10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

Introduction to COSTAS ARRAYS

(Current status of Research and Some Open Problems)

연세대학교 전기전자공학부

송 홍 엽

hysong@yonsei.ac.kr

2014. 3.

10000001000000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111 1

Introduction

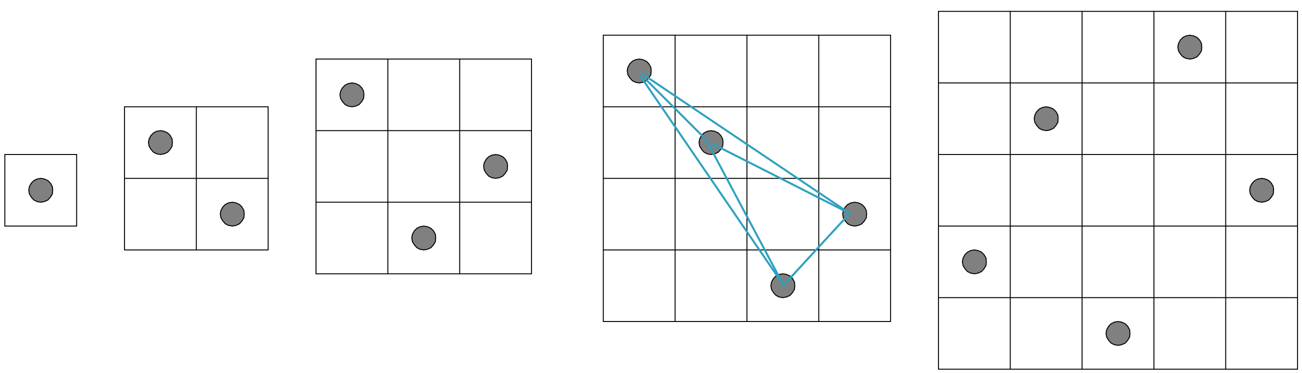
What is a Costas array of order n ?

- 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`.

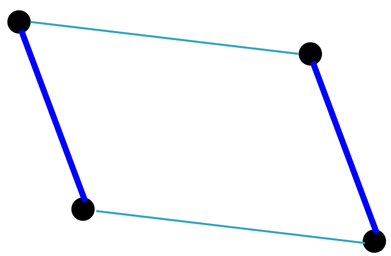
- Examples of Costas arrays of order 1,2,3,4, and 5 are

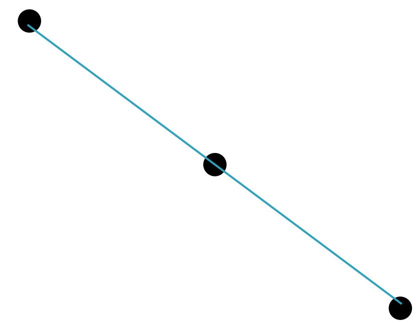


equivalent condition of (2)

(2) all the n-choose-2 lines connecting two dots are distinct in either `slope` or `length`.

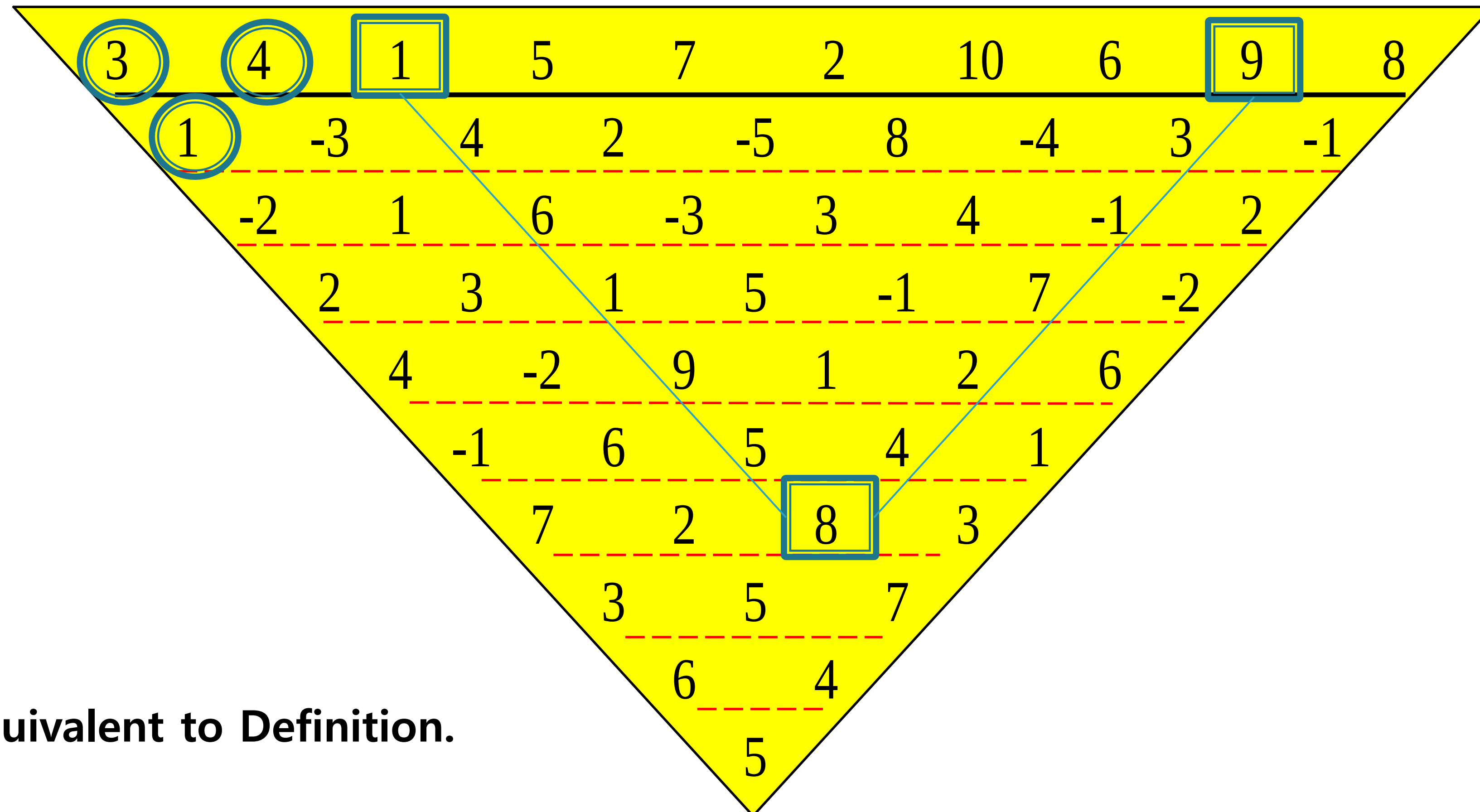
(2') no 4 dots on the vertices of a parallogram (and no 3 dots on a line with equal distance)





Difference Triangle of a Costas array

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111



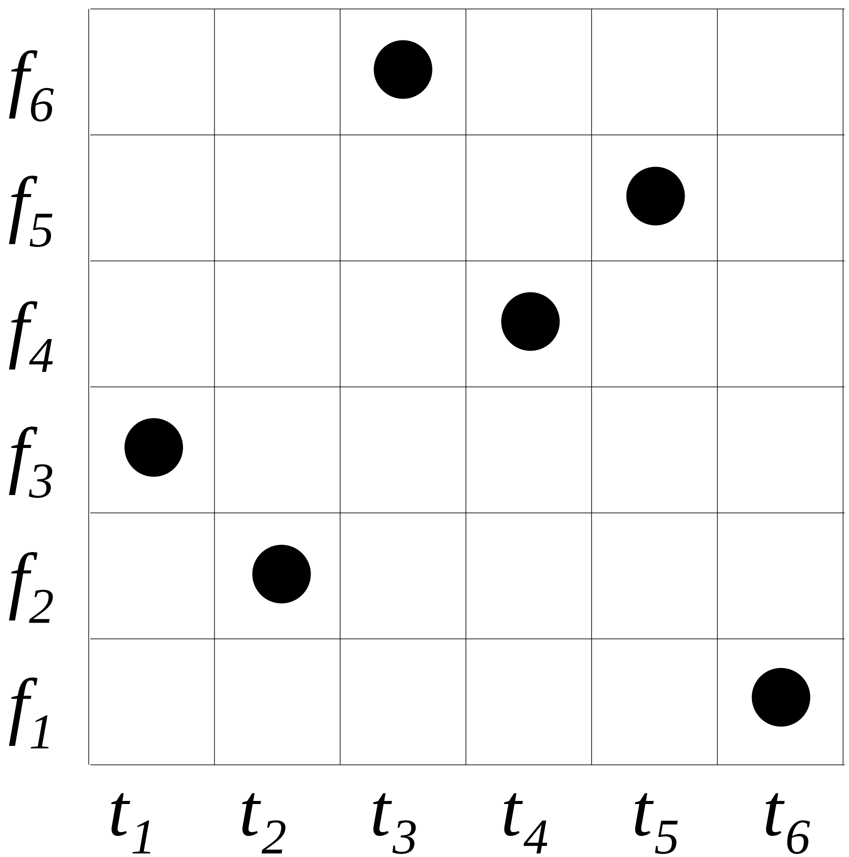
equivalent to Definition.

