Discrete Mathematics 93 (1991) 143–154
North-Holland

Combinatorial designs with Costas arrays properties

Tuvi Etzion*

Computer Science Department, Technion, Haifa, Israel

Received 25 May 1989

Abstract

Etzion, T., Combinatorial designs with Costas arrays properties, Discrete Mathematics 93 (1991) 143–154.

Several constructions for 0–1 three-dimensional arrays, in which some of the two-dimensional subarrays have 'good' two-dimensional autocorrelation function values, i.e., the vectors connecting two 1's in the matrix are all distinct as vectors, are given. Some of those constructions lead to constructions of Vatican squares in which each symbol defines a Costas array.

1. Introduction

Many problems arising from radar, sonar, physical alignment, and time-position synchronization can be formulated in terms of finding one-dimensional or two-dimensional synchronization patterns with 'good' autocorrelation functions. The one-dimensional case and its applications was discussed in detail in [1]. The two-dimensional case includes Sonar sequences [2, 4–6, 9], and Costas arrays [2, 7, 9–10]. In this paper we discuss three-dimensional arrays in which the two-dimensional subarrays have Costas arrays properties.

In the sequel let $A(i, j)$ denote the value of the matrix A in row i and column j. Let $A(i, j, k)$ denote the value of the cube A in row i and column j in the kth two-dimensional subarray of the third direction. Let $A(*, *, k)$ denote the kth two-dimensional subarray of the third direction.

A *Costas array* of order n is an $n \times n$ 0–1 permutation matrix with the property that the $\binom{n}{2}$ vectors connecting two 1's of the matrix are all distinct as vectors. A *near-Costas array* of order n is an $n \times n$ 0–1 matrix with $n-1$ 1's, where in exactly one row and one column there is no 1, and the $\binom{n-1}{2}$ vectors connecting

* This research was supported in part by the Office of Naval Research under Contract N00014-84-K-0189. This work was done while the author was with the Department of Electrical Engineering-Systems, University of Southern California, Los Angeles, CA 90089-0272, USA.

0012-365X/91/$03.50

two 1's of the matrix are all distinct as vectors. There are three essential known constructions of Costas arrays [7].

The Welch Construction. Let α be a primitive root modulo the prime p. Then construct the $(p-1)\times(p-1)$ matrix A, with $A(i,j)=1$ if and only if $\alpha^j \equiv i \pmod p$, $1 \leqslant i, j \leqslant p-1$.

The Lempel Construction. Let α be a primitive element in the field GF(q). Then construct the $(q-2)\times(q-2)$ matrix A, with $A(i,j)=1$ if and only if $\alpha^i+\alpha^j=1$, $1 \leqslant i, j \leqslant q-2$.

The Golomb Construction. Let α and β be primitive elements in the field GF(q). Then construct the $(q-2)\times(q-2)$ matrix A, with $A(i,j)=1$ if and only if $\alpha^i+\beta^j=1$, $1 \leqslant i, j \leqslant q-2$.

All the other known constructions are special ones or modifications of those three by deleting rows and columns or by adding rows and columns with 1's in the corners [10].

In Section 2 we will generate cubes for which in some of the directions each two-dimensional subarray is a Costas array or a near-Costas array, and in the other directions each two-dimensional subarray is a permutation matrix. For this we define four types of cubes.

A cube is called *ADNC* (*All Directions Near-Costas*) if all its two-dimensional subarrays are near-Costas arrays.

A cube is called *ODC* (*One Direction Costas*) if in one of its directions all the two-dimensional subarrays are Costas arrays, and in the other two directions all the two-dimensional subarrays are permutation matrices.

A cube is called *TDC* (*Two Directions Costas*) if in two of its directions all the two-dimensional subarrays are Costas arrays.

A cube is called *ADC* (*All Directions Costas*) if all its two-dimensional subarrays are Coastas arrays.

In the TDC cubes it can be verified that all the subarrays in the third direction are permutation matrices. A stronger result is the following lemma.

