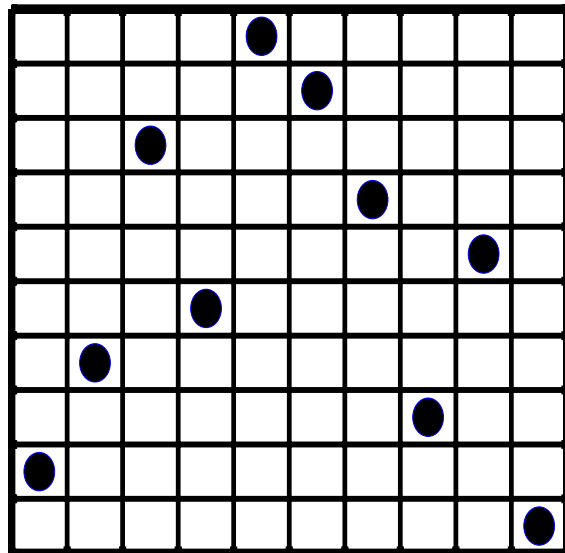


Open Problems in Costas Arrays

In the 1960's, Dr. John P. Costas began searching for permutation matrices with ideal auto-ambiguity properties. By hand, he found examples of such matrices of size up to $N = 12$. Unable to find one of size 13, he contacted



Professor Solomon Golomb who then provided generation techniques based on the theory of finite fields for creating these matrices, dubbed *Costas arrays*. The generation methods produce Costas arrays for infinitely many N , but not all N . For example, the techniques can be used to generate arrays for all $N \leq 31$, but no Costas array of size $N = 32$ or $N = 33$ has been found. Computer search has enumerated all Costas arrays of size $N \leq 26$, but the exponential

growth of the search space prohibits extending these results much further with current computational capabilities. After nearly 40 years of research, the first question concerning Costas arrays remains open:

Do Costas arrays exist for all N ?

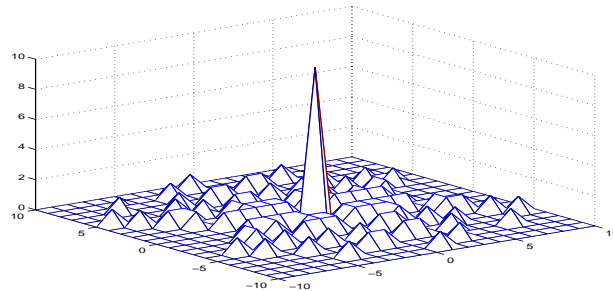
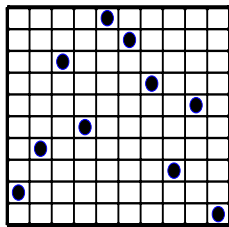
Open Problems in Costas Arrays

Scott Rickard
Claude Shannon Institute
University College Dublin

- Motivation & History
- Constructions & Enumeration Results
- Open Problems

John P. Costas

- famous for the invention of the Costas Loop (1950's)
- help solve mystery concerning poor performance of sonar system (1960's)
 - rapidly time-varying channel made coherent processing inappropriate
- designed frequency-hopped waveforms and hybrid receiver to fix problem
 - one frequency pulse per time for noise limited case
 - all frequencies used for clutter limited case
 - ideal thumbtack auto-ambiguity



[Costas84] J. P. Costas, **A Study of a Class of Detection Waveforms Having Nearly Ideal Range-Doppler Ambiguity Properties**, Proc. IEEE, vol. 72, no. 8, pp. 996-1009, Aug. 1984.



