GENERALIZED WELCH-COSTAS SEQUENCES AND THEIR APPLICATION TO VATICAN ARRAYS

HONG Y. SONG AND SOLOMON W. GOLOMB

January 26, 1994

ABSTRACT. We propose a family of sequences, $a_1, a_2, \ldots, a_{kn}$, of length kn for all positive integers n and k. A permutation $a_1, a_2, a_3, \ldots, a_{kn}$ of $0, 1, 2, \ldots, kn-1$ is an (n,k)-sequence if $a_{s+d} - a_s \not\equiv a_{t+d} - a_t \pmod n$ for every s, t and d such that $1 \le s < t < t+d \le kn$ and such that $\lfloor \frac{a_{s+d}}{n} \rfloor = \lfloor \frac{a_s}{n} \rfloor$ and $\lfloor \frac{a_{t+d}}{n} \rfloor = \lfloor \frac{a_t}{n} \rfloor$, where $\lfloor x \rfloor$ is the integer part of x.

We show that such a sequence exists whenever $kn+1$ is an odd prime, and exhibit all "essentially distinct" $(n,2)$-sequences for $n \le 10$. Furthermore, we demonstrate that whenever an (n,k)-sequence exists then there exists an $n \times kn$ "Vatican array" having cyclic columns. This achieves approximately $1/k$ times the upper bound on the number of Vatican rows on kn symbols. Vatican arrays find applications to various multi-user communications environments such as multi-user radar and sonar, fiber-optic CDMA networks, and frequency-hopping multiple access communications.

1. Introduction

Consider the sequence $0, 1, 4, 6, 5, 3, 7, 2$ of length 8 (a_i for $1 \le i \le 8$) and its difference triangle shown in Fig. 1, where the difference $a_j - a_i \pmod 4$ for $1 \le i < j \le 8$ is calculated whenever $a_i, a_j < 4$ or $a_i, a_j \ge 4$. We designate such a pair (a_i, a_j) as "comparable." A $*$ in the triangle represents an incomparable situation. Observe that in any row of this triangle the differences are all distinct mod 4. We call this sequence $a_1, a_2, \ldots, a_8$ a "(4, 2)-sequence," or a "sequence with parameters (4, 2)."

More generally, we can define "comparability" of a pair (a_i, a_j) to mean that the integer parts of both a_i/n and a_j/n are the same.

Definition 1.1. Let $a_1, a_2, \ldots, a_{kn}$ be a permutation of $0, 1, 2, \ldots, kn-1$. Let (a_i, a_j) be called a "comparable pair" if $\lfloor a_i/n \rfloor = \lfloor a_j/n \rfloor$, where $\lfloor x \rfloor$ is the integer

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 94A12; Secondary 05B30, 94B60.

Key words and phrases. Singly-periodic Costas sequences, Florentine and Vatican arrays, Frequency hopping patterns.

This work was supported in part by the United States Office of Naval Research under Grant No. N00014-90-J-1341.

Part of this paper was presented at the *2nd International Conference on Finite Fields : Theory, Applications and Algorithms*, which was held in the UNLV, Las Vegas, NV, Aug.17-21, 1993.

This paper is in final form and no version of it will be submitted for publication elsewhere.

0		1		4		6		5		3		7		2
	1		*		2		3		*		*		*	
		*		*		1		*		2		3		
			*		*		*		1		*			
				*		2		3		*				
					3		*		*					
						*		1						
							2							

FIGURE 1. Difference triangle (mod 4) of the sequence $0, 1, 4, 6, 5, 3, 7, 2$.

part of x. Then, $a_1, a_2, \ldots, a_{kn}$ is called an "(n, k)-sequence" if

$$a_{s+d} - a_s \not\equiv a_{t+d} - a_t \pmod{n} \tag{1}$$

for every s, t and d such that $1 \le s < t < t + d \le kn$ and such that (a_{s+d}, a_s) and (a_{t+d}, a_t) are comparable pairs.

In Section 2 we will prove that when $kn + 1 = p > 2$ is a prime, there exists a construction for such a sequence $a_1, a_2, \ldots, a_{kn}$. This construction reduces to the "log-Welch construction" [Gol84, GT84] for *singly-periodic Costas sequences* of length $p - 1$ when $k = 1$ and $p = n + 1$ is a prime.

