Cross-correlation of Costas arrays: the current status

Konstantinos Drakakis, Scott Rickard
UCD CASL
University College Dublin
Belfield, Dublin 4
Ireland
Email: {Konstantinos.Drakakis, Scott.Rickard}@ucd.ie

***Abstract*—We study the cross-correlation of pairs of Costas arrays, and more specifically its maximal value over the families of Golomb and Welch permutations. We record the numerical results found, analyze them, formulate conjectures summarizing our findings, and present the current progress towards a rigorous proof of these conjectures.**

***Index Terms*—Costas arrays/permutation, cross-correlation, Golomb construction, Welch construction, finite fields, primitive roots.**

I. Introduction

Costas arrays are, to begin with, permutation arrays, namely square arrangements of dots/1s and blanks/0s, such that there lies exactly one dot per row and column. Furthermore, they are required to satisfy the Costas property: no four dots can form a parallelogram, and no three dots lying on a straight line can be equidistant. They appeared for the first time in 1965 in the context of SONAR detection [2], [3], when J.P. Costas, disappointed by the poor performance of SONAR systems, used them to describe a novel frequency hopping pattern for SONAR systems with optimal auto-correlation properties. About two decades later, Prof. S. Golomb published two generation techniques [4], [7], [8] for Costas permutations, both based on the theory of finite fields, known as the Welch and the Golomb method, respectively. These are still the only general construction methods for Costas permutations available today, and they succeed in constructing $n \times n$ Costas arrays for infinitely many, though not all, n. The existence of $n \times n$ Costas arrays for all $n \geq 1$ remains an open problem; $n = 32$ and 33 are the smallest values of n for which there is currently no known example of a Costas array.

Consider two $n \times n$ Costas arrays A and B placed on top of each other, so that they overlap perfectly, and shift A by u rows and v columns with respect to B: the number of pairs of overlapping dots is the value of the cross-correlation at (u, v), denoted by $C_{A,B}(u, v)$. If $A = B$, the only possible cross-correlation values are 0, 1, and n; for, any other value between 2 and $n - 1$ would require the existence of a shift (u, v) that would bring a set of two or more dots on top of another equinumerous set of dots, implying the existence of either a parallelogram or equidistant dots on a straight line, a contradiction. In this sense, the auto-correlation of a Costas array is optimal. When $A \neq B$, however, it can be shown that, unless A and B are trivially small, they always contain a pair of dots set apart by the same amount of rows and columns [9], so that their maximal cross-correlation is at least 2 (note that $C_{A,B}(u, v) = n$ is possible iff $u = v = 0$ and $A = B$), and therefore no longer optimal. The following questions then arise naturally: What is the maximal cross-correlation between two Costas arrays in a certain Golomb or Welch family? In particular, for which of these families is the maximal cross-correlation small?

The motivation behind studying the cross-correlation of Costas arrays is quite straightforward: assuming there are multiple RADAR/SONAR systems in the same geographical area, the waveforms they transmit are bound to interfere. If each system is transmitting a waveform specified by a Costas array, it is important to determine sufficiently large families of Costas arrays, over which the cross-correlation is uniformly bounded by a small value, so that, by choosing Costas arrays out of such a family, interference is minimized.

The layout of the paper is as follows: Section II gives an overview of the basics about Costas arrays, including relevant definitions and construction techniques; Section III motivates the construction of Costas arrays by explaining the modeling process which results to their definition; Section IV presents numerical results on the cross-correlation of Costas arrays and conjectures suggested by their analysis; and, finally, Section V presents our progress towards a rigorous proof of these conjectures.

II. Basics

We let below $[n] := \{1, \ldots, n\}$, $n \in \mathbb{N}$, along with the obvious variants $[n] - 1 = \{0, 1, \ldots, n - 1\}$ etc. We call $f : A \to B$ a bijection if f is $1 - 1$ and onto (injective and surjective), as usual, but we reserve the word "permutation" for bijective f with $A = B$.

This work is an abridged and slightly updated version of the paper "On the maximal cross-correlation of algebraically constructed Costas arrays", authored by K. Drakakis, R. Gow, S. Rickard, and K. Taylor, currently submitted for publication, and is based upon works supported by the Science Foundation Ireland under Grant No. 05/YI2/I677, 06/MI/006 (Claude Shannon Institute), and 08/RFP/MTH1164.

The authors are also affiliated with the School of Electrical, Electronic & Mechanical Engineering, University College Dublin, Belfield, Dublin 4, Ireland, and with the Claude Shannon Institute for Discrete Mathematics, Coding, and Cryptography.

