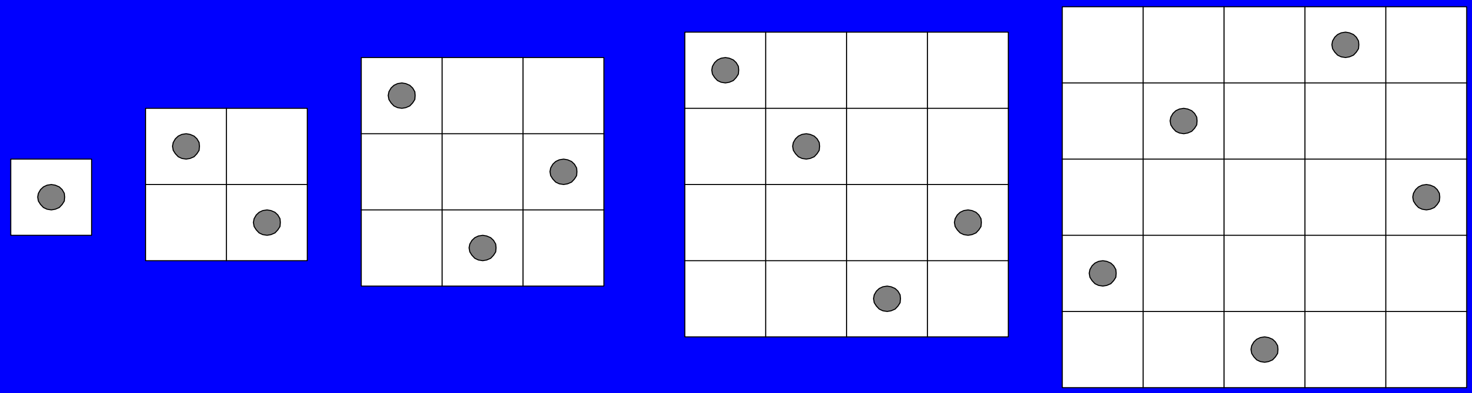
PROBLEMS IN COSTAS ARRAYS

연세대학교 전자공학과
송 홍 엽

1996년 5 월 11 일 (토요일)

What is a Costas array of order n ?

- A Costas array of order n is an n x n, otherwise blanked, array of n dots such that (1) each row (and column) contains exactly one dot and (2) all the n-choose-2 lines connecting two dots are distinct in either slope or length.
- Examples of Costas arrays of order 1,2,3,4, and 5 are