From the $(4, 2)$-sequence shown in Fig. 1, one can construct the following 4×8 array V of 8 symbols in which the top row is $a_1, a_2, \ldots, a_8$ and the columns are cyclic shifts of either $0, 1, 2, 3$ or $4, 5, 6, 7$, as shown in Fig. 2. The array V has the two properties that (1) each row is a permutation of $0, 1, 2, \ldots, 7$ and (2) for any two symbols a and b and for any integer m from 1 to 7 there exists at most one row in which b is m steps to the right of a. A $k \times n$ array which satisfies these properties is known as a "Florentine array." Further, the array V is actually a "Vatican array," which is defined to be a Florentine array such that no two symbols are the same in any column.

$$V = \begin{array}{|cccccccc|} \hline 0 & 1 & 4 & 6 & 5 & 3 & 7 & 2 \\ 1 & 2 & 5 & 7 & 6 & 0 & 4 & 3 \\ 2 & 3 & 6 & 4 & 7 & 1 & 5 & 0 \\ 3 & 0 & 7 & 5 & 4 & 2 & 6 & 1 \\ \hline \end{array}$$

FIGURE 2. A 4×8 Vatican array having cyclic columns.

Florentine and/or Vatican arrays (or squares) were extensively studied in [GT85, EGT89, GET90, Etz90, Song91, Tay91, Song92]. These combinatorial structures have a wide range of applications in communications engineering: design of frequency hopping patterns for multiple-access communications environments [LG74, Maric92, McE81, SD84, Sea82, Song92, SRG93, Tay91], design of radar and sonar arrays for improved range-Doppler measurements [GT82, Maric92], and design of modulation signals for optical PPM modulations [GRT87, SD83]. They also find applications in the area of design of experiments [Bug49, GT85, Song91, Wil49] and in extremal graph theory such as edge-decompositions of complete directed graphs [Etz90, EGT89, GET90, Men68, Song91, Til80].

In [EGT89, GET90], the polygonal-path construction for Florentine squares is introduced, in which the columns are cyclic shifts of each other. It was also proved that a polygonal-path Florentine square of size $n \times n$ exists if and only if there exists a "singly-periodic Costas array" of size $n \times n$, or equivalently, a singly-periodic Costas sequence of length n (which is an $(n, 1)$-sequence in our terminology). Similarly, we will prove in Section 4 that if there exists an (n, k)-sequence of length kn then we can construct an $n \times kn$ Vatican array and hence an $n \times (kn+1)$ Florentine array.

This paper is organized as follows: In Section 2, our main theorem on the construction for (n, k)-sequences (whenever $kn+1$ is a prime) is proved. Some necessary conditions for the existence of $(n, 2)$-sequences are proved. In Section 3, some transformations of $(n, 2)$-sequences are discussed and computer search results for those of length $2n$ for $n = 1, 2, \ldots, 10$ are presented with a brief sketch of an algorithm which has been run to conclude that no $(10, 2)$-sequence exists. (This took about 100 hours of CPU time on a Sun Sparc station 600.) All the "essentially distinct" $(n, 2)$-sequences for $n \leq 10$ found by computer are explicitly shown in Table 1. In Section 4 we discuss the construction of Vatican arrays and the current state of related problems. Some remarks and open problems (conjectures) are presented in Section 5.

2. Existence of (n, k)-sequences

Theorem 2.1. *Let α be a primitive root modulo $p = kn+1 > 2$ where p is a prime. For $i = 1, 2, \ldots, kn$, take the value of $\log_\alpha(i)$ to be between 0 and $kn-1$ such that $\log_\alpha(i) = j$ if $\alpha^j = i$. Let q_i and r_i be the quotient and remainder, respectively, when $\log_\alpha(i)$ is divided by k; that is, $\log_\alpha(i) = kq_i + r_i$, where $0 \leq r_i \leq k-1$. Then, $a_i = q_i + r_i n$ for $i = 1, 2, \ldots, kn$ is an (n, k)-sequence.*

Proof. Since $q_i = \frac{1}{k}(\log_\alpha(i) - r_i)$, we have $a_i = q_i + nr_i = \frac{1}{k}(\log_\alpha(i) - r_i) + nr_i$, or $ka_i = \log_\alpha(i) - r_i + knr_i = \log_\alpha(i) + (kn-1)r_i$, and hence

$$\alpha^{ka_i} \equiv i\alpha^{(kn-1)r_i} \pmod{p}. \tag{2}$$

Since $q_i < n$ for all i, we conclude that a_i is the unique integer satisfying (2) for which the integer part of a_i/n is r_i. Consequently, if (a_i, a_j) is a comparable pair then $r_i = \lfloor a_i/n \rfloor = \lfloor a_j/n \rfloor = r_j$, and hence, $\alpha^{ka_i}/\alpha^{ka_j} \equiv i/j \pmod{p}$.

