Advances in Costas arrays

Konstantinos Drakakis

UCD CASL/Electronic & Electrical Engineering
University College Dublin

10 November 2010

Part 1: Cross-correlation

[Drakakis et al. (2011?)]

Cross-correlation results

We obtained these values for $\max\limits_{A \overset{*}{\neq} B} \max\limits_{(u,v)} \Psi_{A,B}(u,v)$ when A, B are both either W_1 or G_2 Costas arrays:

Prime	W_1	G_2	Prime	W_1	G_2	Prime	W_1	G_2
5	2	2	59	5	12	127	42	41
7	2	2	61	30	29	131	26	25
11	3	4	67	22	21	136	68	67
13	6	5	71	14	13	139	46	45
17	8	7	73	36	35	149	74	73
19	6	6	79	26	25	151	50	49
23	4	6	83	5	9	157	78	77
29	14	13	89	44	43	163	54	53
31	10	9	97	48	47	167	6	12
37	18	17	101	50	49	173	86	85
41	20	19	103	34	33	179	6	12
43	14	13	107	5	10	181	90	89
47	5	8	109	54	53	191	38	37
53	26	25	113	56	55	193	96	95

Cross-correlation results – in color

Prime	W_1	G_2	Prime	W_1	G_2	Prime	W_1	G_2
5	2	2	59	5	12	127	42	41
7	2	2	61	30	29	131	26	25
11	3	4	67	22	21	136	68	67
13	6	5	71	14	13	139	46	45
17	8	7	73	36	35	149	74	73
19	6	6	79	26	25	151	50	49
23	4	6	83	5	9	157	78	77
29	14	13	89	44	43	163	54	53
31	10	9	97	48	47	167	6	12
37	18	17	101	50	49	173	86	85
41	20	19	103	34	33	179	6	12
43	14	13	107	5	10	181	90	89
47	5	8	109	54	53	191	38	37
53	26	25	113	56	55	193	96	95

A plausible conjecture

Conjecture

Let A, B be either both W_1 Costas arrays (not related by a shift) or both G_2 Costas arrays built in $\mathbb{F}(p)$, where $p \neq 19$ is a prime such that $\frac{p-1}{2}$ is not a prime (i.e. p is not a safe prime); then,

$$\max_{(u,v)} \max_{A \neq B} \Psi_{A,B}(u,v) = \max_{A \neq B} \Psi_{A,B}(0,0)$$

The central theorems

Theorem

Let A, B be distinct exponential W_1 Costas arrays built in $\mathbb{F}(p)$ not related by a shift; then,

$$\max_{A \neq B} \Psi_{A,B}(0,0) = \frac{p-1}{r}$$

where r is the smallest prime such that $p \equiv 1 \bmod (2r)$.

Theorem (almost!)

Let A', B' be distinct G_2 Costas arrays built in $\mathbb{F}(p)$, sharing a common primitive root; then,

$$\max_{A' \neq B'} \Psi_{A',B'}(0,0) = \frac{p-1}{r} - 1,$$

where r is the smallest prime such that $p \equiv 1 \bmod (2r)$.

Proof sketch

- Let A, B be exponential W_1 Costas arrays generated by α and α^z, $\alpha \in \mathbb{F}(p)$ a primitive root, $(z, p-1) = 1$, and by constants c and d, respectively. We need the number of solutions of:

$$\alpha^{i-1+c} \equiv \alpha^{z(i-1+d)} \bmod p \Leftrightarrow (z-1)(i-1+d) \equiv c-d \bmod (p-1)$$

- The number of roots is independent of the exact value of $c-d$: it is $(z-1, p-1)$ if $z-1|c-d$ and 0 otherwise.
- It suffices to consider the number of roots of $(z-1)x \equiv 0 \bmod (p-1)$, which is necessarily a divisor of $p-1$.

- The maximum number of solutions possible is $\frac{p-1}{2}$: we need $(z-1, p-1) = \frac{p-1}{2} \Leftrightarrow z = \frac{p+1}{2}$, assuming it is admissible:
- $(z, p-1) = 1 = \left(\frac{p+1}{2}, p-1\right) = \left(\frac{p+1}{2}, 2\right)$, since $2 | p-1$, hence we need $2 \nmid \frac{p+1}{2} \Leftrightarrow p \equiv 1 \bmod 4$.