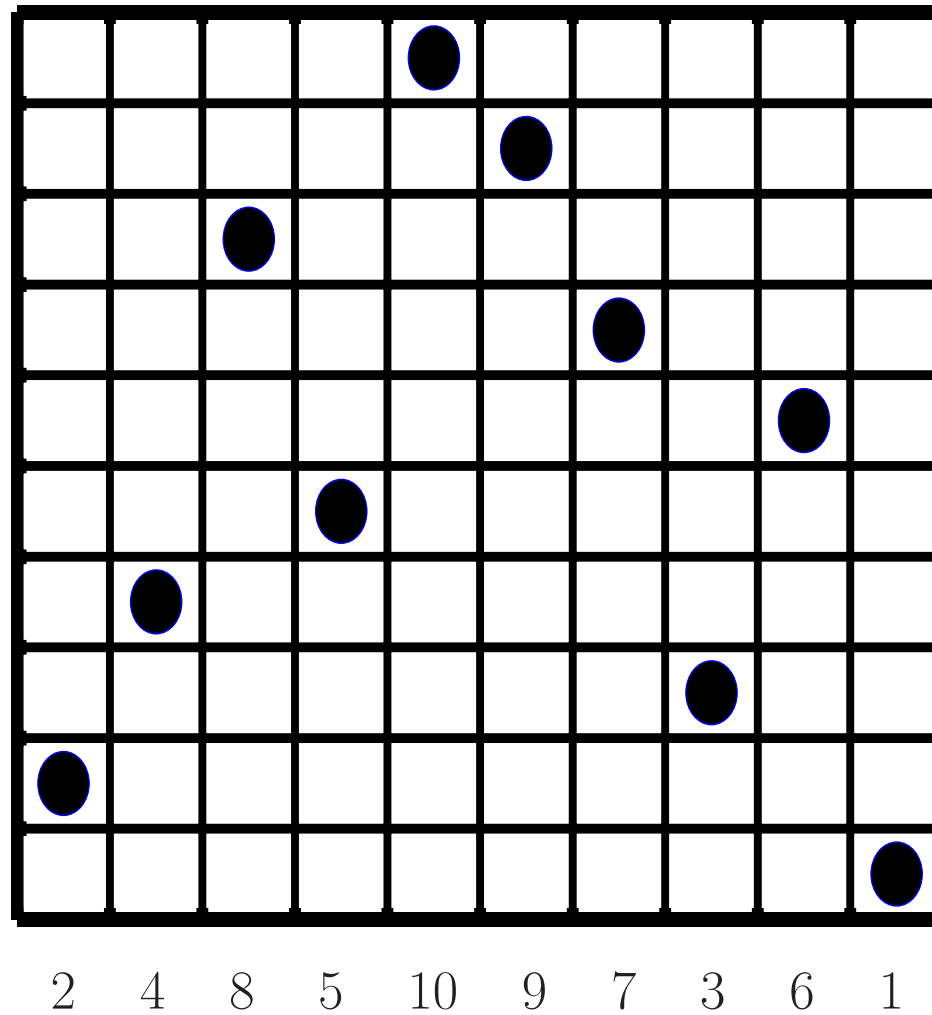
John P. Costas

- born in Wabash Indiana in 1923
- Purdue undergrad
- RADAR engineering in WWII
- MIT graduate student of N. Wiener



Figure 1: Costas in January 2006.

An example 10-by-10 Costas array



Costas Array - Equivalent Definitions

Definition 1. A permutation matrix \mathbf{A} with auto-correlation function taking values N , 1 , and 0 .

Definition 2. An ordering $\{a_1, a_2, \dots, a_N\}$ of the elements of the set $\{1, 2, \dots, N\}$ such that the difference triangle contains no repeated values on any given row. The j th row of the difference triangle contains the differences $a_{i+j} - a_i$ for all $i = 1, \dots, N - j$.

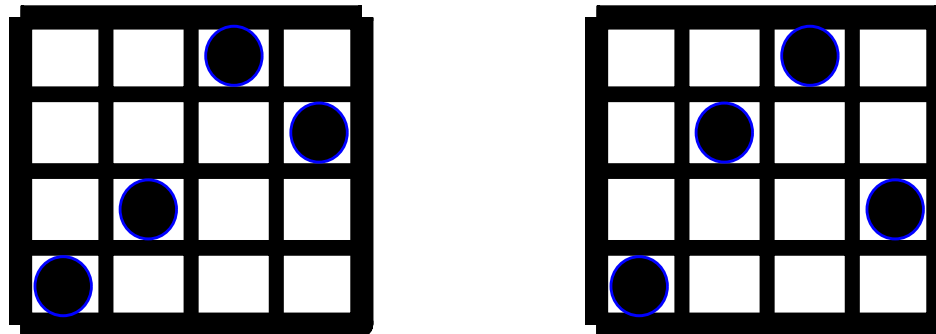
Definition 3. An N -by- N array of dots and blanks which satisfies:

1. There are N dots, one in each row and one in each column.
2. The $\binom{N}{2}$ line segments between pairs of dots differ in length or slope.

