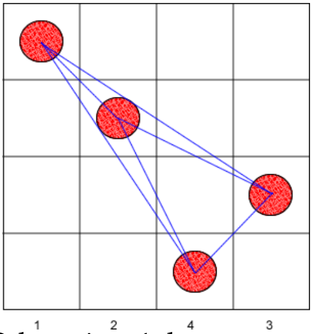
An introduction to Costas arrays

Konstantinos Drakakis

UCD CASL/Electronic & Electrical Engineering
University College Dublin

03 November 2010

Example and definition [Costas (1984)]



Let $[n] = \{1, \ldots, n\}$, $f : [n] \to [n]$ (order n); f is Costas (bijection) iff

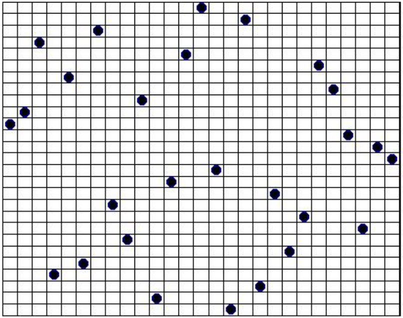
$$\forall i, j \in [n],\ k > 0 :\ i+k, j+k \in [n]$$
$$(f(i+k) - f(i), k) = (f(j+k) - f(j), k)$$
$$\Leftrightarrow i = j$$

(On a straight line: 4 dots cannot form 2 pairs of equidistant dots, 3 dots cannot be equidistant.

Otherwise: 4 dots cannot form a parallelogram)

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

A larger example



The only sporadic Costas array of order 27.

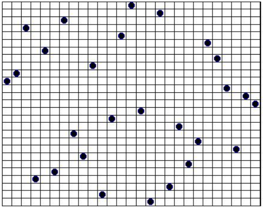
Cross-correlation

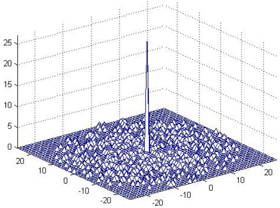
Let f/A_f and g/A_g be permutations/permutation arrays of order n. Their cross-correlation is:

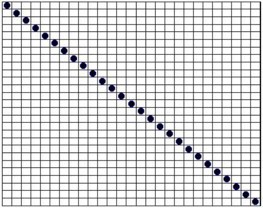
$$\Psi_{f,g}(u,v) = \sum_{i=1}^{n} [f(i-u)+v = g(i)] = \sum_{i,j} a^f_{i-u,j-v} a^g_{ij},$$

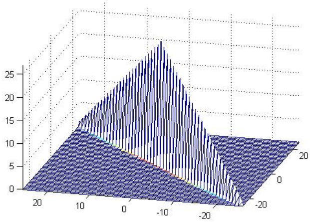
where $[P] = 1/0$ if P is true/false; also assume $f(i) = g(i) = 0$ if $i < 1$ or $i > n$.
In other words, superpose A^f on A^g, slide it by u columns to the right and by v rows downwards and count how many pairs of dots coincide.
If f is a permutation of order n, f is Costas iff $\Psi_{f,f}$ only takes the 3 values $0, 1, n$.

Why Costas arrays?









Aside: Why a permutation?

- [Costas (1984)] states that the original application does not benefit by a violation of the permutation condition.
- Beyond that, no reason!
- Mathematically, permutations are easier to handle and to construct than general binary arrays.
- What is the maximal number of dots that can be placed on a $n \times n$ grid without violating the Costas property?