- Henceforth, assume $p \equiv 3 \bmod 4$, and let w be a prime such that $p \equiv 1 \bmod (2w)$.
- It can be easily shown that $z = \lambda \dfrac{p-1}{w} + 1$, $\lambda \in [w-1]$, is always admissible for $\lambda = 1$ or 2:
  - Let $p = 1 + wk$:$(\lambda(p-1)/w + 1, p-1) = (\lambda k + 1, wk)$; unless $w|\lambda k + 1$, this equals $(\lambda k + 1, k) = (1, k) = 1$.
  - Assuming $w|k+1$ and $w|2k+1$, then $w|k$, so $w|1$, a contradiction; so, either $\lambda = 1$ or $\lambda = 2$ is enough.
  - When is $\lambda = 2$ needed? When $w|k+1$, $k = lw - 1$ for some l, so that $p = 1 + (lw-1)w = lw^2 - w + 1 \leftrightarrow p \equiv w^2 - w + 1 \bmod w^2$.
- Hence, for any prime $w > 2$ there exists a z such that the congruence $(z-1)x \equiv 0 \bmod (p-1)$ has $\dfrac{p-1}{w}$ roots: clearly, this is maximum for $w = r$.

- Let A, B be G_2 Costas arrays built in $\mathbb{F}(p)$, generated by α, β, and α^r, β^s, respectively, where $(r, p-1) = (s, p-1) = 1$.
- We need the number of solutions (i, j) of

  $$\alpha^i + \beta^j = 1, \alpha^{ri} + \beta^{sj} = 1,\ i, j = 1, \ldots, p-2 \Leftrightarrow (1-x)^r + x^s = 1,$$

  where $x = \beta^j \neq 1$.
- Assuming $s = 1$, $(1-x)^{r-1} = 1 \Leftrightarrow (r-1)y = 0 \bmod (p-1)$, where $1 - x = \alpha^y$. This is the same equation as before, except that $x \neq 0 \Leftrightarrow y \neq 0$, so $y = 0$ is rejected.
- Note that a conjecture has been made: the largest number of roots occurs for $s = 1$. This remains open.

Prime power	G_2
4	1
8	3
9	3
16	5
25	11
27	6
32	6
49	23
64	20
81	39
121	59
125	61
128	9
169	83
243	21
256	84

Extension to prime powers for G_2 Costas arrays

The results and conjectures for G_2 Costas arrays above extend verbatim to extension fields, with some caveats:

- For odd powers, the notion of a safe prime power needs to be introduced (e.g. $27 = 1 + 2 \cdot 13$).
- 16 is an exception analogous to 19.
- Even powers q lead to a new phenomenon: $q - 1$ may be a Mersenne prime.

Polynomials

Consider the polynomials $P_{r,s}(x)=(1-x)^r+x^s-1$ in $\mathbb{F}(q)$, such that $(r,q-1)=(s,q-1)=1$, and let $Z_{r,s}$ denote the number of roots of $P_{r,s}$.

- Conjecture: $\max_{r,s} Z_{r,s}=\max_r Z_{r,1}$.
- Fact: $Z_{r,r}\leq (q+1)/2$ (to be proved later).
- $P_{r,r}:=P_r$ is very interesting algebraically.

An algebraically interesting case

For $p > 2$, the set of roots of the polynomial $P_r(x) := P_{r,r}(x) = (1-x)^r + x^r - 1$ remains invariant under two transforms:

- If x is a root, $S(x) = 1 - x$ is also a root.
- If $x \neq 0$ is a root, $R(x) = 1/x$ is also a root (note r odd).

R and S generate a group of 6 elements (observe that $R^2 = S^2 = I$):

$$Ix = x,\ Sx = 1 - x,\ Rx = 1/x,\ SRx = (x-1)/x,$$
$$RSx = 1/(1-x), RSRx = x/(x-1).$$

The orbit of x consists of 6 elements except for:

$$O_1 = \{0, 1\},\ O_2 = \{1/2, 2, -1\},\ \text{and } O_u = \{u, 1/u\}$$

such that $u^2 - u + 1 = 0$.