Lemma 1. *In a cube A of order n all the two-dimensional subarrays are permutation matrices if and only if for each c,* $1 \leqslant c \leqslant n$, $A(*,*,c)$ *and* $A(*,c,*)$ *are permutation matrices of order n.*

Proof. Since each line (row or column) is a line in exactly two projections, then either in all the projections all the matrices are permutation matrices, or in one or zero projections all the matrices are permutation matrices. □

A *Latin square* of order n is an $n \times n$ matrix such that each row and each column is a permutation of the integers $1, 2, \ldots, n$. A comprehensive work on Latin squares can be found in [3]. A Latin square in which each symbol defines a Costas array will be called an *LC* (Latin Costas) square. The following lemma can be easily verified.

Lemma 2. *An ODC cube of order n exists if and only if an LC square of order n exists.*

One kind of Latin squares are the *Vatican squares* defined in [11]. In a Vatican square for each d, $1 \leq d \leq n-1$, all the ordered pairs of the form $(A(i, j), A(i, j+d))$, $1 \leq i \leq n$, $1 \leq j \leq n-d$, are distinct. A Vatican square in which each symbol defines a Costas array will be called a *VC* (Vatican Costas) square.

In Section 3 we give some constructions for VC squares and compare between those constructions. All the constructions in Sections 2 and 3 have some similarity to the known constructions of Costas arrays.

In Section 4 we give some examples from a computer search. Also some unsolved problems are presented with some conjectures.

2. Constructions of three-dimensional arrays

All the constructions in this section involve the use of primitive elements in finite fields.

Construction A. Let α, β and γ be primitive element in the field $\mathrm{GF}(q)$, for any $q > 2$, and let x, y, and z be integers in the range between 0 and $q-2$. Then construct the $(q-1) \times (q-1) \times (q-1)$ cube A, with $A(i, j, k) = 1$ if and only if $\alpha^{i+x} + \beta^{j+y} + \gamma^{k+z} = 0$, $1 \leq i, j, k \leq q-1$.

Theorem 1. *Construction A generates an ADNC cube.*

Proof. It is easily verified that the definition of Construction A gives a cube where in each two-dimensional subarray there are $q-2$ 1's with no two 1's in the same row or the same column. For each c, $1 \leq c \leq q-1$, and the two-dimensional matrix defined by $\alpha^{i+x} + \beta^{j+y} + \gamma^{c+z} = 0$, we may write $j = \log_\beta(-\gamma^{c+z} - \alpha^{i+x}) - y$. If the matrix is not a near-Costas array, we can find two pairs of points in it as follows:

$$\{(i, \log_\beta(-\gamma^{c+z} - \alpha^{i+x}) - y),\ (i+m, \log_\beta(-\gamma^{c+z} - \alpha^{i+m+x}) - y)\};$$

$$\{(l, \log_\beta(-\gamma^{c+z} - \alpha^{l+x}) - y),\ (l+m, \log_\beta(-\gamma^{c+z} - \alpha^{l+m+x}) - y)\}$$

where the corresponding vectors

$$\left(m, \log_\beta \frac{-\gamma^{c+z} - \alpha^{i+m+x}}{-\gamma^{c+z} - \alpha^{i+x}}\right) \quad \text{and} \quad \left(m, \log_\beta \frac{-\gamma^{c+z} - \alpha^{l+m+x}}{-\gamma^{c+z} - \alpha^{l+x}}\right)$$

are equal, with $1 \leqslant m \leqslant q-2$. But this requires each of the following:

$$\log_\beta \frac{\gamma^{c+z} + \alpha^{i+m+x}}{\gamma^{c+z} + \alpha^{i+x}} = \log_\beta \frac{\gamma^{c+z} + \alpha^{l+m+x}}{\gamma^{c+z} + \alpha^{l+x}},$$

$$\frac{\gamma^{c+z} + \alpha^{i+m+x}}{\gamma^{c+z} + \alpha^{i+x}} = \frac{\gamma^{c+z} + \alpha^{l+m+x}}{\gamma^{c+z} + \alpha^{l+x}},$$

$$\gamma^{c+z}\alpha^x(\alpha^m - 1)\alpha^i = \gamma^{c+z}\alpha^x(\alpha^m - 1)\alpha^l,$$

and since $\gamma^{c+z}\alpha^x(\alpha^m - 1) \neq 0$, this requires $\alpha^i = \alpha^l$, and hence $i = l$. The same claims are true for all the two-dimensional subarrays and therefore each two-dimensional subarray of the cube of Construction A, defines a near-Costas array. □

Construction B. Let α and β be primitive roots modulo the prime p, for any $p > 2$, and let x and y be integers in the range between 0 and $p-2$. Then construct the $(p-1) \times (p-1) \times (p-1)$ cube A, with $A(i, j, k) = 1$ if and only if $\alpha^{i+x} + \beta^{j+y} \equiv k \pmod p$, $1 \leqslant i, j, k \leqslant p-1$.

