Improved p-ary codes and sequence families from Galois rings of characteristic p^2

Ling, San; Özbudak, Ferruh

2006

Ling, S., & Özbudak, F. (2006). Improved p-ary codes and sequence families from Galois rings of characteristic p^2 . SIAM Journal of discrete mathematics, 19(4), 1011–1028.

<https://hdl.handle.net/10356/93854>

<https://doi.org/10.1137/S089548010444506x>

©2006 Society for Industrial and Applied Mathematics. This paper was published in SIAM J Discrete Math and is made available as an electronic reprint (preprint) with permission of Society for Industrial and Applied Mathematics. The paper can be found at <http://dx.doi.org/10.1137/S089548010444506x>. One print or electronic copy may be made for personal use only. Systematic or multiple reproduction, distribution to multiple locations via electronic or other means, duplication of any material in this paper for a fee or for commercial purposes, or modification of the content of the paper is prohibited and is subject to penalties under law.

Downloaded on 26 Apr 2023 19:54:09 SGT

IMPROVED p -ARY CODES AND SEQUENCE FAMILIES FROM GALOIS RINGS OF CHARACTERISTIC p^{2*}

SAN LING[†] AND FERRUH ÖZBUDAK[‡]

Abstract. This paper explores the applications of a recent bound on some Weil-type exponential sums over Galois rings in the construction of codes and sequences. A family of codes over $\mathbb{F}_p$, mostly nonlinear, of length p^{m+1} and size $p^2 \cdot p^{m(D - \lfloor D/p^2 \rfloor)}$, where $1 \leq D \leq p^{m/2}$, is obtained. The bound on this type of exponential sums provides a lower bound for the minimum distance of these codes. Several families of pairwise cyclically distinct p -ary sequences of period $p(p^m - 1)$ of low correlation are also constructed. They compare favorably with certain known p -ary sequences of period $p^m - 1$. Even in the case $p = 2$, one of these families is slightly larger than the family $Q(D)$ in section 8.8 in [T. Hellese and P. V. Kumar, *Handbook of Coding Theory*, Vol. 2, North-Holland, 1998, pp. 1765–1853], while they share the same period and the same bound for the maximum nontrivial correlation.

Key words. Galois rings, p -ary code, exponential sum, p -ary sequence

AMS subject classifications. 94B05, 94B40, 11T23

DOI. 10.1137/S089548010444506X

1. Introduction. Bounds on exponential sums over finite fields, such as the Weil–Carlitz–Uchiyama bound, have been found to be useful in applications such as coding theory and sequence designs. The analogue of the Weil–Carlitz–Uchiyama bound for Galois rings was presented in [K-H-C]. An improved bound for a related Weil-type exponential sum over Galois rings of characteristic 4, which is also sometimes called the trace of exponential sums, was obtained in [H-K-M-S] and was used in [S-K-H] to construct a family of binary codes with the same length and size as the Delsarte–Goethals codes, but whose minimum distance is significantly bigger. The shortening of these codes also leads to efficient binary sequences.

Recently, an analogue of the bound of [H-K-M-S] was obtained for Galois rings of characteristic p^2 , for all primes p [L-O]. In this paper, we explore some applications of this bound to the construction of codes and sequences. Starting from some trace codes over $\mathbb{Z}_{p^2}$ and applying the Gray map, a family of codes over $\mathbb{F}_p$ of length p^{m+1} and size $p^2 \cdot p^{m(D - \lfloor D/p^2 \rfloor)}$, where $1 \leq D \leq p^{m/2}$, is constructed. This family is a generalization of the family of binary codes of [S-K-H] and it is a family of nonlinear codes in general. A lower bound for their minimum distance is obtained through the bound of [L-O]. Using the generalized Nechaev–Gray map, several families of

*Received by the editors July 9, 2004; accepted for publication (in revised form) March 29, 2005; published electronically February 3, 2006.

<http://www.siam.org/journals/sidma/19-4/44506.html>

[†]Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Republic of Singapore (matlings@nus.edu.sg). Current address: 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 (lingsan@ntu.edu.sg). The research of this author was partially supported by NUS-ARF research grant R-146-000-029-112 and by DSTA research grant POD0411403.

[‡]Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, İnönü Bulvarı, 06531, Ankara, Turkey (ozbudak@math.metu.edu.tr). The research of this author was partially supported by the Turkish Academy of Sciences in the framework of the Young Scientists Award Programme (F.Ö./TÜBA-GEBİP/2003-13).

pairwise cyclically distinct p -ary sequences of period $p(p^m - 1)$ of low correlation are also obtained. They compare favorably with certain known p -ary sequences of period $p^m - 1$ (cf. [H-K, Table 4]). In fact, even in the case $p = 2$, one of these families is slightly larger than the family $Q(D)$ of [H-K, section 8.8], while they share the same period and the same bound for the maximum nontrivial correlation.

We fix the following conventions throughout the paper:

- p : a prime number,
- m : an integer with $m \geq 2$,
- $\mathbb{F}_p, \mathbb{F}_{p^m}$: finite fields of cardinality p and p^m ,
- $\text{tr}_m : \mathbb{F}_{p^m} \rightarrow \mathbb{F}_p$: the trace map from $\mathbb{F}_{p^m}$ onto $\mathbb{F}_p$,
- $\text{GR}(p^2, m)$: a Galois ring of characteristic p^2 with cardinality p^{2m} ,
- $\mathbb{Z}_{p^2}$: the ring of integers modulo p^2 ,
- $\text{Tr}_m : \text{GR}(p^2, m) \rightarrow \mathbb{Z}_{p^2}$: the trace map from $\text{GR}(p^2, m)$ onto $\mathbb{Z}_{p^2}$,
- Γ_m : the Teichmüller set in $\text{GR}(p^2, m)$,
- β : a primitive $(p^m - 1)$ th root of unity in $\text{GR}(p^2, m)$,
- $\rho : \text{GR}(p^2, m) \rightarrow \text{GR}(p^2, m)/p\text{GR}(p^2, m) \cong \mathbb{F}_{p^m}$: reduction modulo p map in $\text{GR}(p^2, m)$,
- $\omega = \rho(\beta)$: a primitive $(p^m - 1)$ th root of unity in $\mathbb{F}_{p^m}$.

We extend ρ to the polynomial ring mapping $\rho : \text{GR}(p^2, m)[x] \rightarrow \mathbb{F}_{p^m}[x]$ by its action on the coefficients. Note that the restricted map $\rho|_{\Gamma_m[x]} : \Gamma_m[x] \rightarrow \mathbb{F}_{p^m}[x]$ is one-to-one and onto.

We recall that the Frobenius operator Frob on $\text{GR}(p^2, m)$ is defined as

$$\text{Frob}(a + pb) = a^p + pb^p, \text{ where } a, b \in \Gamma_m.$$

Moreover Frob is extended to $\text{GR}(p^2, m)[x]$ as

$$\text{Frob} \left(\sum_{i=1}^l a_i x^i \right) = \sum_{i=1}^l \text{Frob}(a_i) x^{pi}.$$

A polynomial $f(x) \in \text{GR}(p^2, m)[x]$ is called *nondegenerate* if it cannot be written in the form

$$f(x) = \text{Frob}(g(x)) - g(x) + u \bmod p^2,$$

where $g(x) \in \text{GR}(p^2, m)[x]$ and $u \in \text{GR}(p^2, m)$.

2. $\mathbb{Z}_{p^2}$ -linear trace codes. In this section we construct a family of codes over $\mathbb{F}_p$ starting from some trace codes over $\mathbb{Z}_{p^2}$ and applying the Gray map. These codes can be considered as p -ary version of the codes of [S-K-H]. We obtain a lower bound for their minimum distance using a bound of [L-O].

We begin with a definition.

DEFINITION 2.1. For a finite $\mathbb{Z}_{p^2}$ -module $S \subseteq \text{GR}(p^2, m)[x]$, we define the subsets $S_0, S_1 \subseteq \Gamma_m[x]$ as

$$S_0 = \{a(x) \in \Gamma_m[x] : \text{there exists } b(x) \in \Gamma_m[x] \text{ such that } a(x) + pb(x) \in S\} \text{ and}$$

$$S_1 = \{b(x) \in \Gamma_m[x] : \text{there exists } a(x) \in \Gamma_m[x] \text{ such that } a(x) + pb(x) \in S\}.$$

Note that $|S| \leq |S_0| \cdot |S_1|$. Moreover, since S is a $\mathbb{Z}_{p^2}$ -module, we have $S_0 \subseteq S_1$.

It follows from Definition 2.1 that if $S \subseteq \text{GR}(p^2, m)[x]$ is a finite $\mathbb{Z}_{p^2}$ -module, then any element $f(x)$ of S is represented as

$$f(x) = a(x) + pb(x)$$

such that $a(x) \in S_0$ and $b(x) \in S_1$ are uniquely determined elements.

Example 2.2. Let $S = \{x + 2x^2, 2x, x + 2(x + x^2), 0\} \subseteq \text{GR}(2^2, m)[x]$. It is easy to observe that S is a $\mathbb{Z}_4$ -module. The corresponding subsets S_0 and S_1 are

$$S_0 = \{0, x\} \text{ and } S_1 = \{x, x^2, x^2 + x, 0\}.$$

Now we prove some lemmas that we use later in this section as well as in section 3.

