A Note on the Cross-Correlation of Costas Permutations

Domingo Gómez-Pérez and Arne Winterhof

Abstract—We build on the work of Drakakis et al. (2011) on the maximal cross-correlation of the families of Welch and Golomb Costas permutations. In particular, we settle some of their conjectures. More precisely, we prove two results. First, for a prime \( p \geq 5 \), the maximal cross-correlation of the family of the \( \varphi(p-1) \) different Welch Costas permutations of \( \{1, \ldots, p-1\} \) is \( (p-1)/4 \), where \( t \) is the smallest prime divisor of \( (p-1)/2 \) if \( p \) is not a safe prime and at most \( 1 + p^{1/2} \) otherwise. Here \( \varphi \) denotes Euler’s totient function and a prime \( p \) is a safe prime if \( (p-1)/2 \) is also prime. Second, for a prime power \( q \geq 4 \) the maximal cross-correlation of a subfamily of Golomb Costas permutations of \( \{1, \ldots, q-2\} \) is \( (q-1)/2 \) if \( q \) is odd and of \( q-1 \) if \( q \) is even provided that \( (q-1)/2 \) and \( q-1 \) are not prime, and at most \( 1 + q^{1/2} \) otherwise. Note that we consider a smaller family than Drakakis et al. Our family is of size \( \varphi(q-1) \) whereas there are \( \varphi(q-1)^2 \) different Golomb Costas permutations. The maximal cross-correlation of the larger family given in the tables of Drakakis et al. is larger than our bound (for the smaller family) for some \( q \).

Index Terms—Costas arrays, permutations, cross-correlation, Welch construction, Golomb construction, radar, sonar.

I. INTRODUCTION

FOR a positive integer \( n \), let \( \pi \) be a permutation of \( \{1, \ldots, n\} \) satisfying

\[
\pi(i + k) - \pi(i) \neq \pi(j + k) - \pi(j)
\]

for any integers \( 1 \leq k \leq n-2 \) and \( 1 \leq i < j \leq n-k \). Such a permutation is called a Costas permutation of \( \{1, \ldots, n\} \) and the corresponding \( (n \times n) \)-permutation matrix \( A = (a_{ij})_{i,j=1}^n \) defined by

\[
a_{ij} = 1 \quad \text{if and only if} \quad \pi(i) = j
\]
is called a Costas array of size \( n \). These objects are crucial in some problems arising from radar and sonar, see for example [5, Section 7.6] and [3].

The cross-correlation \( C_{f_1,f_2}(u,v) \) between two mappings \( f_1, f_2 : \{1, \ldots, n\} \to \{1, \ldots, n\} \) at \( (u,v) \in \mathbb{Z}^2 \), \( 1-n \leq u, v \leq n-1 \), is the number of solutions \( x \in \{\max\{1,1-u\}, \ldots, \min\{n,n-u\}\} \)
of the equation

\[
f_1(x) + v = f_2(x + u).
\]

In other words, in order to find the cross-correlation of two Costas permutations at \( (u,v) \) we place their arrays on top of each other, slide the first \( v \) columns horizontally and \( u \) rows vertically, and count the number of pairs of ones that overlap.

For a family \( \mathcal{F} \) of Costas permutations of \( \{1, \ldots, n\} \), the maximal cross-correlation \( C(\mathcal{F}) \) is

\[
C(\mathcal{F}) = \max_{u,v} \max_{f_1,f_2 \in \mathcal{F}} C_{f_1,f_2}(u,v).
\]

Studying the maximal cross-correlation of a family of Costas permutations is not only a very interesting mathematical problem, since families with small maximal cross-correlation are of high practical importance, see [2] and references therein.

In this note, we study the maximal cross-correlation of two families of Costas permutations, the family of Welch Costas permutations and a subfamily of Golomb Costas permutations defined below. In particular, we will address some open problems from [2].

Welch’s construction of Costas permutations is defined as follows, see [3], [5]. For a prime \( p > 2 \), let \( g \) be a primitive root modulo \( p \) and \( \pi_g \) the permutation of \( \{1, \ldots, p-1\} \) defined by

\[
\pi_g(i) \equiv g^i \mod p.
\]

Then, for \( p \geq 5 \), the family \( \mathcal{W}_p \) of Welch Costas permutations of \( \{1, \ldots, p-1\} \) is

\[
\mathcal{W}_p = \{\pi_g : g \text{ primitive root modulo } p\},
\]

so that, \( |\mathcal{W}_p| = \varphi(p-1) \), where \( \varphi \) is Euler’s totient function.

