(2)

Unclassified

AD-A220 430

REPORT DOCUMENTATION PAGE

DTIC ELECTE APR 12 1990 S D

1a. REPORT SECURITY CLASSIFICATION: Unclassified	1b. RESTRICTIVE MARKINGS: None
2a. SECURITY CLASSIFICATION AUTHORITY: N/A	3. DISTRIBUTION/AVAILABILITY OF REPORT: DISTRIBUTION STATEMENT A Approved for public release; Distribution Unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE: N/A	
4. PERFORMING ORGANIZATION REPORT NUMBER(S): (U)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION: University of Southern California	6b. OFFICE SYMBOL (If applicable): N/A
7a. NAME OF MONITORING ORGANIZATION: ONR San Diego Resident Representative N66018	
6c. ADDRESS (City, State and ZIP Code): Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089-0272	7b. ADDRESS (City, State and ZIP Code): Univ. of California, San Diego (A-034) 8603 La Jolla Shores Drive, San Diego, CA 92093-0234
8a. NAME OF FUNDING/SPONSORING ORGANIZATION: Office of Naval Research	8b. OFFICE SYMBOL (If applicable):
9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
8c. ADDRESS (City, State and ZIP Code): Mathematical Sciences Division, Department of the Navy, 800 N. Quincy, Arlington, VA 21217-5000	10 SOURCE OF FUNDING NOS.

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT NO.

11. TITLE (Include Security Classification): Discrete Mathematics for Communication Systems

12. PERSONAL AUTHOR(S): Dr. Solomon W. Golomb

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Yr., Mo., Day)	15. PAGE COUNT
Final	FROM 02/01/84 TO 01/31/90	1990, March, 31	47

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB. GR.	

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

A summary of the work accomplished under ONR Contract N00014-84-K-0189 is presented for the years 1 February, 1984 through 31 January 1990. This is accomplished by presenting the abstracts of papers published, those that have been accepted during this reporting period, and those submitted for publication.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
Unclassified UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS ☐	Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b TELEPHONE NUMBER (Include Area Code)	22c OFFICE SYMBOL
-	(202) 696-4320	

DD FORM 1473, 83 APR — EDITION OF 1 JAN 73 IS OBSOLETE.

SECURITY CLASSIFICATION OF THIS PAGE

FINAL TECHNICAL REPORT

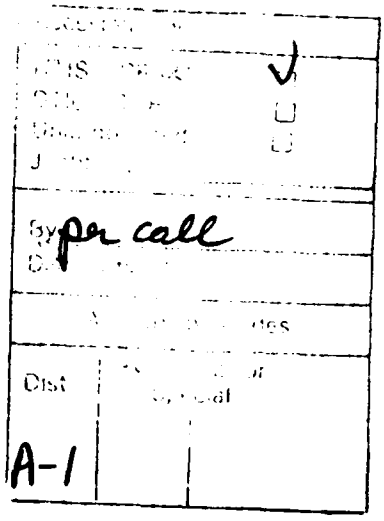
on ONR Contract No. NOOO14-84-K-0189

"Discrete Mathematics for Communication Systems"

1 February 1984 - 31 January 1990

Dr. Solomon W. Golomb
Principal Investigator

Communication Sciences Institute
Department of Electrical Engineering - Systems
University of Southern California
University Park
Los Angeles, CA 90089-0272



STATEMENT "A" per Marc Lipman
ONR/Code 1111SP
TELECON 4/11/90 VG

TABLE OF CONTENTS

APPENDICES

Final Progress Report 1 February 1984 - 31 January, 1987

TUSCAN-K SQUARES

Tuvi Etzion, Solomon Golomb and Herbert Taylor

A B S T R A C T

We prove that an $n \times (n+1)$ polygon path circular Tuscan-n array exists only if $n+1$ is prime. Two results proved are illustrated. One says that an $n \times n$ polygon path Tuscan-$n-1$ square exists if and only if an $\infty \times n$ singly periodic Costas array exists. The other gives a construction for K orthogonal $(n+1) \times (n+1)$ Latin squares, if an $n \times (n+1)$ circular Tuscan-K array exists. We review Tuscan-2 squares found by computer, and discuss nine questions.

Published in Advances in Applied Math., vol. 10, pp. 164-174, 1989.

BOUNDS FOR ARRAYS OF DOTS WITH DISTINCT SLOPES OR DISTINCT DIFFERENCES

Paul Erdos and Herbert Taylor

A B S T R A C T

An $n \times n$ array of dots and blanks is by definition a *Costas array* if it has exactly one dot in each row and column, and any two vectors determined by different pairs of dots differ either in length or slope. Robert Peile raised the question of the maximun number D of dots in an $n \times n$ array in which any two pairs of dots differ in slope. H. Taylor, using the Erdös-Turan method had proved that $D < 7/8\ n$ for large n, but this result was improved by Imre Ruzsa to $D < 5n^{4/5}$ for large n. These and related results for sonar sequences are to appear in a paper with four authors: Erdös, Graham, Ruzsa and Taylor.

To appear in Combinatorica.

ALGEBRAIC CONSTRUCTIONS FOR FREQUENCY HOP PATTERNS

Solomon W. Golomb and Herbert Taylor

A B S T R A C T

This paper presents a survey of the principal results obtained on the known constructions for Costas Arrays and Tuscan Squares, two classes of combinatorial designs applicable to obtaining frequency hop patterns with favorable correlation properties. Several recent results, not previously published, are included.

CONSTRUCTIONS FOR PERFECT MAPS AND PSEUDO-RANDOM ARRAYS

Tuvi Etzion

A B S T R A C T

A construction of perfect maps, i.e., periodic $r \times v$ binary arrays in which each $n \times m$ binary matrix appears exactly once, is given. A similar construction leads to arrays in which only the zero $n \times m$ matrix does not appear, and to a construction in which only few $n \times m$ binary matrices do not appear. Also a generalization for the non-binary case is given. The constructions involve an interesting question in shift register theory. We give the solution for almost all the cases of this question.

Published in the IEEE Transactions on Information Theory, IT-34, no. 5, September 1988, pp. 1308-1316.

ON HAMILTONIAN DECOMPOSITION OF K_n^*, PATTERNS WITH DISTINCT DIFFERENCES, AND TUSCAN SQUARES

Tuvi Etzion

A B S T R A C T

This paper presents a few constructions for the decomposition of the complete directed graph on n vertices into n Hamiltonian paths. Some of the constructions will apply for even n and others to odd n. The constructions will be obtained from some patterns with distinct differences. The constructions will be exhibited by squares (called Tuscan squares) which sometimes are Latin squares (called Roman squares), and sometimes are not Latin.

Revised January 1989. To be submitted for publication..

FLORENTINE ROWS OR LEFT-RIGHT SHIFTED PERMUTATION MATRICES WITH CROSS-CORRELATION VALUES ≤ 1

Herbert Taylor

A B S T R A C T

1. Find $n \times n$ permutation matrices – as many as possible – whose aperiodic horizontal shifting cross-correlation function takes only the values 0 or 1.

2. Find values of $F(n)$ = the maximum number of Florentine rows on n symbols.

3. It turns out that problem (1) is isomorphic to problem (2), so that optimum constructions are available for (1) whenever $n+1$ is prime. Also on exhibit is S. Alquaddoomi's recent discovery that $F(8) = 7$.

Submitted to Annals of Discrete Mathematics (December 1988). Also technical report CSI-88-12-03.

FRAGMENTS OF SYMMETRY IN CIRCULAR ROWS

Herbert Taylor

A B S T R A C T

Suppose we can and do place k distinct symbols $a_1, a_2, ..., a_k$ on the vertices of $n-1$ directed n-gons in such a way that each symbol appears exactly once on each n-gon, and each pair of symbols occurs once in some n-gon at each of the $n-1$ possible directed distances.

Then for $k = 3$ and $k = 4$, as above, and for each circular order $\pi a_1, \pi a_2, ..., \pi a_k$, the number of n-gons with the symbols in that order clockwise must be equal to the number of n-gons with the symbols in that order counterclockwise.

A counterexample found by Tuvi Etzion shows that when $k = 5$, the conclusion does not necessarily follow.