For p=2, $P_r(x) = (1+x)^r + x^r + 1$, and its set of roots remains invariant under $S(x) = 1 + x$ and $R(x) = 1/x$. The orbit of x is

$$Ix = x,\ Sx = 1+x,\ Rx = 1/x,\ SRx = (x+1)/x,$$
$$RSx = 1/(1+x), RSRx = x/(x+1),$$

and consists of 6 elements except for:

$$O_1 = \{0, 1\} \text{ and } O_u = \{u, 1/u\}$$

such that $u^2 + u + 1 = 0$.

Two related notes

- Assuming $r = pm$,

$$P_r(x) = (1-x)^{pm} + x^{pm} - 1 = [(1-x)^m + x^m - 1]^p :$$

  Root multiplicities of P_r are p times root multiplicities of P_m.
- For all p, unless $p|r$, 0 and 1 are single roots.

More on u

Theorem

For $p > 2$, assuming $6|q-1$ and that $p \not| r$, u is a single root, double root, or no root of P_r, according to whether $6|r+1$, $6|r-1$, or otherwise (equivalently, $r \equiv 5,\ 1,$ or $3 \bmod 6$), respectively. If, in addition, $p|r-1$, the former double root case leads now to higher multiplicity.

- Note: in finite fields, derivatives of non-constant polynomials can be identically 0!!!
- Note first that $u^2 - u + 1 = 0 \Leftrightarrow u + 1/u = 1 \Rightarrow u^3 = -1 \Rightarrow u^6 = 1.$
- Since $u^{q-1} = 1$, it follows that, if u is a root of P_r, $6|q-1$.
- u is a root of P_r iff $(1-u)^r + u^r = 1$, hence $0 = (-u^2)^r + u^r - 1 = -(u^r)^2 + u^r - 1$, whence both u^r and u are roots of $x^2 - x + 1$.
- Either then $u^r = u \Leftrightarrow u^{r-1} = 1$ or $u^r = 1/u \Leftrightarrow u^{r+1} = 1$; equivalently, either $6|r-1$ or $6|r+1$.

- $P_r'(x) = r[x^{r-1} - (1-x)^{r-1}] \Rightarrow P_r'(u) = 0$ iff either $p|r$ or $u^{r-1} = (1-u)^{r-1}$.
- u is then (at least) a double root of P_r iff $(1-u)^r + u^r = 1$, $u^{r-1} = (1-u)^{r-1}$, which is equivalent to $(1-u)^{r-1} = u^{r-1} = 1$; as $u^6 = 1$ too, $6|r-1$ and hence $6|(r-1, q-1)$ (but remember that $(r, q-1) = 1$ as well).
- u is (at least) a triple root iff, additionally, $P_r''(u) = r(r-1)[(1-u)^{r-2} + u^{r-2}] = r(r-1)[(1-u)^{-1} + u^{-1}] = r(r-1)[u + u^{-1}] = r(r-1) = 0$ as well. This occurs iff either $p|r$ (uninteresting) or $p|r-1$.

Theorem

For $p = 2$, assuming $3|q-1$ and that $2 \not| r$ (r odd), u is a single root, at least a triple root, or no root of P_r, according to whether $3|r+1$, $3|r-1$, or otherwise (equivalently, $r \equiv 2,\ 1,$ or $0 \bmod 3$), respectively.

- Note first that $u^2 + u + 1 = 0 \Leftrightarrow u + 1/u = 1 \Rightarrow u^3 = 1$.
- Since $u^{q-1} = 1$, it follows that, if u is a root of P_r, $3|q-1$.
- u is a root of P_r iff $(1+u)^r + u^r = 1$, hence $0 = (u^2)^r + u^r + 1 = (u^r)^2 + u^r + 1$, whence both u^r and u are roots of $x^2 + x + 1$.
- Either then $u^r = u \Leftrightarrow u^{r-1} = 1$ or $u^r = 1/u \Leftrightarrow u^{r+1} = 1$; equivalently, either $3|r-1$ or $3|r+1$.