Now suppose (a_s, a_{s+d}) and (a_t, a_{t+d}) are two comparable pairs where $1 \leq s < t < t+d \leq kn$ and $a_{s+d} - a_s \equiv a_{t+d} - a_t \pmod{n}$. Then,

$$\begin{aligned} & k(a_{s+d} - a_s) \equiv k(a_{t+d} - a_t) \pmod{kn}, \\ \Longrightarrow\quad & \alpha^{k(a_{s+d} - a_s)} \equiv \alpha^{k(a_{t+d} - a_t)} \pmod{p}, \\ \Longrightarrow\quad & \frac{s+d}{s} \equiv \frac{t+d}{t} \pmod{p}, \\ \Longrightarrow\quad & d \equiv 0 \quad \text{or} \quad s \equiv t \pmod{p}. \end{aligned}$$

Since $0 < d < kn = p-1$ and $1 \leq s \neq t \leq kn$, we have a contradiction. □

With the prime $p = 13$ and Theorem 2.1 one can construct these sequences with the parameters $(12, 1)$, $(6, 2)$, $(4, 3)$, $(3, 4)$, $(2, 6)$ and $(1, 12)$. The first three of them

$(n,k)=(12,1)$	$a_i = \log_2(i)$	0	1	4	2	9	5	11	3	8	10	7	6
$(n,k)=(6,2)$	r_i	0	1	0	0	1	1	1	1	0	0	1	0
	q_i	0	0	2	1	4	2	5	1	4	5	3	3
	$a_i = q_i + 6r_i$	0	6	2	1	10	8	11	7	4	5	9	3
$(n,k)=(4,3)$	r_i	0	1	1	2	0	2	2	0	2	1	1	0
	q_i	0	0	1	0	3	1	3	1	2	3	2	2
	$a_i = q_i + 4r_i$	0	4	5	8	3	9	11	1	10	7	6	2

FIGURE 3. Examples of (n,k)-sequences of length 12 from $p = 13$.

```
0   6   2   1   10   8   11   7   4   5   9   3
  *   *   5   *   4   3    2   *   1   *   *
    2   *   *   *   1   5    *   *   *   4
      1   4   *   *   3   *    *   2   5
        *   2   *   *   *   *    4   *
          *   5   *   3   *   1    *
            *   1   2   4   5   *
              *   *   3   *   *
                4   *   *   2
                  5   3   1
                    *   *
                      3
```

FIGURE 4. Difference triangle of the $(6,2)$-sequence.

are shown in Fig. 3. Note that the $(12,1)$-sequence, given by $a_i = \log_2 i$, is exactly the "log-Welch construction" for *Costas arrays* [Gol84, GT84] of order 12. The difference triangle mod 6 of the $(6,2)$-sequence for $p = 13$ is shown in Fig. 4.

From Figures 1 and 4, it seems that every non-zero residue occurs exactly the same number of times in the difference $(\mathrm{mod}\ n)$ triangle of an (n,k)-sequence. What we can prove is the following:

Lemma 2.1. *Let N_i, for $i = 1, 2, \ldots, n-1$, be the number of i's in the difference $(\mathrm{mod}\ n)$ triangle of an (n,k)-sequence $\{a_j\}$, and let $N = \sum_{i=1}^{n-1} N_i$. If n is odd then $N_1 + N_{n-1} = kn$, $N_2 + N_{n-2} = kn$, $\ldots$, and $N_{(n-1)/2} + N_{(n+1)/2} = kn$. If n is even, then $N_1 + N_{n-1} = kn$, $N_2 + N_{n-2} = kn$, $\ldots$, $N_{n/2-1} + N_{n/2+1} = kn$, and $N_{n/2} = kn/2$. In both cases, we have $N = kn(n-1)/2$.*

Proof. Since $\{a_j\}$ contains every residue mod kn exactly once, the residue $i+1$ occurs either to the right of i or to the left of i (not both) exactly once for all i. This gives $N_1 + N_{n-1} = kn$. Similarly, all the rest follow easily. □

For the remaining part of this section we will confine ourselves exclusively to the discussion of $(n, k = 2)$-sequences. In this case, we have $N = n(n-1)$ from Lemma 2.1. In particular, we have

Corollary 2.1. *Let $p = 2n+1$ be a prime, and $\{a_i\}$ be an $(n,2)$-sequence determined by the construction in Theorem 2.1. In the difference* (mod n) *triangle we have $N_i = n$ for $i = 1, 2, \dots, n-1$.*

Proof. Suppose n is even, and hence $p \equiv 1 \pmod 4$. We will show that in the difference (mod n) triangle, for $i = 1, 2, \dots, n/2-1$, the difference i occurs at some position if and only if the difference $n-i$ occurs at the mirror position along the constant middle column which contains the difference $n/2$ exactly n times. To show this, note that $a_i = (1/2)\log_\alpha(i) \le n-1$ if i is a quadratic residue mod p and $a_i = (1/2)(\log_\alpha(i)-1)+n \ge n$ otherwise. Therefore (a_s, a_{s+d}) is comparable if and only if (a_{p-s-d}, a_{p-s}) is comparable for $1 \le s < s+d \le n$. The differences of these pairs are

$$\begin{aligned} a_{s+d} - a_s &\equiv \frac{1}{2}\log_\alpha \frac{s+d}{s} \pmod n, \\ a_{p-s} - a_{p-s-d} &\equiv \frac{1}{2}\log_\alpha \frac{p-s}{p-s-d} \equiv \frac{1}{2}\log_\alpha \frac{s}{s+d} \pmod n. \end{aligned}$$

Therefore, $(a_{s+d} - a_s) + (a_{p-s} - a_{p-s-d}) = n$. Since $N_i + N_{n-i} = 2n$, we have $N_i = N_{n-i} = n$ for $i = 1, 2, \dots, n/2-1$. Since (a_i, a_{p-i}) is comparable for $i = 1, 2, \dots, n$, the middle column contains $a_{p-i} - a_i = (1/2)\log_\alpha(-1) = n/2$ exactly n times. This proves $N_{n/2} = n$.

