Almost p-Ary Perfect Sequences

Yeow Meng Chee[1], Yin Tan[1,⋆], and Yue Zhou[2,⋆⋆]

[1] Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, 637371 Singapore
ymchee@ntu.edu.sg, itanyinmath@gmail.com

[2] Department of Mathematics, Otto-von-Guericke-University Magdeburg, 39106 Magdeburg, Germany
yue.zhou@st.ovgu.de

Abstract. A sequence $\mathbf{a} = (a_0, a_1, a_2, \cdots, a_n)$ is said to be an almost p-ary sequence of period $n+1$ if $a_0 = 0$ and $a_i = \zeta_p^{b_i}$ for $1 \le i \le n$, where ζ_p is a primitive p-th root of unity and $b_i \in \{0, 1, \cdots, p-1\}$. Such a sequence $\mathbf{a}$ is called perfect if all its out-of-phase autocorrelation coefficients are zero; and is called nearly perfect if its out-of-phase autocorrelation coefficients are all 1, or are all -1. In this paper, on the one hand, we construct almost p-ary perfect and nearly perfect sequences; on the other hand, we present results to show they do not exist with certain periods. It is shown that almost p-ary perfect sequences correspond to certain relative difference sets, and almost p-ary nearly perfect sequences correspond to certain direct product difference sets. Finally, two tables of the existence status of such sequences with period less than 100 are given.

Keywords: almost p-ary sequences, almost p-ary perfect sequences, almost p-ary nearly perfect sequences, relative difference set, direct product difference set.

1 Introduction

Let $\mathbf{a} = (a_0, a_1, a_2, \cdots, a_n)$ be a complex sequence of period $n+1$. We call $\mathbf{a}$ an *m-ary sequence* if $a_i = \zeta_m^{b_i}$, where ζ_m is a primitive m-th root of unity and $b_i \in \{0, 1, \cdots, m-1\}$ for $0 \le i \le n$. In particular, the sequence $\mathbf{a}$ is called an *almost m-ary sequence if* $a_0 = 0$. For an (almost) m-ary sequence $\mathbf{a}$ with period $n+1$, the *autocorrelation coefficients* of $\mathbf{a}$ are the elements in the set

$$\{C_t(\mathbf{a}) = \sum_{i=0}^{n} a_i \overline{a_{i+t}} : 0 \le t \le n\},$$

⋆ Research of Yeow Meng Chee and Yin Tan is supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03 and by the Nanyang Technological University under Research Grant M58110040.

⋆⋆ Research of Yue Zhou is partially supported by China Scholarship Council.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 399–415, 2010.
© Springer-Verlag Berlin Heidelberg 2010

where $\bar{\cdot}$ is the complex conjugate and all subscripts are computed modulo $n+1$. For all $t \not\equiv 0 \mod (n+1)$, the $C_t(\mathbf{a})'$s are called *out-of-phase* autocorrelation coefficients, and *in-phase* autocorrelation coefficients otherwise.

Motivated by applications in engineering, sequences with small out-of-phase coefficients are of particular interests. Usually, the complex sequence $\mathbf{a}$ is expected to have a *two-level autocorrelation function*, i.e. all out-of-phase autocorrelation coefficients are a constant γ. For an almost m-ary sequence $\mathbf{a}$, we call $\mathbf{a}$ *perfect* if it has a two-level autocorrelation function and $\gamma = 0$. Moreover, we call $\mathbf{a}$ *nearly perfect* if out-of-phase autocorrelation coefficients γ all satisfy $\gamma = 1$, or all they satisfy $\gamma = -1$. We refer to [7] for a well-rounded survey on perfect binary sequences, to [9] for results of perfect and nearly perfect p-ary sequence, where p is an odd prime. In the following we briefly introduce the relationship between (almost) binary (with entries ± 1) perfect sequences and (Conference) Hadamard matrices.

A matrix H with entries ± 1 and order v is called a *Hadamard matrix* if $HH^T = vI$; and a matrix C with entries $0, \pm 1$ and order v is called a *Conference matrix* if $CC^T = (v-1)I$, where I is the identity matrix. It is well known that perfect binary (with entries ± 1) sequences of period v are equivalent to cyclic difference sets (see [7, Section 2]). In particular, when $v \equiv 0 \mod 4$, the perfect binary sequences are equivalent to circulant Hadamard matrices, or cyclic Hadamard difference sets (see [12, Section 1.1]). More precisely, let $\mathbf{a} = (a_0, a_1, \ldots, a_{v-1})$ be a binary perfect sequence of period v. Let $H = (h_{i,j})_{i,j=0}^{v-1}$ be a circulant matrix (H is called *circulant* if $h_{i+1,j+1} = h_{i,j}$ for all i, j) defined by $h_{0,j} = a_j$ for $j \in \mathbb{Z}_v$, then H is a circulant Hadamard matrix of order v. Similarly, let $\mathbf{a} = (a_0, a_1, \ldots, a_{v-1})$ be an almost binary perfect sequence, i.e. $a_0 = 0$ and $a_i = \pm 1$ for $1 \leq i \leq v-1$. Then the circulant matrix $C = (h_{i,j})_{i,j=0}^{v-1}$ defined by $h_{0,j} = a_j$ for $j \in \mathbb{Z}_v$ is a circulant Conference matrix. The famous circulant Hadamard matrices conjecture is that there do not exist circulant Hadamard matrices if $v > 4$. In contrast to this still open problem, an elegant and elementary proof in [13] shows that there do not exist circulant Conference matrices: It seems that the mathematical behavior of binary perfect sequences and almost binary perfect sequences are quite different, which is one motivation of our paper. In this paper, we study the properties of general almost p-ary perfect sequences, where p is a prime. It turns out that almost p-ary perfect sequences of period $n+1$ are equivalent to $(n+1, p, n, (n-1)/p)$ relative difference sets in $\mathbb{Z}_{n+1} \times \mathbb{Z}_p$ relative to $\mathbb{Z}_p$ (Theorem 1).

The lack of examples of almost p-ary perfect sequences motivates our research in almost p-ary nearly perfect sequences. It is shown that periodic almost p-ary nearly perfect sequences correspond to certain direct product difference sets (Theorem 6).

This paper is organized as follows. In Section 2, we give necessary definitions and results. The discussions about almost p-ary perfect and nearly perfect sequences are given in Section 3 and 4 respectively. In Appendix, we give two tables of the existence status of almost p-ary perfect and nearly perfect sequences

with period less than 100. Our results generalize those about perfect and nearly perfect p-ary sequences which have been done by Ma and Ng in [9].

2 Preliminaries

In this section, we give necessary definitions and results used in this paper.

