

# On the hops present in Costas permutations

Konstantinos Drakakis\*

January 26, 2009

## Abstract

We determine that exponential Welch permutations lead in general to the smallest maximal frequency hops among all Costas permutations, and are also relatively easy to study, as a closed formula exists for the maximal hop. Through extensive collection of data for logarithmic Welch and Golomb permutations, on the other hand, it is found that a) these 2 families behave (almost) identically, and that b) their maximal hops do not get as small as in exponential Welch permutations.

## 1 Introduction

Mathematical studies of Costas permutations [1, 2] have so far disregarded the limited frequency-hopping rates [6] of filters used in SONAR and RADAR systems: frequencies cannot switch instantaneously. The delay introduced due to the hardware response time tends to be less and less negligible as the size of the frequency hop increases. Therefore, waveforms that contain large frequency hops tend to deviate significantly from their (ideal) expected behavior, as described by the Costas permutation: not all Costas permutations (even if the choice is restricted within the same order) are equally suitable for applications. It becomes therefore essential to identify the families of Costas permutations with the smallest possible frequency hops.

In this work we will see that the maximal hop within an exponential Welch permutation can be completely described in terms of its order and the primitive root used in its generation, but little progress can be made in the cases of logarithmic Welch and Golomb permutations: for these classes tables of results can be compiled, which lead to a quite unexpected conjecture.

## 2 Basics

### 2.1 Definition of the Costas property

Let us begin with the definition of a Costas function/permutation [1, 2, 3]:

---

\***Address:** UCD CASL, University College Dublin, Belfield, Dublin 4, Ireland. **Email:** Konstantinos.Drakakis@ucd.ie. The author is also affiliated with the School of Electrical & Electronic Engineering, University College Dublin, Ireland.

**Definition 1.** Let  $[n] := \{1, \dots, n\}$ ,  $n \in \mathbb{N}$  and consider a bijection  $f : [n] \rightarrow [n]$ ;  $f$  is a Costas permutation iff:

$$f(i+k) - f(i) = f(j+k) - f(j) \Rightarrow i = j \text{ or } k = 0.$$

A permutation  $f$  corresponds to a permutation array  $A_f = [a_{i,j}^f]$  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:  $a_{f(i),i}^f = 1$ . It is customary to represent the 1s of a permutation array as “dots” and the 0s as “blanks”. From now on the terms “array” and “permutation” will be used interchangeably, in view of this correspondence.

The Costas property is invariant under horizontal and vertical flips, as well as transpositions around the diagonals (and therefore also under rotations of the array by multiples of  $90^\circ$ , which can be expressed as combinations of the previous two operations), hence a Costas array gives birth to an equivalence class that contains either 8 Costas arrays, or 4 if the array happens to be symmetric.

**Definition 2.** Let  $f : [n] \rightarrow [n]$ ,  $n \in \mathbb{N}$ : the maximal hop of  $f$  is  $\|f\|_\infty = \max_{k \in [n-1]} |f(k+1) - f(k)|$ .

### 2.2 Construction methods

There exist two algebraic methods for the construction of Costas permutations, known as the Golomb and Welch methods [3, 7, 8]:

**Theorem 1** (Exponential Welch construction  $W_1^{\text{exp}}(p, g, c)$ ). *Let  $p$  be a prime, let  $g$  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  $f : [p-1] \rightarrow [p-1]$  where  $f(i) = g^{i-1+c} \pmod p$  is a bijection with the Costas property.*

It follows from the definition that  $f(i) + f((p-1)/2 + i) = p$ ,  $i \in [(p-1)/2]$ : this property is known as *anti-reflective symmetry*. Flips of  $W_1^{\text{exp}}$ -arrays are also  $W_1^{\text{exp}}$ -arrays; in general, however, their transposes are not: instead, they form a family known as *logarithmic Welch arrays*. The two families are disjoint for  $p > 5$  [5].

**Theorem 2** (Logarithmic Welch construction  $W_1^{\text{exp}}(p, g, c)$ ). *Let  $p$  be a prime, let  $g$  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  $f : [p-1] \rightarrow [p-1]$  where  $i = g^{f(i)-1+c} \pmod p \Leftrightarrow f(i) \equiv \log_g(i) + 1 - c \pmod{p-1}$  is a bijection with the Costas property.*

**Theorem 3** (Golomb construction  $G_2(p, m, a, b)$ ). *Let  $p$  be a prime,  $m \in \mathbb{N}$ , and let  $a, b$  be primitive roots of the finite field  $\mathbb{F}(p^m)$  of  $q = p^m$  elements; then, the function  $f : [q - 2] \rightarrow [q - 2]$  where  $a^{f(i)} + b^i = 1$  is a bijection with the Costas property.*

Flips and transpositions of  $G_2$ -arrays lead also to  $G_2$ -arrays.

