On the Existence of circular Florentine arrays[1]

Hong-Yeop Song

January 12, 1998[2]

Dedicated to Prof. Solomon W. Golomb on his sixtieth birthday

Department of Electronic Engineering, Yonsei University[3]
134 Shinchon, Seodamoon, Seoul 120-749, Korea
Tel:+82-2-361-4861, hysong@bubble.yonsei.ac.kr

Abstract

A $k \times n$ circular Florentine array is an array of n distinct symbols in k *circular* rows such that (1) each row contains every symbol exactly once and (2) for any pair of distinct symbols (a, b) and for any integer m from 1 to $n-1$ there is *at most* one row in which b occurs m steps to the right of a. For each positive integer $n = 2, 3, 4, \ldots$, define $F_c(n)$ to be the *maximum* number such that a $F_c(n) \times n$ circular Florentine array exists.

From the main construction of this paper for a set of mutually orthogonal Latin squares (MOLS) having an additional property, and from the known results on the existence/non-existence of such MOLS obtained by others, it is now possible to reduce the gap between the upper and lower bounds on $F_c(n)$ for infinitely many additional values of n not previously covered. This is summarized in the table for all odd n up to 81.

[1]Part of this paper is based on the presentation in GF(60), Oxnard, CA, May 29 - 31, 1992 in celebration of Professor S. W. Golomb's 60th birthday.

[2]First submitted in May 27, 1992; revised in September 3, 1992 and accepted by the guest editor H. Taylor; final revision done in January 12, 1998.

[3]Original manuiscript was written based on the work done while the author was with Communication Sciences Institute, University of Southern California, Los Angeles, CA 90089-2565.

1 Introduction

It would always be better to begin by a few examples rather than a formal definition to describe a combinatorial object called *circular Florentine array*. An example of a 4×5 circular Florentine array is shown in Figure I. Two other examples are shown below in Figures II and III, which are a 4×15 and 4×27 circular Florentine arrays, respectively. Note that each row has every symbol $0, 1, \ldots, n-1$ exactly once. Observe further that for any symbol a and for any integer $m = 1, 2, \ldots, n-1$ the symbols in m steps circularly to the right of a are all distinct throughout the array.

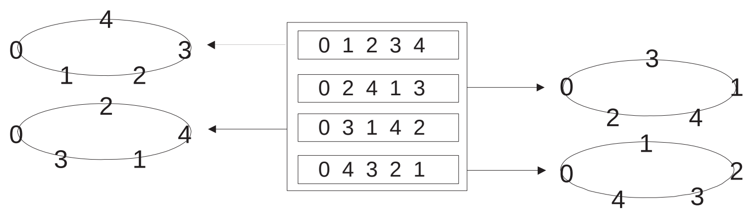

Figure I: A 4×5 circular Florentine array

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	7	1	8	2	12	3	11	9	4	13	5	14	6	10
0	4	11	7	10	1	13	9	5	8	3	6	2	14	12
0	13	7	2	11	6	14	10	3	5	12	9	1	4	8

Figure II: A 4×15 circular Florentine array

14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8	9	10	11	12	13
21	7	10	22	9	23	8	24	11	25	14	26	12	0	15	1	13	2	16	3	19	4	18	5	17	20	6
18	24	15	7	5	25	13	16	6	8	26	17	23	0	4	10	1	19	21	11	14	2	22	20	12	3	9
10	18	22	6	3	1	15	19	2	13	23	11	7	0	20	16	4	14	25	8	12	26	24	21	5	9	17

Figure III: A 4×27 circular Florentine array

Formally, a $k \times n$ circular Florentine array is an array of n distinct symbols in k circular rows such that each row contains every symbol exactly once and that for any pair of distinct symbols (a, b) and for any integer m from 1 to $n-1$ there is *at most* one row in which b occurs m steps (circularly) to the right of a. For convienence, define $F_c(n)$ for each positive integer n to be *the maxmum number such that a $F_c(n) \times n$ circular Florentine array exists.* The examples shown in Figures I, II, and III prove that $F_c(5) \geq 4$, $F_c(15) \geq 4$, and $F_c(27) \geq 4$.