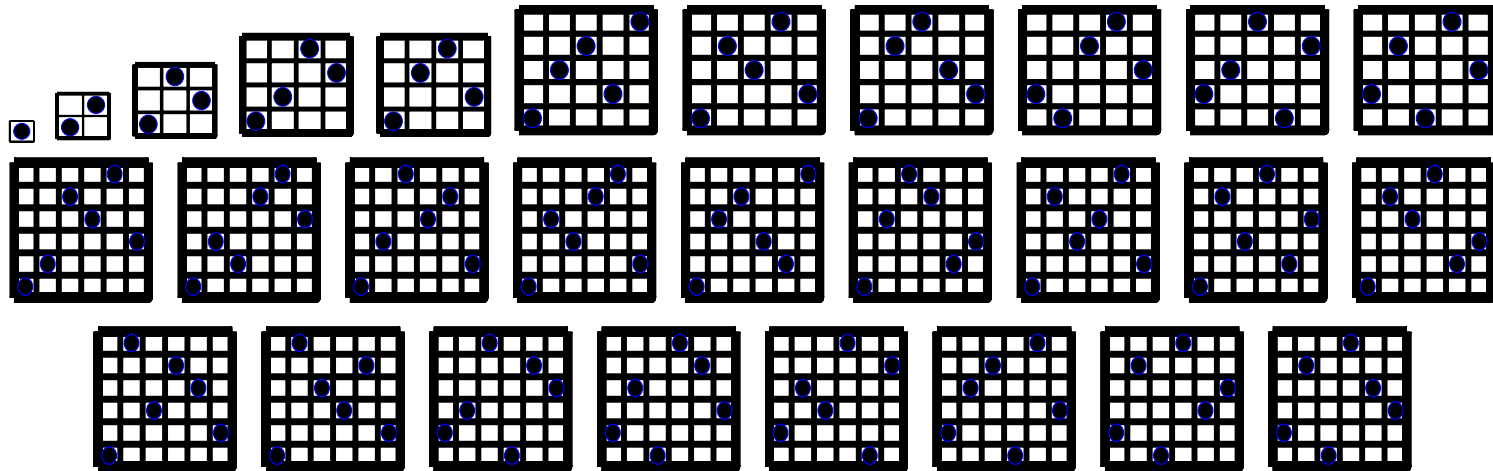
Definition 4. A permutation matrix \mathbf{A} such that if four distinct entries in the matrix $a_{i_1, j_1} = a_{i_2, j_2} = a_{i_3, j_3} = a_{i_4, j_4} = 1$, then $(i_2 - i_1, j_2 - j_1) \neq (i_4 - i_3, j_4 - j_3)$ and if three distinct entries in the matrix $a_{i_1, j_1} = a_{i_2, j_2} = a_{i_3, j_3} = 1$, then $(i_2 - i_1, j_2 - j_1) \neq (i_3 - i_1, j_3 - j_1)$.

Rotations and Reflections

- Each Costas array generates a family (dihedral equivalence class) of 4 or 8 Costas arrays. It is 4 if the array is symmetric across a diagonal.
- $c(N)$ denotes the number of families of Costas arrays of size N
- $C(N) = 8 \cdot c(N) - 4 \cdot s(N)$, where $s(N)$ is the number of families of diagonally symmetric Costas arrays of size N



Golomb's Initial Conjectures



Let $C(N)$ denote the number of N -by- N Costas arrays.

Conjecture 1. $C(N) \geq 1$ for all N .

Conjecture 2. $C(N)$ is monotonic increasing with N .

[Golomb84] S. W. Golomb and H. Taylor, **Constructions and Properties of Costas Arrays**, Proc. IEEE, vol. 72, no. 9, pp. 1143-1163, Sept. 1984.