LEMMA 2.3. *Let $S \subseteq \text{GR}(p^2, m)[x]$ be a finite $\mathbb{Z}_{p^2}$ -module and $S_1 \subseteq \Gamma_m[x]$ be the subset defined in Definition 2.1. Let $T \subseteq \Gamma_m$ be a subset. If the condition*

$$(2.1) \quad \begin{array}{l} \text{for each } h(x) \in \rho(S_1), \\ h(\nu) = 0 \text{ for each } \nu \in \rho(T) \Rightarrow h(x) \text{ is the zero polynomial} \end{array}$$

holds, then we have

$$\begin{array}{l} \text{for each } f(x) \in S, \\ f(\alpha) = 0 \text{ for each } \alpha \in T \Rightarrow f(x) \text{ is the zero polynomial.} \end{array}$$

Similarly if the condition

$$(2.2) \quad \begin{array}{l} \text{for each } h(x) \in \rho(S_1), \\ \text{tr}_m(h(\nu)) = 0 \text{ for each } \nu \in \rho(T) \Rightarrow h(x) \text{ is the zero polynomial} \end{array}$$

holds, then we have

$$\begin{array}{l} \text{for each } f(x) \in S, \\ \text{Tr}_m(f(\alpha)) = 0 \text{ for each } \alpha \in T \Rightarrow f(x) \text{ is the zero polynomial.} \end{array}$$

Proof. For a given $f(x) \in S$, let $a(x) \in S_0$ and $b(x) \in S_1$ be the elements such that $f(x) = a(x) + pb(x)$. Moreover let $a^{(1)}(x) = \rho(a(x)) \in \rho(S_0) \subseteq \rho(S_1)$ and $b^{(1)}(x) = \rho(b(x)) \in \rho(S_1)$.

Assume first that (2.1) holds and also let $f(x)$ be any element of S such that $f(\alpha) = 0$ for each $\alpha \in T$. Then $\rho(f(\alpha)) = 0$ for each $\alpha \in T$ and hence $a^{(1)}(\nu) = 0$ for each $\nu \in \rho(T)$. By (2.1) we have $a^{(1)}(x) = 0$. Since ρ is one-to-one on $\Gamma_m[x]$, we obtain that $a(x) = 0$. Hence $f(x) = pb(x)$. If $b^{(1)}(\nu) = 0$ for each $\nu \in \rho(T)$, then we have $b(x) = 0$ as above and $f(x) = 0$. Otherwise, if there exists $\nu \in \rho(T)$ such that $b^{(1)}(\nu) \neq 0$, then there exists $\alpha \in T$ such that $b(\alpha) = b_0 + pb_1$ with $b_0 \neq 0$ and hence $f(\alpha) \neq 0$.

Next we assume that (2.2) holds and also we assume that $f(x)$ is an element of S such that $\text{Tr}_m(f(\alpha)) = 0$ for each $\alpha \in T$. Then as above we have $\text{tr}_m(a^{(1)}(\nu)) = 0$ for each $\nu \in \rho(T)$. Using (2.2) we obtain that $a(x) = 0$ and hence $f(x) = pb(x)$. Similarly we also obtain that $b(x) = 0$. $\square$

For any integer j with $1 \leq j \leq p^m - 1$, its p -cyclotomic coset modulo $p^m - 1$ is defined as

$$B_j = \{a : 0 \leq a \leq p^m - 2 \text{ and } a \equiv jp^l \pmod{p^m - 1} \text{ for some integer } 0 \leq l \leq m - 1\}.$$

For $1 \leq j \leq p^{m/2}$, let $l = \lfloor m/2 \rfloor$ and $0 \leq j_0, \dots, j_l \leq p-1$ be the integers such that $j = j_0 + j_1p + \dots + j_lp^l$ and hence modulo $(p^m - 1)$ we have

$$(2.3) \quad \begin{bmatrix} j \\ pj \\ \vdots \\ p^{m-1}j \end{bmatrix} \equiv \begin{bmatrix} j_0 & j_1 & \cdots & j_{l-1} & j_l & 0 & \cdots & 0 \\ 0 & j_0 & \cdots & j_{l-2} & j_{l-1} & j_l & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ j_1 & j_2 & \cdots & j_l & 0 & 0 & \cdots & j_0 \end{bmatrix} \begin{bmatrix} 1 \\ p \\ \vdots \\ p^{l-1} \\ p^l \\ p^{l+1} \\ \vdots \\ p^{m-1} \end{bmatrix}.$$

Note that for j in (2.3), $p \nmid j$ means that $j_0 \neq 0$. Using the definition of B_j and the observation in (2.3), the following lemma readily follows.

LEMMA 2.4. *Let j be an integer with $1 \leq j \leq p^{m/2}$. Then the cardinality of its p -cyclotomic coset B_j modulo $p^m - 1$ is m . Moreover, if i and j are positive integers with $i < j \leq p^{m/2}$ and $p \nmid i$, $p \nmid j$, then $B_i \cap B_j = \emptyset$.*

For a nonnegative integer h , let $I(h)$ denote the set of nonnegative integers

$$I(h) = \{i : i \not\equiv 0 \pmod{p} \text{ and } 0 \leq i \leq h\}.$$

Note that $|I(h)| = h - \lfloor \frac{h}{p} \rfloor$.

LEMMA 2.5. *Let D be a positive integer with $D \leq p^{m/2}$ and let M be the set of polynomials in $\mathbb{F}_{p^m}[x]$ defined as*

$$M = \left\{ g(x) \in \mathbb{F}_{p^m}[x] : g(x) = \sum_{i \in I(D)} g_i x^i \right\}.$$

If $g(x) \in M$, $a \in \mathbb{F}_p$, and $a + \text{tr}_m(g(\omega^l)) = 0$ for each $1 \leq l \leq p^m - 1$, then $a = 0$ and $g(x) = 0$.

Proof. For $a \in \mathbb{F}_{p^m}$ and $g(x) \in M$ with $a + \text{tr}_m(g(\omega^l)) = 0$ for each $1 \leq l \leq p^m - 1$, let $f(x) \in \mathbb{F}_{p^m}[x]$ such that $\deg f(x) \leq p^m - 2$ and

$$f(x) \equiv a + \text{tr}_m(g(x)) \pmod{(x^{p^m-1} - 1)}.$$

Then $f(\omega^l) = a + \text{tr}_m(g(\omega^l)) = 0$ for each $1 \leq l \leq p^m - 1$. As $\deg f(x) \leq p^m - 2$, we also obtain that $f(x) = 0$. Assume that $g(x)$ is not the zero polynomial, since otherwise the proof is clear. For each monomial $g_i x^i$ in $g(x)$ with a nonzero coefficient g_i , let $f_i(x) \in \mathbb{F}_{p^m}[x]$ such that $\deg f_i(x) \leq p^m - 2$ and

$$(2.4) \quad f_i(x) \equiv \text{tr}_m(g_i x^i) \pmod{(x^{p^m-1} - 1)}.$$

We have $i \in I(D)$,

$$f_i(x) \equiv g_i x^i + g_i^p x^{ip} + \dots + g_i^{p^{m-1}} x^{ip^{m-1}} \pmod{(x^{p^m-1} - 1)}$$

and hence the set of the degrees of the monomials in $f_i(x)$ with nonzero coefficients is the p -cyclotomic coset B_i of i modulo $p^m - 1$. As $0 = f(x)$ is the sum of a and the sum of the polynomials in (2.4) as $g_i x^i$ runs through the monomials in $g(x)$ with nonzero coefficients, using Lemma 2.4 we obtain that $a = 0$ and $g(x) = 0$. $\square$

DEFINITION 2.6. For a prime number p we define a weight function w_p on $\mathbb{N}$ as

$$\begin{aligned} w_p : \mathbb{N} &\rightarrow \mathbb{N} \\ a &\mapsto \text{the sum of digits of the representation of } a \text{ in base } p. \end{aligned}$$

In other words, if $a = \sum_{i \geq 0} a_i p^i$ with $0 \leq a_i \leq p-1$ for all $i \geq 0$, then $w_p(a) = \sum_{i \geq 0} a_i$.

We recall that the *weighted degree* (cf. [K-H-C]) D_f of a polynomial $f(x) \in \text{GR}(p^2, m)[x]$ is defined as

$$D_f = \max\{p \deg(a(x)), \deg(b(x))\},$$

where $a(x), b(x) \in \Gamma_m[x]$ are the uniquely determined polynomials such that $f(x) = a(x) + pb(x)$.

Let $f(x) = a(x) + pb(x)$ be a nondegenerate polynomial with $a(x), b(x) \in \Gamma_m[x]$. We recall (see [L-O]) some definitions which depend on $f(x)$. Let $I_f, J_f \subseteq \mathbb{N}$ be subsets defined as

$$a(x) = \sum_{i \in I_f} a_i x^i \text{ and } b(x) = \sum_{j \in J_f} b_j x^j, \text{ where } a_i, b_j \in \Gamma_m \setminus \{0\}.$$

We define nonnegative integers W_f, l_f , and h_f as

$$W_f = \max\{p \max\{w_p(i) \mid i \in I_f\}, \max\{w_p(j) \mid j \in J_f\}\},$$

$$l_f = \left\lceil \frac{m}{W_f} \right\rceil - 1 \text{ and } h_f = \left\lfloor \frac{m}{W_f} \right\rfloor.$$

The following result is proved in [L-O].

THEOREM 2.7. For a nondegenerate polynomial $f(x) \in \text{GR}(p^2, m)[x]$, we have

$$\left| \sum_{a \in \mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2}} \sum_{x \in \Gamma_m} e^{2\pi i \frac{\text{Tr}_m(af(x))}{p^2}} \right| \leq p^{l_f+1} \left\lfloor \frac{p^{h_f} \frac{p^2-p}{2} (D_f - 1) \lfloor 2p^{\frac{m}{2}-h_f} \rfloor}{p^{l_f+1}} \right\rfloor.$$

For a positive integer D , let $S(D) \subseteq \text{GR}(p^2, m)[x]$ be the finite $\mathbb{Z}_{p^2}$ -module defined as

$$(2.5) \quad S(D) = \left\{ f(x) \in \text{GR}(p^2, m)[x] : f(x) = \sum_{i \in I(D)} f_i x^i \text{ and } D_f \leq D \right\}.$$

For the subsets $S(D)_0, S(D)_1 \in \Gamma_m[x]$ defined in Definition 2.1 we have

$$\begin{aligned} S(D)_0 &= \left\{ a(x) \in \Gamma_m[x] : a(x) = \sum_{i \in I(\lfloor \frac{D}{p} \rfloor)} a_i x^i \right\}, \\ S(D)_1 &= \left\{ b(x) \in \Gamma_m[x] : b(x) = \sum_{i \in I(D)} a_i x^i \right\}, \end{aligned}$$

and hence

$$(2.6) \quad |S(D)| = p^{m(D - \lfloor \frac{D}{p^2} \rfloor)}.$$

For each $u \in \mathbb{Z}_{p^2}$, recall that its homogeneous weight (cf. [C-H], [L-B]) $w_{\text{hom}}(u)$ is defined as

$$w_{\text{hom}}(u) = \begin{cases} 0 & \text{if } u = 0, \\ p & \text{if } u \in p\mathbb{Z}_{p^2} \setminus \{0\}, \\ p-1 & \text{if } u \in \mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2}. \end{cases}$$

Moreover, for each $l \geq 2$ and $u_1, \dots, u_l \in \mathbb{Z}_{p^2}$, we also have $w_{\text{hom}}(u_1, \dots, u_l) = \sum_{i=1}^l w_{\text{hom}}(u_i)$ by definition.