Applications to Radar, Sonar, and FH Patterns

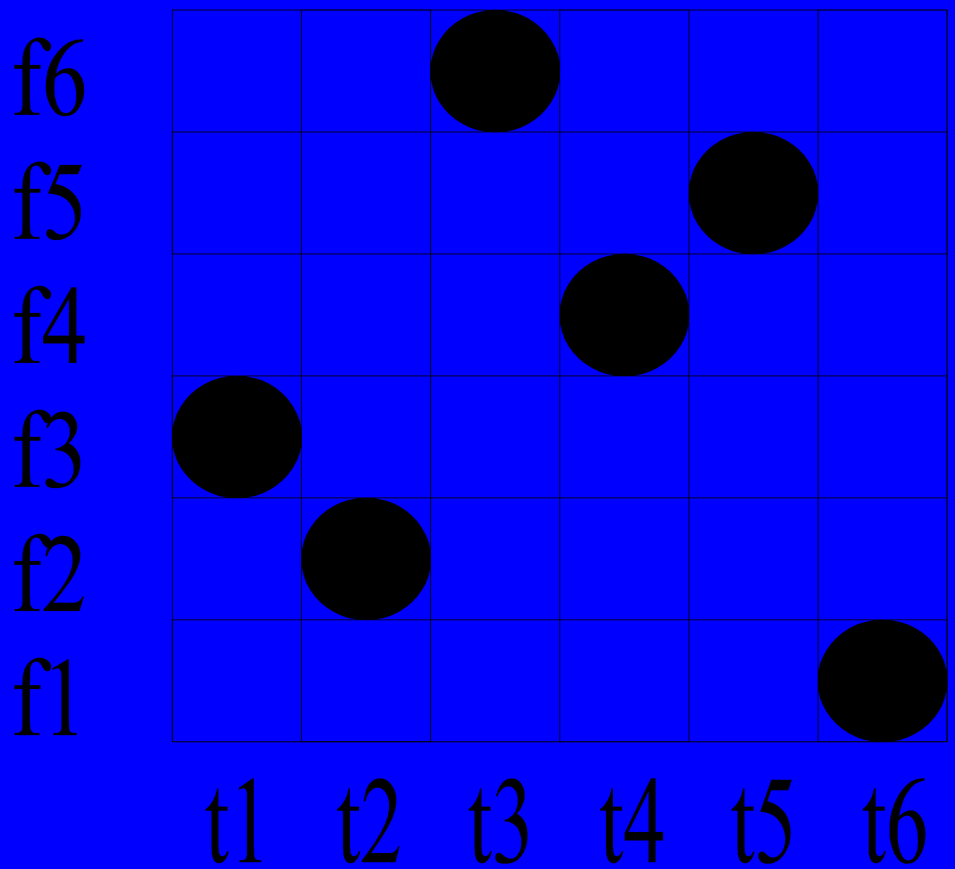
- Let $K(x,y)$ be the number of dots matched between a Costas array of order n and its shifted version when the shift is to the right by x and up by y.
