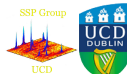


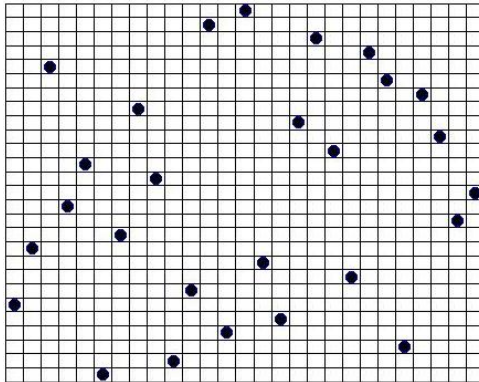
Results of the enumeration of Costas arrays of order 27

Konstantinos Drakakis, Scott Rickard, Rodrigo Caballero,
Francesco Iorio, Gareth O'Brien, John Walsh

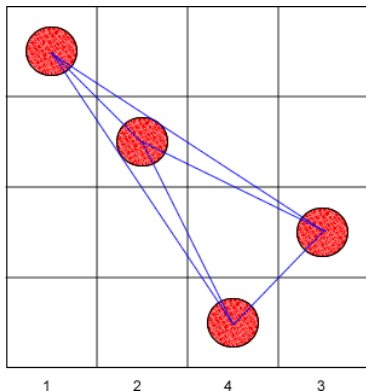
23 May 2008



A Costas array of order 27



Example and definition



Let $[n] = \{1, \dots, n\}$, $f : [n] \rightarrow [n]$;
 f is Costas iff

$$\forall i, j, i', j' \in [n], i > j, i' > j' : \\
(f(i) - f(j), i - j) = (f(i') - f(j'), i' - j') \\
\Leftrightarrow i = i', j = j'$$

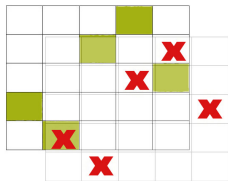
(No 4 dots form a parallelogram – no 3 dots on a straight line are equidistant)

- No two linear segments have the same length and slope!
- Horizontal/vertical flips and transpositions of a Costas array are also Costas arrays: $1 \rightarrow 8$ (or $1 \rightarrow 4$ if symmetric).
 These are equivalence classes (EC) of Costas arrays.



Why Costas arrays?

- Costas array: a time (horizontally)-frequency (vertically) description of a waveform used by a RADAR.
- Received waveform is delayed (distance) and frequency shifted (Doppler effect \rightarrow velocity).
- Cross-correlation: number of overlapping pairs of dots for a given shift between 2 arrays. Here $\Psi_{A,A}(1, 1) = 1$:



- No parallelograms: sidelobes will be of optimally low height (at most 1).



The (exponential) Welch construction $W_1(p, g, c)$

Let p be prime and g a primitive root of the field $\mathbb{F}(p)$; for $c \in \{0, \dots, p-2\}$ constant, we build the permutation

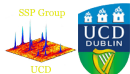
$$f(i) = g^{i-1+c} \pmod{p}, \quad i = 1, \dots, p-1$$

corresponding to a Costas array of order $p-1$. This construction produces $2(p-1)\phi(p-1)$ arrays (along with reflection through the diagonal).

Examples: $W_1(17, 3, 0) \longrightarrow$ 1 3 9 10 13 5 15 11 16 14 8 7 4 12 2 6

By adding and removing corner 1s we obtain the methods W_0 (s), W_1 (ap), W_2 (ap), W_3 (if 2 is a primitive root).

Flips are covered by this formula, but not transpositions: they are the *logarithmic* Welch arrays.



Golomb construction $G_2(p, m, a, b)$

Let p be a prime, $m \in \mathbb{N}$, $q = p^m$ and a, b primitive roots of the field $\mathbb{F}(q)$; we build the permutation f such that

$$a^i + b^{f(i)} = 1, \quad i = 1, \dots, q - 2$$

corresponding to a Costas array of order $q - 2$. The method produces $\frac{\phi^2(q - 1)}{m}$ arrays.

By adding and removing corner 1s (or groups thereof) we obtain the methods $G_0, G_1, G_2, G_3, G_4, G_5$; the conditions are quite involved. The entire family of a Golomb array is obtainable by this formula.