The case where n is odd can be proved similarly. □

Lemma 2.2. *Let $a_1, a_2, \dots, a_{2n}$ be an $(n,2)$-sequence. For $d = 1, 2, \dots, 2n-1$ the number of comparable pairs of the form (a_s, a_{s+d}) must be less than n.*

Proof. In any row of the difference triangle, the differences must all be distinct mod n and zero cannot occur. Therefore, the number of comparable pairs in any row d must be $\le n-1$. □

Given an $(n,2)$-sequence $\{a_i\}$ of length $2n$, let $\{b_i\}$ be the binary sequence of length $2n$ and weight n determined by the rule $b_i = 0$ if $a_i < n$ and $b_i = 1$ if $a_i \ge n$. In this binary sequence, k consecutive 0's (or 1's) surrounded by 1's (by 0's) on the left and right is called a "run" of length k. Now, (a_i, a_j) is a comparable pair if and only if $b_i = b_j$, and in this case we also call (b_i, b_j) comparable. In the sequence of b_j's, let R be the total number of runs, R_i the number of runs of length i, and C_i the number of comparable pairs of the form (b_s, b_{s+i}).

Corollary 2.2. *Let $a_1, a_2, \dots, a_{2n}$ be an $(n,2)$-sequence, $b_i = 0$ if $a_i < n$, and $b_i = 1$ if $a_i \ge n$. Then, in the sequence of b_i's, the total number R of runs is at least $n+1$ and at most $n + \lfloor (n+1)/2 \rfloor$. Furthermore, we have $n - \lfloor (n+1)/2 \rfloor \le C_1 \le n-1$ and $n-1-R_2 \le C_2 \le n-1$.*

Proof. To show the lower bound on R, calculate the number C_1. Since there are R runs in the sequence $\{b_j\}$ if and only if there are $R-1$ incomparable adjacent pairs (b_s, b_{s+1}), we have $C_1 = (2n-1) - (R-1) = 2n - R$. Using Lemma 2.2, we have $n - 1 \ge C_1 = 2n - R$, or $R \ge n+1$.

To show the upper bound on R, estimate R in terms of R_2 in two different ways. The first inequality, $R \le 2n - R_2$, follows from $2n - R = \sum_{i\ge1} iR_i - \sum_{i\ge1} R_i = \sum_{i\ge2}(i-1)R_1 \ge R_2$. The second inequality, $R \le R_2 + n + 1$, follows from the following estimate of C_2, the number of comparable pairs of the form (b_s, b_{s+2}): a run of length 1 contributes one such comparable pair if it is neither the beginning nor the ending of the sequence, a run of length 2 does not contribute at all, and for $i > 2$, a run of length i contributes $i-2$ such comparable pairs. Since these contributions are mutually disjoint, we have, in conjunction with Lemma 2.2, the following:

$$\begin{aligned} n-1 \geq C_2 &\geq (R_1-2)+0+\sum_{i\geq 3}(i-2)R_i \\ &= R+\sum_{i\geq 4}(i-3)R_i-(R_2+2) \geq R-(R_2+2). \end{aligned}$$

The sum of two inequalities, $R \leq 2n - R_2$ and $R \leq R_2 + n + 1$, implies $R \leq n + (n+1)/2$.

The bounds on C_1 and C_2 follow easily. □

Corollary 2.3. *Let $p = 2n+1$ be a prime, the binary sequence $\{b_i\}$ of length $2n$ be given by the "Legendre symbol." Then we have (1) $C_i \leq n-1$ for $i = 1, 2, \ldots, p-2$, (2) $R = n+1$, and hence (3) $C_1 = n-1$ and $n-1-R_2 \leq C_2 \leq n-1$.*

Proof. The statement (1) is easily seen to be true by Theorem 2.1 and Lemma 2.2. See [Dav92] for an elementary proof that $R = \frac{p+1}{2} = n+1$. □

3. Transformations and computer searches

When the computer search is to be done either to find an example or to conclude that none exists, one problem is the time spent by the computer to check exhaustively the validity of all possible candidates. To find an efficient algorithm, one must find all possible transformations which transform one sequence into another preserving the required properties. This gives a partition of the entire search space into disjoint subsets (usually called "equivalence classes"), and enables one to rule out an entire class in the search space by ruling out a single representative of the class [Gol61, Rys63]. Therefore, it is important that the partition be done in such a way that each class contains as many possible search points as possible. This will reduce drastically the number of candidates to be checked.