For $n \geq 1$ we recall that the Gray map (cf. [C], [G-S], [L-B], [L-S]) Φ over $\mathbb{Z}_{p^2}^n$ is defined as follows: For $u \in \mathbb{Z}_{p^2}$ let $u = r_0(u) + pr_1(u)$ with $r_0(u), r_1(u) \in \{0, 1, \dots, p-1\}$. We denote the addition modulo p as $\oplus$. For $(u_0, u_1, \dots, u_{n-1}) \in \mathbb{Z}_{p^2}^n$, we have $\Phi(u_0, u_1, \dots, u_{n-1}) = (a_0, a_1, \dots, a_{pn-1}) \in \mathbb{F}_p^{pn}$ such that for $0 \leq j \leq p-1$ and $0 \leq t \leq n-1$, $a_{jn+t} = r_1(u_t) \oplus jr_0(u_t)$. It follows that for $(u_0, u_1, \dots, u_{n-1}) \in \mathbb{Z}_{p^2}^n$,

$$w_{\text{hom}}(u_0, u_1, \dots, u_{n-1}) = w_H(\Phi(u_0, u_1, \dots, u_{n-1})),$$

where $w_H(\cdot)$ is the Hamming weight on $\mathbb{F}_p^{pn}$ (cf. [L-B]).

Now we construct a family of p -ary codes generalizing the family of binary codes of [S-K-H]. Note that there is another class of binary codes generalizing the Kerdock and Delsarte–Goethals codes using the ring $\mathbb{Z}_{2^k}$ (cf. [C]).

DEFINITION 2.8. For $1 \leq D \leq p^{m/2}$, let $C(D)$ be the $\mathbb{Z}_{p^2}$ -linear code of length p^m defined as

$$C(D) = \left\{ \left(\text{Tr}_m(f(0)) + u, \text{Tr}_m(f(\beta)) + u, \dots, \text{Tr}_m(f(\beta^{p^m-1})) + u \right) \mid f(x) \in S(D) \text{ and } u \in \mathbb{Z}_{p^2} \right\}.$$

The image $\Phi(C(D))$ of $C(D)$ under the Gray map Φ is a p -ary code of length p^{m+1} . From Lemmas 2.3 and 2.4 we obtain that the size of $\Phi(C(D))$ is $p^2|S(D)|$.

Using Theorem 2.7, we may obtain a lower bound for the minimum distance of $\Phi(C(D))$. For $p = 2$, our lower bound coincides with the lower bound of [S-K-H]. We need a further definition in order to state the lower bound on the minimum distance.

DEFINITION 2.9. For $1 \leq D \leq p^{m/2}$, let W_D , l_D , and h_D be the nonnegative integers defined as

$$W_D = \max\{W_f \mid f(x) \in S(D) \setminus \{0\}\}, \quad l_D = \left\lceil \frac{m}{W_D} \right\rceil - 1, \quad \text{and} \quad h_D = \left\lfloor \frac{m}{W_D} \right\rfloor.$$

Note that $l_D = \min\{l_f : f(x) \in S(D) \setminus \{0\}\}$ and $h_D = \min\{h_f : f(x) \in S(D) \setminus \{0\}\}$.

The following theorem follows from Theorem 2.7 and (2.6).

THEOREM 2.10. For $1 \leq D \leq p^{m/2}$, $\Phi(C(D))$ is a p -ary code of length p^{m+1} of minimum distance

$$(2.7) \quad d_{\min} \geq p^{m+1} - p^m - p^{l_D} \left\lfloor \frac{p^{h_D} \frac{p^2 - p}{2} (D - 1) \lfloor 2p^{\frac{m}{2} - h_D} \rfloor}{p^{l_D + 1}} \right\rfloor$$

and of size

$$(2.8) \quad |\Phi(C(D))| = p^2 \cdot p^{m(D - \lfloor \frac{D}{p^2} \rfloor)}.$$

3. p -ary sequences with low correlation. In this section we obtain several families of pairwise cyclically distinct p -ary sequences with low correlation.

We begin with a simple lemma that we use later.

LEMMA 3.1. *For $a \in \text{GR}(p^2, m) \setminus \{0\}$ and a nonnegative integer i , we have*

$$a(1 - \beta^i) = 0 \implies \beta^i = 1.$$

Proof. Let $a = a_0 + pa_1$ with $a_0, a_1 \in \Gamma_m$. If $a_0 \neq 0$, then a is a unit and we get the conclusion. If $a_0 = 0$, then $a = pa_1$ and hence $1 - \beta^i$ belongs to the maximal ideal (p) of $\text{GR}(p^2, m)$. Therefore $1 - \omega^i = 0$, which implies that $\beta^i = 1$. $\square$

For $f(x) \in S(D)$ and for each $i \geq 0$, we have $\text{Tr}_m(f(\beta^i)) = \text{Tr}_m(f(\beta^{i+(p^m-1)}))$. Therefore the period of $\mathbb{Z}_{p^2}$ -sequence $\{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty$ divides $p^m - 1$. We first study the exact periods of the sequences in greater detail.

LEMMA 3.2. *For a positive divisor t of $p^m - 1$ and $f(x) = \sum_{s \in I(D)} f_s x^s \in S(D) \setminus \{0\}$, the period of $\{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty$ is t if and only if $\gcd(\gcd\{s \in I(D) : f_s \neq 0\}, p^m - 1) = \frac{p^m - 1}{t}$.*

Proof. Let $u = \gcd(\gcd\{s \in I(D) : f_s \neq 0\}, p^m - 1)$ and $t_1 = \frac{p^m - 1}{u}$. Assume that the period of $\{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty$ is t . For each $i \geq 0$, we have $\text{Tr}_m(f(\beta^i)) = \text{Tr}_m(f(\beta^{i+t}))$. Then

$$\text{Tr}_m \left(\sum_{s \in I(D)} f_s (1 - \beta^{ts}) \beta^{is} \right) = 0$$

for each $i \geq 0$. Since $\sum_{s \in I(D)} f_s (1 - \beta^{ts}) x^s \in S(D)$, using Lemmas 2.3 and 2.5 we obtain that $f_s (1 - \beta^{ts}) = 0$ for each $s \in I(D)$. By Lemma 3.1, we have $\beta^{ts} = 1$ for each $s \in I(D)$ with $f_s \neq 0$. Then $(p^m - 1) | (ts)$ for each $s \in I(D)$ with $f_s \neq 0$ and hence $\frac{p^m - 1}{t} | u$, i.e., t_1 divides t . On the other hand, note that $\beta^{st_1} = \beta^{\frac{s}{u}(p^m - 1)} = 1$ for each $s \in I(D)$ with $f_s \neq 0$. Hence $\text{Tr}_m(f(\beta^{i+t_1})) = \text{Tr}_m(f(\beta^i))$ for each $i \geq 0$, so t divides t_1 .

Conversely assume that t is a positive divisor of $p^m - 1$ and $f(x) = \sum_{s \in I(D)} f_s x^s \in S(D) \setminus \{0\}$ such that $u = \frac{p^m - 1}{t}$. Then $\beta^{st} = \beta^{\frac{s}{u}(p^m - 1)} = 1$ for each $s \in I(D)$ with $f_s \neq 0$ and hence $\text{Tr}_m(f(\beta^{i+t})) = \text{Tr}_m(f(\beta^i))$ for each $i \geq 0$. Let $t_2 \leq t$ be the period of $\{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty$. If $t_2 < t$, then by the first part of the proof above, we have $u = \frac{p^m - 1}{t_2} \neq \frac{p^m - 1}{t}$, which is a contradiction. This completes the proof. $\square$

The following lemma is used in the proof of Proposition 3.5.

LEMMA 3.3. *For each positive divisor t of $(p^m - 1)$, the mapping $g(x) \in S(\lfloor \frac{D}{t} \rfloor) \mapsto f(x) = g(x^t) \in S(D)$ gives a one-to-one correspondence between $S(\lfloor \frac{D}{t} \rfloor)$ and the polynomials $f(x) \in S(D)$ such that $\{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty$ is a sequence of period dividing $\frac{p^m - 1}{t}$.*

Proof. For $g(x) \in S(\lfloor \frac{D}{t} \rfloor) \setminus \{0\}$ and $f(x) = g(x^t) = \sum_{s \in I(D)} f_s x^s$, we have $f(x) \in S(D) \setminus \{0\}$ and $t | \gcd(\gcd\{s \in I(D) : f_s \neq 0\}, p^m - 1)$. Then the period of $\{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty$ is a divisor of $\frac{p^m - 1}{t}$ by Lemma 3.2. Conversely if $f(x) = \sum_{s \in I(D)} f_s x^s \in S(D) \setminus \{0\}$ with the period t_1 of $\{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty$ such that $t_1 | \frac{p^m - 1}{t}$, then $\gcd(\gcd\{s \in I(D) : f_s \neq 0\}, p^m - 1) = \frac{p^m - 1}{t_1} = ta$ for a positive integer a . Hence $t | s$ for each $s \in I(D)$ with $f_s \neq 0$ and there exists a uniquely determined $g(x) \in S(\lfloor \frac{D}{t} \rfloor)$ such that $g(x^t) = f(x)$. $\square$

Remark 3.4. Using the similar mapping in Lemma 3.3 for $pS(D)_1$, for each positive divisor t of $(p^m - 1)$, we also obtain a one-to-one correspondence between $S(\lfloor \frac{D}{t} \rfloor)_1$ and the polynomials $f(x) \in pS(D)_1$ such that $\{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty$ has period dividing $\frac{p^m-1}{t}$.