- Definition implies that, then,

  $K(x,y) = 0$ or 1 for all $|x|<n$ and $|y|<n$ except for $(x,y)=(0,0)$, and $K(0,0)=n$.

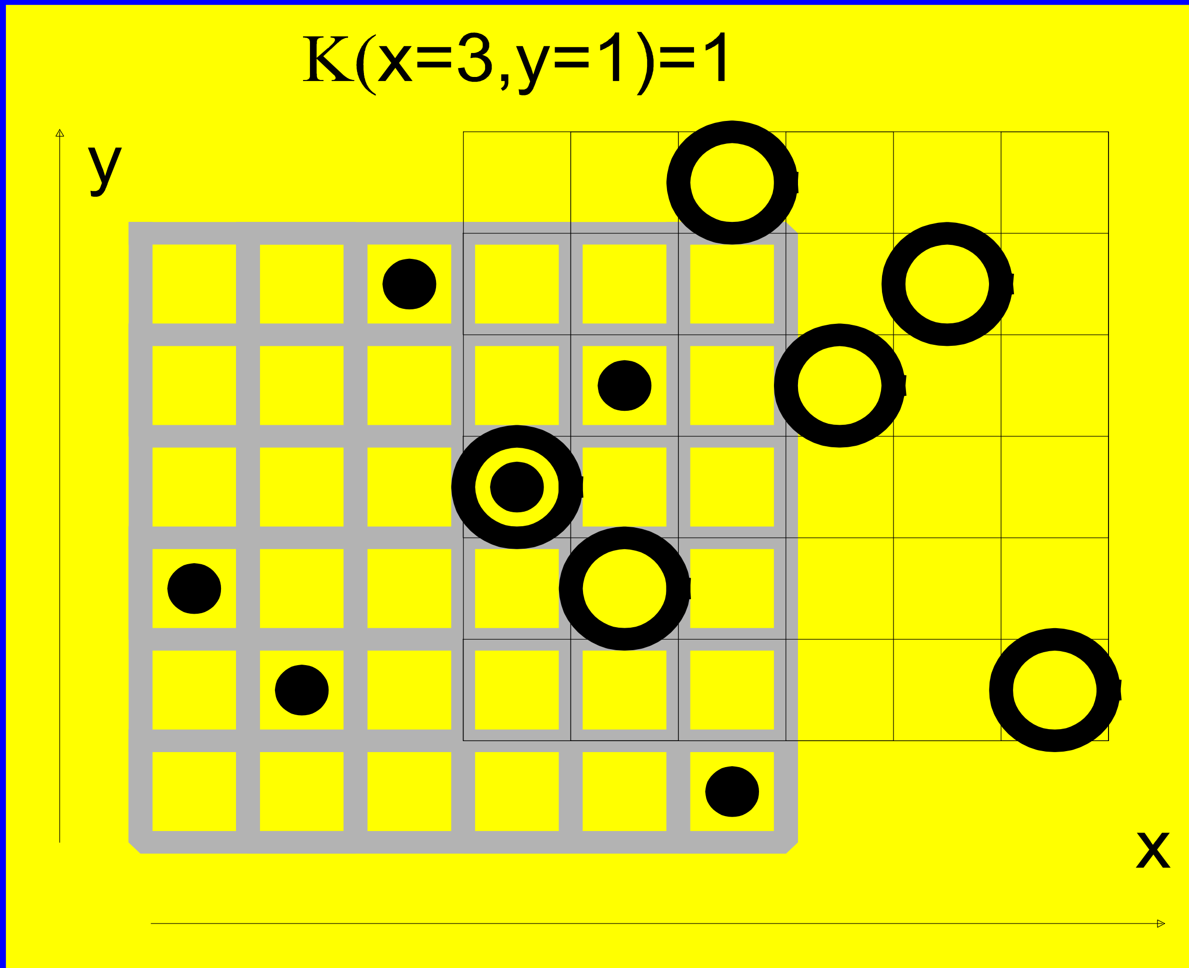
  $\longrightarrow$ Ideal Autocorrelation Function

