Two-Tuple-Balance of Non-binary Sequences with Ideal Two-Level Autocorrelation

2003 IEEE ISIT
June 29 - July 4, 2003

Guang Gong
Dept. Electrical and Computer Engineering,
University of Waterloo, Waterloo, ON, Canada

Hong-Yeop Song
School of Electrical and Electronics Engineering,
Yonsei University, Seoul, Korea
hy.song@coding.yonsei.ac.kr

I. Introduction

- Consider a p-ary sequence $\{s(t)\}$ of period $p^n - 1$, where p is an odd prime. That is, $s(t) \in Z_p$ for all t.

- The autocorrelation function is defined as

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

  where w is a complex primitive p-th root of unity.

- The sequence is said to have the ideal two-level autocorrelation function if

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

◇ **One important example** is the p-ary m-sequences $\{s(t)\}$ of period $p^n - 1$ that are well-known to have the ideal two-level autocorrelation function.

- Trace representation of p-ary m-sequences using trace from F_{p^n} to F_p:

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

  where α is a primitive element of F_{p^n} and where $\theta \in F_{p^n}$ can be assumed to be 1 without loss of generality.

- In one period of $\{s(t)\}$, the symbol distribution is balanced.

- Furthermore, if we define, for a given $\tau \neq 0 \pmod{p^n - 1}$, and $(i, j) \in Z_p \times Z_p$,

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

  then, we have two-tuple-balance property:

$$N(i, j) = \begin{cases} p^{n-2} - 1 & \text{if } (i, j) = (0, 0) \\ p^{n-2} & \text{otherwise.} \end{cases}$$

- If we let
$$v \stackrel{\triangle}{=} (p^n - 1)/(p-1) = p^{n-1} + p^{n-2} + \cdots + 1,$$
then $\alpha^{ivp} = \alpha^{iv}$, and hence α^{iv} belongs to F_p for $i = 0, 1, 2, \ldots, p-2$.

- Letting $\alpha^v \stackrel{\triangle}{=} a \in F_p^*$, we have an array structure:
$$s(t+iv) = Tr_1^n(\alpha^{t+iv}) = a^i Tr_1^n(\alpha^t) = a^i s(t). \tag{3}$$
That is, we have
$$\begin{pmatrix} s(0) & s(1) & \cdots & s(v-1) \\ s(v) & s(v+1) & \cdots & s(2v-1) \\ s(2v) & s(2v+1) & \cdots & s(3v-1) \\ \vdots & & \cdots & \vdots \\ s((p-2)v) & s((p-2)v+1) & \cdots & s((p-1)v-1) \end{pmatrix} = \begin{pmatrix} 1 \\ a \\ a^2 \\ \vdots \\ a^{p-2} \end{pmatrix} \underline{s}$$
where $\underline{s}$ is the row vector $(s(0), s(1), ..., s(v-1))$.

- All three of the above properties of p-ary m-sequences will be generalized in detail in this presentation.

II. Balance, difference-balance, and the array structure properties

Let $q = p^m$ where p is a prime and $m \geq 1$ is an integer.

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 nonzero symbol appears q^{n-1} times in one period. It is said to be difference-balanced if, for any nonzero τ mod $q^n - 1$, the difference $s(t + \tau) - s(t)$ takes the value* zero *$q^{n-1} - 1$ times and each of the non-zero values q^{n-1} times as t runs from 0 to $q^n - 2$.*

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 $c = 0, 1, 2, ..., q^n - 2$, and

(iv) (decimation) $\{s(dt)\}$ for any d which is relatively prime to $q^n - 1$.

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 cyclic shift $\{s'(t)\}$ of $\{s(t)\}$, and for any $i = 0, 1, 2, \ldots, q - 2$, there exists $a_i \in F_q$ such that*

$$s'(t + iv) = a_i s'(t), \quad \textit{for} \quad t = 0, 1, 2, \ldots, v - 1. \tag{4}$$

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

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

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

Following is obvious:

Proposition 4 *If a q-ary sequence $\{s(t)\}$ of period $q^n - 1$ has the array structure, then*

(i) $\{as(t)\}$ for any $a \in F_q^*$ has the array structure;

(ii) $\{s(t) + b\}$ for each $b \in F_q^*$ does NOT have the array structure;

(iii) $\{s(t + c)\}$ for any $c = 0, 1, 2, ..., q^n - 2$ has the array structure; and

(iv) $\{s(dt)\}$ for any d which is relatively prime to $q^n - 1$ has the array structure provided that $\{s(t)\}$ is either balanced or difference-balanced.