In the next proposition, for each positive divisor t of $p^m - 1$, we compute the number of polynomials $f(x)$ in $S(D)$ such that the $\mathbb{Z}_{p^2}$ -sequence $\{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty$ has period $\frac{p^m-1}{t}$.

PROPOSITION 3.5. *For each positive divisor t of $(p^m - 1)$, we have*

$$\left| \left\{ f(x) \in S(D) : \{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty \text{ has period } \frac{p^m-1}{t} \right\} \right| \\ = \sum_{l \mid \frac{p^m-1}{t}} \mu(l) \left| S \left(\left\lfloor \frac{D}{l \cdot t} \right\rfloor \right) \right|,$$

where $\mu(\cdot)$ is the Möbius function.

Proof. For positive integers u and v , let

$$h(u) = |\{f(x) \in S(D) : \text{the period of } \{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty \text{ is } u\}|$$

and

$$H(v) = |\{f(x) \in S(D) : \text{the period of } \{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty \text{ is a positive divisor of } v\}|.$$

Then $h(u) = 0$ if $u \geq 1$ such that u does not divide $(p^m - 1)$. Moreover, for each positive integer v ,

$$H(v) = \sum_{u \mid v} h(u).$$

Using the Möbius inversion formula (cf. [L-N, Theorem 3.24]), for each positive integer u we obtain that

$$h(u) = \sum_{v \mid u} \mu(v) H \left(\frac{u}{v} \right).$$

In particular, for $u = \frac{p^m-1}{t}$ with a positive divisor t of $(p^m - 1)$,

$$h \left(\frac{p^m-1}{t} \right) = \sum_{l \mid \frac{p^m-1}{t}} \mu(l) H \left(\frac{p^m-1}{l \cdot t} \right).$$

Using Lemma 3.3, we obtain $H(\frac{p^m-1}{l \cdot t}) = |S(\lfloor \frac{D}{l \cdot t} \rfloor)|$, which completes the proof. $\square$

Using the same method as the proof of Proposition 3.5 and Remark 3.4, we also obtain the following result.

PROPOSITION 3.6. *For each positive divisor t of $(p^m - 1)$, we have*

$$\left| \left\{ f(x) \in pS(D)_1 : \{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty \text{ has period } \frac{p^m-1}{t} \right\} \right| \\ = \sum_{l \mid \frac{p^m-1}{t}} \mu(l) \left| S \left(\left\lfloor \frac{D}{l \cdot t} \right\rfloor \right)_1 \right|,$$

where $\mu(\cdot)$ is the Möbius function.

For $n = p^m - 1$ we recall that the generalized Nechaev–Gray map (cf. [N], [L-B], [L-S]) Ψ over $\mathbb{Z}_{p^2}^n$ is defined as follows: for $u \in \mathbb{Z}_{p^2}^n$ let $u = r_0(u) + pr_1(u)$ with $r_0(u), r_1(u) \in \{0, 1, \dots, p-1\}$. Let $\oplus$ denote the addition modulo p . For $(u_0, u_1, \dots, u_{n-1}) \in \mathbb{Z}_{p^2}^n$, we have $\Psi(u_0, u_1, \dots, u_{n-1}) = (a_0, a_1, \dots, a_{pn-1}) \in \mathbb{F}_p^{pn}$ such that for $0 \leq j \leq p-1$ and $0 \leq t \leq n-1$, $a_{jn+t} = r_1((1-p)^t u_t) \oplus jr_0((1-p)^t u_t)$. It is known that if C is a cyclic code of length $p^m - 1$ over $\mathbb{Z}_{p^2}$, then $\Psi(C)$ is a cyclic code of length $p(p^m - 1)$ over $\mathbb{F}_p$ (cf. [L-B, Corollary 2.5]). Therefore the generalized Nechaev–Gray map may be used for constructing sequences.

PROPOSITION 3.7. *Assume that $u \in \mathbb{Z}_{p^2}$. For $f(x) \in S(D)$ such that the corresponding $\mathbb{Z}_{p^2}$ -sequence $\{\text{Tr}_m(f(\beta^i))\}_{i=0}^\infty$ has period $p^m - 1$, we have the following:*

- (i) *if $\rho(f(x)) \neq 0$, then the p -ary sequence $\{\Psi(\text{Tr}_m(f(\beta^i)) + u)\}_{i=0}^\infty$ has period $p(p^m - 1)$;*
- (ii) *if $\rho(f(x)) = 0$ and $\rho(u) \neq 0$, then the p -ary sequence $\{\Psi(\text{Tr}_m(f(\beta^i)) + u)\}_{i=0}^\infty$ has period $p(p^m - 1)$;*
- (iii) *if $\rho(f(x)) = 0$ and $\rho(u) = 0$, then the p -ary sequence $\{\Psi(\text{Tr}_m(f(\beta^i)) + u)\}_{i=0}^\infty$ has period $p^m - 1$.*

Proof. Every $z \in \mathbb{Z}_{p^2}$ can be written uniquely as $z = r_0(z) + pr_1(z)$ with $r_0(z), r_1(z) \in \{0, 1, \dots, p-1\}$. Let $\oplus$ and $\ominus$ denote the addition and subtraction, respectively, modulo p while $+$ and $-$ denote the addition and subtraction in $\mathbb{Z}_{p^2}$.

For $f(x) \in S(D)$ satisfying the condition of the proposition and $u \in \mathbb{Z}_{p^2}$, we first observe that the period of the $\mathbb{Z}_{p^2}$ -sequence $\{\text{Tr}_m(f(\beta^i)) + u\}_{i=0}^\infty$ is also $p^m - 1$.

By the definition of Ψ , for $0 \leq t \leq (p^m - 1) - 1$ and $j \geq 0$, the $(j(p^m - 1) + t)$ th term of the p -ary sequence $\{\Psi(\text{Tr}_m(f(\beta^i)) + u)\}_{i=0}^\infty$ is given by

$$\begin{aligned} & r_1((1-p)^t(\text{Tr}_m(f(\beta^t)) + u)) \oplus jr_0((1-p)^t(\text{Tr}_m(f(\beta^t)) + u)) \\ &= r_1((1+jp)(1-p)^t(\text{Tr}_m(f(\beta^t)) + u)) \\ &= r_1((1-p)^{j(p^m-1)+t}(\text{Tr}_m(f(\beta^{j(p^m-1)+t})) + u)). \end{aligned}$$

The period of $\{\text{Tr}_m(f(\beta^i)) + u\}_{i=0}^\infty$ is $p^m - 1$, while the period of $\{(1-p)^i\}_{i=0}^\infty$ is p . Hence, the period T of $\{\Psi(\text{Tr}_m(f(\beta^i)) + u)\}_{i=0}^\infty = \{r_1((1-p)^i(\text{Tr}_m(f(\beta^i)) + u))\}_{i=0}^\infty$ divides $p(p^m - 1)$.

As the period of $\{\Psi(\text{Tr}_m(f(\beta^i)) + u)\}_{i=0}^\infty$ is T , for each $i \geq 0$ and $j \geq 0$ we have

$$\begin{aligned} & r_1((1-p)^{i+j(p^m-1)}(\text{Tr}_m(f(\beta^{i+j(p^m-1)})) + u)) \\ &= r_1((1-p)^{i+j(p^m-1)+T}(\text{Tr}_m(f(\beta^{i+j(p^m-1)+T})) + u)) \end{aligned}$$

and hence

$$(3.1) \quad \begin{aligned} & r_1(\text{Tr}_m(f(\beta^i)) + u) \ominus (i-j)r_0(\text{Tr}_m(f(\beta^i)) + u) \\ &= r_1(\text{Tr}_m(f(\beta^{i+T})) + u) \ominus (i+T-j)r_0(\text{Tr}_m(f(\beta^{i+T})) + u). \end{aligned}$$

Comparing (3.1) for different values of j , we obtain

$$(3.2) \quad r_0(\text{Tr}_m(f(\beta^i)) + u) = r_0(\text{Tr}_m(f(\beta^{i+T})) + u)$$

for each $i \geq 0$. Using (3.1) with $i = j$, we also get

$$(3.3) \quad \begin{aligned} & r_1(\text{Tr}_m(f(\beta^i)) + u) = r_1(\text{Tr}_m(f(\beta^{i+T})) + u) \\ & \quad \ominus Tr_0(\text{Tr}_m(f(\beta^{i+T})) + u). \end{aligned}$$

It follows from (3.2) and (3.3) that

$$\begin{aligned} & r_0(\text{Tr}_m(f(\beta^i)) + u) = r_0(\text{Tr}_m(f(\beta^{i+pT})) + u), \\ & r_1(\text{Tr}_m(f(\beta^i)) + u) = r_1(\text{Tr}_m(f(\beta^{i+pT})) + u), \end{aligned}$$

and hence

$$\mathrm{Tr}_m(f(\beta^i)) + u = \mathrm{Tr}_m(f(\beta^{i+pT})) + u$$

for each $i \geq 0$. Therefore $(p^m - 1)|(pT)$, which implies that $(p^m - 1)|T$. Moreover, recall also that T divides $p(p^m - 1)$, so

$$(3.4) \quad \text{either } T = p^m - 1 \text{ or } T = p(p^m - 1).$$

Now we prove that $T = p(p^m - 1)$ for (i) and (ii). Using (3.4) we assume the contrary that $T = p^m - 1$. As $\beta^T = 1$, by (3.3) we obtain that

$$r_0(\mathrm{Tr}_m(f(\beta^i)) + u) = \mathrm{tr}_m(\rho(f)(\omega^i)) + \rho(u) = 0$$

for each $i \geq 0$. Then by Lemma 2.5 we have $\rho(u) = 0$ and $\rho(f(x)) = 0$, which completes the proof for (i) and (ii).