- Usually, x-axis represents time and y-axis represents frequency so that the Costas array of order n induces a set of n pulses each in different frequency (using exactly once) for the best possible resolution in "pulsed radar" or "active sonar" systems.

Costas array of order 6 and Autocorrelation (I)



Costas array of order 6 and Autocorrelation (II)



Costas array of order 6 and Autocorrelation (III)

		1								
				1		1				
			1				1	1		
1				1			1		1	
	1		1	1		1		1		
					6					
		1		1		1	1		1	
	1		1			1				1
		1	1				1			
				1		1				
								1		

Lempel Construction

- (Lempel) Let a be a primitive element in $GF(q)$, the finite field of q elements. For $x, y=1,2,...,q-2$, the dots are in position (x,y) if and only if $a^x+a^y=1$.
- This produces an infinite family of Costas arrays of order $q-2$ for any prime power q. If there is a in $GF(q)$ which is primitive and $a+a=1$ then the Costas array contains a dot in $(1,1)$ position. Deleting it gives a Costas array of order $q-3$.

- It will be possible to produce a Costas array of order $q-3$ by deleting a corner dot whenever it contains a corner dot. Some sufficient conditions on the primitive element a for this to happen are :

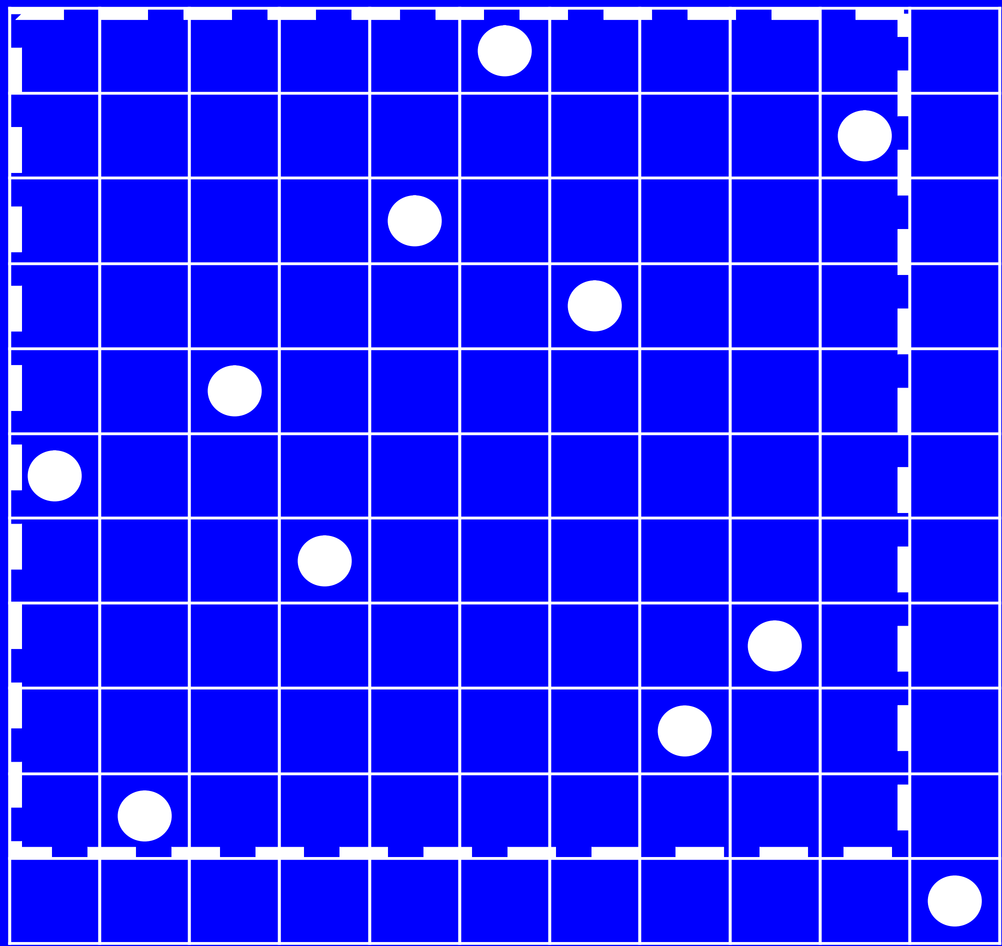
  $a+a=1$ (or, $a=1/2$);

  $a^{-1}+a^{-1}=1$ (or, $a=2$);

  $a+a^{-1}=1$ (or, a is a root of $x^2-x+1=0$)

Example of order 11 (and 10) : Lempel Construction

x	2^x	$1-2^x$	$\log_2(1-2^x)$
1	2	12	6
2	4	10	10
3	8	6	5
4	3	11	7
5	6	8	3
6	12	2	1
7	11	3	4
8	9	5	9
9	5	9	8
10	10	4	2
11	7	7	11



Golomb Construction

- (Golomb) Let a and b be primitive elements (not necessarily distinct) in $GF(q)$, the finite field of q elements. For $x,y=1,2,...,q-2$, the dots are in position (x,y) if and only if $a^x+b^y=1$.

- This produces an infinite family of Costas arrays of order $q-2$ for any prime power q. If there are a and b in $GF(q)$ which are primitive and $a+b=1$ then the Costas array contains a dot in $(1,1)$ position. Deleting it gives a Costas array of order $q-3$.

- If, in addition, $a^2+b^2=1$, then an additional corner dot can be removed so that the result is of order $q-4$.

Golomb Construction (continued)

- If there exist primitive elements a and b (not necessarily distinct) in $GF(q)$ satisfying the conditions below, then a Costas array of order n can be obtained by removing one or more corner dots:

name	CONDITIONS	n
L3	$a^{-1}+a^{-1}=1$ (or, $a=2$)	$q-3$
T4	$a^2+a=1$	$q-4$
G3	$a+b=1$	$q-3$
G4	$a+b=1$ and $a^2+b^2=1$	$q-4$
G4* G5*	$a+b=1$ and $a^2+b^{-1}=1$ and necessarily $a^{-1}+b^2=1$	$q-4$ $q-5$

