Available online at www.sciencedirect.com
ScienceDirect
Discrete Applied Mathematics 154 (2006) 2590–2598
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

Two-tuple balance of non-binary sequences with ideal two-level autocorrelation☆

Guang Gong[a], Hong-Yeop Song[b,*,1]

[a]*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ont., Canada*
[b]*School of Electrical and Electronics Engineering, CITY-Center for Information Technology at Yonsei University, Yonsei University, Seoul 120-749, Korea*

Received 1 February 2004; received in revised form 10 April 2006; accepted 17 April 2006
Available online 21 June 2006

Abstract

Let p be a prime, $q = p^m$ and F_q be the finite field with q elements. In this paper, we will consider q-ary sequences of period $q^n - 1$ for $q > 2$ and study their various balance properties: symbol-balance, difference-balance, and two-tuple-balance properties. The array structure of the sequences is introduced, and various implications between these balance properties and the array structure are proved. Specifically, we prove that if a q-ary sequence of period $q^n - 1$ is difference-balanced and has the "cyclic" array structure then it is two-tuple-balanced. We conjecture that a difference-balanced q-ary sequence of period $q^n - 1$ must have the cyclic array structure. The conjecture is confirmed with respect to all of the known q-ary sequences which are difference-balanced, in particular, which have the ideal two-level autocorrelation function when $q = p$.

Keywords: Non-binary PN sequences; Array structure; Balance property; Difference-balance property; Two-tuple-balance property; Ideal two-level autocorrelation; Cyclic difference sets with singer type parameters

1. Introduction

Let p be an odd prime, and consider a p-ary sequence $\{s(t)\}$ of period $p^n - 1$ with the ideal two-level autocorrelation function. Here, the autocorrelation function is defined as

$$R(\tau) = \sum_{t=0}^{p^n-2} w^{s(t+\tau)-s(t)}, \tag{1}$$

☆ Part of this paper has been presented in 2003 IEEE International Symposium on Information Theory, Yokohama, Japan.

* Corresponding author.
E-mail addresses: ggong@calliope.uwaterloo.ca (G. Gong), hy.song@coding.yonsei.ac.kr (H.-Y. Song).

[1] He was supported by Grant no. R01-2003-000-10330-0 from the Basic Research Program of the Korea Science & Engineering Foundation.

0166-218X/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2006.04.025

where w is a complex primitive pth root of unity. The sequence is said to have the ideal two-level autocorrelation function [2–4] if

$$R(\tau) = \begin{cases} p^n - 1, & \tau \equiv 0 \,(\mathrm{mod}\, p^n - 1), \\ -1, & \tau \not\equiv 0 \,(\mathrm{mod}\, p^n - 1). \end{cases} \tag{2}$$

Sequences with the ideal two-level autocorrelation function have been studied for long time and used in many practical communication systems [3,17].

Let F_{p^n} be the finite field with p^n elements. Let $n = em > 1$ for some positive integers e and m. Then the trace function $Tr_m^n(\cdot)$ is a mapping from F_{p^n} to its subfield F_{p^m} given by

$$Tr_m^n(x) = \sum_{i=0}^{e-1} x^{p^{mi}}.$$

It is easy to check that the trace function satisfies the following: (i) $Tr_m^n(ax + by) = a\,Tr_m^n(x) + b\,Tr_m^n(y)$, for all $a, b \in F_{p^m}$, $x, y \in F_{p^n}$; (ii) $Tr_m^n(x^{p^m}) = Tr_m^n(x)$, for all $x \in F_{p^n}$; and (iii) $Tr_1^n(x) = Tr_1^m(Tr_m^n(x))$, for all $x \in F_{p^n}$. See [12,14] for the detailed properties of the trace function.

The p-ary m-sequences $\{s(t)\}$ of period $p^n - 1$ are well known to have the ideal two-level autocorrelation function. They can be represented as [14,4]

$$s(t) = Tr_1^n(\theta\alpha^t) \quad \text{for } t = 0, 1, 2, \ldots, p^n - 2,$$

where $\alpha \in F_{p^n}$ is a primitive element and $\theta \in F_{p^n}$ can be assumed to be 1 without loss of generality. In one period of $\{s(t)\}$, the symbol distribution is balanced. That is, the symbol *zero* appears $p^{n-1} - 1$ times, and every non-zero symbol of F_p appears exactly p^{n-1} times. Furthermore, if we define, for a given $\tau \not\equiv 0 \,(\mathrm{mod}\,(p^n-1)/(p-1))$, and $i, j \in F_p$,

$$N(i, j) = |\{t | (s(t), s(t + \tau)) = (i, j),\ 0 \leqslant t \leqslant p^n - 2\}|,$$

then, from the ideal two-level autocorrelation function and from the trace function representation of m-sequences, we have $N(0, 0) = p^{n-2} - 1$, and $N(i, j) = p^{n-2}$ for i, j not both zero.

