SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

May 2017, Vol. 60 052102:1–052102:12
doi: 10.1007/s11432-015-5472-x

On s-uniform property of compressing sequences derived from primitive sequences modulo odd prime powers

Yupeng JIANG[1*], Qun-Xiong ZHENG[2] & Dongdai LIN[1]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Information Science and Technology Institute, Zhengzhou* 450002*, China*

Received August 27, 2015; accepted October 13, 2015; published online September 13, 2016

Abstract Let $\mathbb{Z}/(p^e)$ be the integer residue ring modulo p^e with p an odd prime and $e \geqslant 2$. We consider the s-uniform property of compressing sequences derived from primitive sequences over $\mathbb{Z}/(p^e)$. We give necessary and sufficient conditions for two compressing sequences to be s-uniform with $\underline{\alpha}$ provided that the compressing map is of the form $\phi(x_0, x_1, \ldots, x_{e-1}) = g(x_{e-1}) + \eta(x_0, x_1, \ldots, x_{e-2})$, where $g(x_{e-1})$ is a permutation polynomial over $\mathbb{Z}/(p)$ and η is an $(e-1)$-variable polynomial over $\mathbb{Z}/(p)$.

Keywords compressing map, linear recurring sequence, primitive sequence, permutation polynomial, s-uniform

Citation Jiang Y P, Zheng Q-X, Lin D D. On s-uniform property of compressing sequences derived from primitive sequences modulo odd prime powers. Sci China Inf Sci, 2017, 60(5): 052102, doi: 10.1007/s11432-015-5472-x

1 Introduction

For an odd prime p and positive integer e, let $\mathbb{Z}/(p^e)$ denote the residue ring modulo p^e. We identify the elements of $\mathbb{Z}/(p^e)$ with the corresponding representatives in $\{0, 1, 2, \ldots, p^e - 1\}$. As in [1], for two integers m and n, the notation $[n]_{\bmod m}$ denotes the least nonnegative residue of n modulo m. Similarly for integer sequence $\underline{a} = (a(t))_{t \geqslant 0}$, the notation $[\underline{a}]_{\bmod m}$ means the sequence $([a(t)]_{\bmod m})_{t \geqslant 0}$.

Let $f(x)$ be a monic polynomial of degree $n \geqslant 1$ over $\mathbb{Z}/(p^e)$. If $[f(0)]_{\bmod p} \neq 0$, then there exists a positive integer T such that $x^T - 1$ is divisible by $f(x)$ in $\mathbb{Z}/(p^e)[x]$. The least such positive T is called the least period of $f(x)$ and denoted by $\mathrm{per}(f(x), p^e)$. Ward proved that $\mathrm{per}(f(x), p^e) \leqslant p^{e-1}(p^n - 1)$ [2]. In particular, $f(x)$ is called a primitive polynomial of degree n if $\mathrm{per}(f(x), p^e) = p^{e-1}(p^n - 1)$.

If a sequence $\underline{a} = (a(t))_{t \geqslant 0}$ over $\mathbb{Z}/(p^e)$ satisfies

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

for all $i \geqslant 0$, where $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Z}/(p^e)$, then $\underline{a}$ is called a linear recurring sequence of order n over $\mathbb{Z}/(p^e)$ generated by $f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_1 x - c_0$. Usually, the set of all sequences generated

* Corresponding author (email: jiangyupeng@iie.ac.cn)

by $f(x)$ over $\mathbb{Z}/(p^e)$ is denoted by $G(f(x),p^e)$. For a primitive polynomial $f(x)$ of degree n, a sequence $\underline{a}\in G(f(x),p^e)$ is called a primitive sequence of order n if $[\underline{a}]_{\mathrm{mod}\,p}$ is not the all zero sequence. Primitive sequences over $\mathbb{Z}/(p^e)$ of order n have the least period $p^{e-1}(p^n-1)$ and the set of all primitive sequences generated by $f(x)$ is denoted by $G'(f(x),p^e)$. For $e=1$, primitive sequences are just the well known m-sequences over the prime field $\mathbb{Z}/(p)$. More details of linear recurring sequences over integer residue rings can be found in [3].

For a sequence $\underline{a}=(a(t))_{t\geqslant 0}$ over $\mathbb{Z}/(p^e)$, each $a(t)$ has a unique p-adic expansion as

$$a(t)=a_0(t)+a_1(t)\cdot p+\cdots+a_{e-1}(t)\cdot p^{e-1},$$

with $a_i(t)\in\{0,1,\ldots,p-1\}$ for all $0\leqslant i\leqslant e-1$. The p-ary sequence $\underline{a_i}=(a_i(t))_{t\geqslant 0}$ is called the ith-level sequence of $\underline{a}$, and

$$\underline{a}=\underline{a_0}+\underline{a_1}\cdot p+\cdots+\underline{a_{e-1}}\cdot p^{e-1} \tag{1}$$

is called the p-adic expansion of $\underline{a}$.

Let $f(x)$ be a primitive polynomial over $\mathbb{Z}/(p^e)$ and $\phi(x_0,x_1,\ldots,x_{e-1})$ an e-variable polynomial over $\mathbb{Z}/(p)$. We can induce a map from the set of primitive sequences $G'(f(x),p^e)$ to the set of sequences over $\mathbb{Z}/(p)$ by the polynomial ϕ. The new map is denoted by $\hat{\phi}$ and defined by

$$\begin{aligned}\hat{\phi}:\quad & G'(f(x),p^e)\to(\mathbb{Z}/(p))^{\infty}\\ & \underline{a}\mapsto\phi(\underline{a_0},\ldots,\underline{a_{e-1}})=\big(\phi(a_0(t),\ldots,a_{e-1}(t))\big)_{t\geqslant 0}.\end{aligned}$$

The map $\hat{\phi}$ is called a compressing map and $\phi(\underline{a_0},\underline{a_1},\ldots,\underline{a_{e-1}})$ is called a compressing sequence. Moreover, $\phi(x_0,x_1,\ldots,x_{e-1})$ is called an injective function if $\hat{\phi}$ is injective. Huang and Dai in [4, Theorem 1] and Kuzmin and Nechaev in [5, Theorem 2] independently proved that $\phi(x_0,x_1,\ldots,x_{e-1})=x_{e-1}$ is an injective function. Tian, Zhu and Qi [6–8] proved that all the compressing maps with the form $\phi(x_0,x_1,\ldots,x_{e-1})=g(x_{e-1})+\eta(x_0,x_1,\ldots,x_{e-2})$ are injective functions provided that $f(x)$ is a strongly primitive polynomial (Definition 2 in next section).

In this article, we consider the s-uniform property of compressing sequences. The definition is as follows.

Definition 1. Let $\underline{a}=(a(t))_{t\geqslant 0}$, $\underline{b}=(b(t))_{t\geqslant 0}$ and $\underline{c}=(c(t))_{t\geqslant 0}$ be three sequences over $\mathbb{Z}/(p)$, and let $s,k\in\mathbb{Z}/(p)$. Sequences $\underline{a}$ and $\underline{b}$ are called s-uniform, s-uniform with $\underline{c}$ and s-uniform with $\underline{c}|_k$, respectively, if $a(t)=s$ iff $b(t)=s$ for all $t\geqslant 0$, for all $t\geqslant 0$ with $c(t)\neq 0$ and for all $t\geqslant 0$ with $c(t)=k$.

In [9], Zheng and Qi obtained the remarkable result about the s-uniform property of compressing sequences. This result is presented as the following theorem.

Theorem 1. Let $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and $e\geqslant 2$. Assume

$$\phi(x_0,x_1,\ldots,x_{e-1})=x_{e-1}+\eta(x_0,x_1,\ldots,x_{e-2})$$

with the coefficient of $x_{e-2}^{p-1}\cdots x_1^{p-1}x_0^{p-1}$ in η not equal to $(-1)^e\cdot\frac{p+1}{2}$. Then for $\underline{a},\underline{b}\in G'(f(x),p^e)$, $\underline{a}=\underline{b}$ if and only if there exists $s\in\mathbb{Z}/(p)$ such that $\phi(\underline{a_0},\underline{a_1},\ldots,\underline{a_{e-1}})$ and $\phi(\underline{b_0},\underline{b_1},\ldots,\underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}$.

