Permutations with a distinct difference property

Lynn M. Batten\textsuperscript{a,}\textsuperscript{*}, Sharad Sane\textsuperscript{b,1}

\textsuperscript{a}Department of Mathematics, Deakin University, 662 Blackburn Road, 3168 Clayton, Victoria, Australia
\textsuperscript{b}University of Mumbai, Mumbai, India

Received 19 May 2001; accepted 30 September 2001

Dedicated to Alex Rosa on the occasion of his sixty-fifth birthday

Abstract

The topic of this paper arose out of a consideration of Costas sequences, which are used in sonar and radar applications. These sequences have the defining property that all differences of elements the same distance apart, are different. Several infinite families of Costas sequences are known; but there are many existence questions for length $\geq 32$. In this article, we restrict ourselves to sequences with the weaker property that all adjacent differences are different. We give a recursive construction for these, as well as building several infinite families.

\copyright 2002 Elsevier Science B.V. All rights reserved.

Keywords: Difference property; Sequence; Costas

1. Introduction

Multiple user radar and sonar systems, as well as spread-spectrum communication systems have many common properties. All rely on retrieving and identifying frequencies after they have left a transmitter [9,6]. Costas [4] proposed the following problem: ‘We wish to design an $n \times n$ frequency hop pattern using $n$ consecutive time intervals $t_1, t_2, \ldots, t_n$ and $n$ consecutive frequencies $f_1, f_2, \ldots, f_n$, where some permutation of the $n$ frequencies is assigned to the $n$ consecutive time slots. Moreover, this should be done in such a way that if $f_i$ and $f_j, j > i$, occur with time interval $t$, then the difference $f_j - f_i$ can arise from no other pair of frequencies over the same time interval.'
There are three known constructions of infinite families of Costas sequences [11]:

The Welch construction [7] constructs a sequence of length \( p - 1 \) for any prime \( p \). The Logarithmic Welch construction [5] also constructs a sequence of length \( p - 1 \) for any prime \( p \).

Lempel [7] takes a primitive element of \( \text{GF}(q) \), \( q \) a prime power, and uses it to construct a Costas sequence on \( q - 2 \) elements. Golomb [7] generalized this last idea to construct more such sequences.

Computer searches for all Costas sequences on up to \( n = 23 \) elements have been successful [12,10]. Beyond that, only sporadic information is available. The first value of \( n \) for which no Costas sequence is as yet known to exist is \( n = 32 \) [6].

In the present article, we consider a weaker condition on the sequence, asking only that the frequency differences be different for all time intervals of length one. These we call permutation sequences with a distinct difference property (DDP); the corresponding arrays, we call permutation arrays with DDP.

We prove the following results in subsequent sections:

**Theorem.** Any DDP sequence on \( n \) elements can be extended in at least two ways to a DDP sequence on \( n + 1 \) elements.

**Theorem.** Any anti-reflective DDP sequence on \( 2n \) elements can be extended in at least two ways to a DDP sequence on \( 2n + 2 \) elements.

**Theorem.** For any odd prime \( p \) and integer \( \alpha \geq 1 \), there are at least \( p - 1 \) DDP sequences on \( p^{\alpha} - 1 \) elements which can be constructed in \( \mathbb{Z}_{p^{\alpha}} \).

Note that \( n \)-dimensional Costas arrays will be defined in Section 2.

**Theorem.** Let \( p - 1 = m_1 m_2 \cdots m_n \), \( p \) a prime. Then there is an \( n \)-dimensional Costas array of type \( m_1, m_2, \ldots, m_n \).

An obvious generalization of our condition on time intervals of length one, is to require different frequency differences for all time intervals of a fixed length \( l \geq 1 \). It is easy to construct examples for which this property holds for \( l > 1 \), but not for any value less than or equal to one. (125634 is such an example.)

Thus, there seems to be no practical reason for considering \( l > 1 \), as \( l = 1 \) gives the largest set of differences for a fixed permutation.

### 2. Recursive constructions

**Definition 2.1.** We say that a permutation on \( n \) letters, \( a_1 a_2 \ldots a_n \), has the distinct difference property or DDP if \( a_{i+1} - a_i = a_{j+1} - a_j \) implies \( i = j \) for all \( 1 \leq i, j \leq n - 1 \). We also call this a DDP sequence.

