Constructions and Properties of Costas Arrays

SOLOMON W. GOLOMB, FELLOW, IEEE, AND HERBERT TAYLOR

A Costas array is an $n \times n$ 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 $n \times n$ Costas arrays 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 of $n \times n$ Costas arrays. Costas calculated $C(n)$ for $n \leqq 12$. Recently, John Robbins found $C(13) = 12\,828$. We exhibit all the arrays for $n \leqq 8$. From Welch's construction, $C(n) \geqq 2n$ 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.

I. Introduction

Radar and sonar signals are used to determine both the *distance* (also called *range*) of a target from the observer, and the *velocity* (also called *range rate*) at which the target is either approaching or receding from the observer. The range is proportional to the round-trip delay time (or *time shift*) of the signal, and the velocity is proportional to the doppler (or *frequency shift*) of the signal.

In a frequency-hopping radar or sonar system, the *signal* consists of one or more frequencies being chosen from a set $\{f_1, f_2, \cdots, f_m\}$ of available frequencies, for transmission at each of a set $\{t_1, t_2, \cdots, t_n\}$ of consecutive time intervals. For modeling purposes, it is reasonable to consider the situation in which $m = n$, and where a different one of n equally spaced frequencies $\{f_1, f_2, \cdots, f_n\}$ is transmitted during each of the n equal duration time intervals $\{t_1, t_2, \cdots, t_n\}$. Such a signal is conveniently represented by an $n \times n$ permutation matrix A, where the n rows correspond to the n frequencies, the n columns correspond to the n time intervals, and the entry a_{ij} equals 1 if and only if frequency f_i is transmitted in time interval t_j. (Otherwise, $a_{ij} = 0$.)

When this signal is reflected from the target and received back by the observer, it is shifted in both time and frequency, and from the amounts of these shifts, both range and velocity are determined. The observer determines the amounts of these shifts by comparing all shifts (in both time and frequency) of a replica of the transmitted signal with the actual received signal, and noting for which combination of time shift and frequency shift the coincidence is greatest. This may be thought of as counting the number of coincidences between 1s in the matrix $A = (a_{ij})$ with 1s in a shifted version A^* of A, in which all entries have been shifted r units to the right (r is negative if there is a shift to the left), and s units upward (s is negative if the shift is downward).

The *number* of such coincidences, $C(r, s)$, is the (*unnormalized*) *autocorrelation* between A and A^*, and clearly satisfies the following conditions:

$$C(0,0) = n$$
$$C(r,s) = 0, \qquad \text{if } |r| \geqslant n \text{ or if } |s| \geqslant n.$$
$$0 \leqslant C(r,s) < n \quad \text{except when } r = s = 0.$$

(This conforms to the assumption that the signal is 0 outside the intervals $f_1 \leqslant f \leqslant f_n$ and $t_1 \leqslant t \leqslant t_n$. If the sequence of frequencies is to be repeated periodically in time, a singly periodic correlation function can be defined accordingly. In this context, periodicity in frequency does not appear to be a useful notion.)

In the real world, the returning signal is always noisy. The two-dimensional autocorrelation function $C(r, s)$, called the *ambiguity function* in the radar and sonar literature, should be thought of as the total "coincidence" between the actual returning noisy signal and the shift of the ideal transmitted signal by r units in time and s units in frequency. It is useful to think of the signal matrix $A = (a_{ij})$ as a two-dimensional template of n^2 cells, which is opaque at the $n^2 - n$ cells where $a_{ij} = 0$, and transparent at the n cells where $a_{ij} = 1$. The total signal energy behind these n windows is *summed* (via a double integral in time and frequency) to give the value of $C(r, s)$ when the template is shifted r units on the time axis and s units on the frequency axis.

Among the 2^{n^2} matrices of 0s and 1s of order n, there are only $n!$ permutation matrices, and some of these are better than others as signal patterns for radar and sonar. For example, the $n \times n$ identity matrix I_n can be shifted one unit up and one unit left, and will then produce $n - 1$

Manuscript received November 28, 1983; revised May 2, 1984. This research was supported in part by the United States Navy, Office of Naval Research, under Contracts N00014-80-C-0745 and N00014-84-K-0189.

The authors are with the Communication Sciences Institute, School of Engineering, University of Southern California, Los Angeles, CA 90089-0272, USA.

0018-9219/84/0900-1143$01.00 ©1984 IEEE

coincidences with the original matrix. For large values of n and a noisy environment, the signal pattern I_n would be almost guaranteed to produce spurious targets, shifted an equal number of units in both time and frequency from the real target.

At a minimum, there is a shift of $A = (a_{ij})$ which will make any of the n 1s land on any of the $n - 1$ remaining 1s, so we know that

$$\min_{\text{all "codes"}} \max_{(r,s)\neq(0,0)} C(r,s) \geqslant 1$$

where $C(r,s)$ is the *ideal* ambiguity function of the permutation matrix itself. This led J. P. Costas [1] to look for those $n \times n$ permutation matrices for which

$$\max_{(r,s)\neq(0,0)} C(r,s) = 1 \tag{1}$$

as the best possible case. By computer-aided search, he found examples of such matrices for all $n \leqslant 12$, but was unable to find an example for $n = 13$, and was tempted to conclude that these patterns "die out" beyond $n = 12$.

In subsequent papers ([2], [3]), permutation matrices which satisfy (1) have been called either *constellations* or *Costas arrays*. They are now known to exist for *all* $n \leqslant 31$ and for arbitrarily large values of n related to the occurrence of prime numbers and prime powers. It is conjectured that these arrays exist for all positive integers n. In [16], M. J. Sites defined these same arrays, which he called "F-matrices with thumbtack ambiguity functions." However, Costas had described these arrays still earlier, in an originally classified report [17].

In this paper, a survey of all that is currently known about Costas arrays is presented. In addition to earlier systematic algebraic methods of construction by Welch [2], Lempel [2], and Golomb [3], new algebraic constructions by Golomb and by Taylor are described, along with a sporadic method of Taylor which succeeds in filling in some of the gaps (e.g., at $n = 19$, the first case where no systematic construction is known).

It is convenient to represent the $n \times n$ permutation matrix corresponding to a Costas array, $A = (a_{ij})$, on an $n \times n$ grid, with a dot in the middle of cell (i,j) if and only if $a_{ij} = 1$. The Costas condition then says that the $(n^2 - n)/2$ lines connecting pairs of distinct dots are all different *as vectors*; that is, no two of these lines are equal in both length and slope.

In [3], Golomb advanced four conjectures concerning primitive roots in finite fields. Two of these, Conjectures A and D, have direct bearing on the success of certain methods for constructing Costas arrays. O. Moreno [4] has recently proved Conjecture D for all fields of characteristic 2; and as observed by A. Odlyzko, the methods of M. Szalay [5], and J. Johnson [9], can be extended to show that Conjecture A holds with at most a finite number of exceptions. Conjecture A is stated in Section II-C of this paper, and Conjecture D in Section III-F.

Costas arrays which satisfy additional constraints, involving either single or double periodicity, or symmetry, or additional separation requirements on the 1s in the permutation matrix, are also considered in this paper. A lower bound on the cross correlation between any two Costas arrays of order n is obtained. This has obvious applicability to the case of multiple signals in the same environment. Finally, it should be mentioned that frequency-hop patterns such as the ones considered here are also useful in spread-spectrum communication systems, where the objective may be to achieve either jamming resistance, or low probability of intercept (LPI), or frequency diversity for a selectively fading channel.

II. Systematic Methods of Construction

The finite field with q elements, denoted $GF(q)$, exists when and only when q is a power of a prime. Detailed proofs (in order of increasing complexity) that the Welch, Lempel, and Golomb construction methods produce Costas arrays, are contained in [3]. These proofs depend on the arithmetic of finite fields, and particularly on two properties of all primitive elements in finite fields.

The element α in $GF(q)$ is called *primitive* if the successive powers of α (i.e., $\alpha^1, \alpha^2, \alpha^3, \cdots, \alpha^{q-1} = 1$) run through all the nonzero elements of $GF(q)$. For primitive α the two essential facts are as follows.

1) For every nonzero element x in $GF(q)$ there is an integer i such that $\alpha^i = x$.
2) $\alpha^i = \alpha^k$ in $GF(q)$ if and only if $i \equiv k (\operatorname{mod} q - 1)$.

Equivalently, corresponding to each nonzero x belonging to $GF(q)$, there is the uniquely determined "logarithm of x to the base α," which looks like an ordinary whole number, and belongs to the cyclic group of integers with respect to addition modulo $q - 1$. That is, if $\alpha^i = x$, then $\log_\alpha x = i$.

The only information needed to construct a Costas array by any of these methods is a "log table" for $GF(q)$, consisting of a list of ordered pairs of the form $(x, \log_\alpha x) = (\alpha^j, j)$, for j running through $0, 1, 2, \cdots, q - 2$, and corresponding α^j taking on all the field values except 0.

A. The Welch Construction

For every prime $p > 2$, the Welch construction yields an $n \times n$ Costas array W_1 with $n = p - 1$, and a Costas array W_2 with $n = p - 2$. For certain primes, it also yields a Costas array W_3 with $n = p - 3$.

This construction requires a log table for $GF(p)$ where p is an odd prime, and the base α is a primitive element of $GF(p)$. (For prime p, $GF(p)$ is simply the field of integers modulo p.)

W_1: $(n = p - 1)$ The $n \times n$ matrix plots the log. That is, with columns numbered $j = 0, 1, 2, \cdots, p - 2$, and rows numbered $i = 1, 2, \cdots, p - 1$, we put a dot in position (i,j) if and only if $i = \alpha^j$.

W_2: $(n = p - 2)$ This is obtained from W_1 by deleting the dot at $(1,0)$, along with the top row and left column.

W_3: $(n = p - 3)$ This works *only when 2 is primitive in $GF(p)$*. Using $\alpha = 2$, W_1 has dots at both $(1,0)$ and $(2,1)$. W_3 is the result of deleting these two dots, along with the two top rows, and the two left columns.

Fig. 1 illustrates W_1 with $n = 42$. Removing the top row and left column from the figure illustrates W_2 with $n = 41$.

B. The Lempel Construction

This uses a log table for $GF(q)$ where q can be any power p^k of any prime p, and the "logarithmic base" α is a primitive element of $GF(q)$.

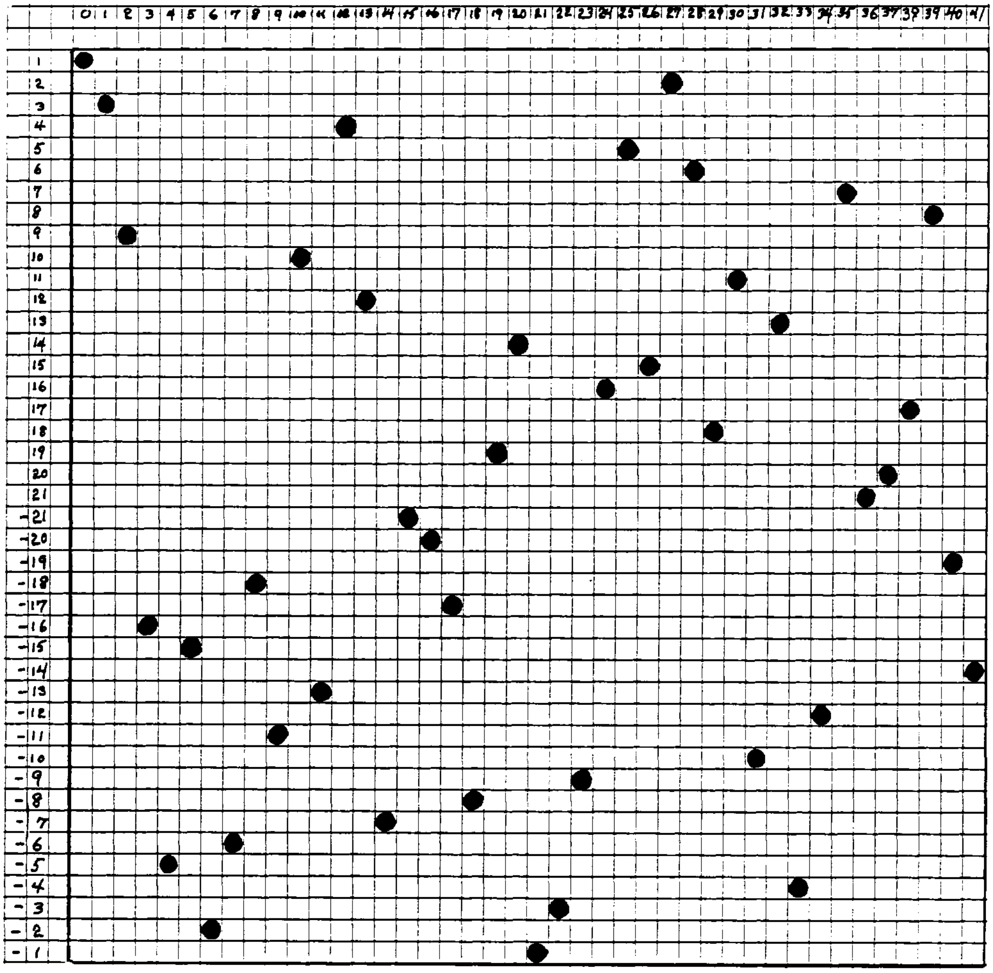
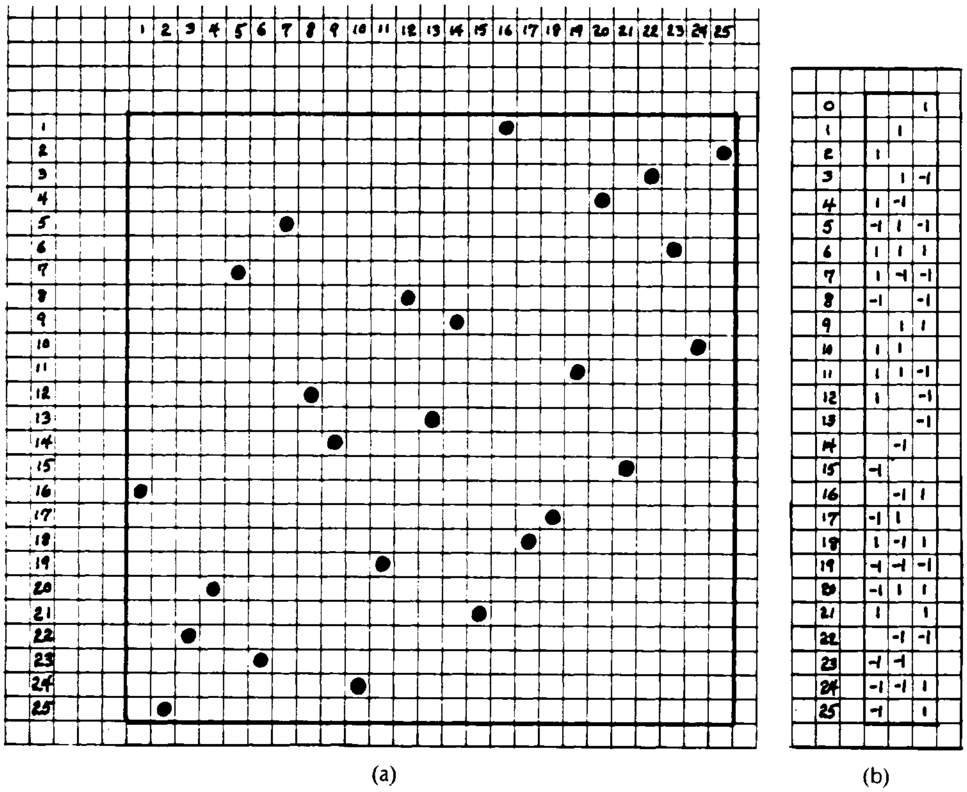


Fig. 1. W_1 with $p = 43$, $n = 42$.