Theorem 2. *Construction B generates an ADNC cube.*

Proof. It is easily verified that the definition of Construction B gives a cube in which for each two-dimensional subarray there are $p-2$ 1's with no two 1's in the same row or the same column. For each c, $1 \leqslant c \leqslant p-1$, if the two-dimensional matrix defined by $\alpha^{i+x} + \beta^{c+y} \equiv k \pmod p$, $1 \leqslant i, k \leqslant p-1$, is not a near-Costas array, we can find two pairs of points in it as follows:

$$\{(i, \alpha^{i+x} + \beta^{c+y}), (i+m, \alpha^{i+m+x} + \beta^{c+y})\},$$

$$\{(l, \alpha^{l+x} + \beta^{c+y}), (l+m, \alpha^{l+m+x} + \beta^{c+y})\}$$

where the corresponding vectors

$$(m, \alpha^{i+m+x} - \alpha^{i+x}) \quad \text{and} \quad (m, \alpha^{l+m+x} - \alpha^{l+x})$$

are equal, with $1 \leqslant m \leqslant p-1$. But this requires

$$\alpha^x(\alpha^m - 1)\alpha^i = \alpha^x(\alpha^m - 1)\alpha^l,$$

and since $\alpha^x(\alpha^m - 1) \not\equiv 0 \pmod p$, we must have $i = l$. Hence the corresponding two-dimensional subarrays are near-Costas arrays. In a proof similar to the proof of Theorem 1 we can show that the other two-dimensional subarrays are near-Costas arrays. □

A singly periodic Costas array is an $n \times \infty$ pattern such that each $n \times n$ subarray of it is a Costas array.

Construction C. Let B be an $n \times \infty$ singly periodic Costas array. Then construct the $n \times n \times n$ cube A, with $A(i, j, k) = 1$ if and only if $B(i, j+k) = 1$, $1 \leq i, j, k \leq n$.

Theorem 3. *Construction C generates a TDC cube.*

Proof. It is easily verified that for each c, $1 \leq c \leq n$, the columns of $A(*, *, c)$ are the consecutive columns from $c+1$ to $c+n$ of B, and since B is singly periodic Costas array $A(*, *, c)$ forms a Costas array. In a similar proof we can show that for each c, $1 \leq c \leq n$, $A(*, c, *)$ is a Costas array. By Lemma 1, for each c, $1 \leq c \leq n$, $A(c, *, *)$ is a permutation matrix. □

The only known singly periodic Costas arrays are those of the Welch Construction. The formal construction of TDC cubes from those singly periodic Costas arrays is given in Construction C1.

Construction C1. Let α be a primitive root modulo the prime p. Then construct the $(p-1) \times (p-1) \times (p-1)$ cube A, with $A(i, j, k) = 1$ if and only if $\alpha^{i+j} \equiv k \pmod{p}$, $1 \leq i, j, k \leq p-1$.

Construction D. Let α be a primitive root modulo the prime p. Then for each d, $0 \leq d \leq p-2$, construct the $(p-1) \times (p-1) \times (p-1)$ cube A, with $A(i, j, k) = 1$ if and only if $jk \equiv \alpha^{i+d} \pmod{p}$, $1 \leq i, j, k \leq p-1$.

Theorem 4. *Construction D generates a TDC cube.*

Proof. For each d, $0 \leq d \leq p-2$, and for each c, $1 \leq c \leq p-1$, α^{i+d} and cj are permutations of $1, 2, \ldots, p-1$ for $1 \leq i, j \leq p-1$. In a proof similar to the proof of Theorem 2, we can show that for each c, $1 \leq c \leq p-1$, $A(*, *, c)$ and $A(*, c, *)$ are Costas arrays. By Lemma 1, for each c, $1 \leq c \leq p-1$, $A(c, *, *)$ is a permutation matrix. □

Construction E. Let $p = 2^r - 1$ be a Mersenne prime and let α and β be primitive elements in the field $GF(p+1)$. Then construct the $(p-1) \times (p-1) \times (p-1)$ cube A, with $A(i, j, k) = 1$ if and only if $\alpha^i + \beta^{jk} = 1$, $1 \leq i, j, k \leq p-1$.