Although many Costas sequences on \( n \) letters cannot be extended to one on \( n + 1 \) letters by the placing of the element \( n + 1 \) within the sequence, we prove in the first theorem that this always is the case for DDP sequences.
Theorem 2.1. Let $\pi = a_1a_2 \ldots a_n$ be a permutation on $\{1, 2, \ldots, n\}$ with DDP. Then there are at least two positions at which $n + 1$ can be inserted into $\pi$, resulting in a DDP sequence on $n + 1$ letters.

Proof. Define for $i = 0, 1, \ldots, n$, sets $A_i \subseteq \{1, 2, \ldots, n - 1\}$ as follows:

For $i = 1, 2, \ldots, n - 1$, consider

$$
(n + 1) - a_i = a_{j+1} - a_j,
$$

(1)

$$
a_{i+1} - (n + 1) = a_{k+1} - a_k.
$$

(2)

Define $A_i = \{j\}$ if only (1) is satisfied, $A_i = \{k\}$ if only (2) is satisfied, $A_i = \{j, k\}$ if both (1) and (2) are satisfied and $A_i = \emptyset$ otherwise.

For $i = 0$, consider

$$
a_1 - (n + 1) = a_{j+1} - a_j.
$$

(3)

Similarly, for $i = n$, consider

$$
(n + 1) - a_n = a_{k+1} - a_k.
$$

(4)

Define $A_n = \{k\}$ if (4) is satisfied, and $A_n = \emptyset$ otherwise.

Clearly $|A_i| \leq 2$ for $1 \leq i \leq n - 1$, $|A_0| \leq 1$ and $|A_n| \leq 1$.

We now claim that for $i \neq m, A_i \cap A_m = \emptyset$. Suppose first that $i$ and $m$ lie in the range 1 to $n - 1$, and that, on the contrary, $j \in A_i \cap A_m$. If $j$ is in each because of (1), then $a_i = a_m$, a contradiction. Similarly for (2). So assume $(n + 1) - a_i = a_{j+1} - a_j = a_m - (n + 1)$; but this is false since the first term is positive and the last is negative. The other cases are similarly eliminated.

Finally, since $\bigcup_{i=0}^{n} A_i \subseteq \{1, 2, \ldots, n - 1\}$, we must have $A_i = \emptyset$ for at least two values of $i$.

If $A_0 = \emptyset$, then the sequence $(n + 1) a_1 \ldots a_n$ is a DDP sequence.

If $A_n = \emptyset$, we take $a_1 \ldots a_n (n + 1)$.

If $A_i = \emptyset$, $1 \leq i \leq n - 1$, we take $a_1 \ldots a_i (n + 1) a_{i+1} \ldots a_n$. $\square$

Corollary 2.1. For all $n \geq 1$, there are at least $2^{n-1}$ different DDP sequences on $n$ elements.

Proof. This follows easily by induction and Theorem 1.1. $\square$

In [12], an anti-reflective Costas sequence is defined. We borrow the definition for DDP sequences:

Definition 2.2. A DDP sequence $a_1a_2 \ldots a_n$, $n$ even, is said to be anti-reflective if $a_i + a_{i+n/2} = n + 1$ for all $1 \leq i \leq n/2$.

Theorem 2.2. Let $\pi = a_1a_2 \ldots a_n b_1b_2 \ldots b_n$ be an anti-reflective DDP sequence on $2n$ elements; thus $a_i + b_i = 2n + 1$, for $1 \leq i \leq n$. Then there are at least two ways that
the pair \((1, 2n+2)\) can be added to the sequence \(\pi' = a_1 + 1, a_2 + 1 \ldots a_n + 1, b_1 + 1, b_2 + 1 \ldots b_n + 1\) to obtain an anti-reflective DDP sequence on \(2n+2\) elements.

**Proof.** We follow the proof of Theorem 2.1 with the insertion of the element 1 somewhere in the first half of the sequence, and of the element \(2n+2\) somewhere in the second half.

For \(i = 1, 2, \ldots, n - 1\), consider
\[
1 - (a_i + 1) = (2n + 2) - (b_i + 1) \Rightarrow -a_i = a_i, \quad \text{false;}
\]
\[
1 - (a_i + 1) = (b_{i+1} + 1) - (2n + 2) \Rightarrow -a_i = -a_{i+1}, \quad \text{false;}
\]
\[
(a_{i+1} + 1) - 1 = (2n + 2) - (b_i + 1) \Rightarrow a_{i+1} = a_i, \quad \text{false;}
\]
\[
(a_{i+1} + 1) - 1 = (b_{i+1} + 1) - (2n + 2) \Rightarrow a_{i+1} = -a_{i+1}, \quad \text{false.}
\]