Necessary and Sufficient condition !!

Costas array is a discrete model of a frequency-modulated signal for pulse compression radar.

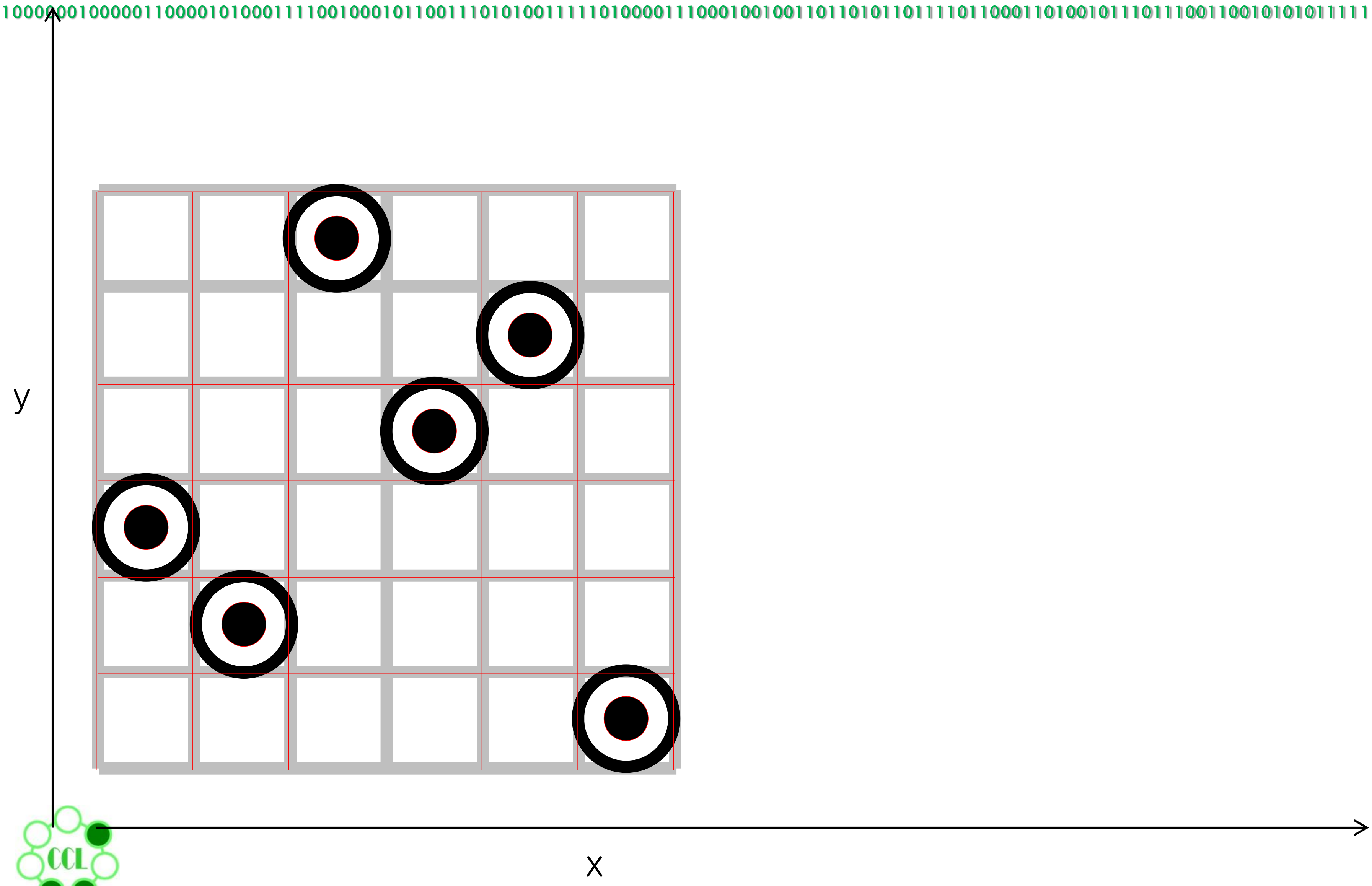
10000001000000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

Following is a Costas array of order 6.



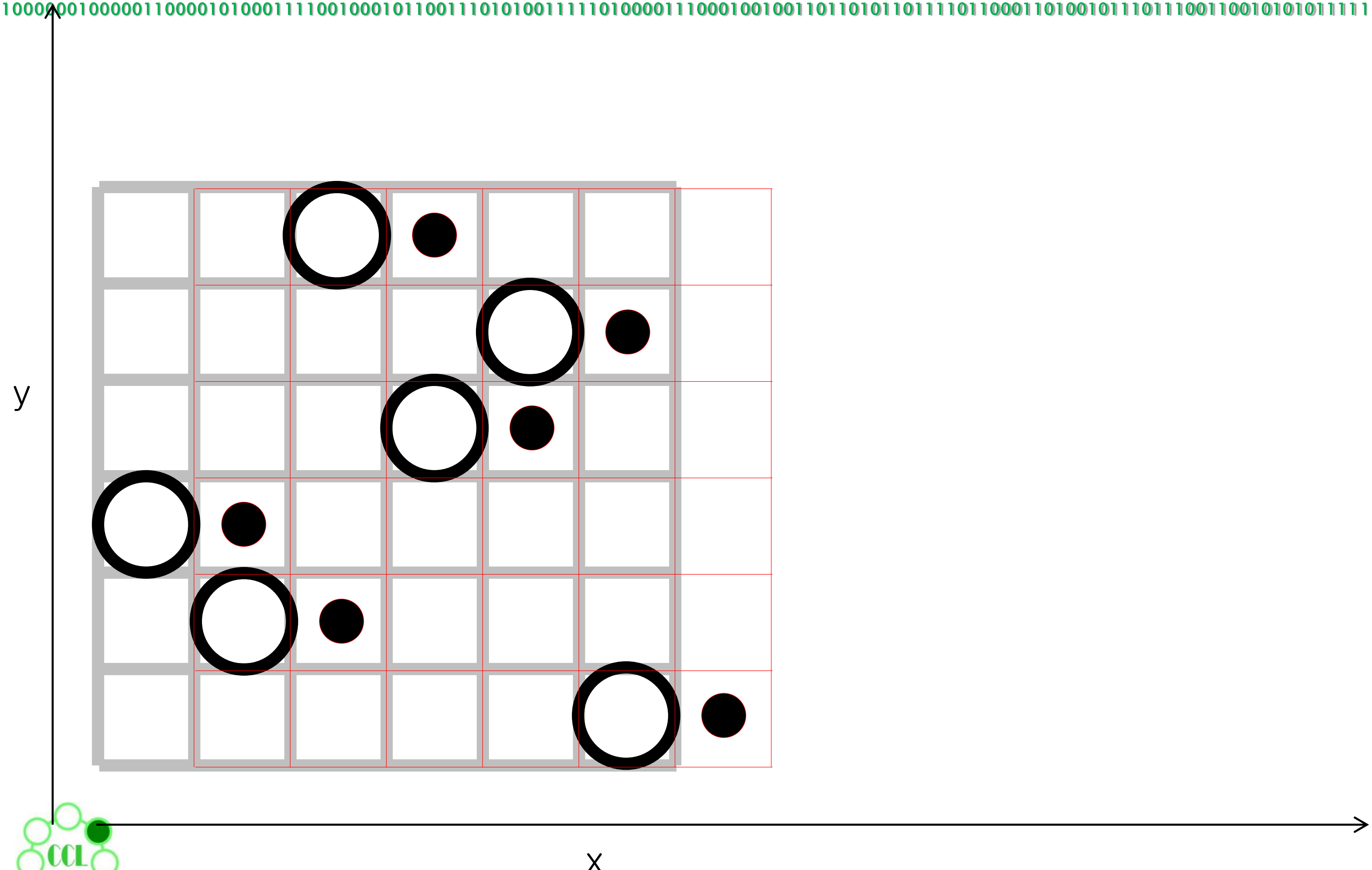
Costas array of order 6 and Autocorrelation at (x=0,y=0)

1000000100000011000010100011110010001011001110101001111110100001110001001001101101011011110110001101001011101110011001010101111111