The difference triangle [Chang (1987), Barker-Drakakis-Rickard (2009)]

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

-4 12 -14 10 -5 -2 5 7 2 -8 -10 17 -3 -12 11 6 -11 -9 13 -7

8 -2 -4 5 -7 3 12 9 -6 -18 7 14 -15 -1 17 -5 -20 4 6

-6 8 -9 3 -2 10 14 1 -16 -1 4 2 -4 5 6 -14 -7 -3

4 3 -11 8 5 12 6 -9 1 -4 -8 13 2 -6 -3 -1 -14

-1 1 -6 15 7 4 -4 8 -2 -16 3 19 -9 -15 10 -8

-3 6 1 17 -1 -6 13 5 -14 -5 9 8 -18 -2 3

2 13 3 9 -11 11 10 -7 -3 1 -2 -1 -5 -9

9 15 -5 -1 6 **8 -2 4** 3 -10 -11 12 -12

11 7 -15 **16 3 -4 9 10 -8** -19 2 5

3 **-3 2 13 -9 7 15 -1 -17 -6** -5

-7 14 -1 1 2 13 4 -10 -4 -13

10 11 -13 12 8 2 -5 3 -11

7 -1 -2 18 -3 -7 8 -4

-5 10 4 7 -12 6 1

6 16 -7 -2 1 -1

12 5 -16 11 -6

1 -4 -3 4

-8 9 -10

5 2

-2

Aside: Complexity considerations

- A permutation of order n is Costas iff no row of the difference triangle contains repeated entries, so

$$\binom{n-1}{2} + \binom{n-2}{2} + \ldots + \binom{2}{2} = \sum_{k=0}^{n-1} \binom{k}{2} = \binom{n-1}{3}$$

  comparisons need to be carried out.
- Polynomial complexity: $O(n^3)$ comparisons.
- There is no known fast way to discover Costas permutations of order n, except for brute-force search.
- Exponential complexity: $n!$ objects.
- So, existence of Costas arrays is in NP; but is it NP complete?

Important basic open problems

(Note: the numbers below refer to the list of problems in [Golomb-Taylor (1984)].)
For order n, let $C(n)$ be the number of Costas arrays and $c(n)$ the number of equivalence classes of Costas arrays.

1. $C(n) \geq 1$ for all $n \geq 1$.

4.+6. $C(n)/n!$ is monotonically decreasing to 0. [It is known [Drakakis (2006)] that $C(n)/n! = O(1/n)$.]

7. $C(n)/c(n) \to 8$ as $n \to \infty$.

10. Are there Costas arrays representing configurations of non-attacking queens?

New. Can all Costas arrays be "systematically" constructed?

New. Are there Costas arrays of order 32 or 33 (the smallest orders where none is currently known)?

Known Costas arrays

- All Costas arrays of order $n \leq 28$ (through exhaustive search) [Drakakis et al. (2010), Drakakis et al. (2008), Rickard et al. (2006), Beard et al. (2007)].
- Two construction algorithms (Golomb and Welch) working for infinitely many (but not all) orders [Golomb (1984), Golomb-Taylor (1984)].
- Four additional equivalence classes of Costas arrays, of orders 29(2), 36 and 42 [Rickard (2004)].

Any Costas array belonging in the first set but not in the second or third is characterized as *sporadic*.

Aside: The mystery of sporadic Costas arrays

- Definitely the vast majority in "small" orders: for example, only 16 out of the 10240 known Costas arrays of order 19 are not sporadic!
- Almost die out later: only 2 sporadic equivalence classes of order 26 are known, 1 of 27, and 0 of 28...
- Do sporadic Costas arrays eventually die out?
- Are there unknown constructions that can account for sporadic Costas arrays?

Number of known Costas arrays

1	1	10	2160/28	19	10240/12	28	712/0
2	2	11	4368/36	20	6464/8	29	$\geq$ 164/10
3	4	12	7852/34	21	3536/16	30	$\geq$ 664/8
4	12/2	13	12828/50	22	2052/10	31	$\geq$ 8/0
5	40/4	14	12752/46	23	872/20	32	?
6	116/10	15	19612/62	24	200/0	33	?
7	200/20	16	21104/40	25	88/4		
8	444/18	17	18276/38	26	56/4		
9	760/20	18	15096/20	27	204/14		

The exponential Welch construction $W_1(p, \alpha, c)$

Let p be prime, α a primitive root of the field $\mathbb{F}(p)$, and $c \in \{0, \ldots, p-2\}$; then,

$$f(i) = \alpha^{i-1+c} \bmod p, \; i = 1, \ldots, p-1$$

is a Costas permutation of order $p-1$.