Suppose there exists an $(n,2)$-sequence $a_1, a_2, \ldots, a_{2n}$. Let a_i be called of type A if $0 \leq a_i \leq n-1$, and of type B otherwise. We will describe a representative of the "class" containing this sequence, which we denote by $\hat{a_1}, \hat{a_2}, \ldots, \hat{a_{2n}}$, and which can be obtained by a combination of the following five operations, S_A, S_B, M, R, and P, all of which preserve the required properties: S_A (or S_B) is to add (mod n) some constant c to every term of type A (or, of type B, respectively); M is to multiply (mod n) some constant m times all the a_i's, where m is relatively prime to n; R is to take the mirror image (reversal of the a_i's); P is to interchange type A and type B in $\{a_i\}$ by either adding n if $a_i < n$ or by subtracting n if $a_i \geq n$. Note that the operations S_A, S_B, and M must take their values from the same range so that the result is of the same type as the original, and the operation P must take its values from the other range, so that the type is changed. It is easy to verify that all of the above transformations preserve the property that in the difference triangle (mod n) the differences of comparable pairs having the same distance are all distinct (mod n).

We may assume that a_1 is of type A without loss of generality. (Otherwise, use P to make the first term of type A.) Subtract $a_1 \pmod{n}$ from every term of type A. If j is the smallest subscript for which a_j is of type B, then subtract a_j (mod n) from every term of type B. This gives $\hat{a_1} = 0$ and $\hat{a_j} = n$. Now, let $i > 1$ be the smallest subscript for which a_i is of type A. We know that $1 \leq a_i \leq n-1$ since $a_1 = 0$ and $i > 1$. By Lemma 3.1 there exists m such that (1) m is relatively prime to n, and (2) $a_i m \pmod{n}$ in the range from 1 to $n-1$ is a divisor of n. Therefore, by multiplying such m times every term, we obtain $\hat{a_i} = d$ where d is a divisor of n such that $1 \leq d < n$.

Lemma 3.1. *Let U be the multiplicative group mod n, and let $dU = \{dm | m \in U\}$ for every divisor d of n such that $1 \leq d < n$. Then, $Z_n - \{0\} = \bigcup_{d|n} dU$, where the union is over all the divisors d, $1 \leq d < n$, of n and where $d_1U \bigcap d_2U = \emptyset$ if $d_1 \neq d_2$.*

Now, the following is a brief sketch of a backtracking algorithm [GB65] which took only about 100 hours of CPU time in a Sun Sparc station 600 to search exhaustively for a $(10,2)$-sequence, and concluded that none exists: First, find all the "essentially distinct" binary vectors[1] $b_1 = 0, b_2, \dots, b_{20}$ with weight 10 (we call these "patterns") such that for each d from 1 to 10 the number of occurrences of $b_s = b_{s+d}$ is ≤ 9. It turned out there exist exactly 6214 such binary patterns. For each such pattern, we will assign a value of type A (in the range from 0 to 9) to each position i if $b_i = 0$, or a value of type B (in the range from 10 to 19) if $b_i = 1$. For the positions of type A, note that we could fix $a_1 = 0$ and we only have to try $a_i = d$ for the divisors $1 \leq d < n$ of n where i is the second smallest subscript for which $b_i = 0$. For the positions of type B, we could fix $a_j = 10$ where j is the smallest subscript for which $b_j = 1$.

Let $w_2(n)$ be the number of "essentially distinct" $(n,2)$-sequences, where two sequences are not essentially distinct if one can be transformed into another by the above transformations. The exact value of $w_2(n)$ for $1 \leq n \leq 10$ is shown in Table 1.

4. Applications of (n,k)-sequences

An application of (n,k)-sequences is to construct $n \times kn$ Vatican arrays such that the columns are cyclic shifts of $cn, cn+1, cn+2, \dots, (c+1)n-1$ for some c. Recall the definitions of "Florentine array" and "Vatican array" of size $n \times kn$ in the Introduction.

Theorem 4.1. *Assume there exists an (n,k)-sequence $a_1, a_2, \dots, a_{kn}$. Then there exists an $n \times kn$ Vatican array. (Hence, there exists an $n \times (kn+1)$ Florentine array by adjoining a constant column of "asterisks.")*

Proof. Let $V = (v(i,j))$ denote an $n \times kn$ matrix where $i = 0, 1, \dots, n-1$ and $j = 0, 1, \dots, kn-1$ are row and column indices respectively. Put $a_1, a_2, \dots, a_{kn}$ in the top row of V, and fill column j of V using a cyclic shift of $cn, cn+1, \dots, (c+1)n-1$ where $c = \lfloor a_j/n \rfloor$ is the integer part of a_j/n.