Lemma 5 *Assume that a q-ary sequence $\{s(t)\}$ of period $q^n - 1$ is either balanced or difference-balanced, and assume that it has the array structure with $a_0 = 1, a_1, a_2, ..., a_{q-2}$ as defined in (4). Then, (i) $a_i \neq 0$ for all i, and (ii) $a_i = \beta^i$ for some primitive element $\beta \in F_q$.*

The above lemma leads to a very special case of the array structure.

Definition 6 *Let $v = (q^n - 1)/(q - 1)$. A q-ary sequence $\{s(t)\}$ of period $q^n - 1$ is said to have* the primitive array structure *if there exists a primitive element β of F_q such that, for any cyclic shift $\{s'(t)\}$ of $\{s(t)\}$, the following is true:*

$$s'(t + iv) = \beta s'(t), \quad \textit{for} \quad t = 0, 1, 2, \ldots, v - 1. \tag{5}$$

The primitive 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:

$$\begin{pmatrix} s(0) & s(1) & \cdots & s(v-1) \\ s(v) & s(v+1) & \cdots & s(2v-1) \\ s(2v) & s(2v+1) & \cdots & s(3v-1) \\ \vdots & & \cdots & \vdots \\ s((q-2)v) & s((q-2)v+1) & \cdots & s((q-1)v-1) \end{pmatrix} = \begin{pmatrix} 1 \\ \beta \\ \beta^2 \\ \vdots \\ \beta^{q-2} \end{pmatrix} \underline{s} \tag{6}$$

where $\underline{s}$ is the row vector $(s(0), s(1), ..., s(v-1))$.

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

Remark 8 *J. S. No (2001) has essentially obtained the above result.*

We would like to note that the sequence comes from a d-homogeneous function with $(d, q^n - 1) = 1$ if and only if the sequence has the primitive array structure.

We also would like to note that the array structure in (4) is a slightly more general condition than the primitive array structure.

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 array structure, and hence, has the primitive array structure.*

Remark 10 *The above conjecture can be written as the following simple form: if a q-ary sequence $\{s(t)\}$ of period $q^n - 1$ is balanced and difference-balanced, then it has the array structure. Note that the balance property guarantees the right affine shift among the q possibilities.*

When we consider only the case of $q = p$, i.e., the case of p-ary sequences, the above conjecture says that a p-ary sequence with the ideal two-level autocorrelation function has a unique affine shift with the array structure. If it is balanced then it is the one that has the array structure, and the balance property is followed from the fact that it has the ideal two-level autocorrelation function.

- It was confirmed in Introduction that p-ary m-sequences have the array structure.
- Similarly, one can easily show that p-ary GMW sequences and all its generalizations [Klapper-Chan-Goresky-93, Gong-96] have the array structure.
- It is also not difficult to show that d-form sequences and all its generalizations [Klapper-95, No-01] have the array structure.
- Recently, two families of p-ary sequences with the ideal two-level autocorrelation function were explicitly constructed [Heleseth-Gong-01]. They turned out to have the array structure.

- This confirms that the conjecture is true for all the known p-ary sequences with the ideal two-level autocorrelation function.

III. Two-tuple-balance Property

Definition 12 *Let $v = (q^n - 1)/(q - 1)$ and $\{s(t)\}$ be a q-ary sequence of period $q^n - 1$. We define, for a given τ with $1 \le \tau \le q^n - 2$, and for $x, y \in F_q$,*

$$N(x, y) = |\{\ t \mid (s(t), s(t + \tau)) = (x, y),\ 0 \le t \le q^n - 2\}|. \tag{7}$$

Then, $\{s(t)\}$ is said to be two-tuple-balanced if, for any $\tau = 1, 2, \ldots, q^n - 2$, $N(x, y) = q^{n-2}$ unless $(x, y) = (0, 0)$ for which case $N(0, 0) = q^{n-2} - 1$.

Remark 13 *The balance property in Definition 1 is in fact one-tuple-balance property. In general, one can consider k-tuple-balance property.*

Proposition 14 *If a q-ary sequence $\{s(t)\}$ of period $q^n - 1$ is two-tuple-balanced, then it is balanced and also difference-balanced.*

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 array structure.