2.1 Relative Difference Sets, Characters and Group Rings

To facilitate the study of difference sets by using group rings and character theory, we use the multiplicatively written group $G = \langle g | g^n = 1 \rangle$ instead of the additively written group $\mathbb{Z}_n$. We refer to [10] for the basic facts of group rings and [8] for character theory on finite fields. In the following, we identify a subset A of G with a group ring element $\sum_{a \in A} a$ of $\mathbb{C}[G]$ and we still denote it by A. For any integer t, we define $A^{(t)} = \sum_{a \in A} a^t$. For a group ring element $A = \sum_{g \in G} a_g g \in \mathbb{C}[G]$, we define $|A| = \sum_{g \in G} a_g$.

Let G be an abelian group of order mn and let N be a subgroup of order n. A k-subset R of G is said to be an (m, n, k, λ) *relative difference set* (RDS) in G relative to N if all elements not in N can be represented exactly λ times as the form

$$r_1 r_2^{-1},\ r_1, r_2 \in R \text{ and } r_1 \neq r_2,$$

and no element in N can be represented as this form. In the language of group rings, R is an (m, n, k, λ) relative difference set in G relative to N if and only if

$$RR^{(-1)} = k + \lambda(G - N).$$

A k-subset D of a group G is said to be a (v, k, λ) *difference set* (DS) if all non-identity elements of G can be represented exactly λ times as the form

$$d_1 d_2^{-1},\ d_1, d_2 \in D, d_1 \neq d_2.$$

We refer to [2] for details on difference sets. Relative difference sets can be regarded as the "lifting" of difference sets.

Result 1. *[11, Lemma 1.1.12] Let R be an abelian (m, n, k, λ)-RDS in G relative to N, where N is a subgroup of G of order n. Let L be a subgroup of N of order l and let $\rho : G \to G/L$ be the natural epimorphism. Then $\rho(R)$ is an $(m, \frac{n}{l}, k, l\lambda)$-RDS in G/L relative to N/L. Moreover, if $L = N$, then $\rho(R)$ is an $(m, k, n\lambda)$ difference set in G/L.*

The following result provides a useful method to prove a k-subset R of G to be an (m, n, k, λ)-RDS.

Result 2. *Let G be an abelian group of order mn and let N be a subgroup of G of order n. A k-subset R is an (m, n, k, λ)-RDS in G relative to N if and only if*

$$\chi(R)\overline{\chi(R)} = \begin{cases} n & \text{if } \chi \text{ is not principal on } N, \\ k - n\lambda & \text{if } \chi \text{ is principal on } N \text{ but nonprincipal on } G, \\ k^2 & \text{if } \chi \text{ is principal on } G, \end{cases} \tag{1}$$

where χ is a character of G.

A prime p is said to be *self-conjugate* modulo w if $p^j \equiv -1 \mod (w')$ for some j, where w' is the maximal p-free part of w, i.e. the maximal factor of w which is relative prime to p. A composite integer m is said to be self-conjugate modulo w if every prime divisor of m is self-conjugate modulo w. The self-conjugate condition is quite useful in determining the existence of RDSs. The following two results are used later; see [11].

Result 3. *Let p be a prime and ζ_w be a primitive w-th root of unity in $\mathbb{C}$.*

1. *If $w = p^e$, then the decomposition of the ideal (p) into prime ideals is $(p) = (1 - \zeta_w)^{\phi(w)}$.*
2. *If $(w, p) = 1$, then the prime ideal decomposition of the ideal (p) is $(p) = \pi_1 \cdots \pi_g$, where $\pi_i's$ are distinct prime ideals. Furthermore, $g = \phi(w)/f$ where f is the order of p modulo w. The field automorphism $\zeta_w \to \zeta_w^p$ fixes the ideals π_i.*
3. *If $w = p^e w'$ with $(w', p) = 1$, then the prime ideal (p) decomposes as $(p) = (\pi_1 \cdots \pi_g)^{\phi(p^e)}$, where $\pi_i's$ are distinct prime ideals and $g = \phi(w')/f$. If t is an integer not divisible by p and $t \equiv p^s \mod (w')$ for a suitable integer s, then the field automorphism $\zeta_w \to \zeta_w^t$ fixes the ideals π_i.*

2.2 Two Important Lemmas

The following two lemmas are crucial to the proof of our results in Section 3 and 4. They deal with the cases whether the self-conjugate condition is satisfied or not. We record them here for the convenience of the reader.

Lemma 1. *[9] Let q be a prime and α be a positive integer. Let K be an abelian group such that either q does not divide $|K|$ or the Sylow q-subgroup of K is cyclic. Let L be any subgroup of K and $Y \in \mathbb{Z}[K]$ where the coefficients of Y lie between a and b where $a < b$. Suppose*

1. *q is self-conjugate modulo $\exp(K)$;*
2. *$q^r | \chi(Y)\overline{\chi(Y)}$ for all $\chi \notin L^\perp$ and $q^{r+1} \nmid \chi(Y)\overline{\chi(Y)}$ for some $\chi \notin L^\perp$;*
3. *$\chi(Y) \neq 0$ for some $\chi \notin L^\perp \cup Q^\perp$ where $Q = K$ if $q \nmid |K|$ and Q is the subgroup of K of order q otherwise. Here $L^\perp$ denotes the subset of the character group which is non-principal on L.*

Then

1. *if $q \nmid |K|$, r is even and $q^{\frac{r}{2}} \leq b - a$; and*
2. *if Sylow q-subgroup of K is cyclic, $q^{\lfloor \frac{r}{2} \rfloor} \leq 2(b - a)$ when L is a proper subgroup of $|K|$ and $q^{\lfloor \frac{r}{2} \rfloor} \leq b - a$ when $L = K$.*

Lemma 2. *[1] Let $G = \langle \alpha \rangle \times H$ be an abelian group of exponent $v = uw$, where $\mathrm{ord}(\alpha) = u, \exp(H) = w$ and $(u, w) = 1$. Suppose $y \in \mathbb{Z}[G]$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_v)/\mathbb{Q})$ such that*

1. *$\chi(y)\overline{\chi(y)} = n$ for all characters χ of G such that $\chi(\alpha) = \zeta_u$, where n is an integer relative prime to w; and*
2. *σ fixes every prime ideal divisor of $n\mathbb{Z}[\zeta_v]$.*

If $\sigma(\zeta_v) = \zeta_v^t$, *then*

$$y^{(t)} = \pm\beta y + \sum_{i=1}^{r} \langle \alpha^{u/p_i} \rangle x_i,$$

where $\beta \in G, x_1, \cdots, x_r \in \mathbb{Z}[G]$ *and* $p_1, \cdots, p_r$ *are all prime divisors of* u.

Furthermore, if u *is even, then the sign* $\pm$ *can be chosen arbitrarily by choosing appropriate* β.

2.3 Direct Product Difference Sets

We conclude this section by introducing the direct product difference sets. They were first defined in [4], but studied only the case $\lambda_1 = 0, \lambda_2 = 0$. The general definition of direct product difference sets is given in [9].