[1] Two binary patterns are not essentially distinct if two $(n,2)$-sequences having these patterns (assuming they exist) are not essentially distinct.

TABLE 1. The number $w_2(n)$ of "essentially distinct" $(n,2)$-sequences for $n \leq 10$ is shown. The sequences $\{a_i\}$ are $(n,2)$-sequences, and $\{b_i\}$ are corresponding binary patterns. For convenience, $10, 11, \ldots, 21$ are represented by $A, B, \ldots, L$. The sequences followed by "$\star$" are essentially the same as those given by the construction in Theorem 2.1 for $2n+1$ a prime.

n	$2n$	$w_2(n)$	CPU time	$b_i \longrightarrow a_i$
1	2	1		$01 \longrightarrow 01\star$
2	4	1		$0110 \longrightarrow 0231\star$
3	6	2		$001011 \longrightarrow 013254\star$
				$011001 \longrightarrow 035124$
4	8	3		$00111010 \longrightarrow 01465372$
				$01001110 \longrightarrow$ 04217563 04235761
5	10	5	~ 0.1 Sec.	$0011101001 \longrightarrow 0159738246$
				$0100011101 \longrightarrow$ 0513476928 $0514367928\star$
				$0111010001 \longrightarrow$ 0589173246 0596184237
6	12	4	~ 4.0 Sec.	$001110010101 \longrightarrow 026B831A4957$
				$010011110010 \longrightarrow$ $06218A7B4593$ $0621A8B74593\star$
				$010111000110 \longrightarrow 061BA8452793$
7	14	8	~ 18.5 Sec.	$00110010110011 \longrightarrow$ $017B24D5CA3698$ $017B64C3D825A9$
				$01001110001101 \longrightarrow 07148AB6539D2C$
				$01011000111010 \longrightarrow 071CA524D986B3$
				$01100010111001 \longrightarrow 07A124958DC63B$
				$01100101011001 \longrightarrow 07B1395A48D62C$
				$01101110001001 \longrightarrow 0791AB8365D42C$
				$01110010110001 \longrightarrow 079A14D28C653B$
8	16	8	~ 16.3 Min.	$0010111001110100 \longrightarrow$ $0182AFD379BE6C54$ $0182E9B37FDA6C54\star$
				$0011101001011100 \longrightarrow$ $018AD3B26F79EC54$ $018EB3D2697FAC54$
				$0111001001001110 \longrightarrow$ $08BD23A15E769FC4$ $08DB23E15A76F9C4$ $089F27E51A36BDC4$ $08F927A51E36DBC4$
9	18	1	~ 1.5 Hrs.	$011000010101111001 \longrightarrow$ $09F1873A4H6GBCE25D\star$
10	20	0	~ 100 Hrs.	NONE
11	22	≥ 1	$\overset{?}{\sim} 21$ Days	$0000101001100110101111 \longrightarrow$ $0182B9K35CFA7LJ4E6IDHG\star$

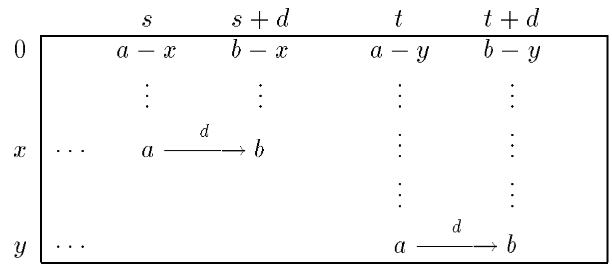

FIGURE 5. Proof that V is a Vatican array.

Suppose V is not a Vatican array. Then there exist two rows, say row x and row y, and two numbers, say a and b, such that b is d steps to the right of a in both row x and row y for some integer d, as shown in Fig. 5. Find the numbers in the top row at the columns in which those a and b occur. These must be $a-x$ and $b-x$ from a and b in row x, and $a-y$ and $b-y$ from those in row y. The arithmetic is taken mod n and the values must be in an appropriate range so that $\lfloor \frac{a-x}{n} \rfloor = \lfloor \frac{a-y}{n} \rfloor = \lfloor \frac{a}{n} \rfloor$ and $\lfloor \frac{b-x}{n} \rfloor = \lfloor \frac{b-y}{n} \rfloor = \lfloor \frac{b}{n} \rfloor$. Observe that $a-x$ and $a-y$ are comparable, and so are $b-x$ and $b-y$. Thus, we have $a_t - a_s = (a-y) - (a-x) \equiv x - y \equiv a_{t+d} - a_{s+d} \pmod{n}$, a contradiction. □

In [Song91] a function $F(n)$ is defined to be the maximum number such that an $F(n) \times n$ Florentine array exists, and its possible values for $1 \leq n \leq 32$ are listed in a table. Among these values, $F(14)$, $F(15)$ and $F(21)$ are improved so that we now know $F(14) \geq 7$, $F(15) \geq 7$, and $F(21) \geq 7$. The first two are from the examples of $(7,2)$-sequences explicitly shown in Table 1. $F(21) \geq 7$ is from the $(7,3)$-sequence found by computer (about 1 day of CPU time), which is the top row of the 7×21 Vatican array shown in Fig. 6.