Next we assume $\rho(f(x)) = 0$, $\rho(u) = 0$ and consider the remaining case. For each $i \geq 0$, the i th and $(i + (p^m - 1))$ th terms of $\{\Psi(\mathrm{Tr}_m(f(\beta^i)) + u)\}_{i=0}^\infty$ are

$$r_1(\mathrm{Tr}_m(f(\beta^i)) + u) \ominus ir_0(\mathrm{Tr}_m(f(\beta^i)) + u)$$

and

$$(3.5) \quad r_1(\mathrm{Tr}_m(f(\beta^i)) + u) \ominus (i - 1)r_0(\mathrm{Tr}_m(f(\beta^i)) + u),$$

respectively. Therefore, as $\rho(f(x)) = 0$, the i th and $(i + (p^m - 1))$ th terms of $\{\Psi(\mathrm{Tr}_m(f(\beta^i)) + u)\}_{i=0}^\infty$ are equal for each $i \geq 0$ if and only if

$$(3.6) \quad r_0(u) = \rho(u) = 0.$$

We complete the proof for (iii) using (3.4) and (3.6). $\square$

Now we begin our construction of families of pairwise cyclically distinct p -ary sequences of low correlation.

For a p -ary sequence $\{s(i)\}_{i=0}^\infty$ and $\tau \geq 0$, the *cyclic shift of $\{s(i)\}_{i=0}^\infty$ by τ* is the p -ary sequence $\{s(i + \tau)\}_{i=0}^\infty$. For two p -ary sequences $\{s_1(i)\}_{i=0}^\infty$ and $\{s_2(i)\}_{i=0}^\infty$, we say $\{s_1(i)\}_{i=0}^\infty$ and $\{s_2(i)\}_{i=0}^\infty$ are *cyclically distinct* if for each $\tau \geq 1$ neither is $\{s_1(i)\}_{i=0}^\infty$ the cyclic shift of $\{s_2(i)\}_{i=0}^\infty$ by τ nor is $\{s_2(i)\}_{i=0}^\infty$ the cyclic shift of $\{s_1(i)\}_{i=0}^\infty$ by τ .

Let $\mathcal{P}_D^1$ be the subset of $S(D) \times \mathbb{Z}_{p^2}$ defined as

$$\mathcal{P}_D^1 = \left\{ (f(x), u) \in S(D) \times \mathbb{Z}_{p^2} : \rho(f(x)) \neq 0, \right. \\ \left. \text{and } \{\mathrm{Tr}_m(f(\beta^i))\}_{i=0}^\infty \text{ has period } p^m - 1 \right\}.$$

Using Propositions 3.5 and 3.6, we obtain that

$$(3.7) \quad |\mathcal{P}_D^1| = p^2 \left(\sum_{l|(p^m-1)} \mu(l) \left\{ p^{m(\lfloor \frac{D}{l} \rfloor - \lfloor \frac{D}{p^2 l} \rfloor)} - p^{m(\lfloor \frac{D}{l} \rfloor - \lfloor \frac{D}{p l} \rfloor)} \right\} \right).$$

By Proposition 3.7, for each $(f(x), u) \in \mathcal{P}_D^1$, the corresponding p -ary sequence $\{\Psi(\mathrm{Tr}_m(f(\beta^i)) + u)\}_{i=0}^\infty$ has period $p(p^m - 1)$. For $(f(x), u) \in \mathcal{P}_D^1$, $0 \leq t \leq (p^m - 1) - 1$, and $0 \leq j \leq p - 1$, let $g(x) = (1 + p)^j(1 - p)^t f(\beta^t x)$ and $v = (1 + p)^j(1 - p)^t u$. Note that $(g(x), v) \in \mathcal{P}_D^1$. Now we prove that, for $0 \leq t \leq (p^m - 1) - 1$ and $0 \leq j \leq$

$p-1$, $(f(x), u) = (g(x), v)$ as elements of $\mathcal{P}_D^1$ if and only if $j = t = 0$. Note that $(f(x), u) = (g(x), v)$ as elements of $\mathcal{P}_D^1$ if and only if the corresponding p -ary sequences $\{\Psi(\text{Tr}_m(f(\beta^i)) + u)\}_{i=0}^\infty$ and $\{\Psi(\text{Tr}_m(g(\beta^i)) + v)\}_{i=0}^\infty$ are equal. Let $\{s_1(i)\}_{i=0}^\infty$ be the p -ary sequence $\{\Psi(\text{Tr}_m(f(\beta^i)) + u)\}_{i=0}^\infty$ and $\{s_2(i)\}_{i=0}^\infty$ be the p -ary sequence $\{\Psi(\text{Tr}_m(g(\beta^i)) + v)\}_{i=0}^\infty$. Therefore $\{s_2(i)\}_{i=0}^\infty$ is the cyclic shift of $\{s_1(i)\}_{i=0}^\infty$ by $t + j(p^m - 1)$ since both sequences have period $p(p^m - 1)$ and, under the notation of the proof of Proposition 3.7, for each $i \geq 0$

$$\begin{aligned} s_2(i) &= r_1(\text{Tr}_m(f(\beta^{i+t})) + u) \ominus (i + t - j)r_0(\text{Tr}_m(f(\beta^{i+t})) + u) \\ &= s_1(i + t + j(p^m - 1)). \end{aligned}$$

For $(f(x), u), (g(x), v) \in \mathcal{P}_D^1$, we say $(f(x), u)$ and $(g(x), v)$ are *cyclically related* if there exist $0 \leq j \leq p-1$ and $0 \leq t \leq (p^m - 1) - 1$ such that $g(x) = (1+p)^j(1-p)^t f(\beta^t x)$ and $v = (1+p)^j(1-p)^t u$. From the arguments above, we observe that cyclically related elements of $\mathcal{P}_D^1$ form an equivalence relation on $\mathcal{P}_D^1$ and each equivalence class has $p(p^m - 1)$ elements.

Let $\overline{\mathcal{P}}_D^1$ be the set of these equivalence classes in $\mathcal{P}_D^1$. Then

$$(3.8) \quad |\overline{\mathcal{P}}_D^1| = \frac{1}{p(p^m - 1)} |\mathcal{P}_D^1|.$$

Let $\tilde{\mathcal{P}}_D^1$ be a full set of representatives of the equivalence classes in $\overline{\mathcal{P}}_D^1$.

The element, i.e., the equivalence class, of $\overline{\mathcal{P}}_D^1$ containing $(f(x), u)$ is denoted by $\overline{(f(x), u)}$. Now we prove the following property of the equivalence relation on $\mathcal{P}_D^1$:

$$(3.9) \quad \begin{aligned} f(x) \in \mathcal{P}_D^1, \quad u \in \mathbb{Z}_{p^2}, \quad 0 \leq j_1 < j_2 \leq p-1 \\ \Rightarrow (f(x), u + j_1 p) \neq (f(x), u + j_2 p). \end{aligned}$$

Assume the contrary and let $(f(x), u + j_2 p) \in \overline{(f(x), u + j_1 p)}$. By definition of the equivalence, there exist integers $0 \leq j \leq p-1$ and $0 \leq t \leq (p^m - 1) - 1$ such that

$$(3.10) \quad f(x) = (1 + (j - t)p) f(\beta^t x)$$

and

$$(3.11) \quad u + j_2 p = (1 + (j - t)p) (u + j_1 p).$$

As $\rho(f(x)) \neq 0$, there exists a coefficient f_s of x^s in $f(x)$ with $\rho(f_s) \neq 0$. From (3.10) we obtain that

$$(3.12) \quad f_s = (1 + (j - t)p) \beta^{ts} f_s.$$

Let $f_s = a_0 + pa_1$ with $a_0, a_1 \in \Gamma_m$. Then using (3.12) we get

$$\rho(a_0) = \rho(a_0) \rho(\beta^{ts}) \quad \text{and} \quad \rho(a_1) = \rho((j - t)a_0 + a_1) \rho(\beta^{ts}).$$

As $\rho(a_0) \neq 0$ we have $\rho(\beta^{ts}) = 1$ and

$$(3.13) \quad \rho(a_1) = \rho((j - t)a_0 + a_1).$$

Using $\rho(a_0) \neq 0$ and (3.13) we obtain that $(j - t) \equiv 0 \pmod{p}$. Therefore from (3.11) we get a contradiction.

Now we introduce a new relation on $\mathcal{P}_D^1$: we say that $(f(x), u)$ and $(g(x), v)$ are related in the new sense if there exist $0 \leq j, k \leq p-1$, and $0 \leq t \leq (p^m-1)-1$ such that

$$(3.14) \quad \begin{aligned} g(x) &= (1+p)^j(1-p)^t f(\beta^t x), \\ v &= (1+p)^j(1-p)^t u + kp. \end{aligned}$$

It is easy to observe that (3.14) also gives an equivalence relation on $\mathcal{P}_D^1$, and the equivalence relation obtained by the cyclically related elements is finer than the one obtained by (3.14). Let $\tilde{\mathcal{P}}_D^1$ be a full set of representatives of the new equivalence relation. We have $|\tilde{\mathcal{P}}_D^1| = \frac{|\mathcal{P}_D^1|}{p}$. Moreover we assume, without loss of generality, that the elements of $\tilde{\mathcal{P}}_D^1$ are of the form $(f(x), u)$ with $u \in \{0, 1, \dots, p-1\} \subseteq \mathbb{Z}_{p^2}$ and $\hat{\mathcal{P}}_D^1 \subseteq \tilde{\mathcal{P}}_D^1$.