(a)

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

(b)

Fig. 2. (a) L_2 with $q = 27$, $n = 25$. (b) A log table for $GF(27)$.

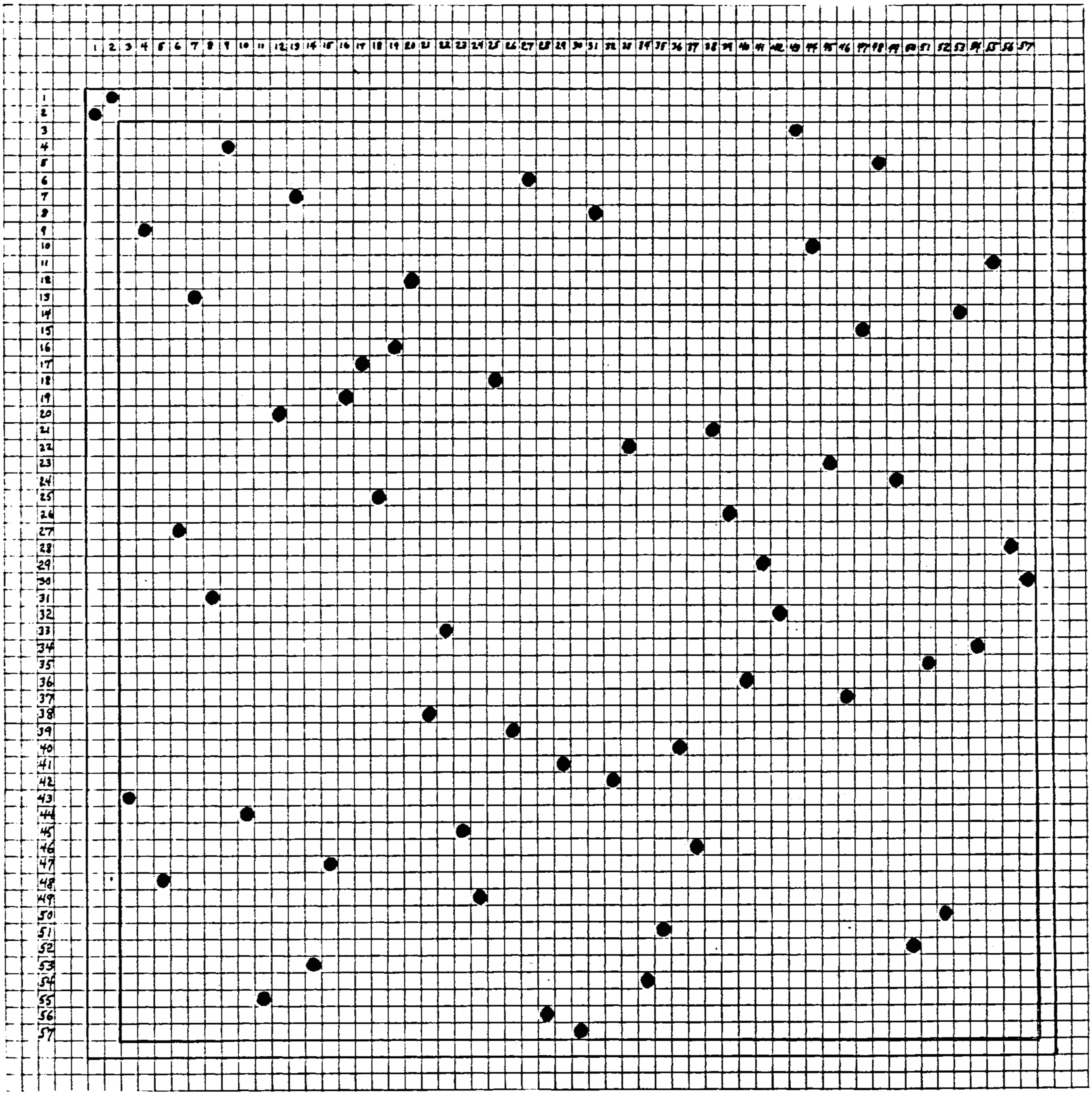


Fig. 3. T_4 with $q = 59$, $n = 55$.

L_2: $(n = q - 2)$ The $n \times n$ matrix has columns numbered $j = 1, 2, \cdots, q - 2$ and rows $i = 1, 2, \cdots, q - 2$. We put a dot in position (i, j) if and only if $\alpha^i + \alpha^j = 1$.

L_3: $(n = q - 3)$ This works *only when 2 is primitive in* $GF(q)$, where q is an odd prime. Using $\alpha = 2^{-1} = \frac{1}{2}$ will mean that $\alpha^1 + \alpha^1 = 1$, and hence that the dot at position $(1, 1)$ can be deleted from L_2 along with the entire top row and left column.

Fig. 2 illustrates L_2 with $n = 25$, that is with $q = 27$.

Taylor Variant to the Lempel Construction:

T_4: $(n = q - 4)$ This works *only when the primitive* α *in* $GF(q)$ *satisfies* $\alpha^2 + \alpha^1 = 1$. Then the dots at $(1, 2)$ and $(2, 1)$ can both be deleted simultaneously from L_2, along with the two top rows and the two left columns.

Fig. 3 shows an example of T_4 with $n = 55$, corresponding to $q = 59$.

Note: When $q = p^k$ with p prime and $k > 1$, $GF(q)$ is *not* the ring of integers modulo q. Rather, it can be represented as a k-dimensional vector space over $GF(p)$.

C. Golomb Construction

This construction uses *two* log tables for $GF(q)$, where the two bases α and β are both primitive elements in $GF(q)$, and q can be any power of any prime.

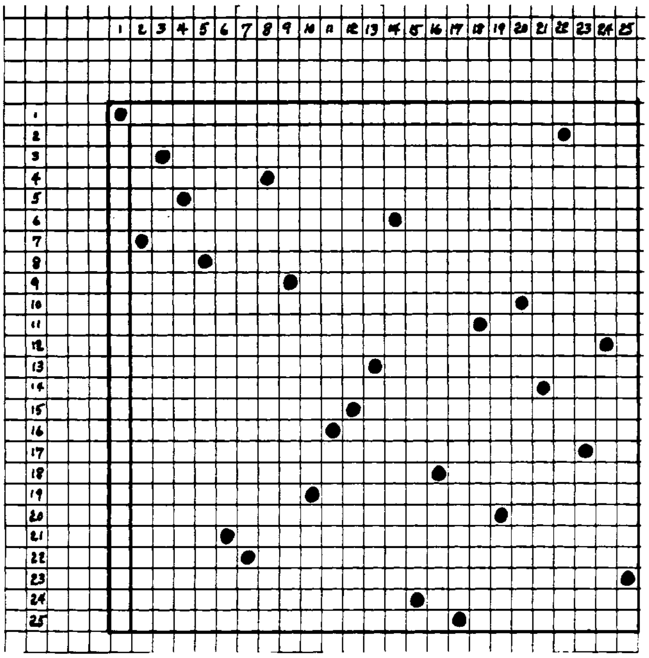


Fig. 4. G_3 with $q = 27$, $n = 24$.

G_2: $(n = q - 2)$ The $n \times n$ matrix has columns numbered $j = 1, 2, \cdots, q - 2$, and rows $i = 1, 2, \cdots, q - 2$. We put a dot in position (i, j) if and only if $\alpha^i + \beta^j = 1$.

G_3: $(n = q - 3)$ If $\alpha^1 + \beta^1 = 1$ (that is, $\alpha + \beta = 1$), then there is a dot at position (1,1) which can be deleted from G_2, along with the top row and left column. Conjecture A (see [3]) asserts that it is always possible to find primitive α and β in $GF(q)$ with $\alpha + \beta = 1$.

Fig. 4 illustrates G_3 with $n = 24$, that is with $q = 27$.

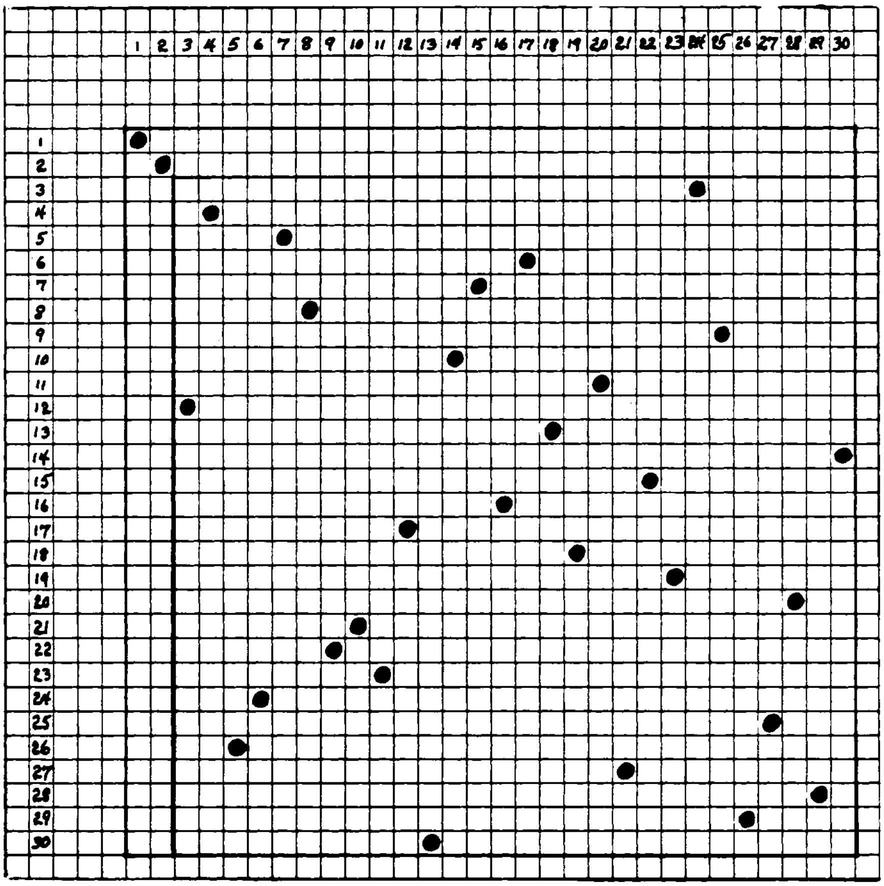
G_4: $(n = q - 4)$ This works *only when* $q = 2^k$, *and* $\alpha + \beta = 1$, in the field $GF(q)$. Here the basic arithmetic is modulo 2, so that $\alpha^1 + \beta^1 = 1$ implies $\alpha^2 + \beta^2 = 1$. Then the dots at (1,1) and (2,2) can *both* be deleted from G_2, along with the two top rows and the two left columns.

Fig. 5 illustrates G_4 with $n = 28$, $q = 32$.

Golomb Variant:

G_4^*: $(n = q - 4)$ This works *only when the primitive elements* α *and* β *satisfy* $\alpha^1 + \beta^1 = 1$ *and* $\alpha^2 + \beta^{-1} = 1$ *in* $GF(q)$. Since $-1 = q - 2$ in the arithmetic of the logarithms (exponents), there will be a deletable dot at $(2, q - 2)$ after deleting the dot at (1,1) from G_2.

G_5^*: $(n = q - 5)$ This construction *always follows* G_4^*. When $\alpha + \beta = 1$ and $\alpha^2 + \beta^{-1} = 1$, then necessarily also $\alpha^{-1} + \beta^2 = 1$ in



(a)

0					1
1				1	
2			1		
3		1			
4	1				
5			1		1
6		1		1	
7	1		1		
8		1	1		1
9	1	1		1	
10	1				1
11			1	1	1
12		1	1	1	
13	1	1	1		
14	1	1	1		1
15	1	1	1	1	1
16	1	1		1	1
17	1			1	1
18				1	1
19			1	1	
20		1	1		
21	1	1			
22	1		1		1
23		1	1	1	1
24	1	1	1	1	
25	1	1			1
26	1		1	1	1
27		1		1	1
28	1		1	1	
29		1			1
30	1			1	

(b)

Fig. 5. (a) G_4 with $q = 32$, $n = 28$. (b) A log table for $GF(32)$.

$GF(q)$. Thus, after (1,1) and (2, −1) are deleted, along with their respective rows and columns, there will be another deletable dot at (−1,2).

Fig. 6 illustrates G_5^* with $n = 144$, $q = 149$.

Taylor Variant to the Golomb Construction:

T_1: ($n = q - 1$) Add a corner dot at one of (0,0) or (0, $q - 1$) or ($q - 1$, 0) or ($q - 1$, $q - 1$). This is possible when $q \neq 2^k$ and the conditions at one of the corners do not prevent it.

T_0: ($n = q$) Add two corner dots at (0,0) and ($q - 1$, $q - 1$), or at (0, $q - 1$) and ($q - 1$, 0). This is possible when $q \equiv -1 (\text{mod}\, 6)$ and when not prevented by the condition (Appendix II) on the two corners. Fig. 7 illustrates T_0 with $n = q = 47$.

D. Adding a Corner Dot to W_1

The Welch construction W_1 is singly periodic, and hence there is a chance that one of the ($p - 1$) × ($p - 1$) windows for one of the primitive roots may allow the addition of a corner dot. In fact, the only examples of Costas arrays we have for $n = 19$ and $n = 31$ were found as instances of this sporadic occurrence. Figs. 8 and 9 exhibit them.

E. Table of Known Constructions

Up to $n = 360$, Fig. 10 tabulates for each n which constructions, if any, are known to exist.