Theorem 5. *Construction E generates a TDC cube.*

Proof. We make use of the fact that since p is a prime all the elements, except for 0 and 1, of $GF(p+1)$ are primitive elements. For each c, $1 \leq c \leq p-1$, it is easily verified that $A(*, *, c)$ defined by $\alpha^i + \beta^{cj} = \alpha^i + \gamma^j = 1$ is a Costas array of the Golomb Construction. Hence $A(*, *, c)$ is a Costas array and by a similar argument $A(*, c, *)$ is also a Costas array. By Lemma 1, for each c, $1 \leq c \leq p-1$, $A(c, *, *)$ is a permutation matrix. □

Two cubes A and B will be called *equivalent* if A can be transformed into B by a symmetry of a cube. It should be mentioned that Constructions A and B generate inequivalent ADNC cubes, and Constructions C, D, and E generate inequivalent TDC cubes.

3. Construction of VC squares

In this section we give two methods to generate VC squares. The first one is a polygonal path construction [8].

Construction F1. Let α be a primitive root modulo the prime p. Then construct the $(p-1) \times (p-1)$ square A, with $A(i, j) = k$ if and only if $\alpha^{k-i} \equiv j \pmod{p}$, $1 \leq i, j, k \leq p-1$.

Lemma 3. *Construction F1 generates a Vatican square.*

Proof. It is easy to verify that A is a Latin square. If A is not a Vatican square, we can find two symbols k_1 and k_2 such that

$$A(i_1, j_1) = k_1, \qquad A(i_1, j_1 + l) = k_2,$$
$$A(i_2, j_2) = k_1, \quad \text{and} \quad A(i_2, j_2 + l) = k_2,$$

where $i_1 \neq i_2$, $j_1 \neq j_2$, and $k_1 \neq k_2$.

By definition

$$\alpha^{k_1 - i_1} \equiv j_1 \pmod{p}, \qquad \alpha^{k_2 - i_1} \equiv j_1 + l \pmod{p},$$
$$\alpha^{k_1 - i_2} \equiv j_2 \pmod{p}, \quad \text{and} \quad \alpha^{k_2 - i_2} \equiv j_2 + l \pmod{p},$$

and hence $\alpha^{k_1 - i_1} - \alpha^{k_2 - i_1} \equiv \alpha^{k_1 - i_2} - \alpha^{k_2 - i_2} \pmod{p}$. But this requires

$$\alpha^{-i_1}(\alpha^{k_1} - \alpha^{k_2}) \equiv \alpha^{-i_2}(\alpha^{k_1} - \alpha^{k_2}) \pmod{p}$$

and since $\alpha^{k_1} - \alpha^{k_2} \not\equiv 0 \pmod{p}$ we must have $i_1 = i_2$, a contradiction. Hence A is a Vatican square. □

Construction F2. Let α be a primitive root modulo the prime p. Then for each d, $0 \leq d \leq p-2$, construct the $(p-1) \times (p-1)$ square A, with $A(i, j) = k$ if and only if $jk \equiv \alpha^{i+d} \pmod{p}$, $1 \leq i, j, k \leq p-1$.

Lemma 4. *Construction F2 generates an LC square.*

Proof. In a proof similar to the one of Theorem 4, we can show that each symbol in A defines a Costas array. Hence A is an LC square. □

Two VC squares A and B are *equivalent* if A can be transformed into B only by a symmetry of a square and permutation of the symbols. We will show now that the squares of Constructions F1 and F2 are equivalent.

A singly periodic VC square is an $\infty \times n$ pattern such that each $n \times n$ subarray of it is a VC square.

Lemma 5. *In a square A of Construction F2 each column is a cyclic permutation of $\alpha, \alpha^2, \ldots, \alpha^{p-1} = 1$.*

Proof. By definition $A(i,j) \equiv \alpha^{i+d}/j \pmod p$, $1 \leqslant i, j \leqslant p-1$. Hence $A(i+1,j) \equiv \alpha^{i+1+d}/j \equiv \alpha A(i,j) \pmod p$, where $i+1$ is taken modulo $p-1$. Therefore each column is a cyclic shift of $\alpha, \alpha^2, \ldots, \alpha^{p-1} = 1$. □

From the definition of construction F2 and Lemma 5 we can observe the following.