- $P_r'(x) = r[x^{r-1} + (1+x)^{r-1}] \Rightarrow P_r'(u) = 0$ iff either $2|r$ (rejected) or $u^{r-1} = (1+u)^{r-1}$.
- u is then (at least) a double root of P_r iff $(1+u)^r + u^r = 1$, $u^{r-1} = (1+u)^{r-1}$, which is equivalent to $(1-u)^{r-1} = u^{r-1} = 1$; as $u^3 = 1$ too, $3|r-1$ and hence $3|(r-1, q-1)$.
- u is (at least) a triple root iff, additionally, $P_r''(u) = r(r-1)[(1-u)^{r-2} + u^{r-2}] = r(r-1)[(1-u)^{-1} + u^{-1}] = r(r-1)[u + u^{-1}] = r(r-1) = 0$ as well. As $2|r-1$, this always occurs.

$Z_{r,r} \leq (q+1)/2$: a proof (by J. Sheekey)

- Let $P_{r,r}(x) = P_{r,r}(y) = 0$: then $\frac{x}{y}$ is a root iff $\frac{1-x}{1-y}$ is a root (assume $x, y \neq 0, 1$). This is because

  $$(1-x)^r + x^r = 1 = (1-y)^r + y^r \Rightarrow x^r - y^r = (1-y)^r - (1-x)^r$$

  so that

  $$\left(\frac{x}{y}\right)^r + \left(1 - \frac{x}{y}\right)^r = 1 \Leftrightarrow x^r + (y-x)^r = y^r \Leftrightarrow$$
  $$x^r - y^r = (x-y)^r = (1-y)^r - (1-x)^r \Leftrightarrow$$
  $$\left(\frac{1-x}{1-y}\right)^r + \left(1 - \frac{1-x}{1-y}\right)^r = 1.$$

- As x^{-1} and y^{-1} are also roots, $\frac{x^{-1}}{y^{-1}} = \frac{y}{x}$ is a root iff $\frac{1-x^{-1}}{1-y^{-1}} = \frac{y}{x}\frac{1-x}{1-y}$ is a root.
- $\frac{y}{x}$ is a root iff $\frac{x}{y}$ is a root.
- To sum up,

$$P_{r,r}\left(\frac{x}{y}\right) = 0 \Leftrightarrow P_{r,r}\left(\frac{y}{x}\right) = 0 \Leftrightarrow$$
$$P_{r,r}\left(\frac{1-x}{1-y}\right) = 0 \Leftrightarrow P_{r,r}\left(\frac{y}{x}\frac{1-x}{1-y}\right) = 0$$

Let R be the set of nonzero roots of $P_{r,r}$, c be such that $P_{r,r}(c) \neq 0$ (such a c definitely exists, as the degree of $P_{r,r}$ is at most $r < q$). Considering the sets R and $c^{-1}R$, there are two possibilities:

- If $R \cap c^{-1}R = \emptyset$, then $|R \cup c^{-1}R| = 2|R| \leq q-1 \Leftrightarrow |R| \leq \dfrac{q-1}{2}$.
- If $R \cap c^{-1}R \neq \emptyset$, then if $x \in R \cap c^{-1}R$, i.e. if x and $y = cx$ are roots, then $\dfrac{y}{x} = c$ is not a root, hence neither are $c\dfrac{1-x}{1-cx}$ and $\dfrac{1-x}{1-cx}$: $\dfrac{1-x}{1-cx}$ does not lie in $R \cup c^{-1}R$. However, $x \to \dfrac{1-x}{1-cx}$, $x \in R \cap c^{-1}R$ is bijective. Denoting its range by U, $(R \cup c^{-1}R) \cap U = \emptyset$, namely $|(R \cup c^{-1}R) \cup U| = |R \cup c^{-1}R| + |U| =$ $|R \cup c^{-1}R| + |R \cap c^{-1}R| = |R| + |c^{-1}R| = 2|R| \leq q-1$, whence $|R| \leq \dfrac{q-1}{2}$.