The sequence $\underline{\alpha}$ in the above theorem is a p-ary sequence related to $\underline{a}$. We will give its definition in next section. If $\phi(x_0,x_1,\ldots,x_{e-1})$ is an injective function, then the p-ary compressing sequence $\phi(\underline{a_0},\underline{a_1},\ldots,\underline{a_{e-1}})$ contains all the information of primitive sequence $\underline{a}$ over $\mathbb{Z}/(p^e)$. Moreover, if ϕ satisfies the condition in the above theorem, then the distribution of any $s\in\mathbb{Z}/(p)$ of compressing sequence $\phi(\underline{a_0},\underline{a_1},\ldots,\underline{a_{e-1}})$ can determine the original sequence $\underline{a}$. Thus, it is possible for us to save storage space when preserving the information of the primitive sequences. This motivates us to find more compressing functions such that s-uniform compressing sequences imply the same original primitive sequences.

In [1], Zheng et al. obtained an improved result and we state it in the following theorem.

Theorem 2. Let $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and $e \geqslant 2$. Assume

$$\phi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2})$$

with the coefficient of $x_{e-2}^{p-1} \cdots x_1^{p-1} x_0^{p-1}$ in η not equal to $(-1)^e \cdot \frac{p+1}{2}$. Then for $\underline{a}, \underline{b} \in G'(f(x), p^e)$, $\underline{a} = \underline{b}$ if and only if there exists $s \in \mathbb{Z}/(p)$ and $k \in (\mathbb{Z}/(p))^*$ such that $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}|_k$.

In a recent paper [10], the authors proved that if x_{e-1} in Theorem 1 is replaced by a general polynomial $g(x_{e-1})$, the result does not hold any more. Especially, when $g(x_{e-1})$ is not a permutation polynomial and satisfies an additional condition, then for any $s \in \mathbb{Z}/(p)$, there may exist many choices of $\eta(x_0, x_1, \ldots, x_{e-2})$ such that for different primitive sequences $\underline{a}$ and $\underline{b}$, the corresponding compressing sequences can be s-uniform. We fix $g(x_{e-1})$ to be a permutation polynomial in this article and give necessary and sufficient conditions for two compressing sequences to be s-uniform with $\underline{\alpha}$, and then we can get many compressing functions such that s-uniform compressing sequences imply the same original primitive sequences. In particular, we can explain why we need the coefficient of $x_{e-2}^{p-1} \cdots x_1^{p-1} x_0^{p-1}$ in η not equal to $(-1)^e \cdot \frac{p+1}{2}$ in Theorem 1. We also get a generalized result of Theorem 2.

The rest of this paper is organized as follows. In Section 2, we give some basic facts about primitive sequences module odd prime powers. We devote Section 3 to proving our main theorem. In Section 4, we have a simple discussion on the property of s-uniform with $\underline{\alpha}|_k$. We give conclusion in Section 5.

2 Preliminaries

In this section, we will introduce some facts about sequences over $\mathbb{Z}/(p^e)$. We only consider the case that p is an odd prime.

For sequences $\underline{a} = (a(t))_{t \geqslant 0}, \underline{b} = (b(t))_{t \geqslant 0}$ over $\mathbb{Z}/(p^e)$, and $c \in \mathbb{Z}/(p^e)$, we have the following operations:

$$\underline{a} + \underline{b} = ([a(t) + b(t)]_{\bmod p^e})_{t \geqslant 0}, \quad c \cdot \underline{a} = ([c \cdot a(t)]_{\bmod p^e})_{t \geqslant 0},$$

$$x^k \underline{a} = (a(t+k))_{t \geqslant 0}.$$

Then the operation of a polynomial $g(x) = \sum_{k=0}^{n} c_k x^k \in \mathbb{Z}/(p^e)[x]$ on the sequence $\underline{a}$ is defined as

$$g(x)\underline{a} = \sum_{k=0}^{n} c_k \cdot x^k \underline{a}.$$

Let $f(x)$ be a primitive polynomial of degree n over the finite field $\mathbb{Z}/(p)$ and $\underline{a} \in G'(f(x), p)$. It is well known that each $\underline{b} \in G(f(x), p)$ can be uniquely written as $g(x)\underline{a}$, where $g(x)$ is a polynomial over $\mathbb{Z}/(p)$ of degree less than n. Moreover, $\underline{b}$ equals to the all zero sequence if and only if $g(x)$ is the zero polynomial. We have a similar result about sequences over $\mathbb{Z}/(p^e)$.

Proposition 1. Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ and $\underline{a} \in G'(f(x), p^e)$. Then for each $\underline{b} \in G(f(x), p^e)$, there are unique polynomials $g_0(x), g_1(x), \ldots, g_{e-1}(x)$ such that

$$\underline{b} = \big(g_0(x) + p \cdot g_1(x) + \cdots + p^{e-1} \cdot g_{e-1}(x)\big)\underline{a}, \tag{2}$$

where each $g_i(x)$ is of degree less than n and with coefficients in $\{0, 1, \ldots, p-1\}$. Moreover, $\underline{b} \in G'(f(x), p^e)$ if and only if $g_0(x) \neq 0$.

Proof. Each sequence over $\mathbb{Z}/(p^e)$ has a unique p-adic expansion as (1). Let $\underline{a_0}$ and $\underline{b_0}$ be the 0th level sequences of $\underline{a}$ and $\underline{b}$ respectively. Letting each coefficient of $f(x)$ modulo p, we can regard $f(x)$ as a primitive polynomial over $\mathbb{Z}/(p)$. Then $\underline{a_0}, \underline{b_0} \in G(f(x), p)$. Since $\underline{a} \in G'(f(x), p^e)$, we have $\underline{a_0} \in G'(f(x), p)$ and then $\underline{b_0} = g_0(x)\underline{a_0} = [g_0(x)\underline{a}]_{\bmod p}$, where $g_0(x)$ is of degree less than n with coefficients in $\{0, 1, \ldots, p-1\}$. Now we consider the sequence $\underline{c} = \underline{b} - g_0(x)\underline{a} \in G(f(x), p^e)$. We have the 0th sequence $\underline{c_0} = \underline{0}$ and 1st sequence $\underline{c_1} \in G(f(x), p)$. Then $\underline{c_1} = [g_1(x)\underline{a}]_{\bmod p}$, where $g_1(x)$ is of degree less than n with coefficients in $\{0, 1, \ldots, p-1\}$. Similarly, we can consider the sequence $\underline{d} = \underline{b} - (g_0(x) + p \cdot g_1(x))\underline{a}$, which

satisfies $\underline{d_0} = \underline{d_1} = \underline{0}$. By induction, if the sequence $\underline{b} - (\sum_{j=0}^{m-1} p^j \cdot g_j(x))\underline{a}$ satisfies that all the jth level sequences are zero sequences for $0 \leqslant j \leqslant m-1$, we can find a unique polynomial $g_m(x)$ with degree less than n and coefficients in $\{0, 1, \ldots, p-1\}$ such that any jth level sequence of $\underline{b} - (\sum_{j=0}^{m} p^j \cdot g_j(x))\underline{a}$ is zero sequence, for $0 \leqslant j \leqslant m$. Then we finally get a sequence $\underline{b} - (g_0(x) + p \cdot g_1(x) + \cdots + p^{e-1} \cdot g_{e-1}(x))\underline{a}$ which is the all zero sequence over $\mathbb{Z}/(p^e)$. So $\underline{b} = \big(g_0(x) + p \cdot g_1(x) + \cdots + p^{e-1} \cdot g_{e-1}(x)\big)\underline{a}$. The uniqueness of $g_i(x)$ comes from the unique expression of sequence in $G(f(x), p)$. According to the definition of primitive sequences, $\underline{b} \in G'(f(x), p^e)$ means $\underline{b_0} \neq \underline{0}$, which just means $g_0(x) \neq 0$. This completes the proof.