Published in Advances in Applied Mathematics, vol. 10, pp. 131-136, 1989.

THE UNGRACEFULNESS OF AN EXTENDED PENTAGON FOR A PROBLEM POSED BY KNUTH

Herbert Taylor

A B S T R A C T

Donald E. Knuth proposed the following problem in a letter to Solomon W. Golomb, dated mid April, 1989.

"Here's a problem in 'graceful numbering' of the regions defined by straight lines in the plane. If there are n regions, is it always possible to number them with consecutive numbers such that we have constant differences between numbers on adjacent regions along each line? " Examples showing that what Knuth asked for is not always possible, have been found by H. Taylor, and independently by R.L. Graham and son.

To be submitted for publication.

A DISTINCT DISTANCE SET OF 9 NODES IN A TREE OF DIAMETER 36

Herbert Taylor

A B S T R A C T

A "distinct distance set" in a graph is a set of nodes each pair of which has a different number of edges on a shortest path between them. Given n, the problem is to find a tree with minimum diameter d containing a DDS of n nodes. Previously the minimum d was only known for $n \leq 6$. This node establishes $d = 22$ for $n = 7$, $d = 29$ for $n = 8$, and $d = 36$ for $n = 9$. These are confirming instances of a conjecture put forth by Richard A. Gibbs and Peter J. Slater to appear in *Annals of Discrete Mathematics.*

Accepted for publication in Annals of Discrete Mathematics.

Ph.D. THESES

- **Gregory Lawrence Mayhew**, "Statistical Properties of Modified de Bruijn Sequences", Ph.D. Dissertation, Department of Electrical Engineering, University of Southern California, December 1987.

A B S T R A C T

First background information on de Bruijn sequences is highlighted and a new method to obtain these sequences is presented. The major properties of Modified de Bruijn sequences are explored. Order n Modified de Bruijn sequences are created by removing a single zero from the longest run of zeros in a period 2^n de Bruijn sequence. The de Bruijn and Modified de Bruijn sequences are inexorably linked to binary shift registers in the Fibonacci configuration. By focusing on period $2^n - 1$ instead of period 2^n, the $\phi(2^n - 1)/n$ M sequences are then the undisguised linear subset of the $2^{2^{n-1}-n}$ Modified de Bruijn sequences. By default, the bulk of Modified de Bruijn sequences are nonlinearly generated. Recursions which are the nonlinear duals to primitive irreducible polynomials over $GF(2)$ are developed. Theorems are given on the weight classes, linear spans, and generating recursions of Modified de Bruijn sequences. In particular, a sequence and its reverse form a symmetry group which is present in each of these properties. A sequence and its reverse belong to the same weight class and have the same linear span. A sequences and its reverse also have reciprocal recursions, regardless of linearly or nonlinearly generated. Complete statistical data is presented for orders 4,5, and 6. Partial statistical data is presented for orders 7 through 12. The resulting theorems are generic for all orders n.

Solomon Golomb's efforts on behalf of this thesis research, were supported in part by ONR.

- **Gregory S. Yovanof**, "Homometric Structures", Ph.D. Dissertation, Department of Electrical Engineering, University of Southern California, August 1988.

A B S T R A C T

The majority of the cases where ambiguities arise in the study of inverse problems can be attributed to the existence of *homometric structures,* i.e., structures which share the same autocorrelation function without being *congruent.* In 1939, S. Piccard claimed the proof of a theorem asserting the nonexistence of homometric structures among the members of a class of $\{0,1\}$-sequences whose unnormalized autocorrelation function is either 0 or 1 out-of-synch. G. Bloom (1975) demonstrated the falsity of that theorem by means of a counterexample. G. Bloom and S.W. Golomb generalized this counterexample to two infinite families of counterexamples in the case of sequences of Hamming weight six.

The theories of graph labelings and combinatorial designs provide us with examples of homometric structures over various metric spaces which, however, do not contradict S. Piccard's 'theorem'. *Numbered undirected graphs, spanning rulers* and the *factorization of polynomials over the field of rational numbers* are introduced as the underlying mathematical models for this problem. We prove the nonexistence of counterexamples in many cases. The proof of the existence of a unique, infinite, parametric family of counterexamples in the case of sequences of weight six completes the classification of all counterexamples to S. Piccard's 'theorem' up to that weight. The unique reconstruction of signals of this type from their *convolution functions* is also proved.

Next, we generalize the conditions of S. Piccard's theorem so that it applies to higher dimensional $\{0,1\}$-patterns. We conjecture that there exist no homometric *Costas Arrays.* In our attempt to prove this conjecture we develop a new fast *decorrelation algorithm* for permutation arrays. Strong *necessary conditions for the existence* of homometric permutation arrays are proved and the nonexistence of such matrices of small order is demonstrated. As a byproduct of our study we derive properties concerning the structure of Costas arrays which might lead to a classification of these patterns.

Solomon Golomb's efforts on behalf of this thesis research, were supported in part by ONR. Gregory Yovanof's research was partially supported by ONR.

- **Ning Zhang**, "Generalized Barker Sequences", Ph.D. Dissertation, Department of Electrical Engineering, University of Southern California, August 1988.

ABSTRACT

A generalized Barker sequence can be easily distinguished from the time-shifted versions of itself. This property is important for such applications as radar systems, synchronization systems and spread-spectrum communications systems.

First, we study some properties of the summation of K unit vectors. Then we prove a twenty-year-old conjecture (given by S. W. Golomb) about the uniqueness of the generalized Barker sequence of length 6. We also study the solution space of generalized Barker sequences with small length L. Moreover, we prove that $N_L(n)$ (the total number of n-phase Barker sequences of length L) goes to $+\infty$ for $3 \leq L \leq 19$ except for $L = 6$.

A relatively efficient algorithm is given which enables us to find all 5-phase Barker sequences up to length $L = 16$; 6-phase Barker sequences up to $L = 22$; 8-phase Barker sequences up to length $L = 14$ with partial results for $L = 15$ and 16. Moreover, we have found a 15-phase Barker sequence of length $L = 17$; a 24-phase Barker sequence of length

$L = 18$; and 60-phase Barker sequences for all L, $1 \leq L \leq 19$.

Some properties of generalized Barker sequences are investigated, including palindromic and left-right invariant generalized Barker sequences, multipliers of generalized Barker sequences, and other properties related to the structure of generalized Barker sequences.

Properties of cross correlation of generalized Barker sequences are studied. Specifically, we obtain a non-trivial lower bound on the magnitude of cross correlation values between generalized Barker sequences of the same length.

Solomon Golomb's efforts on behalf of this thesis research, were supported in part by ONR.

TRAVEL

- January 1990, Dr. Solomon W. Golomb was invited to the *University of Tel Aviv*, Israel to give a series of talks, abstracts of which are outlined below. (Dr. Golomb also lectured at the Technion in Haifa and the Weizman Institute in Rehovot while in Israel.)
- June 25-July 1, 1989, Dr. Solomon W. Golomb attended and participated in the *Symposium on Applications of Algebra to Error-Correcting codes*, Toulouse, France. He presented a paper titled "Algebraic Constructions for Frequency Hop Patterns."
- August 26-29, 1989, Dr. Herbert Taylor attended and participated in the *2na International Conference on Graph Theory, Combinatorics, Algorithms and Applications*, San Francisco, CA.
- September 18-19, 1989, Dr. Solomon W. Golomb attended and participated in the *Workshop on Error-Correcting Codes*, held at the IBM Research Labs, San Jose, CA., September 18-19, 1989. He presented a paper titled "Algebraic Constructions for Costas Arrays."
- November 1988, Dr. Solomon W. Golomb attended and presented an address on "Reflections of a Mathematician" at a meeting of the *Mathematical Association of America*, at Claremont-McKenna College, Claremont, CA.
- January 10-13, 1988, Dr. Herbert Taylor was invited by Prof. A.C. Lazer to attend the *Knight Memorial Lectures* at the University of Miami. Professor Steven Smale gave four lectures on the topology of algorithms. Dr. Taylor gave a talk on Euler's surface formula.
- January 14-17, 1988, Dr. Herbert Taylor was invited by Professor Oscar Moreno to give four lectures at the *Rio Piedras campus* at the University of Puerto Rico.