For \(i = 0\), consider
\[
(a_1 + 1) - 1 = (2n + 2) - (a_n + 1) \Rightarrow a_1 = b_n, \quad \text{false;}
\]
\[
(a_1 + 1) - 1 = (b_1 + 1) - (2n + 2) \Rightarrow a_1 = -a_1, \quad \text{false.}
\]

For \(i = n\), consider
\[
(2n + 2) - (b_n + 1) = 1 - (a_n + 1) \Rightarrow a_n = -a_n, \quad \text{false;}
\]
\[
(2n + 2) - (b_n + 1) = (b_1 + 1) - 1 \Rightarrow a_n = b_1, \quad \text{false.}
\]

Thus, no repeats in differences can occur around insertion points.

So consider now the following possibilities:

For \(i = 1, 2, \ldots, n - 1\),
\[
1 - (a_i + 1) = a_{j+1} - a_j \quad \text{or} \quad b_{j+1} - b_j.
\]

But \(a_j + b_j = a_{j+1} + b_{j+1} = 2n + 1\), so this yields
\[
-a_i = \pm (a_{j+1} - a_j), \tag{5}
\]
where only one sign on the right can actually occur.

Also, in a similar way, we have
\[
(a_{i+1} + 1) - 1 = a_{i+1} = \pm (a_{k+1} - a_k), \tag{6}
\]
\[
-a_i = (b_1 + 1) - (a_n + 1) = b_1 - a_n, \tag{7}
\]
\[
a_{i+1} = b_1 - a_n. \tag{8}
\]

Note that (6) can only have one sign holding, and (7) and (8) cannot hold for the same \(i\).

Noting that each of (5) through (8) holds for at most one \(j, k, \) or \(i\), we define \(A_i = \{j\}\) if (5) is satisfied, \(A_i = \{k\}\) if (6) is satisfied, \(A_i = \{j, k\}\) if both (5) and (6) are satisfied, where \(j = k\) is possible in this case, and \(A_i = \emptyset\) otherwise. Clearly, (7) or (8) occurs for at most one \(i\). We take this into consideration later.

We claim then, that for \(i \neq m\), \(A_i \cap A_m = \emptyset\). Suppose \(j \in A_i \cap A_m\). Then this arose from (5) and (6) which implies \(a_{i+1} = -a_i\), a contradiction.
Thus \( \bigcup_{i=0}^{n} A_i \subseteq \{1, 2, \ldots, n-1\} \) and so at least two of the \( A_i \) are empty. Since one of these sets may actually correspond to a repeat as in (7) or (8), we can conclude that at least one set must be empty. This means that there is at least one way to extend \( \pi \) to an anti-reflexive DDP sequence on \( 2n+2 \) symbols by inserting 1 in the first half and \( 2n+2 \) in the second half.

By symmetry, there is also an extension placing \( 2n+2 \) in the first half and 1 in the second half.

**Corollary 2.2.** For all \( 2n \geq 2 \), there are at least \( 2^{n-1} \) anti-reflective DDP sequences on \( 2n \) elements.

Finally, in this section, we present a generalization of the construction of Welch [6] which finds DDP sequences on \( p^x - 1 \) elements, \( p \) a prime. In fact, Welch constructs modular sequences, as defined below. This is a particularly pleasant, and strong form of DDP sequence, which is a result of the underlying algebraic structure.

**Definition 2.3.** A modular DDP sequence \( a_1a_2 \cdots a_n \) is a sequence on \( n \) elements such that \( a_{i+1} - a_i \neq a_{j+1} - a_j \) for all \( i \neq j \) (mod \( n \)).

For any prime \( p \), Theorem 2.1 proves that there exist at least \( 2^{p-1} \) DDP sequences on \( n \) elements. In the next result, we give explicit constructions for some of these in the case \( p \) odd.

**Theorem 2.3.** Let \( p \) be an odd prime and \( x \) an integer \( \geq 1 \). Then there are at least \( p-1 \) DDP sequences on \( p^x - 1 \) elements which can be constructed in \( \mathbb{Z}_{p^x} \).

**Proof.** For each \( i, 1 \leq i \leq x \), the group of units in \( \mathbb{Z}_{p^i} \) is cyclic and generated by the same primitive root \( g \) for \( p \) such that \( gp^{i-1} = 1 + mp \) for some integer \( m \) with \( p \nmid m \) [3]. (This is false for \( p = 2 \).)