- $\phi(p-1)$ choices for α, $p-1$ for $c \longrightarrow (p-1)\phi(p-1)$ distinct permutations.
- Flips of $W_1(p, \alpha, c)$ are also of this form, possibly for different α, c.
- For $p > 5$, transposes of $W_1(p, \alpha, c)$ form a disjoint set [Drakakis-Gow-O'Carroll (2009)]: they are known as logarithmic Welch arrays.
- In total, there are $2(p-1)\phi(p-1)$ arrays in this family.

Proof

Let $i, j, i+k, j+k \in [p-1]$:

$$\begin{aligned} f(i+k)-f(i) = f(j+k)-f(j) \Rightarrow \\ f(i+k)-f(i) \equiv f(j+k)-f(j) \bmod p \Leftrightarrow \\ \alpha^{i+k}-\alpha^{i} \equiv \alpha^{j+k}-\alpha^{j} \bmod p \Leftrightarrow \\ (\alpha^{i}-\alpha^{j})(\alpha^{k}-1) \equiv 0 \bmod p \Leftrightarrow \\ i \equiv j \bmod (p-1) \text{ or } k \equiv 0 \bmod (p-1) \Leftrightarrow \\ i = j \text{ or } k = 0. \end{aligned}$$

The last step follows because of the range i, j, k lie in.

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

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

Note the *anti-reflective symmetry*:

$6+11=2+15=12+5=\ldots=17.$

c circularly shifts columns: W_1 Costas arrays are *singly periodic*.

Aside: Inverse problems

- Anti-reflective symmetry does not characterize W_1!
- Does single periodicity characterize W_1? Most likely, but still not formally proved!

In general:

- Problem: show that Costas arrays in a certain collection have a certain property.
- Inverse problem: show that all Costas arrays having a certain property must belong in a certain collection.

Inverse problems are very hard!

Derived methods

- $W_1(p,\alpha,0)$ begins with 1 (corner dot): removing it yields a new Costas permutation $W_2(p,\alpha)$ of order $p-2$:
  $W_2(17,3) \longrightarrow$ 2 8 9 12 4 14 10 15 13 7 6 3 11 1 5
- If 2 is a primitive root of $\mathbb{F}(p)$, $W_1(p,2,0)$ begins with 1 2 (two corner dots): removing them yields a new Costas permutation $W_3(p)$ of order $p-3$.
- Adding a corner dot to $W_1(p,\alpha,c)$ may lead to a new Costas array $W_0(p,\alpha,c)$ of order p.

Golomb construction $G_2(p^m, \alpha, \beta)$

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

$$\alpha^i + \beta^{f(i)} = 1,\ i = 1, \ldots, q-2$$

is a Costas permutation of order $q - 2$.

- $\phi(q-1)$ choices for $\alpha, \beta \longrightarrow \phi^2(q-1)/m$ distinct permutations: if $\alpha^i + \beta^{f(i)} = 1$, then, for $k = 0, \ldots, m-1$, $1 = (\alpha^i + \beta^{f(i)})^{p^k} = (\alpha^{p^k})^i + (\beta^{p^k})^{f(i)}$.
- Flips and transposes of $G_2(p^m, \alpha, \beta)$ are also of this form, possibly for different α, β.
- There are two subfamilies of symmetric arrays [Drakakis-Gow-O'Carroll (2009)]: i) $\alpha = \beta$ (Lempel Costas arrays); ii) $q = r^2$ and $\beta = \alpha^r$.
- The main diagonal of the latter construction is an asymptotically optimally dense Golomb ruler, equivalent to the Bose-Chowla construction [Drakakis (2009)].