Some Conditions

- L3: $a^{-1}+a^{-1}=1$ (or, $a=2$)
  - This works only when 2 is primitive in $GF(q)$.
- T4: $a^2+a=1$
  - A necessary condition for $GF(q)$ to have a primitive a satisfying $a^2+a=1$ is that $q=4$, $q=5$, $q=9$, a prime p with $p=1 \pmod{10}$, or $p=9 \pmod{10}$.
- G3: $a+b=1$
  - It was proved that all the $GF(q)$ has a and b with $a+b=1$.
- G4: $a+b=1$ and $a^2+b^2=1$
  - This works only when $q=2^k$.
- G4*: $a+b=1$ and $a^2+b^{-1}=1$
  - This works for precisely the subset of values of q for which T4 construction occurs: $q=4,5,9$, and those primes p for which T4 construction occurs which satisfy either $p=1 \pmod{20}$ or $p=9 \pmod{20}$

Welch Construction

- Let a be a primitive root mod p, a prime.
- For $x, y = 1, 2, ..., p-1$, the dots are in position (x, y) if and only if $a^x = y$.

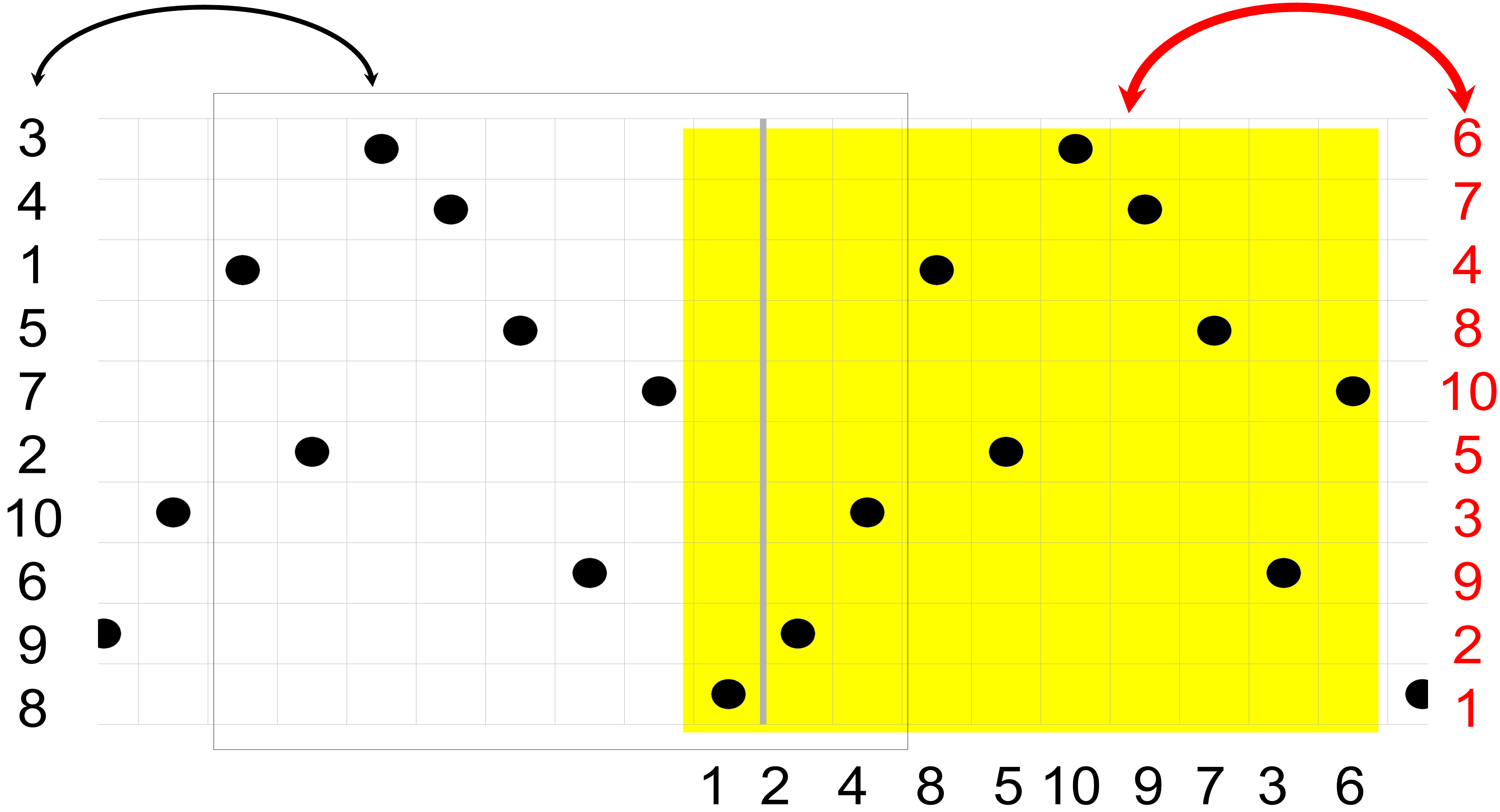
  That is, the dots are in (x, a^x) for $x = 1, 2, ..., p-1$.