ISBN 978-963-311-370-7

A. Definitions

Definition 1. Consider a bijection $f : [n] \to [n]$; f is *a Costas permutation* iff it satisfies *the Costas property*, also known as *Distinct Differences Property (DDP):*

$$\forall i,j,k: \ i,j,i+k,j+k \in [n],$$
$$f(i+k)-f(i)=f(j+k)-f(j) \Rightarrow i=j \text{ or } k=0. \quad (1)$$

A permutation f corresponds to a permutation array $A_f = [a^f_{i,j}]$ by setting the elements of the permutation to denote the positions of the (unique) 1 in the corresponding column of the array, counting from top to bottom: $a^f_{f(i),i} = 1$. Costas arrays are permutation arrays corresponding to Costas permutations.

It is customary to represent 1s in a permutation array as "dots" and 0s as "blanks". From now on the terms "array" and "permutation" will be used interchangeably, in view of this correspondence, though some results are easier to understand having one representation in mind than the other. Thinking in terms of arrays rather than permutations, for example, we see that the Costas property is equivalent to the fact that the *distance vector* $(f(j)-f(i), j-i)$ between the dots of the ith and jth columns, $1 \le i < j \le n$ is not repeated between any other pair of dots: hence, as stated in the Introduction, no four dots form a parallelogram, and no three dots lying on a straight line are equidistant. Furthermore, as horizontal and vertical flips, transpositions around the diagonals, and rotations of the array by multiples of 90^o (which can be expressed as compositions of flips and transpositions) have no effect on the relation between distance vectors in the array, all arrays resulting from a sequence of such operations on a Costas array are Costas arrays themselves: a Costas array thus gives birth to an equivalence class containing either eight Costas arrays or four (if the original array happens to be symmetric, so that transposition has no effect). Note that, if A^f corresponds to f, the transpose corresponds to the inverse permutation: $(A^f)^T = A^{f^{-1}}$. The values of n for which all $n \times n$ Costas permutations are guaranteed to have been found (through exhaustive computer search) are currently $1 \le n \le 27$ (see, for example, [1], [6], [12] and references therein).

The following definition of the cross-correlation formalizes the descriptive definition given in the Introduction:

Definition 2. Let $f_1, f_2 : [n] \to [n]$ be Costas permutations. Their cross-correlation at $(u,v) \in \mathbb{Z}^2$ is defined as

$$C_{f_1,f_2}(u,v) = |\{i \in [n]: \ i-u \in [n], f_1(i-u)+v = f_2(i)\}|.$$

Equivalently, the cross-correlation can be defined on the corresponding arrays:

$$C_{A^{f_1},A^{f_2}}(u,v) = \sum_{\{i,j \in [n]: |i+u,j+v \in [n]\}} a^{f_1}_{i+u,j+v} a^{f_2}_{i,j}.$$

B. Construction methods

There exist two algebraic construction techniques for Costas permutations, namely the Golomb method and the Welch method [4], [7], [8].

Theorem 1 (Exponential Welch construction $W_1^{\exp}(p,\alpha,c)$)**.** Let p be a prime, let α be a primitive root of the finite field $\mathbb{F}_p$ of p elements, and let $c \in [p-1]-1$ be a constant; then, the function $f : [p-1] \to [p-1]$ where $f(i) = \alpha^{i-1+c} \mod p$ is a Costas permutation. Overall, this family contains $(p-1)\phi(p-1)$ distinct permutations.

Flips of $W_1^{\exp}$-arrays are also $W_1^{\exp}$-arrays; in general, however, their transposes are not: instead, they form a family known as *logarithmic Welch arrays*.

Corollary 1 (Logarithmic Welch construction $W_1^{\exp}(p,\alpha,c)$)**.** Let p be a prime, let α be a primitive root of the finite field $\mathbb{F}_p$ of p elements, let $c \in [p-1]-1$ be a constant, and let f be the exponential Welch Costas permutation $W_1^{\exp}(p,\alpha,c)$; then, the permutation $f^{-1} : [p-1] \to [p-1]$ has the Costas property.