- March 15, 1988, Dr. Herbert Taylor gave a talk at the *Information Theory Meeting of the IEEE*. The talk was on the subject matter of *CSI-88-03-03*.

- March-May, 1988, Dr. Herbert Taylor sent an abstract entitled "Let a Sequence of Integer Line Segments be Joined by Hinges. How Short a One-Dimensional Box can Hold it Folded Up?" to the *International Workshop on Sequences*. The abstract was accepted but Dr. Taylor was unable to travel at the last minute because of having forgotten his expired passport. The paper has nevertheless been accepted for publication in the proceedings of that workshop. *International Workshop on Sequences*, June 5-11, 1988, University of Salerno, Positano, Italy.

CONSTRUCTION OF COSTAS ARRAYS FOR RADAR AND SONAR

- Solomon W. Golomb

A B S T R A C T

When a radar or sonar signal is bounced off a target, it returns to the sender shifted in both time and frequency. The time shift is proportional to the distance of the target, and the frequency shift is proportional to the velocity of the target relative to the observer. John A. Costas was the first to suggest using a "frequency hop pattern", involving a permutation of n uniformly spaced frequencies in n consecutive time intervals, and configured in such a way that the returning echo, shifted in both time and frequency, would have the minimum possible amount of coincidence with any shift of the original pattern except for the shift corresponding to the actual distance and velocity of the target. He asked for which values of n these "Costas arrays" exist.

A mathematically equivalent problem is to determine which $n \times n$ permutation matrices have the additional properties that all vectors connecting pairs of 1's in the permutation matrix are distinct as vectors (i.e. no two are identical in both magnitude and slope). A large number of constructions for Costas arrays are now known, all based on properties of primitive roots in finite fields. Although constructions are known for arbitrarily large values of n, it has not yet been shown that Costas arrays exist for every value of n.

TUSCAN SQUARES, FLORENTINE SQUARES, AND FREQUENCY HOP COMMUNICATIONS

- *Solomon W. Golomb*

ABSTRACT

A Latin square is an $n \times n$ array of n symbols, in which each symbol occurs exactly once in each row and in each column. A row Latin square is similar, but without the constraint on the columns. Such a square is called row-complete if each of the $n(n-1)$ ordered pairs of the n symbols occurs exactly once as an adjacent pair in one of the rows of the square. We call a row complete row Latin square a Tuscan square.

A Tuscan square is called a Tuscan-k square if no ordered pair of symbols j apart in one row of the square occurs j apart in the same order in another row of the square, for every j, $1 \leq j \leq k$. A Tuscan-$(n-1)$ square is also called a Florentine Square.

Tuscan-k squares arise in the solution of a number of combinatorial problems, in the design of unbiased statistical experiments, and in the design of multi-user frequency hop communication systems.

Tuscan squares which are not Latin are now known to exist for all $n \geq 6$. Various constructions, as well as several Tuscan-preserving transformations, have been found. At present, all known examples of Florentine squares are also Latin, and in fact are isomorphic to the multiplication table of the multiplicative group modulo p, where $p = n+1$ is a prime.

SHIFT REGISTER SEQUENCES

- *Solomon W. Golomb*

ABSTRACT

A shift register sequence $\{a_k\}$ of order n is a sequence of terms from a field, defined recursively by $a_k = \mathbf{F}(a_{k-1}, a_{k-2}, ..., a_{k-n})$ plus an initial condition (or initial state of the shift register), obtained by specifying the values of $(a_{-1}, a_{-2}, ..., a_{-n})$.

In the linear case, the "feedback function" $\mathbf{F}$ has the form $\mathbf{F}(x_1, x_2 ..., x_n) = \sum_{i=1}^{n} c_i x_i$. For this case, an analytic model exists whereby $A(z) = \sum_{k=0}^{\infty} a_k z^k = g(z)/f(z)$, with $f(z) = 1 - \sum_{i=1}^{n} c_i z^i$, and where $g(z)$ is a polynomial of degree $\leq n-1$ whose coefficients depend on the initial conditions as well as the c_i's.

The general (nonlinear) case is best understood for binary sequences, where $\mathbf{F}(x_1, x_2, ..., x_n)$ is one of the 2^{2^n} Boolean functions of n binary variables, of which $2^{2^{n-1}-n}$ result in "de Bruijn sequences", having the maximum possible periodicity of 2^n.

For binary sequences of period $2^n - 1$ having 2^{n-1} ones and $2^{n-1} - 1$ zeros, there is a hierarchy of randomness properties, with the linear shift register sequences having this period (so-called "m-sequences") being in the intersection of the families defined by each of these properties. The characterization of m-sequences in terms of randomness properties is not yet complete.

PERSONNEL RECEIVING SUPPORT FROM THIS CONTRACT

Dr. Solomon Golomb
Dr. Herbert Taylor
Gregory Yovanof - Research Assistant
Hong-Yeop Song - Research Assistant
Secretary

FINAL PROGRESS REPORT

on ONR Contract No. NOOO14-84-K-0189

"Discrete Mathematics for Communication Systems"

covering the period

1 February, 1984 - 31 January, 1987

prepared by

Dr. Solomon W. Golomb, Principal Investigator

Communication Sciences Institute
Department of Electrical Engineering - Systems
University of Southern California
University Park
Los Angeles, CA 90089-0272

Table of Contents

SELF-DUAL SEQUENCES[1]

Tuvi Etzion

Department of Electrical Engineering Systems
University of Southern California
Los Angeles, CA 90089-0272

The complement of a binary sequence S is obtained from S by replacing every 0 by 1 and every 1 by 0. For $S = [00100111]$ the complement is [11011000]. The sequence is called a self-dual sequence if it is equal to its complement when the sequence is taken as a cyclic sequence. For example [0011] is equal to its complement [1100]. We give an expression for the number, $SD(n)$, of self-dual sequences of length n, where the "length" of the sequence is one period of the sequence. For example [00110011] is the same as [0011] and has length 4. We also give a connection between $SD(n)$ and the number of cycles generated by some known feedback shift registers.

Self-dual sequences have an important role in determining the parity of the number of sequences of length k which can be produced by an n-stage shift register. We give important information for computing this parity.

A full cycle is a sequence of length 2^n where each n-tuple appears as a window in the sequence, for example [00011101] is a full cycle of length $2^3 = 8$. Since a full cycle can be generated by an n-stage shift register we can write a truth table with 2^n rows for the cycle. The weight of the truth table is the number of ones in the output of the first 2^{n-1} rows. We give an algorithm for generating full cycles with maximum weight of truth table. The algorithm is based on joining together the cycles of an n-stage shift register whose cycles are all self-dual.

---

[1] The full article appears in *Journal of Combinatorial Theory, Series A*, vol. 44, pp. 288-298, March 1987.

POLYGONAL PATH CONSTRUCTIONS FOR TUSCAN-K SQUARES[2]

Solomon W. Golomb, Tuvi Etzion, and Herbert Taylor

Department of Electrical Engineering Systems
University of Southern California
Los Angeles, CA 90089-0272

INTRODUCTION AND SUMMARY

An *Italian square* is an $n \times n$ array in which each of the symbols $1,2,...,n$ appears exactly once in each row.

By definition a *Tuscan-k square* is an Italian square with the further property that for any two symbols a and b, and for each m from 1 to k, there is at most one row in which b is the m^{th} symbol to the right of a.

Tuscan-1 squares are known to exist [7] for all n except $n = 3$ and $n = 5$, although no simple construction is known for odd $n > 5$.

By definition a *Circular Tuscan-k array* is an $n \times (n+1)$ array A in which each of the symbols $*,1,2,...,n$ appears exactly once in each row, and in which the Tuscan-k property holds when the rows are taken to be circular. In matrix notation the rows are indexed 1 to n while the columns are indexed 0 to n (mod $n+1$). For each m from 1 to k, $(A(i,j),A(i,j+m)) \neq (A(r,t),A(r,t+m))$ unless $i = r$ and $j = t$.

A Tuscan-$(n-1)$ square is called a *Florentine square*, and a circular Tuscan-n array is called a *Circular Florentine array*. A Florentine square is known to exist whenever $n+1$ is prime, and not known otherwise. All those known can be made into circular Florentine arrays by adjoining a column full of asterisks on the left. When a Florentine square is Latin we call it a *Vatican square*.