Finite Field Review

- Golomb in 1984 “*All known systematic constructions for Costas Arrays involve the use of primitive elements in finite fields.*”
- A finite field with q elements, $GF(q)$, exists iff $q = p^m$, where p is prime.
- For example, $GF(11) = \mathbb{Z}_{11}$, the integers modulo 11 under $(+, \cdot)$.
- \exists at least one $\alpha \in GF(q)$ such that $\{\alpha^1, \alpha^2, \dots, \alpha^{q-1}\}$ runs through all non-zero elements of $GF(q)$. Such α are called primitive elements.
- $\alpha^x = \alpha^y$ in $GF(q)$ iff $x \equiv y \pmod{q-1}$.
- $\exists \phi(q-1)$ distinct primitive elements in $GF(q)$. $\phi(x)$ is Euler's totient function, the number of integers less than x relatively prime to x .
- When $m > 1$, $GF(p^m)$ is not \mathbb{Z}_{p^m} .
- There is (essentially) just one field of order q .

Welch Costas

Definition [Welch construction]

Given prime p and primitive element α , $\{\alpha^1, \alpha^2, \dots, \alpha^{p-1}\}$ is a length $N = p - 1$ Costas sequence.

- 2 is primitive in $GF(11)$. Therefore, $\{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}\} = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ is a Costas array.
- Circular shifts of Welch Costas arrays are still Costas arrays (singly periodic). For example, $2\ 4\ 3\ 1 \rightarrow 4\ 3\ 1\ 2 \rightarrow 3\ 1\ 2\ 4 \rightarrow 1\ 2\ 4\ 3$
- Construction with circular shifts: *exponential Welch construction*.
- The diagonal reflection: *log Welch sequence*.
- $2(p - 1)\phi(p - 1)$ arrays are produced of size $N = p - 1$.

Golomb Costas

Definition [Golomb construction]

Given prime power $q = p^m$ and primitive elements $\alpha, \beta \in GF(q)$, $\{\log_\beta(1 - \alpha^1), \log_\beta(1 - \alpha^2), \dots, \log_\beta(1 - \alpha^{q-2})\}$ is a length $q - 2$ Costas sequence.

- If $\beta^i = x$, then $\log_\beta x = i$.
- Sample construction ($q = 11, \alpha = \beta = 2$):
 $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6$
 $\log_2\{1 - 2^1, 1 - 2^2, 1 - 2^3, 1 - 2^4, 1 - 2^5, 1 - 2^6, 1 - 2^7, 1 - 2^8, 1 - 2^9\} =$
 $\log_2\{10, 8, 4, 7, 2, 3, 5, 9, 6\} = \{5, 3, 2, 7, 1, 8, 4, 6, 9\}$
- In other words, the $(q - 2)$ -by- $(q - 2)$ permutation matrix A with $a_{ij} = 1$ iff $\alpha^i + \beta^j = 1$ is a Costas array.
- When $\alpha = \beta$, the construction is due to Lempel and the generated matrix is symmetric.
- $\frac{(\phi(p^m - 1))^2}{m}$ arrays are produced of size $N = p^m - 2$.

Costas by Construction

W_1 is the Welch construction, G_2 is the Golomb construction.

N	S	W_0	W_1	W_2	W_3	T_0	T_1	G_2	G_3	G_4	G_4^*	T_4	G_5^*
25	?	G_2
26	?	.	.	.	W_3	.	.	.	G_3
27	?	.	.	W_2	.	.	.	G_2	.	.	.	T_4	.
28	?	.	W_1	.	.	.	T_1	.	G_3	G_4	.	.	.
29	?	.	.	W_2	.	T_0	.	G_2	G_3
30	?	.	W_1	G_2
31	?	W_0
32	?
33	?
34	?	G_3
35	?	.	.	W_2	.	.	.	G_2
36	?	.	W_1	G_5^*
37	?	G_4^*	T_4	.

Note W_1, W_2, G_2, G_3 are the only guarantees.