Let $\mathcal{F}_D^1 \subseteq \mathcal{C}_D^1$ be the chain of families of p -ary sequences defined as

$$\mathcal{F}_D^1 = \{ \{ \Psi(\text{Tr}_m(f(\beta^i)) + u) \}_{i=0}^\infty : (f(x), u) \in \hat{\mathcal{P}}_D^1 \}$$

and

$$\mathcal{C}_D^1 = \{ \{ \Psi(\text{Tr}_m(f(\beta^i)) + u) \}_{i=0}^\infty : (f(x), u) \in \tilde{\mathcal{P}}_D^1 \}.$$

THEOREM 3.8. *The families $\mathcal{F}_D^1$ and $\mathcal{C}_D^1$ have the following properties:*

- (i) *The period of each sequence in $\mathcal{C}_D^1$ (and hence in $\mathcal{F}_D^1$) is $p(p^m-1)$.*
- (ii) *The sequences in $\mathcal{C}_D^1$ (and hence in $\mathcal{F}_D^1$) are pairwise cyclically distinct.*
- (iii) *$|\mathcal{F}_D^1| = \frac{1}{p^m-1} \sum_{l|(p^m-1)} \mu(l) \{ p^{m(\lfloor D/l \rfloor - \lfloor D/p^2 l \rfloor)} - p^{m(\lfloor D/l \rfloor - \lfloor D/pl \rfloor)} \}$ and $|\mathcal{C}_D^1| = p|\mathcal{F}_D^1|$, where $\mu(\cdot)$ is the Möbius function.*
- (iv) *For the maximal nontrivial correlation $\theta_{\max}$ of $\mathcal{F}_D^1$, we have*

$$(3.15) \quad \theta_{\max} \leq \frac{1}{p-1} p^{l_D+1} \left\lfloor \frac{p^{h_D} \frac{p^2-p}{2} (D-1) \lfloor 2p^{\frac{m}{2}-h_D} \rfloor}{p^{l_D+1}} \right\rfloor + p,$$

where l_D and h_D are as in Definition 2.9.

Proof. As $\tilde{\mathcal{P}}_D^1 \subseteq \mathcal{P}_D^1$, by Proposition 3.7, each sequence in $\mathcal{C}_D^1$ has period $p(p^m-1)$.

Now we prove items (ii) and (iii) together. Let $(f(x), u) \in \tilde{\mathcal{P}}_D^1$ and $\{s(i)\}_{i=0}^\infty$ be the p -ary sequence $\{\Psi(\text{Tr}_m(f(\beta^i)) + u)\}_{i=0}^\infty$. Assume that $0 \leq j \leq p-1$ and $0 \leq t \leq (p^m-1)-1$ are integers such that the p -ary sequence $\{s(i+j(p^m-1)+t)\}_{i=0}^\infty$ is in $\mathcal{C}_D^1$. Let $(g(x), u_2) \in \tilde{\mathcal{P}}_D^1$ such that the p -ary sequence $\{\Psi(\text{Tr}_m(g(\beta^i)) + u_2)\}_{i=0}^\infty$ is $\{s(i+j(p^m-1)+t)\}_{i=0}^\infty$. Let $h(x) = (1+p)^j(1-p)^t f(\beta^t x)$ and $u_1 = u(1+p)^j(1-p)^t \in \mathbb{Z}_{p^2}$. Note that $\overline{(h(x), u_1)} = \overline{(f(x), u)}$ and hence $(h(x), u_1) \notin \tilde{\mathcal{P}}_D^1$ if either $j \neq 0$ or $t \neq 0$. Let $\{s_1(i)\}_{i=0}^\infty$ be the p -ary sequence $\{\Psi(\text{Tr}_m(h(\beta^i)) + u_1)\}_{i=0}^\infty$ and $\{s_2(i)\}_{i=0}^\infty$ be the p -ary sequence $\{\Psi(\text{Tr}_m(g(\beta^i)) + u_2)\}_{i=0}^\infty$. From the proof of Proposition 3.7 we observe that $s_1(i) = s_2(i)$ for each $i \geq 0$. Then for each $i \geq 0$ we have

$$(3.16) \quad \text{Tr}_m(h(\beta^i)) + u_1 = \text{Tr}_m(g(\beta^i)) + u_2$$

and hence

$$\rho(u_1) + \text{tr}_m(\rho(h)(\omega^i)) = \rho(u_2) + \text{tr}_m(\rho(g)(\omega^i)).$$

As $h(x), g(x) \in S(D)$, using Lemmas 2.5 and 2.3 we obtain that $h(x) = g(x)$ and $\rho(u_1) = \rho(u_2)$. Also using (3.16) we obtain that $u_1 = u_2$ and hence $(h(x), u_1) =$

$(g(x), u_2)$. This completes the proof of item (ii). We complete the proof of item (iii) using item (i) and Propositions 3.5 and 3.6.

It remains to prove item (iv). Assume that $(f_1(x), u_1), (f_2(x), u_2) \in \widehat{\mathcal{P}}_D^1$, and let the corresponding p -ary sequences be $\{s_1(i)\}_{i=0}^\infty = \{\Psi(\text{Tr}_m(f_1(\beta^i)) + u_1)\}_{i=0}^\infty$ and $\{s_2(i)\}_{i=0}^\infty = \{\Psi(\text{Tr}_m(f_2(\beta^i)) + u_2)\}_{i=0}^\infty$. We consider two cases separately.

Case 1. Correlation at $0 < \tau \leq p(p^m - 1) - 1$. Let $\tau = t + j(p^m - 1)$, where $0 \leq t \leq (p^m - 1) - 1$ and $0 \leq j \leq p - 1$. Let $f_3(x) = (1 + p)^j(1 - p)^t f_1(\beta^t x)$, $u_3 = (1 + p)^j(1 - p)^t u_1$, $f(x) = f_3(x) - f_2(x) \in S(D)$, and $u = u_3 - u_2$.

Assume first that $f(x) \neq 0$. Let

$$(3.17) \quad \mathbf{y} = \Psi(\text{Tr}_m(f(\beta^0)) + u, \text{Tr}_m(f(\beta^1)) + u, \dots, \text{Tr}_m(f(\beta^{(p^m-1)-1})) + u).$$

Let $\theta_1(\cdot)$ be the exponential sum function on $\mathbb{F}_p^{p(p^m-1)}$ defined in [L-S, section 3]. The correlation between $\{s_1(i)\}_{i=0}^\infty$ and $\{s_2(i)\}_{i=0}^\infty$ at shift $(t + j(p^m - 1))$ is given by (cf. [L-S, Theorem 3.1])

$$(3.18) \quad \theta_1(\mathbf{y}) = \sum_{l=0}^{p-1} \sum_{x \in \Gamma_m \setminus \{0\}} e^{2\pi i \frac{(1+lp)(\text{Tr}_m(f(x)) + u)}{p^2}}.$$

Next we assume that $f(x) = 0$. Let $u = r_0(u) + pr_1(u)$ with $r_0(u), r_1(u) \in \{0, 1, \dots, p-1\}$. Using (3.9) we obtain that $r_0(u) \neq 0$. Then the correlation between $\{s_1(i)\}_{i=0}^\infty$ and $\{s_2(i)\}_{i=0}^\infty$ at shift $(t + j(p^m - 1))$ is

$$\sum_{l=0}^{p-1} \sum_{x \in \Gamma_m \setminus \{0\}} e^{2\pi i \frac{(1+lp)u}{p^2}} = (p^m - 1)e^{2\pi i \frac{r_0(u)}{p^2}} \sum_{l=0}^{p-1} e^{2\pi i \frac{lr_0(u) + r_1(u)}{p}} = 0.$$

Case 2. Correlation at $\tau = 0$. In this case we have $(f_1(x), u_1) \neq (f_2(x), u_2)$. Let $f(x) = f_1(x) - f_2(x) \in S(D)$ and $u = u_1 - u_2$. Assume first that $f_1(x) \neq f_2(x)$. The correlation in this subcase is also given by the same formula in (3.18).

Next we assume that $f_1(x) = f_2(x)$. Then $\rho(u) \neq 0$ and we obtain that the correlation is 0 as in Case 1.

Therefore in order to complete the proof of item (iv), it is enough to prove that for each $f(x) \in S(D) \setminus \{0\}$ and $u \in \mathbb{Z}_{p^2}$, the absolute value of $\theta_1(\mathbf{y})$ given in (3.18) is bounded from above by the value on the right-hand side of (3.15).

Let $f(x) \in S(D) \setminus \{0\}$ and $u \in \mathbb{Z}_{p^2}$. For $0 \leq c \leq (p-1)$, let

$$(3.19) \quad \phi_c(f, u) = \sum_{l=0}^{p-1} \sum_{x \in \Gamma_m} e^{2\pi i \frac{(c+lp)(\text{Tr}_m(f(x)) + u)}{p^2}}.$$

For $1 \leq c \leq (p-1)$ and $0 \leq l \leq p-1$, let $0 \leq l_{c-1} \leq p-1$ be the integer such that $cl_{c-1} \equiv l \pmod{p}$. Then

$$(3.20) \quad (c + lp)(\text{Tr}_m(f(x)) + u) = (c + cl_{c-1}p)(\text{Tr}_m(f(x)) + u)$$

for $1 \leq c \leq (p-1)$ and $x \in \Gamma_m$. For $1 \leq c \leq (p-1)$, as c is both invertible in $\mathbb{F}_p$ and in Γ_m , using (3.19) and (3.20) we obtain

$$(3.21) \quad \phi_c(f, u) = \phi_1(f, u).$$

By (3.19) and (3.21), we have

$$\sum_{a \in \mathbb{Z}_{p^2}} \sum_{x \in \Gamma_m} e^{2\pi i \frac{a(\text{Tr}_m(f(x)) + u)}{p^2}} = \sum_{c=0}^{p-1} \phi_c(f, u) = \phi_0(f, u) + (p-1)\phi_1(f, u).$$

Hence

$$(p-1)\phi_1(f, u) = \sum_{a \in \mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2}} \sum_{x \in \Gamma_m} e^{2\pi i \frac{a(\text{Tr}_m(f(x)) + u)}{p^2}}.$$

Using Theorem 2.7, as $f(x) \in S(D) \setminus \{0\}$, we have

$$(3.22) \quad |\phi_1(f, u)| \leq \frac{1}{p-1} p^{l_D+1} \left\lfloor \frac{p^{h_D} \frac{p^2-p}{2} (D-1) \lfloor 2p^{\frac{m}{2}-h_D} \rfloor}{p^{l_D+1}} \right\rfloor,$$

where l_D and h_D are as in Definition 2.9. By definition of $\theta_1(\mathbf{y})$ and $\phi_1(f, u)$, we also have

$$(3.23) \quad |\theta_1(\mathbf{y}) - \phi_1(f, u)| = \left| \sum_{l=0}^{p-1} e^{2\pi i \frac{(1+lp)(\text{Tr}_m(f(0)) + u)}{p^2}} \right| \leq p.$$

