Characterization and Construction of Ideal Waveforms

Myoung An and Richard Tolimieri
Prormetheus Inc.
17135 Front Beach Road, Unit 9
Panama City Beach, FL 32413 USA

Abstract

Using the finite Zak transform (FZT) periodic polyphase sequences satisfying the ideal cyclic autocorrelation property and sequence pairs satisfying the optimum cyclic cross correlation property are constructed. The Zak space correlation formula plays a major role in the design of signals having special correlation properties. Sequences defined by permutation matrices in Zak space always satisfy the ideal cyclic autocorrelation property. A necessary and sufficient condition on pairs of permutation matrices in Zak space such that the corresponding pairs of sequences satisfy the optimum cyclic correlation property is derived. This condition is given in terms of a collection of permutations, called $*$-permutations. The development is restricted to the case $N = L^2$, L an odd integer. An algorithm for constructing $*$-permutations is provided.

1 Introduction

In this work we use the finite Zak transform (FZT) to construct periodic polyphase sequences satisfying the ideal cyclic autocorrelation property and sequence pairs satisfying the optimum cyclic cross correlation property. In communication theory these sequences are called Z_q-sequences. Their correlation properties have been extensively studied in [1,2,3,5,8]. A detailed treatment of Z_q-sequences and their application to spread spectrum can be found in [4]. The approach in these works has the merit that it is direct.

The approach in this work is based on designing periodic sequences in Zak space (ZS). The ZS correlation formula plays a major role in the design of signals having special correlation properties.

Sequences defined by permutation matrices in ZS always satisfy the ideal cyclic autocorrelation property. The analogous result proved directly in communication theory can be found in [2,3]. We will derive a necessary and sufficient condition on pairs of permutation matrices in ZS such that the corresponding pairs of sequences satisfy the optimum cyclic correlation property. This condition is given in terms of a collection of permutations, called $*$-permutations. The development is restricted to the case $N = L^2$, L an odd integer. We will show examples and provide an algorithm for constructing $*$-permutations. We believe this concept to be new. The main consequence is that we can construct significantly larger collections of sequence pairs satisfying the optimal correlation property than those constructed in [5].

The following notation and elementary results will be used throughout this work. A vector $\mathbf{x} \in \mathbf{C}^N$ is written

$$\mathbf{x} = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix} = [x_n]_{0 \le n < N} .$$

We will also denote vectors in $\mathbf{C}^N$ by capitals such as X and Y. The inner product of two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{C}^N$ is

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{n=0}^{N-1} x_n y_n^*,$$

where $*$ denotes complex conjugation. $\mathbf{e}_n^N$, $0 \leq n < N$, is the vector in $\mathbf{C}^N$ having 1 in the n-th component and 0 in all other components. The set

$$\{\mathbf{e}_n^N : 0 \leq n < N\}$$

is an orthonormal basis of $\mathbf{C}^N$. The notation

$$\mathbf{xy}, \text{ and } XY$$

denotes the vector in $\mathbf{C}^N$ formed by the componentwise multiplication.

The trace of an $N \times N$ matrix $\mathbf{x}$ is

$$T_r \mathbf{x} = \sum_{n=0}^{N-1} \mathbf{x}_{n,n}.$$

F is the N-point Fourier transform matrix

$$F = [w^{mn}]_{0 \leq m,\, n < N}\,, \qquad w = e^{2\pi i \frac{1}{N}}.$$

The $N \times N$ time reversal matrix R_N is defined by

$$R_N \mathbf{x} = [x_{N-n}]_{0 \leq n < N}\,, \qquad N - n \text{ taken modulo } N.$$

F and R_N are related by

$$F R_N = R_N F = F^*$$

and

$$F^2 = N R_N.$$

We also have

$$R_N^2 = I_N, \quad \text{the identity matrix,}$$

and

$$F F^* = N I_N.$$

As a result

$$F^{-1} = N^{-1} F^*.$$

S_N is the $N \times N$ cyclic shift matrix defined by

$$S_N \mathbf{x} = [x_{N-1+n}]\,, \qquad \mathbf{x} \in \mathbf{C}^N.$$

D_N is the diagonal matrix defined by

$$D_N = Diag\left([w^n]_{0 \leq n < N} \right), \qquad w = e^{2\pi i \frac{1}{N}}.$$

An important result is

$$F S_N F^{-1} = D_N.$$

Linear combinations of vectors and matrices will be used. For example

$$\sum_{n=0}^{N-1} x_n D_N^n = Diag\,(F\mathbf{x})\,, \qquad \mathbf{x} \in \mathbf{C}^N.$$

$\mathbf{1}^N$ is the vector in $\mathbf{C}^N$ all of whose components are 1. $E(L,K)$ is the $L \times K$ matrix of all ones.