Let $G = H \times N$, where the order of H and N are m and n respectively. A k-subset R is said to be an $(m, n, k, \lambda_1, \lambda_2, \mu)$ *direct product difference set* (DPDS) in G relative to H and N if

$$r_1 r_2^{-1},\ r_1, r_2 \in R, r_1 \neq r_2$$

represent

1. all non-identity elements in H exactly λ_1 times;
2. all non-identity elements in N exactly λ_2 times;
3. all non-identity elements in $G \backslash H \cup N$ exactly μ times.

In the group ring language, R is an $(m, n, k, \lambda_1, \lambda_2, \mu)$-DPDS in G relative to H and N if and only if

$$RR^{(-1)} = (k - \lambda_1 - \lambda_2 + \mu) + (\lambda_1 - \mu)H + (\lambda_2 - \mu)N + \mu G. \tag{2}$$

3 Almost p-Ary Perfect Sequences

In this section we construct almost p-ary perfect sequences, and prove that they do not exist with certain periods. First we fix some notations which will be frequently used. Let p be a prime and let $G = H \times P$, where $H = \langle h \rangle, P = \langle g \rangle, \mathrm{ord}(h) = n + 1$ and $\mathrm{ord}(g) = p$. Let ζ_p be a primitive p-th root of unity and $\mathbf{a} = \{0, a_1, \cdots, a_n\}$ be an almost p-ary sequence of period $n + 1$, where $a_i = \zeta_p^{b_i}$ with $b_i \in \{0, 1, \cdots, p - 1\}$. For the convenience of expression, we define $a_0 = 0$.

Now we consider the following n-subset R of G

$$R = \{g^{b_i} h^i | i = 1, 2, \cdots, n\}. \tag{3}$$

Obviously,

$$RR^{(-1)} = n + \sum_{t=1}^{n} \sum_{\substack{j=1 \\ j \not\equiv -t \mod (n+1)}}^{n} g^{b_{j+t} - b_j} h^t. \tag{4}$$

Lemma 3. *Let χ be a character of P and extend $\chi : \mathbb{Z}[G] \longrightarrow \mathbb{Q}(\zeta_p)[H]$ to be a ring epimorphism such that $\chi(x) = x$ for all $x \in H$. Then*

$$\chi(R)\chi(R^{(-1)}) = \begin{cases} \sum_{t=0}^{n} C_t(\boldsymbol{a})^{\sigma} h^t & \text{if } \chi \text{ is nonprincipal on } P, \\ 1 + (n-1)H & \text{if } \chi \text{ is principal on } P, \end{cases} \tag{5}$$

where $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and $\sigma(\zeta_p) = \chi(g)$.

Proof. If χ is principal on P, then $\chi(R)\chi(R^{(-1)}) = (H-1)^2 = 1 + (n-1)H$. Otherwise, suppose $\chi(g) = \sigma(\zeta_p)$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, the results follow from (4). □

We remind the reader that $\mathbf{a}$ is an almost p-ary PS of period $n+1$ if its out-of-phase autocorrelation coefficients are all zero and $C_0(\mathbf{a}) = n$.

Theorem 1. *Let $\mathbf{a}$ be an almost p-ary sequence of period $n+1$, then $\mathbf{a}$ is an almost p-ary perfect sequence if and only if R is an $(n+1, p, n, (n-1)/p)$-RDS in G relative to P, i.e.*

$$RR^{(-1)} = n + \frac{n-1}{p}(G - P), \tag{6}$$

where R is defined in (3).

Proof. By Lemma 3, for all characters χ of P,

$$\chi(RR^{(-1)}) = \begin{cases} n & \text{if } \chi \text{ is nonprincipal on } P, \\ 1 + (n-1)H & \text{if } \chi \text{ is principal on } P. \end{cases}$$

Now the result is followed by Result 2. □

By Theorem 1, we get a necessary condition for the existence of almost p-ary PSs with period $n+1$.

Corollary 1. *If there exists an almost p-ary perfect sequence of period $n+1$, then $p \mid n-1$.*

In the following we give an example of almost p-ary PSs from the classical affine difference sets.

Example 1. Let $\mathbb{F} := \mathbb{F}_q$ be the field of order q and $q = w^f$ be a prime power. Let α be a primitive element of the field $\mathbb{K} = \mathbb{F}_{q^2}$ and let G be the multiplicative group of $\mathbb{K}$. Clearly $G \cong \mathbb{Z}_{q^2-1}$. It is well known that the subset

$$D = \{\alpha^i | \mathrm{Tr}_{\mathbb{F}}^{\mathbb{K}}(\alpha^i) = 1\}$$

of $\mathbb{K}$ is a cyclic $(q+1, q-1, q, 1)$-RDS in G relative to N, where $N \leqslant G$ and $N \cong \mathbb{Z}_{q-1}$ (see [11, Theorem 2.2.12]). Let p be a prime divisor of $q-1$ with $\gcd(p, q+1) = 1$ and let $M \leqslant N, M \cong \mathbb{Z}_{\frac{q-1}{p}}$. Let $\rho : G \longrightarrow G/M$ be the natural epimorphism, then $\rho(R)$ is a $(q+1, p, q, \frac{q-1}{p})$-RDS in G/M relative to N/M. It is clear that $G/M \cong \mathbb{Z}_{q+1} \times \mathbb{Z}_p$ and $N/M \cong \mathbb{Z}_p$. By Theorem 1, there exists an almost p-ary PS of period $q+1$ whenever q is a prime power and $p | q-1, \gcd(p, q+1) = 1$.

Next we give several nonexistence results to show that almost p-ary PSs do not exist with certain periods.

Result 4. *[5] Abelian splitting $(n+1, 2, n, (n-1)/2)$-relative difference sets do not exist.*

By Theorem 1, we have the following result.

Theorem 2. *There do not exist almost binary perfect sequences of period $n+1$ for any n.*

Result 5. *[6] Let R be an abelian $(n+1, n-1, n, 1)$-RDS in G relative to N, then n should be a prime power for $n \leq 10,000$.*

Using the technique in [9], we have the following result. Note that $\gcd(p, q) = 1$, where p is a prime divisor of n and q is a prime divisor of $n+1$. We use the notation $p^r \parallel n$ to denote p^r strictly divide n, namely $p^r \mid n$ but $p^{r+1} \nmid n$.