0	1	11	2	15	8	14	16	19	7	12	9	6	18	3	10	17	13	5	4	20
1	2	12	3	16	9	15	17	20	8	13	10	0	19	4	11	18	7	6	5	14
2	3	13	4	17	10	16	18	14	9	7	11	1	20	5	12	19	8	0	6	15
3	4	7	5	18	11	17	19	15	10	8	12	2	14	6	13	20	9	1	0	16
4	5	8	6	19	12	18	20	16	11	9	13	3	15	0	7	14	10	2	1	17
5	6	9	0	20	13	19	14	17	12	10	7	4	16	1	8	15	11	3	2	18
6	0	10	1	14	7	20	15	18	13	11	8	5	17	2	9	16	12	4	3	19

FIGURE 6. A 7×21 Vatican array.

5. CONJECTURES AND OPEN PROBLEMS

The conjecture that an $(n,2)$-sequence might exist for each of the positive integers $n \geq 1$ turned out to be false by exhaustive search for the case $n = 10$. It took about 100 hours of CPU time on a Sun Sparc station 600 to conclude that no $(10,2)$-sequence exists.

Two examples of sequences with parameters $(7,2)$ and $(7,3)$ shown in Table 1 and Fig. 6 suggest that a $(7,k)$-sequence might exist for each positive integer $k > 1$. Furthermore, we have the

Conjecture A. *Whenever $p > 2$ is a prime there exists at least one (p, k)-sequence of length kp for each positive integer $k > 1$.*
This turned out to be true for $p = 5$ and $1 < k \leq 6$, and for $p = 3$ and $1 < k \leq 10$. The proposed algorithm of exhaustively searching for $(n, 2)$-sequences described in Section 3 is most efficient for the case when $n = p$ is a prime, since in this case there is only one divisor d of p such that $1 \leq d < p$, namely $d = 1$, and hence three terms of the candidate can be fixed at the beginning stage of the search. We believe a little further improvement of this algorithm would reach the case $n = 13$.

For the application to the construction of Vatican/Florentine arrays of size $n \times kn$, we note that the truth of the above conjecture will show that $F(n) \geq p$ and $F(n+1) \geq p$ for all $n > 1$, where p is *any* prime factor of n such that $p < n$, and where $F(n)$ is the maximum number such that an $F(n) \times n$ Florentine array exists. This could be a major breakthrough in determining the values of $F(n)$. The current state of knowledge is that $F(n) \geq 4$ for $n \geq 32$, $F(n) \geq 6$ for $6 \leq n \leq 31$, and $p - 1 \leq F(n) \leq n$ for all $n > 1$ where p is the *smallest* prime factor of n.

Future work will be done to determine the values of N_i's of (n, k)-sequences (following Lemma 2.1 and Cor. 2.1), and also to determine the values of C_i and R_i of "binary patterns (sequences)" of $(n, 2)$-sequences (following Lemma 2.2, Cor. 2.2 and Cor. 2.3), since this will directly give the values of "non-periodic" autocorrelation values for these sequences. To be specific, let $b_i = 1$ (or $b_i = -1$, resp.) if $a_i < n$ (or $a_i \geq n$, resp.), and $\theta(\tau)$ be its non-periodic correlation function defined by $\theta_b(\tau) = \sum_{i=1}^{2n-\tau} b_i b_{i+\tau}$ where $\tau = 0, 1, 2, \ldots, 2n-1$. Then, for $\tau \neq 0$, we have $\theta_b(\tau) = C_\tau - (2n - \tau - C_\tau) = 2C_\tau - (2n - \tau)$ since $b_i b_{i+\tau} = 1$ occurs C_τ times and $b_i b_{i+\tau} = -1$ occurs $2n - \tau - C_\tau$ times. For its application to communication engineering, we are most interested in the ratio of $\max_{\tau \neq 0}\{\theta_b(\tau)\}$ to $\theta_b(0) = 2n$ for any binary sequence b_i's of length $2n$.
Conjecture B. *If the b_i's are from an $(n, 2)$-sequence of length $2n$, then*

$$\liminf_{n \to \infty} \frac{\max_{\tau \neq 0}\{\theta_b(\tau)\}}{2n} = 0.$$

Acknowledgment

The authors would like to thank Professor D. Estes in the Department of Mathematics at USC and an anonymous referee for many helpful suggestions.

References

[Bug49] B. R. Bugelski, *A note on Grant's discussion of the Latin square principle in the design of experiments*, Psychological Bulletin, **46** (1949), 49–50.