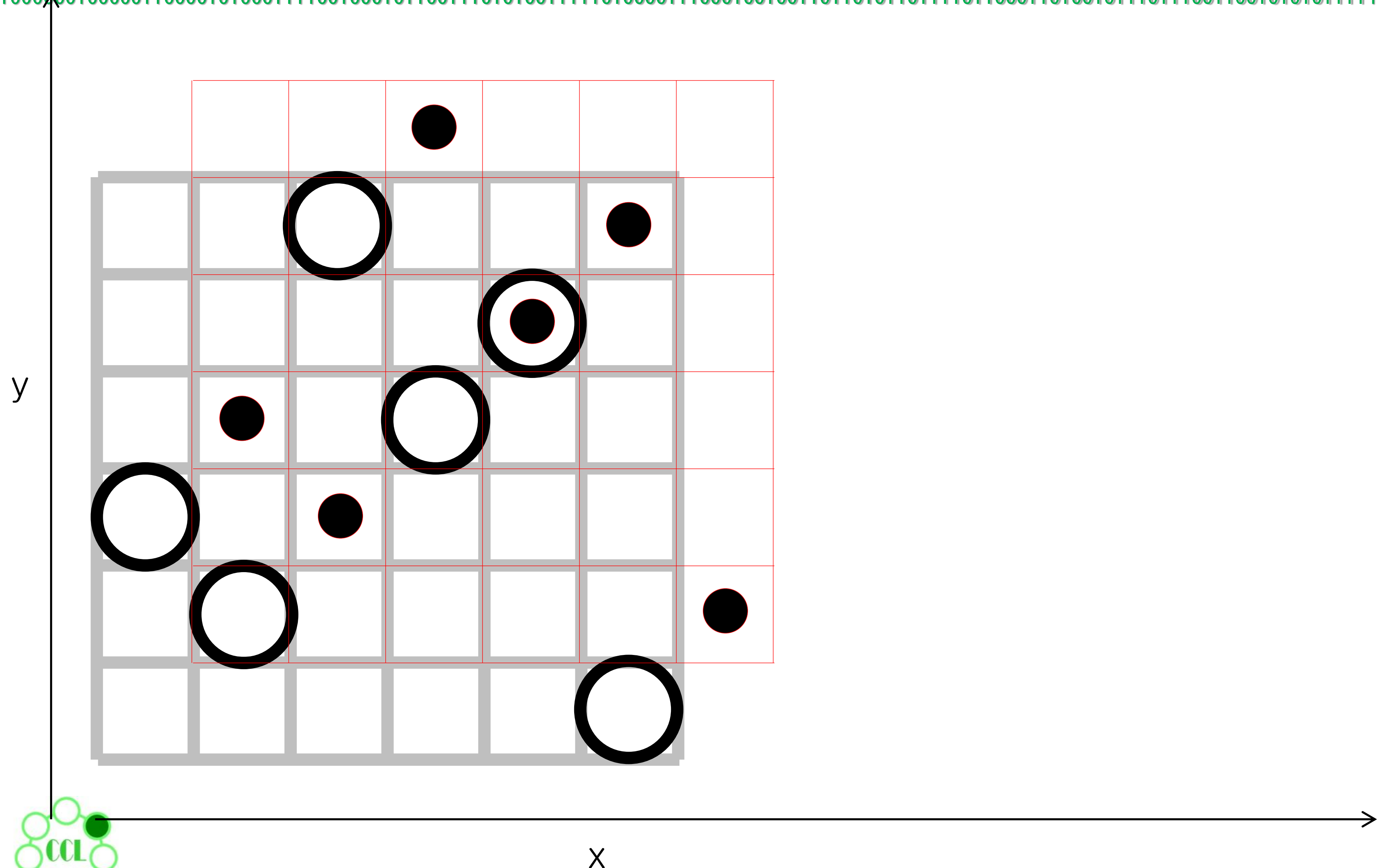
Costas array of order 6 and Autocorrelation at (x=1,y=0)

1000000100000011000010100011110010001011001110101001111110100001110001001001101101011011110110001101001011101110011001010101111111



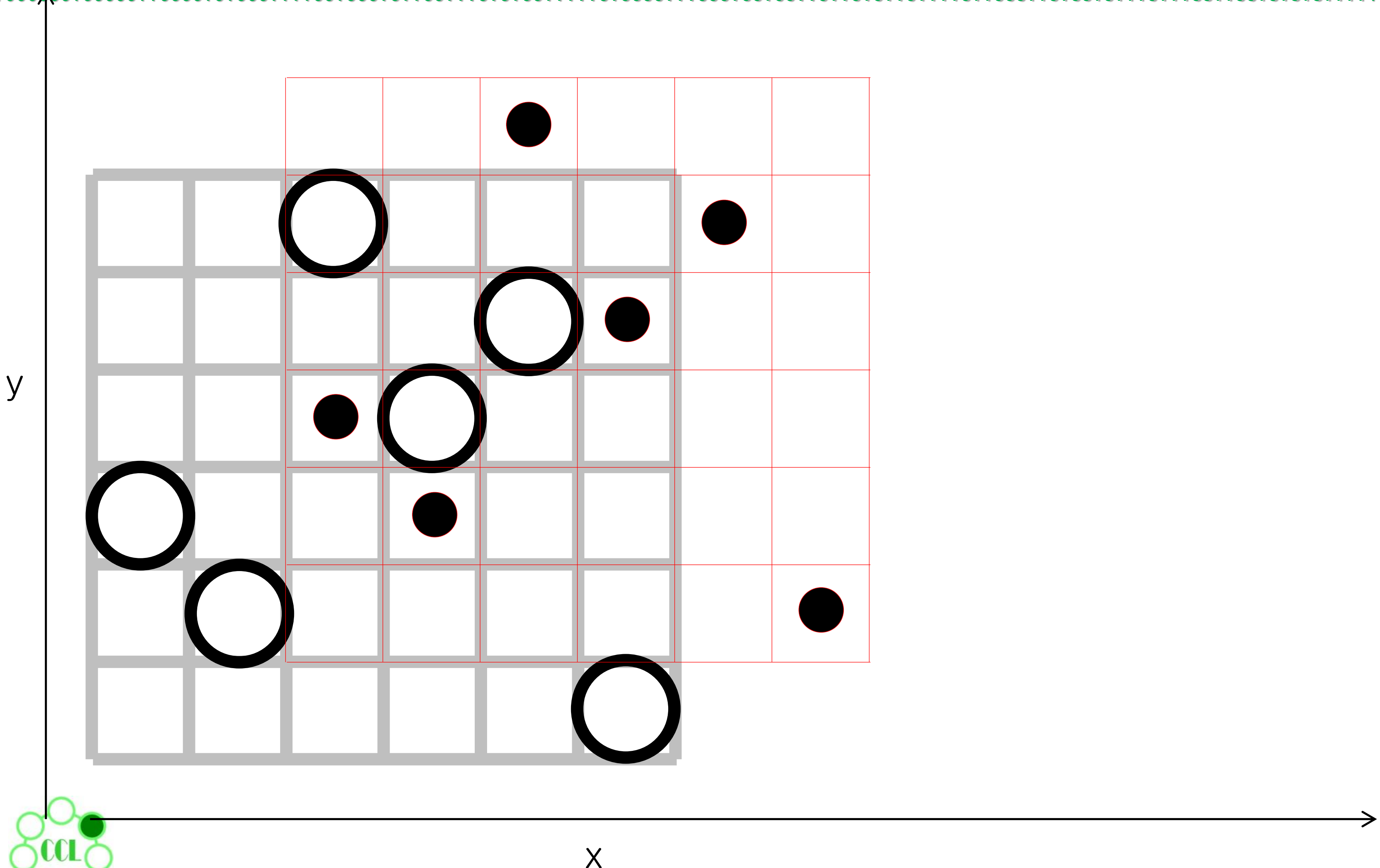
Costas array of order 6 and Autocorrelation at (x=1,y=1)

1000000100000011000010100011110010001011001110101001111110100001110001001001101101011011110110001101001011101110011001010101111111