Theorem 3. *Let R be an $(n+1, p, n, \frac{n-1}{p})$-RDS in G relative to P. Assume that there exists a prime divisor $q \neq p$ of n and q is self-conjugate modulo $p \cdot u$, where $u \mid n+1$. Let $q^r \parallel n$, then r is even and $q^{\frac{r}{2}} \leq \frac{n+1}{u}$.*

Proof. Let $\rho : G \to K := G/\langle h^u \rangle$ be the natural epimorphism. By (6),

$$\rho(R)\rho(R^{(-1)}) = n + \frac{n-1}{p}(\frac{n+1}{u}K - \rho(P)).$$

It is clear that the coefficients of $\rho(R)$ lie between 0 and $\frac{n+1}{u}$. Let χ be a nonprincipal character of K, we have

$$\chi(\rho(R))\overline{\chi(\rho(R))} = \begin{cases} n \text{ if } \chi \text{ is nonprincipal on } \rho(P), \\ 1 \text{ if } \chi \text{ is principal on } \rho(P). \end{cases}$$

Now set $L = \rho(P)$ and $Y = \rho(R)$, where L and Y are defined in Lemma 1. It is routine to verify that the conditions in Lemma 1 are satisfied for L and Y here. Therefore we complete the proof. □

The following two results can be easily followed from Theorem 3.

Corollary 2. *Assume that there exists a prime divisor $q \neq p$ of n such that q is self-conjugate modulo $p(n+1)$, then there do not exist $(n+1, p, n, \frac{n-1}{p})$-RDSs in G relative to P. In other words, there do not exist almost p-ary perfect sequences of period $n+1$.*

Corollary 3. *Assume that there exists a prime divisor $q \neq p$ of n such that q is self-conjugate modulo p. If $q^{2s+1} \parallel n$, then there do not exist $(n+1, p, n, \frac{n-1}{p})$-RDSs in G relative to P. In other words, there do not exist almost p-ary perfect sequences of period $n+1$.*

The above results depend on the self-conjugate condition. Usually it is difficult to determine the existence status of almost p-ary PSs if this condition is not satisfied. However, in some cases we can determine whether the almost p-ary PSs exist or not when n is small. We briefly introduce the main idea of this method here. An (m, n, k, λ)-RDS is called *regular* if $k^2 \neq \lambda mn$. Let D be a RDS in G and let t be an integer with $\gcd(t, |G|) = 1$. We call t a *multiplier* of D if $D^{(t)} = Dg$ for some $g \in G$. It is well known that Rg is also a RDS for any $g \in G$. The following result tells us that we may assume R satisfying $R^{(t)} = R$ if R is regular.

Result 6. *[11] Let R be a regular (m, n, k, λ)-RDS and let t be a multiplier of D. Then there exists at least one translate Rg such that $(Rg)^{(t)} = Rg$.*

Let Ω be the set of orbits of G under the group automorphism $x \mapsto x^t$. Since $R^{(t)} = R$, we see that R is the union of elements in Ω, namely

$$R = \bigcup_{\omega \in \Phi} \omega,$$

where $\Phi \subseteq \Omega$. A natural way to construct R is to combine the elements in Ω. On the one hand, if there do not exist a subset Φ of Ω such that $|\bigcup_{\omega\in\Phi} \omega| = |R|$, then clearly R do not exist. On the other hand, to construct R, we may find suitable Φ with $|\bigcup_{\omega\in\Phi} \omega| = |R|$ and verify whether $\bigcup_{\omega\in\Phi} \omega$ is a RDS. Next result gives a way to find multipliers of RDSs.

Theorem 4. *Let R be an $(n+1, p, n, \frac{n-1}{p})$-RDS in $G = H \times P = \langle h\rangle \times \langle g\rangle \cong \mathbb{Z}_{n+1} \times \mathbb{Z}_p$ relative to P, where p is an odd prime. Let $n = p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l}$ be the prime decomposition of n. For $1 \leq i \leq l$, let $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta)/Q)$ defined by $\sigma_i(\zeta) = \zeta^{p_i}$, where ζ is a primitive $(n+1)p$-th root of unity. Assume that $\bigcap_{i=1}^{l} \langle\sigma_i\rangle \neq \{1\}$ and let $\varphi \in \bigcap_{i=1}^{l} \langle\sigma_i\rangle$. If $\varphi(\zeta) = \zeta^{\alpha}$, then α is a multiplier of R.*

Proof. By (6), we have $RR^{(-1)} = n + \frac{n-1}{p}(G - P)$. Let χ be a character of G such that $\chi(g) = \zeta_p$, then $\chi(R)\overline{\chi(R)} = n$. By Result 3, the prime ideal factorization of (n) in $\mathbb{Z}[\zeta_{(n+1)p}]$ is

$$(n) = (p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l}) = \prod_{i=1}^{l} (P_{1,i} \cdots P_{s_i,i})^{r_i},$$

where $s_i = \phi((n+1)p)/f_i$ and $f_i = \mathrm{ord}_{(n+1)p}(p_i)$. By Result 3 (ii) and $\gcd(n, (n+1)p) = 1$, we know that σ_i fixes the prime ideals $P_{j,i}$ for $1 \leq j \leq s_i$. Therefore, φ fixes all prime ideals $P_{j,i}$ for $1 \leq j \leq s_i$ and $1 \leq i \leq l$. By Lemma 2,

$$R^{(\alpha)} = \pm\beta R + Px,$$

where $\beta \in G$ and $x \in \mathbb{Z}[G]$. Let χ_0 be the principal character of G, then

$$n = \chi_0(R^{(\alpha)}) = \chi_0(\pm\beta R + Px) = \pm n + p|x|.$$

It follows that $|x| = 0$ as $\gcd(p, n) = 1$. Next we show that x must be 0. Note that $|R| = |G/P| - 1$ and we can assume that

$$R = \sum_{i=1}^{n} g^{b_i} h^i,$$

where $0 \le b_i \le p-1$. Therefore we have $RP = G - P$. Now

$$\begin{aligned} R^{(\alpha)}R^{(-\alpha)} &= (\beta R + Px)(\beta R + Px)^{(-1)} \\ &= RR^{(-1)} + \beta x^{(-1)}RP^{(-1)} + \beta^{-1}xR^{(-1)}P + p\, xx^{(-1)}P \\ &= n + (\tfrac{n-1}{p} + \beta x^{(-1)} + \beta^{-1}x)G - (\tfrac{n-1}{p} + \beta x^{(-1)} - pxx^{(-1)} + x\beta^{-1})P. \end{aligned}$$

On the other hand, note that $\gcd(\alpha, |G|) = 1$, we have

$$R^{(\alpha)}R^{(-\alpha)} = (RR^{(-1)})^{(\alpha)} = (n + \frac{n-1}{p}(G-P))^{(\alpha)} = n + \frac{n-1}{p}(G-P).$$

Therefore,

$$\begin{cases} \beta x^{(-1)} + \beta^{-1}x & = 0, \\ \beta x^{(-1)} - pxx^{(-1)} + x\beta^{-1} & = 0. \end{cases}$$

From above we have $xx^{(-1)} = 0$, which implies that $x = 0$. It follows that $R^{(\alpha)} = \beta \cdot R$ for some $\beta \in G$. The proof is completed. □

Next we give an example to disprove the existence of an almost p-ary PS by applying Theorem 4.

Example 2. There do not exist almost 7-ary PS with period 23.