Part 2: Generalizations

[Drakakis (2010)]

Motivation

- Isotropic RADAR: a Costas array leads to the optimal detection of the radial velocity and the distance of the target.
- No directionality: this RADAR is spherically blind. Instead, it can be directional and rotate or…
- a RADAR array can be used!
- Linear array: Target Position Ambiguity Surface (TPAS) is a circle.
- Square array: TPAS is 2 points (front or back).
- Cubic array: TPAS is a point (no ambiguity).

This needs a 5D Costas "array"!

Costas property in higher dimensions

Definition

Let $m \in \mathbb{N}$, consider a sequence $f : \mathbb{Z}^m \to \{0,1\}$, and suppose further that $f(i) = 0,\ i \notin [N], N \in \mathbb{N}^m$, where $i = (i_1, \ldots, i_m)$, $N = (N_1, \ldots, N_m)$, $[N] = [N_1] \times \ldots \times [N_m]$, and the vector N has the smallest possible entries (for the given sequence f). Let the autocorrelation of f be

$$A_f(k) = \sum_{i \in \mathbb{Z}^m} f(i) f(i+k),\ k \in \mathbb{Z}^m.$$

Then, f will be a Costas hyper-rectangle iff

$$\forall k \in \mathbb{Z}^m - \{0\},\ A_f(k) \leq 1.$$

What about permutations?

In even dimensions, a satisfactory generalization of a permutation can be found:

Definition

Let $m = 2s,\ s \in \mathbb{N}$, and let $g : [n]^s \to [n]^s$ be a bijection, that is a permutation on vectors in general. Let $f : \mathbb{Z}^m \to \{0, 1\}$ be a sequence such that $f(i) = 1$ iff $(i_{s+1}, \ldots, i_{2s}) = g(i_1, \ldots, i_s),\ (i_1, \ldots, i_s) \in [n]^s$, and such that it has the Costas property; then, f will be called a permutation Costas hypercube in m dimensions with side length n.

In odd dimensions, no such result is available: we can "cut the dimension in half", if the side length is a square (see below).

Example of a Costas hypercube

$m = 4$ dimensions, $n = 3$ side length:

1	1	2	1
1	2	2	3
1	3	3	1
2	1	2	3
2	2	1	2
2	3	1	3
3	1	3	2
3	2	3	1
3	3	1	2

Each vector with 2 coordinates taking values 1,2,3 (9 of them in total) appears exactly once on each side; the Costas property holds.

Reshaping: the main construction method

Theorem

Let $m, n \in \mathbb{N}^*$, $n = \prod_{i=1}^{m} n_i$, $n_i > 1, i \in [m]$, *and let* $g : [n] - 1 \to [n] - 1$ *be a Costas permutation of order* n. *Expand* $i = \sum_{j=1}^{m} v_j(i) \prod_{l=j+1}^{m} n_l$, *so that* i *gets mapped bijectively to* $V(i) = (v_1(i), \ldots, v_m(i))$, *where* $v_j \in [n_j] - 1,\ j \in [m]$; *similarly,* $g(i)$ *gets mapped bijectively to* $V(g(i)) = (v_1(g(i)), \ldots, v_m(g(i)))$. *Then, the hyper-rectangle of side length* n_i *in dimension* i *and* $i + m$, $i \in [m]$, *whose dots (*n *in total) lie at the points* $(V(i), V(g(i))) := (v_1(i), \ldots, v_m(i), v_1(g(i)), \ldots, v_m(g(i)))$, $i \in [n] - 1$, *is actually a permutation Costas hyper-rectangle.*

Proof

Choose 2 values for i, say i_1 and i_2; the corresponding distance vector is:

$$
\begin{aligned}
&(V(i_1) - V(i_2), V(g(i_1)) - V(g(i_2))) = \\
&\qquad = (v_1(i_1) - v_1(i_2), \ldots, v_m(i_1) - v_m(i_2), \\
&\qquad\quad v_1(g(i_1)) - v_1(g(i_2)), \ldots, v_m(g(i_1)) - v_m(g(i_2)))
\end{aligned}
$$