Proof

Let $i, j, i+k, j+k \in [q-2]$:

$$f(i+k) - f(i) = f(j+k) - f(j) \Rightarrow$$
$$f(i+k) - f(i) \equiv f(j+k) - f(j) \bmod (q-1) \Leftrightarrow$$
$$\beta^{f(i+k)-f(i)} = \beta^{f(j+k)-f(j)} \Leftrightarrow$$
$$\frac{1-\alpha^{i+k}}{1-\alpha^{i}} = \frac{1-\alpha^{j+k}}{1-\alpha^{j}} \Leftrightarrow$$
$$(\alpha^k - 1)(\alpha^i - \alpha^j) = 0 \Leftrightarrow$$
$$i \equiv j \bmod (q-1) \text{ or } k \equiv 0 \bmod (q-1) \Leftrightarrow$$
$$i = j \text{ or } k = 0.$$

The last step follows because of the range i, j, k lie in.

An example of a Golomb construction

$q = 16 = 2^4$, $P(x) = x^4 + x + 1$, $a = x$, $b = x + 1 = x^4$

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

This is a non-Lempel symmetric Costas permutation with 4 fixed points.

Derived methods

- Let $\alpha + \beta = 1$: this is possible in any finite field [Cohen-Mullen (1991)]; then, $G_2(p^m, \alpha, \beta)$ has a corner dot, and, removing it, yields a new Costas permutation $G_3(p^m, \alpha)$ of order $q - 3$.
- Derived Golomb Costas permutations of order $q - 4$ are possible through three different techniques:
  - G_4 Assuming G_3 and $p = 2$, it follows that $(\alpha + \beta)^2 = \alpha^2 + \beta^2 = 1$; then, $G_2(2^m, \alpha, \beta)$ begins with 1 2 (has two corner dots), so, removing them, yields $G_4(2^m, \alpha)$.
  - G_4^* Assuming $p > 2$, G_3, and $\alpha^2 + \beta^{-1} = 1$, $G_2(p^m, \alpha, \beta)$ begins with 1 $q - 2$ and has 2 corner dots: removing them yields $G_4^*(p^m, \alpha)$.
  - T_4 Assuming $p > 2$, $\alpha = \beta$, and $\alpha^2 + \alpha = 1$, $G_2(p^m, \alpha, \alpha)$ begins with 2 1 and has a 2×2 corner array: removing it yields $T_4(p^m, \alpha)$.

- Assume G_4^*: it always follows that $\alpha^{-1} + \beta^2 = 1$, so that $G_2(p^m, \alpha, \beta)$ begins with 1 $q-2$ and ends with 2, so that it has 3 corner dots: removing them yields $G_5^*(p^m, \alpha)$ of order $q-5$.
- Adding one or two anti-diametrical corner dots to $G_2(p^m, \alpha, \beta)$ may lead to a Costas array of order $q-1$ or q, respectively: these are $G_1(p^m, \alpha, \beta)$ and $G_0(p^m, \alpha, \beta)$.

Note the following:

- T_4 Costas arrays represent configurations of non-attacking kings on the chessboard [Drakakis-Gow-Rickard (2009)].
- Let f be a G_2 Costas permutation for $p > 2$: then [Drakakis (2010+)], for $\mu = (q-1)/2$ and $i \in [\mu - 1]$,

$$f(\mu + i) - f(\mu - i) \equiv i\,[f(\mu + 1) - f(\mu - 1)] \bmod (q-1).$$

This is an analog of the anti-reflective symmetry.

Welch Rickard construction

- The proof of W_1 construction shows that these permutations satisfy a stricter version of the Costas property (modulo p).
- Add a blank row at the bottom, and circularly shift the rows any number of times. The resulting $p \times (p-1)$ rectangle has the Costas property.
- Add a blank column, either to the left or to the right, and place a dot at the intersection of the blank row and column.
- The result is a permutation array which may have the Costas property.