**Step 1:** Fix such an element \( g \), and in \( \mathbb{Z}_{p^i} \) consider the sequence

\[
g, g^2, \ldots, g^{p^i-p^{i-1}-1}, 1 \quad \text{for } 1 \leq i \leq x.
\]

We show that, in \( \mathbb{Z}_{p^i} \),

\[
g^j - g^{j-1} \neq g^k - g^{k-1} \quad \text{for any } i \leq j < k \leq p^i - p^{i-1}.
\]

If not, \( g^{i-1}(g-1)(g^{k-j} - 1) = 0 \), which implies that the product is divisible by \( p^i \). But \( p^i \mid g-1 \) or \( g^{i-1} \). Thus \( p^i \mid (g^{k-j} - 1) \). Now \( p^m \mid (g^{p^i-p^{i-1}} - 1) \) implies \( m \leq n \) [3]. So \( p^i \mid (g^{k-j} - 1) \) only if \( k - j \geq p^i - p^{i-1} - 1 \), which is false.

**Define the sequences** \( \Pi_i = p^{x-i}g, p^{x-i}g^2, \ldots, p^{x-i}g^{p^x-p^{i-1}-1}, p^{x-i} \), for \( 1 \leq i \leq x \).

**Step 2:** We now juxtapose the sequences corresponding to \( i = 1 \) and 2:

\[
p g \quad p g^2 \quad \ldots \quad p g^{p-2} \quad p \quad g \quad g^2 \quad \ldots \quad g^{p^2-p-1}.
\]
and claim that we can do so for a suitable cyclic permutation of each which results in a DDP sequence. It suffices to do this for \(\alpha = 2\), and so we prove that for each \(0 \leq \beta < p - 2\) there exists \(0 \leq i \leq p^2 - p - 1\) such that for all \(0 \leq j \leq p^2 - p - 1\), 
\[ pg^\beta - g^i \neq g^{j+1} - g^j, \]
working with exponents modulo \(p^2\). (Clearly, differences in \(\Pi_1\) are divisible by \(p\), while those in \(\Pi_2\) are not.)

Suppose, on the contrary, that for all \(0 \leq i \leq p^2 - p - 1\) we have 
\[ pg^\beta - g^i = g^{j+1} - g^j \]
for some \(j\). Since the DDP holds in \(\mathbb{Z}^*_p\), it follows that every \(i\) determines a unique \(j\). Summing over all \(i\) gives
\[
\sum_{i=0}^{p^2-p-1} pg^\beta - \sum_{i=0}^{p^2-p-1} g^i = \sum_{j=0}^{p^2-p-1} g^{j+1} - \sum_{j=0}^{p^2-p-1} g^j = 0.
\]

Hence 
\[ pg^\beta(p^2 - p) = \sum_{i=0}^{p^2-p-1} g^i \]
which also equals zero since the negative of every element in the sum also appears in the sum. The left-hand side is a positive integer, and so we have a contradiction.

Consequently, for each \(0 \leq \beta < p - 2\), there exists an \(i\) such that 
\[ g^{\beta+1}, \ldots, g^{(p^2-p-1)}, \ldots, g^{\beta}, pg^\beta, pg^{\beta+1}, \ldots, pg^{(p^2-p-1)} \]
is a DDP sequence.

Let the corresponding permutations of \(\Pi_1\), and \(\Pi_2\) be \(\Pi'_1, \Pi'_2\).

Step 3: Recursively, now, there is, by step 2, a permutation \(\Pi'_3\) of \(\Pi_3\) such that the juxtaposition \(\Pi'_1\Pi'_2\Pi'_3\) is a DDP sequence. Continuing, there exist permutations \(\Pi'_i\) of all \(\Pi_i\), \(1 \leq i \leq \alpha\) such that \(\Pi'_1\Pi'_2\ldots\Pi'_\alpha\) is a DDP sequence.

Since there are \(p - 1\) choices for juxtaposing the first two, there are \(p - 1\) ways in which such a DDP can be formed.

**Example.** We compute the sequences from Theorem 2.3 corresponding to \(p = 5\), \(\alpha = 2\) and \(1 \leq i \leq 2\).

The generator \(g = 3\) can be used for both groups of units \(Z_5\) and \(Z_{25}\).

For \(i = 1\) the (modular) DDP sequence is 3, 4, 2, 1.

For \(i = 2\), we obtain the sequence
\[ 3, 9, 2, 6, 18, 4, 12, 11, 8, 24, 22, 16, 23, 19, 7, 21, 13, 14, 17, 1. \]

Note that this has length \(\phi(5^2) = 5^2 - 5 = 20\), and is not a DDP sequence.