The two families are disjoint for $p > 5$ [5], which leads to the result that there exist in total $2(p-1)\phi(p-1)$ W_1-arrays of order $p-1$. Note also that a cyclic shift of the columns/rows of a $W_1^{\exp}$/$W_1^{\log}$-array, indicated by the presence of the constant c in the two definitions above, results in a new $W_1^{\exp}$/$W_1^{\log}$-array. For this reason, c is referred to as the shift parameter of a W_1-array: the fact that cyclic shifts of the columns/rows of $W_1^{\exp}$/$W_1^{\log}$-arrays also lead to Costas arrays is usually referred to as the *single periodicity property* of $W_1^{\exp}$/$W_1^{\log}$-arrays. The subscript in W_1 signifies that the constructed permutation's order is one less than the size of the finite field used. By adding and removing corner dots, this construction yields a range of derived methods, denoted by W_i, $i = 0,1,2,3$.

Theorem 2 (Golomb construction $G_2(q,a,b)$)**.** Let p be a prime, $m \in \mathbb{N}^*$, and let α, β be primitive roots of the finite field $\mathbb{F}_q$ of $q = p^m$ elements; then, the function $f : [q-2] \to [q-2]$ where $\alpha^i + \beta^{f(i)} = 1$ is a Costas permutation. Overall, this family contains $\dfrac{\phi^2(q-1)}{m}$ distinct permutations.

Flips and transpositions of G_2-arrays lead also to G_2-arrays; by adding and removing corner dots we again obtain a whole range of derived methods G_i, $i = 0,1,\ldots,5$. The special case $\alpha = \beta$ is known as the *Lempel construction*.

The proofs of these results are omitted here, but can be found in [4], [7], [8] in detail. Costas permutations constructed/not constructed by the algebraic techniques described above are commonly referred to as *algebraic/sporadic Costas permutations.*

III. Why Costas arrays? Some motivation

RADAR and SONAR systems detect the the distance and velocity of targets around them by transmitting periodically a waveform W and listening for reflections R. Assuming an ideal noiseless environment, R is just a copy of W, only attenuated and shifted in frequency and time. The time delay indicates the distance of the target, while the frequency shift, through the Doppler effect, its velocity (we assume here that the frequency content of W is narrowband enough

for the Doppler effect, which is multiplicative, to be well approximated by a uniform additive shift for all frequencies).

How are the time and frequency shifts detected? The simplest solution would be to apply a matched filter: R is cross-correlated with shifted versions of W for various time and frequency shifts, and the pair of shifts corresponding to the maximal cross-correlation are the true shifts sought:

$$(s_t^*, s_f^*) = \underset{(s_t,s_f)}{\operatorname{argmax}} |\psi(s_t, s_f)|\,,$$
$$\text{where } \psi(s_t, s_f) = \int_{-\infty}^{+\infty} (F_{s_f} W)(t - s_t) R(t) dt, \quad (2)$$

where s_t and $s_f \geq 0$ denote the time and frequency shifts, respectively, and the operator F_{s_f} maps W to the signal obtained by translating every positive frequency of W's spectrum by s_f to the right and every negative frequency by s_f to the left (so that $F_{s_f} W$ remains real).

Alas, this simple idea fails to work in practice, because all real media are incoherent: phase delay varies with frequency, hence waveforms tend to spread while traveling in the medium [3], so that, by the time R reaches the receiver, it may look so different from W that coherent processing becomes inappropriate.

J.P. Costas's idea [3] was to discard phase information, since it is unreliable, and carry out the cross-correlation based on the energy contents of W and R alone. Consider a waveform of the form:

$$W(t) = A \cos\left(\phi_k + 2\pi \left(f_0 + \frac{a_k}{n} f_1\right) t\right),$$
$$t \in \left[\frac{k-1}{n} T, \frac{k}{n} T\right], \quad (3)$$

where $k \in [n]$, T is the time duration of the pulse, f_0, f_1 are two predetermined frequencies, ϕ_k are phases suitably chosen so that the phase of W is continuous in t (we may choose $\phi_1 = 0$), and $a : [n] \to [n]$ is a bijection. This is a frequency hopping waveform whose instantaneous frequency is

$$f(t) = f_0 + \frac{a_k}{n} f_1, \; t \in \left(\frac{k-1}{n} T, \frac{k}{n} T\right), k \in [n]. \quad (4)$$

We observe that W is completely determined by a, given that f_0, f_1, and T are set.