Golomb Rickard construction

- The proof of G_2 construction shows that these permutations satisfy a stricter version of the Costas property (modulo $q-1$).
- Add a blank row at the bottom and a blank column at the right, and circularly shift the rows and columns any number of times. The resulting $(q-1)\times(q-1)$ rectangle has the Costas property.
- Place a dot at the intersection of the blank row and column.
- The result is a permutation array which may have the Costas property.

Aside: Reinventing the wheel (and failing)

Can known Costas arrays be combined into larger new Costas arrays? Not in an "obvious" way! For example, letting $A = [a]$, $B = [b]$ be Costas arrays whose orders exceed 3:

- The following composite array seems to never be Costas:

$$\begin{matrix} A & 0 \\ 0 & B \end{matrix}$$

- The following "interlaced" array is never Costas:

$$\begin{matrix} a & 0 & a & 0 & \dots \\ 0 & b & 0 & b & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{matrix}$$

The reason is that any two Costas arrays of orders either equal or differing by 1 (and the smallest exceeding 3) have a common distance vector [Drakakis-Gow-Rickard (2008)].

Aside: Common distance vectors

- To disqualify composite Costas arrays, one needs to establish that any two "large" Costas arrays have a common distance vector.
- [Drakakis-Gow-Rickard (2009)] attempted to investigate this, but only for Welch and Golomb Costas arrays.
- Bottom line: there is no proof yet that composition is futile, though, in practice, it works when the order of A is 1 or 2 (when it is 3, the last successful case is for $n = 7$).

Aside: How close to interlacing do Costas arrays come? [Drakakis-Gow-Rickard (2007)]

- Define parity populations ee, oo, eo, oe to stand for the number of dots whose coordinates are both even, both odd, and of mixed parity, respectively.
- $ee + oo + eo + oe = n$, $eo = oe$,
  $oo + oe - (eo + ee) = oo - ee = n \bmod 2$: need a 4th equation.
- For G_2 Costas arrays with $p > 2$:
  - If $q \equiv 1 \bmod 4$, $oo = eo = oe = (q-1)/4$, $ee = (q-5)/4$;
  - If $q \equiv 3 \bmod 4$, $ee = eo = oe = (q-3)/4$, $ee = (q+1)/4$;
- For W_1 Costas arrays:
  - If $p \equiv 1 \bmod 4$, $oo = eo = oe = ee$;
  - If $p \equiv 3 \bmod 4$, then $|ee - oe| = h(-p)$ if $p \equiv 7 \bmod 8$, and $|ee - oe| = 3h(-p)$ if $p \equiv 3 \bmod 8$.

In particular, parity populations are only dependent on p and q; this is no longer true for G_2 with $p = 2$.

Future directions

Enumeration:

- Enumeration of order 29 projected to require 350 years of CPU time!
- Complexity of current enumeration algorithm increases 5 times whenever order increases by 1.
- Realistically, order 30 is the last one within reach today…

Genetic algorithms:

- "Mutate" random permutations into Costas ones.
- Current algorithms fail for "large" orders (20 or above).
- Problem: the structure of Costas arrays is very tight. It seems that, for any large order n, i, j, k exist such that the values $f(i), f(j), f(k)$ determine at most one Costas permutation! [Drakakis (2010)]

Classification (finite simple groups style!)

Known Costas arrays seem to fall into 4 categories:

- Generated (G): they are constructed by an algorithm whose applicability is determined by a sufficient condition involving the order alone (W_1, W_2, G_2, G_3, G_4).
- Predictably emergent (PE): they are constructed by an algorithm whose applicability can be asserted by a condition involving the order and some additional parameters (W_3, G_4^*, T_4, G_5^*).
- Unpredictably emergent (UE): they are heuristically constructed and the Costas property has to be explicitly checked (W_0, G_0, G_1, Welch Rickard, Golomb Rickard).
- Sporadic (S): of unknown origin.