Gaps at $N = 32, 33, 43, 48, 49, 54, 63, 73, 74, 83-85, 89-93, 97, \dots$

Enumeration Results

N	$C(N)$	N	$C(N)$
1	1	14	17252
2	2	15	19612
3	4	16	21104
4	12	17	18276
5	40	18	15096
6	116	19	10240
7	200	20	6464
8	444	21	3536
9	760	22	2052
10	2160	23	872
11	4368	24	200
12	7852	25	88
13	12828	26	56

- $N \leq 12$ [Costas84] J. P. Costas, A Study of a Class of Detection Waveforms Having Nearly Ideal Range-Doppler Ambiguity Properties, Proc. IEEE, vol. 72, no. 8, pp. 996-1009, Aug. 1984.
- $N \leq 17$ [Silverman88] J. Silverman, V. Vickers, J. Moody, On the Number of Costas Arrays as a Function of Array Size, Proceedings of the IEEE, 76:7, pp. 851-853, 1988.
- $N \leq 23$ [Moreno02] O. Moreno, J. Ramirez, E. Orozco, D. Bollman, Faster Backtracking Algorithms for the Generation of Symmetry-Invariant Permutations, Journal of Applied Mathematics, 2:6, pp. 277-287, 2002.
- $N \leq 25$ [Beard04] J. Beard, J. Russo, K. Erickson, M. Monteleone, M. Wright, Combinatoric collaboration on Costas arrays and radar applications, IEEE Radar Conference, Philadelphia, PA, USA, April 2004.
- $N = 26$ done in 3 months on 120 machines (30 years of CPU time) [Rickard06] S. Rickard et. al., CISS, 2006. (Also, [Beard06] J. Beard et al., IEEE Trans. Aero. Elec. Sys., 2006.)
- Many note exponential growth with factor 5 in search time from N to $N + 1$.

The 26-by-26 arrays

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

Table 1: The 26-by-26 Costas arrays.

- Grid search
 - 113,729 jobs (minimal starting positions - 4 deep)
 - 120 machines of mixed ability (some 5+ years old)
 - 930,959,944 seconds (or 29.52 years) of single CPU time
- Three of the arrays (those beginning with (2 18 ...), (3 9 ...), and (5 3 ...)) are 27-by-27 Golomb arrays with the corner dot removed.
- One of the arrays, (2 6 ...), is a 28-by-28 Welch array with the leading (1 2) corner array removed. This array is also two different 28-by-28 Welch arrays with the leading (2 1) corner array removed, and is a 28-by-28 Welch array with the leading (1 28) removed.
- The array starting with (1 18 ...) is a 25-by-25 Golomb array with a corner dot added.
- This leaves 3 arrays that are not ‘explained’ by the generation techniques.

$N = 32$, the holy grail

- [Golomb84] “...we have no actual proof that $C(32)$ is not zero...”
- [Silverman88] “Observing that the first gaps in the list of known constructions occur at $n = 32$ and $n = 33$, we challenge the reader to find a Costas array for either of these n .”
- [Brown93] C. Brown, M. Cenkli, R. Games, J. Rushanan, O. Moreno, P. Pei, **New Enumeration Results for Costas Arrays**, IEEE Int. Symp. on Information Theory, p. 405, Jan. 1993. “Our aim was to discover a 32×32 Costas array or gather new evidence for its possible nonexistence.”
- [Moreno95] O. Moreno, P. Pei, J. Ramirez, **A parallel algorithm for the enumeration of Costas sequences**, Proc. SIAM Conf. on Parallel Proc. for Sci. Comp., pp. 255-260, Feb. 1995. “Thus we estimated 20 million years to find solutions for size 32.”
- [Huang86] Huang Lou-sheng, **Constructions for Costas Arrays**, The Journal of the Fujian Teachers University (Natural Science), 2(1):17-22, 1986. “all the constructions of $n \times n$ Costas Arrays, when $n \leq 130$, have been solved.” FALSE!

Open Problem: Existence

Problem 1 (Golomb 84). *Do Costas arrays exist for all N ?*

$$C(N) \geq 0 \quad \forall N \quad (1)$$

Problem 2 (Golomb 84). *Do Costas arrays exist for $N = 32$?*

$$C(32) \geq 0 \quad (2)$$

Problem 3. *Are there other construction techniques besides Welch and Golomb?*

Problem 4. *Are there arbitrarily large ‘sporadic’ arrays (ie, arrays not produced by generation techniques or extensions)? If not, what is the largest sporadic array?*