Combining (3.22) and (3.23) we complete the proof. $\square$

Remark 3.9. The maximal nontrivial correlation $\theta_{\max}(\mathcal{C}_D^1)$ of $\mathcal{C}_D^1$ is large. In fact even for any subset $S \subseteq \mathcal{C}_D^1$ with $\mathcal{F}_D^1 \subsetneq S$, the maximal nontrivial correlation $\theta_{\max}(S)$ of S is at least $p(p^m - 1)$. Indeed if $\mathcal{F}_D^1 \subsetneq S \subseteq \mathcal{C}_D^1$, then there exist $(f(x), u_1), (f(x), u_2) \in \tilde{\mathcal{P}}_D^1$ with $u_2 - u_1 = jp$ and $1 \leq j \leq p-1$ such that $\{s_1(i)\}_{i=0}^\infty = \{\Psi(\text{Tr}_m(f(\beta^i)) + u_1)\}_{i=0}^\infty$ and $\{s_2(i)\}_{i=0}^\infty = \{\Psi(\text{Tr}_m(f(\beta^i)) + u_2)\}_{i=0}^\infty$ are two cyclically distinct p -ary sequences in S . Then the modulus of the correlation between $\{s_1(i)\}_{i=0}^\infty$ and $\{s_2(i)\}_{i=0}^\infty$ at shift 0 is

$$\left| \sum_{l=0}^{p-1} \sum_{x \in \Gamma_m \setminus \{0\}} e^{2\pi i \frac{(1+lp)jp}{p^2}} \right| = (p^m - 1) \left| e^{2\pi i \frac{j}{p}} \right| \cdot \left| \sum_{l=0}^{p-1} e^{2\pi i \frac{lj}{p}} \right| = p(p^m - 1).$$

Remark 3.10. For $p = 2$, from $\mathcal{F}_D^1$ we retrieve the family of binary sequences $Q(D)$ of [H-K, section 8.8]. Let $\mathcal{F}_D^{1,0}$ be the subfamily of $\mathcal{F}_D^1$ defined as

$$\mathcal{F}_D^{1,0} = \{ \{ \Psi(\text{Tr}_m(f(\beta^i))) \}_{i=0}^\infty : (f(x), 0) \in \hat{\mathcal{P}}_D^1 \}.$$

Note that $\mathcal{F}_D^1$ is larger than $\mathcal{F}_D^{1,0}$ with the same upper bound on the maximal nontrivial correlation. For $p = 2$, from $\mathcal{F}_D^{1,0}$ we obtain the family of binary sequences of [S-K-H].

Let $\mathcal{P}_D^2$ be the subset of $pS(D)_1 \times (\mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2})$ defined as

$$\mathcal{P}_D^2 = \left\{ (pf(x), u) \in pS(D)_1 \times (\mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2}) : \{ \text{Tr}_m(pf(\beta^i)) \}_{i=0}^\infty \text{ has period } p^m - 1 \right\}.$$

Using Proposition 3.6, we obtain that

$$(3.24) \quad |\mathcal{P}_D^2| = (p^2 - p) \sum_{l|(p^m-1)} \mu(l) p^{m(\lfloor \frac{p}{l} \rfloor - \lfloor \frac{p}{pl} \rfloor)},$$

where $\mu(\cdot)$ is the Möbius function.

For $(pf(x), u), (pg(x), v) \in \mathcal{P}_D^2$, we say $(pf(x), u)$ and $(pg(x), v)$ are *cyclically related* if there exist $0 \leq j \leq p-1$ and $0 \leq t \leq (p^m-1)-1$ such that $pg(x) = (1+p)^j(1-p)^t pf(\beta^t x)$ and $v = (1+p)^j(1-p)^t u$. Following the arguments similar to the ones for the case of $\mathcal{P}_D^1$, we observe that cyclically related elements of $\mathcal{P}_D^2$ form an equivalence relation and each equivalence class has $p(p^m-1)$ elements.

Let $\overline{\mathcal{P}}_D^2$ denote the set of equivalence classes in $\mathcal{P}_D^2$. We denote the equivalence class of $(pf(x), u) \in \mathcal{P}_D^2$ as $\overline{(pf(x), u)}$.

Let $(pf(x), u) \in \mathcal{P}_D^2$ be an element with $u = r_0(u) + pr_1(u)$, $r_0(u), r_1(u) \in \{0, 1, \dots, p-1\}$. Let $1 \leq j \leq p-1$ be the integer with $jr_0(u) \equiv 1 \pmod{p}$. Then $(1+p)^j pf(x) = (1+jp)pf(x) = pf(x)$ and $(1+p)^j u = (1+jp)(r_0(u) + pr_1(u)) = u + p$. Therefore we have

$$(3.25) \quad (pf(x), u) \in \mathcal{P}_D^2 \Rightarrow (pf(x), u+p) \in \overline{(pf(x), u)}.$$

From (3.9) and (3.25) we observe a different behavior of the equivalence classes in $\mathcal{P}_D^1$ and $\mathcal{P}_D^2$. Using (3.25) we choose a full set of representatives $\tilde{\mathcal{P}}_D^2$ of the equivalence classes in $\overline{\mathcal{P}}_D^2$ such that

$$\tilde{\mathcal{P}}_D^2 = \{(pf(x), u) \in \mathcal{P}_D^2 : u \in \{1, \dots, p-1\} \subseteq (\mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2})\}.$$

Let $\mathcal{F}_D^2$ be the family of p -ary sequences defined as

$$\mathcal{F}_D^2 = \{\{\Psi(\text{Tr}_m(pf(\beta^i)) + u)\}_{i=0}^\infty : (pf(x), u) \in \tilde{\mathcal{P}}_D^2\}.$$

THEOREM 3.11. *The family $\mathcal{F}_D^2$ has the following properties:*

- (i) *The period of each sequence in $\mathcal{F}_D^2$ is $p(p^m-1)$.*
- (ii) *The sequences in $\mathcal{F}_D^2$ are pairwise cyclically distinct.*
- (iii) $|\mathcal{F}_D^2| = \frac{p-1}{p^m-1} \sum_{l|(p^m-1)} \mu(l) p^{m(\lfloor D/l \rfloor - \lfloor D/pl \rfloor)}$, where $\mu(\cdot)$ is the Möbius function.
- (iv) *For the maximal nontrivial correlation $\theta_{\max}$ of $\mathcal{F}_D^2$, we have*

$$\theta_{\max} \leq \frac{1}{p-1} p^{l_D+1} \left\lfloor \frac{p^{h_D} \frac{p^2-p}{2} (D-1) \lfloor 2p^{\frac{m}{2}-h_D} \rfloor}{p^{l_D+1}} \right\rfloor + p,$$

where l_D and h_D are as in Definition 2.9.

Proof. Item (i) is clear. Next we prove items (ii) and (iii) together. Let $(pf(x), u) \in \tilde{\mathcal{P}}_D^2$ with the corresponding p -ary sequence $\{s(i)\}_{i=0}^\infty$. We proceed as in the proof of Theorem 3.8. Assume that $0 \leq j \leq p-1$, $0 \leq t \leq (p^m-1)-1$ with the corresponding p -ary sequence $\{s_2(i)\}_{i=0}^\infty$ satisfying $s_2(i) = s(i+j(p^m-1)+t)$ for each $i \geq 0$. Let $(pg(x), u_2) \in \tilde{\mathcal{P}}_D^2$ such that the p -ary sequence $\{\Psi(\text{Tr}_m(pg(\beta^i)) + u_2)\}_{i=0}^\infty$ is $\{s_2(i)\}_{i=0}^\infty$. Note that $pf(x) = (1+p)^j(1-p)^t pg(x)$. Let $u_1 = (1+p)^j(1-p)^t u$ and let $\{s_1(i)\}_{i=0}^\infty$ be the corresponding p -ary sequence of $(pf(x), u_1) \in \mathcal{P}_D^2$. If either $j \neq 0$ or $t \neq 0$, then $(pf(x), u_1) \notin \tilde{\mathcal{P}}_D^2$. As in the proof of Theorem 3.8 we have

$$(3.26) \quad \text{Tr}_m(pf(\beta^i) + u_1) = \text{Tr}_m(pg(\beta^i) + u_2)$$

for each $i \geq 0$. Then $\rho(u_1) = \rho(u_2)$ and hence $u_2 = u_1 + kp$, where $0 \leq k \leq p-1$. From (3.26) and Lemma 2.3 we obtain $pf(x) = pg(x) + kp$. By definition of $S(D)$ in (2.5), there is no monomial in $g(x)$ and $f(x)$ of degree zero with a nonzero coefficient. Therefore $k = 0$ and $(pf(x), u_1) = (pg(x), u_2)$, which completes the proof of item (ii). We complete the proof of item (iii) as in the proof of Theorem 3.8.

The proof of item (iv) is similar to the proof of Theorem 3.8 (iv). $\square$

Now we give our main family of the p -ary sequences. Let $\mathcal{F}_D$ be the family of p -ary sequences defined as

$$\mathcal{F}_D = \mathcal{F}_D^1 \cup \mathcal{F}_D^2.$$

THEOREM 3.12. *The family $\mathcal{F}_D$ has the following properties:*

- (i) *The period of each sequence in $\mathcal{F}_D$ is $p(p^m - 1)$.*
- (ii) *The sequences in $\mathcal{F}_D$ are pairwise cyclically distinct.*
- (iii)

$$|\mathcal{F}_D| = \frac{1}{p^m - 1} \sum_{l|(p^m - 1)} \mu(l) p^{m(\lfloor \frac{D}{l} \rfloor - \lfloor \frac{D}{p^2 l} \rfloor)} \\ + \frac{p - 2}{p^m - 1} \sum_{l|(p^m - 1)} \mu(l) p^{m(\lfloor \frac{D}{l} \rfloor - \lfloor \frac{D}{p l} \rfloor)},$$

where $\mu(\cdot)$ is the Möbius function.