---

[2] The full article was submitted to *Ars Combinatoria*, December 19, 1986.

The "Add Zero" transformation [1] starts by adjoining a zeroth column full of asterisks on the left of a Tuscan-k square. The rows are then cycled to bring another symbol into the zero column, which is then deleted. The symbol * is then replaced with the deleted symbol. A Tuscan-k square can be made into a circular Tuscan-k square iff all of its Add Zero transforms are Tuscan-k squares.

Our main effort has been to explore the Tuscan possibilities with the polygonal path construction described in section C. An exhaustive (computer) search of polygonal path Tuscan-1 squares up to $n = 14$ was carried out by Peter Pacini, who is a sophomore at the University of Southern California. Sample results are exhibited in the figures of section C.

Twelve Questions

For which integers $n > 1$ do these exist?

1. Tuscan-2 square.
2. Polygonal Path Tuscan-2 square.
3. Symmetric Polygonal Path Tuscan-2 square.
4. Circular Tuscan-2 array.
5. Polygonal Path Circular Tuscan-2 array.
6. Symmetric Polygonal Path Circular Tuscan-2 array.
7. Florentine square.
8. Polygonal Path Florentine square.
9. Symmetric Polygonal Path Florentine Square.
10. Circular Florentine array.
11. Polygonal Path Circular Florentine array.
12. Symmetric Polygonal Path Circular Florentine array.

Our current state of knowledge is as follows.

1. Tuscan-2 squares.
   None exist for odd $n \leq 7$.
   None known for odd $n > 1$.
   Six in standard form for $n = 8$, none of them circular, none of them Latin.
   There are no known examples of Tuscan-3 squares when $n+1$ is composite.
   We do not have proof that $n \times n$ Tuscan-2 squares exist for infinitely many composite values of $n+1$.

2. Polygonal Path Tuscan-2 squares.
   Enumerated by exhaustive search to $n = 18$. See E12. All that exist from $n = 4$ to $n = 14$ are in Figures 4A, 6A, 10A, 10B, 14B, 14C.

3. Symmetric Polygonal Path Tuscan-2 squares.
   (3.) exist iff (6.) exist, by Lemma E12. Enumerated by exhaustive search to $n = 28$.

4. Circular Tuscan-2 arrays.
   Existence implies a pair of orthogonal $(n+1) \times (n+1)$ Latin squares by Theorem A.
   Existence guarantees non-Latin Tuscan-2 squares.

5. Polygonal Path Circular Tuscan-2 arrays.
   See Lemma E1.
   Some of these have asymmetric paths.

6. Symmetric Polygonal Path Circular Tuscan-2 arrays.
   (6.) iff (3.).
   We have examples by exploratory search up to $n = 50$.

7. Florentine squares.
   None are known when $n+1$ is composite.
   None exist for odd $n \leq 9$.
   No Vatican squares exist for odd $n \leq 11$.

8. Polygonal Path Florentine squares.
   Equivalent to a singly periodic Costas array, by Theorem D.
   For $n \leq 20$ the only ones that exist are those in (12.) where $n+1$ is prime.

9. Symmetric Polygonal Path Florentine squares.
   Existence implies that an "isotope" of C_n exists with 0 on the main diagonal, $\frac{n}{2}$ on the cross main diagonal, and each of the remaining symbols forming a pattern of n non-attacking queens. In the terminology of [2] an isotope of a Latin square is anything obtainable from the Latin square by permuting rows, columns, and symbols.

10. Circular Florentine arrays.
    Non-existence is known for all odd $n > 1$, by Theorem B.
    Non-existence is known for composite odd $n+1$ when the Bruck-Ryser theorem rules out a projective plane of the same odd order, by Theorem A.

11. Polygonal Path Circular Florentine arrays.
    (11.) exist iff (12.) exist, by Lemma E1.
    Non-existence is known for several infinite classes, covered in E1-E12. Fewer than 33 values of $n \leq 1000$ remain unsettled.

12. Symmetric Polygonal Path Circular Florentine arrays.
These exist whenever $n+1$ is prime.

COMBINATORIAL DESIGNS WITH COSTAS ARRAYS' PROPERTIES[3]

Tuvi Etzion

Department of Electrical Engineering Systems
University of Southern California
Los Angeles, CA 90089-0272

SUMMARY

Consider the 4×4×4 array:

	1	4	2	3		4	2	1	3	
upper	3	2	4	1		1	3	4	2	right
face	4	1	3	2		3	1	2	4	face
	2	3	1	4		2	4	3	1	

4	2	1	3	
1	3	4	2	front
3	1	2	4	face
2	4	3	1	

This array has sixteen dots and forty-eight blanks, one dot in each line, and a Costas array in every 4×4 subarray. T. Etzion calls such an $n \times n \times n$ array an ADC (All Directions Costas) cube. His Conjecture 1 is that except for $n = 1$, 2, and 4, there are no ADC cubes of order n.

Exhaustive computer search has verified Conjecture 1 for $n \leq 8$.

In this paper Tuvi Etzion gives seven different algebraic constructions for $n \times n \times n$ arrays. The ADNC (All Directions Near Costas) cubes have the property that every $n \times n$ subarray is a pattern of $n-1$ dots with at most one dot in each line (row or column), and no repeated vector differences between dots. One construction works when $n = q-1$ where q is any prime power. The other construction works when $n = p-1$ where p is prime.

---

[3] The full article was submitted to *Discrete Mathematics*, January 1987.

The TDC (Two Directions Costas) cubes have Costas arrays in all the $n \times n$ subarrays perpendicular to two of the coordinate directions. Three different constructions work when $n+1$ is prime, one of them requiring that $n+2$ be a power of 2.

The LC (Latin Costas) cubes correspond to one direction Costas, but, since every $n \times n$ subarray is a permutation matrix of dots and blanks, they can be represented by Latin squares in which each symbol marks a Costas array. These are constructed whenever $n = p-1$ where p is prime.

The VC (Vatican Costas) array is the same as LC with the added property that the Latin square is a Vatican square. One construction gives a VC array whenever $n+1$ is prime. The other when $n+1$ is a Mersenne prime gives another VC inequivalent by permutation of the symbols or symmetries of the square.

The paper also has examples found by computer search -- especially an 8×8 LC which yields an 8×8×8 TDC not covered by the constructions.

AN ALGORITHM FOR REALIZATION OF PERMUTATIONS IN A SHUFFLE-EXCHANGE NETWORK[4]

Tuvi Etzion

Department of Electrical Engineering Systems
University of Southern California
Los Angeles, CA 90089-0272

The shuffle-exchange network is an efficient tool for implementing various types of parallel processes. We present an algorithm for generating all the permutations on a shuffle-exchange network of 2^n processors in $0(n^2)$ time. This algorithm does not use comparisons between elements of the processors and all the computation is performed on the network.

[4] The full article was submitted to *Information Processing Letters*, January 1987.

A LEMMA ON CIRCULAR PERMUTATIONS WITH DISTINCT DIFFERENCES[5]

Herbert Taylor

Submitted to Congressus Numerantium - proceedings of the 18th S.E. Conference on Combinatorics, Graph Theory, and Computing, Boca Raton, Florida, February, 1987. Talk given by H. Taylor at the Congress.

ABSTRACT

Put symbols $a_1, a_2, \ldots, a_k$ on the vertices of $n-1$ directed n-gons in such a way that each symbol appears exactly once on each n-gon, and each pair of symbols occurs once in some n-gon at each of the $n-1$ possible directed distances.

LEMMA For $k=3$ and $k=4$, as above, and for each circular order $(\pi a_1, \pi a_2, \ldots, \pi a_k)$, the number of n-gons with the symbols in that order clockwise must be equal to the number of n-gons with the symbols in that order counterclockwise.

A counterexample found by Tuvi Etzion shows that the Lemma fails when $k=5$.

[5] This work was supported in part by the Office of Naval Research under Contract NOOO14-84-K-0189.