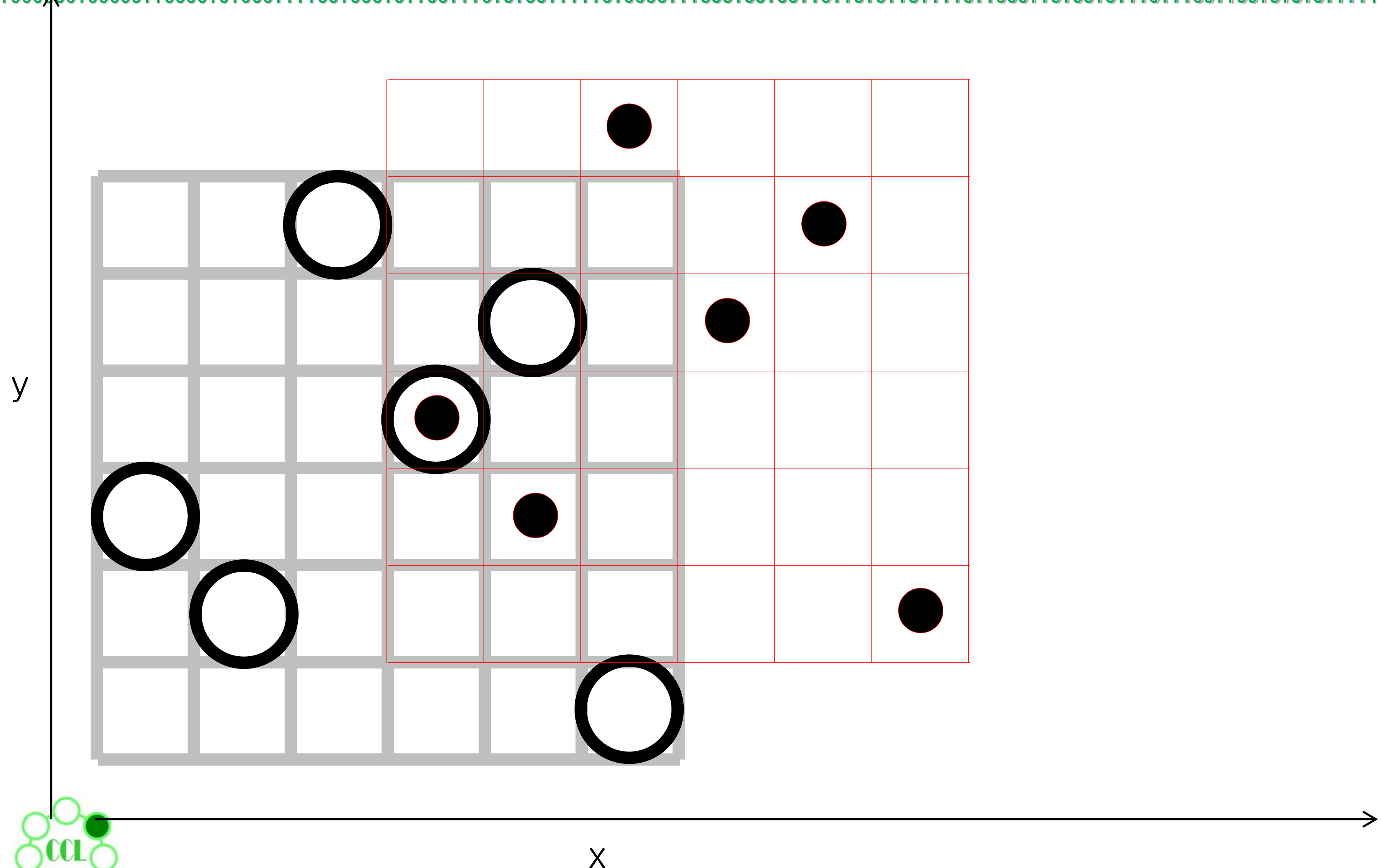
Costas array of order 6 and Autocorrelation at (x=2,y=1)

10000001000000110000101000111100100010110011101010011111010000011100010010011011010110111101100011010010111011100110010101011111 11



Costas array of order 6 and Autocorrelation at (x=3,y=1)

1000000100000011000010100011110010001011001110101001111110100000111000100100110110101101111011000110100101110111001100101010111111



discrete version of ambiguity function

Full (non-periodic) Autocorrelation Function

10000001000000110000101000 | 0111011100110010101011111

		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		

y

x

x=0, y=0

Applications to Radar, Sonar, and FH Patterns

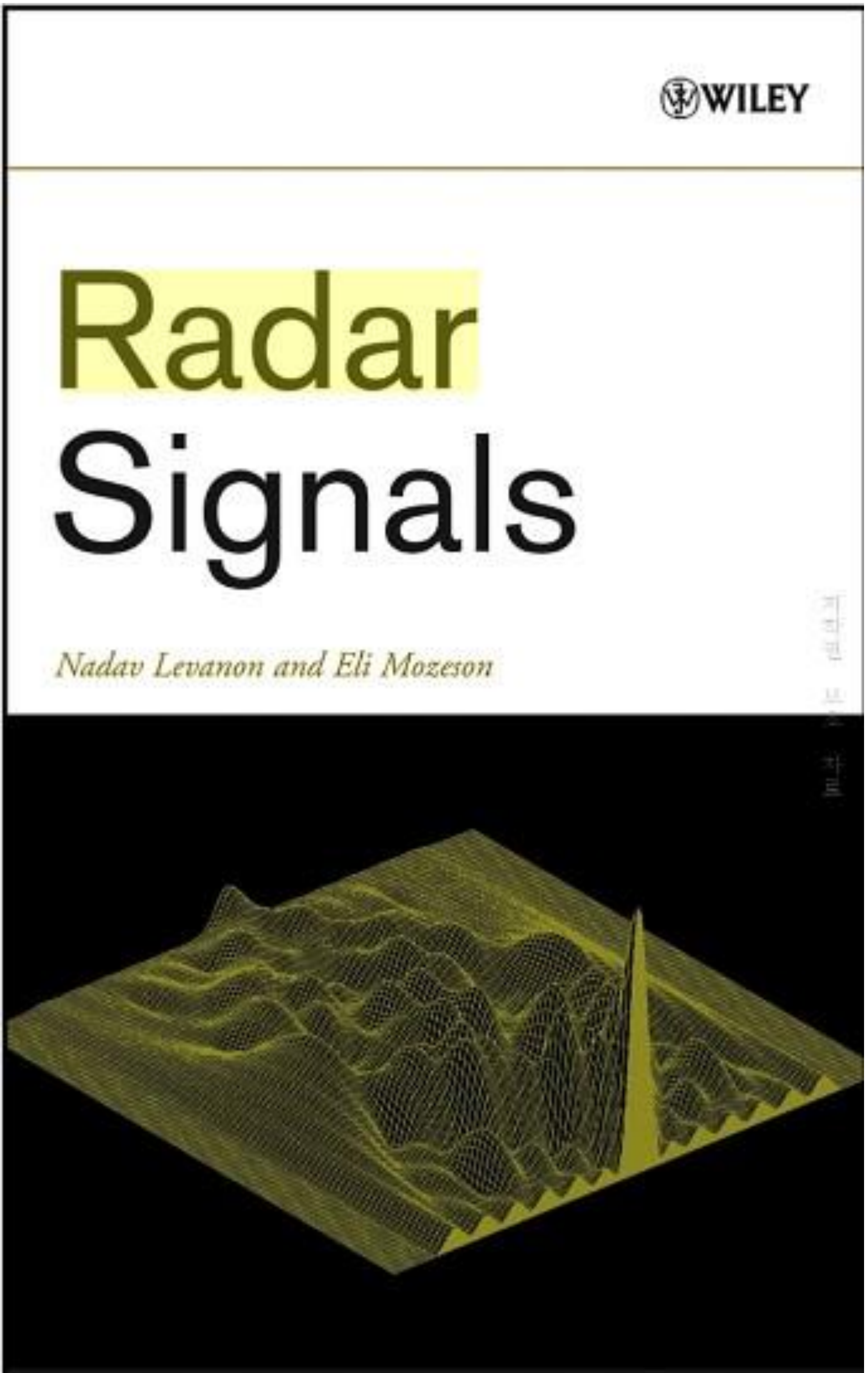
1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- 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

  $K(0,0)=n$.