Remark 1. Applying the above proposition, we can count the number of primitive sequences generated by a primitive polynomial of degree n. We have $p^n - 1$ choices of $g_0(x)$ and p^n choices of each $g_i(x)$ for $1 \leqslant i \leqslant e-1$. The number is $p^{n(e-1)}(p^n - 1)$, which coincides with $p^{en} - p^{(e-1)n}$ obtained by counting the choices of the first n elements of primitive sequences.

If $f(x)$ is a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$, it is known [4] that there exist polynomials $h_i(x)$ of degree less than n over $\mathbb{Z}/(p^e)$ such that for $1 \leqslant i \leqslant e$,

$$x^{p^{i-1}T} \equiv 1 + p^i \cdot h_i(x) \mod f(x), \tag{3}$$

where $T = p^n - 1$ and $h_1(x) \equiv h_2(x) \equiv \cdots \equiv h_e(x) \not\equiv 0 \bmod p$. For a given $f(x)$, denote by $h_f(x)$ the polynomial $h_1(x)$ modulo p. The sequence $\underline{\alpha}$ over $\mathbb{Z}/(p)$ mentioned in Theorem 1 is defined to be $[h_f(x)\underline{a_0}]_{\bmod p}$.

Definition 2. Let $f(x)$ be a primitive polynomial over $\mathbb{Z}/(p^e)$. If $\deg(h_f(x)) \geqslant 1$, then $f(x)$ is called a strongly primitive polynomial.

Let the equality (3) operate on a sequence $\underline{a}$ generated by $f(x)$ over $\mathbb{Z}/(p^e)$. The following result can be proved. For details see [6].

Proposition 2. Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$. Assume $\underline{a} \in G(f(x), p^e)$, $T = p^n - 1$, and $\underline{\alpha}$ is defined as above. Then the equality

$$(x^{j \cdot p^{e-2}T} - 1)\underline{a_{e-1}} \equiv j \cdot \underline{\alpha} \mod p \tag{4}$$

holds for $e \geqslant 2$ and $j \geqslant 0$.

The following statements about periods of level sequences of a linear recurring sequence over $\mathbb{Z}/(p^e)$ can be proved similarly as in [11].

Proposition 3. Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ and $\underline{a} \in G(f(x), p^e)$ with p-adic expansion as $\underline{a} = \underline{a_0} + \underline{a_1} \cdot p + \cdots + \underline{a_{e-1}} \cdot p^{e-1}$. Assume $T = p^n - 1$. Then

(1) if $\underline{a_0} \neq \underline{0}$, then $\mathrm{per}(\underline{a_i}) = p^i T$ for $0 \leqslant i \leqslant e-1$ and $\mathrm{per}(\underline{a}) = p^{e-1}T$, and

(2) if $\underline{a_0} = \underline{a_1} = \cdots = \underline{a_{i-1}} = \underline{0}$ and $\underline{a_i} \neq \underline{0}$ for $0 \leqslant i \leqslant e-1$, then $\mathrm{per}(\underline{a}) = p^{e-1-i}T$.

For primitive sequences over finite field $\mathbb{Z}/(p)$, the following results are well known.

Proposition 4. Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p)$ and $\underline{a}, \underline{b}, \underline{c} \in G(f(x), p)$. Then

(1) if $\underline{a}$ and $\underline{b}$ are linearly independent over $\mathbb{Z}/(p)$, then for any $w \in \mathbb{Z}/(p)$ and $k \in (\mathbb{Z}/(p))^*$, there exists an integer t, such that $a(t) = w$ and $b(t) = k$, and

(2) if $\underline{a}$, $\underline{b}$ and $\underline{c}$ are linearly independent over $\mathbb{Z}/(p)$, then for any $w, z \in \mathbb{Z}/(p)$ and $k \in (\mathbb{Z}/(p))^*$, there exists an integer t, such that $a(t) = w$, $b(t) = z$ and $c(t) = k$.

3 Main results

Let p be an odd prime and $e \geqslant 2$. We consider the s-uniform property of compressing sequences derived from primitive sequences over $\mathbb{Z}/(p^e)$. We fix the compressing map with the form

$$\phi(x_0, x_1, \ldots, x_{e-1}) = g(x_{e-1}) + \eta(x_0, x_1, \ldots, x_{e-2}),$$

where $g(x_{e-1})$ is a permutation polynomial over $\mathbb{Z}/(p)$ and $\eta(x_0, x_1, \ldots, x_{e-2})$ is an $(e-1)$-variable polynomial over $\mathbb{Z}/(p)$. There exists a unique permutation polynomial $h(x)$ over $\mathbb{Z}/(p)$, such that

$h(g(x_{e-1})) = x_{e-1}$. For any $s \in \mathbb{Z}/(p)$, we denote the $(e-1)$-variable polynomial $h(s-\eta(x_0, x_1, \ldots, x_{e-2}))$ by $\theta_{s,e-2}(x_0, x_1, \ldots, x_{e-2})$.

Lemma 1. Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ and $\underline{a}, \underline{b} \in G'(f(x), p^e)$. Assume

$$\phi(x_0, x_1, \ldots, x_{e-1}) = g(x_{e-1}) + \eta(x_0, x_1, \ldots, x_{e-2})$$

with $g(x_{e-1})$ a permutation polynomial over $\mathbb{Z}/(p)$. For $s \in \mathbb{Z}/(p)$ and $k \in (\mathbb{Z}/(p))^*$, if $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}|_k$, then there exists $\lambda \in (\mathbb{Z}/(p))^*$ such that $\underline{b_0} = \lambda \cdot \underline{a_0}$ and

$$\lambda \cdot a_{e-1}(t) - \lambda \cdot \theta_{s,e-2}(a_0(t), a_1(t), \ldots, a_{e-2}(t)) = b_{e-1}(t) - \theta_{s,e-2}(b_0(t), b_1(t), \ldots, a_{e-2}(t)) \tag{5}$$

holds for all t with $\alpha(t) = k$, where $\theta_{s,e-2}$ is defined as above and $\underline{\alpha} = [h_f(x)\underline{a_0}]_{\mathrm{mod}\, p}$.

Proof. Let $T = p^n - 1$. Then $p^{e-2}T$ is a period of $\underline{\alpha}$, $\underline{a_i}$ and $\underline{b_i}$ for $i < e-1$. Assume $\alpha(t) = k$ for some t, where $k \in (\mathbb{Z}/(p))^*$. Since $g(x_{e-1})$ is a permutation polynomial, by (4), we have

$$\begin{aligned}&\{\phi(a_0(t + j \cdot p^{e-2}T), a_1(t + j \cdot p^{e-2}T), \ldots, a_{e-1}(t + j \cdot p^{e-2}T)) \mid j = 0, 1, \ldots, p-1\}\\ &\quad = \{g(a_{e-1}(t) + j \cdot k) + \eta(a_0(t), a_1(t), \ldots, a_{e-2}(t)) \mid j = 0, 1, \ldots, p-1\}\\ &\quad = \{0, 1, \ldots, p-1\}.\end{aligned}$$

Let $\underline{\beta} = [h_f(x)\underline{b_0}]_{\mathrm{mod}\, p}$. If $\beta(t) = 0$ for this t, then

$$\begin{aligned}&\{\phi(b_0(t + j \cdot p^{e-2}T), b_1(t + j \cdot p^{e-2}T), \ldots, b_{e-1}(t + j \cdot p^{e-2}T)) \mid j = 0, 1, \ldots, p-1\}\\ &\quad = \{g(b_{e-1}(t)) + \eta(b_0(t), b_1(t), \ldots, b_{e-2}(t)) \mid j = 0, 1, \ldots, p-1\},\end{aligned}$$

which is a singleton. It contradicts to that $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}|_k$. So when $\alpha(t) = k$, $\beta(t) \neq 0$. By the first part of Proposition 4, $\underline{\alpha}$ and $\underline{\beta}$ can not be linearly independent. Since both $\alpha(t)$ and $\beta(t)$ are not zero, there exists some $\lambda \in (\mathbb{Z}/(p))^*$ such that $\underline{\beta} = \lambda \cdot \underline{\alpha}$. Thus $\underline{b_0} = \lambda \cdot \underline{a_0}$.