We need to show that all of these vectors are distinct:

$$
\begin{aligned}
&(V(i_1) - V(i_2), V(g(i_1)) - V(g(i_2))) = \\
&\qquad = (V(i_3) - V(i_4), V(g(i_3)) - V(g(i_4))) \Rightarrow i_1 = i_2,\ i_3 = i_4.
\end{aligned}
$$

Extend V^{-1} by $V^{-1}(v_1, \ldots, v_m) = \sum_{j=1}^{m} v_j \prod_{l=j+1}^{m} n_l$ on the class of vectors where $|v_j| < n_j$, $j \in [m]$. It follows that $V^{-1}(V(i_1) - V(i_2)) = i_1 - i_2$, as $V(i_1) - V(i_2)$ falls within this class of vectors. Then:

$$(V(i_1) - V(i_2), V(g(i_1)) - V(g(i_2))) =$$
$$= (V(i_3) - V(i_4), V(g(i_3)) - V(g(i_4))) \Rightarrow$$

$$V^{-1}(V(i_1) - V(i_2), V(g(i_1)) - V(g(i_2))) =$$
$$= V^{-1}(V(i_3) - V(i_4), V(g(i_3)) - V(g(i_4))) \Leftrightarrow$$
$$(V^{-1}(V(i_1) - V(i_2)), V^{-1}(V(g(i_1)) - V(g(i_2)))) =$$
$$= (V^{-1}(V(i_3) - V(i_4)), V^{-1}(V(g(i_3)) - V(g(i_4)))) \Leftrightarrow$$
$$(i_1 - i_2, g(i_1) - g(i_2)) = (i_3 - i_4, g(i_3) - g(i_4)) \Leftrightarrow$$
$$i_1 - i_2 = i_3 - i_4,\ g(i_1) - g(i_2) = g(i_3) - g(i_4) \Rightarrow$$
$$i_1 = i_3,\ i_2 = i_4$$

In the last step we used the fact that g is Costas; the construction is clearly a permutation.

Odd dimensions

Heuristic

Let $\sqrt{n} \in \mathbb{N}$, and let $g : [n]^m \times [\sqrt{n}] - 1 \to [n]^m \times [\sqrt{n}] - 1$ be a Costas permutation of order $n^m\sqrt{n}$. Expand

$$i = v_0(i)n^m + \sum_{j=1}^{m} v_j(i)n^{m-j} \Leftrightarrow i \leftrightarrow V(i) = (v_0(i), v_1(i), \ldots, v_m(i)),$$

where $v_j \in [n] - 1$, $j \in [m]$ and $v_0 \in [\sqrt{n}] - 1$;
$g(i) \leftrightarrow V(g(i)) = (v_0(g(i)), v_1(g(i)), \ldots, v_m(g(i)))$. This process forms a Costas hyper-rectangle in $2m + 2$ dimensions, whose side length in $2m$ dimensions is n and in the remaining 2 dimensions $\sqrt{n}$. Set $(v_0(i), v_0(g(i))) \longrightarrow \sqrt{n}v_0(g(i)) + v_0(i)$, $i \in [n^m\sqrt{n}] - 1$, which takes values in the range $[n] - 1$. Then, the hypercube of side length n whose dots ($n^m\sqrt{n}$ in total) lie at the points
$(\sqrt{n}v_0(g(i)) + v_0(i), v_1(i), \ldots, v_m(i), v_1(g(i)), \ldots, v_m(g(i)))$,
$i \in [n^m\sqrt{n}] - 1$ may be a Costas hypercube.

Example: $25 \to 5^4$

0	10
1	7
2	6
3	9
4	17
5	23
6	21
7	2
8	20
9	11
10	15
11	3
12	12
13	22
14	1
15	16
16	18
17	19
18	5
19	0
20	13
21	24
22	14
23	8
24	4

0	0	0	2
1	0	2	1
2	0	1	1
3	0	4	1
4	0	2	3
0	1	3	4
1	1	1	4
2	1	2	0
3	1	0	4
4	1	1	2
0	2	0	3
1	2	3	0
2	2	2	2
3	2	2	4
4	2	1	0
0	3	1	3
1	3	3	3
2	3	4	3
3	3	0	1
4	3	0	0
0	4	3	2
1	4	4	4
2	4	4	2
3	4	3	1
4	4	4	0