- Welch Costas array has an additional property:

  After you roll up the square so that the left-most column comes right next to the right most column (the square plane now becomes the surface of a cylinder), cut vertically along any column, then the resulting square array is also a Costas array.

  - This is called the “single periodicity.”

Singly Periodic Costas Array of order 10



Number of distinct Costas arrays of order n

- C(n) = number of distinct Costas arrays of order n
- c(n) = number of distinct Costas arrays of order n, inequivalent under the dihedral group of rotations and reflections of the square
- s(n) = number of distinct Costas arrays of order n which are symmetric across a diagonal AND inequivalent under the dihedral group of rotations and reflections of the square

EXAMPLE : C(4)=12, c(4)=2, and s(4)=1

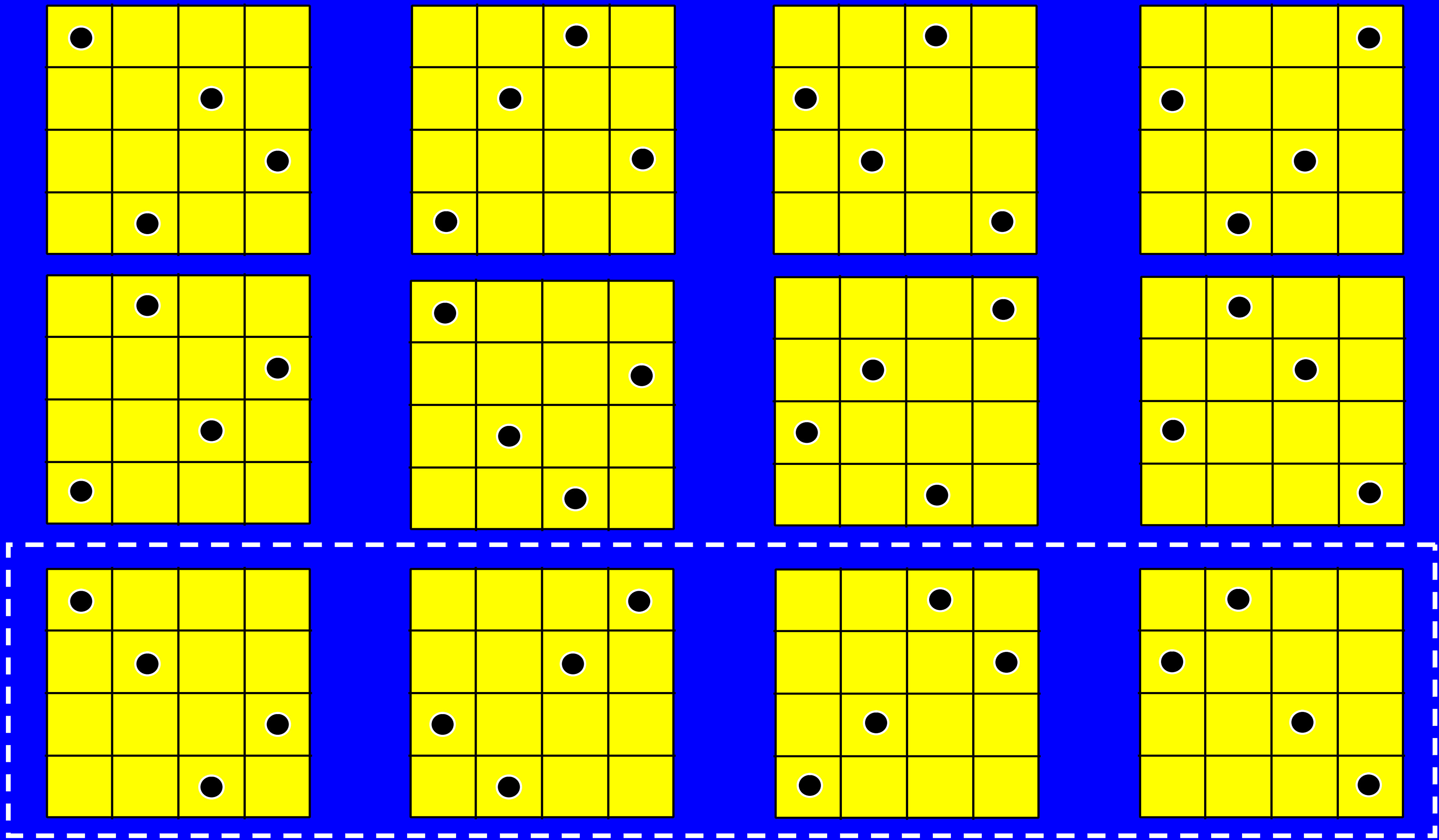
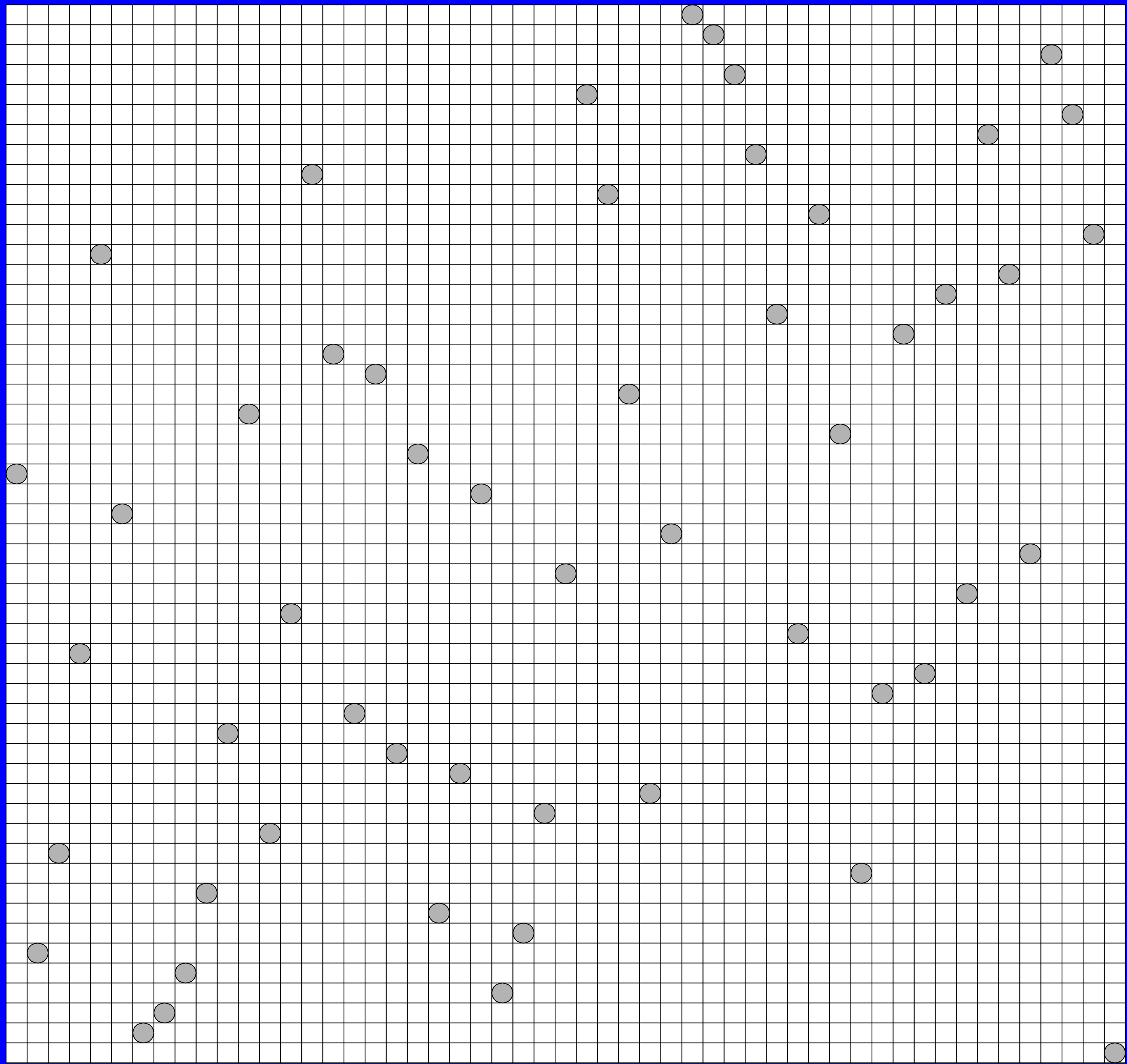