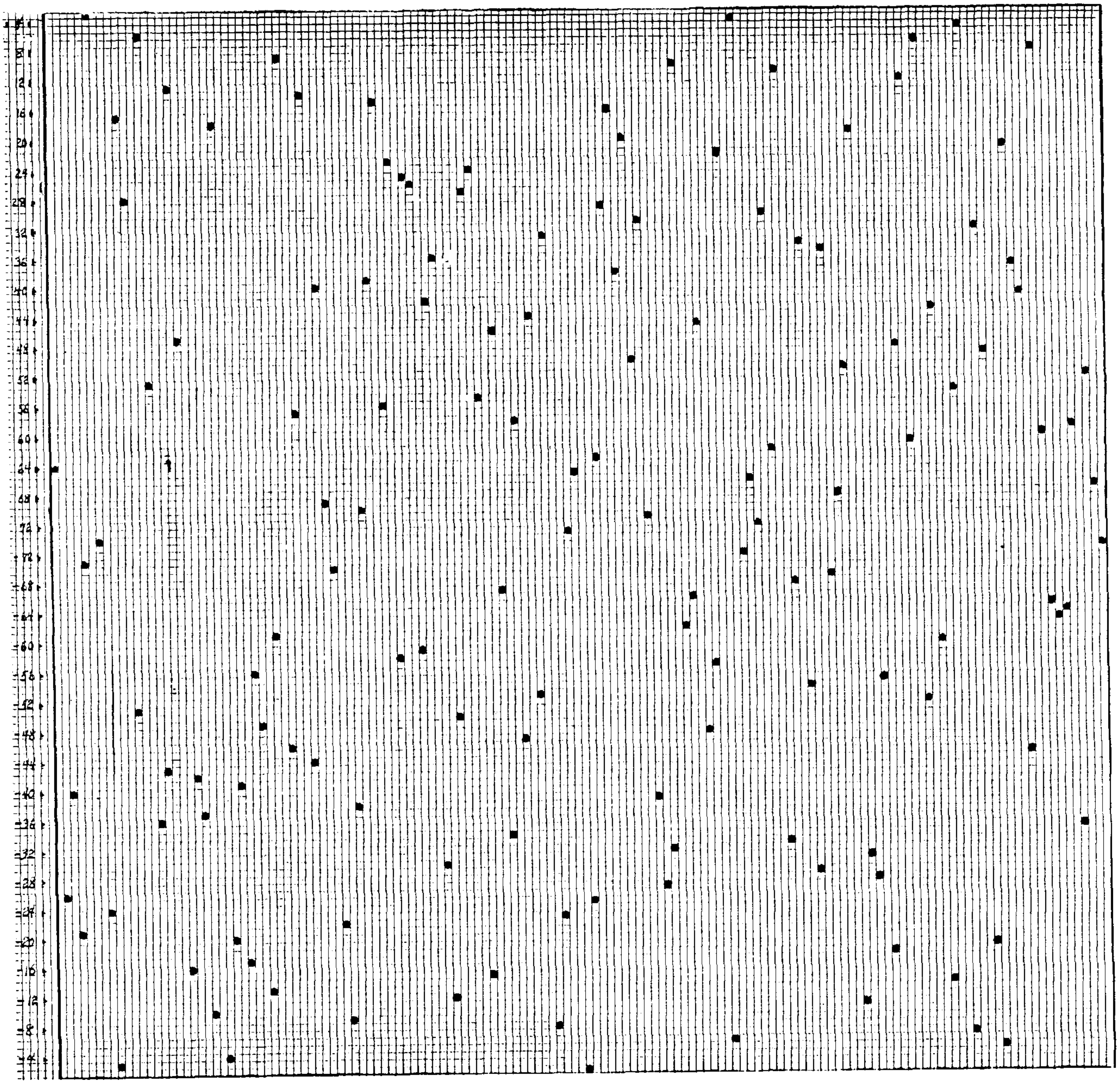


Fig. 6. G_5^* with $q = 149$, $n = 144$.

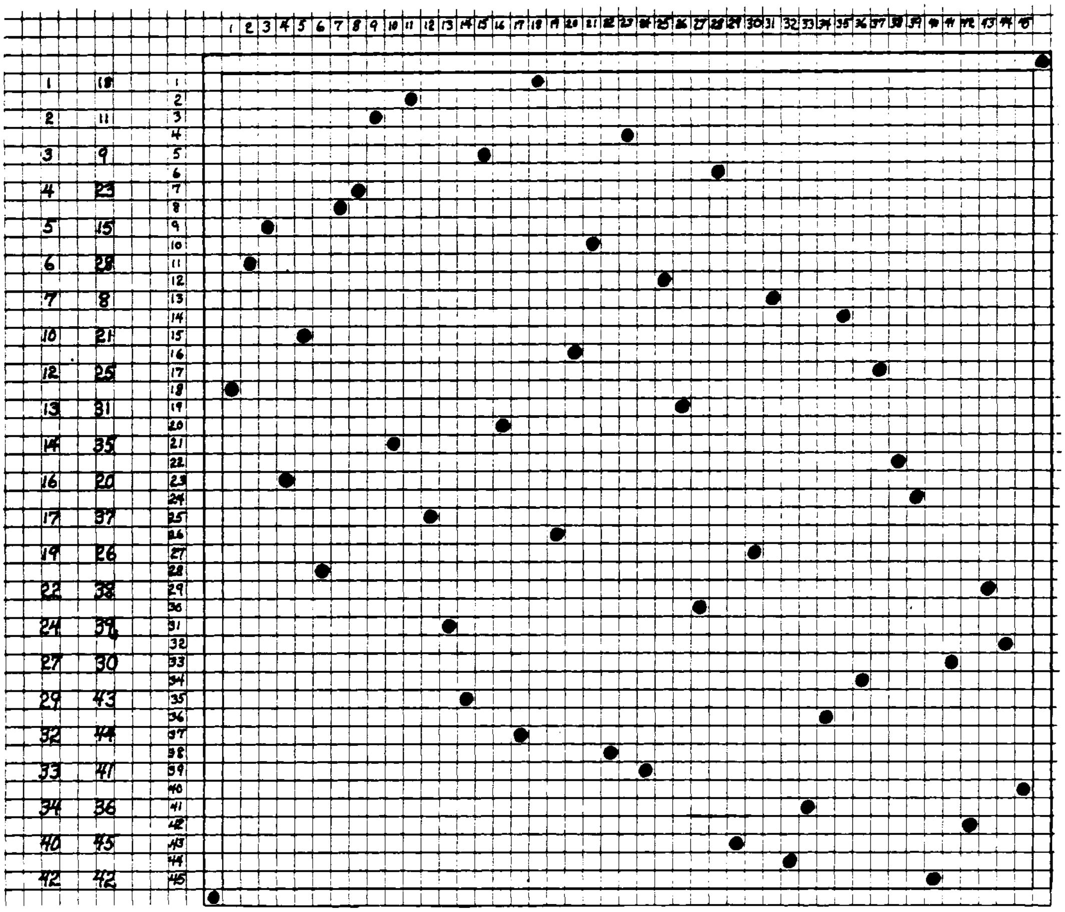


Fig. 7. T_0 with $q = 47 = n$.

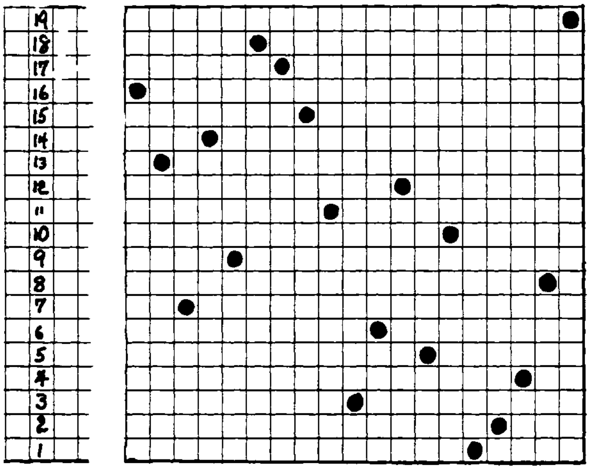


Fig. 8. Sporadic corner dot added, $p = 19 = n$.

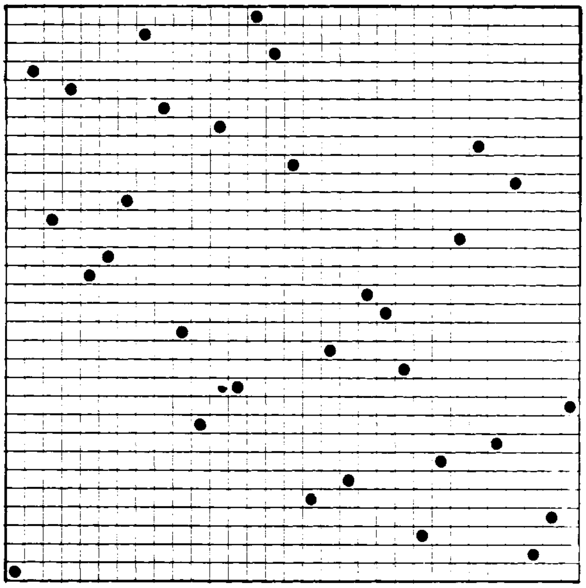


Fig. 9. Corner dot added to W_1, $p = 31 = n$.

		T_ψ	W_1	W_2	W_3	L_2	L_3	T_4	G_2	G_3	G_4	G_4°	G_5°
0	1	·	·	W_2	W_3	L_2	L_3	T_4	G_2	G_3	G_4	G_4°	G_5°
1	1	T_1	W_1	W_2	·	L_2	·	T_4	G_2	G_3	·	G_4°	·
2	1	T_ψ	W_1	·	W_3	L_2	L_3	·	G_2	G_3	·	·	—
3	1	T_1	·	W_2	·	L_2	·	—	G_2	·	·	—	—
4	1	T_1	W_1	·	—	·	—	—	·	G_3	G_4	—	G_5°
5	1	T_0	·	W_2	·	L_2	·	T_4	G_2	G_3	·	G_4°	·
6	1	T_1	W_1	·	·	L_2	·	·	G_2	G_3	·	·	—
7	1	S	·	·	·	L_2	·	T_4	G_2	·	·	—	·
8	1	T_1	·	·	W_3	·	L_3	·	·	G_3	·	·	—
9	1	—	·	W_2	·	L_2	·	—	G_2	·	·	—	·
10	1	T_1	W_1	·	W_3	·	L_3	·	·	G_3	·	·	·
11	1	T_0	·	W_2	·	L_2	·	·	G_2	·	·	·	—
12	1	—	W_1	·	·	·	·	—	·	·	G_4	—	—
13	1	S	·	·	·	·	·	—	·	G_3	·	—	·
14	1	·	·	·	—	L_2	—	·	G_2	G_3	·	·	—
15	1	—	·	W_2	·	L_2	·	T_4	G_2	·	·	—	·
16	1	T_1	W_1	·	W_3	·	L_3	·	·	G_3	·	·	·
17	1	T_0	·	W_2	·	L_2	·	·	G_2	·	·	·	·
18	1	?	W_1	·	·	·	·	·	·	·	·	·	—
19	1	S	·	·	·	·	·	—	·	·	·	—	·
20	1	·	·	·	—	·	—	·	·	G_3	·	·	—
21	1	·	·	W_2	·	L_2	·	—	G_2	·	·	—	·
22	1	T_1	W_1	·	·	·	·	·	·	G_3	·	·	—
23	1	T_0	·	·	·	L_2	·	—	G_2	·	·	—	·
24	1	?	·	·	·	·	·	·	·	G_3	·	·	—
25	1	?	·	·	·	L_2	·	—	G_2	·	·	—	·
26	1	?	·	·	W_3	·	L_3	·	·	G_3	-	·	—
27	1	—	·	W_2	·	L_2	·	T_4	G_2	·	·	—	—
28	1	T_1	W_1	·	—	·	—	—	·	G_3	G_4	—	·
29	1	T_0	·	W_2	·	L_2	·	·	G_2	G_3	·	·	·
30	1	?	W_1	·	·	L_2	·	·	G_2	·	·	·	·
31	1	S	·	·	·	·	·	·	·	·	·	·	·
32	0	—	·	·	·	·	·	·	·	·	·	·	—
33	0	·	·	·	·	·	·	—	·	·	·	—	·
34	1	·	·	·	W_3	·	L_3	·	·	G_3	·	·	·
35	1	·	·	W_2	·	L_2	·	·	G_2	·	·	·	·
36	1	?	W_1	·	·	·	·	·	·	·	·	·	G_5°
37	1	?	·	·	·	·	·	T_4	·	·	·	G_4°	·
38	1	·	·	·	—	·	—	·	·	G_3	·	·	—
39	1	·	·	W_2	·	L_2	·	—	G_2	·	·	—	·
40	1	?	W_1	·	—	·	—	·	·	G_3	·	·	·
41	1	?	·	W_2	·	L_2	·	·	G_2	·	·	·	·
42	1	?	W_1	·	·	·	·	·	·	·	·	·	—
43	0	?	·	·	·	·	·	—	·	·	·	—	·
44	1	·	·	·	—	·	—	·	·	G_3	·	·	—
45	1	·	·	W_2	·	L_2	·	—	G_2	·	·	—	·
46	1	T_1	W_1	·	·	·	·	·	·	G_3	·	·	·
47	1	T_0	·	·	·	L_2	·	·	G_2	·	·	·	·
48	0	?	·	·	·	·	·	·	·	·	·	·	—
49	0	—	·	·	·	·	·	—	·	·	·	—	·
50	1	·	·	·	W_3	·	L_3	·	·	G_3	·	·	·
51	1	·	·	W_2	·	L_2	·	·	G_2	·	·	·	·
52	1	?	W_1	·	·	·	·	·	·	·	·	·	·
53	0	?	·	·	·	·	·	·	·	·	·	·	·
54	0	·	·	·	·	·	·	·	·	·	·	·	—
55	1	·	·	·	·	·	·	T_4	·	·	·	—	·
56	1	·	·	·	W_3	·	L_3	·	·	G_3	·	·	G_5°
57	1	·	·	W_2	·	L_2	·	T_4	G_2	·	·	G_4°	·
58	1	?	W_1	·	W_3	·	L_3	·	·	G_3	·	·	·
59	1	?	·	W_2	·	L_2	·	·	G_2	·	·	·	—
60	1	?	W_1	·	·	·	·	—	·	·	G_4	—	·
61	1	?	·	·	·	·	·	·	·	G_3	·	·	·
62	1	·	·	·	·	L_2	·	·	G_2	·	·	·	—
63	0	—	·	·	·	·	·	—	·	·	·	—	·
64	1	—	·	·	W_3	·	L_3	·	·	G_3	·	·	·
65	1	·	·	W_2	·	L_2	·	·	G_2	·	·	·	·
66	1	?	W_1	·	·	·	·	·	·	·	·	·	—
67	1	?	·	·	·	·	·	T_4	·	·	·	—	·
68	1	·	·	·	—	·	—	·	·	G_3	·	·	—
69	1	·	·	W_2	·	L_2	·	—	G_2	·	·	—	·
70	1	?	W_1	·	—	·	—	·	·	G_3	·	·	·
71	1	?	·	W_2	·	L_2	·	·	G_2	·	·	·	·
72	1	?	W_1	·	·	·	·	·	·	·	·	·	·
73	0	?	·	·	·	·	·	·	·	·	·	·	·
74	0	·	·	·	·	·	·	·	·	·	·	·	—
75	1	·	·	·	·	·	·	T_4	·	·	·	—	·
76	1	·	·	·	—	·	—	·	·	G_3	·	·	—
77	1	·	·	W_2	·	L_2	·	—	G_2	·	·	—	·
78	1	?	W_1	·	·	·	·	·	·	G_3	·	·	—
79	1	?	·	·	·	L_2	·	—	G_2	·	·	—	·
80	1	?	·	·	W_3	·	L_3	·	·	G_3	·	·	·
81	1	—	·	W_2	·	L_2	·	·	G_2	·	·	·	·
82	1	?	W_1	·	·	·	·	·	·	·	·	·	·
83	0	?	·	·	·	·	·	·	·	·	·	·	·

Fig. 10. Table of known constructions up to $n = 360$.