Proof. First it can be verified that almost 7-ary PSs with period 23 do not satisfy the conditions of Theorem 3. By Theorem 1, it is equivalent to prove that there do not exist $(23, 7, 22, 3)$-RDS, say R, in $G = \mathbb{Z}_{23} \times \mathbb{Z}_7$ relative to $\mathbb{Z}_7$. It can be checked that 2 is a multiplier of R by Theorem 4. Using MAGMA[3], we compute the orbits of G under the group automorphism $x \mapsto x^2$. The results are in the following table.

We checked that the only possible combination of orbits such that the cardinality is 22 and find it is not a RDS. Then we finish the proof. □

Using similar argument, we get the following result.

Table 1. Orbits of G under $x \mapsto x^2$

Length of orbit	number
1	1
3	2
11	2
33	4

Theorem 5. *There do not exist almost p-ary PSs of period $n+1$, where $p|n-1$ and $n \in \{22, 28, 45, 52\}$.*

Remark 1. The method in Example 2 cannot determine the existence of RDSs if the number of orbits gets larger. Indeed, in this case usually there exist many combinations of the orbits such that the size of the sum of these orbits equal to the cardinality of the RDS, and therefore it is impossible to verify all of them whether is an RDS one by one. For example, when $n = 77$ and $p = 19$ in Theorem 4, it can be verified that 49 is a multiplier of the corresponding $(78, 19, 77, 19)$-RDS. The orbits of $G = \mathbb{Z}_{78} \times \mathbb{Z}_{19}$ under the group automorphism $x \mapsto x^{49}$ is $1^6 3^{36} 6^{228}$, where i^j implies that there are j orbits with length i. It can be computed that the number of the combinations of the orbits such that the size of the sum of them equal to $|R| = 77$ is

$$\sum_{i=0}^{12} \binom{228}{12-i} \left(\binom{36}{1+i}\binom{6}{2} + \binom{36}{i}\binom{6}{5} \right) \approx 2^{75}.$$

In Table 2, we have the following open cases to be determined. They cannot be excluded by using the above method.

Question 1. Whether almost p-ary PSs exist for $n = 50, 76, 77, 94, 99, 100$, where odd prime $p \mid n-1$.

Table 2 in Appendix lists the existence status of p-ary PSs of period $n+1$ for $3 \le n \le 100$ and p is a prime divisor of $n-1$. The question mark "?" in the table is used to denote an undecided case.

4 Almost p-Ary Nearly Perfect Sequences

Let $G, H, P, \mathbf{a}$ be the same as those in the last section. The sequence $\mathbf{a}$ is called an *almost p-ary nearly perfect sequence* (*NPS*) *of type I* (*II*) if the out-of-phase autocorrelation coefficients are all $-1(1)$. Similar to Theorem 1, we have the following result.

Theorem 6. *Let $\mathbf{a} = (0, a_1, a_2, \cdots, a_n)$ be an almost p-ary sequence of period $n+1$, where $a_i = \zeta_p^{b_i}$ and $0 \le b_i \le p-1$ for $1 \le i \le n$. Let $R = \sum_{i=1}^{n} g^{b_i} h^i$. Then*

1. *$\mathbf{a}$ is an almost p-ary NPS of type I if and only if R is an $(n+1, p, n, \frac{n}{p}-1, 0, \frac{n}{p})$ direct product difference set in G relative to H and P.*
2. *$\mathbf{a}$ is an almost p-ary NPS type II if and only if R is an $(n+1, p, n, \frac{n-2}{p}+1, 0, \frac{n-2}{p})$ direct product difference set in G relative to H and P.*

From Theorem 6 we have the following necessary condition for the existence of almost p-ary NPSs.

Corollary 4. (1) *If there exists an almost p-ary NPS of period $n+1$ of type I, then $p \mid n$.* (2) *If there exists an almost p-ary NPS of period $n+1$ of type II, then $p \mid n-2$.*

Next we construct a family of almost p-ary NPSs of type I.

Example 3. Let q be a prime and let p be a prime divisor of $q-1$. Let H be the additive group of the finite field $\mathbb{F}_q$ and let N be the multiplicative group of $\mathbb{F}_q$. Let $G = H \times N \cong \mathbb{Z}_q \times \mathbb{Z}_{q-1}$. Define

$$R = \{(x, x) | x = 0, 1, \cdots, q-2\}.$$

Clearly R is a $(q, q-1, q-1, 0, 0, 1)$ direct product difference set in G relative to H and N (see [11, Example 5.3.2]). By (2),

$$RR^{(-1)} = q + (G - H - N). \tag{7}$$

Let $\rho : G \to G/M$ be the natural epimorphism, where $M \leqslant N$ and $M \cong Z_{\frac{q-1}{p}}$. Then by (7), we have $\rho(R)\rho(R^{(-1)}) = q - N/M + \frac{q-1}{p}(G/M - N/M)$, which follows that $\rho(R)$ is a $(q, p, q-1, \frac{q-1}{p} - 1, 0, \frac{q-1}{p})$-DPDS in $G/M \cong \mathbb{Z}_q \times \mathbb{Z}_p$ relative to $H/M \cong \mathbb{Z}_q$ and $N/M \cong \mathbb{Z}_p$. By Theorem 6 (1), there exists an almost p-ary NPS of type I with period q.

In the following we present results to show almost p-ary NPSs of type I do not exist with certain periods.

Lemma 4. *Let n be an odd integer and $b_i \in \{0, 1, \cdots, n-1\}$ for $1 \leq i \leq n$. Assume that $b_i \neq b_j$ when $i \neq j$, then $|\{b_{i+1} - b_i | i = 1, 2, \cdots, n-1\}| < n-1$ ($b_i - b_j$ is computed modulo n).*

Proof. Let $S = \{b_{i+1} - b_i | i = 1, 2, \cdots, n-1\}$. Clearly $|S| \leq n-1$. Now assume that $|S| = n-1$, then $S = \{1, \ldots, n-1\}$ as $b_i \neq b_j$ for $i \neq j$. Therefore, $\sum_{i=1}^{n-1}(b_{i+1} - b_i) = \sum_{i=1}^{n-1} i \equiv \frac{n(n-1)}{2} \equiv 0 \mod n$ as n is odd. On the other hand, $\sum_{i=1}^{n-1}(b_{i+1} - b_i) = b_n - b_1$. The contradiction arises as $b_i \not\equiv b_j \mod n$. □

Theorem 7. *Let $G = H \times P = \langle h \rangle \times \langle g \rangle = \mathbb{Z}_{n+1} \times \mathbb{Z}_n$ and let R be an $(n+1, n, n, 0, 0, 1)$-DPDS in G relative to H and P. Then R does not exist if n is an odd integer. Therefore, for any odd prime p, there do not exist almost p-ary NPSs of type I with period $p+1$.*

Proof. Since $|R| = |G/P| - 1$ and no elements in P can be represented as the differences of elements in R, we can assume that $R = \sum_{i=1}^{n} g^{b_i} h^i$ and $b_i \in \{0, 1, \ldots, n-1\}$. Similarly, as there are also no elements in H can be represented as the differences of elements in R and $|P| = |R| = n$, we have $\{b_i | i = 1, \ldots, n\} = \{0, 1, \ldots, n-1\}$. Now

$$n + 1 + (G - H - P) = RR^{(-1)} = n + \sum_{t=1}^{n} \sum_{\substack{i=1 \\ i \not\equiv -t \mod (n+1)}}^{n} g^{b_{i+t} - b_i} h^t.$$

It follows that for each $t \neq 0$,

$$\{b_{i+t} - b_i : 1 \leq i \leq n | i \not\equiv -t \mod (n+1)\} = \{1, \ldots, n-1\}.$$

However, by letting $t = 1$ and we see the above equation cannot hold by Lemma 4. We finish the proof. □

By Lemma 1, we have the following nonexistence result.