Costas's idea amounts effectively to placing an energy content detector before the matched filter, thus reconstructing a from W, and similarly for R. The signals fed to the matched filter can then each be abstracted as a 2D infinite sequence (representing the time-frequency plane), which is full of 0s/blanks (denoting the absence of energy), except for a $n \times n$ square than corresponds to a permutation array (whose 1s/dots denote that energy is present there), exactly as described in Definition 1. The filter overlays the two 2D sequences, then shifts one with respect to the other by some rows vertically and some columns horizontally, and counts how many pairs of dots overlap, in accordance with the description in the Introduction and with Definition 2. In the absence of noise, R is an exact copy of W, only shifted in time and frequency, so the matched filter will have found the correct shift parameters when the cross-correlation becomes equal to n.

When noise is present, however, some of R's dots may have shifted irregularly or even gone altogether missing: R will no longer be an exact copy of W, and the maximal cross-correlation will no longer be n. The filter will have no alternative than to locate the maximal cross-correlation (note that now it won't know a priori what the maximum will be) and return the shift parameters corresponding to it; but this maximum may no longer be unique, or one of the (former) sidelobes may have grown taller than the main lobe: either case will result to spurious target detection.

What should the form of a (or the corresponding array A) be in order to minimize the probability of spurious detections? In the absence of noise, the cross-correlation is just a shifted form of the autocorrelation of A, so we need to choose A in such a way as to suppress as much as possible the height of the autocorrelation sidelobes relatively to the main lobe (whose height is n):

$$A = A^* = \underset{A}{\operatorname{argmin}} \max_{(u,v)\neq(0,0)} C_{A,A}(u, v).$$

Choosing any pair of dots in A, there exists a shift (their distance vector) that will move these dots on top of each other, so sidelobes of height 1 will exist and nothing can be done about it. If, however, we stipulate that distance vectors be unique, there will be no sidelobe of height 2 or more; but, according to Definition 1, this is precisely the Costas property! Autocorrelation is known as *auto-ambiguity* in the SONAR/RADAR community, and waveforms with the Costas property are said to have *ideal thumbtack auto-ambiguity* [3], [8].

Why should the optimal A be a permutation array, as we assumed (summarily and without any further explanation) above? Would using twice the same frequency, or using two frequencies simultaneously, not improve the autocorrelation? Costas argued on basic engineering principles that indeed it would not [3].

Why, finally, do we need the full force of the Costas property? Would sidelobes of height 2 or more, but still much shorter than the main lobe, not suffice? We argue that indeed they would not, but for a reason we have not mentioned so far: even if such a signal performed well under noise conditions, as discussed above, there is still the issue of multipath interference. In the real world R will most likely be the sum of attenuated and shifted noisy versions of W (by different attenuation and shift parameters) representing echoes from different reflection paths, which may add up constructively at the receiver: the taller the sidelobes of W are, the easier it is for them to add up to a really tall sidelobe in R.

IV. Numerical results and conjectures

Tables I and II show

$$C_S(q) = \max_{f_1 \neq f_2,\; f_1, f_2 \in S} \max_{(u,v)} C_{f_1,f_2}(u, v), \quad (5)$$

where S is either the family $W_1(q)$ of W_1-permutations or the family $G_2(q)$ of G_2-permutations generated in $\mathbb{F}_q$, as a function of the prime (power) q. *An important note regarding W_1-permutations, which will be assumed throughout this work without being referred to explicitly again, is that pairs (f_1, f_2) such that f_1 and f_2 are a) either both exponential or both logarithmic W_1-permutations and b) generated by the same primitive root are not considered in the maximization.*

Focusing on Table I and II, respectively, we collect our observations in the following conjectures:

Conjecture 1 (Main conjecture for primes)**.** With respect to $C_{W_1}(p)$ and $C_{G_2}(p)$, primes p can be classified into three groups:

- For primes $p \neq 19$ such that $(p-1)/2$ is not a prime, $C_{W_1}(p) = C_{G_2}(p) + 1$ and $C_{W_1}(p) = (p-1)/r$, where r is the smallest divisor of $(p-1)/2$.
- $p = 19$ is the only prime for which $C_{W_1}(p) = C_{G_2}(p)$ and $C_{W_1}(p) = (p-1)/r = 6$, where $r = 3$ is the smallest divisor of $(p-1)/2 = 9$.
- Primes p such that $(p-1)/2$ is also a prime (known as safe primes) correspond to local minima of both $C_{W_1}(p)$ and $C_{G_2}(p)$.

Observe that the conjecture suggests that the maximal cross-correlations of the two families of G_2- and W_1-permutations are closely related (they almost always differ by 1), despite being based on completely different mechanisms. This is indeed remarkable!