Corollary 5.1. *For a given α, all the squares of Construction F2 are equivalent and singly periodic.*

Lemma 6. *Let α be a primitive root modulo the prime p. Then the squares produced from Construction F2 for α and α^{-1} are equivalent.*

Proof. Let A be the square constructed by the equation $A(i,j) \equiv \alpha^i/j \pmod p$, $1 \leqslant i, j \leqslant p-1$, and B be the square constructed by the equation $B(i,j) \equiv (\alpha^{-1})^i/j \pmod p$, $1 \leqslant i, j \leqslant p-1$. First, we will show that for all $1 \leqslant j \leqslant p-1$

$$A(p-1,j) = B\left(\frac{p-1}{2}, p-j\right) \quad \text{and} \quad A(p-2,j) = B\left(\frac{p+1}{2}, p-j\right).$$

$$A(p-1,j) \equiv \frac{\alpha^{p-1}}{j} \equiv \frac{p-\alpha^{p-1}}{p-j} \equiv \frac{p-1}{p-j} \equiv \frac{(\alpha^{-1})^{(p-1)/2}}{p-j}$$

$$\equiv B\left(\frac{p-1}{2}, p-j\right) \pmod p.$$

$$A(p-2,j) \equiv \frac{\alpha^{p-2}}{j} \equiv \frac{p-\alpha^{p-2}}{p-j} \equiv \frac{p-\alpha^{-1}}{p-j} \equiv \frac{\alpha^{-1}p-\alpha^{-1}}{p-j} \equiv \frac{\alpha^{-1}(p-1)}{p-j}$$

$$\equiv \frac{\alpha^{-1}(\alpha^{-1})^{(p-1)/2}}{p-j} \equiv \frac{(\alpha^{-1})^{(p+1)/2}}{p-j} \equiv B\left(\frac{p+1}{2}, p-j\right) \pmod p.$$

Hence we have found two consecutive rows in A which are the same as two consecutive rows in B, in reverse order of symbols. Therefore, it follows from Lemma 5 and Corollary 5.1 that the squares produced from Construction F2 for α and α^{-1} are equivalent. □

Lemma 7. *Let α be a primitive root modulo the prime p. Then the squares produced from Construction F1 for α and from Construction F2 for α^{-1} are equivalent.*

Proof. Let A be the square constructed by the equation $A(i, j) \equiv \alpha^i/j \pmod p$, $1 \leqslant i, j \leqslant p-1$, and B be the square constructed by the equation $B(i, j) \equiv i + \log_{\alpha^{-1}} j \pmod{p-1}$, $1 \leqslant i, j \leqslant p-1$, $1 \leqslant i + \log_{\alpha^{-1}} j \leqslant p-1$. It is easy to verify that each column of B is a cyclic shift of $1, 2, \ldots, p-1$. From this observation, Lemma 5, and the definitions we only have to prove that by substituting $i \pmod{p-1}$ instead of α^i, $1 \leqslant i \leqslant p-1$, in A to produce A_1, the first row of B and the first row of A_1 are identical. For each j, $1 \leqslant j \leqslant p-1$, $A(1, j) \equiv \alpha/j \equiv \alpha^{1+\log_{\alpha^{-1}} j} \pmod p$, and hence $A_1(1, j) = B(1, j)$. □

From Lemmas 3 through 7 we can infer the following theorem.

Theorem 6. *Constructions F1 and F2 generate equivalent VC squares.*

Construction G. Let $p = 2^r - 1$ be a Mersenne prime and let α and β be primitive elements in the field $\mathrm{GF}(p+1)$. Then construct the $(p-1) \times (p-1)$ square A, with $A(i, j) = k$ if and only if $\alpha^i + \beta^{jk} = 1, 1 \leqslant i, j, k \leqslant p-1$.