		$T_{1,0}$	W_1	W_2	W_3	L_2	L_3	T_4	G_2	G_3	G_4	G_4°	G_5°
84	0	·	·	·	·	·	·	·	·	·	·	·	—
85	0	·	·	·	·	·	·	—	·	·	·	—	·
86	1	·	·	·	—	·	—	·	·	G_3	·	·	·
87	1	·	·	W_2	·	L_2	·	·	G_2	·	·	·	·
88	1	?	W_1	·	·	·	·	·	·	·	·	·	·
89	0	?	·	·	·	·	·	·	·	·	·	·	·
90	0	·	·	·	·	·	·	·	·	·	·	·	·
91	0	·	·	·	·	·	·	·	·	·	·	·	·
92	0	·	·	·	·	·	·	·	·	·	·	·	—
93	0	·	·	·	·	·	·	—	·	·	·	—	·
94	1	·	·	·	—	·	—	·	·	G_3	·	·	·
95	1	·	·	W_2	·	L_2	·	·	G_2	·	·	·	·
96	1	?	W_1	·	·	·	·	·	·	·	·	·	—
97	0	?	·	·	·	·	·	—	·	·	·	—	·
98	1	·	·	·	W_3	·	L_3	·	·	G_3	·	·	—
99	1	·	·	W_2	·	L_2	·	—	G_2	·	·	—	·
100	1	?	W_1	·	—	·	—	·	·	G_3	·	·	·
101	1	?	·	W_2	·	L_2	·	·	G_2	·	·	·	·
102	1	?	W_1	·	·	·	·	·	·	·	·	·	—
103	0	?	·	·	·	·	·	—	·	·	·	—	·
104	1	·	·	·	W_3	·	L_3	·	·	G_3	·	·	G_5°
105	1	·	·	W_2	·	L_2	·	T_4	G_2	·	·	G_4°	·
106	1	?	W_1	·	—	·	—	·	·	G_3	·	·	·
107	1	?	·	W_2	·	L_2	·	·	G_2	·	·	·	·
108	1	?	W_1	·	·	·	·	·	·	·	·	·	—
109	0	?	·	·	·	·	·	—	·	·	·	—	·
110	1	·	·	·	—	·	—	·	·	G_3	·	·	·
111	1	·	·	W_2	·	L_2	·	·	G_2	·	·	·	·
112	1	?	W_1	·	·	·	·	·	·	·	·	·	·
113	0	?	·	·	·	·	·	·	·	·	·	·	·
114	0	·	·	·	·	·	·	·	·	·	·	·	·
115	0	·	·	·	·	·	·	·	·	·	·	·	·
116	0	·	·	·	·	·	·	·	·	·	·	·	—
117	0	·	·	·	·	·	·	—	·	·	·	—	·
118	1	·	·	·	·	·	·	·	·	G_3	·	·	·
119	1	·	·	·	·	L_2	·	·	G_2	·	·	·	·
120	0	?	·	·	·	·	·	·	·	·	·	·	—
121	0	—	·	·	·	·	·	—	·	·	·	—	·
122	1	·	·	·	·	·	·	·	·	G_3	·	·	—
123	1	·	·	·	·	L_2	·	—	G_2	·	·	—	—
124	1	?	·	·	—	·	—	—	·	G_3	G_4	—	·
125	1	?	·	W_2	·	L_2	·	·	G_2	G_3	·	·	·

		$T_{1,0}$	W_1	W_2	W_3	L_2	L_3	T_4	G_2	G_3	G_4	G_4°	G_5°
126	1	?	W_1	·	·	L_2	·	·	G_2	·	·	·	—
127	1	?	·	·	·	·	·	T_4	·	·	·	—	·
128	1	—	·	·	W_3	·	L_3	·	·	G_3	·	·	·
129	1	·	·	W_2	·	L_2	·	·	G_2	·	·	·	·
130	1	?	W_1	·	·	·	·	·	·	·	·	·	·
131	0	?	·	·	·	·	·	·	·	·	·	·	·
132	0	·	·	·	·	·	·	·	·	·	·	·	—
133	0	·	·	·	·	·	·	—	·	·	·	—	·
134	1	·	·	·	—	·	—	·	·	G_3	·	·	—
135	1	·	·	W_2	·	L_2	·	—	G_2	·	·	—	·
136	1	?	W_1	·	W_3	·	L_3	·	·	G_3	·	·	·
137	1	?	·	W_2	·	L_2	·	·	G_2	·	·	·	·
138	1	?	W_1	·	·	·	·	·	·	·	·	·	·
139	0	?	·	·	·	·	·	·	·	·	·	·	·
140	0	·	·	·	·	·	·	·	·	·	·	·	·
141	0	·	·	·	·	·	·	·	·	·	·	·	·
142	0	·	·	·	·	·	·	·	·	·	·	·	·
143	0	·	·	·	·	·	·	·	·	·	·	·	·
144	1	·	·	·	·	·	·	·	·	·	·	·	G_5°
145	1	·	·	·	·	·	·	T_4	·	·	·	G_4°	·
146	1	·	·	·	W_3	·	L_3	·	·	G_3	·	·	—
147	1	·	·	W_2	·	L_2	·	—	G_2	·	·	—	·
148	1	?	W_1	·	—	·	—	·	·	G_3	·	·	·
149	1	?	·	W_2	·	L_2	·	·	G_2	·	·	·	·
150	1	?	W_1	·	·	·	·	·	·	·	·	·	·
151	0	?	·	·	·	·	·	·	·	·	·	·	·
152	0	·	·	·	·	·	·	·	·	·	·	·	—
153	0	·	·	·	·	·	·	—	·	·	·	—	·
154	1	·	·	·	—	·	—	·	·	G_3	·	·	·
155	1	·	·	W_2	·	L_2	·	·	G_2	·	·	·	·
156	1	?	W_1	·	·	·	·	·	·	·	·	·	·
157	0	?	·	·	·	·	·	·	·	·	·	·	·
158	0	·	·	·	·	·	·	·	·	·	·	·	—
159	0	·	·	·	·	·	·	—	·	·	·	—	·
160	1	·	·	·	W_3	·	L_3	·	·	G_3	·	·	·
161	1	·	·	W_2	·	L_2	·	·	G_2	·	·	·	·
162	1	?	W_1	·	·	·	·	·	·	·	·	·	—
163	0	?	·	·	·	·	·	—	·	·	·	—	·
164	1	·	·	·	—	·	—	·	·	G_3	·	·	—
165	1	·	·	W_2	·	L_2	·	—	G_2	·	·	—	·
166	1	?	W_1	·	·	·	·	·	·	G_3	·	·	·
167	1	?	·	·	·	L_2	·	·	G_2	·	·	·	·

Fig. 10 (*continued*).

		$T_{1,2}$	W_1	W_2	W_3	L_2	L_3	T_4	G_2	G_3	G_4	G_4^*	G_5^*
168	0	?	•	•	•	•	•	•	•	•	•	•	—
169	0	—	•	•	•	•	•	—	•	•	•	—	•
170	1	•	•	•	W_3	•	L_3	•	•	G_3	•	•	•
171	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
172	1	?	W_1	•	•	•	•	•	•	•	•	•	•
173	0	?	•	•	•	•	•	•	•	•	•	•	•
174	0	•	•	•	•	•	•	•	•	•	•	•	—
175	1	•	•	•	•	•	•	T_4	•	•	•	—	•
176	1	•	•	•	W_3	•	L_3	•	•	G_3	•	•	—
177	1	•	•	W_2	•	L_2	•	—	G_2	•	•	—	•
178	1	?	W_1	•	W_3	•	L_3	•	•	G_3	•	•	•
179	1	?	•	W_2	•	L_2	•	•	G_2	•	•	•	•
180	1	?	W_1	•	•	•	•	•	•	•	•	•	•
181	0	?	•	•	•	•	•	•	•	•	•	•	•
182	0	•	•	•	•	•	•	•	•	•	•	•	•
183	0	•	•	•	•	•	•	•	•	•	•	•	•
184	0	•	•	•	•	•	•	•	•	•	•	•	•
185	0	•	•	•	•	•	•	•	•	•	•	•	•
186	0	•	•	•	•	•	•	•	•	•	•	•	—
187	1	•	•	•	•	•	•	T_4	•	•	•	—	•
188	1	•	•	•	—	•	—	•	•	G_3	•	•	—
189	1	•	•	W_2	•	L_2	•	—	G_2	•	•	—	•
190	1	?	W_1	•	—	•	—	•	•	G_3	•	•	•
191	1	?	•	W_2	•	L_2	•	•	G_2	•	•	•	•
192	1	?	W_1	•	•	•	•	•	•	•	•	•	—
193	0	?	•	•	•	•	•	—	•	•	•	—	•
194	1	•	•	•	W_3	•	L_3	•	•	G_3	•	•	—
195	1	•	•	W_2	•	L_2	•	—	G_2	•	•	—	•
196	1	?	W_1	•	—		—	•	•	G_3	•	•	•
197	1	?	•	W_2	•	L_2	•	•	G_2	•	•	•	•
198	1	?	W_1	•	•	•	•	•	•	•	•	•	•
199	0	?	•	•	•	•	•	•	•	•	•	•	•
200	0	•	•	•	•	•	•	•	•	•	•	•	•
201	0	•	•	•	•	•	•	•	•	•	•	•	•
202	0	•	•	•	•	•	•	•	•	•	•	•	•
203	0	•	•	•	•	•	•	•	•	•	•	•	•
204	0	•	•	•	•	•	•	•	•	•	•	•	•
205	0	•	•	•	•	•	•	•	•	•	•	•	•
206	0	•	•	•	•	•	•	•	•	•	•	•	—
207	0	•	•	•	•	•	•	—	•	•	•	—	•
208	1	•	•	•	W_3	•	L_3	•	•	G_3	•	•	•
209	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
210	1	?	W_1	•	•	•	•	•	•	•	•	•	•
211	0	?	•	•	•	•	•	•	•	•	•	•	•
212	0	•	•	•	•	•	•	•	•	•	•	•	•
213	0	•	•	•	•	•	•	•	•	•	•	•	•
214	0	•	•	•	•	•	•	•	•	•	•	•	•
215	0	•	•	•	•	•	•	•	•	•	•	•	•
216	0	•	•	•	•	•	•	•	•	•	•	•	•
217	0	•	•	•	•	•	•	•	•	•	•	•	•
218	0	•	•	•	•	•	•	•	•	•	•	•	—
219	0	•	•	•	•	•	•	—	•	•	•	—	•
220	1	•	•	•	—	•	—	•	•	G_3	•	•	•
221	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
222	1	?	W_1	•	•	•	•	•	•	•	•	•	—
223	0	?	•	•	•	•	•	—	•	•	•	—	•
224	1	•	•	•	W_3	•	L_3	•	•	G_3	•	•	—
225	1	•	•	W_2	•	L_2	•	—	G_2	•	•	—	•
226	1	?	W_1	•	—	•	—	•	•	G_3	•	•	•
227	1	?	•	W_2	•	L_2	•	•	G_2	•	•	•	•
228	1	?	W_1	•	•	•	•	•	•	•	•	•	—
229	0	?	•	•	•	•	•	—	•	•	•	—	•
230	1	•	•	•	—	•	—	•	•	G_3	•	•	•
231	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
232	1	?	W_1	•	•	•	•	•	•	•	•	•	•
233	0	?	•	•	•	•	•	•	•	•	•	•	•
234	0	•	•	•	•	•	•	•	•	•	•	•	—
235	1	•	•	•	•	•	•	T_4	•	•	•	—	•
236	1	•	•	•	—	•	—	•	•	G_3	•	•	G_5^*
237	1	•	•	W_2	•	L_2	•	T_4	G_2	•	•	G_4^*	•
238	1	?	W_1	•	—	•	—	•	•	G_3	•	•	—
239	1	?	•	W_2	•	L_2	•	—	G_2	•	•	—	•
240	1	?	W_1	•	•	•	•	•	•	G_3	•	•	•
241	1	?	•	•	•	L_2	•	•	G_2	•	•	•	•
242	0	?	•	•	•	•	•	•	•	•	•	•	•
243	0	—	•	•	•	•	•	•	•	•	•	•	•
244	0	•	•	•	•	•	•	•	•	•	•	•	•
245	0	•	•	•	•	•	•	•	•	•	•	•	•
246	0	•	•	•	•	•	•	•	•	•	•	•	—
247	1	•	•	•	•	•	•	T_4	•	•	•	—	•
248	1	•	•	•	—	•	—	•	•	G_3	•	•	•
249	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
250	1	?	W_1	•	•	•	•	•	•	•	•	•	•
251	0	?	•	•	•	•	•	•	•	•	•	•	—

Fig. 10 (*continued*)

		$T_{1,0}$	W_1	W_2	W_3	L_2	L_3	T_4	G_2	G_3	G_4	G_4^*	G_5^*
252	1	•	•	•	•	•	•	–	•	•	G_4	–	–
253	1	•	•	•	•	•	•	–	•	G_3	•	–	•
254	1	•	•	•	–	L_2	–	•	G_2	G_3	•	•	•
255	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
256	1	?	W_1	•	•	•	•	•	•	•	•	•	•
257	0	?	•	•	•	•	•	•	•	•	•	•	•
258	0	•	•	•	•	•	•	•	•	•	•	•	–
259	0	•	•	•	•	•	•	–	•	•	•	–	•
260	1	•	•	•	–	•	–	•	•	G_3	•	•	•
261	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
262	1	?	W_1	•	•	•	•	•	•	•	•	•	•
263	0	?	•	•	•	•	•	•	•	•	•	•	•
264	1	•	•	•	•	•	•	•	•	•	•	•	G_5^*
265	1	•	•	•	•	•	•	T_4	•	•	•	G_4^*	•
266	1	•	•	•	W_3	•	L_3	•	•	G_3	•	•	–
267	1	•	•	W_2	•	L_2	•	T_4	G_2	•	•	–	•
268	1	?	W_1	•	–	•	–	•	•	G_3	•	•	•
269	1	?	•	W_2	•	L_2	•	•	G_2	•	•	•	•
270	1	?	W_1	•	•	•	•	•	•	•	•	•	•
271	0	?	•	•	•	•	•	•	•	•	•	•	•
272	0	•	•	•	•	•	•	•	•	•	•	•	–
273	0	•	•	•	•	•	•	–	•	•	•	–	•
274	1	•	•	•	–	•	–	•	•	G_3	•	•	•
275	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
276	1	?	W_1	•	•	•	•	•	•	•	•	•	–
277	0	?	•	•	•	•	•	–	•	•	•	–	•
278	1	•	•	•	–	•	–	•	•	G_3	•	•	–
279	1	•	•	W_2	•	L_2	•	–	G_2	•	•	–	•
280	1	?	W_1	•	•	•	–	•	•	G_3	•	•	•
281	1	?	•	W_2	•	L_2	•	•	G_2	•	•	•	•
282	1	?	W_1	•	•	•	•	•	•	•	•	•	•
283	0	?	•	•	•	•	•	•	•	•	•	•	•
284	0	•	•	•	•	•	•	•	•	•	•	•	–
285	0	•	•	•	•	•	•	–	•	•	•	–	•
286	1	•	•	•	•	•	•	•	•	G_3	•	•	•
287	1	•	•	•	•	L_2	•	•	G_2	•	•	•	•
288	0	?	•	•	•	•	•	•	•	•	•	•	–
289	0	–	•	•	•	•	•	–	•	•	•	–	•
290	1	•	•	•	W_3	•	L_3	•	•	G_3	•	•	•
291	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
292	1	?	W_1	•	•	•	•	•	•	•	•	•	•
293	0	?	•	•	•	•	•	•	•	•	•	•	•