For each t with $\alpha(t) = k$, there exists $0 \leqslant j \leqslant p-1$ such that we have

$$g(a_{e-1}(t) + j \cdot k) + \eta(a_0(t), a_1(t), \ldots, a_{e-2}(t)) = s.$$

We also have

$$g(b_{e-1}(t) + j \cdot \lambda k) + \eta(b_0(t), b_1(t), \ldots, b_{e-2}(t)) = s.$$

According to the definition of $\theta_{s,e-2}(x_0, x_1, \ldots, x_{e-2})$, we have

$$a_{e-1}(t) + j \cdot k = \theta_{s,e-2}(a_0(t), a_1(t), \ldots, a_{e-2}(t)) \tag{6}$$

and

$$b_{e-1}(t) + j \cdot \lambda k = \theta_{s,e-2}(b_0(t), b_1(t), \ldots, b_{e-2}(t)). \tag{7}$$

Multiplying (6) by λ and subtracting (7), we can get (5). This completes the proof.

Now we introduce the following useful lemma in [1, Lemma 15].

Lemma 2. Let $e \geqslant 3$ and $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$, and let $\underline{a}, \underline{b} \in G'(f(x), p^e)$ with $\underline{b_0} = \lambda \cdot \underline{a_0}$ for some $\lambda \in (\mathbb{Z}/(p))^*$. Assume

$$\phi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} - \eta_{e-3}(x_0, x_1, \ldots, x_{e-3}) \cdot x_{e-2}^{p-1} + \rho_{e-2}(x_0, x_1, \ldots, x_{e-2})$$

is an e-variable polynomial over $\mathbb{Z}/(p)$, where the degree of x_{e-2} in the polynomial $\rho_{e-2}(x_0, x_1, \ldots, x_{e-2})$ is less than $p-1$. If there exist $k \in (\mathbb{Z}/(p))^*$ and $\delta \in \mathbb{Z}/(p)$ such that

$$\lambda \cdot \phi(a_0(t), \ldots, a_{e-1}(t)) = \phi(b_0(t), \ldots, b_{e-1}(t)) + \delta$$

holds for all t with $\alpha(t) = k$, then

$$\lambda \cdot a_{e-2}(t) + \lambda \cdot \eta_{e-3}(a_0(t), \ldots, a_{e-3}(t)) = b_{e-2}(t) + \eta_{e-3}(b_0(t), \ldots, b_{e-3}(t)) - G(\lambda)$$

holds for all t with $\alpha(t) = k$, where $\underline{\alpha} = [h_f(x)\underline{a_0}]_{\mathrm{mod}\, p}$ and $G(\lambda) = [\frac{p+1}{2}(\lambda - 1)]_{\mathrm{mod}\, p}$.

Applying Lemma 2 to the result of Lemma 1, we can prove the following proposition.

Proposition 5. Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ and $\underline{a}, \underline{b} \in G'(f(x), p^e)$. Assume

$$\phi(x_0, x_1, \ldots, x_{e-1}) = g(x_{e-1}) + \eta(x_0, x_1, \ldots, x_{e-2})$$

with $g(x_{e-1})$ a permutation polynomial over $\mathbb{Z}/(p)$. If $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}$ for some $s \in \mathbb{Z}/(p)$, then $\underline{a} = \lambda \cdot \underline{b}$ for some $\lambda \in (\mathbb{Z}/(p^e))^*$. Here $(\mathbb{Z}/(p^e))^*$ denotes all the units in the ring $\mathbb{Z}/(p^e)$.

Proof. By Lemma 1, there exists some $\lambda_0 \in \{1, 2, \ldots, p-1\}$ such that $\underline{b_0} = \lambda_0 \cdot \underline{a_0}$ and

$$\lambda_0 \cdot a_{e-1}(t) - \lambda_0 \cdot \theta_{s,e-2}(a_0(t), a_1(t), \ldots, a_{e-2}(t)) = b_{e-1}(t) - \theta_{s,e-2}(b_0(t), b_1(t), \ldots, b_{e-2}(t))$$

holds for all t with $\alpha(t) \neq 0$. Repeatedly using Lemma 2, we have that

$$\lambda_0 \cdot a_j(t) - \lambda_0 \cdot \theta_{s,j-1}(a_0(t), a_1(t), \ldots, a_{j-1}(t)) = b_j(t) - \theta_{s,j-1}(b_0(t), b_1(t), \ldots, b_{j-1}(t)) - G(\lambda_0) \quad (8)$$

holds at all t with $\alpha(t) \neq 0$ for $j = 1, 2, \ldots, e-2$, where

$$\theta_{s,j}(x_0, x_1, \ldots, x_j) = -\theta_{s,j-1}(x_0, x_1, \ldots, x_{j-1}) \cdot x_j^{p-1} + \rho_j(x_0, x_1, \ldots, x_j)$$

and the degree of x_j in the polynomial $\rho_j(x_0, x_1, \ldots, x_j)$ is less than $p-1$. Especially for $j = 1$, we have that

$$\lambda_0 \cdot a_1(t) - \lambda_0 \cdot \theta_{s,0}(a_0(t)) = b_1(t) - \theta_{s,0}(b_0(t)) - G(\lambda_0) \quad (9)$$

holds for all t with $\alpha(t) \neq 0$. This means that if $a_0(t)$, $a_1(t)$ and $b_0(t)$ are fixed, then $b_1(t)$ is determined uniquely. Since $\underline{b_0} = \lambda_0 \cdot \underline{a_0}$, then $g_0(x) = \lambda_0$ in (2), and we have

$$\underline{b_0} + p \cdot \underline{b_1} = [\lambda_0 \cdot \underline{a_0} + p \cdot (\lambda_0 \cdot \underline{a_1} + g_1(x)\underline{a_0})]_{\bmod p^2}. \quad (10)$$

Now we consider the three sequences $\underline{\alpha}, \underline{a_0}, g_1(x)\underline{a_0} \in G(f(x), p)$. If $\deg(g_1(x)) \geqslant 1$, then by Proposition 4, we can choose t_1 and t_2 such that

$$a_0(t_1) = a_0(t_2) \quad \text{and} \quad g_1(x)a_0(t_1) \neq g_1(x)a_0(t_2).$$

No matter whether $\underline{\alpha}$ is linearly dependent on $\underline{a_0}$ and $g_1(x)\underline{a_0}$ or not, by the same proposition, we can make $\alpha(t_1) \neq 0$ and $\alpha(t_2) \neq 0$ at the same time. Applying (4) for $e = 2$, there exist $j_1, j_2 \in \{0, 1, \ldots, p-1\}$ such that

$$a_1(t_1 + j_1 T) = a_1(t_2 + j_2 T).$$

Then $a_0(t_1 + j_1 T) = a_0(t_2 + j_2 T)$, $a_1(t_1 + j_1 T) = a_1(t_2 + j_2 T)$ and $b_0(t_1 + j_1 T) = b_0(t_2 + j_2 T)$. Since $g_1(x)a_0(t_1 + j_1 T) \neq g_1(x)a_0(t_2 + j_2 T)$, we have $b_1(t_1 + j_1 T) \neq b_1(t_2 + j_2 T)$ by (10). It contradicts to (9). So we have $\deg g_1(x) = 0$, and then $g_1(x) = \lambda_1 \in \{0, 1, \ldots, p-1\}$.

If we have proved that in (2), $g_i(x) = \lambda_i \in \{0, 1, \ldots, p-1\}$ for $i = 0, 1, \ldots, j-1 < e-1$, then

$$\underline{b_0} + \cdots + p^j \cdot \underline{b_j} = [(\lambda_0 + \cdots + p^{j-1} \cdot \lambda_{j-1} + p^j \cdot g_j(x))(\underline{a_0} + \cdots + p^{j-1} \cdot \underline{a_{j-1}} + p^j \cdot \underline{a_j})]_{\bmod p^{j+1}}.$$

For the same reason, if $\deg(g_j(x)) \geqslant 1$, we can choose t_1 and t_2 satisfying

- $\alpha(t_1) \neq 0$ and $\alpha(t_2) \neq 0$,
- $a_i(t_1) = a_i(t_2)$ for $0 \leqslant i \leqslant j$,
- $b_i(t_1) = b_i(t_2)$ for $0 \leqslant i \leqslant j-1$,
- $g_j(x)a_0(t_1) \neq g_j(x)a_0(t_2)$, and then $b_j(t_1) \neq b_j(t_2)$.