A prime \( p \) is a safe prime if \( (p-1)/2 \) is also a prime, called Sophie Germain prime. Therefore,

\[
|\mathcal{W}_p| = \frac{p-3}{2} \quad \text{if } p \geq 7 \text{ is a safe prime}
\]

and \( |\mathcal{W}_5| = 2 \).

In this note we prove the following result on \( C(\mathcal{W}_p) \).

Theorem 1: For a prime \( p \geq 5 \), let \( t \) be the smallest prime divisor of \( (p-1)/2 \). Then, the maximal cross-correlation
The maximal cross-correlation $C(W_p)$ of the family of Welch Costas permutations $W_p$ of \{1, \ldots, p-1\} satisfies

$$C(W_p) \leq 1 + \left\lfloor \frac{1}{2(p-1)} \right\rfloor$$

if $p$ is a safe prime, otherwise.

Note that we can substitute each $\pi_i(i)$ by a shift $\pi_i(i + c)$ and get the same result. However, $W_p$ must not contain two shifts for the same primitive element $g$. In particular, for non-safe primes, Theorem 1 settles the first conjecture in Drakakis et al. [2, Conjecture 3]. We prove Theorem 1 in Section II.

Golomb’s construction of Costas permutations is the following, see [1], [4], [5], [7]. For a prime power $q > 2$ and primitive elements $g_1$ and $g_2$ of the finite field $F_q$, let $\pi_{g_1, g_2}$ be the permutation of \{1, \ldots, q-2\} defined by

$$\pi_{g_1, g_2}(i) = h \text{ if and only if } g_1^i + g_2^i = 1.$$ 

For $q \geq 4$ and fixed $g_2$, we study the subfamily $G_q$ of the family of Golomb Costas permutations $G_q$ of \{1, \ldots, q-2\} defined by

$$G_q = \{ \pi_{g_1, g_2} : g_1 \text{ primitive element of } F_q \}.$$ 

Then we have $|G_q| = \varphi(q-1)$. In Section III, we prove the following result on $C(G_q)$.

**Theorem 2:** For a prime power $q \geq 4$, let $t$ be the smallest prime divisor of $(q-1)/2$ if $q$ is odd and of $q-1$ if $q$ is even. Then, the maximal cross-correlation $C(G_q)$ of the family of Golomb Costas permutations $G_q$ of \{1, \ldots, q-2\} satisfies

$$C(G_q) \leq \begin{cases} 1 + \left\lfloor \frac{1}{2(q-1)^2} \right\rfloor & \text{if } q \text{ is odd and } t = (q-1)/2, \\ \left\lfloor \frac{1}{2(q-1)(q+1)^2} \right\rfloor & \text{if } q \text{ is even and } t = q-1, \\ (q-1)/t - 1 & \text{otherwise.} \end{cases}$$

Besides $C(G_q)$, it is interesting to study the cross-correlation $C(L_q)$ of the larger set $L_q$ of all Golomb Costas permutations

$$L_q = \{ \pi_{g_1, g_2} : g_1, g_2 \text{ primitive elements of } F_q \}$$

of size

$$|L_q| = \varphi(q-1)^2.$$ 

The tables of [2] show that $C(L_q)$ is larger than $C(G_q)$ for some small values of $q$. For example, for $q = 59$, we have $C(L_{59}) = 12$ but $C(G_{59}) \leq 8$. However, for all prime values of $q$ with $61 \leq q \leq 271$ and all strict prime powers $25 \leq q \leq 343$, the bound of Theorem 2 is also valid for $C(L_q)$. It remains an open problem to prove the conjecture that this bound holds for $C(L_q)$ up to a few exceptions of $q$ with $q \leq 59$.

**II. PROOF OF THEOREM 1**

By [2, Theorem 1], we have

$$\max_{u \in \mathbb{Z}} \max_{f_1, f_2} C_{f_1, f_2}(u, 0) = \frac{p-1}{t}.$$ 

Since $t \leq \sqrt{(p-1)/2}$ if $p$ is not a safe prime, it remains to prove the following lemma, from which Theorem 1 follows immediately after verifying

$$\frac{p-1}{t} \geq \sqrt{2(p-1)} \geq 1 + p^{1/2} \quad \text{for } p \geq 11$$

and that 5 and 7 are both safe primes.