Theorem 15 (main) *Assume that a q-ary sequence $\{s(t)\}$ of period $q^n - 1$ is difference-balanced and has the array structure. Then it is two-tuple-balanced.*

Remark 16 *We would like to note that [No-01] has already calculated the value $N(0,0) = q^{n-2} - 1$. The above theorem calculates values of $N(x,y)$ for all $x, y \in F_q$.*

Proof. (SKETCH. Theorem 15) We will prove the theorem for the case $q = p$ only. In the following, we assume that $\{s(t)\}$ is a p-ary sequence of period $p^n - 1$, which is difference-balanced, and has the array structure. We also assume that a non-zero τ is fixed.

- From Lemma 5 and Lemma 7, then, that the sequence has the primitive array structure, and is balanced.
- Now, we use i, j as elements of F_p and consider the $p \times p$ array $N = (N(i, j))$ for $i, j = 0, 1, 2, ..., p - 1$, as defined in (7). We will consider the various sums of the entries in this array.

First, we can compute the row-sum and the column-sum of the array N. Since the sequence is balanced, we have

$$\sum_{j=0}^{p-1} N(0, j) = p^{n-1} - 1 = \sum_{j=0}^{p-1} N(j, 0). \tag{8}$$

Similarly,

$$\sum_{j=0}^{p-1} N(i, j) = p^{n-1} = \sum_{j=0}^{p-1} N(j, i), \quad \text{for each } i = 1, 2, ..., p - 1. \tag{9}$$

Second, we consider the main diagonal and its parallel lines of N. The difference-balance property implies the ideal two-level autocorrelation function. From the fact that $R(\tau) = -1$, we have

$$\begin{aligned} -1 &= R(\tau) = \sum_{t=0}^{p^n-2} w^{s(t+\tau)-s(t)} \\ &= w^0 \sum_{i=0}^{p-1} N(i,i) + w^1 \sum_{i=0}^{p-1} N(i,i+1) + \cdots + w^{p-1} \sum_{i=0}^{p-1} N(i,i+p-1), \\ &= b_0 w^0 + b_1 w^1 + \cdots + b_{p-1} w^{p-1}, \end{aligned}$$

where we let $b_j = \sum_{i=0}^{p-1} N(i,i+j) \in Z$ for $j = 0, 1, 2, ..., p-1$. Since b_j counts the number of two-tuples $(s(t), s(t+\tau))$ such that $s(t+\tau) - s(t) = j$, we have

$$b_0 = \sum_{i=0}^{p-1} N(i,i) = p^{n-1} - 1, \tag{10}$$

$$b_j = \sum_{i=0}^{p-1} N(i,i+j) = p^{n-1}, \quad \text{for } j = 1, 2, ..., p-1. \tag{11}$$

Third, we consider any pair of columns with distance τ, not both all-zero columns, of the 2-dimensional array of the sequence shown in (6). Then, it can easily be seen that, we have

$$N(i,j) = N(xi, xj), \quad \text{for } i,j \text{ not both zero and for any } x \neq 0. \tag{12}$$

This gives some further information on the matrix N:

(i) we must have $N(i,0) = N(j,0)$ and $N(0,i) = N(0,j)$ for all $i \neq 0$ and $j \neq 0$;

(ii) for all $i = j \neq 0$, it implies that $N(i,i) = N(j,j)$; and

(iii) in the $(p-1) \times (p-1)$ array N' obtained from N by deleting the top row and the left-most column, every row or every column is a permutation of the same set of $p-1$ numbers, since the set of positions indexed by (xi, xj) when x runs through F_p^* forms $p-1$ non-attacking-rook-positions of the matrix N'.

These three results further imply that

$$N(0,j) = N(i,0) = N(x,x), \tag{13}$$

for all $i \neq 0$, $j \neq 0$, and $x \neq 0$.

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 $N = (N(i,j))$. Now, we let $N = (N(i,j)) = N_0 = (N_0(i,j))$, and define $N_m = (N_m(i,j))$ to be the $p \times p$ arrays for $m = 0, 1, 2, ..., p-1$, where

$$N_m(i,j) = |\{\ t \mid (s(t), s(t+\tau+mv)) = (i,j), \quad 0 \le t \le p^n - 2\}|.$$

These are the occurrences of the pair (i,j) with the relative distance $\tau + mv$. Note that the same relations as in (8), (9), (10), (11), (12), and (13) apply to each array N_m, and hence, exactly the same relation as those up to the previous paragraph holds for the entries of N_m for each m, individually.