Proposition 1.1 *$p - 1 \leq F_c(n) \leq n - 1$, for each $n = 2, 3, 4, \ldots$, where p is the smallest prime factor of n.*

Proof : Let $n \geq 2$ be a positive integer. For any fixed symbol a, since there are at most $n-1$ ordered pairs of the form (a, x) where $a \neq x$, the number of circular Florentine rows that could possibly exist is clearly at most $n - 1$. On the other hand, it is not hard to show that the top $p - 1$ rows of the multiplication table mod n with borders in the natural order form a $(p - 1) \times n$ circular Florentine array, where p is the smallest prime factor of n. ∎

The exact value of $F_c(n)$ and the related problems have been investigated by others [GET90, GT85, Song91, Tay91] for the direct application of $F_c(n)$ rows of a circular Florentine array into communication signal designs such as frequency hopping patterns, radar arrays and sonar arrays. There are at least two previous results concerning the value of $F_c(n)$. These are (1) $F_c(n) = 1$ whenever n is even [GET90], and (2) $F_c(n) \leq n - 2$ whenever "Bruck-Ryser Theorem" rules out the existence of a finite projective plane of order n [GET90, EGT89, Rys82, Hal86].

In Section 2, we will prove the following necessary and sufficient condition for the existence of a $k \times n$ circular Florentine array. The construction in the proof results in not only the above two previous results, but also some refinement for the exact value of $F_c(n)$ for infinitely many values of n other than listed in (1) or (2) above.

Theorem 1.1 *There exists a circular Florentine array of size $k \times n$ if and only if there exists a set of k mutually orthogonal Latin squares of order n such that the rows of any square are cyclic shifts of each other and that every square is obtainable from any other only by permuting the rows.*

n	$F_c(n)$	LB	UB	n	$F_c(n)$	LB	UB
3	2	*prime*		43	42	*prime*	
5	4	*prime*		45	$2,\ldots,43$	$*$	Cor.2.3
7	6	*prime*		47	46	*prime*	
9	2	search		49	$6,\ldots,48$	$*$	$\star$
11	10	*prime*		51	$2,\ldots,48$	$*$	Cor.2.4
13	12	*prime*		53	52	*prime*	
15	4	search		55	$4,\ldots,54$	$*$	$\star$
17	16	*prime*		57	$7,\ldots,55$	‡	Cor.2.1
19	18	*prime*		59	58	*prime*	
21	$4,\ldots,19$	‡	Cor.2.1	61	60	*prime*	
23	22	*prime*		63	$6,\ldots,62$	‡	$\star$
25	$4,\ldots,24$	$*$	$\star$	65	$4,\ldots,63$	$*$	Cor.2.3
27	$4,\ldots,26$	search	$\star$	67	66	*prime*	
29	28	*prime*		69	$2,\ldots,66$	$*$	Cor.2.4
31	30	*prime*		71	70	*prime*	
33	$3,\ldots,30$	†	Cor.2.4	73	72	*prime*	
35	$4,\ldots,33$	$*$	Cor.2.3	75	$2,\ldots,73$	$*$	Cor.2.3
37	36	*prime*		77	$6,\ldots,75$	$*$	Cor.2.1
39	$3,\ldots,38$	†	$\star$	79	78	*prime*	
41	40	*prime*		81	$2,\ldots,80$	$*$	$\star$

Table I: Possible values of $F_c(n)$ for all odd n from 3 to 81.

$*$ — basic lower bound, one less than the smallest prime factor.

† — Theorem 1.1 and Schellenberg *et. al.*

‡ — Theorem 1.1 and Jungnickel (See Section 3 for †, ‡, and "search").

$\star$ — basic upper bound, which is $n-1$.

Cor.— See Section 2 for Corollaries.

Finally, all possible values of $F_c(n)$ for $3 \leq n \leq 81$, n odd, are shown in Table 1. This summarizes our current state of knowledge on $F_c(n)$ and is an updated table from [Song91].

2 Proof by construction and its implication

Proof of Theorem 1.1 : Suppose we are given a $k \times n$ circular Florentine array, which will be denoted by $C = (c(i,j))$ in matrix notation where $c(i,j) \in \{a_0, a_1, \ldots, a_{n-1}\}$ for $i = 1, 2, \ldots, k$ and $j = 0, 1, 2, \ldots, n-1$. Assume that the top row is in the natural order $a_0, a_1, a_2, \ldots, a_{n-1}$ (rename the symbols if necessary).