Theorem 8. *Let q be a prime divisor of $n+1$ such that $q^r \| n+1, q \neq p$. Assume that q is self-conjugate modulo $p \cdot u$ for a divisor u of $n+1$. Let $G = H \times P = \langle h \rangle \times \langle g \rangle \cong \mathbb{Z}_{n+1} \times \mathbb{Z}_p$ and let $K = G/\langle h^u \rangle \cong \mathbb{Z}_u \times \mathbb{Z}_p$. If there exists an almost p-ary NPS of type I with period $n+1$, then*

1. *If $q \nmid |K|$, r is even and $q^{\frac{r}{2}} \leq \frac{n+1}{u}$; and*
2. *If $q \mid |K|$, $q^{\lfloor \frac{r}{2} \rfloor} \leq 2\frac{n+1}{u}$.*

Proof. By Theorem 6, we can assume that there is an $(n+1, p, n, \frac{n}{p} - 1, 0, \frac{n}{p})$-DPDS R in G relative to H and P. Then $RR^{(-1)} = (n+1) - H + \frac{n}{p}(G - P)$. Let $\rho : G \to K$ be the natural epimorphism. Clearly the coefficients of $\rho(R) \in \mathbb{Z}[K]$ lie between 0 and $\frac{n+1}{u}$. Since q is self-conjugate modulo $\exp(K) = p \cdot u$ and for any nonprincipal character χ of K,

$$\chi(\rho(R))\overline{\chi(\rho(R))} = \begin{cases} n+1 & \text{if } \chi \text{ is nonprincipal on both } \rho(P) \text{ and } \rho(H), \\ 1 & \text{if } \chi \text{ is nonprincipal on } \rho(H), \\ 0 & \text{if } \chi \text{ is nonprincipal on } \rho(P). \end{cases}$$

Take $L = \rho(P)$ and $K = \rho(R)$ in Lemma 1, then obviously $q^r | \chi(\rho(R))(\overline{\chi(\rho(R))})$ for $\chi \notin \rho(P)^\perp$ and $q^{r+1} \nmid \chi(\rho(R))(\overline{\chi(\rho(R))})$ for $\chi \notin \rho(H)^\perp \cup \rho(P)^\perp$. If $q \mid |K|$, it is also easy to see $\chi(\rho(R)) \neq 0$ because $\chi(\rho(R))\overline{\chi(\rho(R))} = n+1$ for $\chi \notin \rho(Q)^\perp \cup \rho(P)^\perp$, where Q is the subgroup of K of order q. Now the result follows from Lemma 1. □

Corollary 5. *If there exists a prime divisor q of $n+1$ with $q^{2s+1} \parallel n+1$ and q is self-conjugate modulo p, then there do not exist almost p-ary NPSs of type I with period $n+1$.*

Proof. Take $u = 1$ in Theorem 8 and note that $|K| = p$. By Theorem 8, the result follows as $q \nmid p$ for every prime divisor q of $n+1$. □

Corollary 6. *Let q be a prime divisor of $n+1$ with q is self-conjugate modulo $(n+1)p$. Assume that $q^r \mid n+1$ for $r \geq 4$ if $q = 2$. Then there do not exist almost p-ary NPSs of type I with period $n+1$.*

For almost p-ary NPSs of type II with period $n+1$, we only find the example with $p = 2$ and $n = 2$, namely $\mathbf{a} = \{0, 1, 1\}$. We have done a computer search for $p = 3$ and $n \in \{2, 5, 8, 11, 14, 17\}$, and however, no example is found. We leave it as the following open question.

Question 2. Do almost p-ary NPSs of type II with period $n+1$ exist?

In Appendix, Table 3 lists the existence status of the almost p-ary NPSs of type I with period $n+1$ for $2 \leq n \leq 100$, where p is a prime divisor of n. The question mark "?" in the table is used to denote an undecided case.

Acknowledgement

The authors are grateful to the invaluable discussions with Professor Alexander Pott which enables this work. They also thank the anonymous referees for their valuable suggestions.

Part of this work was done during the second author's visit at the Otto-von-Guericke- University. He would like to thank the hospitality of the Institute of Algebra and Geometry.

References

1. Arasu, K.T., Ma, S.L.: Abelian difference sets without self-conjugacy. Des. Codes Cryptography 15(3), 223–230 (1998)
2. Beth, T., Jungnickel, D., Lenz, H.: Design theory, 2nd edn. Cambridge University Press, New York (1999)
3. Bosma, W., Cannon, J., Playoust, C.: The magma algebra system I: The user language. Journal of Symbolic Computation 24(3-4), 235–265 (1997), http://www.sciencedirect.com/science/article/B6WM7-45M2XHC-7/2/1774bb42b9fe09d31c90f383c419c7d2
4. Ganley, M.J.: Direct product difference sets. Journal of Combinatorial Theory, Series A 23(3), 321–332 (1977), http://www.sciencedirect.com/science/article/B6WHS-4D7D14S-XS/2/4f3316fe57bc9e1b6b685433891ca6aa
5. Jungnickel, D.: On automorphism groups of divisible designs, II: group invariant generalised conference matrices. Archiv der Mathematik 54(2) (February 1990)
6. Jungnickel, D., Pott, A.: Computational non-existence results for abelian affine difference sets. Congressus Numerantium 68, 91–98 (1989)
7. Jungnickel, D., Pott, A.: Perfect and almost perfect sequences. Discrete Applied Mathematics 95(1-3), 331–359 (1999)
8. Lidl, R., Niederreiter, H.: Finite fields, Encyclopedia of Mathematics and its Applications, 2nd edn., vol. 20. Cambridge University Press, Cambridge (1997)
9. Ma, S.L., Ng, W.S.: On nonexistence of perfect and nearly perfect sequences. Int. J. Inf. Coding Theory 1(1), 15–38 (2009)
10. Passman, D.S.: The algebraic structure of group rings. John Wiley & Sons, New York (1977)
11. Pott, A.: Finite Geometry and Character Theory. LNM, vol. 1601. Springer, Heidelberg (1995)
12. Schmidt, B.: Characters and cyclotomic fields in finite geometry. LNM, vol. 1797. Springer, Berlin (2002)
13. Stanton, R., Mullin, R.C.: On the nonexistence of a class of circulant balanced weighing matrices. SIAM Journal on Applied Mathematics 30, 98–102 (1976)