[Dav92] H. Davenport, *The Higher Arithmetic*, 6th ed., Chapter 3, Cambridge University Press, New York, 1992.

[Etz90] Tuvi Etzion, *Hamiltonian decomposition of K_n^*, patterns with distinct differences, and Tuscan squares*, Discrete Mathematics, **91** (1991), 259–276.

[EGT89] T. Etzion, S. W. Golomb, and H. Taylor, *Tuscan-k squares*, Adv. in Appl. Math., **10**, (1989), 164–174.

[GRT87] R. Gagliardi, J. Robbins and H. Taylor, *Acquisition sequences in PPM communications*, IEEE Trans. on Information Theory, **IT-33**, (1987), 738–744.

[Gol61] Solomon W. Golomb, *A mathematical theory of discrete classification*, Fourth London Symposium on Information Theory, London, Butterworth, 1961.

[Gol84] , *Algebraic constructions for Costas arrays*, Journal of Combinatorial Theory, series A, **37**, (1984), 13–21.

[GB65] S. W. Golomb and L. D. Baumert, *Backtrack programming*, Association for Computing Machinary, **12**, (1965), 516–524.

[GET90] S. W. Golomb, T. Etzion and H. Taylor, *Polygonal path constructions for Tuscan-k squares*, Ars Combinatoria, **30**, (1990), 97–140.

[GT82] S. W. Golomb and H. Taylor, *Two-dimensional synchronization patterns for minimum ambiguity*, IEEE Trans. Information Theory, **IT-28**, (1982), 600–604.

[GT84] , *Constructions and properties of Costas arrays*, Proceedings of the IEEE, **72**, (1984), 1143–1163.

[GT85] , *Tuscan squares — A new family of combinatorial designs*, Ars Combinatoria, **20-B**, (1985), 115–132.

[LG74] Abraham Lempel and Haim Greenberger, *Families of sequences with optimal Hamming correlation properties*, IEEE Trans. on Information Theory, **IT-20**, (1974), 90–94.

[Maric92] S. V. Maric and E. L. Titlebaum, *A class of frequency hop codes with nearly ideal characteristics for use in multiple-access spread-spectrum communications and radar and sonar systems*, IEEE Trans. Communications, **40** (1992), 1442–1447.

[McE81] R. J. McEliece, *Some combinatorial aspects of spread-spectrum communication systems*, New concepts in multi-user communication, (J. K. Skwirzynski, ed.) Sijthoff and Noordhoff, Rockville, Maryland, 1981, pp. 199–211.

[Men68] N. S. Mendelsohn, *Hamiltonian decomposition of the complete directed n-graph*, Theory of Graphs (P. Erdös and G. Katona, eds.), Proceedings of the Colloquium (Tihany, Hungary, Sept. 1966), Academic Press, 1968.

[Rys63] Herbert J. Ryser, *Combinatorial Mathematics*, The Carus Mathematical Monographs No. 14. John Wiley and Sons, 1963.

[SD83] A. A. Sharr and P. A. Davies, *Prime sequences: quasi-optimal sequences for OR channel code division multiplexing*, Electronic Letters, **19**, (1983), 888–890.

[SD84] , *A survey of one-coincidence sequences for frequency-hopped spread-spectrum systems*, IEE Proceedings, Part F, **131**, (1984), 719–724.

[Sea82] T. S. Seay, *Hopping patterns for bounded mutual interference in frequency hopping multiple access*, MILCOM, October 1982.

[Song91] Hong Y. Song, *On aspects of Tuscan squares*, Ph.D. Thesis, University of Southern California, 1991.

[Song92] , *Existence of circular Florentine arrays and mutually orthogonal Latin squares*, Discrete Applied Mathematics, a special issue (H. Taylor and G. S. Bloom, eds.) devoted to presentations in GolombFest(60), Oxnard, California, 1992, (to appear).

[SRG93] H. Y. Song, I. Reed, and S. W. Golomb, *On the non-periodic cyclic equivalence classes of RS codes*, IEEE Trans. on Information Theory, **IT-39**, (1993), 1431–1434.

[Tay91] Herbert Taylor, *Florentine rows or left-right shifted permutation matrices with cross-correlation values* ≤ 1, Discrete Mathematics, **93**, (1991), 247–260.

[Til80] T. W. Tilson, *A Hamiltonian decomposition of* K_{2m}^*, $2m \geq 8$, Journal of Combinatorial Theory, Series B, **29**, (1980), 68–74.

[Wil49] E. J. Williams, *Experimental designs balanced for the estimation of residual effects of treatments*, Australian Journal of Scientific Research, **A-2**, (1949), 149–168.

Communication Sciences Institute, Department of EE-Systems, m.c.-2565, University of Southern California, 3740 McClintock Ave., Los Angeles, CA 90089.

E-mail: hysong@solar.usc.edu