If we let $v = (p^n - 1)/(p - 1) = p^{n-1} + p^{n-2} + \cdots + 1$, then $\alpha^{ivp} = \alpha^{iv}$, and hence α^{iv} belongs to F_p for $i = 0, 1, 2, \ldots, p - 2$. Since $\alpha \in F_{p^n}$ is primitive, the element $\alpha^v = a \in F_p^*$ must be primitive in F_p, and we have the "array structure" given as

$$s(t + iv) = Tr_1^n(\alpha^{t+iv}) = a^i Tr_1^n(\alpha^t) = a^i s(t). \tag{3}$$

Note that $a^i \neq a^j$ for $i \neq j \,(\mathrm{mod}\, p - 1)$. All of the above properties of p-ary m-sequences will be generalized in detail in this paper.

Section 2 contains a comprehensive discussion on (symbol) balance and "difference-balanced" properties of general q-ary sequences of period $q^n - 1$ as well as the "array structure" and the "cyclic array structure" of the sequences, and investigates various implications between all these conditions. We present a conjecture in Section 2 that balanced and difference-balanced sequences must have the cyclic array structure. Section 3 introduces "two-tuple-balance" property, and proves that a difference-balanced sequence must be two-tuple-balanced if it has the cyclic array structure. Some relations of the main results of this paper with those of [15,10,7] are described in detail whenever it is appropriate as Remarks. Section 4 gives a summary figure showing the hierarchy of various classes of balanced q-ary sequences of period $q^n - 1$.

2. Balance, difference-balance, and array structure properties

Let $q = p^m$ where p is a prime and $m \geqslant 1$ is an integer. We use the notation that F_q is the finite field with q elements and $F_q^* = F_q \backslash \{0\}$. In the remaining of the paper we assume that $q > 2$. Following is a generalization of the balance property and the two-level ideal autocorrelation function property of p-ary m-sequences. Note that the period of a sequence is always the "minimum" period of the sequence in this paper.

Definition 1. A q-ary sequence $\{s(t)\}$ of period $q^n - 1$ is said to be *balanced* if *zero* appears $q^{n-1} - 1$ times and any non-zero element of F_q appears q^{n-1} times in one period. It is said to be *difference-balanced* [15,16] if, for any

non-zero $\tau \bmod q^n - 1$, in the differences $s(t+\tau) - s(t)$ as t runs from 0 to $q^n - 2$, the value *zero* occurs $q^{n-1} - 1$ times and each of the non-zero values of F_q occurs q^{n-1} times.

When $m = 1$ and hence $q = p > 2$ is an odd prime, the difference-balancedness of a p-ary sequence implies and is implied by the ideal two-level autocorrelation property of the sequence. See Lemma 4 in [15]. The following is obvious:

Proposition 2. *If a q-ary sequence $\{s(t)\}$ of period $q^n - 1$ is difference-balanced, then each of the following sequences is also difference-balanced*: (i) (*constant multiple*) $\{as(t)\}$ *for any* $a \in F_q^*$, (ii) (*affine shift*) $\{s(t) + b\}$ *for any* $b \in F_q$, (iii) (*cyclic shift*) $\{s(t + c)\}$ *for any* $c = 0, 1, 2, \ldots, q^n - 2$, *and* (iv) (*decimation*) $\{s(dt)\}$ *for any* d *which is relatively prime to* $q^n - 1$.

Suppose the sequence $\{s(t)\}$ is balanced. Then, except for (ii), *all of the above are also balanced. For* (ii), *the symbol b appears $q^{n-1} - 1$ times and each of all the other symbols of F_q appears q^{n-1} times in one period.*

Following is a generalization of the array structure (3) of p-ary m-sequences.