$G(2, 4, x, x + 1)$ when $P(x) = x^4 + x + 1$

0		1	0		1		
1		x	1		$x + 1$	1	1
2		x^2	2		$x^2 + 1$	2	2
3		x^3	3	$x^3 + x^2 + x + 1$		3	11
4		$x + 1$	4		x	4	4
5		$x^2 + x$	5		$x^2 + x$	5	10
6		$x^3 + x^2$	6		$x^3 + x$	6	7
7		$x^3 + x + 1$	7		$x^3 + x^2 + 1$	7	6
8		$x^2 + 1$	8		x^2	8	8
9		$x^3 + x$	9		$x^3 + x^2$	9	13
10		$x^2 + x + 1$	10		$x^2 + x + 1$	10	5
11		$x^3 + x^2 + x$	11		$x^3 + 1$	11	3
12		$x^3 + x^2 + x + 1$	12		x^3	12	14
13		$x^3 + x^2 + 1$	13		$x^3 + x + 1$	13	9
14		$x^3 + 1$	14		$x^3 + x^2 + 1$	14	12



T_4 : an important special case of G_4

- It is occasionally possible for a primitive root of a finite field $\mathbb{F}(p^m)$ to satisfy:

$$a^2 + a = 1.$$

- Then, $f = G_2(p, m, a, a)$ satisfies $f(1) = 2$ and $f(2) = 1$.
- Removing the first two rows and columns of this array leaves what we define as $T_4(p, m, a)$.
- Interesting property: it is always a non-attacking kings configuration!



On the computation

- The computation needed the equivalent of 25 years on a single CPU at 2.00GHz.
- 68.75% of the jobs were run on GridIreland; 14.14% on the University of Edinburgh's BlueGene; 13.30% on UCD's Rowan cluster.
- Code is written in C but also uses assembly calls.
- Code consists of a number of jobs: each job checks all possible permutations starting with a set of pre-specified integers for the Costas property.



On the results

29 ECs of Costas arrays were found; 7 are symmetric:

$22 \cdot 8 + 7 \cdot 4 = 204$ Costas arrays of order 27 in total.

- one is a $T_4(31, 1)$ and is symmetric.
- 6 are $W_2(29, g)$: there are $\phi(28) = 12$ g , grouped in ECs in pairs related by a vertical flip (inverse primitive roots) \longrightarrow 6 such ECs.
- 21 are $G_2(29, 1, a, b)$ for the various choices of primitive roots a and b : there are $\phi(28) = 12$ such primitive roots. $a = b$ produces 12 symmetric arrays, which fall in ECs in pairs \longrightarrow 6 symmetric ECs. The rest (15 ECs) contain 8 arrays each, are not symmetric: $\phi(28)^2 = 144 = 15 \cdot 8 + 6 \cdot 4$.
- One is *sporadic* (not algebraically constructible).
- Of the above, 4 have corner dots: 3 G_2 (one symmetric) and one W_2 .

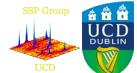
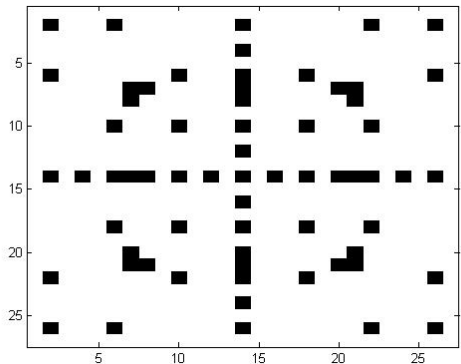
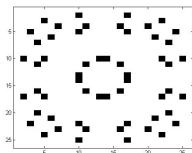
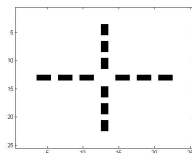