Theorem 7. *Construction G generates a VC square.*

Proof. In a proof similar to the one of Theorem 5 we can show that each symbol of A defines a Costas array and hence the square is a Latin square. If A is not a Vatican square, we can find two symbols k_1 and k_2 such that

$$A(i_1, j_1) = k_1, \qquad A(i_1, j_1 + l) = k_2,$$
$$A(i_2, j_2) = k_1, \quad \text{and} \quad A(i_2, j_2 + l) = k_2,$$

where $i_1 \neq i_2$, $j_1 \neq j_2$, and $k_1 \neq k_2$. By definition

$$\alpha^{i_1} + \beta^{j_1 k_1} = 1, \qquad \alpha^{i_1} + \beta^{(j_1+l)k_2} = 1,$$
$$\alpha^{i_2} + \beta^{j_2 k_1} = 1, \quad \text{and} \quad \alpha^{i_2} + \beta^{(j_2+l)k_2} = 1,$$

and hence $\beta^{j_1 k_1} = \beta^{(j_1+l)k_2}$ and $\beta^{j_2 k_1} = \beta^{(j_2+l)k_2}$. Since $\beta \in \mathrm{GF}(p+1)$ we have

$$j_1 k_1 \equiv (j_1 + l)k_2 \pmod p, \qquad j_2 k_1 \equiv (j_2 + l)k_2 \pmod p,$$

and $(j_1 - j_2)k_1 \equiv (j_1 - j_2)k_2 \pmod p$. Since p is prime and $j_1 \neq j_2$ we have $k_1 = k_2$, a contradiction. Therefore A is a VC square. □

Theorem 8. *Construction G generates VC squares which are inequivalent to the VC squares generated by Constructions F1 and F2.*

Proof. Let $p = 2^r - 1$ be a Mersenne prime and let α and β be primitive elements in the field $GF(p+1)$. Let A be the VC square constructed from the equation $\alpha^i + \beta^{jk} = 1$, where $\alpha + \beta^{k_1} = 1$. Since the operations are in $GF(2^r)$ we have $\alpha^2 + \beta^{2k_1} = 1$ and $\alpha^4 + \beta^{4k_1} = 1$. Hence $A(1, 1) = k_1$, $A(2, 1) = 2k_1$, $A(2, 2) = k_1$, and $A(4, 2) = 2k_1$. Therefore the columns of A are not cyclic shifts of the first column. By Lemma 5 and Theorem 6, A cannot be produced by Constructions F1 and F2. □

Example 1. For $p = 7$, 3 is a primitive root modulo 7. Construction F1 gives us the following VC square:

1	3	2	5	6	4
2	4	3	6	1	5
3	5	4	1	2	6
4	6	5	2	3	1
5	1	6	3	4	2
6	2	1	4	5	3.

Example 2. Let α be a primitive element of $GF(2^3)$ which is produced from $\alpha^3 + \alpha + 1 = 0$. The field $GF(2^3)$ takes the following form:

α^0 0 0 1
α^1 0 1 0
α^2 1 0 0
α^3 0 1 1
α^4 1 1 0
α^5 1 1 1
α^6 1 0 1.

Taking $\beta = \alpha$ Construction G gives us the following VC square:

3	5	1	6	2	4
6	3	2	5	4	1
1	4	5	2	3	6
5	6	4	3	1	2
4	2	6	1	5	3
2	1	3	4	6	5.

4. Examples, conjectures, and unsolved problems

There is one inequivalent ADC cube for $n=1$, one for $n=2$, and one for $n=4$. These are as in the following examples.

Example 3. For $n=1$,

$$A(1,1,1)=1.$$

For $n=2$,

$$A(1,1,1)=1, \qquad A(1,2,2)=1, \qquad A(2,1,2)=1, \qquad A(2,2,1)=1,$$

and all the other entries of A are zeroes.

For $n=4$,

$$\begin{array}{llll} A(1,1,1)=1, & A(2,1,3)=1, & A(3,1,4)=1, & A(4,1,2)=1, \\ A(1,2,4)=1, & A(2,2,2)=1, & A(3,2,1)=1, & A(4,2,3)=1, \\ A(1,3,2)=1, & A(2,3,4)=1, & A(3,3,3)=1, & A(4,3,1)=1, \\ A(1,4,3)=1, & A(2,4,1)=1, & A(3,4,2)=1, & A(4,4,4)=1, \end{array}$$

and all the other entries of A are zeroes.

Exhaustive computer search shows that for other $n \leqslant 8$ there are no ADC cubes, and we have the following conjecture.

Conjecture 1. Except for $n=1, 2,$ and 4 there are no ADC cubes of order n.