Definition 3. Let $v = (q^n - 1)/(q - 1)$. A q-ary sequence $\{s(t)\}$ of period $q^n - 1$ is said to have *the array structure* if, for any $i = 0, 1, 2, \ldots, q - 2$, there exists $a_i \in F_q$ such that

$$s(t + iv) = a_i s(t) \quad \text{for } t = 0, 1, 2, \ldots, v - 1. \tag{4}$$

The array structure of the sequence $\{s(t)\}$ can best be seen by the following array representation of the sequence, with $a_0 = 1, a_1, a_2, \ldots, a_{q-2}$ in F_q:

$$\begin{pmatrix} s(0) & s(1) & s(2) & \cdots & s(v-1) \\ s(v) & s(v+1) & s(v+2) & \cdots & s(2v-1) \\ s(2v) & s(2v+1) & s(2v+2) & \cdots & s(3v-1) \\ \vdots & & & \cdots & \vdots \\ s((q-2)v) & s((q-2)v+1) & s((q-2)v+2) & \cdots & s((q-1)v-1) \end{pmatrix}$$

$$= \begin{pmatrix} s(0) & s(1) & s(2) & \cdots & s(v-1) \\ a_1 s(0) & a_1 s(1) & a_1 s(2) & \cdots & a_1 s(v-1) \\ a_2 s(0) & a_2 s(1) & a_2 s(2) & \cdots & a_2 s(v-1) \\ \vdots & & & \cdots & \vdots \\ a_{q-2} s(0) & a_{q-2} s(1) & a_{q-2} s(2) & \cdots & a_{q-2} s(v-1) \end{pmatrix} = \begin{pmatrix} 1 \\ a_1 \\ a_2 \\ \vdots \\ a_{q-2} \end{pmatrix} \underline{\mathbf{s}}, \tag{5}$$

where $\underline{\mathbf{s}}$ is the row vector $(s(0), s(1), \ldots, s(v-1))$. It is well known that q-ary m-sequences of period $q^n - 1$ and all of its cyclic shifts have the array structure. We generalize this into the following:

Lemma 4. *Let $v = (q^n - 1)/(q - 1)$. Assume that a q-ary sequence $\{s(t)\}$ of period $q^n - 1$ has the array structure as defined in Definition* 3. *If all the cyclic shifts of $\{s(t)\}$ also have the array structure, then there exists a primitive element $\beta \in F_q$ such that $a_i = \beta^i$ for any i and for any cyclic shift of $\{s(t)\}$.*

Proof. Recall that the period is preserved by the cyclic shift operation, and we assume that $q^n - 1$ is the period of $\{s(t)\}$. Suppose $a_i = 0$ for some i. Then the ith row of the array in (5) must be all zero. By taking the cyclic shift so that it now becomes the top row of the array, we can conclude that the sequence is all zero, which is impossible because the all-zero sequence has period 1. Therefore, all a_i are non-zero and $\{s(t)\}$ is not an all-zero sequence. Hence, there is t_0 such that $s(t_0) \neq 0$ for $0 \leqslant t_0 \leqslant q^n - 2$. Now, we consider the cyclic shift $\{s'(t)\}$ of $\{s(t)\}$ by t_0 so that $s'(0) = s(t_0) \neq 0$. Assumption implies that $\{s'(t)\}$and all of its cyclic shifts have the array structure. Let $a_0 = 1, a_1, \ldots, a_{q-2} \in F_q^*$ be the constants in the array structure of $\{s'(t)\}$. Since its cyclic shift by 1 also has the array structure, we see that $a_i = a_1^i$ for $i = 0, 1, 2, \ldots, q - 2$. It is now easy to show that they must all be distinct, with $a_1 = \beta$ being a primitive element of F_q, because otherwise the sequence will have a subperiod lv for some $0 < l < q - 1$. Then we have $s(t + v) = \beta s(t)$ for all t, and this relation is satisfied by any cyclic shifts of $\{s(t)\}$. □

The conclusion of the lemma implies that in the two-dimensional array representation of the sequence the $(i+1)$st row is a constant multiple of the ith row for all $i = 0, 1, 2, \ldots, q-2$, where $i+1$ is taken mod $q-1$ and where the constant is a primitive element of F_q. Furthermore, this property is satisfied by any cyclic shift of the original sequence.

Definition 5. Let $v=(q^n-1)/(q-1)$. A q-ary sequence $\{s(t)\}$ of period q^n-1 is said to have *the cyclic array structure* if there exists a primitive element β of F_q such that, for any cyclic shift $\{s'(t)\}$ of $\{s(t)\}$, and for any $i=1, 2, \ldots, q-2$, the following is true:

$$s'(t+iv) = \beta^i s'(t) \quad \text{for} \quad t = 0, 1, 2, \ldots, v-1. \tag{6}$$