By Step 2 of Theorem 2.3, there is an ordering of 5 · 3, 5 · 4, 5 · 2, 5 · 1 which, combined with the longer sequence results in a DDP. In fact, this can be done as follows:
\[ 3, 9, 2, 6, 18, 4, 12, 11, 8, 24, 22, 16, 23, 19, 7, 21, 13, 14, 17, 1, 20, 10, 5, 15. \]

### 3. Higher dimensions

In this section, we attempt a possible \(n\)-dimensional generalization of the notion of a Costas sequence and construct an infinite class of such objects. We begin with
Definition 3.1. A permutation array

\[ A = (a_{i_1, i_2, \ldots, i_n}) \]

of dimension \( n \) and type \( m_1, m_2, \ldots, m_n \) is an “\( n \)-dimensional matrix” (in the sense of [1]) where \( m_i \) are positive integers, \( 0 \leq i_t \leq m_t - 1 \) for all \( 1 \leq t \leq n \) and satisfying the property that

\[ a_{i_1, i_2, \ldots, i_n} = a_{j_1, j_2, \ldots, j_n} \text{ holds if and only if } (i_1, i_2, \ldots, i_n) = (j_1, j_2, \ldots, j_n). \]

Notice that an \( n \)-dimensional array is just an \( n \)-dimensional arrangement of distinct symbols from the set of the first \( m_1 m_2 \ldots m_n \) numbers. We also define an \( n \)-dimensional permutation array \( A \) as above to be proper if every \( m_t \geq 2 \). Observe that a one-dimensional permutation is just an ordinary permutation.

Definition 3.2. Let \( A \) be a permutation array of dimension \( n \) and type \( m_1, m_2, \ldots, m_n \). We call \( A \) a Costas array of dimension \( n \) and type \( m_1, m_2, \ldots, m_n \) if the equation

\[ a_{i_1 + h_1, i_2 + h_2, \ldots, i_n + h_n} - a_{i_1, i_2, \ldots, i_n} = a_{j_1 + h_1, j_2 + h_2, \ldots, j_n + h_n} - a_{j_1, j_2, \ldots, j_n} \]

holds only when \( h_t = 0 \) for all \( t = 1, 2, \ldots, n \). We assume here that the subscripts take values in the prescribed range, that is, for both \( a_{i_1 + h_1, i_2 + h_2, \ldots, i_n + h_n} \) and \( a_{j_1 + h_1, j_2 + h_2, \ldots, j_n + h_n} \), we have \( i_t + h_t \) and \( j_t + h_t \) are less than or equal to \( m_t - 1 \).

Definition 3.3. Let \( A \) be a permutation array of dimension \( n \) and type \( m_1, m_2, \ldots, m_n \). We call \( A \) a modular Costas array of dimension \( n \) and type \( m_1, m_2, \ldots, m_n \) if the equation

\[ a_{i_1 + h_1, i_2 + h_2, \ldots, i_n + h_n} - a_{i_1, i_2, \ldots, i_n} = a_{j_1 + h_1, j_2 + h_2, \ldots, j_n + h_n} - a_{j_1, j_2, \ldots, j_n} \quad (\ast) \]

holds only when \( i_t \equiv j_t \pmod{m_t} \) for all \( t = 1, 2, \ldots, n \). Observe that every \( n \)-dimensional modular Costas array is necessarily an \( n \)-dimensional Costas array. In fact, an \( n \)-dimensional modular Costas array may be viewed as if the entries are written on an \( n \)-dimensional torus. We would also like to point out that the notion of a Costas sequence (respectively, modular Costas sequence) or Costas array (see [4]) as it obtains in the literature is a special case of our definition. It is, in fact, just a one-dimensional Costas array. Theorem 3.5 is a generalization of the Welch construction and we need the following lemma for its proof.

Lemma 3.1. Let \( m_1, m_2, \ldots, m_n \) be arbitrary positive integers each greater than or equal to 2. Let \( s = m_1 m_2 \ldots m_n \). Then every integer \( h \) between 0 and \( s - 1 \) can be uniquely written in the form

\[ h = \sum_{t=0}^{t=n} h_t m_{t+1} m_{t+2} \ldots m_n, \]

where \( 0 \leq h_t \leq m_t - 1 \) for every \( t = 1, 2, \ldots, n \).
The proof of the above lemma is easy and the easiest way to prove it is to actually divide. In fact, more general results are known; see for example [8].