**Lemma 1:** For any prime $p \geq 5$ we have

$$\max_{u \neq 0} \max_{f_1, f_2, \nu_1, \nu_2} C_{f_1, f_2}(u, v) \leq 1 + \left\lfloor \frac{1}{2} \right\rfloor^{p/2}.$$ 

**Proof:** The maximum in the statement can be bounded by the maximal number $N$ of solutions $x \in F_p$ of any equation of the form

$$ax^r \equiv x + v \mod p,$$

with

$$av \not\equiv 0 \mod p, \quad \gcd(r, p-1) = 1, \quad 1 < r < p-1,$$

since, if $g$ is a fixed primitive root modulo $p$, all other primitive roots modulo $p$ are of the form $g^r$ with $\gcd(r, p-1) = 1$. For fixed $a$ and $v$ with $av \not\equiv 0 \mod p$, the number of solutions of (2) is

$$\frac{1}{p-1} \sum_{x \in F_p^*} \sum_{y \in F_p^*} \chi(ax^r)\chi(x + v)$$

by the orthogonality relations

$$\frac{1}{p-1} \sum_{x \in F_p^*} \chi(x)\chi(y) = \begin{cases} 1, & x = y, \\ 0, & x \neq y \end{cases}$$

for all $x, y \in F_p^*$, where the sum runs through all multiplicative characters $\chi$ of $F_p^*$.

The contribution of the trivial character $\chi_0$ is $\frac{(p-2)}{(p-1)}$ and that of the quadratic character $\eta$ is $-\eta(a)/(p-1)$, see Appendix. Thus,

$$N \leq 1 + \frac{p-3}{p-1} \max_{x \in F_p^*} \max_{\chi \neq \chi_0, \eta} \left| \sum_{x \in F_p^*} \chi(x^r(x + v)^{p-2}) \right|$$

by the Weil bound, see Appendix. Note that the Weil bound is applicable since

$$\gcd(r, p-1) = \gcd(p-2, p-1) = 1$$

and the order $s$ of any character $\chi$ is a divisor of $p-1$. 

**III. PROOF OF THEOREM 2**

For $u = v = 0$, we have, by [2, Theorem 3]

$$\max_{f_1, f_2, \nu_1, \nu_2} C_{f_1, f_2}(0, 0) = \frac{q-1}{t} - 1,$$

where $t$ is the smallest prime divisor of $(q-1)/2$ if $q$ is odd and of $q-1$ if $q$ is even.

Next we prove an upper bound for $v = 0$ and arbitrary $u.$
Lemma 2: We have
\[ \max_u \max_{f_1,f_2 \in \mathbb{Q}} C_{f_1,f_2}(u,0) \leq \frac{q-1}{t} - 1 \]
if \( t \not\in \{(q-1)/2, q-1\} \) and
\[ \max_u \max_{f_1,f_2 \in \mathbb{Q}} C_{f_1,f_2}(u,0) \leq 2 \]
otherwise.