  ⟶ 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.
- **Pulse Compression Radar**



3 Ambiguity Function 34

3.1 Main Properties of the Ambiguity Function 34
3.2 Proofs of the AF Properties 36
3.3 Interpretation of Property 4 38
3.4 Cuts Through the Ambiguity Function 40
3.5 Additional Volume Distribution Relationships 42
3.6 Periodic Ambiguity Function 42
Box 3A: Variants of the Periodic Ambiguity Function 44
3.7 Discussion 46
Appendix 3A: MATLAB Code for Plotting Ambiguity Functions 47
Problems 51
References 52

4 Basic Radar Signals 53

4.1 Constant-Frequency Pulse 53
4.2 Linear Frequency-Modulated Pulse 57
4.2.1 Range Sidelobe Reduction 61
4.2.2 Mismatch Loss 66
4.3 Coherent Train of Identical Unmodulated Pulses 67
Problems 72
References 73

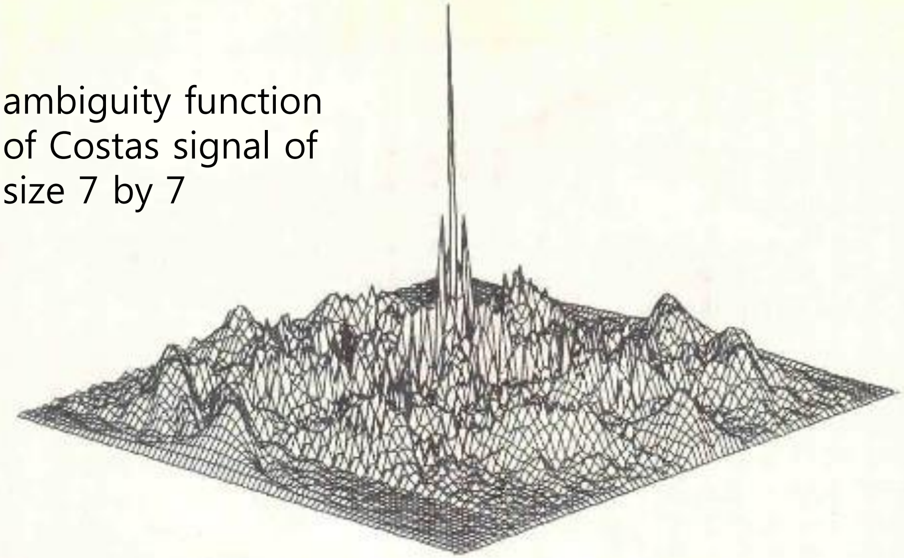
5 Frequency-Modulated Pulse 74

5.1 Costas Frequency Coding 74
5.1.1 Costas Signal Definition and Ambiguity Function 75
5.1.2 On the Number of Costas Arrays and Their Construction 80
5.1.3 Longer Costas Signals 83
5.2 Nonlinear Frequency Modulation 86
Appendix 5A: MATLAB Code for Welch Construction of Costas Arrays 96
Problems 97
References 99

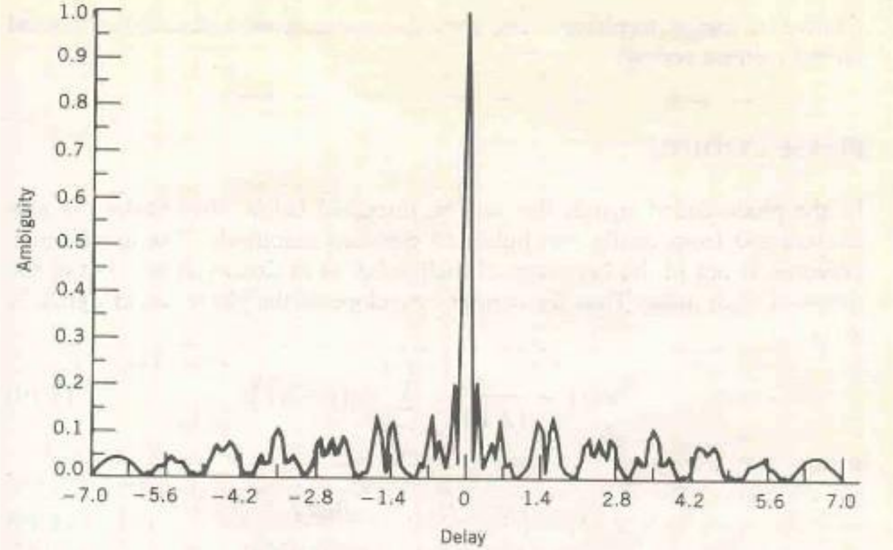
6 Phase-Coded Pulse 100

Box 6A: Aperiodic Correlation Function of a Phase-Coded Pulse 101

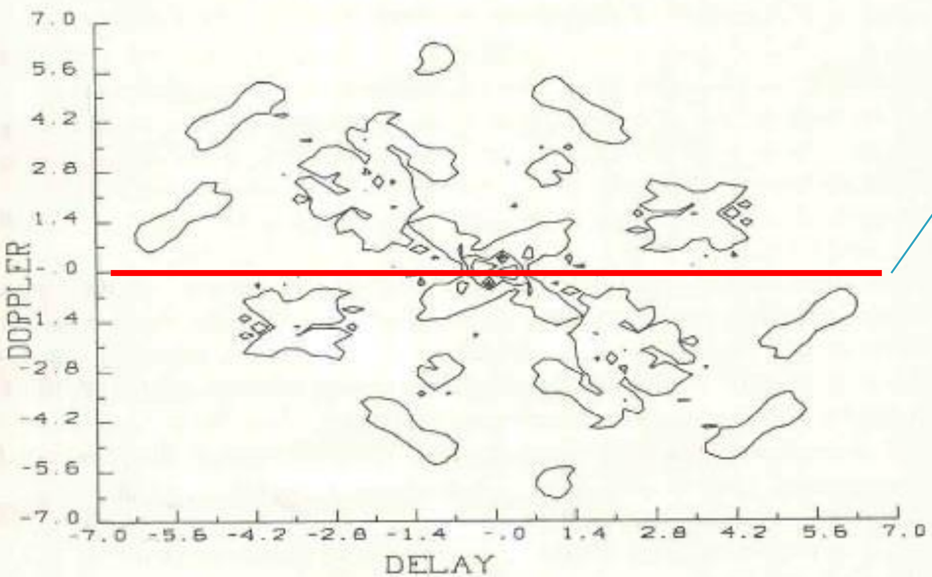
ambiguity function
of Costas signal of
size 7 by 7



(a)

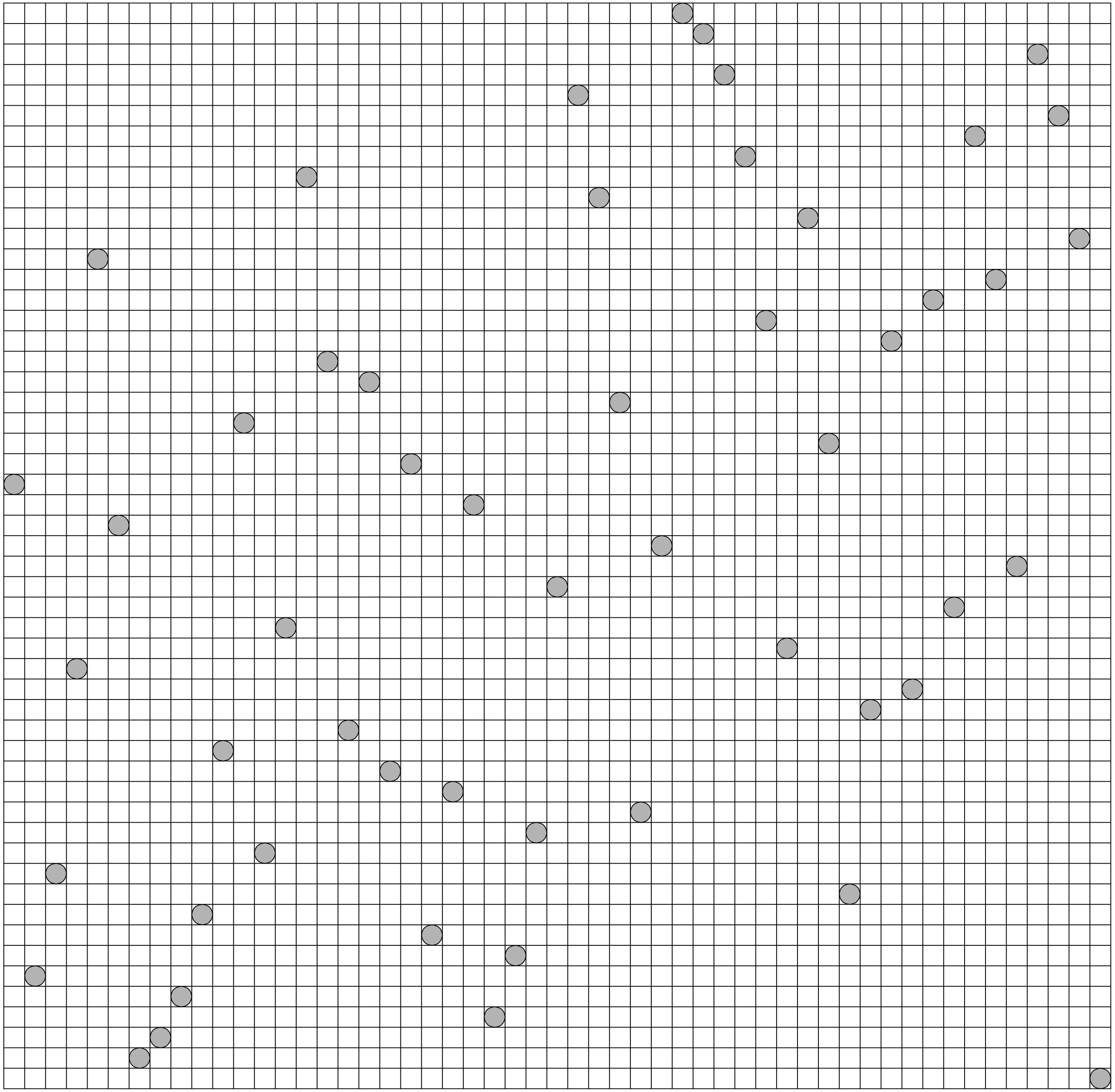


cross cut at zero Doppler



(b)

size 53



Algebraic Constructions

Lempel Construction

1000000100000110000101000111100100010110011101010011111010000011100010010011011010110111101100011010010111011100110010101011111