Appendix

Table 2. Existence Status of Perfect Sequences

n	p	Existence Status	n	p	Existence Status
3	2	not exist by Theorem 2	4	3	exist by Example 1
5	2	not exist by Theorem 2	6	5	not exist by Corollary 3 with q=2
7	2	not exist by Theorem 2	7	3	exist by Example 1
8	7	exist by Example 1 2	9	2	not exist by Theorem 2
10	3	not exist by Corollary 3 with q=2	11	2	not exist by Theorem 2
11	5	exist by Example 1	12	11	not exist by Result 5
13	2	not exist by Theorem 2	13	3	exist by Example 1
14	13	not exist by Corollary 3 with q=2	15	2	not exist by Theorem 2
15	7	not exist by Corollary 3 with q=3	16	3	exist by Example 1
16	5	exist by Example 1	17	2	not exist by Theorem 2
18	17	not exist by Corollary 3 with q=2	19	2	not exist by Theorem 2
19	3	exist by Example 1	20	19	not exist by Result 5
21	2	not exist by Theorem 2	21	5	not exist by Corollary 3 with q=3
22	3	not exist by Corollary 3 with q=2	22	7	not exist by Theorem 5
23	2	not exist by Theorem 2	23	11	exist by Example 1
24	23	not exist by Result 5	25	2	not exist by Theorem 2
25	3	exist by Example 1	26	5	not exist by Corollary 3 with q=2
27	2	not exist by Theorem 2	27	13	exist by Example 1
28	3	not exist by Theorem 5	29	2	not exist by Theorem 2
29	7	exist by Example 1	30	29	not exist by Corollary 3 with q=2
31	2	not exist by Theorem 2	31	3	exist by Example 1
31	5	exist by Example 1	32	31	exist by Example 1
33	2	not exist by Theorem 2	34	3	not exist by Corollary 3 with q=2
34	11	not exist by Corollary 3 with q=2	35	2	not exist by Theorem 2
35	17	not exist by Corollary 3 with q=5	36	5	not exist by Corollary 2 with q=2
36	7	not exist by Corollary 2 with q=3	37	2	not exist by Theorem 2
37	3	exist by Example 1	38	37	not exist by Corollary 3 with q=2
39	2	not exist by Theorem 2	39	19	not exist by Corollary 3 with q=3
40	3	not exist by Corollary 3 with q=2	40	13	not exist by Corollary 3 with q=2
41	2	not exist by Theorem 2	41	5	exist by Example 1
42	41	not exist by Corollary 3 with q=2	43	2	not exist by Theorem 2
43	3	exist by Example 1	43	7	exist by Example 1
44	43	not exist by Result 5	45	2	not exist by Theorem 2
45	11	not exist by Theorem 5	46	3	not exist by Corollary 3 with q=2
46	5	not exist by Corollary 3 with q=2	47	2	not exist by Theorem 2
47	23	exist by Example 1			
48	47	not exist by Result 5	49	2	not exist by Theorem 2
49	3	exist by Example 1	50	7	?
51	2	not exist by Theorem 2	51	5	not exist by Corollary 3 with q=3
52	3	not exist by Theorem 5	52	17	not exist by Corollary 3 with q=13
53	2	not exist by Theorem 2	53	13	exist by Example 1

Table 2. (*continued*)

54	53	not exist by Corollary 3 with q=2	55	2	not exist by Theorem 2
55	3	not exist by Corollary 3 with q=5	56	5	not exist by Corollary 3 with q=2
56	11	not exist by Corollary 3 with q=2	57	2	not exist by Theorem 2
57	7	not exist by Corollary 3 with q=3	58	3	not exist by Corollary 3 with q=2
58	19	not exist by Corollary 3 with q=2	59	2	not exist by Theorem 2
59	29	exist by Example 1	60	59	not exist by Result 5
61	2	not exist by Theorem 2	61	3	exist by Example 1
61	5	exist by Example 1	62	61	not exist by Corollary 3 with q=2
63	2	not exist by Theorem 2	63	31	not exist by Corollary 3 with q=3
64	3	exist by Example 1	64	7	exist by Example 1
65	2	not exist by Theorem 2	66	5	not exist by Corollary 3 with q=2
66	13	not exist by Corollary 3 with q=2	67	2	not exist by Theorem 2
67	3	exist by Example 1	67	11	exist by Example 1
68	67	not exist by Result 5	69	2	not exist by Theorem 2
69	17	not exist by Corollary 3 with q=3	70	3	not exist by Corollary 3 with q=2
70	23	not exist by Corollary 3 with q=5	71	2	not exist by Theorem 2
71	5	exist by Example 1	71	7	exist by Example 1
72	71	not exist by Result 5	73	2	not exist by Theorem 2
73	3	exist by Example 1	74	73	not exist by Result 5
75	2	not exist by Theorem 2	75	37	not exist by Corollary 3 with q=3
76	3	?	77	2	not exist by Theorem 2
77	19	?	78	7	not exist by Corollary 3 with q=3
78	11	not exist by Corollary 3 with q=2	79	2	not exist by Theorem 2
79	39	exist by Example 1	80	79	not exist by Result 5
81	2	not exist by Theorem 2	81	5	exist by Example 1
82	3	not exist by Corollary 3 with q=2	83	2	not exist by Theorem 2
83	41	exist by Example 1	84	83	not exist by Result 5
85	2	not exist by Theorem 2	85	3	not exist by Corollary 3 with q=5
85	7	not exist by Corollary 3 with q=5	86	5	not exist by Corollary 3 with q=2
85	17	not exist by Corollary 3 with q=2	87	2	not exist by Theorem 2
87	43	not exist by Corollary 3 with q=3	88	3	not exist by Corollary 3 with q=2
88	29	not exist by Corollary 3 with q=2	89	2	not exist by Theorem 2
89	11	exist by Example 1	90	89	not exist by Corollary 3 with q=3
91	2	not exist by Theorem 2	91	3	exist by Example 1
91	5	exist by Example 1	92	91	not exist by Result 5
93	2	not exist by Theorem 2	93	23	not exist by Corollary 3 with q=7
94	3	not exist by Corollary 3 with q=2	94	31	?
95	2	not exist by Theorem 2	95	47	not exist by Corollary 3 with q=5
96	5	not exist by Corollary 3 with q=2	96	19	not exist by Corollary 3 with q=2
97	2	not exist by Theorem 2	97	3	exist by Example 1
98	97	not exist by Corollary 3 with q=2	99	2	not exist by Theorem 2
99	7	?	100	3	?
100	11	?			