CROSS CORRELATION OF 2-DIMENSIONAL ARRAYS

Herbert Taylor

Department of Electrical Engineering Systems
University of Southern California
Los Angeles, CA 90089-0272

At the CSI Review in February 1987, H. Taylor gave a talk entitled "Compatible Permutation Arrays with Good Correlation." The best example included has a set of eight 5×5 permutation matrices with autocorrelation values only 5, 2, 1, and 0, and cross-correlation values only 2, 1, and 0. This example was found by H. Taylor by hand, and verified by Gregory Yovanof with a computer. We do not know of any $n > 5$ where more than eight exist with those correlation properties. At least two exist whenever a symmetric[6] $n \times n$ Costas array exists, as discovered by Tuvi Etzion.

Miscellaneous Citations

In the *Proceedings of the IEEE*, October 1985, a correspondence appeared by Avraham Freedman and Nadar Levanon entitled "Any Two $N \times N$ Costas Signals Must Have at Least One Common Ambiguity Sidelobe If $N > 3$ -- A Proof," (submitted November 1984).

In a "note added in proof" they mention that they had learned from S. W. Golomb that the same result with a similar proof had been contained in "Non-attacking Rooks with Distinct Differences" by H. Taylor, Tech. Rept. CSI-84-03-02, March 1984. The result had been given as a talk in February 1983 by H. Taylor, at the 14^{th} Southeastern Conference on Combinatorics, Graph Theory and Computing.

The abovementioned result tells us that the cross-correlation between two Costas arrays will be ≥ 2 for $n > 3$. This necessity of allowing cross-correlation greater than 1 is the motivation for studying

[6] "Symmetric" has since then been found unnecessary. Given any $n \times n$ Costas array, T. Etzion can provide two Costas arrays having cross-correlation values 2, 1, 0.

permutation matrices where both auto- and cross-correlations are merely kept ≤ 2.

Miscellaneous Citations

Gerry Silverman (Hanscom AFB) gave a talk at the International Symposium on Information The . . Ann Arbor, Michigan, October 1986, on his probabilistic calculations predicting that the number of 17×17 Costas arrays would be smaller than the number of 16×16. He has been corresponding with H. Taylor for about three years, i.e. since our article in the proceedings.

He phoned H. Taylor in mid-June 1987 to say that his computers had finished counting $C(17)$ = the number of 17×17 Costas arrays. As predicted $C(17) < C(16)$ but even more, $C(17) < C(15) < C(16)$.

In April 1986, H. Taylor gave four talks on Costas arrays at the invitation of Prof. Oscar Moreno at the University of Puerto Rico. In the summer of 1986 a student of Oscar Moreno's, named Pedro Carbonera, discovered a Costas array of size 53×53, where none had been known. This is the only discovery as far as we know, of a Costas array not listed in our *Proceedings* article of 1984 entitled "Constructions and Properties of Costas Arrays." Pedro Carbonera's write-up (in Spanish) is the only publication of his result as yet.

Up to order 5, there exist no dihedrally distinct permutation matrices with the same autocorrelation function (found by exhaustive computer search) -- done by Gregory Yovanof, reported June 15, 1987.

Hong Song, a graduate student at USC, has discovered a new construction for non-Latin Tuscan squares. The family is provably new because none of the add-zero transforms of these are Latin.

Weita Chang[7] has corresponded with S. W. Golomb and H. Taylor on the subject of Costas

[7] USN Submarine Base, New London, CT.

arrays. In the past year a correspondence of his was accepted for the *Proc. IEEE* [H. Taylor has not yet seen it].

A conjecture in "Constructions and Properties of Costas Arrays" has been proved true by Benjamin Weiss of the Hebrew University, and also (later, independently) by a student, Victor Reiner, at Princeton. The probability that an $n \times n$ permutation matrix taken at random will be a Costas array goes to zero as $n \to \infty$.

PERSONNEL RECEIVING SUPPORT FROM THIS CONTRACT

Dr. Tuvi Etzion

Dr. Solomon W. Golomb

Dr. Herbert Taylor

Gregory Yovanof - Research Assistant

Secretary

OFFICE OF NAVAL RESEARCH

PUBLICATIONS/PATENTS/PRESENTATIONS/HONORS REPORT

for

1 October 1985 through 30 September 1986

for

Contract NOOO14-84-K-0189

"DISCRETE MATHEMATICS FOR COMMUNICATION SYSTEMS"

PRINCIPAL INVESTIGATOR: DR. SOLOMON W. GOLOMB

COMMUNICATION SCIENCES INSTITUTE
DEPARTMENT OF ELECTRICAL ENGINEERING/SYSTEMS
UNIVERSITY OF SOUTHERN CALIFORNIA
LOS ANGELES, CALIFORNIA 90089-0272

PROGRESS REPORT, 1 Oct. 1985 - 30 Sep. 1986

a. **Papers submitted to refereed journals (and not yet published):**

i. S. W. Golomb, B. Tang, and R. L. Graham, "A new result on comma-free codes of even wordlength," *accepted* for publication in the *Canadian Journal of Mathematics*.

ii. T. Etzion, "Constructions and Complexity Distribution of de Bruijn Sequences," submitted to the *Siam Journal on Computing*.

iii. T. Etzion, "Self-Dual Sequences," *accepted* (Sept. 1986) for publication in the *Journal of Combinatorial Theory (Series A)*.

iv. T. Etzion, S. W. Golomb, and H. Taylor, "Polygonal Path Constructions for Tuscan-k Squares," submitted to *Ars Combinatoria*.

b. **Papers published in refereed journals:**

i. Solomon W. Golomb and Herbert Taylor, "Tuscan Squares -- A New Family of Combinatorial Designs," *Ars Combinatoria*, vol. 20-B, December, 1985, pp. 115-132.

c. **Books (and sections thereof) submitted for publication:**

NONE

d. **Books (and sections thereof) published:**

NONE

e. **Patents filed:**

NONE

f. **Patents granted:**

NONE

g. **Invited Presentations at Scientific Conferences, Colloquia, etc.:**

i. S. W. Golomb, "Algebraic aspects of optimum rulers," Invited lecture, Special Session on Directed Graphs, American Mathematical Society Annual Meeting, New Orleans, LA, January 10, 1986.

ii. S. W. Golomb, "Tuscan squares and their applications," Invited lecture, Caltech Colloquium on Coding Theory, Pasadena, CA, January 20, 1986.

iii. S. W. Golomb, "Theory and applications of Tuscan squares," Invited lecture, Stanford Electrical Engineering Colloquium, Palo Alto, CA, February 27, 1986.

iv. S. W. Golomb, "Shift Register Sequences -- Solved and Unsolved Problems," Invited Keynote Address, Built-In Self-Test Workshop, Kiawah Island, South Carolina, March 12, 1986.

v. S. W. Golomb, "Tuscan Squares -- A new class of combinatorial designs," Invited lecture, Emory University Mathematics Colloquium, March 13, 1986.

vi. S. W. Golomb, "Tilings of Rectangle, Torus and Plane," Invited lecture, Strens Memorial Conference, University of Calgary, Alberta, Canada, July 31, 1986.

vii. S. W. Golomb, "Tuscan Squares as Combinatorial Designs," Invited lecture, Combinatorics and Optimization Colloquium, University of Waterloo, Ontario, Canada, September 15, 1986.

viii. H. Taylor, "Lectures on Costas Arrays," Four invited lectures at the University of Puerto Rico, Rio Piedras campus, San Juan, P.R., April 1-4, 1986.

ix. H. Taylor, "Bee Rooks on Honeycomb Boards," Invited lecture, Caltech Colloquium on Coding Theory, Pasadena, CA, April 28, 1986.

h. **Contributed Presentations at Scientific Conferences, Colloquia, etc.:**

i. Herbert Taylor, "V-E+F = 2, A New Proof of a Stronger Theorem," Strens Memorial Conference, University of Calgary, Alberta, Canada, August 1, 1986.

i. **Honors/Awards/Prizes:**

S. W. Golomb elected to membership in the "Golden Key" National Honor Society, February 26, 1986.

j. **Technical Reports Published on Non-Refereed Journals:**

i. S. W. Golomb, "Optical Disk Error Correction," *BYTE Magazine*, May, 1986, pp. 203-210.

k. **Personnel Supported During Year Ended 30 September, 1986:**

i. **Principal Investigator:** Dr. Solomon W. Golomb, Professor of Electrical Engineering and Mathematics.

ii. **Associate Investigator:** Dr. Herbert Taylor, Research Associate Professor of Electrical Engineering.

iii. **Visiting Research Scholar:** Dr. Tuvi Etzion

iv. **Graduate Student:** Mr. Gregory Yovanof

DISCRETE MATHEMATICS FOR COMMUNICATIONS SYSTEMS

ONR CONTRACT N00014-84-K-0189

Second Annual Report

1 February 1985 - 31 January 1986

Solomon W. Golomb

SECOND ANNUAL REPORT

FEBRUARY 1986

A summary of the work accomplished under ONR Contract No. N00014-84-K-0189 is presented for the year February 1, 1985 to January 31, 1986. This is accomplished by presenting the abstracts of the papers published and those that are in progress. In addition, copies of papers published are attached.