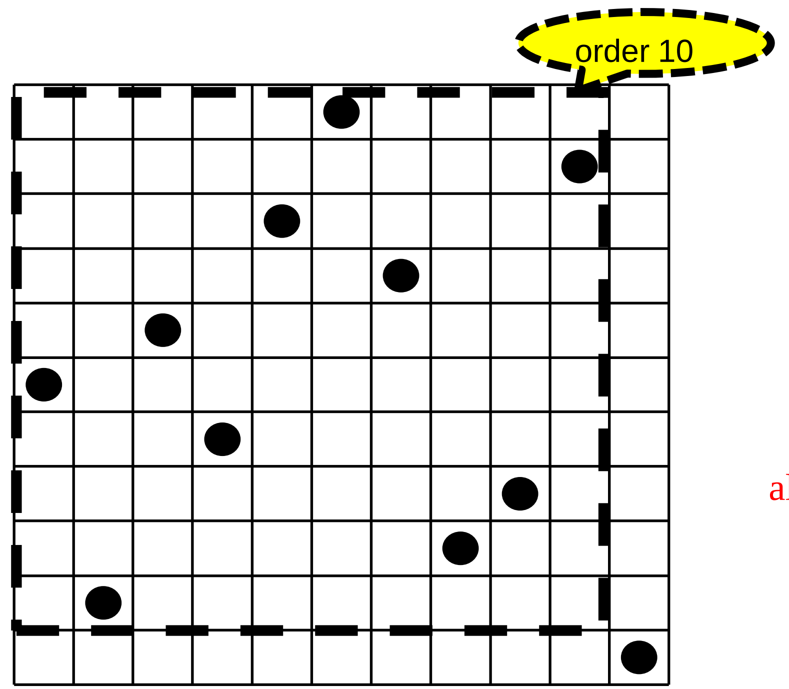
- (Lempel) Let α be a **primitive element** in GF(q), the finite field of q elements.

For x, y=1, 2, . . ., q−2,

the dots are in position (x, y) if and only if $\alpha^x+\alpha^y=1$.

Example of order 11 (mod 13): 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



always symmetric!!

Comments on Lempel Construction

- It produces an infinite family of Costas arrays of order $q-2$ for any prime power q. (including the case where q is itself a prime)
  - An answer to the following question:

Given a positive integer N, does there exist a Costas array of order n for some n bigger than N?

- 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 $q-3$.

Does there exist such a primitive element for ANY finite field GF(q)?

- 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 $x^2-x+1=0$)

Golomb Construction

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- (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 $a^x+b^y=1$.

- When a=b, this becomes Lempel construction.

- 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*	$a+b=1$ and $a^2+b^{-1}=1$	$q-4$
G5*	and necessarily $a^{-1}+b^2=1$	$q-5$

Some Conditions

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- 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 (mod 10), or p=9 (mod 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 (mod 20) or p=9 (mod 20)

Welch Construction

1000000100000011000010100011110010001011001110101001111101000011100010010011011010110111101100011010010111011100110010101011111

- 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 $x = 1, 2, ..., p-1$.**

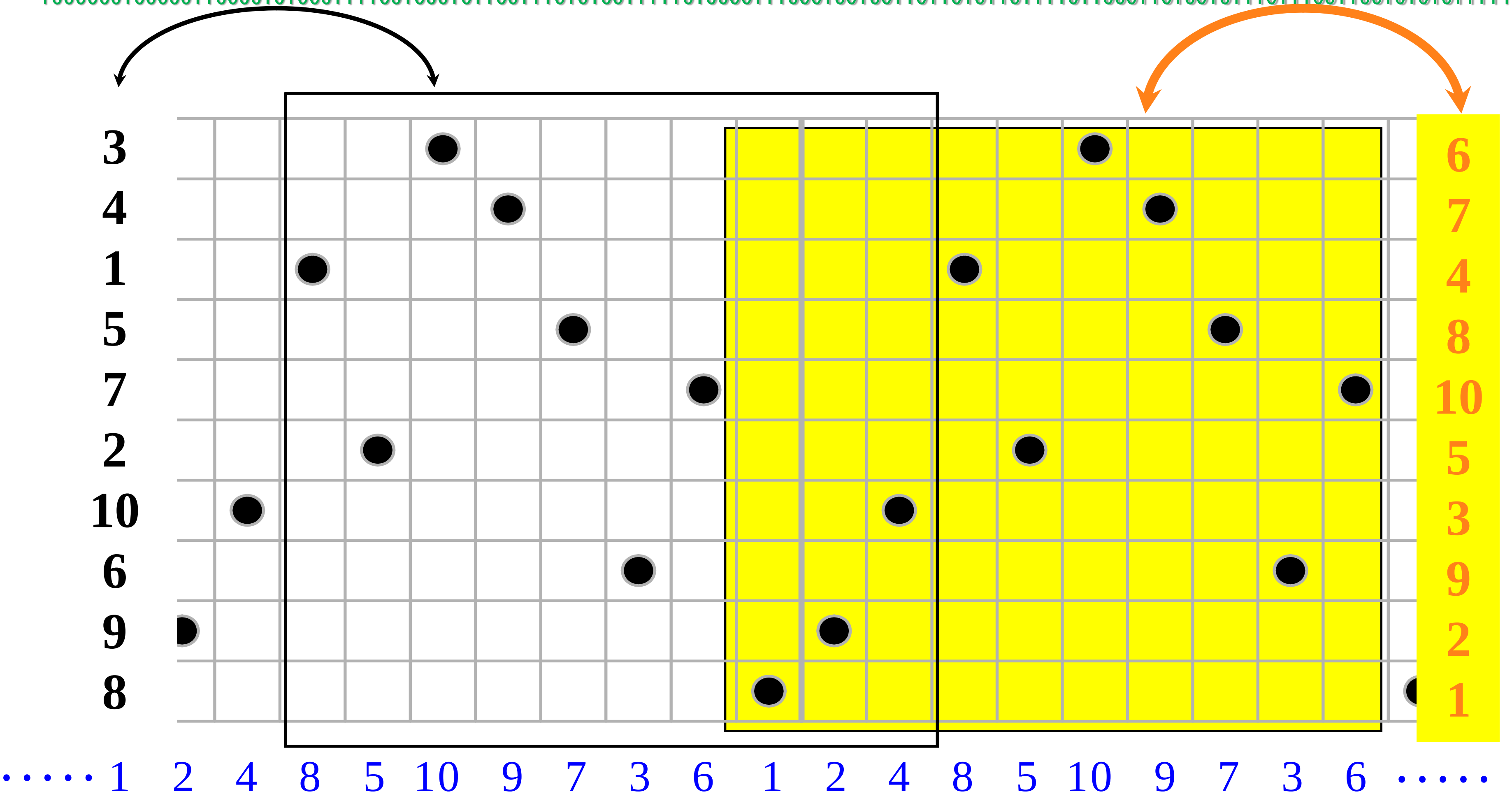
  mod p

- **Welch Costas array has an additional property:**

  "singly periodic" costas array

Singly Periodic Costas Array of order 10

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111



sequence of 2^x (mod 11)

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 symmetries 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

