\tau)| \geq L\sqrt{\frac{S-1}{S(2L-1)-1}}, \tag{9}$$

where $S = \frac{1}{p^m-1}\sum_{l|(p^m-1)}\mu(l)p^{m\left(\lfloor\frac{D}{7}\rfloor-\lfloor\frac{D}{p^2_7}\rfloor\right)} + \frac{p-2}{p^m-1}\sum_{l|(p^m-1)}\mu(l)p^{m(\lfloor\frac{D}{7}\rfloor-\lfloor\frac{D}{p^2}\rfloor)}$ is the size of the family $\mathcal{F}_D$ (cf. [1, Theorem 3.12]). For $p = 2$, $D = 5$ and $m = 40$, Welch's lower bound in (9) and the corresponding upper bound of Theorem 2.15 give

$$\frac{|\theta^a_{f_1,f_2}(\tau)|}{\sqrt{L}} \geq 0.7071067811\ldots$$

$$\text{and } \frac{|\theta^a_{f_1,f_2}(\tau)|}{\sqrt{L}\ln L} < 4.7388970959\ldots.$$

Similarly for $p = 3$, $D = 5$ and $m = 19$, using Welch's bound and Theorem 2.15 we get

$$\frac{|\theta^a_{f_1,f_2}(\tau)|}{\sqrt{L}} \geq 0.7071067812\ldots$$

$$\text{and } \frac{|\theta^a_{f_1,f_2}(\tau)|}{\sqrt{L}\ln L} < 10.2004297952\ldots.$$

References

[1] S. Ling and F. Özbudak, "Improved p-ary codes and sequence families from Galois rings of characteristic p^2," SIAM J. Discrete Math., vol.19, no.4, pp.1011–1028, 2006.

[2] S. Ling and F. Özbudak, "Improved p-ary codes and sequence families from Galois rings," in Sequences and Their Applications—SETA 2004, ed. T. Helleseth, D. Sarwate, H.-Y. Song, and K. Yang, LNCS 3486, pp.236–242, 2005.

[3] T. Helleseth and P.V. Kumar, "Sequences with low correlation," in Handbook of Coding Theory, vol.I, II, ed. V.S. Pless and W.C. Huffman, pp.1765–1853, North-Holland, Amsterdam, 1998.

[4] I.V. Vinogradov, Elements of Number Theory, Dover, New York, 1954.

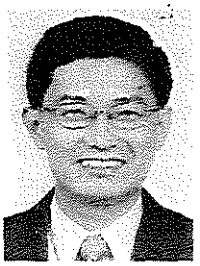
[5] A.G. Shanbhag, P.V. Kumar, and T. Helleseth, "Upper bound for a hybrid sum over Galois rings with applications to aperiodic and odd correlation of some q-ary sequences," IEEE Trans. Inf. Theory, vol.42, no.1, pp.250–254, 1996.

[6] S. Koponen and J. Lahtonen, "On the aperiodic and odd correlations of the binary Shanbhag-Kumar-Helleseth sequences," IEEE Trans. Inf. Theory, vol.43, no.5, pp.1593–1595, Sept. 1997.

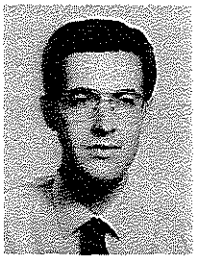
[7] P.V. Kumar, T. Helleseth, and A.R. Calderbank, "An upper bound for Weil exponential sums over Galois rings and applications," IEEE Trans. Inf. Theory, vol.41, no.1, pp.456–468, 1995.

[8] D.V. Sarwate, "An upper bound on the aperiodic autocorrelation function for a maximal-length sequence," IEEE Trans. Inf. Theory, vol.30, no.4, pp.685–687, 1984.

[9] L.R. Welch, "Lower bounds on the cross correlation of signals," IEEE Trans. Inf. Theory, vol.20, no.3, pp.397–399, 1974.



San Ling received the B.A. degree in mathematics from the University of Cambridge and the Ph.D. degree in mathematics from the University of California, Berkeley. Since April 2005, he has been a Professor with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, in the Nanyang Technological University, Singapore. Prior to that, he was with the Department of Mathematics, National University of Singapore. His research fields include: arithmetic of modular curves and application of number theory to combinatorial designs, coding theory, cryptography and sequence.



Ferruh Özbudak received the B.S. degree in electrical engineering in 1993 and in mathematics in 1997, both from Bilkent University, Ankara, Turkey. Currently he is an Associate Professor at the Middle East Technical University, Ankara, Turkey. His research interests includes algebraic curves, codes, sequences, finite fields and Galois rings.