$Perm(N)$ is the group of permutations of the set

$$\{0,\ 1,\ \ldots,\ N-1\}.$$

An element $\pi \in Perm(N)$ is defined by

$$(\pi(0)\ \pi(1)\ \cdots\ \pi(N-1))\,.$$

If X is an $N \times N$ matrix

$$X = [X_0\ \cdots\ X_{N-1}]\,,$$

where X_n, $0 \le n < N$ is the n-th column vector of X, and for $\pi \in Perm(N)$ we define

$$X_\pi = \left[X_{\pi(0)}\ \cdots X_{\pi(N-1)}\right].$$

2 Cyclic Correlation

We identify $\mathbf{C}^N$ with the space of periodic complex sequences of period N.

For $\mathbf{x}$, $\mathbf{y} \in \mathbf{C}^N$ the *cyclic correlation* $\mathbf{v} = \mathbf{x} \circ \mathbf{y} \in \mathbf{C}^N$ is defined by

$$v_m = \sum_{n=0}^{N-1} x_n y_{n-m}^*.$$

$\mathbf{x} \circ \mathbf{x}$ is called the *cyclic autocorrelation* of $\mathbf{x}$, while if $\mathbf{x}$ and $\mathbf{y}$ are distinct, $\mathbf{x} \circ \mathbf{y}$ is called the *cyclic cross correlation* of $\mathbf{x}$ and $\mathbf{y}$.

A vector $\mathbf{x} \in \mathbf{C}^N$ satisfies the *ideal cyclic autocorrelation property* if

$$\mathbf{x} \circ \mathbf{x} = ||\mathbf{x}||^2 \mathbf{e}_0^N = ||\mathbf{x}||^2 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

where $||\mathbf{x}||$ is the norm of $\mathbf{x}$.

Set $\mathbf{v} = \mathbf{x} \circ \mathbf{y}$. If $\mathbf{x}$ and $\mathbf{y}$ satisfy the ideal cyclic autocorrelation property, then we must have [6]

$$|v_n| \le \frac{||\mathbf{x}||\,||\mathbf{y}||}{\sqrt{N}}, \qquad 0 \le n < N.$$

A pair of vectors $\mathbf{x}$, $\mathbf{y} \in \mathbf{C}^N$ satisfying the ideal cyclic autocorrelation property satisfies the optimum *cross correlation property* if

$$|v_n| = \frac{||\mathbf{x}||\,||\mathbf{y}||}{\sqrt{N}}, \qquad 0 \le n < N.$$

In this case we say that the pair $(\mathbf{x}, \mathbf{y})$ satisfies the *ideal cyclic correlation property.*

3 Zak space correlation formula

The finite Zak transform (FZT) of a vector determines a two-dimensional time-frequency representation of the vector called the *Zak space representation*. In this section we define the FZT and derive the ZS correlation formula.

$N = LK = L^2M$, L and M positive integers. Identify $\mathbf{C}^L \times \mathbf{C}^K$ with the space of $L \times K$ complex matrices. For $\mathbf{y} \in \mathbf{C}^N$ define the vectors $\mathbf{y}_k \in \mathbf{C}^L$, $0 \le k < K$, by

$$\mathbf{y}_k = [y_{k+lK}]_{0 \le l < L}, \qquad 0 \le k < K.$$

We called the vectors $\mathbf{y}_k$, $0 \le k < K$, the *decimated components* of $\mathbf{y}$. Define

$$M_L \mathbf{y} = [\mathbf{y}_0 \ \cdots \ \mathbf{y}_{K-1}].$$

M_L is a linear isomorphism from the one-dimensional space $\mathbf{C}^N$ onto the two-dimensional space $\mathbf{C}^L \times \mathbf{C}^K$. No computations are involved. It is simply a data rearrangement.

For the remainder of this work, F is the L-point Fourier transform matrix. Define

$$Z_L \mathbf{y} = F M_L \mathbf{y}, \qquad \mathbf{y} \in \mathbf{C}^N.$$

$Z_L \mathbf{y}$ is called the $L \times K$ *ZS representation* of $\mathbf{y}$. The mapping

$$Z_L : \mathbf{C}^N \longrightarrow \mathbf{C}^L \times \mathbf{C}^K$$

is called the $L \times K$ *finite Zak transform* (FZT). The FZT is, up to scalar factor L, a linear isometry from $\mathbf{C}^N$ onto $\mathbf{C}^L \times \mathbf{C}^K$.