Conjecture 2 (Main conjecture for prime powers)**.** With respect to $C_{G_2}(q)$, prime powers q can be classified into three groups:

- For prime powers $q \neq 16$ such that neither $(q-1)/2$ nor $q-1$ is a prime, $C_{W_1}(q) = (q-1)/r - 1$, where r is either the smallest divisor of $(q-1)/2$, if q is odd, or of $q-1$, if q is even.
- $q = 16$ is the only prime power for which $C_{G_2}(q) = (q-1)/r = 5$, where $r = 3$ is the smallest divisor of $q - 1 = 15$.
- Prime powers q such that either $(q-1)/2$ is prime (in which case $q = 3^m$ for some prime m) or $q-1$ is prime (in which case $q = 2^m$ for some prime m and $q-1$ is a Mersenne prime) correspond to local minima of $C_{G_2}(q)$.

V. Theoretical results

The following theorems summarize the extent of our success in proving the conjectures of the previous section.

Theorem 3. Let p be a prime, and let r be the smallest prime such that $p \equiv 1 \bmod (2r)$; then $\max_{f_1 \neq f_2,\ f_1, f_2 \in W_1^{\exp}(p)} C_{f_1,f_2}(0,0) = (p-1)/r$.

Proof: We consider the number of solutions $i \in [p-1]$ of the equation

$$\alpha^{i-1+c} \equiv \beta^{i-1+d} \bmod p, \tag{6}$$

where $c, d \in [p-1]-1$ are constants, and $\alpha,\ \beta$ are distinct primitive roots. Since there exists an $s \in [p-1]\backslash\{1\}$, such that $(s, p-1) = 1$ and that $\beta = \alpha^s$, the equation above becomes

$$(s-1)(i-1) \equiv c - sd \bmod (p-1). \tag{7}$$

Since $c - sd$ spans all residue classes modulo $p-1$, the maximal number of roots of the equation above over all possible pairs (c, d) equals the number of roots x of the equation

$$(s-1)x \equiv 0 \bmod (p-1), \tag{8}$$

so we may focus on this one instead. It is well known that this congruence has $(s-1, p-1)$ roots, so that indeed $(s-1, p-1) = (p-1)/w$, where w is a divisor of $p-1$; the maximal number of roots corresponds to the smallest possible w which is obtainable by an allowed value of s (recall the constraint $(s, p-1) = 1$). That is,

$$\max_{f_1 \neq f_2,\ f_1, f_2 \in W_1^{\exp}(p)} C_{f_1,f_2}(0,0) = \\ = \max_{\{s \in [p-1]\backslash\{1\}:\ (s,p-1)=1\}} (s-1, p-1). \tag{9}$$

In general, the maximal possible value of $(s-1, p-1)$ is $(p-1)/2$, in which case $s - 1 = (p-1)/2 \Leftrightarrow s = (p+1)/2$. Is this value of s admissible?

$$1 = (s, p-1) = \left(\frac{p+1}{2}, p-1\right) = \left(\frac{p+1}{2}, 2\right) \Leftrightarrow \\ \frac{p+1}{2} \equiv 1 \bmod 2 \Leftrightarrow p \equiv 1 \bmod 4. \tag{10}$$

In other words, $s = (p+1)/2$, leading to $r = 2$, is admissible iff $p-1$ is divisible by 4, in which case 2 is indeed the smallest divisor of $(p-1)/2$.

Assume now $p \equiv 3 \bmod 4$, let w be a prime such that $p \equiv 1 \bmod w$, and let $s = \lambda(p-1)/w + 1$, for some $\lambda \in [w-1]$. It is clear that

$$(s-1, p-1) = \left(\lambda\frac{p-1}{w}, p-1\right) = \left(\lambda\frac{p-1}{w}, w\frac{p-1}{w}\right) = \\ = \frac{p-1}{w}(\lambda, w) = \frac{p-1}{w}. \tag{11}$$

We will show that s is admissible for either $\lambda = 1$ or $\lambda = 2$. Let $p = 1 + wk$, and observe that $\left(\lambda\frac{p-1}{w} + 1, p-1\right) = (\lambda k + 1, wk)$; unless $w | \lambda k + 1$, this is equal to $(\lambda k + 1, k) = (1, k) = 1$. Assuming now that $w | k + 1$ and $w | 2k + 1$, it follows that $w | k$, so that $w | 1$, a contradiction; so, either $\lambda = 1$ or $\lambda = 2$ leads to an admissible value of s. When is $\lambda = 2$ needed? When $w | k + 1$, $k = lw - 1$ for some l, so that $p = 1 + (lw - 1)w = lw^2 - w + 1 \leftrightarrow p \equiv w^2 - w + 1 \bmod w^2$.