Table of C(n), c(n), and s(n)

n	C(n)	c(n)	s(n)
1	1	1	1
2	2	1	1
3	4	1	1
4	12	2	1
5	40	6	2
6	116	17	5
7	200	30	10
8	444	60	9
9	760	100	10
10	2160	277	14
11	4368	555	18
12	7852	990	17
13	12828	1616	25
14	17252	2168	23
15	19612	2467	31
16	21104	2648	20
17	18276	2294	19
18	15096	1892	10
19	10240	1283	6
20	6464	810	4
21	3536	446	8
22	2052	259	5
23	872	114	10
24	at least 1	at least 1	0
25	at least 1	at least 1	2
26	at least 1	at least 1	2
27	at least 1	at least 1	7
28	at least 1	at least 1	0
29	at least 1	at least 1	5
30	at least 1	at least 1	4
31	at least 1	at least 1	0
32	??	??	0



Difference Triangle of a Costas array

3	4	1	5	7	2	10	6	9	8
1	-3	4	2	-5	8	-4	3	-1	
-2	1	6	-3	3	4	-1	2		
2	3	1	5	-1	7	-2			
4	-2	9	1	2	6				
-1	6	5	4	1					
7	2	8	3						
3	5	7							
6	4								
5									

Difference Triangle mod 10

3 4 1 5 7 2 10 6 9 8

1 7 4 2 5 8 6 3 9

8 1 6 7 3 4 9 2

2 3 1 5 9 7 8

4 8 9 1 2 6

9 6 5 4 1

7 2 8 3

3 5 7

6 4

5

Some Open Problems

- Does there exist a Costas array of order 32 ?
  - The table of C(n) gives a “hunch” that it does not, because C(n) is monotonically increasing from 1 to 16 and then decreasing from 16 to 22 (current state of computer search).
  - On the other hand, For any positive integer n, there is a Costas array of size bigger than n from the algebraic constructions.

- Does there exist a singly periodic Costas array which is essentially not from the Welch construction ?
  - No other examples are known except for those by the Welch construction.
  - It is known that every singly periodic Costas array of order up to 22 comes essentially from the Welch construction.