It contradicts to (8). Thus $g_j(x) = \lambda_j \in \{0, 1, \ldots, p-1\}$. Finally, we can prove that $\underline{a} = \lambda \cdot \underline{b}$. Since $\lambda_0 \in \{1, 2, \ldots, p-1\}$, then $\lambda \in (\mathbb{Z}/(p^e))^*$. The proof is complete.

Remark 2. If the condition in the above theorem is released to that the sequences $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}|_k$ for some $k \in (\mathbb{Z}/(p))^*$, the result does not hold any more. In the above proof, if $\underline{\alpha}$, $\underline{a_0}$ and $g_1(x)\underline{a_0}$ are linearly independent, we can choose t_1 and t_2 such that $\alpha(t_1) = \alpha(t_2) = k$, $a_0(t_1) = a_0(t_2)$ and $g_1(x)a_0(t_1) \neq g_1(x)a_0(t_2)$ by Proposition 4. But when they are linearly dependent, say $g_1(x)\underline{a_0} = c_1 \cdot \underline{a_0} + c_2 \cdot \underline{\alpha}$, for $c_1, c_2 \in \mathbb{Z}/(p)$, there do not exist such t_1 and t_2. We will give more details in Section 4. If we release the condition to that $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}|_{k_1}$ and $\underline{\alpha}|_{k_2}$ for different $k_1, k_2 \in (\mathbb{Z}/(p))^*$, the result still holds.

Now we introduce some notations from number theory. For two integers m and n with $\gcd(m, n) = 1$, there exists positive integers l such that $m^l \equiv 1 \bmod n$. The least such positive l is called the order of m modulo n, denoted by $\mathrm{ord}_n(m)$. For an integer n and prime p, the notation $p^i \parallel n$ means $p^i \mid n$ but $p^{i+1} \nmid n$. It is well known that for an odd prime p and an integer m, if $p^i \parallel (m^j - 1)$, then $p^{i+1} \parallel (m^{pj} - 1)$.

Let $z \in \{0, 1, \ldots, p^e - 1\}$ with $z = z_0 + z_1 \cdot p + \cdots + z_{e-1} \cdot p^{e-1}$. For simplicity, we use $\phi(z)$ to denote $\phi(z_0, z_1, \ldots, z_{e-1})$. Similarly for $z \in \{0, 1, \ldots, p^{e-1} - 1\}$, $\eta(z)$ means $\eta(z_0, z_1, \ldots, z_{e-2})$. We have the following theorem.

Theorem 3. Let $f(x)$, $\underline{a}$, $\underline{b}$ and $\phi(x_0, x_1, \ldots, x_{e-1})$ be as in Proposition 5. If the compressing sequences $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}$ for some $s \in \mathbb{Z}/(p)$, then $\underline{a} = \lambda \cdot \underline{b}$ for some $\lambda \in (\mathbb{Z}/(p^e))^*$ with $\mathrm{ord}_{p^e}(\lambda) = \mathrm{ord}_p(\lambda)$.

Proof. We have $\underline{a} = \lambda \cdot \underline{b}$ for some $\lambda \in (\mathbb{Z}/(p^e))^*$ by Proposition 5. For any $r \in \{1, 2, \ldots, p-1\}$, no matter whether $\underline{\alpha}$ and $\underline{a_0}$ are linearly independent or not, we can choose t with $a_0(t) = r$ and $\alpha(t) \neq 0$. Then by (4), we have $\{a(t) : \alpha(t) \neq 0\} \supseteq (\mathbb{Z}/(p^e))^*$.

Since $g(x_{e-1})$ is a permutation polynomial, we can choose $z \in (\mathbb{Z}/(p^e))^*$ such that $\phi(z) = s$. Assume $a(t) = z$. Then we have $b(t) = [\lambda \cdot z]_{\bmod p^e}$. By the s-uniform property, $\phi([\lambda \cdot z]_{\bmod p^e}) = s$ too. We can also choose $a(t) = [\lambda \cdot z]_{\bmod p^e}$, then $\phi([\lambda^2 \cdot z]_{\bmod p^e}) = s$. So for any nonnegative l, we have $\phi([\lambda^l \cdot z]_{\bmod p^e}) = s$. If $\mathrm{ord}_{p^e}(\lambda) \neq \mathrm{ord}_p(\lambda)$, then $p^i \parallel (\lambda^{\mathrm{ord}_p(\lambda)} - 1)$ with some $1 \leqslant i < e$. Then by the statement before this proposition, $p^{e-1} \parallel (\lambda^l - 1)$ holds for some l. Let $\lambda^l = m \cdot p^{e-1} + 1$ with $\gcd(m, p) = 1$. If z has its p-adic expansion as

$$z = z_0 + z_1 \cdot p + \cdots + z_{e-1} \cdot p^{e-1},$$

then

$$[\lambda^l \cdot z]_{\bmod p^e} = z_0 + \cdots + z_{e-2} \cdot p^{e-2} + [m \cdot z_0 + z_{e-1}]_{\bmod p} \cdot p^{e-1}.$$

Since $[m \cdot z_0 + z_{e-1}]_{\bmod p} \neq z_{e-1}$ and $g(x_{e-1})$ is a permutation polynomial, we can not have $\phi([\lambda^l \cdot z]_{\bmod p^e}) = \phi(z) = s$, which is a contradiction. Thus we must have $\mathrm{ord}_{p^e}(\lambda) = \mathrm{ord}_p(\lambda)$. The proof is complete.

Remark 3. Since $(\mathbb{Z}/(p^e))^*$ is a cyclic group of order $p^{e-1}(p-1)$, an element λ satisfies $\mathrm{ord}_{p^e}(\lambda) = \mathrm{ord}_p(\lambda)$ just means that the order of λ is a divisor of $p - 1$. Then there are exactly $p - 1$ such λ's in $(\mathbb{Z}/(p^e))^*$.

When $f(x)$ is a strongly primitive polynomial over $\mathbb{Z}/(p^e)$, for a fixed permutation polynomial $g(x_{e-1})$ and $\underline{b} = \lambda \cdot \underline{a}$ for some $\lambda \in (\mathbb{Z}/(p^e))^*$ with $\mathrm{ord}_{p^e}(\lambda) = \mathrm{ord}_p(\lambda)$, we can give the exact number of $\eta(x_0, x_1, \ldots, x_{e-2})$, such that the compressing sequences of $\underline{a}$ and $\underline{b}$ derived by $g(x_{e-1}) + \eta(x_0, x_1, \ldots, x_{e-2})$ are s-uniform with $\underline{\alpha}$.

Theorem 4. Let $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ and $\underline{a}, \underline{b} \in G'(f(x), p^e)$. Assume $\underline{b} = \lambda \cdot \underline{a}$ for some $\lambda \in (\mathbb{Z}/(p^e))^*$ with $\mathrm{ord}_{p^e}(\lambda) = \mathrm{ord}_p(\lambda) = l$. For a fixed permutation polynomial $g(x_{e-1})$ over $\mathbb{Z}/(p)$ and $s \in \mathbb{Z}/(p)$, when $l \neq 1$, there are exactly $p^{(p^{e-1}-1)/l}$ polynomials $\eta(x_0, x_1, \ldots, x_{e-2})$ such that $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}$, where $\phi(x_0, x_1, \ldots, x_{e-1}) = g(x_{e-1}) + \eta(x_0, x_1, \ldots, x_{e-2})$. When $l = 1$, i.e., $\lambda = 1$, then any $(e-1)$-variable polynomial $\eta(x_0, x_1, \ldots, x_{e-2})$ is allowed.

Proof. Since $f(x)$ is a strongly primitive polynomial, by the first part of Proposition 4 and (4), then $\{a(t) : \alpha(t) \neq 0\} = \mathbb{Z}/(p^e)$. Since $g(x_{e-1})$ is a permutation polynomial, there are exactly p^{e-1} elements $z \in \{0, 1, \ldots, p^e - 1\}$ such that $\phi(z) = s$ and these elements modulo p^{e-1} run over all elements in $\{0, 1, \ldots, p^{e-1} - 1\}$. We need to determine the value $\eta(w)$ for each $w \in \{0, 1, \ldots, p^{e-1} - 1\}$. if $l = 1$, then

$\underline{a} = \underline{b}$. Thus it is obvious that for any $\eta(x_0, x_1, \ldots, x_{e-2})$, $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}$. There are totally $p^{p^{e-1}}$ $(e-1)$-variable polynomials.