We have shown that for every prime $p \equiv 3 \bmod 4$ and every prime w such that $p \equiv 1 \bmod (2w)$ (note that necessarily $w > 2$ so that $p-1$ is divisible by both 2 and w), there exists an admissible s such that (8) has $(p-1)/w$ roots. This is clearly maximized when w is the least possible such prime, namely $w = r$. This completes the proof. ∎

Prime	W_1	G_2	Prime	W_1	G_2	Prime	W_1	G_2	Prime	W_1	G_2
5	2	2	59	5	12	127	42	41	197	98	97
7	2	2	61	30	29	131	26	25	199	66	65
11	3	4	67	22	21	136	68	67	211	70	69
13	6	5	71	14	13	139	46	45	223	74	73
17	8	7	73	36	35	149	74	73	227	6	13
19	6	6	79	26	25	151	50	49	229	114	113
23	4	6	83	5	9	157	78	77	233	116	115
29	14	13	89	44	43	163	54	53	239	34	33
31	10	9	97	48	47	167	6	12	241	120	119
37	18	17	101	50	49	173	86	85	251	50	49
41	20	19	103	34	33	179	6	12	257	128	127
43	14	13	107	5	10	181	90	89	263	7	12
47	5	8	109	54	53	191	38	37	269	134	133
53	26	25	113	56	55	193	96	95	271	90	89

TABLE I

THE VALUE OF THE MAXIMAL CROSS-CORRELATION BETWEEN PAIRS OF W_1 ARRAYS AND OF G_2 ARRAYS GENERATED IN $\mathbb{F}_p$, FOR THE FIRST FEW PRIMES p: ENTRIES IN RED CORRESPOND TO SAFE PRIMES, WHILE 19 APPEARS IN BLUE BECAUSE OF A SLIGHT IRREGULARITY IN THE G_2 CASE. W_1 RESULTS FOR $p < 80$ FIRST APPEARED IN [10], [14]; W_1 RESULTS FOR $p < 200$ AND G_2 RESULTS FOR $p < 80$ FIRST APPEARED IN [11].

Prime power	G_2	Prime power	G_2	Prime power	G_2
4	1	32	6	128	9
8	3	49	23	169	83
9	3	64	20	243	21
16	5	81	39	256	84
25	11	121	59	289	143
27	6	125	61	343	113

TABLE II

THE VALUE OF THE MAXIMAL CROSS-CORRELATION BETWEEN PAIRS OF G_2 ARRAYS GENERATED IN $\mathbb{F}_q$, FOR THE FIRST FEW STRICT PRIME POWERS q: ENTRIES IN RED CORRESPOND TO IRREGULAR CASES, WHILE 16 APPEARS IN BLUE BECAUSE IT SEEMS TO BE SEMI-IRREGULAR.

Theorem 4. Let q be an odd prime power, and let r be the smallest prime such that $q \equiv 1 \bmod (2r)$; then there exist $f_1, f_2 \in G_2(q)$ such that $C_{f_1,f_2}(0,0) = (q-1)/r - 1$.

Proof: Let f_1 be generated through $\alpha^i + \beta^{f_1(i)} = 1$, and let f_2 be generated through $\gamma^j + \delta^{f_2(j)} = 1$, $i, j \in [q-1]$. There exist s and t such that $(s, q-1) = (t, q-1) = 1$ and $\gamma = \alpha^s$, $\delta = \beta^t$. Whenever $f_1(i) = f_2(j)$ and $i = j$, it follows that

$$y^s + (1-y)^t = 1, y = \beta^{f_1(i)}, \tag{12}$$

so $C_{f_1,f_2}(0,0)$ is equal to the number of roots y of this polynomial in $\mathbb{F}_q$, with the exception of $y = 0$ and $y = 1$ (due to what y stands for). Letting now $t = 1$ and $y = \alpha^x$ leads to the equation

$$(s-1)x \equiv 0 \bmod (q-1), \tag{13}$$

which is the same as (8). The proof now follows verbatim the proof of Theorem 3, with the only exception that $x = 0 \Leftrightarrow y = 1$ has to be discounted, leading to one root less. This completes the proof. ∎

Theorem 5. Let q be an even prime power (i.e. a power of 2) and let r be the smallest prime such that $q \equiv 1 \bmod r$; then there exist $f_1, f_2 \in G_2(q)$ such that $C_{f_1,f_2}(0,0) = (q-1)/r - 1$.