1. S. W. Golomb and H. Taylor,
"Tuscan Squares - A New Family of Combinatorial Designs," *Ars Combinatoria*, vol. 20-B, December, 1985, pp. 115-132.

ABSTRACT

By definition an *Italian Square* is an $n \times n$ array in which each of the symbols 1,2,...,n appears exactly once in each row. A *Tuscan-k Square*, besides being Italian, has the property that for any two symbols, a, b, and for each m from 1 to k, there is at most one row in which b is the m^{th} symbol to the right of a. A Tuscan-1 is simply called *Tuscan*, and a Tuscan-$(n-1)$ is called *Florentine*. A *Latin Square* is an Italian Square in which each of the symbols also appears exactly once in each column. A square is *Roman* if it is both Tuscan and Latin. A square which is both Florentine and Latin is a *Vatican Square*.

Tuscan Squares exist for all even orders, and all odd orders $n \geq 7$. Tuscan Squares which are not Latin appear to exist for all $n \geq 6$. The Tuscan Squares for $n = 6$ and $n = 7$ have been completely enumerated. Several transformations which preserve the Tuscan property have been identified. The multiplication table modulo p, for prime p, is a Vatican Square. No other examples of Vatican Squares, nor even of Florentine Squares, have been found.

Several contexts and applications for these designs are described.

2. S. W. Golomb,
"The Fifteen Billiard Balls - A Case Study in Combinatorial Problem Solving," *Mathematics Magazine*, vol. 58, no. 3, May, 1985, pp. 156-159.

ABSTRACT

Balls bearing the numbers from 1 to 15 are on a billiard table. The object of the "game" is to knock all fifteen off the table (into the pockets), where any one of the fifteen balls can be knocked off *first*, but thereafter the next ball to go must be numbered consecutively to one which is already pocketed. Thus if "3" is the first to go, the next one to be removed can be either "2" or "4". If "3" and "4" are off the table, the next one to go can be either "2" or "5". If "3", "4", "2", and "1" are gone, the next one to go *must* be "5", and thereafter "6", then "7", etc., up to "15". (We do not regard "1" and "15" as adjacent.) The question is: *how many different sequences are permitted for removing all fifteen balls from the table?*

Many different methods can be used, illustrating different problem-solving techniques in combinatorial analysis, and all leading to the correct answer, 2^{14}. More generally, if we start with n balls on the table, numbered from 1 to n, and remove t of them subject to the consecutivity rules described above, the number of different sequences $s(t)$ which are possible is given by $s(t) = (n + 1 - t) \cdot 2^{t-1}$ for $1 \leq t \leq n$. The original problem is the special case $n = t = 15$.

3. S. W. Golomb (with B. Tang and R. L. Graham),
"A New Result on Comma-Free Codes of Even Wordlength," submitted to the *Canadian Journal of Mathematics*. (Accepted for publication.)

ABSTRACT

It has long been known that no comma-free code of even word-length k can attain the bound $B_k(n) = \frac{1}{k} \sum_{d \mid k} \mu(d) k^{n/d}$ if the alphabet size n satisfies $n - \frac{k}{2} > 2^{k/2}$. This paper improves the result to $n - \frac{k}{2} > (k/2)^{(\log \frac{k}{2})/0.71}$, which is also an upper bound on the possible number of sequences of length $k/2$ composed of 0, 1 and * which are pairwise comparable and compatible. (Two such sequences are *comparable* if there is at least one position where they differ and where neither has the value *. They are *compatible* if in *all* such positions where they differ, it is the same sequence which has the value 1.)

4. T. Etzion, S. W. Golomb and H. Taylor,
"Polygonal Path Constructions for Tuscan-k Squares," manuscript in preparation.

ABSTRACT

A polygonal path (directed) on the numbered vertices of a regular n-gon can be rotated to generate the rows of a Latin square. Every such square will be equivalent by column/row permutation to the addition table for integers modulo n.

An $n \times n$ array in which each of the symbols $1,2,...,n$ appears exactly once in each row, but not necessarily once in each column, is a *Tuscan-k square* if it has the property that for any two symbols a, b, and for each m from 1 to k, there is at most one row in which b is the m^{th} symbol to the right of a.

We have the results of exhaustive search up to $n = 14$ for polygonal path generated Tuscan-1 squares, and up to $n = 18$ for polygonal path Tuscan-2 squares.

With symmetric polygonal paths we have done an exhaustive search up to $n = 28$ for Tuscan-k squares with $k \geq 2$, and an exploratory search finding Tuscan-2 examples up to $n = 52$.

Using the "add-zero" transformations has given us many examples of non-Latin Tuscan-1 and Tuscan-2 squares. The only known Tuscan-$(n-1)$ squares, which occur whenever $n+1$ is prime, are obtainable by polygonal path constructions, and are unchanged by the add-zero transformations. As a consequence of several theorems, we can rule out the existence of polygonal path add-zero Tuscan-$(n-1)$ examples for all but 33 composite values of $n+1$ below 1001.

TRAVEL

During this reporting period, Dr. S. W. Golomb participated in the following meetings, with partial travel support from ONR. Dr. H. Taylor also attended the meeting in Brighton, England.

1. *International Symposium on Information Theory*, Brighton, England, June 23-28, 1985.

   Talks presented:

   a. S. W. Golomb, "Shift Register Sequences - Solved and Unsolved Problems," June 26, 1985. (This was the invited Shannon Lecture at this Symposium.)

   b. S. W. Golomb and H. Taylor, "Tuscan Squares and Distinct Ordered Pairs of Symbols," June 25, 1985.

   c. H. Taylor (with J. Robbins and R. Gagliardi), "PPMQ Acquisition Sequences," June 24, 1985.

2. *Symposium on Analytic Number Theory*, Imperial College, London, England, July 1-10, 1985.

   Invited talks presented:

   S. W. Golomb, "Probability Distributions on the Integers and Formulas for Primes," July 9, 1985.

3. *Tenth British Combinatorial Conference*, Glasgow, Scotland, July 21-26, 1986.

   Talks presented:

   S. W. Golomb, "Tuscan Squares - A New Class of Combinatorial Designs," July 23, 1985.

SCIENTIFIC PERSONNEL SUPPORTED IN PART DURING THIS PERIOD

Dr. S. W. Golomb	Professor of Electrical Engineering and Mathematics
Dr. Herbert Taylor	Research Associate Professor
Dr. Tuvi Etzion	Post-Doctoral Fellow
Mr. Gregory Yovanof	Research Assistant (graduate student)

DISCRETE MATHEMATICS FOR COMMUNICATIONS SYSTEMS

ONR CONTRACT NOOO14-84-K-0189

Annual Report

1 February 1984 - 31 January 1985

Solomon W. Golomb

FIRST ANNUAL REPORT

FEBRUARY 1985

A summary of the work accomplished under ONR Contract No. NOOO14-84-K-0189 is presented for the year February 1, 1984 to January 31, 1985. This is accomplished by presenting the abstracts of the papers published and those that are in progress. In addition, copies of papers published are attached.

****

-S.W. Golomb, "Algebraic Constructions for Costas Arrays", *Journal of Combinatorial Theory, Series A*, Vol. 37, No. 1, July 1984, pp. 13-21.

ALGEBRAIC CONSTRUCTIONS FOR COSTAS ARRAYS

A B S T R A C T

The following is equivalent to a problem posed by John P. Costas [1], who encountered it in the context of attempting to construct sonar signal patterns.