The cyclic array structure of the sequence $\{s(t)\}$ can be seen by the following array representation of the sequence, where β is primitive in F_q:

$$\begin{pmatrix} s(0) & s(1) & \cdots & s(v-1) \\ s(v) & s(v+1) & \cdots & s(2v-1) \\ s(2v) & s(2v+1) & \cdots & s(3v-1) \\ \vdots & & \cdots & \vdots \\ s((q-2)v) & s((q-2)v+1) & \cdots & s((q-1)v-1) \end{pmatrix} = \begin{pmatrix} 1 \\ \beta \\ \beta^2 \\ \vdots \\ \beta^{q-2} \end{pmatrix} \underline{\mathbf{s}}, \tag{7}$$

where $\underline{\mathbf{s}}$ is the row vector $(s(0), s(1), \ldots, s(v-1))$. Note that the cyclic array structure implies that $s(t+v) = \beta s(t)$ for all t. In fact, the cyclic array structure in the above definition is equivalent to the "projective cyclic equivalence relation" (with a multiplier being a primitive element $\beta \in F_q$) between $\{s(t)\}$ and its cyclic shift $\{s(t+v)\}$ according to [14]. The following is obvious:

Proposition 6. *If a q-ary sequence $\{s(t)\}$ of period q^n-1 has the cyclic array structure, then* (i) *$\{as(t)\}$ for any $a \in F_q^*$ has the cyclic array structure*; (ii) *$\{s(t)+b\}$ for each $b \in F_q^*$ does NOT have the array structure* (*and hence does NOT have the cyclic array structure either*); (iii) *$\{s(t+c)\}$ for any $c = 0, 1, 2, \ldots, q^n-2$ has the cyclic array structure*; *and* (iv) *$\{s(dt)\}$ for any d which is relatively prime to q^n-1 has the cyclic array structure.*

Lemma 7. *Assume that a q-ary sequence $\{s(t)\}$ of period q^n-1 has the cyclic array structure. If it is difference-balanced then it is balanced, but the converse is not true in general.*

Proof. Assume that $\{s(t)\}$ has the cyclic array structure. If we use $\tau = v$, then

$$s(t+\tau) - s(t) = s(t+v) - s(t) = \beta s(t) - s(t) = (\beta - 1)s(t).$$

Since $\beta - 1 \neq 0$, the difference-balance property implies the balance property. The falsity of the converse is obvious. □

Remark 8. J.S. No has essentially obtained the above result. See Lemma 1 in [15]. He started from the assumption that the sequence comes from a d-homogeneous function f from F_{q^n} to F_q, as $s(t) = f(\alpha^t)$, where d is relatively prime to $q-1$ and α is a primitive element of F_{q^n} [15,10]. Then the cyclic array structure of the sequence follows. Finally, the balance property follows from the condition that the sequence is difference-balanced.

Conjecture 9. *If a q-ary sequence $\{s(t)\}$ of period q^n-1* is *difference-balanced, then there exists a unique $b \in F_q$ such that the q-ary sequence $\{s'(t)\}$ defined by $s'(t) = s(t) + b$ for all t has the cyclic array structure.*

Remark 10. From *Proposition* 6, if $\{s(t)\}$ has the cyclic array structure, then none of its "affine shifts" $s'(t) = s(t) + b$ where $b \in F_q^*$ has the array structure. The above conjecture indicates there is a unique affine shift of $\{s(t)\}$ that has the cyclic array structure if the sequence is difference-balanced. The above conjecture can be written as the following simpler form: *if a q-ary sequence $\{s(t)\}$ of period q^n-1 is balanced and difference-balanced, then it has the cyclic array structure*. Note that the balance property guarantees the right affine shift among the q possibilities.

Remark 11. In terms of the terminology in [14], the conjecture states that *if a q-ary sequence* $\{s(t)\}$ *of period* $q^n - 1$ *is balanced and difference-balanced, then it is projectively cyclically equivalent to* $\{s(t + v)\}$.

Remark 12. In terms of d-homogeneous functions [15,10], the conjecture states that *if a q-ary sequence* $\{s(t)\}$ *of period* $q^n - 1$ *is balanced and difference-balanced, then there exist a d-homogeneous function from* F_{q^n} *to* F_q *with d relatively prime to* $q^n - 1$ *such that* $s(t) = f(\alpha^t)$ *for all t where* α *is a primitive element of* F_{q^n}.

Remark 13. When we consider only the case where $q = p > 2$ is an odd prime, the above conjecture says that *a p-ary sequence with the ideal two-level autocorrelation function has a unique affine shift with the cyclic array structure.* The unique affine shift with the cyclic array structure among the q possibilities is the one that is balanced. But the balance property has been proved in [13] only from the ideal two-level autocorrelation function in the case where $q = p > 2$ is an odd prime without assuming the cyclic array structure.