Proof: Since
\[ C_{f_1,f_2}(-u,0) = C_{f_2,f_1}(u,0) \]
we may assume \( u \geq 1 \). Let \( f_1 \) and \( f_2 \) be defined by \( f_1(x) = h \) if and only if \( g_1^u + g_1^b = 1 \) and \( f_2(x) = h \) if and only if \( g_2^v + g_2^b = 1 \), respectively, for some integer \( r \) with \( \gcd(r,q-1) = 1 \) and \( 1 < r < q-1 \). Then, the number of solutions \( x \) of \( (1) \) with \( v = 0 \) (and \( u = q-2 \)) is the number of integers \( x \) in the range \( 1 \leq x \leq q-2-u \) such that
\[ g_1^u = g_1^{(x+u)r}, \]
that is, \( x \) satisfies
\[ (r-1)x \equiv -ur \mod (q-1). \]
Put \( d = \gcd(r-1,q-1) \) and let \( a \) be the inverse of \((r-1)/d\) modulo \((q-1)/d\). There is no solution if \( d \) does not divide \( u \). Otherwise, the solutions are those \( x \) with
\[ x \equiv -a(u/d)r \mod (q-1)/d. \]
(3)
We have at most \( d \) such solutions \( x \) with \( 1 \leq x \leq q-2 \). Obviously, we have \( d \leq (q-1)/t \). The result follows immediately if \( d < (q-1)/t \). It remains to study the case \( d = (q-1)/t \). Then either
\[ u \geq d = (q-1)/t \geq (q-1)^{1/2} \]
or
for \( q \) odd, \( t = (q-1)/2 \) and \( d = 2 \)
and
for \( q \) even, \( t = q-1 \) and \( d = 1 \).
In the first case, the solutions \( x \) of \( (3) \) are of the form \( x = x_0 + kt \) with \( 1 \leq x_0 \leq t \) and \( 0 \leq k \leq d-1 \). However, \( k = d-1 \) is not possible since
\[ x_0 + (d-1)t > q-1-t > q-2 - (q-1)^{1/2} \geq q-2-d \geq q-2-u \]
and there are at most \( d-1 = (q-1)/t-1 \) solutions. In the remaining cases we have at most 2 solutions. \( \square \)
For \( v \neq 0 \), analogously to Lemma 1, we get the following bound.

Lemma 3: For odd \( q \), we have
\[ \max_u \max_{v \neq 0} \max_{f_1,f_2 \in \mathbb{Q}} C_{f_1,f_2}(u,v) \leq 1 + \left( 1 - \frac{2}{q-1} \right) q^{1/2} \]
and, for even \( q \),
\[ \max_u \max_{v \neq 0} \max_{f_1,f_2 \in \mathbb{Q}} C_{f_1,f_2}(u,v) \leq \left( 1 - \frac{1}{q-1} \right) \left( 1 + q^{1/2} \right) \].

Proof: Again, let \( f_1(x) = h \) whenever \( g_1^u + g_1^b = 1 \) and \( f_2(x) = h \) whenever \( g_2^v + g_2^b = 1 \) for some \( r \) with \( \gcd(r,q-1) = 1 \) and \( 1 < r < q-1 \). Then, \( (1) \) implies
\[ g_2^v(1-g_1^x) = 1 - g_1^{(x+u)}. \]
Substituting \( y = 1 - g_1^x \), \( a = g_2^v \) and \( b = g_1^u \), we get
\[ ay = 1 - b(1-y)^r. \]
Note that \( a \neq 1 \) since \( v \neq 0 \) and \( y \not\in \{0,1\} \) since \( 1 \leq x \leq q-2 \). Hence, we have to estimate the number \( N \) of solutions of equations of the form
\[ b(1-y)^r = 1 - ay, \quad y \in F_q^* \setminus \{1\}, \]
for any \( a \in F_q^* \setminus \{1\} \) and \( b \in F_q^* \). We can represent \( N \) by character sums
\[ N = \frac{1}{q-1} \sum_{x} \sum_{y \in F_q^* \setminus \{1\}} \chi(b)\chi((1-y)^r(1-ay)^q-2). \]
The contribution of the trivial character is \( (q-2)/(q-1) \) and, for odd \( q \), that of the quadratic character is \( -\chi(b)/(q-1) \). For the remaining characters, the absolute value of the inner sum is at most \( q^{1/2} \) by the Weil bound. Collecting these facts, the result follows. \( \square \)

Theorem 2 is proved by combining Lemmas 2 and 3, after verifying that \( t < (q-1)/2 \) implies the following results.

For any odd \( q \), we have \( t \leq \sqrt{q-1} \), and thus
\[ 1 + q^{1/2} \leq \frac{q-1}{t} - 1 \]
for any odd \( q \geq 27 \).