Assume $l \neq 1$. We determine the value $\eta(0)$ first. Since $g(x_{e-1})$ is a permutation polynomial, there is a unique $c \in \{0, 1, \ldots, p-1\}$, such that $\phi(cp^{e-1}) = g(c) + \eta(0) = s$. From the proof of Theorem 3, we know that $\phi(cp^{e-1}) = \phi([\lambda \cdot cp^{e-1}]_{\bmod p^e})$. Thus c must be zero, and then

$$\eta(0) = s - g(0).$$

Now we consider elements not of the form cp^{e-1}. We can divide all the $p^e - p$ elements into $\frac{p^e-p}{l}$ classes. Each class contains l elements,

$$\{z, [\lambda \cdot z]_{\bmod p^e}, \ldots, [\lambda^{l-1} \cdot z]_{\bmod p^e}\}.$$

For each element z not of the form cp^{e-1}, since $\mathrm{ord}_{p^e}(\lambda) = \mathrm{ord}_p(\lambda) = l$, then $[\lambda^i \cdot z]_{\bmod p^{e-1}} \neq [z]_{\bmod p^{e-1}}$ for all $1 \leqslant i < l$, which means that in each class, the elements modulo p^{e-1} are termwise different. It is obvious that $[\lambda^i \cdot z]_{\bmod p^{e-1}} = [\lambda^i \cdot w]_{\bmod p^{e-1}}$ if and only if $[z]_{\bmod p^{e-1}} = [w]_{\bmod p^{e-1}}$. Therefore, if we reduce each class modulo p^{e-1}, then for any $w \in \{1, 2, \ldots, p^{e-1} - 1\}$, the class

$$\{w, [\lambda \cdot w]_{\bmod p^{e-1}}, \ldots, [\lambda^{l-1} \cdot w]_{\bmod p^{e-1}}\}$$

is covered p times. In fact, each class containing $w + ip^{e-1}$ for $0 \leqslant i \leqslant p-1$ is reduced to the above class. Since $\phi(z) = \phi([\lambda^i \cdot z]_{\bmod p^e})$, we choose $\frac{p^{e-1}-1}{l}$ classes from all the $\frac{p^e-p}{l}$ classes, such that these classes modulo p^{e-1} cover all the elements in $\{1, 2, \ldots, p^{e-1} - 1\}$. We let $\phi(z) = s$ if z belongs to the chosen classes. For $w \in \{1, 2, \ldots, p^{e-1} - 1\}$, there exists a unique $c \in \{0, 1, \ldots, p-1\}$, such that $w + cp^{e-1}$ belongs to a chosen class, and then

$$\eta(w) = s - g(c).$$

Each such a choice uniquely determines the value $\eta(w)$ for each $w \in \{1, 2, \ldots, p^{e-1} - 1\}$, and then determines the function $\eta(x_0, x_1, \ldots, x_{e-2})$. For $z = w + c'p^{e-1}$ not in any chosen class, we know $\phi(z) \neq s$ since $g(x_{e-1})$ is a permutation polynomial. Thus for such an $\eta(x_0, x_1, \ldots, x_{e-2})$, $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform. If $\eta(x_0, x_1, \ldots, x_{e-2})$ satisfies that $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform, then the set $S = \{1 \leqslant z \leqslant p^e - 1 \mid \phi(z) = s\}$ can be divided into classes

$$\{z, [\lambda \cdot z]_{\bmod p^e}, \ldots, [\lambda^{l-1} \cdot z]_{\bmod p^e}\}.$$

Since $g(x_{e-1})$ is a permutation polynomial, if reduce the elements in S modulo p^{e-1}, we get a cover of $\{1, 2, \ldots, p^{e-1} - 1\}$. Then $\eta(x_0, x_1, \ldots, x_{e-2})$ must correspond to such a choice of the classes. There are $\frac{p^{e-1}-1}{l}$ classes in $\{1, 2, \ldots, p^{e-1} - 1\}$ and p choices for each class

$$\{w, [\lambda \cdot w]_{\bmod p^{e-1}}, \ldots, [\lambda^{l-1} \cdot w]_{\bmod p^{e-1}}\}.$$

Thus there are $p^{(p^{e-1}-1)/l}$ functions $\eta(x_0, x_1, \ldots, x_{e-2})$ such that $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform. The proof is complete.

We give an example for the determination of η.

Example 1. We consider the ring $\mathbb{Z}/(5^2)$. Let $g(x_1) = x_1$ and $\lambda = 7$. Then $\mathrm{ord}_{5^2}(7) = \mathrm{ord}_5(7) = 4$. Let $\underline{a}$ be a primitive sequence generated by a strongly primitive polynomial over $\mathbb{Z}/(5^2)$. We want the compressing sequences of $7 \cdot \underline{a}$ and $\underline{a}$ to be 0-uniform with $\underline{\alpha}$, By the above theorem, we have $\eta(0) = 0 - g(0) = 0$. There are 20 elements not multiple of 5. We can divide them into 5 classes as follows:

- $1 + 0 \cdot 5$, $2 + 1 \cdot 5$, $4 + 4 \cdot 5$, $3 + 3 \cdot 5$,
- $2 + 0 \cdot 5$, $4 + 2 \cdot 5$, $3 + 4 \cdot 5$, $1 + 2 \cdot 5$,
- $3 + 0 \cdot 5$, $1 + 4 \cdot 5$, $2 + 4 \cdot 5$, $4 + 0 \cdot 5$,
- $1 + 1 \cdot 5$, $2 + 3 \cdot 5$, $4 + 3 \cdot 5$, $3 + 1 \cdot 5$,
- $4 + 1 \cdot 5$, $3 + 2 \cdot 5$, $1 + 3 \cdot 5$, $2 + 2 \cdot 5$.

We choose the first class to be evaluated as 0 under $\phi(x_0, x_1) = g(x_1) + \eta(x_0)$. Then $\eta(1) = 0 - g(0) = 0$, $\eta(2) = 0 - g(1) = 4$, $\eta(4) = 0 - g(4) = 1$ and $\eta(3) = 0 - g(3) = 2$.

From Theorems 3 and 4, we have our main theorem.

Theorem 5. Let $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ and $\underline{a}, \underline{b} \in G'(f(x), p^e)$. Assume

$$\phi(x_0, x_1, \ldots, x_{e-1}) = g(x_{e-1}) + \eta(x_0, x_1, \ldots, x_{e-2})$$

with $g(x_{e-1})$ a permutation polynomial over $\mathbb{Z}/(p)$. Then $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}$ for some $s \in \mathbb{Z}/(p)$ if and only if (1) $\underline{a} = \underline{b}$, or (2) $\underline{a} \neq \underline{b}$ and $\underline{a} = \lambda \cdot \underline{b}$ for some $\lambda \in (\mathbb{Z}/(p^e))^*$ with $\mathrm{ord}_{p^e}(\lambda) = \mathrm{ord}_p(\lambda) = l$. At the same time $\eta(x_0, x_1, \ldots, x_{e-1})$ must be defined as in the proof of Theorem 4. Moreover, in the second case, there are totally $p^{(p^{e-1}-1)/l}$ η's satisfying the condition.

In [10, Theorem16], the authors prove that when $g(x_{e-1}) = x_{e-1}^2$ and $\eta(x_0, x_1, \ldots, x_{e-2})$ is a suitable polynomial, then for $\underline{b} = -\underline{a}$, $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ can be s-uniform for $[\frac{p}{4}] + 1$ elements $s \in \mathbb{Z}/(p)$. When $g(x_{e-1})$ is a permutation polynomial, the result is completely different.