It was confirmed in Introduction that p-ary m-sequences have the cyclic array structure. Similarly, one can easily show that q-ary GMW sequences and all its generalizations [11,5] have the cyclic array structure. It is also not difficult to show that q-ary d-form sequences and all its generalizations [10,15] have the cyclic array structure. Recently, two families of p-ary sequences with the ideal two-level autocorrelation function were explicitly constructed [7]. We will show in the following that both families constructed in [7] have the cyclic array structure. This confirms that *the conjecture is true for all the known p-ary sequences with the ideal two-level autocorrelation function.*

Two families of sequences in [7] can be written as

$$s(t) = Tr_1^n(f(\alpha^t)), \quad t = 0, 1, 2, \ldots, p^n - 2, \tag{8}$$

where the function $f(x)$ over F_{p^n} satisfies some conditions, and α is a primitive element of F_{p^n}. Two examples of $f(x)$ are explicitly specified that result in $\{s(t)\}$ with the ideal two-level autocorrelation function. These are

$$f_1(x) = \sum_{l=0}^{m} u_l x^{(q^{2l}+1)/2}, \tag{9}$$

and

$$f_2(x) = \sum_{l=0}^{m} u_{m-l} x^{(q^{2l+1}+1)/(q+1)}, \tag{10}$$

for some $u_l \in F_p$ and where $q = p^k$ and $n/k = 2m + 1$ must be odd [7].

Lemma 14. *The sequences given in* (8) *using* (9) *or* (10) *have the cyclic array structure for any* $u_l \in F_p$.

Proof. Note that $v = (p^n - 1)/(p - 1)$ implies that $\alpha^v \in F_p$, and in fact that $\alpha^v = a$ is a primitive root mod p. For the case of $f_1(x)$, consider the element of ith row and jth column in its two-dimensional array of size $(p - 1) \times v$. Here, $Tr_1^n(\cdot)$ is a trace map from F_{p^n} to F_p.

$$\begin{aligned} s(iv + j) &= \sum_{l=0}^{m} u_l \, Tr_1^n(\alpha^{(iv+j)(q^{2l}+1)/2}) \\ &= \sum_{l=0}^{m} u_l a^{i(q^{2l}+1)/2} \, Tr_1^n(\alpha^{j(q^{2l}+1)/2}) \\ &= a^i \sum_{l=0}^{m} u_l \, Tr_1^n(\alpha^{j(q^{2l}+1)/2}) = a^i s(j), \end{aligned}$$

where we use the fact that

$$(q^{2l} + 1)/2 \equiv 1 \,(\mathrm{mod}\, q - 1) \equiv 1 \,(\mathrm{mod}\, p - 1), \quad l = 0, 1, 2, \ldots, m.$$

Similarly for $f_2(x)$, one can easily check using the fact that

$$(q^{2l+1}+1)/(q+1) \equiv 1 \pmod{q-1} \equiv 1 \pmod{p-1}, \quad l = 0, 1, 2, \ldots, m. \qquad \square$$

3. Two-tuple-balance property

Definition 15. Let $\{s(t)\}$ be a q-ary sequence of period $q^n - 1$, and let $v = (q^n - 1)/(q - 1)$. We define, for a given integer τ with $0 < \tau < q^n - 1$, and for $x, y \in F_q$,

$$N(x, y) = |\{t | (s(t), s(t+\tau)) = (x, y),\ 0 \leqslant t \leqslant q^n - 2\}|. \tag{11}$$

Then, $\{s(t)\}$ is said to be *two-tuple-balanced* if we have $N(x, y) = q^{n-2}$ for $(x, y) \neq (0, 0)$ with $N(0, 0) = q^{n-2} - 1$ when $\tau \not\equiv 0 \pmod{v}$, and $N(x, y) = q^{n-1}$ for $(x, y) \neq (0, 0)$ with $N(0, 0) = q^{n-1} - 1$ when $\tau \equiv 0 \pmod{v}$.

Remark 16. The balance property in *Definition* 1 is in fact one-tuple-balance property. In general, one can consider *k-tuple-balance property*. For example, for $k = 3$, we can define 3-tuple-balance property of sequences as follows: defining, for a given pair of integers $0 < \tau < \delta < q^n - 1$,

$$N(x, y, z) = |\{t | (s(t), s(t+\tau), s(t+\delta)) = (x, y, z), \quad 0 \leqslant t \leqslant q^n - 2\}|, \quad x, y, z \in F_q,$$