For the remaining odd \( q \) with \( q \leq 25 \), the following refinement holds,
\[ 1 + \left( 1 - \frac{2}{q-1} \right) q^{1/2} \leq \frac{q-1}{t} - 1. \]

For even \( q \geq 4 \), by Mihăilescu’s Theorem (former Catalan conjecture), \( q-1 \) is not a perfect square and thus \( q-1 \leq t(t+2) \), that is, \( t \leq -1 + q^{1/2} \).
If \( q = 2^r \) with an odd \( r \), then
\[ 1 + q^{1/2} < 1 + q^{1/2} \leq \frac{q-1}{t} \].
If \( q = 2^r \) with an even \( r \), then \( t = 3 \) and
\[ 1 + q^{1/2} \leq \frac{q-1}{3} - 1 \] for \( q \geq 64 \).
In the remaining case, that is \( q = 16 \), the more precise bound of Lemma 3 equals \( (q-1)/t = 1 - 4 \). \( \square \)

Note that for estimating \( C(L_q) \) we have to study the number of solutions of equations of the form
\[ b(1-y)^r = 1 - ay^s \]
also for \( s > 1 \). However, the Weil bound becomes trivial for large \( s \) and the method fails.
APPENDIX

In this appendix we state two well-known results used in the proofs for the convenience of the reader.

**Lemma 4:** For odd $q$ let $\eta$ be the quadratic character of $\mathbb{F}_q$.
Then we have

$$\sum_{x \in \mathbb{F}_q} \eta(x)\eta(x + a) = -1, \quad a \in \mathbb{F}_q^*.$$  

**Proof:** See for example [5, Lemma 7.3.7]. $\square$

**Theorem 3 (Weil):** Let $\chi$ be a multiplicative character of $\mathbb{F}_q$ of order $s > 1$ and $f(X) \in \mathbb{F}_q[X]$ a polynomial which is not of the form $ag(X)^s$ with $d$ different zeros. Then we have

$$\left|\sum_{x \in \mathbb{F}_q} \chi(f(x))\right| \leq (d - 1)q^{1/2}.$$  

**Proof:** See for example [6, Theorem 5.41]. $\square$

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their useful comments.

REFERENCES

[1] S. D. Cohen and G. L. Mullen, “Primitive elements in finite fields and Costas arrays,” *Applicable Algebra Eng., Commun. Comput.*, vol. 2, no. 1, pp. 45–53, Mar. 1991.
[2] K. Drakakis, R. Gow, S. Rickard, J. Sheekey, and K. Taylor, “On the maximal cross-correlation of algebraically constructed Costas arrays,” *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4612–4621, Jul. 2011.
[3] S. Golomb and H. Taylor, “Two-dimensional synchronization patterns for minimum ambiguity,” *IEEE Trans. Inf. Theory*, vol. IT-28, no. 4, pp. 600–604, Jul. 1982.
[4] S. W. Golomb and H. Taylor, “Constructions and properties of Costas arrays,” *Proc. IEEE*, vol. 72, no. 9, pp. 1143–1163, Sep. 1984.
[5] D. Jungnickel, *Finite Fields: Structure and Arithmetic*. Mannheim, Germany: Bibliographisches Institut, 1993.
[6] R. Lidl and H. Niederreiter, *Finite Fields* (Encyclopedia of Mathematics and Its Applications), 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 1997.
[7] O. Moreno and J. Sotero, “Computational approach to conjecture a of Golomb,” in *Proc. 20th Southeastern Conf. Combinatorics, Graph Theory, Comput.*, Boca Raton, FL, USA, vol. 70, 1990, pp. 7–16.

Domingo Gómez-Pérez received the Ph.D. degree in mathematics and computer science from the University of Cantabria, Santander, Spain, in 2006. He has been a Visiting Academic in different research centers, including the Johann Radon Institute for Computational and Applied Mathematics (RICAM), Macquarie University, the University of New South Wales, Royal Holloway, and the University of London. He is currently an Associate Professor with the University of Cantabria. His research interests include cryptography, sequences, finite fields, and quasi-Monte Carlo methods.

Arne Winterhof received the Diploma and Ph.D. degrees in mathematics from the Technical University of Braunschweig, Germany, in 1994 and 1996, respectively, and the Habilitation degree (Post-Doctoral Lecture Qualification) from the University of Vienna, Austria. From 1999 to 2002, he worked as a Research Scientist with the Institute of Discrete Mathematics, Austrian Academy of Sciences, Vienna, Austria. From 2002 to 2003, he was with Temasek Laboratories, National University of Singapore. Since 2003, he has been with the Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Linz, Austria. His main research interests include finite fields and their applications, in particular, cryptography and pseudorandom number generation. He was awarded the Hlawka Prize in 2004 and the Advanced Award of the Austrian Mathematical Society in 2010.