		$T_{1,0}$	W_1	W_2	W_3	L_2	L_3	T_4	G_2	G_3	G_4	G_4^*	G_5^*
294	0	•	•	•	•	•	•	•	•	•	•	•	•
295	0	•	•	•	•	•	•	•	•	•	•	•	•
296	0	•	•	•	•	•	•	•	•	•	•	•	•
297	0	•	•	•	•	•	•	•	•	•	•	•	•
298	0	•	•	•	•	•	•	•	•	•	•	•	•
299	0	•	•	•	•	•	•	•	•	•	•	•	•
300	0	•	•	•	•	•	•	•	•	•	•	•	•
301	0	•	•	•	•	•	•	•	•	•	•	•	•
302	0	•	•	•	•	•	•	•	•	•	•	•	–
303	0	•	•	•	•	•	•	–	•	•	•	–	•
304	1	•	•	•	–	•	–	•	•	G_3	•	•	•
305	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
306	1	?	W_1	•	•	•	•	•	•	•	•	•	–
307	1	?	•	•	•	•	•	T_4	•	•	•	–	•
308	1	•	•	•	–	•	–	•	•	G_3	•	•	–
309	1	•	•	W_2	•	L_2	•	–	G_2	•	•	–	•
310	1	?	W_1	•	–	•	–	•	•	G_3	•	•	•
311	1	?	•	W_2	•	L_2	•	•	G_2	•	•	•	•
312	1	?	W_1	•	•	•	•	•	•	•	•	•	–
313	0	?	•	•	•	•	•	–	•	•	•	–	•
314	1	•	•	•	W_3	•	L_3	•	•	G_3	•	•	•
315	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
316	1	?	W_1	•	•	•	•	•	•	•	•	•	•
317	0	?	•	•	•	•	•	•	•	•	•	•	•
318	0	•	•	•	•	•	•	•	•	•	•	•	•
319	0	•	•	•	•	•	•	•	•	•	•	•	•
320	0	•	•	•	•	•	•	•	•	•	•	•	•
321	0	•	•	•	•	•	•	•	•	•	•	•	•
322	0	•	•	•	•	•	•	•	•	•	•	•	•
323	0	•	•	•	•	•	•	•	•	•	•	•	•
324	0	•	•	•	•	•	•	•	•	•	•	•	•
325	0	•	•	•	•	•	•	•	•	•	•	•	•
326	0	•	•	•	•	•	•	•	•	•	•	•	–
327	1	•	•	•	•	•	•	–	•	•	•	–	•
328	1	•	•	•	–	•	–	•	•	G_3	•	•	•
329	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
330	1	?	W_1	•	•	•	•	•	•	•	•	•	•
331	0	?	•	•	•	•	•	•	•	•	•	•	•
332	0	•	•	•	•	•	•	•	•	•	•	•	–
333	0	•	•	•	•	•	•	–	•	•	•	–	•
334	1	•	•	•	–	•	–	•	•	G_3	•	•	•
335	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•

Fig. 10 (*continued*).

		$T_{1,0}$	W_1	W_2	W_3	L_2	L_3	T_4	G_2	G_3	G_4	G_4^*	G_5^*
336	1	?	W_1	•	•	•	•	•	•	•	•	•	•
337	0	?	•	•	•	•	•	•	•	•	•	•	•
338	0	•	•	•	•	•	•	•	•	•	•	•	—
339	0	•	•	•	•	•	•	—	•	•	•	—	•
340	1	•	•	•	•	•	•	•	•	G_3	•	•	•
341	1	•	•	•	•	L_2	•	•	G_2	•	•	•	•
342	0	•	•	•	•	•	•	•	•	•	•	•	—
343	0	•	•	•	•	•	•	—	•	•	•	—	•
344	1	•	•	•	W_3	•	L_3	•	•	G_3	•	•	—
345	1	•	•	W_2	•	L_2	•	—	G_2	•	•	—	•
346	1	?	W_1	•	W_3	•	L_3	•	•	G_3	•	•	•
347	1	?	•	W_2	•	L_2	•	•	G_2	•	•	•	•
348	1	?	W_1	•	•	•	•	•	•	•	•	•	—
349	0	?	•	•	•	•	•	—	•	•	•	—	•
350	1	•	•	•	—	•	—	•	•	G_3	•	•	•
351	1	•	•	W_2	•	L_2	•	•	G_2	•	•	•	•
352	1	?	W_1	•	•	•	•	•	•	•	•	•	•
353	0	?	•	•	•	•	•	•	•	•	•	•	•
354	0	•	•	•	•	•	•	•	•	•	•	•	—
355	1	•	•	•	•	•	•	T_4	•	•	•	—	•
356	1	•	•	•	—	•	—	•	•	G_3	•	•	—
357	1	•	•	W_2	•	L_2	•	—	G_2	•	•	—	•
358	1	?	W_1	•	•	•	•	•	•	G_3	•	•	•
359	1	?	•	•	•	L_2	•	•	G_2	•	•	•	•
360	0	?	•	•	•	•	•	•	•	•	•	•	•

Fig. 10 (*continued*).

III. Costas Arrays with Special Properties

A. Periodic Constructions

Repeating the 2 × 2 Costas array in both directions over the entire plane gives a doubly periodic checkerboard pattern with a Costas array in every 2 × 2 window. For any $n > 2$, however, there does not exist a doubly periodic pattern with a Costas array in every $n \times n$ window. (A proof of this result is given in [11].) The nearest approximation to such a pattern is given by the extended Welch construction, as follows.

Let p be an odd prime, with primitive root α. Put a dot in position (i,j) iff $i \equiv \alpha^j (\bmod p)$. The resulting infinite integer matrix of dots and blanks has the property that in every $p \times p$ window there are p dots with no repeated vector difference. (Each $p \times p$ window fails to be a Costas array by having one empty row and one row with two dots.)

Singly periodic patterns, $(p-1) \times \infty$, exist which have a Costas array in every $(p-1) \times (p-1)$ window, where the windows are only left–right shifted. The only known examples are those arising from the extended Welch construction, but the possibility of other examples has not been entirely ruled out.

B. Nonattacking Queens

For $n > 1$ we have found no example of a Costas array consisting of nonattacking Queens. It would even be interesting to find a Costas array for $n > 10$ having only one occurrence of a Queen attack. (Another sort of near miss is shown in Fig. 11.)

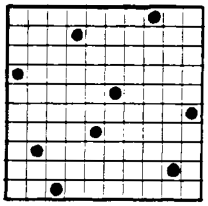


Fig. 11. Nine nonattacking Queens on a 10 × 10 board.

If an application could be satisfied with "semi-Queens," then we already have an infinite supply from the Lempel construction. A "semi-Queen" would attack its row and column but only the diagonal parallel to the main diagonal. Symmetry prohibits two dots in any line parallel to but off of the main diagonal, because reflection would repeat their difference vector. In the Lempel construction with q any power of an odd prime, there will be exactly one solution to $\alpha^x + \alpha^x = 1$, for each primitive α, and hence exactly one dot on the main diagonal. With q a power of two, there will be no solution to $\alpha^x + \alpha^x = 1$, and hence no dot on the main diagonal.

It may be useful to note that we can describe exactly which Queen attacks do occur in the Lempel construction. Each dot at (i,j) attacks the dot at (j,i), and no others. This is illustrated in Fig. 12 with $GF(3^3)$.

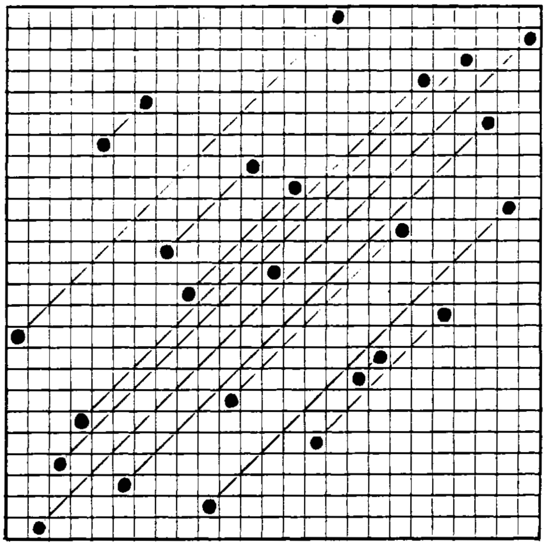


Fig. 12. Queen attack in Lempel construction.

C. Shearing

Distinctness of differences will be preserved by any nonsingular linear transformation, such as multiplying by a complex number, or applying the matrix

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$$

to shear the integer lattice. There are a few Costas arrays which shear by

$$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

into other Costas arrays. Fig. 13 shows the Lempel construc-

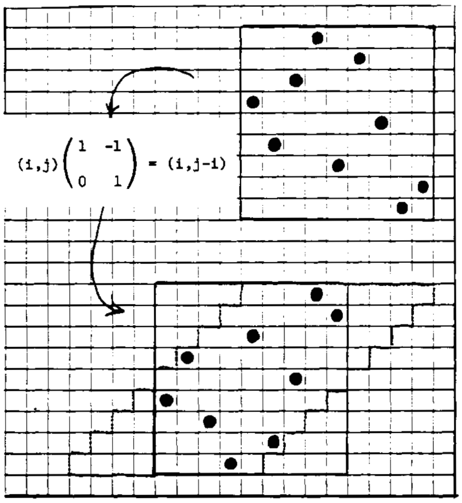


Fig. 13. An example of shearing.

tion for $GF(11)$ with $\alpha = -3$ sheared into what appears to be a 90° rotation of itself.

To be shearable by

$$\begin{bmatrix}1 & -1\\0 & 1\end{bmatrix}$$

into another Costas array, the array needs to have one dot in each of n consecutive lines parallel to the main diagonal, since these lines will become columns after shearing. Rows remain rows, and columns become lines at right angles to the main diagonal, so that the figure could be sheared again by

$$\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}$$

to produce yet another Costas array. The array of Fig. 13 goes through a cycle of four different patterns, as do all but one of the known shearable arrays for $n > 1$. "But one" refers to the array of Fig. 14 which, sheared alternately by

$$\begin{bmatrix}1 & -1\\0 & 1\end{bmatrix}$$

(horizontal) and

$$\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}$$

(vertical), goes through a remarkable cycle of twelve patterns. Except for $n = 2$, all n for which shearable arrays are known correspond exactly to the n for which honeycomb arrays are known, as described in the next section.

D. Honeycomb Arrays (Nonattacking Bee-Rooks)

Shear-compression by

$$\begin{bmatrix}3/2 & -1/2\\0 & 1\end{bmatrix}$$

will convert the square grid (Gaussian integers) into the triangular grid (Eisenstein integers), or square cells into hexagonal cells. When it happens on an $n \times n$ board that n nonattacking semi-Queens occupy n consecutive lines parallel to the main diagonal, then we can delete the unoccupied diagonal lines and apply shear-compression to convert the board into a "honeycomb array" with n lines parallel to each of the three pairs of opposite sides. The semi-Queens get converted into n nonattacking "bee-Rooks." The pattern of Fig. 13 becomes a honeycomb array with nonattacking bee-Rooks, as illustrated in Fig. 15.

On the honeycomb board having n parallel lines we have a quick proof that the maximum number of nonattacking

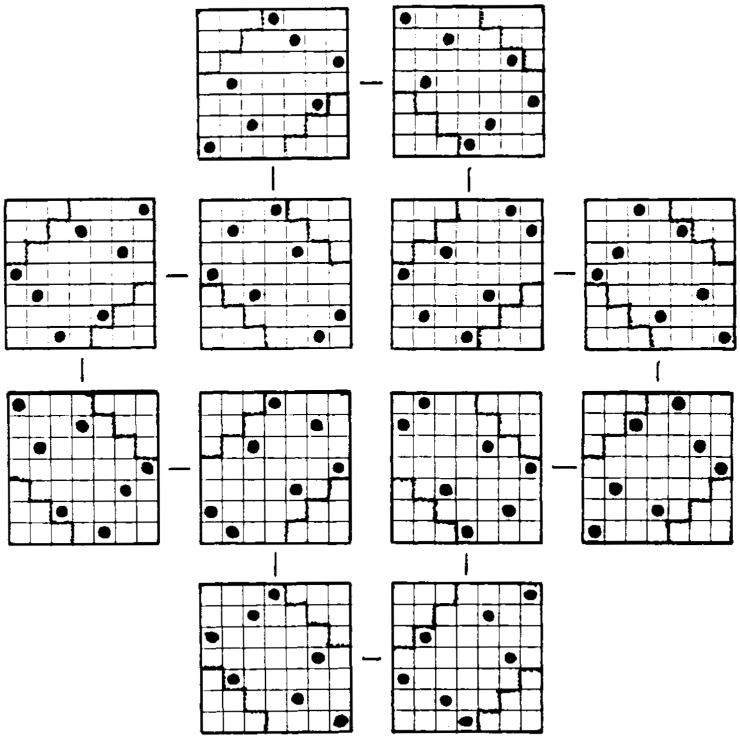


Fig. 14. A cycle of twelve by shearing.

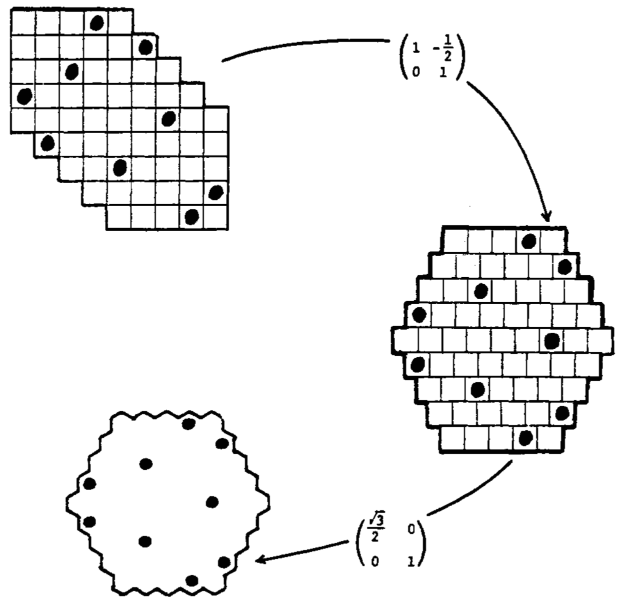

$\begin{pmatrix} 1 & -\frac{1}{2} \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} \frac{\sqrt{3}}{2} & 0 \\ 0 & 1 \end{pmatrix}$

Fig. 15. Shear compression.

bee-Rooks is n. If there were more than n bee-Rooks on the board, then at least one line would contain at least two bee-Rooks attacking each other.