We will construct a set of k squares, $L_1, L_2, \ldots, L_k$, of size $n \times n$ using only the cyclic shits of $a_0, a_1, a_2, \ldots, a_{n-1}$. Therefore, it is sufficent to specify the left-most column of each square (column 0). Rows and columns of the square have lables $0, 1, 2, \ldots, n-1$. For each $x = 1, 2, \ldots, k$, consider the following relation:

$$\text{For } i = 0, 1, 2, \ldots, n-1, \quad c(x,i) = a_j \quad \Longrightarrow \quad L_x(j,0) = a_i. \tag{2.1}$$

First, note that the left-most column of L_x given by Eq.(2.1) is the inverse permutation of those induced by the row x of C. Here, we use the interpretation of each row as a permutation of symbols by the rule $c(1,i) \to c(x,i)$ for $i = 0, 1, 2, \ldots, n-1$. Therefore, each column of L_x is a permutation. Since each row is a cyclic shift of $a_0, a_1, \ldots, a_{n-1}$, this proves that L_x is Latin.

To show the orthogonality of L_s and L_t for some $1 \leq s < t \leq k$, suppose, on the contrary, that they are not orthogonal. Then, there are two corresponding positions in both the squares such that the two ordered pairs from these positions are the same. That is, for some indices x, y, u, and v,

$$L_s(x,y) = L_s(u,v) = a_i \quad \text{and} \quad L_t(x,y) = L_t(u,v) = a_j,$$

for some symbol a_i and a_j. This implies

$$\begin{aligned} L_s(x,0) &= a_{i \ominus y}, \quad L_t(x,0) = a_{j \ominus y}, \quad \text{and} \\ L_s(u,0) &= a_{i \ominus v}, \quad L_t(u,0) = a_{j \ominus v}, \end{aligned}$$

where $\ominus$ denotes mod n subtraction. This can happen only if

$$\begin{aligned} c(s, i \ominus y) = \quad & a_x & = c(t, j \ominus y), \quad \text{and} \\ c(s, i \ominus v) = \quad & a_u & = c(t, j \ominus v). \end{aligned}$$

But, it implies that the symbol a_u is $y \ominus v$ steps to the right of a_x in both the row s and the row t of C, a desired contradiction.

Similarly for the converse. ■

From the above Theorem, the following two results can easily be derived.

Corollary 2.1 [GET90, EGT89, Rys82] $F_c(n) \leq n - 2$ *whenever* the Bruck-Ryser Theorem *rules out the existence of a finite projective plane of order* n*, or more specifically, whenever* $n \equiv 1$ *or* $2 \pmod 4$ *such that the square-free part of* n *contains at least one prime factor* p *which is congruent to* 3 *mod* 4.

Corollary 2.2 [GET90] $F_c(n) = 1$ *whenever* n *is even.*

Proof : Note that any of the Latin squares given by the construction is essentially an addition table of integers mod n, and hence does not have a single *transversal* [DK74] if n is even. ■

Additional results on the non-existence of an $(n-1) \times n$ circular Florentine array can be obtained from the non-existence of MOLS described in Theorem 1.1 by de Launey [dL86, Jun90]. This can be translated in our terminology as:

Corollary 2.3 $F_c(n) \leq n - 2$ *whenever the existence of the set of* $n - 1$ *MOLS of order* n *having the property described in Theorem 1.1 is ruled out, or more specifically, whenever* m *is a quadratic non-residue mod* p *where* $m \not\equiv 0 \pmod p$ *is an integer dividing the square-free part of* n *and* $p \neq 2$ *is a prime divisor of* n.

For example, for each positive integer t, if $n = 5^t \cdot 7$, then $n \equiv 3 \pmod 4$ and $7 \equiv 2 \pmod 5$ is a quadratic non-residue modulo 5. Therefore, there does not exist an $(n-1) \times n$ circular Florentine array whenever $n = 5^t \cdot 7$ for any positive integer t. These are infinitely many additional values of n, not covered by the Bruck-Ryser Theorem (See Cor. 2.1).

Woodcock [Woo86] in 1986 proved independently that the set of $n-1$ MOLS of order n having the property described in Theorem 1.1 does not exist whenever $n \equiv 15 \pmod{18}$. Though these values of n are already ruled out by Corollary 2.3, the proof actually rules out the existence of $n-2$ such squares.