Proof: The derivation of (13) in the proof of Theorem 4 did not rely on the parity of q, so it remains valid. The proof now follows almost verbatim the proof of Theorem 3, with the exception that again $x = 0 \Leftrightarrow y = 1$ has to be discounted, leading to one root less. The extra caveat is that $q-1$ is now odd, hence not divisible by 2; fortunately, the relevant second part of the proof of Theorem 4 (concerning $p \equiv 3 \bmod 4$) does not rely on the parity of p, or even the fact that p is prime, so the argument can be repeated verbatim for q (which is now even). This completes the proof. ∎

Note that, whenever $q-1$ is a (Mersenne) prime, Theorem 5 asserts the existence of two G_2-permutations whose cross-correlation at $(0,0)$ is 0; this is interesting in itself.

Comparing the theorems of this section with the conjectures of Section IV, we can now be more specific regarding what remains to be shown:

Conjecture 3. Assuming p is a prime such that $(p-1)/2$ is not a prime, $C_{W_1}(p) = \max_{f_1 \neq f_2,\ f_1,f_2 \in W_1^{\exp}(p)} C_{f_1,f_2}(0,0)$. Assuming $q \neq 16, 19$ is a prime power such that neither $q-1$ nor $(q-1)/2$ is prime, $C_{G_2}(q) = C_{f_1,f_2}(0,0)$, where f_1 is generated by primitive roots (α, β) and f_2 by primitive roots (α^s, β), where s is as determined in the proofs of Theorems 4 and 5.

It is clear that Conjecture 3 sets forth four tasks. First, we need to understand the results pertaining to the exceptional values of p and q: at the moment, our only observation is that the maximal cross-correlation there appears to be lower than elsewhere, but we are unable to qualify this statement further.

Second, we need to determine whether, for non-exceptional values of q, the maximal cross-correlation at $(0,0)$ over

the family of G_2-permutations $G_2(q)$ occurs for the pair of permutations mentioned in the conjecture. To this end, it is enough to consider the polynomials defined in (12), and show that $P_{s,t}(x) := x^s + (1-x)^t - 1$ has at most as many roots as $P_{s,1}(x)$. Partial progress towards this result has been made recently: J. Sheekey, currently a doctorate student in Claude Shannon Institute, under the supervision of R. Gow, demonstrated, as part of his doctorate thesis, that, for any odd prime power q, the total number of roots of $P_{s,s}(x)$ is bounded above by $(q+1)/2$ [13]. The proof is a counting argument making use of orbits of roots not present in the general polynomial $P_{s,t}(x)$: indeed, $P_{s,s}(x) = 0 \Leftrightarrow P_{s,s}(1-x) = 0 \Leftrightarrow P_{s,s}(1/x) = 0$ (the latter assuming that $x \neq 0$). To show this, the fact that q is odd, hence s, satisfying $(s, q-1) = 1$ is odd, must be used.

Third, we need to establish that, for non-exceptional values of p and q, the maximal cross-correlation values $C_{W_1}(p)$ and $C_{G_2}(q)$ correspond to cross-correlation values at $(0,0)$. No tangible progress has been made towards this direction, chiefly because of the "unalgebraic" form of the equations involved. In the case of $W_1(p)$, revisiting (6), the value of the cross-correlation of two W_1-permutations at (u,v) equals the number of values of $i \in [p-1]$ such that $i+u \in [p-1]$, and such that

$$\alpha^{i-1+c} \bmod p + v = \beta^{i+u-1+d} \bmod p. \tag{14}$$

This equation is extremely complicated. An upper bound for the number of its roots is the number of $i \in [p-1]$ such that

$$\alpha^{i-u-1+c} + v \equiv \beta^{i-1+d} \bmod p, \tag{15}$$

which, in turn, is bounded above by s, assuming $\beta = \alpha^s$ in $\mathbb{F}_p$. In the case of $G_2(q)$, revisiting the beginning of the proof of Theorem 4, we now require that $j = i + u$ and $f_2(j) = f_1(i) + v$, so that the cross-correlation of f_1 and f_2 at (u,v) equals the number of roots $y = \alpha^i$ of the polynomial equation $Ay^s + B(1-y)^t = 1$, $A = \alpha^u$, $B = \beta^{tv}$, such that $i \in [q-2]$ and $i+u \in [q-2]$, which is clearly bounded above by the number of roots of $Ay^s + B(1-y)^t = 1$ in $\mathbb{F}_q$, in turn clearly bounded above by $\max(s,t)$.