a q-ary sequence $\{s(t)\}$ of period $q^n - 1$ is 3-*tuple-balanced* if $N(x, y, z) = q^{n-3}$ for $(x, y, z) \neq (0, 0, 0)$ with $N(0, 0, 0) = q^{n-3} - 1$ when both $\tau \not\equiv 0 \pmod{v}$ and $\delta \not\equiv 0 \pmod{v}$, and $N(x, y, z) = q^{n-2}$ for $(x, y, z) \neq (0, 0, 0)$ with $N(0, 0, 0) = q^{n-2} - 1$ when either $\tau \equiv 0 \pmod{v}$ or $\delta \equiv 0 \pmod{v}$ (but not both), and $N(x, y, z) = q^{n-1}$ for $(x, y, z) \neq (0, 0, 0)$ with $N(0, 0, 0) = q^{n-1} - 1$ when both $\tau \equiv 0 \pmod{v}$ and $\delta \equiv 0 \pmod{v}$.

Proposition 17. *If a q-ary sequence $\{s(t)\}$ of period $q^n - 1$ is two-tuple-balanced, then it is balanced and also difference-balanced. Furthermore, if it is $(k+1)$-tuple-balanced, then it is k-tuple-balanced, for all $k \geqslant 1$.*

Proof. For any element $x \in F_q$, counting the pair (x, y) for all $y \in F_q$ gives the balance property. Similarly for the difference-balance property. $\square$

For binary sequences, it is easy to see that the balance and difference-balance properties together imply the two-tuple-balance property. For non-binary sequences, we need an additional condition which is the cyclic array structure. If Conjecture 9 will turn out to be true, then they are difference-balanced if and only if they are two-tuple-balanced.

Theorem 18 (*Main*). *Assume that a q-ary sequence $\{s(t)\}$ of period $q^n - 1$ is difference-balanced and has the cyclic array structure. Then it is two-tuple-balanced.*

Remark 19. We would like to note that the main theorem of [15] has already calculated only the value $N(0, 0) = q^{n-2} - 1$. The above theorem calculates $N(x, y)$ for all $x, y \in F_q$. The value $N(0, 0) = q^{n-2} - 1$ is essential in order to construct a (v, k, λ) cyclic difference set with Singer parameters [1,6,8,9,18], because we have the relation that $\lambda = N(0, 0)/(q - 1)$ due to the cyclic array structure of the sequences. In the following proof, we proceed without using the result of [15] that $N(0, 0) = q^{n-2} - 1$.

Proof (*Theorem 18*). We assume that $\{s(t)\}$ is a q-ary sequence of period $q^n - 1$, which is difference-balanced, and has the cyclic array structure. We also assume that a non-zero integer τ is fixed, where $0 < \tau < q^n - 1$. We note from Lemma 7, then, that the sequence is balanced.

Recall that $v = (q^n - 1)/(q - 1)$ and β be a primitive element of F_q. Then the cyclic array structure implies that

$$s(t + iv) = \beta^i s(t),$$

for $t = 0, 1, 2, \ldots, v - 1$ and $i = 0, 1, 2, \ldots, q - 2$. From this structure, the assertion on $\tau \equiv 0 \pmod{v}$ is immediate. So, in the following we only show the case for which $\tau \not\equiv 0 \pmod{v}$.

Now, we use x, y as elements of F_q and consider the $q \times q$ array $N = (N(x, y))$ for $x, y \in F_q$, as defined in (11). We use $x, y = 0, 1, \beta, \beta^2, \ldots$ as the indices of the rows and columns of the array N and consider the various sums of the entries of this array.

First, the balance property implies the following:

$$\sum_{y\in F_q} N(0, y) = q^{n-1} - 1 = \sum_{x\in F_q} N(x, 0), \tag{12}$$

and similarly,

$$\forall x \in F_q^*, \ \sum_{y\in F_q} N(x, y) = q^{n-1} \quad \text{and} \quad \forall y \in F_q^*, \ \sum_{x\in F_q} N(x, y) = q^{n-1}. \tag{13}$$

Second, the difference-balance property implies the following:

$$\sum_{x\in F_q} N(x, x) = q^{n-1} - 1, \tag{14}$$

$$\sum_{x\in F_q} N(x, x + y) = q^{n-1} \quad \forall y \in F_q^*. \tag{15}$$

Third, the cyclic array structure of the sequence shown in (7) implies the following:

$$N(x, y) = N(zx, zy), \quad \text{for } x, y \text{ not both zero and for any } z \neq 0. \tag{16}$$

This gives some further information on the array N: (i) $N(x_1, 0)=N(x_2, 0)$ and $N(0, y_1)=N(0, y_2)$ for all $x_1, x_2, y_1, y_2 \in F_q^*$; (ii) $N(x, x) = N(z, z)$ for all $x, z \in F_q^*$; and therefore we have, in particular,

$$N(x, x) = N(x_1, 0) = N(0, y_1), \tag{17}$$

for all $x, x_1, y_1 \in F_q^*$, since the row sums and the column sums of N except for the top row and the left-most column are all the same, and since the sum of the top row is the same as that of the left-most column, which is again the same as that of the main diagonal.