Open Problem: Forbidden Positions

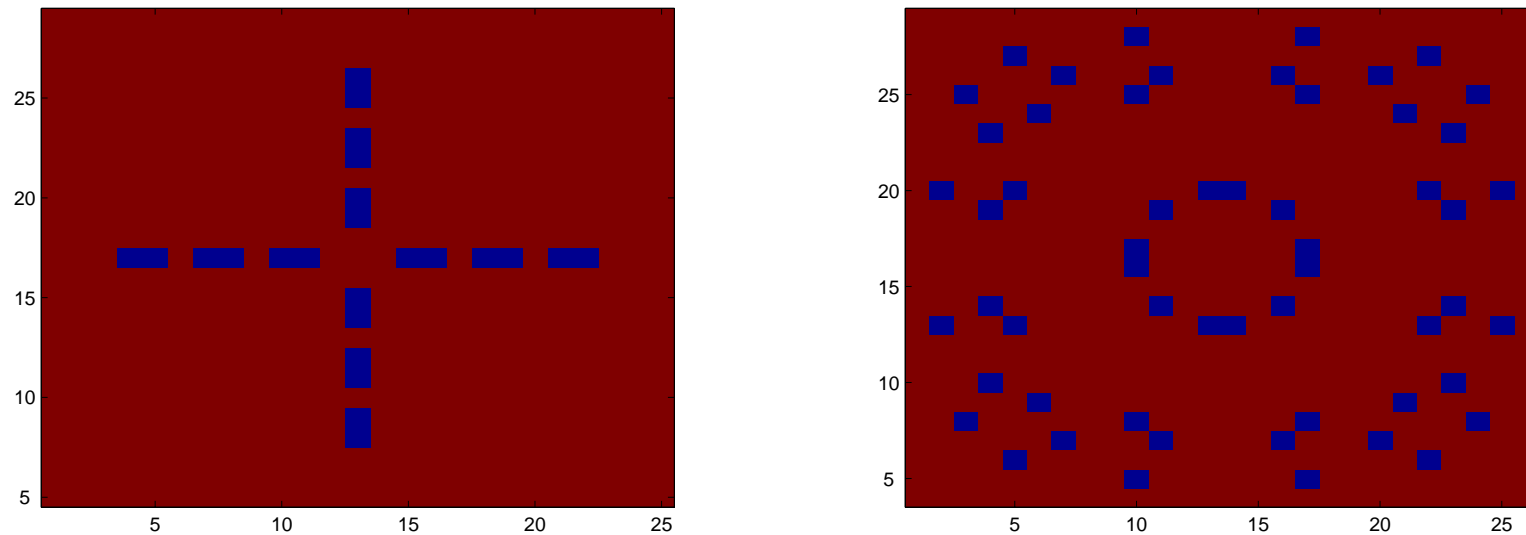


Figure 2: Blue squares are the positions in a 25-by-25 (left) and 26-by-26 (right) array where no Costas array has a dot.

Problem 5 (Rickard 06). *There exist forbidden positions – locations in the matrix where no Costas arrays of a given size has a dot. For example, none of the 3-by-3 Costas arrays has a dot in the middle. The next examples occur for $N = 25$ and $N = 26$. Is it possible to prove that forbidden positions must exist for larger N ?*