Fourth, we need to show that, for non-exceptional values of p, $C_{W_1}(p)$ is attained by $f_1, f_2 \in W_1^{\exp}(p)$, as opposed to, without loss of generality, $f_1 \in W_1^{\exp}(p)$ and $f_2 \in W_1^{\log}(p)$. We currently have no theoretical results describing the cross-correlation of such "mixed" pairs.

VI. Conclusion and Future Work

We studied the maximal cross-correlation over the families of Golomb- or Welch-constructed Costas permutations. We compiled tables with the results, and we formulated conjectures based on our observations. We then presented our progress towards a rigorous justification of these observations, and a new conjecture describing what remains to be done. Simply put, we have an almost complete understanding of the exact value of the cross-correlation when the two arrays overlap perfectly, and it seems that, as a rule, the maximal cross-correlation over a family occurs between two perfectly overlapping arrays, which we were able to determine. The exceptions are families of Welch arrays built in the finite field $\mathbb{F}_p$ where $(p-1)/2$ is also a prime, and families of Golomb arrays built in $\mathbb{F}_q$ where $q = 16$ or 19, or where either $q-1$ or $(q-1)/2$ is prime. The word "almost" refers to the fact that, in the Golomb case, we still cannot prove rigorously that the pair of arrays leading to the maximal cross-correlation value recorded in the tables through our numerical experiments is indeed maximal.

Regarding the exceptions, no specific formula is known for the behavior of the maximal cross-correlation there, except that it tends to be much lower than in the other cases. Finally, proving rigorously that the maximal value of the cross-correlation occurs when arrays overlap perfectly (except possibly for the exceptional cases), despite some small progress, seems to lie still outside our reach.

Acknowledgements

This work is an abridged and slightly updated version of the paper "On the maximal cross-correlation of algebraically constructed Costas arrays", authored by K. Drakakis, R. Gow, S. Rickard, and K. Taylor, currently submitted for publication. It is based upon works supported by the Science Foundation Ireland under Grant No. 05/YI2/I677, 06/MI/006 (Claude Shannon Institute), and 08/RFP/MTH1164. The authors would finally like to acknowledge the input of J. Sheekey and Prof. R. Gow.

References

[1] 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, April 2007.

[2] J.P. Costas. "Medium constraints on sonar design and performance." Technical Report Class 1 Rep. R65EMH33, GE Co., 1965.

[3] J.P. Costas. "A study of detection waveforms having nearly ideal range-doppler ambiguity properties." Proceedings of the IEEE, Volume 72, Issue 8, August 1984, pp. 996–1009.

[4] K. Drakakis. "A review of Costas arrays." Journal of Applied Mathematics, Volume 2006.

[5] K. Drakakis, R. Gow, L. O'Carroll. "On the symmetry of Welch- and Golomb-constructed Costas arrays" Discrete Mathematics, Volume 309, Issue 8, April 2009, pp. 2559–2563.

[6] 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.

[7] S.W. Golomb. "Algebraic constructions for Costas arrays." Journal Of Combinatorial Theory Series A, Volume 37, Issue 1, 1984, pp. 13–21.

[8] S.W. Golomb and H. Taylor. "Constructions and properties of Costas arrays." Proceedings of the IEEE, Volume 72, September 1984, pp. 1143–1163.

[9] A. Freedman and N. Levanon. "Any two $N \times N$ Costas signals must have at least one common ambiguity sidelobe if $N > 3$ — A proof." Proceedings of the IEEE, Volume 73, Issue 10, 1985, pp. 1530–1531.

[10] S. Maric, I. Seskar, and E. Titlebaum. "On Cross-Ambiguity Properties of Welch-Costas Arrays When Applied in SS/FH Multiuser Radar and Sonar Systems." IEEE Transactions on Aerospace and Electronic Systems, Volume 30, Issue 4, October 1994, pp. 489–493.

[11] S. Rickard. "Large sets of frequency hopped waveforms with nearly ideal orthogonality properties." Masters thesis, MIT, 1993.

[12] S. Rickard, E. Connell, F. Duignan, B. Ladendorf, and A. Wade. "The enumeration of Costas arrays of size 26." IEEE CISS 2006.

[13] J. Sheekey. Personal communication, November 2009.

[14] E. Titlebaum and S. Maric. "Multiuser sonar properties for Costas array frequency hop coded signals." Proceedings of IEEE ICASSP 1990, pp. 2727–2730.