Corollary 2.4 $F_c(n) \leq n-3$ *whenever* $n \equiv 15 \pmod{18}$.

3 Lower bound on $F_c(n)$ and conclusion

The basic lower bound which is one less than the smallest prime factor of n (Prop. 1.1) can be improved by the constructions from Jungnickel [Jun80] and Theorem 1.1. For $n < 100$, this gives $F_c(21) \geq 4$, $F_c(57) \geq 7$, and $F_c(63) \geq 6$.

Schellenberg, van Rees, and Vanstone in 1978 have searched by computer for those MOLS described in Theorem 1.1 [SvRV78]. From their explicit examples of 3 MOLS of order $n = 33$ and $n = 39$, and from Theorem 1.1, we have $F_c(33) \geq 3$ and $F_c(39) \geq 3$.

It is believed that an $(n-1) \times n$ circular Florentine array does not exist whenever n is not a prime. When p is a prime, the multiplication table of the integers $1, 2, \ldots, p-1$ mod p (by adjoining a constant column of all 0's) provides an example of a $(p-1) \times p$ circular Florentine array. Therefore, $F_c(p) = p-1$ if p is a prime. In addition to the corollaries in the previous section, two more cases were determined by some exhaustive computer search, which are $F_c(9) \leq 2$, and $F_c(15) \leq 4$, the latter by R. Wilson and R. Roth [WR].

References

[BR49] R. H. Bruck and H. J. Ryser, "The non-existence of certain finite projective planes," *Canadian Journal of Mathematics*, vol. 1, pp. 88-99, 1949.

[DK74] J. Dénes and A. D. Keedwell, *Latin squares and their application.* English University Press Ltd., London, 1974; revised edition, *Latin Squares – New developments in the theory and applications*, Annals of Discrete Mathematics, vol. 46, North-Holland, Elsevier Science, 1991.

[EGT89] T. Etzion, S. W. Golomb, and H. Taylor, "Tuscan-k squares," *Advances in Applied Mathematics*, vol. 10, pp. 164-174, 1989.

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

[GT85] S. W. Golomb and H. Taylor, "Tuscan squares - A new family of combinatorial designs," *Ars Combinatoria*, vol. 20-B, pp. 115-132, 1985.

[Hal86] M. Hall Jr., *Combinatorial Theory*, Second Ed., John Wiley and Sons, 1986.

[Jun80] D. Jungnickel, "On difference matrices and regular Latin squares," *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, vol. 50, pp. 219-231, 1980.

[Jun90] D. Jungnickel, "Latin squares, their geometries and their groups," in book, *Coding Theory and Design Theory, part II*, volume 21 of *IMA*, edited by D. Ray-Chaudhuri, pp. 166-225, 1990.

[dL86] W. de Launey, "A survey of generalized Hadamard matrices and difference matrices $D(k, \lambda; G)$ with large k," *Utilitas Mathematica*, vol. 30, pp. 5-29, 1986.

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

[Rys82] H. J. Ryser, "On the existence of symmetric block designs," *Journal of Combinatorial Theory*, Series A, vol. 32, pp. 103-105, 1982.

[SvRV78] P. J. Schellenberg, G. H. J. van Rees, and S.A. Vanstone, "Four pairwise orthogonal Latin squares of order 15," *Ars Combinatoria*, vol. 6, pp. 141-150, 1978.

[Song91] H. Y. Song, *On Aspects of Tuscan Squares*, Ph.D. Thesis, University of Southern California, 1991.

[SD96] Hong-Yeop Song and Jeffrey H. Dinitz, "Tuscan Squares," Chapter 48 of a book titled *The CRC Handbook of Combinatorial Designs*, edited by Charles J. Colbourn and Jeffrey H. Dinitz, CRC Press, pp. 480-484, 1996.

[Tay91] H. Taylor, "Florentine rows or left-right shifted permutation matrices with cross-correlation values ≤ 1," *Discrete Mathematics*, vol. 93, pp. 247-260, 1991.

[WR] R. Wilson and R. Roth, a letter to the author, (private communication), Oct. 1990.

[Woo86] C. F. Woodcock, "On orthogonal Latin squares," *Journal of Combinatorial Theory*, Series A, vol. 43, pp. 146-148, 1986.