**Theorem 3.4.** Let \( p \) be a prime number and suppose \( p − 1 \) = \( m_1m_2...m_n \). Let \( A = (a_{i_1,i_2,...,i_n}) \) be an \( n \)-dimensional array of type \( m_1, m_2, ..., m_n \) defined as follows. Let \( \alpha \) be a primitive element in the field \( \mathbb{F} = \text{GF}(p) \). Let

\[
\begin{align*}
a_{i_1,i_2,...,i_n} &= \alpha^{\sum_{t=0}^{m_n} t_i m_{i+1} m_{i+2}...m_n}.
\end{align*}
\]

Then \( A \) is an \( n \)-dimensional modular Costas array of type \( m_1, m_2, ..., m_n \).

**Proof.** Using Lemma 3.4, we immediately see that the entries in \( A \) are all distinct and hence \( A \) is an \( n \)-dimensional permutation array of type \( m_1, m_2, ..., m_n \). Suppose (*) holds for some \( i_1, i_2, ..., i_n, j_1, j_2, ..., j_n \) and \( h_1, h_2, ..., h_n \). Then we get the following equation:

\[
(\alpha^{\sum_{t=0}^{m_n} h_t m_{i+1} m_{i+2}...m_n} - 1)\alpha^{\sum_{t=0}^{m_n} i_t m_{i+1} m_{i+2}...m_n} = (\alpha^{\sum_{t=0}^{m_n} h_t m_{i+1} m_{i+2}...m_n} - 1)\alpha^{\sum_{t=0}^{m_n} j_t m_{i+1} m_{i+2}...m_n}.
\]

Write \( h = \sum_{t=0}^{m_n} h_t m_{i+1} m_{i+2}...m_n \). Then our given conditions imply that \( h < m_1 m_2 ... m_n = p - 1 \) and hence the only way \( \alpha^h - 1 \) could equal 0 is by having \( h = 0 \) and then we are done since in that case, each \( h_t \) must equal 0. We may therefore assume that \( \alpha^h - 1 \) is not 0 and hence cancel it on both the sides to get

\[
\sum_{t=0}^{m_n} i_t m_{i+1} m_{i+2}...m_n = \sum_{t=0}^{m_n} j_t m_{i+1} m_{i+2}...m_n.
\]

Then either using Lemma 3.1 or by using the fact that we are working in a field, it follows that we get the equality

\[
(i_1, i_2, ..., i_n) = (j_1, j_2, ..., j_n)
\]

and so \( A \) is a modular Costas array of type \( m_1, m_2, ..., m_n \) as claimed.

**Example.** Let \( p = 6t + 1 \) be a prime power and let \( \alpha \) be a primitive element in \( \text{GF}(p) \). Consider the following matrix \( A \) of order 3 \( \times \) 2\( t \):

\[
\begin{pmatrix}
1 & \alpha & \alpha^2 & ... & \alpha^{2t-1} \\
\alpha^{2t} & \alpha^{2t+1} & \alpha^{2t+2} & ... & \alpha^{4t-1} \\
\alpha^{4t} & \alpha^{4t+1} & \alpha^{4t+2} & ... & \alpha^{6t-1}
\end{pmatrix}.
\]

Theorem 3.1 shows that \( A \) is a Costas array of type 3, 2\( t \). It is worth noting here that the 2\( t \) columns of the matrix \( A \) give the set of all non-zero differences in \( \text{GF}(p) \) and hence are a set of initial blocks for the construction of a Steiner triple system on \( v = 6t + 1 \). This construction (due to Peltesohn, see [2]) is among the oldest known constructions of Steiner systems.
4. Conclusions and conjectures

The fact that any DDP sequence can be extended to a longer one (Theorem 2.1) in more than one way makes them inherently far more abundant than Costas sequences. We nevertheless make the following conjecture:

**Conjecture 4.1.** For any \( n \geq 2 \), with only finitely many exceptions there are at least \( n \) Costas sequences on \( n \) elements.

The algebra behind the proof of Theorem 2.3 appears to indicate that there are far more than \( p - 1 \) ways of building DDP sequences in the manner outlined.

**Conjecture 4.2.** There are at least \( (p - 1)^2 / 2 \) DDP sequences on \( p^x - 1 \) elements, \( p \) any odd prime, \( x \geq 1 \).

Acknowledgements

The second author wishes to thank Deakin University for supporting his visit to Australia where this work was completed. Both authors wish to thank Dr. S. Boztas for introducing them to the Costas sequence problem.

References