The number of empty cells attacked by a bee-Rook placed in the middle of the board is larger than the number attacked by one near the edge. This happens because in the conversion from square to honeycomb we deleted some diagonal lines. Now on the honeycomb board some elementary counting problems become nontrivial.

Let us define a "bee-Duke" on the board with hexagonal cells as a piece which can move to any one of the six adjacent cells. [This is the natural analog to the Duke defined in [14]. (The "Duke" also appears in *Winning Ways*, and in R. A. Epstein's *Theory of Games and Statistical Logic*.)] The *distance* between two cells in the hexagonal Lee metric is then defined as the minimum number of bee-Duke moves needed to go from one cell to the other. In terms of this metric a "Lee-sphere of radius r" consists of a center cell together with all the cells at distance $\leqslant r$ from the center. For all the known honeycomb arrays, with n nonattacking bee-Rooks on a board having n lines parallel to each of the three pairs of opposite sides, the honeycomb board is in fact a Lee sphere, but we have not proved that this must always be the case.

Computing six or seven terms and looking in Neil Sloane's *Handbook of Integer Sequences* [15] has led us from honeycomb arrays to some old questions which are not well-known today.

The CUBAN PRIMES of Cunningham [13] show up when we simply count the number of cells on a honeycomb board when it is a Lee sphere of radius r. The number is always a difference of two consecutive cubes, $(r+1)^3 - r^3$, and often prime: whether *infinitely* often or not is an old question, still unanswered.

The ZERO SUM ARRAYS of Bennett and Potts [12] arrive at the problem of counting the number $N(r)$ of configurations of $n = 2r + 1$ nonattacking bee-Rooks on a honeycomb board which is a Lee sphere of radius r. On a square $n \times n$ board with n nonattacking Rooks the corresponding number of configurations would be simply $n!$, but on the honeycomb board it is not so simple. With the aid of a computer they found answers up to $r = 7$, as tabulated below. Let $\eta(r)$ be the number of configurations inequivalent under the dihedral group of symmetries of the hexagon.

r	0	1	2	3	4	5	6	7
$N(r)$	1	2	6	28	244	2544	35600	659632
$\eta(r)$	1	1	1	5	29	224	3012	55200

Counting honeycomb arrays presents a new problem with the requirement that all differences be distinct among $2r + 1$ nonattacking bee-Rooks on a honeycomb board of radius r.

Let $H(r)$ = the total number of honeycomb arrays of radius r.
Let $h(r)$ = the number of honeycomb arrays of radius r inequivalent under the dihedral group of symmetries of the hexagon.

The following table exhibits the full extent of our knowledge about $H(r)$ and $h(r)$.

r	0	1	2	3	4	5	6	7
$H(r)$	1	2	0	8	4	?	?	$\geqslant 2$
$h(r)$	1	1	0	2	2	?	?	$\geqslant 1$
r	8	9	10	11	12	13	$\cdots$	22
$H(r)$	?	?	$\geqslant 2$	?	?	$\geqslant 2$	? $\cdots$?	$\geqslant 2$
$h(r)$	?	?	$\geqslant 1$	?	?	$\geqslant 1$	? $\cdots$?	$\geqslant 1$

The first six honeycomb arrays are pictured in Fig. 16. The only ones known for radii 7, 10, and 13 are pictured in Figs. 17–19, respectively. The example with radius 22 is used in Section II to illustrate the T_0 construction for the prime number 47 (Fig. 7).

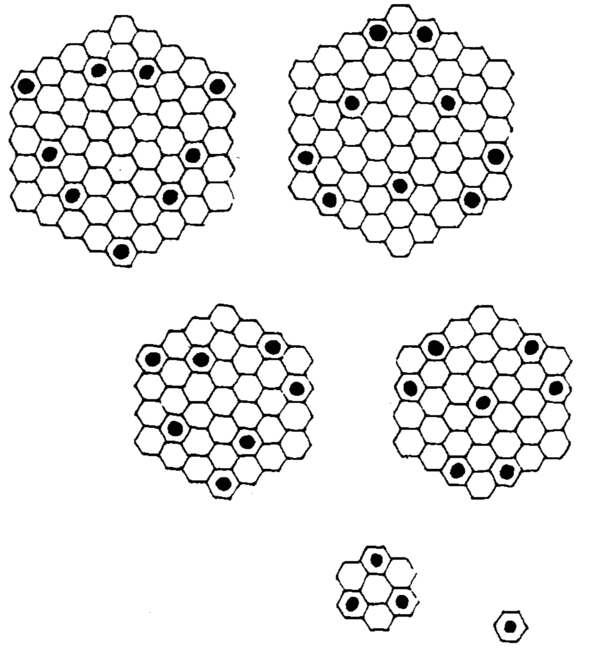


Fig. 16. The first six honeycomb arrays.

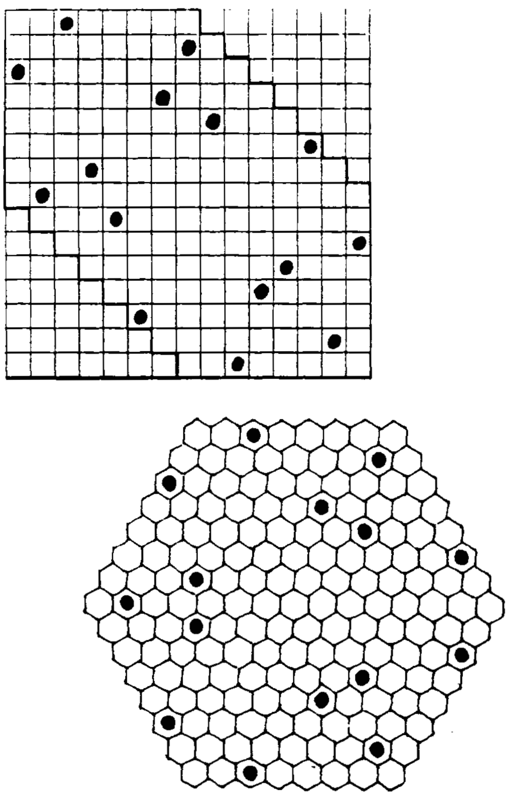


Fig. 17. Honeycomb array with $r = 7$.

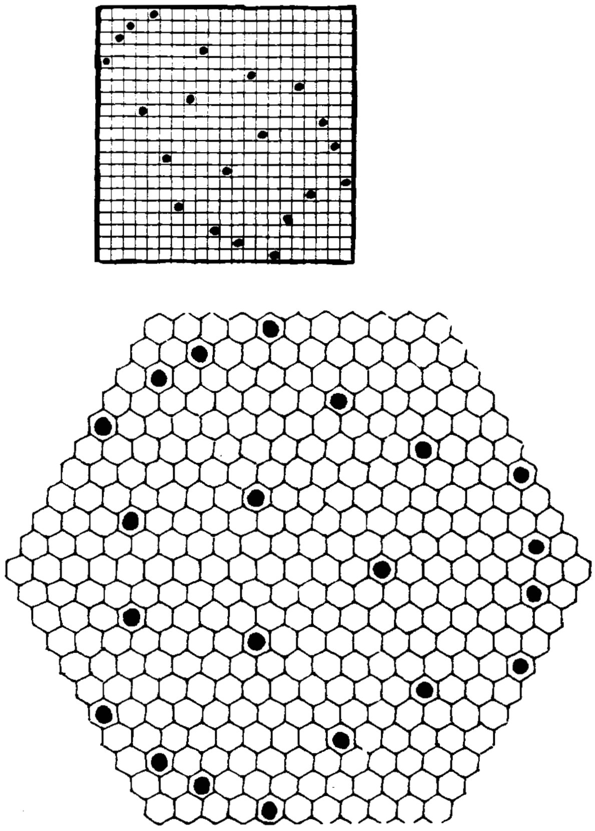


Fig. 18. Honeycomb array with $r = 10$.

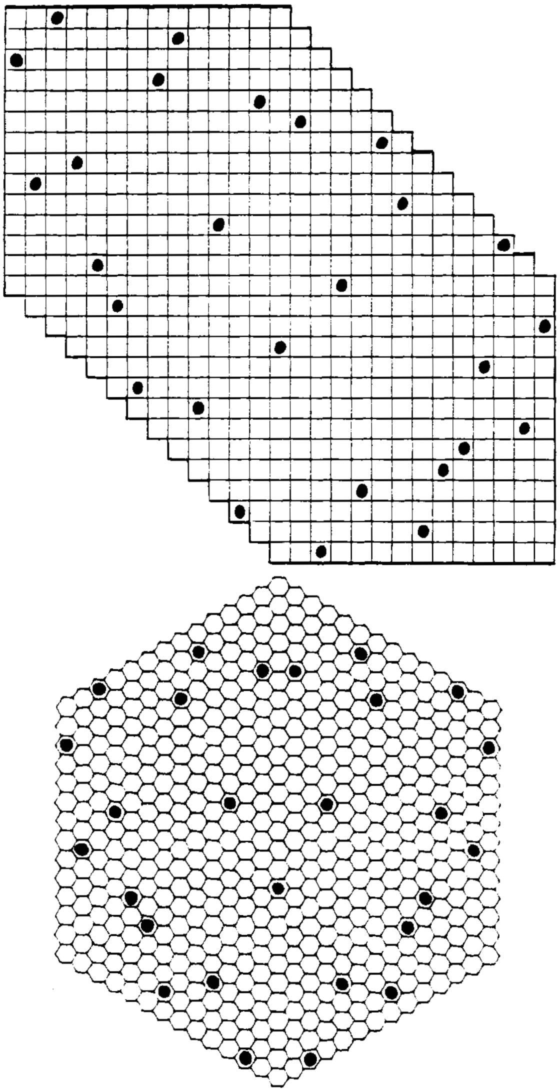


Fig. 19. Honeycomb array with $r = 13$.

E. Nonattacking Kings

Another *special property* is that every pair of dots be separated by a distance $\geqslant 3$ in the Lee metric of coding theory. This makes the Costas array a configuration of nonattacking chess Kings. There are only five of these for $n \leqslant 8$, shown in Fig. 20.

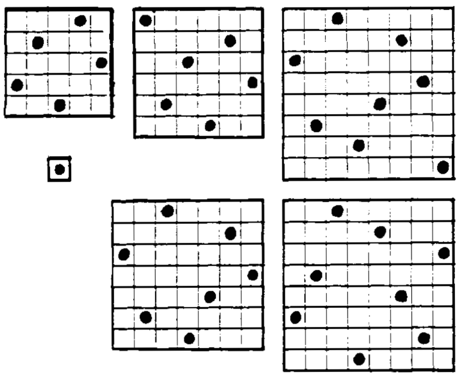


Fig. 20. Costas arrays with nonattacking Kings for $n \leqslant 8$.

In the Costas arrays derived from the Welch construction (for $p \geqslant 7$) at least one pair of attacking Kings will always appear, as a consequence of the following fact about odd prime fields: For any primitive root α in $GF(p)$ there exists exactly one j such that $\alpha^{j+1} - \alpha^j = 1$.

To obtain a Costas array of nonattacking Kings by systematic construction we can use the "T_4 variant," that is, a Lempel-type construction where some primitive α in $GF(q)$ satisfies $\alpha^2 + \alpha^1 = 1$. With no Queen attack parallel to the main diagonal in *any* Lempel-type array, as mentioned in Section III-B, *a fortiori* there will be no King attack in the T_4 variant after removing the rows and columns containing (1, 2) and (2, 1).

F. Symmetric Arrays

In all examples of the Lempel type, $\alpha^i + \alpha^j = 1$ implies that both (i, j) and (j, i) are dots in the array, whence these arrays are always symmetric. The reduced arrays with $q - 3$ in the L_3 case or $q - 4$ in the T_4 case are also symmetric, since the dot or pair of dots deleted were from (1, 1), or, respectively, from both (1, 2) and (2, 1) simultaneously.

The Golomb-type constructions give symmetric arrays in every case where $q = p^{2k}$ is an even power of a prime. If α is any primitive root, then $\alpha^{p^k} = \beta$ will also be a primitive root, and if $\alpha^i + \beta^j = 1$ it follows that $(\alpha^i + \alpha^{p^k j})^{p^k} = \alpha^{p^k i} + \alpha^j = \beta^i + \alpha^j = 1$. A dot goes at (i, j) iff a dot goes at (j, i), so the array is symmetric. One of these is illustrated in Fig. 21. In Conjecture D of [3], Golomb conjectured that $GF(p^{2k})$ can always be generated over $GF(p^k)$ by finding a primitive quadratic of trace 1, $f(x) = x^2 - x + g$, over $GF(p^k)$. The roots α and β of $f(x)$ will then be primitive in $GF(p^{2k})$ with $\alpha + \beta = 1$, and $\alpha\beta = g$ will be primitive in $GF(p^k)$. (See the Theorem in Appendix I, p. 1161.) In [4], Moreno has proved this conjecture when $p = 2$, for all values of k.

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$c(n)$	1	1	1	2	6	17	30	60	100	277	555	990	1616
$C(n)$	1	2	4	12	40	116	200	444	760	2160	4368	7852	12828
$\frac{C(n)}{n!}$	1	1	0.66	0.5	0.33	0.16	0.039	0.011	0.002	0.0006	0.00011	0.000016	0.000002

An even more special $n \times n$ Costas array is one which is symmetric and has the main diagonal empty. Of course n must be even. These are given systematically by L_2 when q is a power of 2, and by L_3 when 2 is a primitive root of an odd prime p. In Fig. 22, the exhibit of all such arrays for $n \leqslant 8$ includes one 8×8 example which is not given by any known systematic symmetric construction. It is not known whether any of these special arrays exist for $n = 12$.

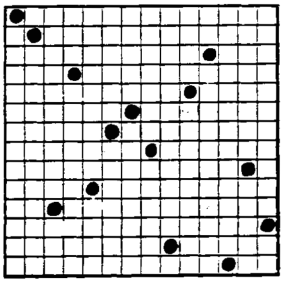


Fig. 21. Symmetric Golomb type. Example of G_2 when $q = p^{2k}$ and $\alpha^{p^k} = \beta$.