Theorem 1 *If $\mathbf{x}$, $\mathbf{y} \in \mathbf{C}^N$ and $\mathbf{v} = \mathbf{x} \circ \mathbf{y}$, then*

$$V_0 = \sum_{m=0}^{K-1} X_m Y_m^*$$

and

$$V_k = D_L^{-1} \sum_{m=0}^{k-1} X_m Y_{K-(k-m)}^* + \sum_{m=k}^{K-1} X_m Y_{m-k}^*, \qquad 1 \le k < K,$$

where V_k is the k-th column of $Z_L \mathbf{v}$.

Example 1 $N = 9$ and $L = K = 3$.

$$\begin{aligned} V_0 &= X_0 Y_0^* + X_1 Y_1^* + X_2 Y_2^*, \\ V_1 &= D_3^{-1} X_0 Y_2^* + X_1 Y_0^* + X_2 Y_1^*, \\ V_2 &= D_3^{-1} (X_0 Y_1^* + X_1 Y_2^*) + X_2 Y_0^*. \end{aligned}$$

4 Permutation Waveforms

In this section we use the ZS correlation formula to derive correlation properties of signals whose ZS representations are permutation matrices. Set $N = L^2$, $E = I_L$ and

$$F = [F_0 \cdots F_{L-1}] .$$

Define $\mathbf{e}_\pi \in \mathbf{C}^N$ by

$$Z_L \mathbf{e}_\pi = E_\pi, \qquad \pi \in Perm(L).$$

Then

$$M_L \mathbf{e}_\pi = F^{-1} E_\pi = L^{-1} F_\pi^* .$$

In the following discussion set $\mathbf{1} = \mathbf{1}^L$ and $\mathbf{0} = \mathbf{0}^L$.

Consider $\pi \in Perm(L)$ and set $\mathbf{v} = \mathbf{e}_\pi \circ \mathbf{e}_\pi$. By the ZS correlation formula

$$V_0 = \sum_{m=0}^{L-1} E_{\pi(m)} E_{\pi(m)} = \sum_{m=0}^{L-1} E_{\pi(m)} = \mathbf{1}$$

and

$$V_k = D_L^{-1} \sum_{m=0}^{k-1} E_{\pi(m)} E_{\pi(m-k)} + \sum_{m=k}^{L-1} E_{\pi(m)} E_{\pi(m-k)}, \qquad 1 \leq k < L,$$

where $m - k$ is taken modulo L. Since

$$E_{\pi(m)} E_{\pi(m-k)} = \mathbf{0}, \qquad 1 \leq k < L,$$

we have $V_k = 0$, $1 \leq k < L$, proving the following result.

Theorem 2 *If $\pi \in Perm(L)$, then*

$$Z_L (\mathbf{e}_\pi \circ \mathbf{e}_\pi) = [\mathbf{1}\, \mathbf{0} \cdots \mathbf{0}]$$

and $\mathbf{e}_\pi$ satisfies the ideal cyclic autocorrelation property.

5 $*$-Permutations

In this section we determine a necessary and sufficient algebraic condition on a permutation pair (π, σ) such that $(\mathbf{e}_\pi, \mathbf{e}_\sigma)$ satisfies the ideal cyclic correlation property. This condition is given in terms of a collection of permutations, the $*$-permutations. For an odd integer L the collection of $*$-permutations is nonempty. Details are given in the next section. For even L it is likely, but not proved, that the collection of $*$-permutations is the empty set.

Suppose $\gamma \in Perm(L)$, and define the subsets

$$\Delta_k(\gamma) = \{0 \leq m < L : m = \gamma(m - k)\}, \qquad 0 \leq k < L,$$

where $m - k$ is taken modulo L. Setting

$$E_\gamma = \left[E_{\gamma(0)} \ \cdots \ E_{\gamma(L-1)}\right],$$

we have

$$Tr\left(E_\gamma S_L^{-k}\right) = o\left(\Delta_k(\gamma)\right), \qquad 0 \leq k < L.$$

Theorem 3 *For $\gamma \in Perm(L)$,*

$$L = \sum_{k=0}^{L-1} o\left(\Delta_k(\gamma)\right).$$

Proof By linearity of Tr

$$\sum_{k=0}^{L-1} Tr\left(E_\gamma S_L^{-k}\right) = Tr\left(E_\gamma \sum_{k=0}^{L-1} S_L^{-k}\right) = Tr\left(E_\gamma I(L,L)\right),$$

where $I(L,L)$ is the $L \times L$ matrix of all ones. The theorem follows from

$$Tr\left(E_\gamma I(L,L)\right) = Tr(I(L,L)) = L.$$

The following corollary will be useful in describing the sets $\Delta_k(\gamma)$, $0 \le k < L$, when γ is a $*$-permutation.