The computer search did not find any LC squares for odd n between 2 and 10, which by Lemma 2 implies the non-existence of ODC squares in this range. From this we have the following conjecture.

Conjecture 2. There are no LC squares of odd order $n>1$.

Example 4. Except for the two VC squares of Examples 1 and 2 there is only one other inequivalent VC square of order 6:

1	6	4	3	2	5
2	4	1	5	3	6
3	1	2	6	5	4
4	5	6	2	1	3
5	2	3	4	6	1
6	3	5	1	4	2.

The first case of LC squares which was found by the computer search and is not covered by any of our constructions is for $n=8$.

Example 5. For $n = 8$ the following square is an LC square.

$$\begin{array}{cccccccc}
1 & 5 & 3 & 8 & 7 & 4 & 6 & 2 \\
2 & 6 & 4 & 7 & 8 & 3 & 5 & 1 \\
3 & 7 & 1 & 6 & 5 & 2 & 8 & 4 \\
4 & 8 & 2 & 5 & 6 & 1 & 7 & 3 \\
5 & 1 & 7 & 4 & 3 & 8 & 2 & 6 \\
6 & 2 & 8 & 3 & 4 & 7 & 1 & 5 \\
7 & 3 & 5 & 2 & 1 & 6 & 4 & 8 \\
8 & 4 & 6 & 1 & 2 & 5 & 3 & 7.
\end{array}$$

This LC square implies the existence of a TDC cube where symbol k, $1 \leqslant k \leqslant 8$ defines the positions of the 1's in the kth two-dimensional subarray of the third direction. Only two inequivalent Costas arrays participate in this construction.

Costas array number 1:

$$\begin{array}{cccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0.
\end{array}$$

Costas array number 2:

$$\begin{array}{cccccccc}
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0.
\end{array}$$

Constructions for Vatican squares of order n are known only when $n+1$ is prime [8, 11]. The following is a natural conjecture.

Conjecture 3. VC squares of order n exist only when $n+1$ is prime.

Some other open problems are:

(1) Find new constructions for ADNC cubes, ODC cubes, TDC cubes, and ADC cubes.

(2) Find values of n for which no ADNC cubes, or no ODC cubes, or no TDC cubes, or no ADC cubes of order n exist.

(3) Find new constructions for VC squares of order n where $n+1$ is prime.

(4) Find values of n for which ODC cubes of order n exist but TDC cubes of order n do not exist.

Acknowledgments

The author wishes to thank Prof. Solomon W. Golomb who introduced him the area of Costas arrays. He also thanks Prof. Herbert Taylor for many helpful discussions which contributed to this paper.

References

[1] G.S. Bloom and S.W. Golomb, Applications of numbered undirected graphs, IEEE Proc. 65 (1977) 562–570.

[2] J.P. Costas, A study of a class of detection waveforms having nearly ideal range-Doppler ambiguity properties, IEEE Proc. 72 (1984) 996–1009.

[3] J. Denes and A.D. Keedwell, Latin Squares and their Applications (Academic Press, New York, 1974).

[4] R. Gagliardi, J. Robbins and H. Taylor, Acquistion sequences in PPM communications, IEEE Trans. Inform. Theory (1987) 738–744.

[5] R. Games, Crosscorrelation of M-sequences and GMW-sequences with the same primitive polynomial, Discrete Appl. Math 12 (1985) 139–146.

[6] R. Games, An algebraic construction of sonar sequences using M-sequences, SIAM J. Algebraic Discrete Methods 8 (1987) 753–761.

[7] S.W. Golomb, Algebraic constructions for Costas arrays, J. Combin. Theory Ser. A 37 (1984) 13–21.

[8] S.W. Golomb, T. Etzion and H. Taylor, Polygonal path constructions for Tuscan-k squares, Ars Combin. 20 (1990) 97–140.

[9] S.W. Golomb and H. Taylor, Two-dimensional synchronization patterns for minimum ambiguity, IEEE Trans. Inform. Theory 28 (1982) 600–604.

[10] S.W. Golomb and H. Taylor, Constructions and properties of Costas arrays, IEEE Proc. 72 (1984) 1143–1163.

[11] S.W. Golomb and H. Taylor, Tuscan squares—a new family of combinatorial designs, Ars Combin. 20 (B) (1985) 115–132.