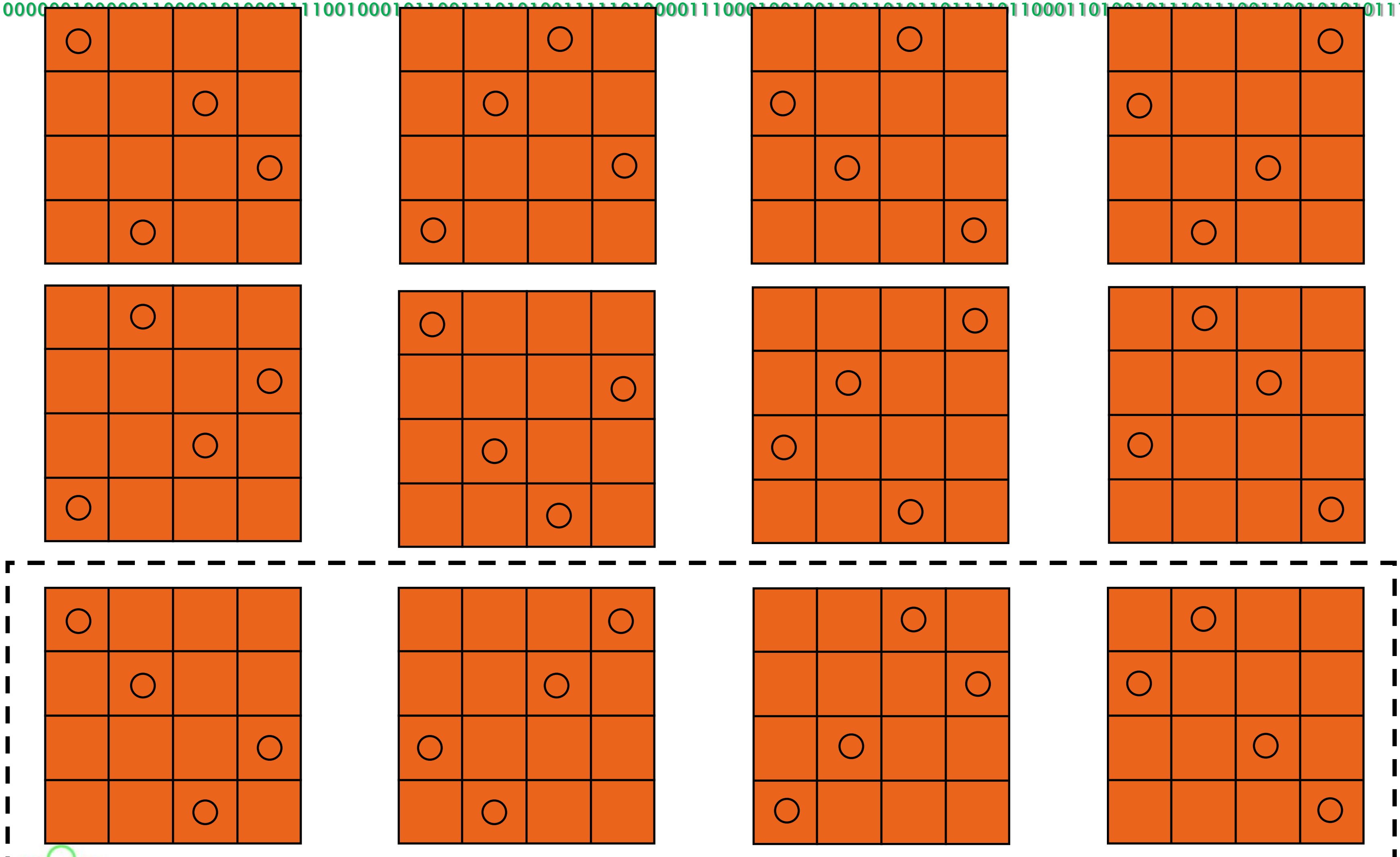


Table of C(n), c(n), and s(n) as of 1996

by ~ 1986

by ~ 1988
(숫자가 감소??)
J. Silverman

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

Open problem:
Find an example of order 32
or
prove that none exists

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

RECENT UPDATES

1996-2014

Some history

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- **시작**
- J.P.Costas - 1983
- **S.W.Golomb**, H. Taylor, O. Moreno

  and some more,....(Lempel, Welch,...) - 80년대~90년대

from USC, Los Angeles

Puerto Rico.
exhaustive search
for n up to 23

Advances in Mathematics of Communications
Volume 5, No. 3, 2011, 547–553
doi:10.3934/amc.2011.5.547

- **2000년대 이후**
- Konstantinos Drakakis, Scott Rickard, etc, from Dublin (exhaustive search for n=24,...,29)

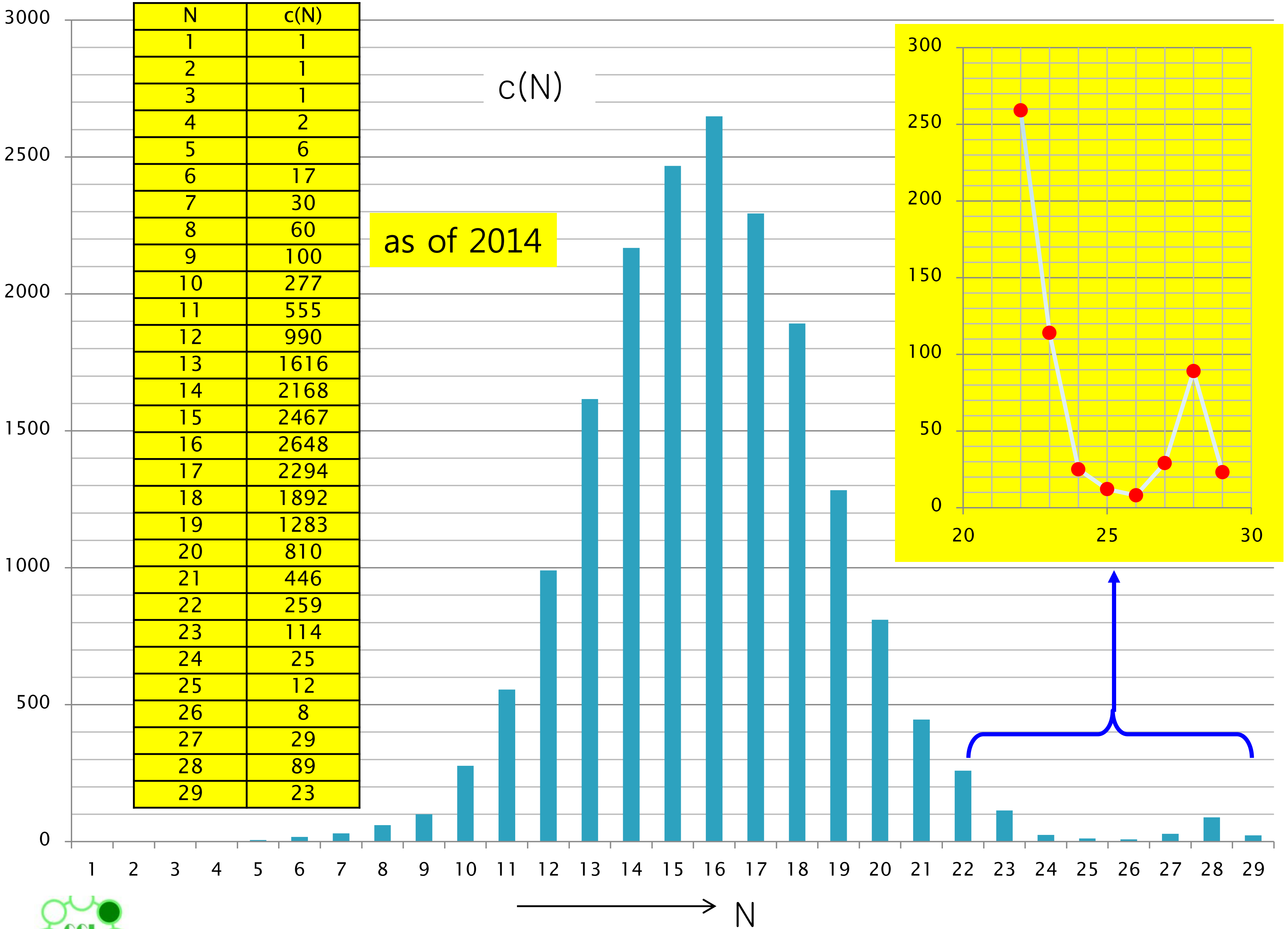
RESULTS OF THE ENUMERATION OF COSTAS ARRAYS OF ORDER 29

Konstantinos Drakakis

School of Electrical, Electronic & Mechanical Engineering
University College Dublin, Belfield, Dublin 4, Ireland


06 01 2007

N	c(N)
1	1
2	1
3	1
4	2
5	6
6	17
7	30
8	60
9	100
10	277
11	555
12	990
13	1616
14	2168
15	2467
16	2648
17	2294
18	1892
19	1283
20	810
21	446
22	259
23	114
24	25
25	12
26	8
27	29
28	89
29	23



forbidden positions??

