A Note on Periodic Complementary Binary Sequences

Cantian Lin
Department of Mathematical Sciences
University of Nevada, Las Vegas
Las Vegas, NV 89154

J.L. Selfridge
Department of Mathematical Sciences
Northern Illinois University
Dekalb, IL 60115

Peter Jau-Shyong Shiue
Department of Mathematical Sciences
University of Nevada, Las Vegas
Las Vegas, NV 89154

ABSTRACT. A simple new proof of an existence condition for periodic complementary binary sequences is given. In addition, this result is extended to the general case, which is previously unsolved.

Let a be a binary sequence of length (period) n with elements $a(j)$ chosen from $\{1, -1\}$. The periodic autocorrelation function $\tilde{\phi}_{aa}(k)$ is defined by

$$\tilde{\phi}_{aa}(k) = \sum_{j=0}^{n-1} a(j)a(j+k) \text{ for } k = 0, 1, 2, \ldots, n-1. a(n+j) := a(j)$$

The set of sequences $\{a_i : 0 \leq i \leq q-1\}$ each of length n is called a set of periodic complementary sequences, denoted by $PCS_q^n(a_i)$ or PCS if

$$\sum_{i=0}^{q-1} \tilde{\phi}_{a_i a_i}(k) = \begin{cases} nq & \text{if } k = 0 \\ 0 & \text{if } k \neq 0 \end{cases}.$$

i.e.

$$\sum_{i=0}^{q-1} \sum_{j=0}^{n-1} a_i(j)a_i(j+k) = \begin{cases} nq & \text{if } k = 0 \\ 0 & \text{if } k \neq 0 \end{cases}.$$

Because of important applications in communications, PCS have been extensively investigated. For general background, see [1] and [2]. A diagram providing a general view of PCS up to length 50 and up to 12 sequences was given by Bomer and Antweiler in [2]. Existence conditions for PCS with $q = 2$ and 3 were given by Arasu and Xiang in [1].

In this note, a simple new proof of an existence condition which is given by Arasu and Xiang in [1], is given and this result is extended to the general case, a result not previously known.

Suppose there is a $PCS_q^n(a_i)$. Let A_i denote the circulant matrix of order n whose initial row consists of the elements of a_i. Then the equation

$$\sum_{i=0}^{q-1} A_i A_i^T = nqI_n$$

is precisely equivalent to

$$\sum_{i=0}^{q-1} \tilde{\phi}_{a_i a_i}(k) = \begin{cases} nq & \text{if } k = 0 \\ 0 & \text{if } k \neq 0 \end{cases}$$

Suppose $r_i = \sum_{j=0}^{n-1} a_i(j)$ $(i = 0, 1, 2, \ldots, q-1)$. By the circulant matrix property we have

$$A_i J = r_i J$$
$$A_i^T J = r_i J$$

where J is the matrix of order n with all elements $+1$. Thus, we immediately get

$$\left(\sum_{i=0}^{q-1} A_i A_i^T\right) J = (nqI_n)J$$

i.e.

$$\sum_{i=0}^{q-1} (r_i^2 J) = nqJ.$$

This gives

$$\left(\sum_{i=0}^{q-1} r_i^2\right) J = (nq)J.$$

From the definition of J, we have

$$\sum_{i=0}^{q-1} r_i^2 = nq.$$

i.e. nq is a sum of q squares. We have the following result.

Theorem 1. *If there is a $PCS_q^n(a_i)$, then nq is a sum of q squares.*

Corollary 1. *If there is a $PCS_q^n(a_i)$ where n is an odd integer, then nq is a sum of q nonzero integral squares.*

Proof: By the definition of r_i, r_i is an odd integer when n is an odd integer. □

As a by-product, we give the existence condition for a *perfect binary array* by showing the relationship between PCS and perfect binary arrays.

$[b(i,j)]$ is called a perfect binary array, where $b(i,j) = +1$ for $i = 0,1,\ldots,q-1$, $j = 0,1,\ldots,n-1$, if

$$\sum_{i=0}^{q-1}\sum_{j=0}^{n-1} b(i,j)b(i+l,j+k) = \begin{cases} nq & \text{if } l=0, k=0 \\ 0 & \text{otherwise.} \end{cases}$$

$$b(q+i,n+j) := b(i,j)$$

For general information on perfect binary arrays, we refer to [3]. In [2], perfect binary arrays have been used to construct PCS. It is easy to verify that if $b(i,j)$ is a perfect binary array, then

$$\{(b(i,0), b(i,1), \ldots, b(i,n-1))|i = 0,1,\ldots,q-1\}$$
$$\{b(0,j), b(1,j), \ldots, b(q-1,j)|j = 0,1,\ldots,n-1\}$$

are two PCS. Thus, the dimensions of perfect binary array must satisfy the existence conditions for PCS. Therefore, we have the following corollary.