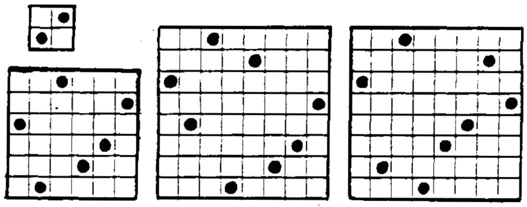


Fig. 22. Symmetric with main diagonal empty.

IV. $C(n)$ and $c(n)$: The Number of Costas Arrays

Let $C(n)$ = the total number of $n \times n$ Costas arrays.

Let $c(n)$ = the number of $n \times n$ Costas arrays inequivalent under the dihedral group of symmetries of the square.

We can prove that the limit superior (lim sup) of $C(n)$ is infinite because the Welch construction guarantees $C(n) \geqslant 2n$ when $n + 1$ is an odd prime.

On the other hand, we have no actual proof that $C(32)$ is not zero, or that $C(n)$ is not zero infinitely often. That is, we cannot show

$$\liminf_{n \to \infty} C(n) > 0.$$

The exact values of $C(7)$, $C(8)$, $C(9)$, and $C(10)$ were first brought to our attention by Richard Games and Michael Chao, who found them by computer in the summer of 1983 at the Mitre Corp. All values of $C(n)$ for $n \leqslant 12$ were first found by John P. Costas of the General Electric Company. The currently known values of $C(n)$ and $c(n)$ are as follows. The values of $c(n)$ for $9 \leqslant n \leqslant 13$ and of $C(13)$ were found in May, 1984, by John Robbins.

The value $C(7) = 200$ corrects an error in [2].

It is worth noting how rapidly $C(n)/n!$ is approaching zero, since it represents the probability that a randomly chosen $n \times n$ permutation matrix will be a Costas array. If the growth rate $C(n + 1) \leqslant 3 \cdot C(n)$ persists, it will make this probability less than 10^{-21} when $n = 32$.

Up to $n = 8$ the pictures in Fig. 23 exhibit one representative of each of the $c(n)$ equivalence classes. (Two arrays are equivalent under the dihedral group of the square if one can be transformed into the other by any combination of rigid rotations and reflections.)

V. Unsolved Problems

Is $C(n)$ asymptotic to some well-behaved function of n? In the following list of conjectures, proof or disproof of any of those marked OPEN would constitute significant progress on this question. (Of these, we believe question 5 may be the easiest to settle.)

−1. $C(n) \geqslant 1$ is true for infinitely many n. PROVED TRUE

0. $C(n) \geqslant 1$ is true for all $n \geqslant N$, for some positive integer N. OPEN

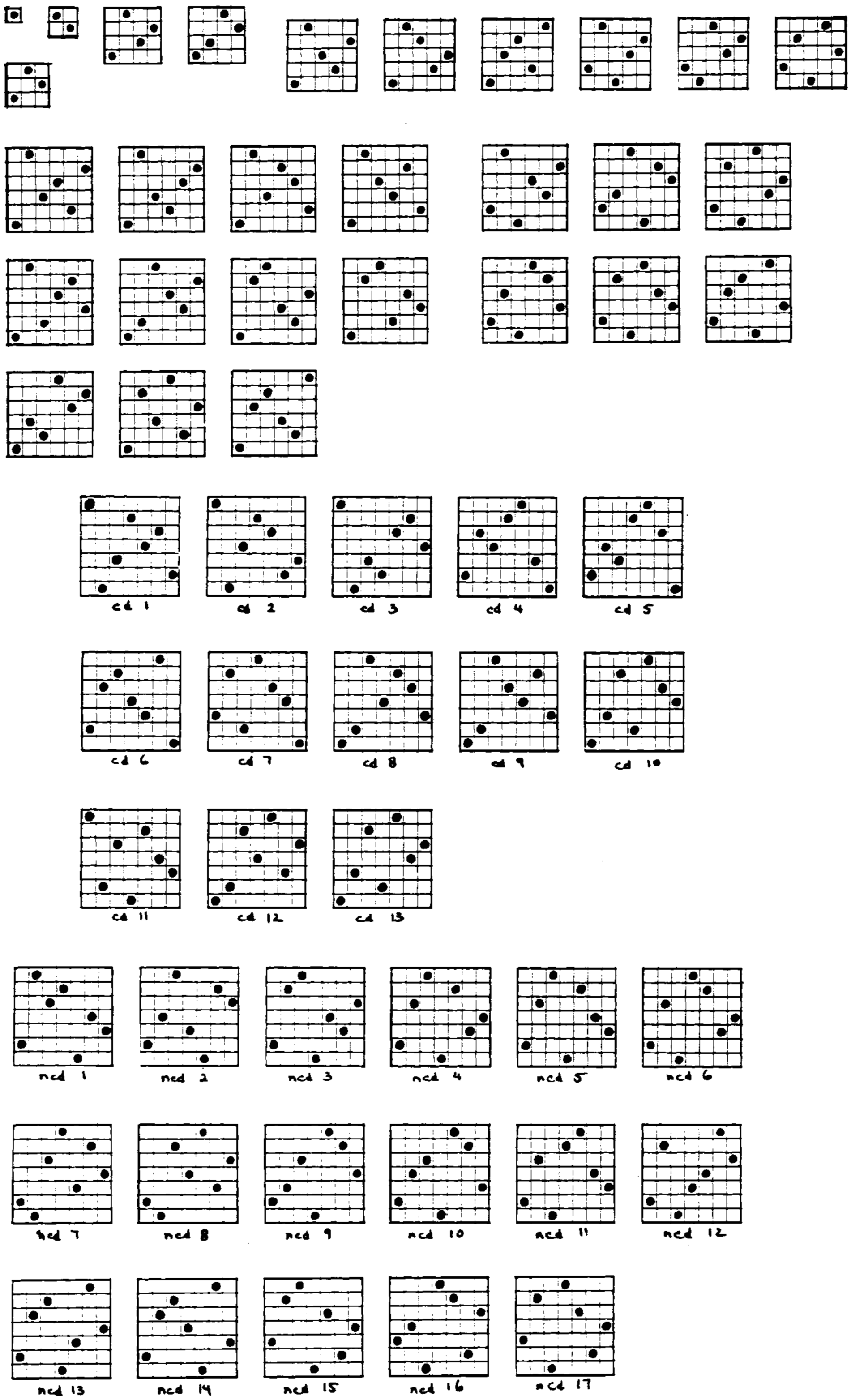


Fig. 23. Pictures of the Costas arrays from 1 × 1 to 8 × 8.

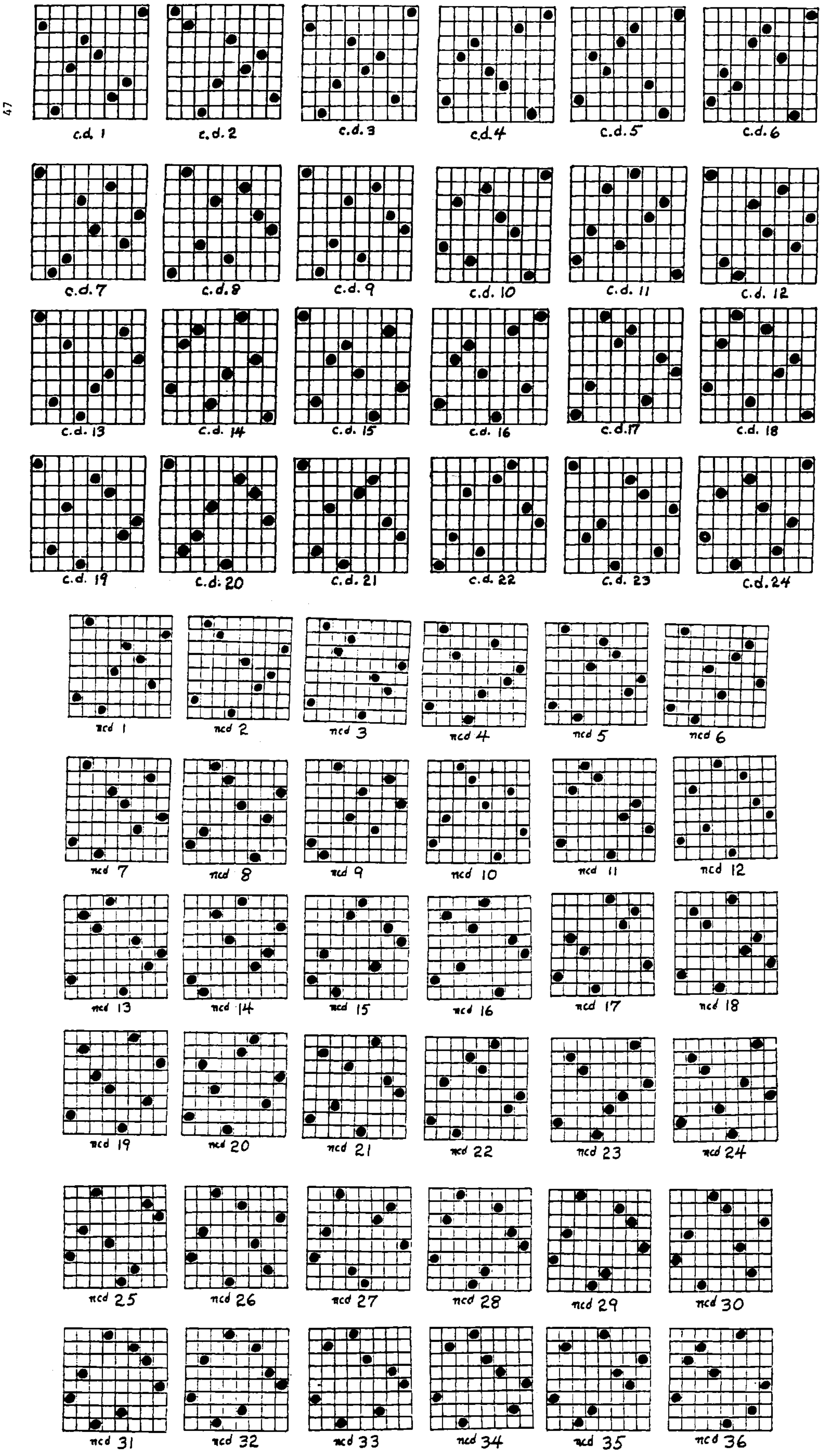


Fig. 23 (*continued*).

1. $C(n) \geqslant 1$ for all $n \geqslant 1$. OPEN
2. $C(n)$ is monotonic increasing. OPEN
3. $\limsup C(n) = \infty$. That is, $C(n)$ has an infinite subsequence which is unbounded above. PROVED TRUE
4. $C(n)/n!$ is monotonic decreasing. OPEN
5. $C(n)/n! \to 0$ as $n \to \infty$. OPEN
6. $C(n)/n!$ goes monotonically to 0 as $n \to \infty$. OPEN
7. $C(n)/c(n) \to 8$ as $n \to \infty$. OPEN

The next three are simply existence questions.

8. Do any other singly periodic Costas arrays exist besides the ones given by the Welch construction? (The conjectured answer to question 8 might have been YES before it turned out to be NO for $n \leqslant 16$, and NO for all odd n.)
9. Do honeycomb arrays exist for infinitely many n?
10. Do any $n \times n$ Costas arrays exist (for $n > 1$) which are configurations of nonattacking Queens?

For question 9 we conjecture YES, and for question 10, NOT SO SURE. Computer search by John Robbins has found that the answer for question 10 is NO for $11 \leqslant n \leqslant 17$.

Appendix I
Some Basic Polynomial Algebra Over Finite Fields

Lemma 1 (Fermat's "Little" Theorem)

For every element $a \in GF(q)$, $a^q = a$ in $GF(q)$.

Proof:

i) $0^q = 0$.

ii) The nonzero elements of $GF(q)$ form a group of order $q-1$ under multiplication. Hence $q^{q-1} = 1$ for all $a \neq 0$ in $GF(q)$.

Thus $a^q = a$ for all $a \in GF(q)$. ■

Lemma 2

Let $f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$ be a polynomial over $GF(q)$. (That is, $a_i \in GF(q)$ for $i = 0, 1, 2, \cdots, n$.) Then $\{f(x^{1/q})\}^q = f(x)$.

Proof: If there is a field $GF(q)$ of q elements, then $q = p^k$ for some prime p and some positive integer k, and the additive structure of $GF(q)$ is that of k-dimensional vectors modulo p. It is easily shown that the binomial coefficient $\binom{q}{r}$ satisfies $\binom{q}{r} \equiv 0 (\mathrm{mod}\, p)$ for all r, $1 \leqslant r \leqslant q-1$. Hence, over $GF(q)$, $(u+v)^q = u^q + v^q$.

Then $f(x)^q = (a_0x^n)^q + (a_1x^{n-1})^q + (a_2x^{n-2})^q + \cdots + (a_{n-1}x)^q + (a_n)^q = f(x^q)$ over $GF(q)$, where we have used $a_i^q = a_i$ from Lemma 1. From $f(x)^q = f(x^q)$, the result immediately follows. ■

Lemma 3

Let $f(x) = (x-\alpha)(x-\beta)$ be the factorization in $GF(q^2)$ of the quadratic polynomial $f(x) = x^2 + Ax + B$ which is irreducible over $GF(q)$. Then $\alpha = \beta^q$ and $\beta = \alpha^q$.

Proof: By Lemma 2, $f(x^q) = f(x)^q = (x-\alpha)^q(x-\beta)^q = (x^q - \alpha^q)(x^q - \beta^q)$. Thus $f(x) = f(x^{1/q})^q = (x - \alpha^q)(x - \beta^q)$, and the roots α^q, β^q of $f(x)$ must be the same (in some order) as α, β. But if $\alpha^q = \alpha$ (and $\beta^q = \beta$) then α (as well as β) is a root of $x^q - x = 0$, which, as an equation of degree q, has at most q roots in $GF(q^2)$. By Lemma 1, all q elements of $GF(q)$ are roots of $x^q - x = 0$, so that α (and β) are already in $GF(q)$, and $f(x)$ would factor over $GF(q)$ into linear factors $(x-\alpha)$ and $(x-\beta)$, contradicting the hypothesis that $f(x)$ is irreducible over $GF(q)$. Hence $\alpha^q = \beta$ and $\beta^q = \alpha$. ■

Theorem

If $f(x) = x^2 - x + g$ is an irreducible polynomial over $GF(q)$ whose roots are primitive elements of $GF(q^2)$, then g is a primitive element of $GF(q)$.

Proof: Write $f(x) = (x-\alpha)(x-\beta)$ with $\alpha, \beta \in GF(q^2)$. By Lemma 3, $\beta = \alpha^q$. Then $g = \alpha\beta = \alpha^{q+1}$. Let r be the smallest positive exponent such that $g^r = 1$. If $r < q-1$, then $r(q+1) < (q-1)(q+1) = q^2 - 1$, and we have $1 = g^r = \alpha^{r(q+1)}$, contradicting the assumption that α is a *primitive* element of $GF(q^2)$. ■

Corollary

The roots of $f(x) = x^2 - x - 1$ over $GF(q)$ fail to be primitive elements of $GF(q^2)$ unless either $q = 2$ or $q = 3$.