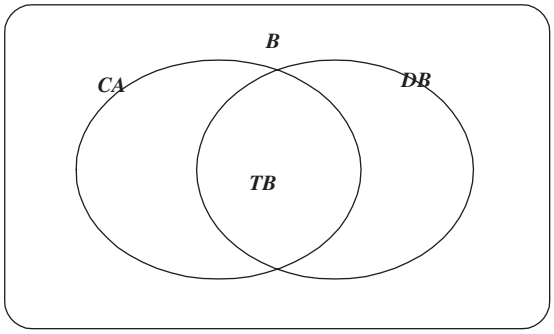
So far, we have considered the occurrences of pairs of symbols with the relative distance τ, and we have analyzed the relation between the entries of the array $N = (N(x, y))$. In order to show the two-tuple balance, we need to introduce a set of arrays $N_m = (N_m(x, y))$, where $N_0 = (N_0(x, y)) = (N(x, y)) = N$. Here, we define $N_m = (N_m(x, y))$ to be the $q \times q$ array for each $m = 0, 1, 2, \ldots, q - 1$ and

$$N_m(x, y) = |\{t | (s(t), s(t + \tau + mv)) = (x, y), \ 0 \leqslant t \leqslant q^n - 2\}|.$$

These are the occurrences of the pair (x, y) with the relative distance $\tau + mv$. Note that the same relations as in (12)–(17) apply to each array N_m, and hence, exactly the same relations as those up to the previous paragraph hold for the entries of N_m for each m, individually.

The final step of this proof is to show that, for any given $x \in F_q^*$, the entries in the positions (x, y) for $y \in F_q$ in N_0 are all the same. We will show this by comparing the values of xth row in N_0 and N_m. For this, we need to observe the following. Since the two-dimensional array of the sequence shown in (7) has the property that every row is a constant multiple of the row one above it, we have the pair $(s(t), s(t + \tau)) = (x, \beta^{-m} y)$ with the distance τ as many as the pair $(s(t), s(t + \tau + mv)) = (x, y)$ with the distance $\tau + mv$. This can seen from the following for the case $m = 1$:

$$\begin{array}{ccccccccc}
\cdots & x & \overset{\text{distance } \tau}{\longleftrightarrow} & \beta^{-1}y & \cdots & & & & \cdots \\
\cdots & \beta x & \longleftrightarrow & y & \cdots & & & & \cdots \\
 & \vdots & & \vdots & & \vdots & & \vdots & \cdots \\
\cdots & & & & \cdots & x & \overset{\text{distance } \tau}{\longleftrightarrow} & \beta^{-1}y & \cdots \\
\cdots & & & & \cdots & \beta x & \longleftrightarrow & y & \cdots
\end{array}$$



B: Balanced q-ary sequences of period q^n-1
DB: Difference-Balanced q-ary sequences
TB: Two-Tuple-Balanced q-ary sequences
CA: q-ary sequences with Cyclic Array Structure

Fig. 1. Hierarchy of balanced q-ary sequences of period $q^n - 1$.

Therefore, we have for each $x \in F_q^*$,

$$N_m(x, y) = N_0(x, \beta^{-m} y) \quad \text{for } y \in F_q. \tag{18}$$

For $y = 0$, the relation (18) gives $N_m(x, 0) = N_0(x, 0)$, for all $x \in F_q^*$. This implies that the $3(q-1)$ entries of N_m and the corresponding entries of N_0 in the top row, in the left-most column, and in the main diagonal, except for the position $(0, 0)$ are all the same, because of (17). Especially, we have

$$N_m(x, x) = N_0(x, x) \quad \text{for all } x \in F_q^*. \tag{19}$$

For $y = x$, the relation (18) gives $N_m(x, x) = N_0(x, \beta^{-m} x)$. This implies that, if we let $z = \beta^{-m} x$, then

$$N_m(x, x) = N_0(x, z) \quad \text{for all } x \in F_q^*. \tag{20}$$

Combining the two relations (19) and (20), we finally have the equality $N_0(x, x) = N_0(x, z)$ for $z = \beta^{-m} x$. As m runs through the values from 0 to $q^n - 2$, the value β^{-m} runs through all the non-zero elements of F_q, and so does $z = \beta^{-m} x$ for any given $x \neq 0$. Therefore, we have shown that the q entries of the xth row of N_0 must be all the same for $x \in F_q^*$. Since the row sum is q^{n-1}, the individual entry must all be q^{n-2}. This implies that all the entries of N_0 must be the same as q^{n-2} except for the position $(0, 0)$, and $N_0(0, 0) = q^{n-2} - 1$. □