Table 3. Existence Status of Nearly Perfect Sequences

n	p	Existence Status	n	p	Existence Status
2	2	exist by example 3	3	3	not exist by Theorem 7 with q=3
4	2	exist by example 3	5	5	not exist by Corollary 5 with q=2
6	2	exist by example 3	6	3	exist by example 3
7	7	not exist by Theorem 7 with q=7	8	2	not exist by Corollary 6 with q=3
9	3	not exist by Corollary 5 with q=2	10	2	exist by example 3
10	5	exist by example 3	11	11	not exist by Theorem 7 with q=11
12	2	exist by example 3	12	3	exist by example 3
13	13	not exist by Corollary 5 with q=2	14	2	not exist by Corollary 5 with q=3
14	7	not exist by Corollary 5 with q=3	15	3	not exist by Corollary 6 with q=2
15	5	not exist by Corollary 6 with q=2	16	2	exist by example 3
17	17	not exist by Corollary 5 with q=2	18	2	exist by example 3
18	3	exist by example 3	19	19	not exist by Theorem 7 with q=19
20	2	not exist by Corollary 5 with q=3	20	5	not exist by Corollary 5 with q=3
21	3	not exist by Corollary 5 with q=2	21	7	?
22	2	exist by example 3	22	11	exist by example 3
23	23	not exist by Theorem 7 with q=23	24	2	not exist by Corollary 6 with q=5
24	3	not exist by Corollary 6 with q=5	25	5	not exist by Corollary 5 with q=2
26	2	not exist by Corollary 5 with q=3	26	13	?
27	3	?	28	2	exist by example 3
28	7	exist by example 3	29	29	not exist by Corollary 5 with q=2
30	2	exist by example 3	30	3	exist by example 3
30	5	exist by example 3	31	31	not exist by Theorem 7 with q=31
32	2	not exist by Corollary 5 with q=3	33	3	not exist by Corollary 5 with q=2
33	11	not exist by Corollary 5 with q=2	34	2	not exist by Corollary 5 with q=5
	17	not exist by Corollary 5 with q=5	35	5	?
35	7	not exist by Corollary 6 with q=3	36	2	exist by example 3
36	3	exist by example 3	37	37	not exist by Theorem 7 with q=37
38	2	not exist by Corollary 5 with q=3	38	19	not exist by Corollary 5 with q=3
39	3	not exist by Corollary 5 with q=2	39	13	not exist by Corollary 5 with q=2
40	2	exist by example 3	40	5	exist by example 3
41	41	not exist by Corollary 5 with q=2	42	2	exist by example 3
42	3	exist by example 3	42	7	exist by example 3
43	43	not exist by Theorem 7 with q=43	44	2	not exist by Corollary 5 with q=5
44	11	?	45	3	not exist by Corollary 5 with q=2
45	5	not exist by Corollary 5 with q=2	46	2	exist by example 3
46	23	exist by example 3	47	47	not exist by Theorem 7 with q=47
48	2	not exist by Corollary 6 with q=7	48	3	not exist by Corollary 6 with q=7
49	7	not exist by Corollary 6 with q=5	50	2	not exist by Corollary 5 with q=3
50	5	not exist by Corollary 5 with q=3	51	3	?
51	17	not exist by Corollary 5 with q=13	52	2	exist by example 3
52	13	exist by example 3	53	53	not exist by Corollary 5 with q=2

Table 3. (*continued*)

54	2	not exist by Corollary 5 with q=5	54	3	not exist by Corollary 5 with q=5
55	5	not exist by Corollary 5 with q=2	55	11	not exist by Corollary 5 with q=2
56	2	not exist by Corollary 5 with q=3	56	7	not exist by Corollary 5 with q=3
57	3	not exist by Corollary 5 with q=2	57	19	not exist by Corollary 5 with q=2
58	2	exist by example 3	58	29	exist by example 3
59	59	not exist by Theorem 7 with q=59	60	2	exist by example 3
60	3	exist by example 3	60	5	exist by example 3
61	61	not exist by Corollary 5 with q=2	62	2	not exist by Corollary 5 with q=7
62	31	not exist by Corollary 6 with q=3	63	3	not exist by Corollary 6 with q=2
63	7	?	64	2	not exist by Corollary 5 with q=5
65	5	not exist by Corollary 5 with q=2	65	13	not exist by Corollary 5 with q=2
66	2	exist by example 3	66	2	exist by example 3
66	11	exist by example 3	67	67	not exist by Theorem 7 with q=67
68	2	not exist by Corollary 5 with q=3	68	17	not exist by Corollary 5 with q=3
69	3	not exist by Corollary 5 with q=2	69	23	not exist by Corollary 5 with q=5
70	2	exist by example 3	70	5	exist by example 3
70	7	exist by example 3	71	71	not exist by Theorem 7 with q=71
72	2	exist by example 3	72	3	exist by example 3
73	73	not exist by Theorem 7 with q=73	74	2	not exist by Corollary 5 with q=3
74	37	not exist by Corollary 5 with q=3	75	3	?
75	5	not exist by Corollary 5 with q=15	76	2	not exist by Corollary 5 with q=7
76	19	?	77	7	?
77	11	not exist by Corollary 5 with q=2	78	2	exist by example 3
78	39	exist by example 3	79	79	not exist by Theorem 7 with q=79
80	2	not exist by Corollary 6 with q=3	80	5	not exist by Corollary 6 with q=3
81	3	not exist by Corollary 6 with q=2	82	2	exist by example 3
82	41	exist by example 3	83	83	not exist by Theorem 7 with q=83
84	2	not exist by Corollary 5 with q=5	84	3	not exist by Corollary 5 with q=5
84	7	not exist by Corollary 5 with q=5	85	5	not exist by Corollary 5 with q=2
85	17	not exist by Corollary 5 with q=2	86	2	not exist by Corollary 5 with q=3
86	43	not exist by Corollary 5 with q=3	87	3	not exist by Corollary 5 with q=11
87	29	not exist by Corollary 5 with q=11	88	2	exist by example 3
88	11	exist by example 3	89	89	not exist by Corollary 5 with q=5
90	2	exist by example 3	90	3	exist by example 3
90	5	exist by example 3	91	91	not exist by Theorem 7 with q=91
92	2	not exist by Corollary 5 with q=3	92	23	?
93	3	not exist by Corollary 5 with q=2	93	31	?
94	2	not exist by Corollary 5 with q=5	94	47	not exist by Corollary 5 with q=5
95	5	not exist by Corollary 5 with q=2	95	19	not exist by Corollary 5 with q=2
96	2	exist by example 3	96	3	exist by example 3
97	97	not exist by Corollary 5 with q=2	98	2	not exist by Corollary 5 with q=11
98	7	?	99	3	not exist by Corollary 6 with q=5
99	11	?	100	2	exist by example 3