Up to order 300, the last Rickard Costas arrays are the ones reported, while the last G_1 and W_0 Costas arrays were found in orders 52 and 53, respectively. UE seem to die out!

- J.P. Costas. “A study of detection waveforms having nearly ideal range-doppler ambiguity properties.” Proceedings of the IEEE, Volume 72, Issue 8, pp. 996–1009, Aug 1984.
- S.W. Golomb. “Algebraic constructions for Costas arrays.” Journal of Combinatorial Theory Series A, Volume 37, 1984, pp. 13–21.
- S.W. Golomb and H. Taylor. “Constructions and properties of Costas arrays.” Proceedings of the IEEE, Volume 72, Issue 9, Sep 1984, pp. 1143–1163.
- W. Chang. “A remark on the definition of Costas arrays.” Proceedings of the IEEE, Volume 75, Issue 4, Apr 1987, pp. 522–523.
- J. Silverman, V. Vickers, and J. Mooney. “On the Number of Costas arrays as a function of array size.” Proceedings of the IEEE, Volume 76, Issue 7, Jul 1988, pp. 851–853.

S. Rickard. “Searching for Costas arrays using periodicity properties.” IMA International Conference on Mathematics in Signal Processing at The Royal Agricultural College, Cirencester, UK, December 2004.

K. Drakakis. “A review of Costas arrays.” Journal of Applied Mathematics, Volume 2006.

- K. Drakakis, R. Gow, and S. Rickard. "Parity properties of Costas arrays defined via finite fields." Advances in Mathematics of Communications **[0.97]**, Volume 1, Issue 3, August 2007, pp. 323–332.
- K. Drakakis, S. Rickard, and R. Gow. "Interlaced Costas arrays do not exist." Mathematical Problems in Engineering, Volume 2008.
- K. Drakakis, R. Gow, and S. Rickard. "Common distance vectors between Costas arrays." Advances in Mathematics of Communications, Volume 3, Issue 1, February 2009, pp. 35–52.
- K. Drakakis, R. Gow, and L. O'Carroll. "On the symmetry of Welch- and Golomb-constructed Costas arrays." Discrete Mathematics, Volume 309, Issue 8, Apr 2009, pp. 2559–2563.

- K. Drakakis. “A review of the available construction methods for Golomb rulers.” Advances in Mathematics of Communications, Volume 3, Issue 3, Aug 2009, pp. 235–250.
- L. Barker, K. Drakakis, and S. Rickard. “On the complexity of the verification of the Costas property.” Proceedings of the IEEE, Volume 97, Issue 3, Mar 2009, pp. 586–593.
- K. Drakakis. “Some results on the degrees of freedom of Costas arrays.” IEEE CISS 2010.
- K. Drakakis. “A structural constraint for Golomb Costas arrays.” (accepted for publication in) IEEE Transactions on Information Theory.

K. Drakakis, F. Iorio, and S. Rickard. “The enumeration of Costas arrays of order 28.” IEEE ITW 2010.

K. Drakakis, S. Rickard, J. Beard, R. Caballero, F. Iorio, G. O’Brien, and J. Walsh. “Results of the enumeration of Costas arrays of order 27.” IEEE Transactions on Information Theory, Volume 54, Issue 10, October 2008, pp. 4684–4687.

S. Rickard, E. Connell, F. Duignan, B. Ladendorf, and A. Wade. “The enumeration of Costas arrays of size 26.” IEEE CISS 2006.

J.K. Beard, J.C. Russo, K.G. Erickson, M.C. Monteleone, and M.T. Wright. “Costas arrays generation and search methodology.” IEEE Transactions on Aerospace and Electronic Systems, Volume 43, Issue 2, Apr 2007, pp. 522–538.

S. Cohen and G. Mullen. "Primitive elements in finite fields and Costas arrays." Applicable Algebra in Engineering, Communication and Computing, Volume 2, Issue 1, Mar 1991, pp. 45–53.