4. Concluding remarks

In this paper, we have considered q-ary sequences of period $q^n - 1$ (for $q > 2$) and studied their various balance properties: (symbol or one-tuple) balance, difference-balance, and two-tuple-balance properties. The array structure of the sequences was introduced, and various implications between these balance properties and the array structure are proved. All these results can be summarized in Fig. 1. Our main theorem states that a difference-balanced q-ary sequence of period $q^n - 1$ is two-tuple-balanced if it has the cyclic array structure. We conjecture that a difference-balanced q-ary sequence of period $q^n - 1$ must have the cyclic array structure. With regard to Fig. 1, the conjecture implies that the set DB–CA is empty. The conjecture is confirmed with respect to all of the known q-ary sequences which are difference-balanced, in particular, which have the ideal two-level autocorrelation function when $q = p$ is an odd prime. Note that the set CA-DB in Fig. 1 is trivially non-empty. This completes the classification of various classes of two-tuple-balanced q-ary sequences of period $q^n - 1$, for a prime or a power of a prime q greater than 2.

Acknowledgements

One of Authors Guang Gong wishes to acknowledge the support of NSERC Grant RG-PIN 227700-00.

References

[1] L.D. Baumert, Cyclic Difference Sets, Lecture Notes in Mathematics, vol. 182, Springer, New York, 1971.

[2] S.W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, CA, 1967;
S.W. Golomb, Shift Register Sequences, revised ed., Aegean Park Press, Laguna Hills, CA, 1982.

[3] S.W. Golomb, Construction of signals with favourable correlation properties, in: A.D. Keedwell (Ed.), Survey in Combinatorics, LMS Lecture Note Series 166, Cambridge University Press, Cambridge, 1991. pp. 1–40.

[4] S.W. Golomb, G. Gong, Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar, Cambridge University Press, Cambridge, 2005.

[5] G. Gong, Q-ary cascased GMW sequences, IEEE Trans. Inform. Theory 42 (1) (1996) 263–267.

[6] M. Hall Jr., A survey of difference sets, Proc. Amer. Math. Soc. 7 (1956) 975–986.

[7] T. Helleseth, G. Gong, New nonbinary sequences with ideal two-level autocorrelation function, IEEE Trans. Inform. Theory 48 (11) (2002) 2868–2872.

[8] D. Jungnickel, Difference sets, in: J.H. Dinitz, D.R. Stinson (Eds.), Contemporary Design Theory, Wiley, New York, 1992, pp. 241–324.

[9] D. Jungnickel, A. Pott, Difference sets: abelian, in: C.J. Colbourn, J.H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, New York, 1996.

[10] A. Klapper, d-form sequences: families of sequences with low correlation values and large linear span, IEEE Trans. Inform. Theory 41 (2) (1995) 423–431.

[11] A. Klapper, A.H. Chan, M. Goresky, Cascaded GMW sequences, IEEE Trans. Inform. Theory 39 (1) (1993) 177–183.

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

[13] M. Ludkowski, G. Gong, Ternary ideal 2-level autocorrelation sequences, CORR 2000-59, Technical Report of CACR, University of Waterloo, 2000.

[14] R.J. McEliece, Finite Fields for Computer Scientists and Engineers, Kluwer Academic Publishers, Dordrecht, 1987.

[15] J.-S. No, New cyclic difference sets with singer parameters constructed from d-homogeneous functions, Des. Codes Cryptogr. 33 (2004) 199–213.

[16] J.-S. No, H.-Y. Song, Expanding generalized hadamard matrices over G^m by substituting several generalized hadamard matrices over G, J. Comm. Networks 3 (4) (2001) 361–364.

[17] M.K. Simon, J.K. Omura, R.A. Scholtz, B.K. Levitt, Spread Spectrum Communications Handbook, Computer Science Press, Rockville, MD, 1985;
M.K. Simon, J.K. Omura, R.A. Scholtz, B.K. Levitt, Spread Spectrum Communications Handbook, revised ed., McGraw-Hill, 1994.

[18] J. Singer, A theorem in finite projective geometry and some applications to number theory, Trans. Amer. Math. Soc. 43 (1938) 377–385.