Problem.

For each positive integer n, construct an n×n permutation matrix with the property that the $\binom{n}{2}$ vectors connecting two 1's of the matrix are all distinct as vectors. (That is, no two vectors are equal in both magnitude and slope.)

Thus if $a_{i_1,j_1} = a_{i_2,j_2} = a_{i_3,j_3} = a_{i_4,j_4} = 1$ in the matrix, we must not have $(i_2 - i_1, j_2 - j_1) = (i_4 - i_3, j_4 - j_3)$, nor may we have $(i_2 - i_1, j_2 - j_1) = (i_3 - i_2, j_3 - j_2)$.

Such matrices have been called either Costas Arrays or constellations in Ref. [2], which explores constructions as well as applications for these patterns. It is convenient to represent these arrays on an n×n grid, using dots for the 1's and blanks for the 0's of the matrix. Three examples of 6×6 Costas arrays are shown in Fig. 1.

Previous constructions [2] for Costas Arrays, for special values of n, have been discovered by L.R. Welch and by A. Lempel. This paper contains the first published proofs of the validity of the Welch and Lempel constructions, as well as a major new construction.

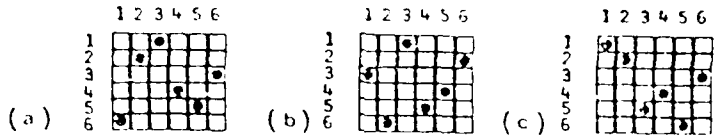


FIG. 1. Three examples of Costas Arrays of degree 6.

As a consequence of all these constructions, n×n Costas Arrays are now known to exist for the following positive values of n:

(i) $n = p - 1$, p prime,

(ii) $n = q - 2$, $q = p^k$ (any prime power),

(iii)* $n = q - 3$, $q = p^k$ (any prime power),

(iv)* $n = 2^k - 4$, $k \geq 3$.

Cases (iii) and (iv) depend on the conjecture that the field of q elements, $q > 2$, contains primitive roots α and β (not necessarily distinct) for which $\alpha + \beta = 1$. This conjecture has been verified for all prime powers q on the range $2 < q \leq 2^{11} = 2048$, and is discussed further in Section 3.

As an application of these results, algebraic constructions for n×n Costas Arrays are known for all $n \leq 130$ except for n = 19, 31, 32, 33, 27, 43, 48, 49, 53, 54, 55, 63, 67, 73, 74, 75, 83, 84, 85, 89, 90, 91, 92, 93, 97, 103, 109, 113, 114, 115, 116, 117, 120, 121, 127. However, the great majority of all integers n will not be included in these four classes of known constructions. It is hoped that this paper will inspire others to discover additional constructions for Costas Arrays. The major new constructions starts with Theorem 3 as follows:

Theorem 3. Let α and β be primitive elements in the field GF(q), for any $q > 2$. Then the $(q - 2)\times(q - 2)$ permutation matrix with $a_{ij} = 1$ iff $\alpha^i + \beta^j = 1$ is a Costas Array. (This reduces to Theorem 2 in the special case $\alpha = \beta$.)

References

1. J.P. Costas, "Medium constraints on sonar design and performance," *EASCON Convention Record* (1975), 68A-68L.

2. S.W. Golomb and H. Taylor, "Two-dimensional synchronization patterns for minimum ambiguity," *IEEE Trans. Inform. Theory*, IT-28, No. 4, (1982).

****

-Solomon W. Golomb and Herbert Taylor, "Constructions and Properties of Costas Arrays", *Proceedings of the IEEE*, Vol. 72, No. 9, September 1984.

CONSTRUCTIONS AND PROPERTIES OF COSTAS ARRAYS

A B S T R A C T

A Costas array is an n×n array of dots and blanks with exactly one dot in each row and column, and with distinct vector differences between all pairs of dots. As a frequency-hop pattern for radar or sonar, a Costas array has an optimum ambiguity function, since any translation of the array parallel to the coordinate axes produces at most one out-of-phase coincidence.

We conjecture that n×n Costas array exist for every positive integer n. Using various constructions due to L. Welch, A. Lempel, and the authors, Costas arrays are shown to exist when $n = p - 1$, $n = q - 2$, $n = q - 3$, and sometimes when $n = q - 4$ and $n = q - 5$, where p is a prime number, and q is any power of a prime number.

All known Costas array constructions are listed for 271 values of n up to 360. The first eight gaps in this table occur at n = 32, 33, 43, 48, 49, 53, 54, 63. (The examples for n = 19 and n = 31 were obtained by augmenting Welch's construction.)

Let C(n) denote the total number n×n Costas arrays. Costas calculated C(n) for $n \leq 12$. Recently, John Robbins found C(13) = 12828. We exhibit all the arrays for $n \leq 8$. From Welch's construction, $C(n) \geq 2n$ for infinitely many n.

Some Costas arrays can be sheared into "honeycomb arrays". All known honeycomb arrays are exhibited, corresponding to n = 1, 3, 7, 9, 15, 21, 27, 45.

Ten unsolved problems are listed.

COMPUTER

Two of three VAX-750's purchased on our DoD University Instrumentation Grant have been connected to the local computer net and are fully operational.

Our new dedicated computer system has definitely allowed us to carry out research which would have been prohibitively expensive if time were purchased for this effort. For example, three distinct kinds of searches, using sophisticated backtrack programs, have been carried out which have led to new results:

1. PPM sequence designs: Exhaustive search through 13×14 arrays took 228 hours of CPU time.

2. Costas Arrays: Exhaustive search through 13×13 arrays took 58 hours of CPU time.

3. Sonar Arrays: Exhaustive search through 11×17 arrays used 251 hours.

Extensions of the Costas array search are now being undertaken cooperatively with researchers at other organizations.

We hope to obtain an array processor for our VAX-750's in order to carry out research activities involving the coupling in phased-array antenna systems and spread spectrum receivers, and several aspects of sonar signal processing.

TRAVEL

During this reporting period, Dr. S.W. Golomb participated in the following meetings and workshops:

1. The Institute of Management Sciences (TIMS XXVii) International meeting, Copenhagen, Denmark, June 17-21, 1984. He delivered a presentation entitled "Information and Control in Management Systems," Session WB3 on June 20, 1984.

2. The Information Theory Workshop, Caesarea, Israel, July 1-5, 1984.

3. XXIst General Assembly of the International Scientific Radio Union (U.R.S.I.) in Florence, Italy, from August 28 to September 5, 1984, as an official representative of the United States National Academy of Sciences - National Research Council. *Partial travel support for this trip was provided by ONR with prior approval.*

Abstracts of Dr. Golomb's talks in Israel and Italy appear below.

Frequency Hop Patterns with Thumb-Tack Ambiguity Functions

M.J. Sites (1969) and J. Costas (1975) have posed the problem of finding n×n frequency hop patterns (n adjacent frequencies assigned to n consecutive time intervals in some permuted order) with the "thumb-tack property" that any non-zero shift of the pattern in time and/or frequency will result in at most one coincidence between occupied cells in the shifted and unshifted pattern. Systematic constructions for such hop patterns have been found by Welch, Lempel, Taylor, and Golomb, as described by Golomb and Taylor (1982) and Golomb (1984). In particular, n×n patterns can now be systematically constructed whenever n+1 is a prime, whenever n+2 is a prime or power of a prime, whenever n+4 is a power of two, and in many other cases as well. These patterns are directly applicable to signal design problems for frequency-hopped radar and sonar, and as two-dimensional synchronization patterns. They are also closely related to the patterns which arise in the synthetic aperture design problem for radio astronomy telescopes.

References

1. J. Costas (1975), "Medium Constraints on Sonar Design and Performance," in *EASCON Convention Record*, 1975, pp. 68A-68L.

2. S. Golomb (1984), "Algebraic Constructions for Costas Arrays," *Journal of Combinatorial Theory (A)*, vol. 37, no. 1, July 1984 (to appear).

3. S. Golomb and H. Taylor (1982), "Two-Dimensional Synchronization Patterns

for Minimum Ambiguity," *IEEE Trans. on Information Theory*, vol. IT-28, no. 4, July, 1982, pp. 600-604.