Corollary 1. Let $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ and $\underline{a}, \underline{b} \in G'(f(x), p^e)$. Assume

$$\phi(x_0, x_1, \ldots, x_{e-1}) = g(x_{e-1}) + \eta(x_0, x_1, \ldots, x_{e-2})$$

with $g(x_{e-1})$ a permutation polynomial over $\mathbb{Z}/(p)$. If $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}$ for two different s in $\mathbb{Z}/(p)$, then $\underline{a} = \underline{b}$.

Proof. We know $\underline{b} = \lambda \cdot \underline{a}$. Let $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s_1-uniform and s_2-uniform for $s_1 \neq s_2$. When $\lambda \neq 1$, as in the proof of Theorem 4, we have $\eta(0) = s_1 - g(0)$ and $\eta(0) = s_2 - g(0)$, which is a contradiction. So we have $\lambda = 1$, i.e., $\underline{a} = \underline{b}$.

When $g(x_{e-1}) = x_{e-1}$, we can get more information about $\eta(x_0, x_1, \ldots, x_{e-2})$, which can explain why we need the coefficient of $x_{e-2}^{p-1} \cdots x_1^{p-1} x_0^{p-1}$ in $\eta(x_0, x_1, \ldots, x_{e-2})$ not equal to $(-1)^e \cdot \frac{p+1}{2}$ in Theorem 1.

Theorem 6. Let $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ and $\underline{a}, \underline{b} \in G'(f(x), p^e)$ with $\underline{a} \neq \underline{b}$. Assume

$$\phi(x_0, x_1, \ldots, x_{e-1}) = g(x_{e-1}) + \eta(x_0, x_1, \ldots, x_{e-2}),$$

with $g(x_{e-1}) = x_{e-1}$. If $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}$, then the coefficient of $x_{e-2}^{p-1} \cdots x_1^{p-1} x_0^{p-1}$ in $\eta(x_0, x_1, \ldots, x_{e-2})$ is equal to $(-1)^e \cdot \frac{p+1}{2}$.

Proof. Each $w \in \{0, 1, \ldots, p^{e-1} - 1\}$ has a unique p-adic expression as

$$w = w_0 + w_1 \cdot p + \cdots + w_{e-2} \cdot p^{e-2}.$$

By interpolation, we know that the polynomial expression of η is

$$\eta(x_0, x_1, \ldots, x_{e-2}) = \sum_{w \in \{0,1,\ldots,p^{e-1}-1\}} \eta(w) \prod_{i=0}^{e-2} (1 - (x_i - w_i)^{p-1}).$$

Denote the coefficient of $x_{e-2}^{p-1} \cdots x_1^{p-1} x_0^{p-1}$ in $\eta(x_0, x_1, \ldots, x_{e-2})$ by δ. Then

$$\delta = (-1)^{e-1} \sum_{w \in \{0,1,\ldots,p^{e-1}-1\}} \eta(w).$$

Let $\underline{a} = \lambda \cdot \underline{b}$ with $\mathrm{ord}_{p^e}(\lambda) = \mathrm{ord}_p(\lambda) = l$. Since $\underline{a} \neq \underline{b}$, according to the proof of Theorem 4, we have $\eta(0) = s - g(0) = s$. For $w \neq 0$, assume $\phi(z) = s$ with $z = w + c_w p^{e-1}$. Then $\eta(w) = s - g(c_w)$. We have

$$\delta = (-1)^{e-1} \sum_{w \in \{0,1,\ldots,p^{e-1}-1\}} (s - g(c_w)) = (-1)^e \sum_{w \neq 0} c_w.$$

Table 1 0-uniform with $\underline{\alpha}|_1$

	$\underline{a}$	$0,1,8,8,3,8,4,7,3,1,2,5,0,8,1,1,6,1,5,2,6,8,7,4$
	$\underline{b}$	$3,8,4,7,3,1,2,5,0,8,1,1,6,1,5,2,6,8,7,4,0,1,8,8$
	$\underline{\alpha}$	$\mathbf{1},0,\mathbf{1},2,2,0,2,\mathbf{1},\mathbf{1},0,\mathbf{1},2,2,0,2,\mathbf{1},\mathbf{1},0,\mathbf{1},2,2,0,2,\mathbf{1}$
$d_1=0$	$\phi(\underline{a})$	$1,0,2,2,2,2,1,2,2,0,\mathbf{0},1,1,2,0,\mathbf{0},\mathbf{0},0,1,0,0,2,2,1$
	$\phi(\underline{b})$	$2,2,1,2,2,0,0,1,1,2,\mathbf{0},0,0,0,1,\mathbf{0},\mathbf{0},2,2,1,1,0,2,2$
$d_1=1$	$\phi(\underline{a})$	$1,1,1,1,2,1,2,\mathbf{0},2,1,2,0,1,1,1,1,\mathbf{0},1,\mathbf{0},2,0,1,0,2$
	$\phi(\underline{b})$	$2,1,2,0,2,1,2,\mathbf{0},1,1,1,1,0,1,0,2,\mathbf{0},1,\mathbf{0},2,1,1,1,1$
$d_1=2$	$\phi(\underline{a})$	$1,2,\mathbf{0},0,2,0,0,1,2,2,1,2,1,0,2,2,\mathbf{0},2,2,1,0,0,1,\mathbf{0}$
	$\phi(\underline{b})$	$2,0,\mathbf{0},1,2,2,1,2,1,0,2,2,0,2,2,1,\mathbf{0},0,1,0,1,2,0,\mathbf{0}$

Since for each class $\{[\lambda^i z]_{\bmod p^e} : 0 \leqslant i < l\}$, we have

$$\sum_{i=0}^{l-1} \lambda^i \cdot z \equiv 0 \mod p^e.$$

We also have

$$\sum_{w\in\{0,1,\ldots,p^{e-1}-1\}} w = \frac{p^{e-1}(p^{e-1}-1)}{2} \equiv \frac{p^{e-1}(p-1)}{2} \mod p^e,$$

and then

$$\Big(\sum_{w\neq 0} c_w\Big)p^{e-1} + \frac{p^{e-1}(p-1)}{2} \equiv 0 \mod p^e.$$

Thus $\sum_{w\neq 0} c_w \equiv \frac{p+1}{2} \bmod p$ and then we have $\delta = (-1)^e \sum_{w\neq 0} c_w = (-1)^e \frac{p+1}{2}$. The proof is complete.

4 *s*-uniform with $\underline{\alpha}|_k$ property

In this section, we will discuss the property of s-uniform with $\underline{\alpha}|_k$. In Proposition 5, we prove that if the compressing sequences of two primitive sequences are s-uniform with $\underline{\alpha}$, then these two primitive sequences must be linearly dependent. But if the compressing sequences are just s-uniform with $\underline{\alpha}|_k$ for some nonzero k, the primitive sequences can be linearly independent. See the following example.

Example 2. Let $f(x) = x^2 + x + 2$ over $\mathbb{Z}/(3^2)$ and $\phi(x_0, x_1) = x_1 + 2x_0^2 + d_1x_0 + 1$ with $d_1 \in \mathbb{Z}/(3)$. Let $\underline{a} \in G'(f(x), 3^2)$ with $a(0) = 0$ and $a(1) = 1$. Assume $\underline{b} = (2 + 3 \cdot x)\underline{a}$. Then we have $\phi(\underline{a_0}, \underline{a_1})$ and $\phi(\underline{b_0}, \underline{b_1})$ are 0-uniform with $\underline{\alpha}|_1$. See Table 1.

It is hard to get necessary and sufficient conditions similar to Theorem 5 for compressing sequences to be s-uniform with $\underline{\alpha}|_k$. But we can obtain a sufficient condition similar to Theorem 2.

Theorem 7. Let $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and $e \geqslant 2$. Assume

$$\phi(x_0, x_1, \ldots, x_{e-1}) = g(x_{e-1}) + \eta(x_0, x_1, \ldots, x_{e-2})$$

with $g(x_{e-1})$ a permutation polynomial over $\mathbb{Z}/(p)$. Let $h(x_{e-1})$ be the unique polynomial satisfying $h(g(x_{e-1})) = x_{e-1}$ and assume

$$\sum_{(a_0,\ldots,a_{e-2})\in(\mathbb{Z}/(p))^{e-1}} h(s - \eta(a_0, \ldots, a_{e-2})) \neq \frac{p+1}{2}.$$

Then for $\underline{a}, \underline{b} \in G'(f(x), p^e)$, $\underline{a} = \underline{b}$ if and only if there exists $s \in \mathbb{Z}/(p)$ and $k \in (\mathbb{Z}/(p))^*$ such that $\phi(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{e-1}})$ and $\phi(\underline{b_0}, \underline{b_1}, \ldots, \underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}|_k$.