Corollary 1 *For $\gamma \in Perm(L)$, $o\left(\Delta_k(\gamma)\right) > 0$, $0 \le k < L$, if and only if $o\left(\Delta_k(\gamma)\right) = 1$, $0 \le k < L$.*

For any γ_1, $\gamma_2 \in Perm(L)$, define $\gamma_1 + \gamma_2$ by

$$(\gamma_1 + \gamma_2)(r) \equiv \gamma_1(r) + \gamma_2(r) \bmod L, \qquad 0 \le r < L.$$

$\gamma_1 + \gamma_2$ is a mapping from $\mathbf{Z}/L$ into itself, but is not necessarily a permutation.

Denote the identity permutation in $Perm(L)$ by π_0. γ is called a *$*$-permutation* if $\pi_0 - \gamma$ is a permutation. Since

$$(\pi_0 - \gamma)\,\gamma^{-1} = -\left(\pi_0 - \gamma^{-1}\right),$$

γ is a $*$-permutation if and only if γ^{-1} is a $*$-permutation.

For odd L, there always exist $*$-permutations. The mapping

$$\gamma(n) \equiv 2n \bmod L, \qquad 0 \le n < L,$$

is a $*$-permutation.

For the rest of this section γ is a $*$-permutation. Since γ^{-1} is a $*$-permutation

$$\pi_{\mathbf{m}} = \left(\pi_0 - \gamma^{-1}\right)^{-1}$$

is a permutation, where $\pi_{\mathbf{m}} = (m_0\ m_1\ \cdots m_{L-1})$. $\pi_{\mathbf{m}}$ satisfies

$$\pi_{\mathbf{m}} - \pi_0 = \gamma^{-1}\pi_{\mathbf{m}}$$

and $\pi_{\mathbf{m}}$ is a $*$-permutation. This means

$$m_k - k \equiv \gamma^{-1}\left(m_k\right) mod\ L$$

and

$$m_k = \gamma\left(m_k - k\right), \qquad 0 \le k < L,$$

which by Theorem 3 implies the following result.

Theorem 4 *If γ is a $*$-permutation, then*

$$\Delta_k(\gamma) = \{m_k\}, \quad 0 \leq k < L.$$

The converse of Theorem 4 is also true. Suppose $\sigma \in Perm(L)$ and

$$\Delta_k(\sigma) = \{r_k\}, \quad 0 \leq r < L.$$

r_k is the unique solution of

$$r \equiv \sigma(r-k) \bmod L, \quad 0 \leq k < L.$$

This implies that

$$r_k \neq r_j, \quad 0 \leq j,\ k < L, \quad k \neq j,$$

and we can form the permutation

$$\pi_{\mathbf{r}} = (r_0\ r_1\ \cdots r_{L-1})\,.$$

$\pi_{\mathbf{r}}$ satisfies $\pi_{\mathbf{r}} = \sigma\left(\pi_{\mathbf{r}} - \pi_0\right)$ implying

$$\pi_{\mathbf{r}}^{-1} = \pi_0 - \sigma^{-1}.$$

Since $\pi_{\mathbf{r}}^{-1}$ is a permutation, σ^{-1} and σ are $*$-permutations, proving the converse.

Theorem 5 *Suppose π, $\sigma \in Perm(L)$ and $\gamma = \pi^{-1}\sigma$. The sequence pair $(\mathbf{e}_\pi, \mathbf{e}_\sigma)$ satisfies the ideal correlation property if and only if γ is a $*$-permutation.*

Set Λ_L equal to the set of $*$-permutations in $Perm(L)$. For $\sigma \in \Lambda_L$ the set of pairs of permutations

$$\Lambda_L(\sigma) = \{(\pi, \pi\sigma) : \pi \in Perm(L)\}$$

determines a set of pairs of sequences

$$\{(\mathbf{e}_\pi, \mathbf{e}_{\pi\sigma}) : \pi \in Perm(L)\}$$

satisfying the ideal cyclic correlation property.