Proof: If $f(x)$ is *reducible* over $GF(q)$, its roots are *in* $GF(q)$, and cannot be primitive in $GF(q^2)$. If $f(x)$ is *irreducible* over $GF(q)$, then the *Theorem* applies, and -1 must be a primitive element of $GF(q)$. Since $(-1)^2 = 1$, we find $q - 1 \leqslant 2$, so that $q \leqslant 3$. Thus $GF(2)$ and $GF(3)$ are the only candidates. It turns out that $f(x) = x^2 - x - 1$ *is* primitive over $GF(2)$ and over $GF(3)$. ■

Exercises

1) Let $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$ be the factorization, in $GF(q^k)$, of the polynomial $f(x)$ which is irreducible of degree k over $GF(q)$. Then the set of roots, $\{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_k\}$, is the same set as $\{\alpha_1, \alpha_1^q, \alpha_1^{q^2}, \cdots, \alpha_1^{q^{k-1}}\}$.

2) Suppose $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$ is an irreducible polynomial of degree k over $GF(q)$. Show that all the roots $\alpha_1, \alpha_2, \cdots, \alpha_k$ have the same primitivity t, as elements of $GF(q^k)$. That is, $\alpha_i^t = 1$ for $i = 1, 2, \cdots, k$, while $\alpha_i^s \neq 1$ for $1 \leqslant s < t$. Moreover, t is an integer factor of $q^k - 1$, and is *not* an integer factor of $q^m - 1$, for any $m \in \{1, 2, \cdots, k-1\}$.

Appendix II
Algebraic Exclusions and Terminal Cases

A. Conditions which Prevent Adding a Corner Dot to a Golomb Construction

Adding a dot at $(0,0)$ or $(0, q-1)$ or $(q-1, 0)$ or $(q-1, q-1)$ is prevented if and only if the G_2 constructions contain dots at (a,b), (x,y), and $(a+x, b+y)$. In this case, a dot cannot be added in the same quadrant as the midpoint between (a,b) and (x,y).

When $\alpha^a + \beta^b = 1$ and $\alpha^x + \beta^y = 1$, we have $\alpha^{a+x} + \beta^{b+y} + \alpha^a\beta^y + \alpha^x\beta^b = 0$ and $\alpha^{a-x} + \beta^{b-y} = 0$.

Let k be the number (coprime to $q-1$) such that $\beta = \alpha^k$. Then we have $\alpha^{a-x} = \alpha^{(q-1)/2 + k(b-y)}$, which holds if and only if $(q-1)/2 = (kb - a) - (ky - x)$.

These conditions give us the following tests:

TEST$(0,0)$: A dot cannot be added at $(0,0)$ if and only if there exist dots (x,y) and (a,b) in G_2 such that:
1) $(q-1)/2=(kb-a)-(ky-x)$
2) $a+x<q-1$
3) $b+y<q-1$.

TEST$(0,q-1)$: A dot cannot be added at $(0,q-1)$ if and only if there exist dots (x,y) and (a,b) in G_2 such that:
1) $(q-1)/2=(kb-a)-(ky-x)$
2) $a+x<q-1$
3) $b+y>q-1$.

TEST$(q-1,0)$: A dot cannot be added at $(q-1,0)$ if and onyy if there exist dots (x,y) and (a,b) in G_2 such that:
1) $(q-1)/2=(kb-a)-(ky-x)$
2) $a+x>q-1$
3) $b+y<q-1$.

TEST$(q-1,q-1)$: A dot cannot be added at $(q-1,q-1)$ if and only if there exist dots (x,y) and (a,b) in G_2 such that:
1) $(q-1)/2=(kb-a)-(ky-x)$
2) $a+x>q-1$
3) $b+y>q-1$.

B.1) T_1 never works for $q=2^k>4$.

Proof: Whenever $\alpha^i+\beta^j=1$, the simplified binomial theorem over $GF(2^k)$ tells us that $\alpha^{2i}+\beta^{2j}=1$. Having dots at (i,j) and $(2i,2j)$ prevents adding a corner dot in the quadrant that contains (i,j). For $n=6$ all the G_2 constructions have dots in all four quadrants by inspection. For $n=2m>6$, having dots in all quadrants is a property of all $n\times n$ Costas arrays, as a consequence of the fact that for $m>3$ any two $m\times m$ Costas arrays must have a difference in common. (This fact is proved in [11].) ■

B.2) T_0 never works when $q=3^k$.

Proof: There will be a dot at the exact center of the $(q-2)\times(q-2)$ array because $\alpha^{(q-1)/2}=\beta^{(q-1)/2}=-1$, and in $GF(3^k)$, $(-1)+(-1)=1$. Therefore, we cannot add dots at both $(0,0)$ and $(q-1,q-1)$, nor at both $(0,q-1)$ and $(q-1,0)$. ■

B.3) T_0 never works when $q\equiv 1(\text{mod}\,6)$.

Proof: Let us write $q=6m+1$, and let α and β be primitive in $GF(q)$. We have $\alpha^{3m}=\beta^{3m}=\alpha^{-3m}=\beta^{-3m}=-1$, while $\alpha^m\neq-1\neq\beta^m$. We see that $\alpha^m,\alpha^{-m},\beta^m,\beta^{-m}$ are all primitive sixth roots of unity; that is, roots of $x^2-x+1=0$. Therefore, either $\alpha^m+\beta^m=1$ and $\alpha^{-m}+\beta^{-m}=1$, or else $\alpha^m+\beta^{-m}=1$ and $\alpha^{-m}+\beta^m=1$. (The two distinct primitive sixth roots of unity sum to 1.) In either case, we cannot add dots at both $(0,0)$ and $(q-1,q-1)$, nor at both $(0,q-1)$ and $(q-1,0)$. ■

Corollary to B.3)

The proof of B.3) shows that the G_2 construction will not yield a honeycomb array when $q\equiv 1(\text{mod}\,6)$.

B.4) A G_2 construction will never contain two diagonally opposite corner dots, if $q>7$.

Proof: If $\alpha^1+\beta^1=1$ and $\alpha^{-1}+\beta^{-1}=1$, then $\alpha^{-1}+1/(1-\alpha)=1$, and $\alpha^2-\alpha+1=0$. If $\alpha^1+\gamma^{-1}=1$ and $\alpha^{-1}+\gamma^1=1$ we can take $\beta=\gamma^{-1}$ and again we find $\alpha^2-\alpha+1=0$. Thus in either case α is a root of $\alpha^6-1=0$. With α primitive in $GF(q)$ and $\alpha^6=1$ we conclude that $GF(q)$ has at most 7 elements. ■

B.5) If a G_2 construction over $GF(q)$ has dots at $(1,3)$, $(3,1)$, and $(2,-1)$, then $q=8$.

Proof: Starting with $\alpha^3+\beta=1$ and $\alpha^2+\beta^{-1}=1$, we have $\beta\cdot\beta^{-1}=1=(1-\alpha^2)(1-\alpha^3)=1-\alpha^2-\alpha^3+\alpha^5$. Thus $\alpha^3=\alpha+1$, whence $\alpha+\beta=0$. Now using $\alpha+\beta^3=1$, $\alpha^3+\beta=1$, and $\alpha=-\beta$ we deduce that $-1=1$, which means that $q=2^k$ and $\alpha=\beta$. When α is primitive in $GF(q)=GF(2^k)$, $\alpha^3=\alpha+1$ implies that $\alpha^7=1$, and $q=8$. ■

B.6) If a G_2 construction has dots at $(1,1)$, $(2,3)$, and $(3,2)$, over $GF(q)$, then $q=5$.

Proof: With $\alpha+\beta=1$ and $\alpha^2+\beta^3=1$, we have $(1-\beta)^2+\beta^3=1=1-2\beta+\beta^2+\beta^3$, and therefore $\beta^2+\beta-2=0=(\beta-1)(\beta+2)$. Since β is primitive, $\beta\neq1$, so that $\beta=-2$ and $\alpha=3$. At this point we have also gained the information that q must be prime, because one of its primitive roots is an integer.

Now using $\alpha^3+\beta^2=1$ we find that $\alpha=-2$ and $\beta=3$, so $-2=3$. Thus $5=0$ in $GF(q)$, and we conclude that $q=5$. ■

B.7) If a G_2 construction has dots at $(1,2)$, $(2,3)$, and $(3,1)$ over $GF(q)$, then $q=5$.

Proof: With $\alpha+\beta^2=1$ and $\alpha^2+\beta^3=1$ we have $\beta^3-\beta^2=\alpha-\alpha^2$ and $\beta^2=1-\alpha$. Then $\beta^2(\beta-1)=\alpha(1-\alpha)=\alpha\beta^2$, and therefore $\beta-1=\alpha$. This tells us that $\alpha^2=-1$, so $\alpha^4=1$, and hence $q=5$. ■

B.8) For $q>9$, T_4 never works unless q is a prime whose last digit is 1 or 9.

Proof: Suppose $q=p^k$ with $k\geqslant2$, and suppose $\alpha^2+\alpha=1$ where α is primitive in $GF(p^k)$. Under these conditions $\alpha^p\neq\alpha$.

Using the simplified binomial theorem, we have $(\alpha^2+\alpha)^p=1^p=1=(\alpha^p)^2+\alpha^p$. Thus α and α^p are the two roots of the quadratic $x^2+x-1=(x-\alpha)(x-\alpha^p)=x^2-(\alpha+\alpha^p)x+\alpha^{p+1}$. We conclude that $\alpha^{p+1}=-1$.

In the special case $p=2$ this can only happen when $k=2$, so that $q=4$.

For an odd prime p, $\alpha^{p+1}=-1$ implies that $(p^k-1)/2=p+1$, which is only possible when $k=2$ and $p=3$, that is, when $q=9$.

For $q>9$ we know that T_4 cannot work with $k\geqslant2$ because α cannot then be primitive. We shall see that in some prime fields, T_4 is prevented by the nonexistence of α.

The quadratic formula tells us that for prime $p>2$, $x^2+x-1=0$ has a solution

$$x=\frac{-1\pm\sqrt{5}}{2}$$

in $GF(p)$ if and only if $y^2=5$ has a solution y in $GF(p)$. According to the Law of Quadratic Reciprocity, 5 is a quadratic residue of $p>2$ if and only if p is a quadratic residue of 5. Thus except for $p=5$, solutions to $y^2=5$ exist in $GF(p)$ if and only if $p\equiv1(\text{mod}\,5)$ or $p\equiv4(\text{mod}\,5)$; that is, the last digit of p is either 1 or 9. ■

Comment

Checking whether T_4 works is made easier by B.8). When p is a prime ending in 1 or 9 we will find y in $GF(p)$ such that $y^2 = 5$ by looking in the log table. Then let $\alpha = (1 + y)/2$ and $\gamma = (-1 - y)/2$ so that $\alpha^2 + \alpha = 1$ and $\gamma^2 + \gamma = 1$. To see if T_4 works it remains only to check whether one or both of α and γ is primitive.

B.9) G_5^* and G_4^* work if and only if T_4 works and $q \equiv 1 (\mathrm{mod}\, 4)$.

Proof: G_5^* and G_4^* work if and only if there exist primitive elements α, β in $GF(q)$ such that $\alpha + \beta = 1$ and $\alpha^2 + \beta^{-1} = 1$.

Given such α, β we deduce that $\beta^{-1}\beta = (1 - \alpha^2)(1 - \alpha) = 1 - \alpha^2 - \alpha + \alpha^3 = 1$, and hence that $\alpha^2 = \alpha + 1$, $\alpha = -\beta^{-1}$, and $\alpha^{-2} + \alpha^{-1} = 1$. The primitivity of α^{-1} tells us that T_4 works. The primitivity of both β^{-1} and $-\beta^{-1}$ tells us that $q \equiv 1 (\mathrm{mod}\, 4)$.

Conversely, assuming T_4 works and $q \equiv 1 (\mathrm{mod}\, 4)$, we have primitive γ such that $\gamma^2 + \gamma = 1$. Also, γ^{-1} primitive and $q \equiv 1 (\mathrm{mod}\, 4)$ implies that $-\gamma$ is primitive. Thus taking $\alpha = -\gamma$ and $\beta = \gamma^{-1}$ we have primitive α, β such that $\alpha^2 + \beta^{-1} = 1$ and $\alpha + \beta = 1$. ■

References

[1] J. P. Costas, "Medium constraints on sonar design and performance," in *FASCON Conv. Rec.*, pp. 68A–68L, 1975.

[2] S. W. Golomb and H. Taylor, "Two-dimensional synchronization patterns for minimum ambiguity," *IEEE Trans. Inform. Theory*, vol. IT-28, no. 4, pp. 600–604, July 1982.

[3] S. W. Golomb, "Algebraic constructions for Costas arrays," *J. Combinatorial Theory*, ser. A, vol. 37, no. 1, July 1984.

[4] O. Moreno, "On primitive quadratics of trace 1 over $GF(2^m)$," in preparation.

[5] M. Szalay, "On the distribution of primitive roots of a prime," *J. Number Theory*, vol. 7, no. 2, pp. 184–188, May 1975.

[6] O. Moreno, "On primitive elements of trace equal to 1 in $GF(2^m)$," *Discrete Math.*, vol. 41, pp. 53–56, 1982.

[7] M. Szalay, "On the distribution of primitive roots mod p" (in Hungarian), *Mat. Lapok*, vol. 21, pp. 357–362, 1970.

[8] E. Vegh, "A note on the distribution of the primitive roots of a prime," *J. Number Theory*, vol. 3, pp. 13–18, 1971.

[9] J. Johnson, "On the distribution of powers in finite fields," *J. Reine Angew. Math.*, vol. 251, pp. 10–19 (*Crelles J.*), 1971.

[10] H. Davenport, "On the distribution of the l-th power residues mod p," *J. London Math. Soc.*, vol. 7, pp. 117–121, 1932.

[11] H. Taylor, "Non-attacking Rooks with distinct differences," EE Systems, Univ. of Southern Calif., Tech. Rep. CSI-84-03-2.

[12] B. T. Bennett and R. B. Potts, "Arrays and brooks," *J. Australian Math. Soc.*, vol. 7, pp. 23–31, 1967.

[13] Lt. Col. A. Cunningham, "On quasi-Mersennian numbers," *Messenger of Math.*, vol. XLI, no. 41, pp. 119–146, 1912.

[14] S. W. Golomb and L. R. Welch, "Perfect codes in the Lee metric and the packing of polyominoes," *SIAM J. Appl. Math.*, vol. 18, no. 2, pp. 302–317, Jan. 1970.

[15] N. J. A. Sloane, *A Handbook of Integer Sequences.* New York, London: Academic Press, 1973.

[16] M. J. Sites, "Coded frequency shift keyed sequences with applications to low data rate communication and radar," Radioscience Lab., Stanford Electronics Lab., Tech. Rep. 3606-5, Sept. 1969.

[17] J. P. Costas, "Project Medior—A medium-oriented approach to sonar signal processing," HMED Tech. Publ. R66EMH12, General Electric Co., Syracuse, NY, Jan. 1966.