Open Problem: Couples

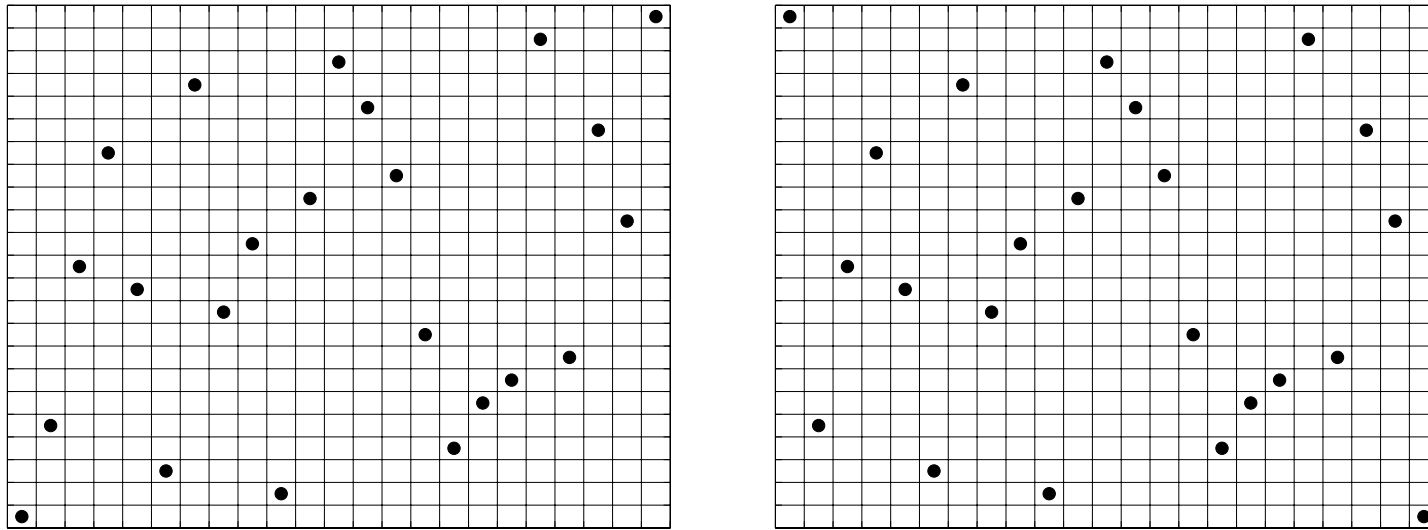


Figure 3: 23-by-23 Costas array pairing related by swapping first and last columns, both of which contain corner dots.

Problem 6 (Rickard 06). *We call two arrays a couple if one array is transformed into the other by swapping two elements. One notable example is the pictured pair of size 23 because it is the corner dots that are swapped and because both arrays are also symmetric. Is there a construction technique for Costas couples?*

Open Problem: Cross-correlation Golomb

prime	# codes	max hits	prime	# codes	max hits
5	4	2	41	256	19
7	4	2	43	144	13
11	16	4	47	484	8
13	16	5	53	576	25
17	64	7	59	784	12
19	36	6	61	256	29
23	100	6	67	400	21
29	144	13	71	576	13
31	64	9	73	576	35
37	144	17	79	576	25

Table 2: Golomb-Costas number of codes and maximum number of cross hits.

Problem 7 (Rickard 93). *Establish the worst-case number of cross-correlation hits for the set of Golomb-Costas arrays (Conjecture: $\frac{p-3}{2}$).*

Problem 8 (Rickard 93). *Prove the best cross-correlation properties of Golomb-Costas array sets occur when the sets are generated over primes of the form $2p + 1$, where p is prime.*

Open Problem: Cross-correlation

prime	# codes	max hits	prime	# codes	max hits
5	2,4	2,2	97	32	48
7	2,4	2,2	101	40	50
11	4,16	3,4	103	32	34
13	4,16	6,5	107	52	5
17	8,64	8,7	109	36	54
19	6,36	6,6	113	48	56
23	10,100	4,6	127	36	42
29	12,144	14,13	131	48	26
31	8,64	10,9	137	64	68
37	12,144	18,17	139	44	46
41	16,256	20,19	149	72	74
43	12,144	14,13	151	40	50
47	22,484	5,8	157	48	78
53	24,576	26,25	163	54	54
59	28,784	5,12	167	82	6
61	16,256	30,29	173	84	86
67	20,400	22,21	179	88	6
71	24,576	14,13	181	48	90
73	24,576	36,35	191	72	38
79	24,576	26,25	193	64	96
83	40,1600	5,?	197	84	98
89	40,1600	44,?	199	60	66

Table 3: Welch number of codes and maximum number of cross hits (Golomb for $p < 80$).

Problem 9 (Rickard 93). *Prove the best cross-correlation properties of Welch-Costas array sets occur when the sets are generated over primes of the form $2p + 1$, where p is prime.*

Problem 10 (Rickard 93). *Prove the maximum number of cross-correlation hits for a set of Golomb-Costas arrays is one less than the maximum number of cross-correlation hits for a set of Welch-Costas arrays generated over the same prime (not 19 or of the form $2p + 1$ where p is prime).*

Conclusions

- Costas arrays are ugly and beautiful
- Goal: fill gaps in table of known Costas arrays (32,33,43,...)
- Goal: Enumeration beyond 26
- Goal: Proof strange connection between Welch and Golomb worst case cross correlation
- Now online: www.costasarrays.org