Suppose $N = LK = L^2R$, L an odd positive integer, R a positive integer. Define $\mathbf{x} \in \mathbf{C}^N$ by

$$Z_L\mathbf{x} = [E_\pi\ \ldots\ E_\pi]\, D,$$

where E_π is the $L \times L$ permutation matrix corresponding to $\pi \in Perm(L)$ and D is a $K \times K$ diagonal matrix whose diagonal entries have absolute value one.

Theorem 6 *Suppose $\pi \in Perm(L)$ and $\mathbf{x} \in \mathbf{C}^N$ satisfies*

$$Z_L\mathbf{x} = [E_\pi\ \ldots\ E_\pi]\, D,$$

where D is a $K \times K$ diagonal matrix whose diagonal entries have absolute value one. Then $\mathbf{x}$ satisfies the ideal cyclic autocorrelation property if and only if, for $0 \leq s < L$ and $1 \leq r < R$,

$$v^{-\pi(s)} \sum_{t=0}^{r-1} d_{tL+s} d^*_{(K+t-r)Ls} + \sum_{t=r}^{R-1} d_{tL+s} d^*_{(t-r)L+s} = 0,$$

where $v = e^{2\pi i \frac{1}{L}}$.

Example 2 $\pi = \pi_0$, $R = 2$. The condition in Theorem 6 is

$$v^{-s} d_s d_{L+s}^* + d_{L+s} d_s^* = 0, \qquad v = e^{2\pi L \frac{1}{L}}.$$

Choose $d_0, \ldots, d_{L-1}$ arbitrarily having absolute value one. The diagonal entries $d_{L+s}, 0 \le s < L$, must satisfy

$$v^{-s} d_s d_{L+s}^* + d_s^* d_{L+s} = 0, \qquad 0 \le s < L.$$

One class of solutions is given by setting

$$d_{L+s} = e^{-2\pi i \frac{s}{2L}} i d_s, \qquad 0 \le s < L.$$

6 Golay pairs

Suppose π, $\sigma \in Perm(L)$ such that $\gamma = \pi^{-1}\sigma$ is a $*$-permutation. Define $\mathbf{x} \in \mathbf{C}^N$, $N = L^2$, by

$$Z_L \mathbf{x} = E_\pi + E_\sigma$$

and set $\mathbf{v} = \mathbf{x} \circ \mathbf{x}$. The problem is to determine the collection of all permutation pairs (π_1, σ_1), π_1, $\sigma_1 \in Perm(L)$ such that $\gamma_1 = \pi_1^{-1}\sigma_1$ is a $*$-permutation and

$$\mathbf{v}^1 = \mathbf{x}^1 \circ \mathbf{x}^1 = \mathbf{v},$$

where $\mathbf{x}^1 \in \mathbf{C}^N$ is defined by

$$Z_L \mathbf{x}^1 = E_{\pi_1} + E_{\sigma_1}.$$

Given such a permutation pair (π_1, σ_1), the pair $(\mathbf{x}, \mathbf{y})$, where

$$Z_L \mathbf{y} = E_{\pi_1} - E_{\sigma_1},$$

is a Golay pair.

Write

$$\pi_{\mathbf{m}} = \left(\pi_0 - \gamma^{-1}\right)^{-1}, \qquad \pi_{\mathbf{n}} = \left(\pi_0 - \gamma\right)^{-1}$$

and

$$\pi_{\mathbf{m}^1} = \left(\pi_0 - \gamma_1^{-1}\right)^{-1}, \qquad \pi_{\mathbf{n}^1} = \left(\pi_0 - \gamma_1\right)^{-1}.$$

As in Section 5, the sum and difference of permutations is taken modulo L. We will have $\mathbf{v} = \mathbf{v}^1$ if the following two conditions are satisfied.

A. $\pi(m_k) = \pi_1(m_k^1)$ and $\pi(n_k - k) = \pi_1(n_k^1 - k)$, $0 \le k < L$.

B. $0 \le m_k < k$ if and only if $0 \le m_k^1 < k$ and $0 \le n_k < k$ if and only if $0 \le n_k^1 < k$, $0 \le k < L$.

We can have $\mathbf{v} = \mathbf{v}^1$ under other conditions, but we will only discuss this case.