Proof. Since for any e-tuple $(c_0, c_1, \ldots, c_{e-1}) \in (\mathbb{Z}/(p))^e$, $\phi(c_0, c_1, \ldots, c_{e-1}) = s$ if and only if $c_{e-1} - \theta_{s,e-2}(c_0, c_1, \ldots, c_{e-2}) = 0$, where $\theta_{s,e-2}(x_0, x_1, \ldots, x_{e-2}) = h(s - \eta(x_0, x_1, \ldots, x_{e-2}))$. By Theorem 2, we only need to prove that the coefficient of $x_{e-2}^{p-1} \cdots x_1^{p-1} x_0^{p-1}$ in $\theta_{s,e-2}(x_0, x_1, \ldots, x_{e-2})$ is not equal

to $(-1)^{e-1}\cdot\frac{p+1}{2}$. According to the polynomial expression of $\theta_{s,e-2}$, the coefficient of $x_{e-2}^{p-1}\cdots x_1^{p-1}x_0^{p-1}$, denoted by C, is

$$C=(-1)^{e-1}\sum_{(a_0,\ldots,a_{e-2})\in(\mathbb{Z}/(p))^{e-1}}h(s-\eta(a_0,\ldots,a_{e-2}))\neq(-1)^{e-1}\frac{p+1}{2}.$$

This completes the proof.

In particular, if η is a constant polynomial, then $h(s-\eta(a_0,\ldots,a_{e-2}))$ is constant. So

$$\sum_{(a_0,\ldots,a_{e-2})\in(\mathbb{Z}/(p))^{e-1}}h(s-\eta(a_0,\ldots,a_{e-2}))=0\neq\frac{p+1}{2}.$$

If η is a balanced when regarded as a function from $\mathbb{Z}/(p^{e-1})$ to $\mathbb{Z}/(p)$, when $(a_0,\ldots,a_{e-2})$ runs over all the $(e-1)$-tuple in $(\mathbb{Z}/(p))^{e-1}$, $h(s-\eta(a_0,\ldots,a_{e-2}))$ can achieve any element in $\mathbb{Z}/(p)$ for p^{e-2} times. So

$$\sum_{(a_0,\ldots,a_{e-2})\in(\mathbb{Z}/(p))^{e-1}}h(s-\eta(a_0,\ldots,a_{e-2}))=p^{e-2}\sum_{i\in\mathbb{Z}/(p)}i=0\neq\frac{p+1}{2}.$$

We have the following corollary.

Corollary 2. Let $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and $e\geqslant 2$. Assume

$$\phi(x_0,x_1,\ldots,x_{e-1})=g(x_{e-1})+\eta(x_0,x_1,\ldots,x_{e-2})$$

with $g(x_{e-1})$ a permutation polynomial over $\mathbb{Z}/(p)$. If η is a constant polynomial or balanced, then for $\underline{a},\underline{b}\in G'(f(x),p^e)$, $\underline{a}=\underline{b}$ if and only if there exists $s\in\mathbb{Z}/(p)$ and $k\in(\mathbb{Z}/(p))^*$ such that $\phi(\underline{a_0},\underline{a_1},\ldots,\underline{a_{e-1}})$ and $\phi(\underline{b_0},\underline{b_1},\ldots,\underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}|_k$.

Remark 4. It is easy to get that the number of constant polynomials is p and the number of balanced functions is $\frac{p^{e-1}!}{(p^{e-2}!)^p}$.

5 Conclusion

In this paper, we consider the s-uniform property of compressing sequences derived from primitive sequences module $\mathbb{Z}/(p^e)$ with p odd and $e\geqslant 2$. Let $f(x)$ be a strongly primitive polynomial over $\mathbb{Z}/(p^e)$ and $\underline{a},\underline{b}\in G'(f(x),p^e)$. The compressing map is defined to be $\phi(x_0,x_1,\ldots,x_{e-1})=g(x_{e-1})+\eta(x_0,x_1,\ldots,x_{e-2})$ with $g(x_{e-1})$ a permutation polynomial. In Theorem 1 [9, Theorem 3], the authors prove that when $g(x_{e-1})=x_{e-1}$ and the coefficient of $x_{e-2}^{p-1}\cdots x_1^{p-1}x_0^{p-1}$ in η is not equal to $(-1)^e\cdot\frac{p+1}{2}$, then $\underline{a}=\underline{b}$ if and only if $\phi(\underline{a_0},\underline{a_1},\ldots,\underline{a_{e-1}})$ and $\phi(\underline{b_0},\underline{b_1},\ldots,\underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}$. We let $g(x_{e-1})$ be a general permutation polynomial, and give the necessary and sufficient conditions for $\phi(\underline{a_0},\underline{a_1},\ldots,\underline{a_{e-1}})$ and $\phi(\underline{b_0},\underline{b_1},\ldots,\underline{b_{e-1}})$ to be s-uniform with $\underline{\alpha}$. We also obtain that if $\underline{a}\neq\underline{b}$, $g(x_{e-1})=x_{e-1}$ and $\phi(\underline{a_0},\underline{a_1},\ldots,\underline{a_{e-1}})$ and $\phi(\underline{b_0},\underline{b_1},\ldots,\underline{b_{e-1}})$ are s-uniform with $\underline{\alpha}$, then the coefficient of $x_{e-2}^{p-1}\cdots x_1^{p-1}x_0^{p-1}$ in η is $(-1)^e\cdot\frac{p+1}{2}$. So we can also get the result of Theorem 1.

Acknowledgements This work was supported by National Basic Research Program of China (973 Program) (Grant No. 2011CB302400), Strategic Priority Research Program of the Chinese Academy of Sciences (Grant No. XDA06010701), China Postdoctoral Science Foundation Funded Project (Grant No. 2014M560130), National Natural Science Foundation of China (Grant Nos. 61402524, 61502483), and Science and Technology on Information Assurance Laboratory (Grant No. KJ-13-006).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Zheng Q-X, Qi W-F, Tian T. Further result on distribution properties of compressing sequences derived from primitive sequences over $\mathbb{Z}/(p^e)$. IEEE Trans Inf Theory, 2013, 59: 5016–5022
2 Ward M. The arithmetical theory of linear recurring series. Trans Amer Math Soc, 1933, 35: 600–628
3 Kurakin V L, Kuzmin A S, Mikhalev A V, et al. Linear recurring sequences over rings and modules. J Math Sci, 1995, 76: 2793–2915
4 Huang M Q, Dai Z D. Projective maps of linear recurring sequences with maximal p-adic periods. Fibonacci Quart, 1992, 30: 139–143
5 Kuzmin A S, Nechaev A A. Linear recursive sequences over Galois rings. Russ Math Surv, 1993, 48: 171–172
6 Tian T, Qi W-F. Injectivity of compressing maps on primitive sequences over $\mathbb{Z}/(p^e)$. IEEE Trans Inf Theory, 2007, 53: 2960–2966
7 Zhu X-Y, Qi W-F. Compression mappings on primitive sequences over $\mathbb{Z}/(p^e)$. IEEE Trans Inf Theory, 2004, 50: 2442–2448
8 Zhu X-Y, Qi W-F. Further result of compressing maps on primitive sequences modulo odd prime powers. IEEE Trans Inf Theory, 2007, 53: 2985–2990
9 Zheng Q-X, Qi W-F. Distribution properties of compressing sequences derived from primitive sequences over $\mathbb{Z}/(p^e)$. IEEE Trans Inf Theory, 2010, 56: 555–563
10 Jiang Y P, Lin D D. Distribution properties of compressing sequences derived from primitive sequences modulo odd prime powers. IEEE Trans Inf Theory, 2014, 60: 6602–6608
11 Dai Z D. Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials. J Crypt, 1992, 5: 193–207