10000001000

1110100001110001001001101101011011110110001101001011101110011001010101111111

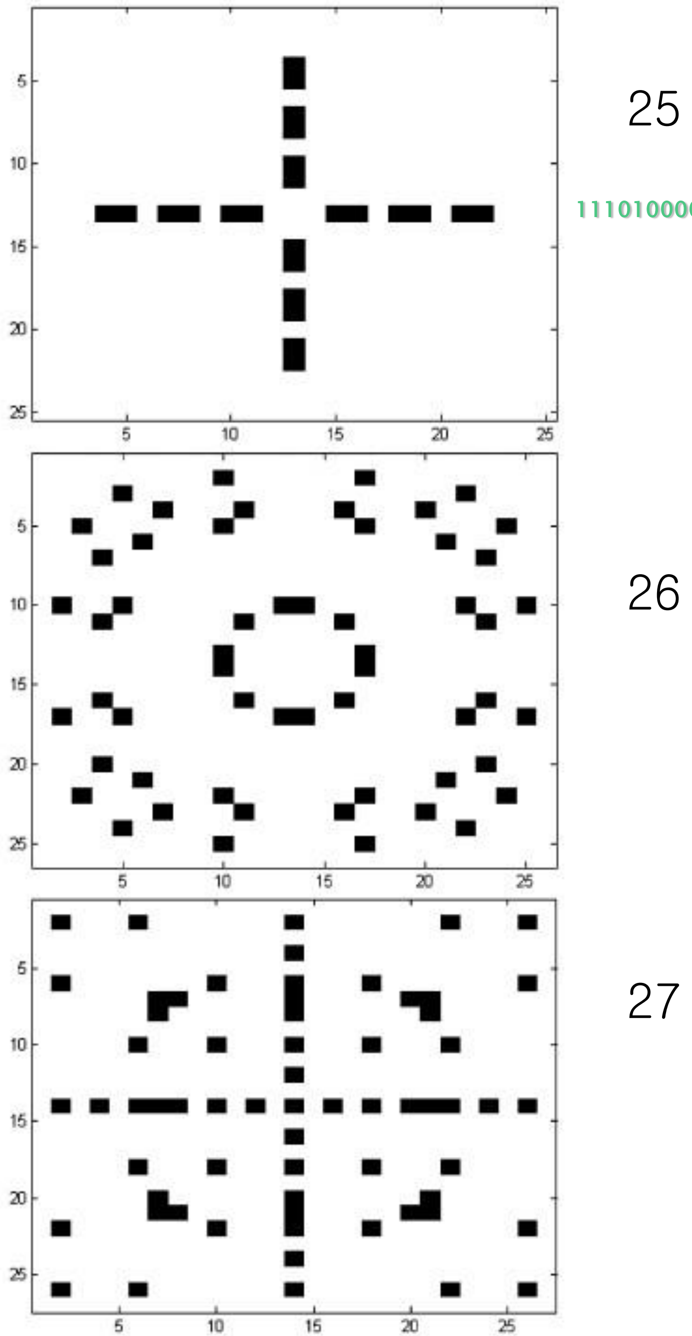


Fig. 2. Forbidden positions for a Costas array of order 25, 26, and 27 (top to bottom).

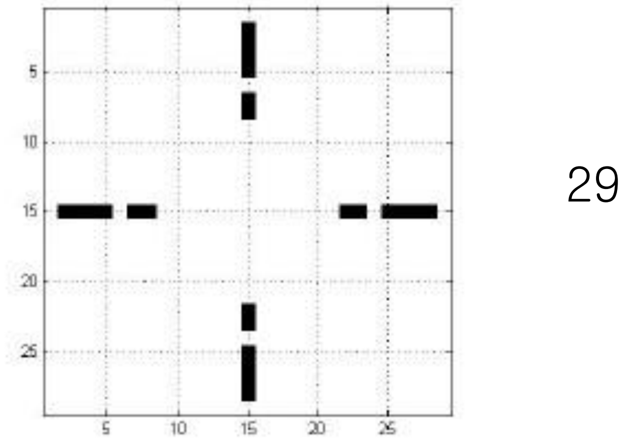
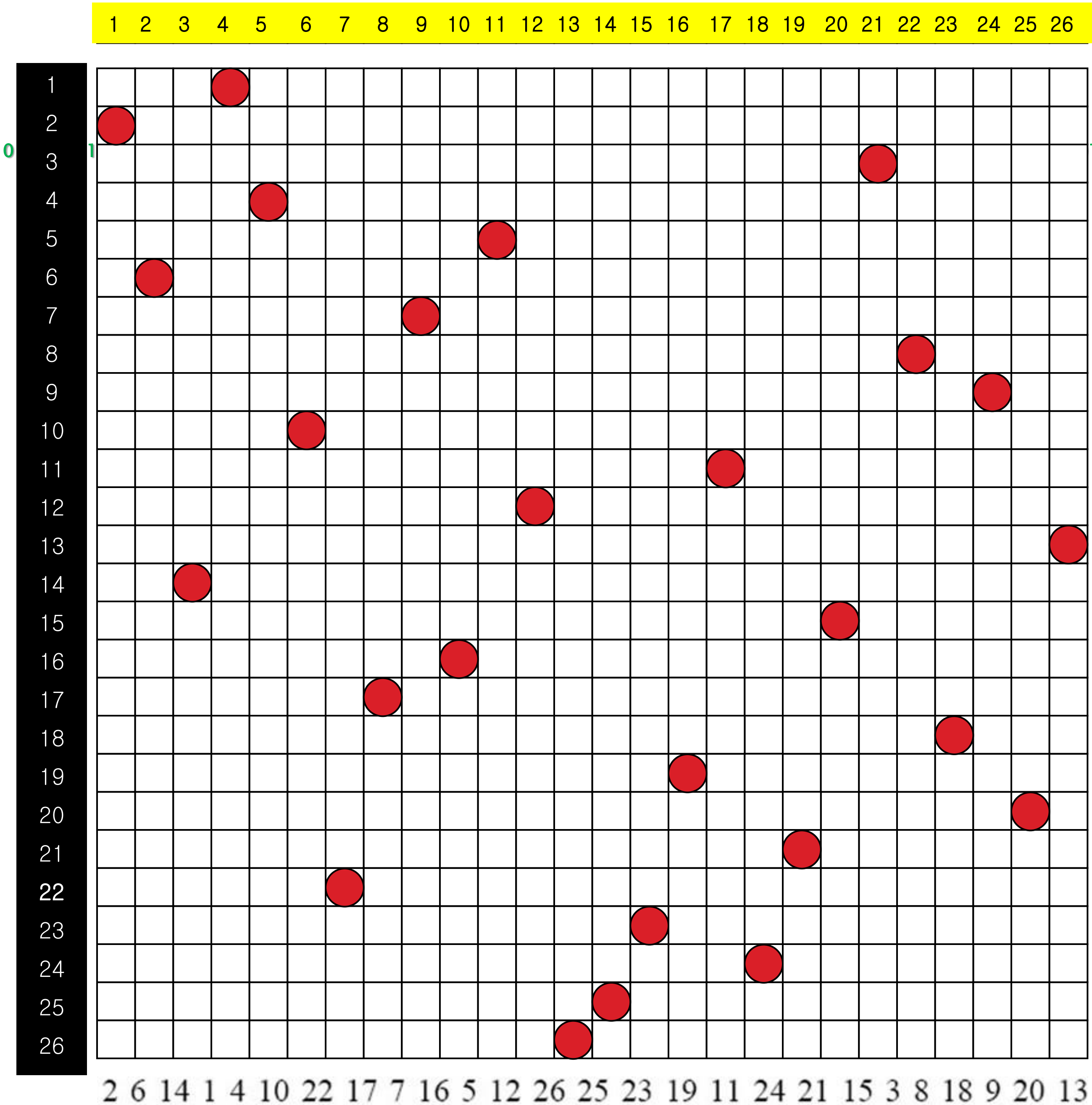


FIGURE 2. Forbidden positions for Costas arrays of order 29

8 (only!!) Essentially distinct Costas arrays of order 26

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

1000000100000011000010



1100101010111111

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. (current state of computer search - 2014).
  - 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 29 comes essentially from the Welch construction.
  - **PROVED to be NO. (2013?)**

2013 ??

On the characterization of a semi-multiplicative analogue of planar functions over finite fields

A. Muratović-Ribić, A. Pott, D. Thomson and Q. Wang

ABSTRACT. In this paper, we present a characterization of a semi-multiplicative analogue of planar functions over finite fields. When the field is a prime field, these functions are equivalent to a variant of a doubly-periodic Costas array and so we call these functions Costas. We prove an equivalent conjecture of Golomb and Moreno that any Costas polynomial over a prime field is a monomial. Moreover, we give a class of Costas polynomials over extension fields and conjecture that this class represents all Costas polynomials. This conjecture is equivalent to the conjecture that there are no non-Desarguesian planes of a given type with prime power order.

Generalization or related topics

10000001000000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- Radar arrays
- Sonar arrays
- 2-dimensional dot patterns
- periodic dot patterns
- etc

1000000100000011000010100011110010001011001110101001111101000011100010010011011010110111101100011010010111011100110010101011111111

any questions ??