Given a permutation pair (π, σ) such that $\gamma = \pi^{-1}\sigma$ is a $*$-permutation, we say that a permutation pair (π_1, σ_1), such that $\gamma_1 = \pi_1^{-1}\sigma_1$ is a $*$-permutation satisfies *condition* A with respect to (π, σ) if

$$\pi\pi_{\mathbf{m}} = \pi_1\pi_{\mathbf{m}^1} \text{ and } \pi(\pi_n - \pi_0) = \pi_1(\pi_{\mathbf{n}^1} - \pi_0).$$

This statement is equivalent to condition A above.

Algorithm A (π, σ) is a permutation pair such that $\pi^{-1}\sigma$ is a $*$-permutation. The algorithm computes a permutation pair (π_1, σ_1) such that $\pi_1^{-1}\sigma_1$ is a $*$-permutation and (π_1, σ_1) satisfies condition A with respect to (π, σ)

- Compute $\delta_1 = \pi^{-1} - \sigma^{-1}$. Since $\pi^{-1}\sigma$ is a $*$-permutation, δ_1 is a permutation.
- Compute $\delta_2 \in Perm(L)$ such that $\delta_2\delta_1^{-1}$ is a $*$-permutation.
- Compute $\sigma_1^{-1} = -\delta_2$.
- Compute $\pi_1^{-1} = \delta_1 - \delta_2$. Since $\delta_2\delta_1^{-1}$ is a $*$-permutation, π_1^{-1} is a permutation.

Example 3 $L = 5$, $u = 2$ and $v = 1$. The permutation pair (γ_3, γ_4) satisfies condition A with respect to (γ_1, γ_2). Since

$$\pi_{\mathbf{m}} = \gamma_2 \text{ and } \pi_{\mathbf{m}^1} = \gamma_4,$$

we have the following table.

k	m_k	m_k^1	$\pi_1\left(m_k^1\right)$
0	0	0	0
1	2	4	2
2	4	3	4
3	1	2	1
4	3	1	3

Example 4 $L = 5$, $u = 2$ and $v = 4$. The permutation pair (γ_4, γ_1) satisfies condition A with respect to (γ_1, γ_2). Since

$$\pi_{\mathbf{m}} = \gamma_2 \text{ and } \pi_{\mathbf{m}^1} = \gamma_3,$$

we have the following table.

k	m_k	m_k^1	$\pi_1\left(m_k^1\right)$
0	0	0	0
1	2	3	2
2	4	1	4
3	1	4	1
4	3	2	3

A modification of algorithm A is convenient for dealing with the construction of permutation pairs satisfying condition B.

Algorithm A1 Consider a permutation pair (π, σ) such that $\pi^{-1}\sigma$ is a $*$-permutation and a $*$-permutation $\pi_{\mathbf{m}^1}$. The algorithm constructs a permutation pair (π_1, σ_1) such that $\pi_1^{-1}\sigma_1$ is a $*$-permutation,

$$\pi_{\mathbf{m}^1} = \left(\pi_0 - \sigma_1^{-1}\pi_1\right)^{-1}$$

and

$$\pi\pi_{\mathbf{m}} = \pi_1\pi_{\mathbf{m}^1}.$$

- Compute $\pi_1 = \pi\pi_{\mathbf{m}}\pi_{\mathbf{m}^1}^{-1}$.
- Compute $\sigma_1 = \pi_1\pi_{\mathbf{m}^1}\left(\pi_{\mathbf{m}^1} - \pi_0\right)^{-1}$.

Since $\pi_{\mathbf{m}^1}$ is a $*$-permutation, σ_1 is a well-defined permutation.

Theorem 7 *For* $0 \leq k < L$,

$$0 \leq m_k < k \text{ if and only if } L - k \leq n_{L-k} < L.$$

Choosing the $*$*-permutation* $\pi_{\mathbf{m}^1}$ *in algorithm A1 such that, for* $0 \leq k < L$,

$$0 \leq m_k < k \text{ if and only if } 0 \leq m_k^1 < k,$$

the permutation pair (π_1, σ_1) *constructed in algorithm A1 satisfies condition A and condition B with respect to* (π, σ).

References

1. D.C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Trans. Inf. Theory* **IT**(18), 531-532, 1972.

2. R. Frank and S. Zadoff, "Phase shift pulse codes with good periodic correlation properties," *IEEE Trans. Inform. Theory* **IT-19**, 244, 1973.

3. R.C. Heimiller, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Inf. Theory* **IT**(7), 254-257, 1961.

4. W. H. Mow, *Sequence Design for Spread Spectrum*, Chinese University Press, Hong Kong, 1995.

5. B.M. Popovic, "Generalized chirp-like polyphase sequences with optimum correlation properties," *IEEE Trans. Inf. Theory* **IT**(38)