We are now going to determine the relation between the entries of N_0 and N_m for $m \neq 0$. Key observation is the following:

> we have the pair $(s(t), s(t+\tau)) = (i, a^{-m}j)$ with the distance τ as many as the pair $(s(t), s(t+\tau+mv)) = (i,j)$ with the distance $\tau + mv$.

This can seen from the following for the case $m = 1$:

$$
\begin{array}{ccccccccc}
\cdots & i & \overset{\text{distance } \tau}{\longleftrightarrow} & a^{-1}j & \cdots & & & & \cdots \\
\cdots & ai & \longleftrightarrow & j & \cdots & & & & \cdots \\
 & \vdots & & \vdots & & \vdots & & \vdots & \cdots \\
\cdots & & & & \cdots & i & \overset{\text{distance } \tau}{\longleftrightarrow} & a^{-1}j & \cdots \\
\cdots & & & & \cdots & ai & \longleftrightarrow & j & \cdots
\end{array}
$$

Therefore, we have for each $i = 1, 2, ..., p-1$,

$$N_m(i,j) = N_0(i, a^{-m}j), \text{ for } j = 0, 1, 2, ..., p-1. \tag{14}$$

For $j = 0$, the relation (14) gives $N_m(i, 0) = N_0(i, 0)$, for all $i \neq 0$. This implies that the $3(p-1)$ entries of N_m and the corresponding entries of N_0 in the top row, left-most column, and main diagonal, except for the position $(0, 0)$ are all the same, because of (13).

Especially, we have

$$N_m(i, i) = N_0(i, i), \text{ for all } i = 1, 2, ..., p-1. \tag{15}$$

For $j = i$, the relation (14) gives $N_m(i, i) = N_0(i, a^{-m}i) = N_0(i, k)$ where $k = a^{-m}i$. This implies that, if now we let $k = a^{-m}i$ to be j, then

$$N_m(i, i) = N_0(i, j), \text{ for all } i = 1, 2, ..., p-1. \tag{16}$$

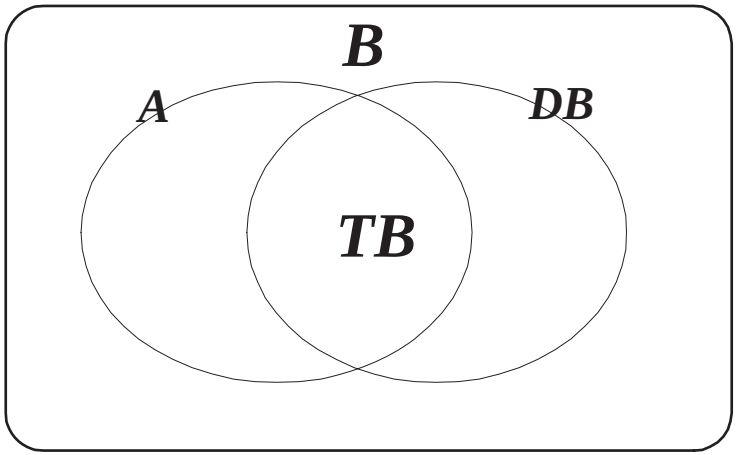
Combining the two relations (15) and (16), we finally have the equality $N_0(i, i) = N_0(i, j)$ for $j = a^{-m}i$. As m runs through the nonzero values mod p, $j = a^{-m}i$ runs also through the nonzero values mod p for any $i \neq 0$. Therefore, all the entries of N_0 must be the same as p^{n-2} except for the position $(0, 0)$, and $N_0(0, 0) = p^{n-2} - 1$.

IV. Summary

- We prove that if a q-ary sequence of period $q^n - 1$ is difference-balanced and has the 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 array structure.

- The conjecture is confirmed with respect to all of the known p-ary sequences which are difference-balanced, i.e., which have the ideal two-level autocorrelation function.



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

Figure 1: Hierarchy of Balanced q-ary Sequences of period $q^n - 1$

- With regard to Fig. 1, the conjecture implies that the set DB-A is empty. The set A-DB is trivially non-empty. This completes the classification of various classes of balanced q-ary sequences of period $q^n - 1$, for an odd prime power q.