- (iv) *For the maximal nontrivial correlation $\theta_{\max}$ of $\mathcal{F}_D$, we have*

$$\theta_{\max} \leq \frac{1}{p - 1} p^{l_D + 1} \left\lceil \frac{p^{h_D} \frac{p^2 - p}{2} (D - 1) \lfloor 2p^{\frac{m}{2} - h_D} \rfloor}{p^{l_D + 1}} \right\rceil + p,$$

where l_D and h_D are as in Definition 2.9.

Proof. Item (i) is clear. Note that any two distinct sequences from $\mathcal{F}_D^1$ (or from $\mathcal{F}_D^2$) are cyclically distinct. Moreover, if $(f(x), u) \in \widehat{\mathcal{P}}_D^1$, $(pg(x), v) \in \widetilde{\mathcal{P}}_D^2$ and $0 \leq j \leq p - 1$, $0 \leq t \leq (p^m - 1) - 1$, then

$$\rho((1 + p)^j (1 - p)^t f(\beta^t x)) \neq 0 \text{ and } \rho((1 + p)^j (1 - p)^t pg(\beta^t x)) = 0.$$

We complete the proof of item (ii) using Lemmas 2.3 and 2.5 as in the proof of Theorem 3.8 (ii).

Now we prove item (iii). Let $\{s_1(i)\}_{i=0}^\infty$ and $\{s_2(i)\}_{i=0}^\infty$ be the p -ary sequences of $\mathcal{F}_D^1$ and $\mathcal{F}_D^2$ obtained from $(f(x), u) \in \widehat{\mathcal{P}}_D^1$ and $(pg(x), v) \in \widetilde{\mathcal{P}}_D^2$, respectively. If $s_1(i) = s_2(i)$ for each $i \geq 0$, then

$$(3.27) \quad r_0(\text{Tr}_m(f(\beta^i)) + u) = r_0(p \text{Tr}_m(g(\beta^i)) + v).$$

Using (3.27) and Lemmas 2.3 and 2.5 we obtain that $f(x) = 0$, which is a contradiction.

We prove item (iv) using the methods of the proof of Theorem 3.8 (iv). $\square$

Note that $\mathcal{F}_D$ is larger than $\mathcal{F}_D^1$ while the sequences in them have the same period and the same upper bound for their maximal nontrivial correlation in Theorems 3.8 and 3.12.

Example 3.13. In this example we assume that $p = 2$. We recall that the subfamily $\mathcal{F}_D^{1,0}$ of $\mathcal{F}_D^1$ given in Remark 3.10 corresponds to the family of sequences in [S-K-H] and $\mathcal{F}_D^1$ corresponds to the family of sequences in [H-K, section 8.8]. For $\mathcal{F}_D^{1,0}$, $\mathcal{F}_D^1$, and $\mathcal{F}_D$, we have the same period length and the same upper bounds for their maximal nontrivial correlation. The size of the family $\mathcal{F}_D^1$ is twice the size of the family $\mathcal{F}_D^{1,0}$. In [S-K-H, Table 2], for small values of D , the upper bounds for the maximal nontrivial correlation of $\mathcal{F}_D^{1,0}$ are given. In Table 1, we compare the family sizes of $\mathcal{F}_D^1$ and $\mathcal{F}_D$ for small values of D and m .

TABLE 1
Comparison of family sizes of $\mathcal{F}_D^1$ and $\mathcal{F}_D$ for $p = 2$.

m	D	$ \mathcal{F}_D^1 $	$ \mathcal{F}_D $
3	2	8	9
5	2	32	33
7	2	128	129
5	3	1024	1057
7	3	16384	16513
5	5	32768	33825
7	5	2097152	2113665

TABLE 2
Comparison of a family for $p = 3$ with some families for $p = 2$ from Theorem 3.12.

p	D	m	$L = \text{period}$	$\log S / \log L$	$\theta_{\max}^* / \sqrt{L}$
3	8	9	59049	6.30003...	12.06820...
2	8	21	4194302	4.77272...	9.84472...
2	9	17	262142	5.66667...	11.25394...
2	10	15	65534	6.56252...	12.63300...
2	11	13	16382	7.42867...	13.76646...

Note that the family sizes of the binary sequences in [U-S] are about half of the family sizes of the binary sequences obtained from Theorem 3.12 for $D = 2$. For $D = 3$, the periods of the binary sequence families match only for one of the families in [B], which is the family noted as twice shortened Delsarte–Goethals codes in the table of [B]. For that family, the sizes are similar while the maximal nontrivial correlation upper bound is better for the sequences from Theorem 3.12. For $D \geq 3$ and $D \geq 5$, the binary sequence families from Theorem 3.12 are much larger than the ones from [U-S] and [B], respectively.

Example 3.14. In this example we compare a sequence family for $p = 3$ with the relevant sequence families for $p = 2$, where the sequences are obtained using Theorem 3.12. For $p = 3$, $D = 8$, and $m = 9$, we get a sequence family of size S and of period $L = 59049$ such that

$$\frac{\log S}{\log L} = 6.30003\dots, \quad \frac{\theta_{\max}^*}{\sqrt{L}} \leq 12.06820\dots$$

In Table 2, S denotes the family size and $\theta_{\max}^*$ denotes the upper bound on the maximal nontrivial correlation $\theta_{\max}$ of the corresponding sequence families from Theorem 3.12. For $p = 2$ and D in Table 2, m is chosen to be the smallest positive odd integer such that the corresponding family size is at least the size of the sequence family for $p = 3$. We observe that the parameters of the sequence family for $p = 3$ are comparable to the parameters of the other sequence families in Table 2. In particular there is no sequence family for $p = 2$ in Table 2 such that $\log S / \log L$ is larger than that of $p = 3$ and $\theta_{\max}^* / \sqrt{L}$ is smaller than that of $p = 3$ simultaneously.

Remark 3.15. Let n be a positive divisor of $p^m - 1$ and let $\zeta = \beta^{\frac{p^m - 1}{n}}$ be a primitive n th root of unity. Changing β with ζ and putting a suitable condition on D , we obtain p -ary codes of length pn and p -ary sequence families of period pn in an analogous way. Moreover, using the methods of this paper, we can also estimate the minimum distance of such codes and the maximum nontrivial correlation of such sequence families.

4. Conclusion. In this paper, a family of codes over $\mathbb{F}_p$ and several families of pairwise cyclically distinct p -ary sequences of period $p(p^m - 1)$ of low correlation have been constructed as the Gray image and generalized Nechaev–Gray images, respectively, of some trace codes over $\mathbb{Z}_{p^2}$. The $\mathbb{F}_p$ -codes, mostly nonlinear, are of length p^{m+1} and size $p^2 \cdot p^{m(D - \lfloor D/p^2 \rfloor)}$, where $1 \leq D \leq p^{m/2}$. A lower bound for their minimum distance is obtained through the bound of [L-O]. The sequences compare favorably with certain known p -ary sequences of period $p^m - 1$ (cf. [H-K, Table 4]). In fact, even in the case $p = 2$, one of these families is slightly larger than the family $Q(D)$ of [H-K, section 8.8], while they share the same period and the same bound for the maximum nontrivial correlation.

Acknowledgments. The authors are thankful to the anonymous referees and the editor for their helpful comments.

REFERENCES

- [B] A. BARG, *On Small Families of Sequences with Low Periodic Correlation*, Lecture Notes in Comput. Sci. 781, Springer-Verlag, Berlin, 1994, pp. 154–158.
- [C] C. CARLET, $\mathbb{Z}_{2^k}$ -linear codes, IEEE Trans. Inform. Theory, 44 (1998), pp. 1543–1547.
- [C-H] I. CONSTANTINESCU AND W. HEISE, *A metric for codes over residue class rings of integers*, Probl. Inf. Transm., 33 (1997), pp. 208–213.
- [G-S] M. GREFERATH AND S. E. SCHMIDT, *Gray isometries for finite chain rings and a non-linear ternary $(36, 3^{12}, 15)$ code*, IEEE Trans. Inform. Theory, 45 (1999), pp. 2522–2524.
- [H-K] T. HELLESETH AND P. V. KUMAR, *Sequences with low correlation*, in Handbook of Coding Theory, Vol. I, II, V. S. Pless and W. C. Huffman, eds., North-Holland, Amsterdam, 1998, pp. 1765–1853.
- [K-H-C] P. V. KUMAR, T. HELLESETH, AND A. R. CALDERBANK, *An upper bound for Weil exponential sums over Galois rings with applications*, IEEE Trans. Inform. Theory, 41 (1995), pp. 456–468.
- [H-K-M-S] T. HELLESETH, P. V. KUMAR, O. MORENO, AND A. G. SHANBHAG, *Improved estimates via exponential sums for the minimum distance of $\mathbb{Z}_4$ -linear trace codes*, IEEE Trans. Inform. Theory, 42 (1996), pp. 1212–1216.
- [N] A. A. NECHAEV, *The Kerdock code in a cyclic form*, Discrete Math. Appl., 1 (1991), pp. 365–384.
- [L-N] R. LIDL AND H. NIEDERREITER, *Finite Fields*, Cambridge University Press, Cambridge, UK, 1997.
- [L-B] S. LING AND J. T. BLACKFORD, $\mathbb{Z}_{p^{k+1}}$ -linear codes, IEEE Trans. Inform. Theory, 48 (2002), pp. 2592–2605.
- [L-O] S. LING AND F. ÖZBUDAK, *An improvement on the bounds of Weil exponential sums over Galois rings with some application*, IEEE Trans. Inform. Theory, 50 (2004), pp. 2529–2539.
- [L-S] S. LING AND P. SOLÉ, *Nonlinear p -ary sequences*, Appl. Algebra Engrg. Comm. Comput., 14 (2003), pp. 117–125.
- [U-S] P. UDAYA AND M. U. SIDDIQI, *Optimal biphasic sequences with large linear complexity derived from sequences over $\mathbb{Z}_4$* , IEEE Trans. Inform. Theory, 42 (1996), pp. 206–217.
- [S-K-H] A. G. SHANBHAG, P. V. KUMAR, AND T. HELLESETH, *Improved binary codes and sequence families from $\mathbb{Z}_4$ -linear codes*, IEEE Trans. Inform. Theory, 42 (1996), pp. 1582–1587.