Example: $27 \to 9 \times 3 \times 3 \times 9 \to 9^3$

0	0
1	2
2	18
3	11
4	22
5	4
6	24
7	19
8	9
9	15
10	12
11	26
12	10
13	14
14	1
15	8
16	13
17	7
18	20
19	21
20	17
21	16
22	25
23	5
24	3
25	6
26	23

0	0	0	0
1	0	0	2
2	0	2	0
3	0	1	2
4	0	2	4
5	0	0	4
6	0	2	6
7	0	2	1
8	0	1	0
0	1	1	6
1	1	1	3
2	1	2	8
3	1	1	1
4	1	1	5
5	1	0	1
6	1	0	8
7	1	1	4
8	1	0	7
0	2	2	2
1	2	2	3
2	2	1	8
3	2	1	7
4	2	2	7
5	2	0	5
6	2	0	3
7	2	0	6
8	2	2	5

0	0	0
1	0	2
2	6	0
3	3	2
4	6	4
5	0	4
6	6	6
7	6	1
8	3	0
0	4	6
1	4	3
2	7	8
3	4	1
4	4	5
5	1	1
6	1	8
7	4	4
8	1	7
0	8	2
1	8	3
2	5	8
3	5	7
4	8	7
5	2	5
6	2	3
7	2	6
8	8	5

The extended Welch construction

Theorem

Let p be a prime, $m \in \mathbb{N}^*$, α a primitive root of $\mathbb{F}(q)$ where $q = p^m$, and $c \in [q-1]-1$. Then:

- *The function $f : [q-1] \to \mathbb{F}^*(q)$, where $f(i) = \alpha^{i-1+c} \bmod P(x),\ i \in [q-1]$, $P(x)$ an irreducible polynomial over $\mathbb{F}(p)$ of degree m, is a permutation over $\mathbb{F}^*(q)$.*
- *The hyper-rectangle in $m+1$ dimensions with side length $q-1$ in the first dimension and p in the others, whose dots lie at $\{(i, f(i)) | i \in [q-1]\}$, has the Costas property.*
- *The hypercube in $2m$ dimensions with side length p, whose dots lie at $\{(V(i), f(i)) | i \in [q-1]\}$, has the Costas property; V denotes the base p expansion.*

Example: $\alpha = x, c = 1, P(x) = x^3 + 2x + 1$ in $\mathbb{F}(27)$

1	0	1	0
2	1	0	0
3	0	1	2
4	1	2	0
5	2	1	2
6	1	1	1
7	1	2	2
8	2	0	2
9	0	1	1
10	1	1	0
11	1	1	2
12	1	0	2
13	0	0	2
14	0	2	0
15	2	0	0
16	0	2	1
17	2	1	0
18	1	2	1
19	2	2	2
20	2	1	1
21	1	0	1
22	0	2	2
23	2	2	0
24	2	2	1
25	2	0	1
26	0	0	1

0	0	1	0	1	0
0	0	2	1	0	0
0	1	0	0	1	2
0	1	1	1	2	0
0	1	2	2	1	2
0	2	0	1	1	1
0	2	1	1	2	2
0	2	2	2	0	2
1	0	0	0	1	1
1	0	1	1	1	0
1	0	2	1	1	2
1	1	0	1	0	2
1	1	1	0	0	2
1	1	2	0	2	0
1	2	0	2	0	0
1	2	1	0	2	1
1	2	2	2	1	0
2	0	0	1	2	1
2	0	1	2	2	2
2	0	2	2	1	1
2	1	0	1	0	1
2	1	1	0	2	2
2	1	2	2	2	0
2	2	0	2	2	1
2	2	1	2	0	1
2	2	2	0	0	1

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

K. Drakakis. “On the generalization of the Costas property in higher dimensions.” Advances in Mathematics of Communications **[0.97]**, Volume 4, Issue 1, 2010, pp. 1–22.

K. Drakakis, R. Gow, S. Rickard, J. Sheekey, and K. Taylor. “On the maximal cross-correlation of algebraically constructed Costas arrays.” (to appear in) IEEE Transactions on Information Theory.