Corollary 2. *If there is a perfect binary array $[b(i,j)]$, where $b(i,j) = \pm 1$ for $i = 0,1,\ldots,q-1$, $j = 0,1,\ldots,n-1$, then nq is a sum of n squares and nq is also a sum of q squares.*

We will use Theorem 1 to give a simple new proof of the existence conditions for PCS with $q = 2$ and 3 given by Arasu and Xiang in [1].

Theorem 2 (see [1]). *If there is a $PCS_2^n(a_i)$, then n is a sum of 2 squares, i.e. every prime divisor of n of the form $4t+3(t>0)$ appears with an even exponent in the prime power decomposition of n.*

Proof: If there is a$PCS_2^n(a_i)$ where $q = 2$, by Theorem 1, $2n$ is a sum of 2 squares. Thus, $2n = r_0^2 + r_1^2$ or $n = \left(\frac{r_0+r_1}{2}\right)^2 + \left(\frac{r_0-r_1}{2}\right)^2$. Since $r_0^2 + r_1^2$ is even, r_0 and r_1 are both even or both odd. Thus $\frac{r_0+r_1}{2}$ and $\frac{r_0-r_1}{2}$ are integers. □

Theorem 3 (see [1]). *There is no $PCS_3^n(a_i)$ with $n = 4^h(8r+5)$, $h \geq 0$, $r \geq 0$.*

Proof: It is well known that for any $h \geq 0$ and $t \geq 0$, $4^h(8t+7)$ is not the sum of three squares of integers. Thus if $n = 4^h(8r+5)$, $3n = 4^h(24r+15) = 4^h(8(3r+1)+7)$ and $3n$ is not the sum of three squares. By Theorem 1, there is no such $PCS_3^n(a_i)$. □

According to Theorem 1, to determine whether a PCS_q^n (for $q \geq 4$) exists or not, we shall need the following propositions. Propositions 1 to 3 all follow easily from the fact that if $m \equiv 3$ or $6 \pmod 8$ or $m \equiv 12$ or $24 \pmod{32}$ then m is the sum of three nonzero squares.

Proposition 1.

$$\begin{array}{llll} \textit{If} & m \equiv 4 & \pmod 8 & \\ \textit{or} & m \equiv 7 & \pmod 8 & \\ \textit{or} & m \equiv 3 & \pmod 8 & (m > 11) \\ \textit{or} & m \equiv 2 & \pmod 4 & (m > 6\ m \neq 14) \\ \textit{or} & m \equiv 1 & \pmod 4 & (m > 9\ m \neq 17, 29, 41), \end{array}$$

then m can be represented as a sum of 4 nonzero integral squares. If $m \equiv 0 \pmod 8$, m can be so represented if and only if $m/4$ can be so represented.

Proposition 2.

$$\begin{array}{llll} \textit{If} & m \equiv 2 & \pmod 3 & (m > 2) \\ \textit{or} & m \equiv 1 & \pmod 3 & (m > 10) \\ \textit{or} & m \equiv 0 & \pmod 3 & (m > 18\ m \neq 33), \end{array}$$

then m can be represented as a sum of 5 nonzero integral squares, otherwise not.

Proposition 3. *Suppose $k \geq 6$.*

$$\begin{array}{llll} \textit{If} & m \equiv 1 & \pmod 3 & (m > k-3) \\ \textit{or} & m \equiv k-1 & \pmod 3 & (m > k+5) \\ \textit{or} & m \equiv k+1 & \pmod 3 & (m > k+13), \end{array}$$

then m can be represented as a sum of k nonzero integral squares, otherwise not.

To determine whether a PCS_q^n exists, we check if nq can be represented as a sum of L nonzero integral squares for $L = q, q-1, q-2, \ldots, 4, 3, 2$. If nq cannot be represented as a sum of L nonzero integral squares for $L = q, q-1, q-2, \ldots, 4, 3, 2$, then there is no such $PCS_q^n(a_i)$ by Theorem 1 and Propositions 1-3. If nq can be represented as a sum of m nonzero integral squares for some integer m, then one could use computer to search the existence of PCS_q^n.

Remarks

Although by the well-known Lagrange Theorem an integer m can be represented as a sum of four integral squares, m might not be representable as a sum of $k \geq 4$ nonzero integral squares by Propositions 1-3. In particular, when n is an odd integer and there is a $PCS_q^n(a_i)$, then nq is a sum of q nonzero integral squares, which is not a trivial generalization of the Lagrange Theorem by adding zero squares.

Acknowledgement

The authors thank the referee for the useful comments and suggestions on an earlier manuscript of this paper.

References

[1] K.T. Arasu and Qing Xiang, On the Existence of Periodic Complementary Binary Sequences, *Designs, Codes, and Cryptography*, 2(1992), 257–262.

[2] L. Bomer and M. Antweiler, Periodic Complementary Binary Sequences, *IEEE Trans. Inform. Theory*, 35(1990), 1487–1494.

[3] Y.K. Chan, M.K. Siu and P. Tong, Two-dimensional binary arrays with good autocorrelation, *Information and Control*, 42(1979), 125–130.