The results

1 3 7 15 2 5 11 23 18 8 17 6 13 27 26 24 20 12 25 22 16 4 9 19 10 21 14	W_2
1 3 19 12 23 5 25 20 10 16 13 27 11 15 2 9 14 8 21 22 18 17 26 6 4 7 24	G_2
1 8 22 18 16 5 23 17 14 19 12 20 26 25 7 10 11 27 3 15 2 21 13 24 9 4 6	G_2
1 25 19 5 4 12 10 16 26 7 18 6 23 27 24 8 21 11 3 22 17 20 13 15 2 9 14	G_2/s
2 3 14 12 21 5 18 20 26 16 4 27 24 15 1 9 19 8 23 22 25 17 10 6 13 7 11	G_2
2 8 26 22 10 3 11 6 20 4 14 15 18 27 25 19 1 5 17 24 16 21 7 23 13 12 9	W_2
2 17 14 12 7 19 18 20 26 16 4 13 24 1 15 23 5 8 9 22 11 3 10 6 27 21 25	G_2
2 20 3 8 23 7 10 5 1 9 13 22 21 27 18 16 4 25 14 15 17 11 24 6 26 12 19	G_2
2 20 17 8 9 21 10 19 15 23 27 22 7 13 18 16 4 11 14 1 3 25 24 6 26 12 5	G_2
2 24 16 4 14 7 5 13 12 1 6 18 27 3 22 8 19 9 15 11 26 23 25 10 17 20 21	G_2
2 24 16 4 14 21 19 27 12 15 6 18 13 17 22 8 5 23 1 25 26 9 11 10 3 20 7	G_2
2 25 8 13 3 23 12 5 19 20 18 22 14 1 27 4 21 16 26 6 17 24 10 9 11 7 15	W_2
3 9 1 8 13 15 19 4 2 20 11 25 5 17 6 27 14 24 7 10 26 23 22 18 12 21 16	G_2/s
3 15 6 10 18 8 9 2 13 19 21 26 11 25 12 7 5 27 16 23 22 4 24 20 1 17 14	W_2
3 17 6 19 18 16 22 26 20 27 11 12 5 23 14 2 10 7 9 24 1 4 15 25 21 13 8	G_2
3 24 10 26 20 15 13 23 14 1 8 4 22 19 21 2 5 25 9 17 6 7 11 16 27 12 18	G_2/s
4 3 7 23 25 16 11 12 15 21 26 22 14 1 27 20 9 17 24 6 18 8 2 13 10 19 5	G_2
4 7 24 22 2 25 10 6 21 20 14 5 26 27 3 15 1 12 18 8 17 9 19 16 23 11 13	G_2
4 17 21 9 11 16 25 12 1 7 26 22 14 15 13 20 23 3 24 6 18 8 2 27 10 5 19	G_2/s
5 13 11 25 20 4 22 24 18 7 6 2 3 23 8 12 21 27 15 26 1 16 9 19 10 17 14	G_2
5 15 11 4 3 25 13 16 22 24 9 23 27 19 10 17 14 12 21 26 6 1 18 2 20 7 8	G_2
5 21 11 18 2 23 19 10 13 24 1 27 3 17 16 25 12 20 22 4 26 15 7 8 14 9 6	G_2
5 25 10 26 2 4 15 22 3 13 7 6 9 23 20 21 27 17 8 1 18 16 12 24 11 19 14	W_2
6 10 23 13 16 1 11 20 15 2 7 26 4 27 9 5 19 25 17 8 24 22 3 21 18 12 14	T_4/s
6 16 20 12 14 7 1 25 8 17 18 26 11 23 10 24 15 13 3 19 22 27 5 2 9 4 21	G_2
6 16 20 12 14 21 15 11 8 3 18 26 25 9 10 24 1 27 17 5 22 13 19 2 23 4 7	G_2/s
6 23 14 8 21 1 26 4 22 20 12 11 16 3 17 13 15 24 27 10 5 9 2 18 25 7 19	G_2/s
7 5 18 6 26 12 16 19 14 3 2 23 17 27 20 22 9 21 1 15 11 8 13 24 25 4 10	W_2
11 10 4 24 7 23 3 18 21 9 26 16 5 1 15 27 2 25 17 22 19 6 8 12 20 13 14	



Forbidden positions



Future work

Assuming all 768 processors of GridIreland were used exclusively for the project:

- 27 could have been completed in 1 week and 5 days;
- 28 will need 8.5 weeks (still doable);
- 29 will need just above 42 weeks (still doable?);
- 30 will need about 212 weeks, just above 4 years (way too much).