4. M.J. Sites (1969), "Coded Frequency Shift Keyed Sequences with Applications to Low Data Rate Communication and Radar," Technical Report 3606-5, *Radioscience Laboratory*, Stanford Electronics Laboratories, Stanford, California, September 1969. SU-SEL-69-0033.

Construction of Frequency Hop Patterns

A Sites-Costas (S-C) array is an n×n array of dots and blanks with exactly one dot in each row and column, and with distinct vector differences between all pairs of dots. As a frequency hop pattern for radar or sonar, an S-C array has an optimum ambiguity function, since any translation of the array parallel to the coordinate axes produces at most one out-of-phase coincidence.

We conjecture that n×n S-C arrays exist for every positive integer n. Using various constructions due to L. Welch, A. Lempel, H. Taylor, and the author, S-C arrays are shown to exist when n=p-1, n=q-2, n=q-3, and sometimes when n=q-4 and n=q-5, where p is a prime number, and q is any power of a prime number.

There are known S-C array constructions for 271 of the values of n up to 360. The first eight gaps occur at n=32, 33, 43, 48, 49, 53, 54, 63. (Examples for n=19 and n=31 were obtained by augmenting Welch's construction.)

Let C(n) denote the total number of n×n S-C arrays. Costas calculated C(n) for $n \leq 12$, with C(12)=7852. From Welch's construction, $C(n) \geq 2n$ for infinitely many n. Many unsolved problems regarding C(n) remain.

In 1966, Yates and Cooper proposed the problem of finding n simultaneous n×n permutation matrices, each regarded as a frequency hop pattern, such that the time cross-correlation between any pair of patterns never produces more than one coincidence for any time shift. There is an interesting relationship, involving the symmetries of a Latin Square, between the Yates-Cooper construction which solves this problem when n+1 is prime, and the Welch construction for Sites-Costas arrays.

SCIENTIFIC PERSONNEL SUPPORTED

Dr. Solomon W. Golomb	Professor of Electrical Engineering and Mathematics
Dr. Herbert Taylor	Research Associate Professor
Gregory Yovanof	Research Assistant

October 28, 1985

PROGRESS REPORT

ONR Contract No. N00014-84-K-0189

DISCRETE MATHEMATICS FOR COMMUNICATIONS SYSTEMS

The principal research efforts under this contract since its inception have been devoted to the further investigation of certain classes of combinatorial design patterns with important communications applications, especially to frequency-hopping spread-spectrum systems.

The earlier work centered on designs called Costas Arrays, which we extensively described and documented in [1] and [2]. The article [3] by John Costas in the Proceedings of the IEEE serves as a companion piece to [1], and goes more deeply into the detailed military applications of these arrays. Since [1] appeared, we have extended the computer search to include the total number, C(14), of Costas arrays for n=14, and the reduced number, c(14), which are distinct relative to the symmetry group of the square.

Considerably greater effort has been devoted during this period to the study of Tuscan Squares, a new family of combinatorial designs, and a major research paper [4] has been submitted for publication. Earlier versions of this paper were presented at conferences, etc., as follows:

On June 27, 1985, at the International Symposium on Information Theory in Brighton, England, a paper titled "Tuscan Squares and Distinct Ordered Pairs of Symbols" was presented by Herbert Taylor and Solomon W. Golomb. A colloquium lecture on this theme was presented by Professor Golomb on July 3, 1985, at the University of Southampton, England. Then, on July 22, 1985, Dr. Golomb presented a paper, "Tuscan Squares - A New Family of Combinatorial Designs" at the Tenth British Combinatorial Conference, held in Glasgow, Scotland. On each of these occasions, there were members of the audience who asked interesting questions, made penetrating comments, and otherwise contributed to the further progress of this research.

A brief summary of all progress on Tuscan Squares since July, 1985, is included as Appendix A to this report. Copies of the four papers listed in the References below also accompany this report.

References

[1] "Constructions and Properties of Costas Arrays," by Solomon W. Golomb and Herbert Taylor, Proceedings of the IEEE, vol. 72, no. 9, September, 1984, pp. 1143-1163.

[2] "Algebraic Constructions for Costas Arrays," by Solomon W. Golomb, Journal of Combinatorial Theory (A), vol. 37, no. 1, July, 1984, pp. 13-21.

[3] "A Study of a Class of Detection Waveforms Having Nearly Ideal Range-Doppler Ambiguity Properties," by John P. Costas, Proceedings of the IEEE, vol. 72, no. 8, August, 1984, pp. 996-1009.

[4] "Tuscan Squares - A New Family of Combinatorial Designs," by Solomon W. Golomb and Herbert Taylor, submitted to Ars Combinatoria, August, 1985.

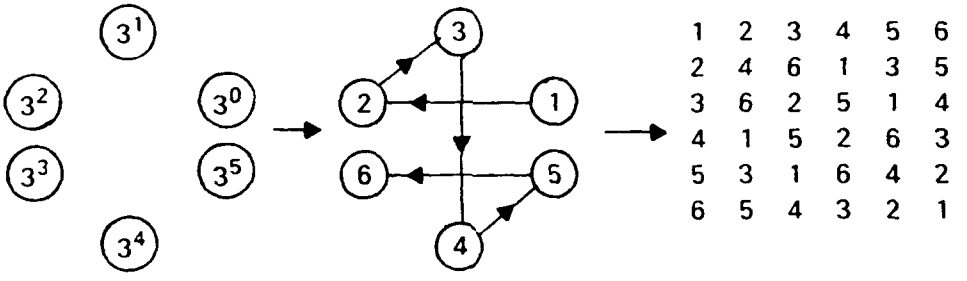
APPENDIX A

In July, 1985, S. W. Golomb gave a talk entitled "Tuscan Squares - A New Family of Combinatorial Designs" at the Tenth British Combinatorial Conference held in Glasgow, Scotland. A paper with the same title, coauthored by H. Taylor, was submitted for the conference proceedings at the end of August. These proceedings are to appear in a special issue of Ars Combinatoria. In this Appendix, we adopt the notation and terminology of that paper.

Since July we have found new uses for the Add-Zero Transformation and variations on the original Zig-Zag construction, as follows.

1. A variation of the Zig-Zag construction will give the Vatican Square of order $n = p-1$ whenever p is prime.

   Take a primitive element g in GF(p) and write the powers of g in a circle. Then draw the zig-zag pattern on successive integers. Here is an example with p=7, g=3:



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

   Rotating the pattern generates the rows of the Vatican Square.

2. H. Taylor did a by hand backtrack search for all the zig-zag patterns that give 8×8 Tuscan Squares. There are twelve patterns, but they reduce to eight by dihedral symmetry (flipping over). The number of distinct 8×8 Tuscan Squares in standard form, produced by the twelve patterns, is six.
3. By hand exploration, H. Taylor found zig-zag patterns for Tuscan-2 Squares for n=10,12,14. The square for n=14 has the remarkable property that every Add-Zero transform of it is also Tuscan-2. As a result, by some special chemistry of orthogonal latin squares and idempotent quasigroups, this square can be made to generate an orthogonal pair of 15×15 latin squares.
4. A computer search by Dr. Tuvi Etzion found all multiplicatively inequivalent symmetric zig-zag pattern Tuscan-2 Squares for all even values of n up to

n=26. There is only one Tuscan-3 among them, excluding the Vatican Squares, which we know appear for each n = p-1 when p is prime. That solitary Tuscan-3 occurs at n=22. With an exploratory (non-exhaustive) computer search he further found examples of symmetric zig-zag pattern Tuscan-2 squares for n = 28, 30, 32, 34, and 36.

5. Herbert Taylor and Tuvi Etzion simultaneously found a proof that there do not exist odd Vatican squares all of whose Add-Zero transforms are Vatican.
6. An open question asks whether non-Latin Tuscan squares exist for all n $\geq$ 6. H. Taylor gave a partial answer by observing that if a Tuscan square is not Vatican, then some Add-Zero transform of it must be non-Latin. This definitely answers "yes" to the question for even n, because the original zig-zag provably never gives Vatican squares for n > 4. For odd n the Tuscan squares known to exist by T. W. Tilson's result are almost surely never Vatican -- but this has not yet been proven.