## 3 Results

### 3.1 A lower bound

The maximal hop of a function can be as low as 0 (when  $f$  is constant). The maximal hop of a permutation has to be at least 1, since no two values of a permutation are equal; the maximal hop of the identity permutation  $f(i) = i$ ,  $i \in [n]$  is 1. The maximal hop of a Costas permutation, however, is significantly larger:

**Theorem 4.** *Let  $f : [n] \rightarrow [n]$ ,  $n \in \mathbb{N}^*$  be a Costas permutation: then  $\|f\|_\infty = \left\lfloor \frac{n}{2} \right\rfloor$ .*

*Proof.*  $\|f\|_\infty$  is the maximum in absolute value over the  $n-1$  numbers  $\{f(1+j) - f(j) : j \in [n-1]\}$ ; no two can be equal, so in order to keep  $\|f\|_\infty$  as low as possible we have to select them in increasing absolute value, making use of both signs:  $-1, +1, -2, +2, -3, +3, \dots$ . If the absolute value  $k$  is included, we have included at least  $2k-1$  and at most  $2k$  elements, and we need the smallest  $k$  such that  $2k-1 = n-1$  if  $n$  is even, and  $2k = n-1$  if  $n$  is odd, implying in either case that  $k = \left\lfloor \frac{n}{2} \right\rfloor$ . This completes the proof.  $\square$

### 3.2 A tight case

Theorem 4 does not guarantee that the smallest possible value for  $\|f\|_\infty$ , namely  $\left\lfloor \frac{n}{2} \right\rfloor$ , is actually attained. This is the subject of the following

**Theorem 5.** *Let  $p$  be a prime such that 2 is a primitive root of  $\mathbb{F}(p)$ ; then  $\|W_1^{\text{exp}}(p, 2, c)\|_\infty = \frac{p-1}{2}$  and therefore  $W_1(p, 2, c)$  is a Costas permutation of order  $p-1$  with the minimal maximal hop possible.*

*Proof.* Let  $f = W_1^{\text{exp}}(p, 2, c)$ ; then  $f(i+1) = 2f(i) \bmod p$ ,  $i \in [p-2]$ . In particular, letting  $k \in \left[ \frac{p-1}{2} \right]$ :

- If  $f(i) = k$ , it follows that  $f(i+1) = 2k$  and  $|f(i+1) - f(i)| = k$ .
- If  $f(i) = \frac{p-1}{2} + k$ , it follows that  $f(i+1) = (p-1 + 2k) \bmod p = 2k-1$ , whence

$$|f(i+1) - f(i)| = \left| 2k-1 - k - \frac{p-1}{2} \right| = \frac{p+1}{2} - k.$$

In either case,  $|f(i+1) - f(i)| \leq \frac{p-1}{2} \Rightarrow \|f\|_\infty \leq \frac{p-1}{2}$ , and Theorem 4 completes the proof.  $\square$

### 3.3 A general result for $W_1^{\text{exp}}$ -permutations

We can actually compute  $\|W_1^{\text{exp}}(p, g, c)\|_\infty$  in general:

**Theorem 6.** *Let  $p$  be a prime and let  $g$  be a primitive root in  $\mathbb{F}(p)$ ; let also  $v = p \bmod g$  and  $u = \left\lfloor \frac{p}{g} \right\rfloor$  so that  $p = ug + v$ .*

*Then:*

- *If  $g \leq u + v + 1$  or  $v = 1$ ,  $\|W_1^{\text{exp}}(p, g, c)\|_\infty = (g - 1) \left\lfloor \frac{p}{g} \right\rfloor$ . In particular, this condition is true if  $g < \sqrt{p}$ .*
- *If  $g > u + v + 1$  and  $v > 1$ ,  $\|W_1^{\text{exp}}(p, g, c)\|_\infty = (g - 1) \left\lfloor \frac{(k+1)p-1}{g} \right\rfloor - kp$  where  $k = \left\lfloor \frac{v-1}{g-v} \right\rfloor$ .*

*The result is in all cases independent of  $c$ .*

*Proof.* That the result does not depend on  $c$  follows directly from the anti-reflective symmetry of  $W_1^{\text{exp}}$ -arrays: including the hop between the first and the last column (that is, assuming the columns of the array are wrapped around a cylinder), every hop appears exactly twice, exactly  $\frac{p-1}{2}$  positions apart. Therefore, as  $c$  varies, the two maximal hops shift positions, but at least one will appear in the array's interior.

Let  $f = W_1^{\text{exp}}(p, g, c)$ ; then  $f$  follows the iteration:

$$f(i+1) = gf(i) \bmod p, \quad i \in [p-2] \Leftrightarrow f(i+1) = gf(i) - kp \text{ whenever } \left\lfloor \frac{kp-1}{g} \right\rfloor + 1 \leq f(i) \leq \left\lfloor \frac{(k+1)p-1}{g} \right\rfloor$$

for  $k \in [g] - 1$ . Note that, for  $k = 0$ , the left floor gives  $-1$ , but we really need 0: instead of using a new symbol, we will keep using the floor function to retain uniformity, but we will keep this exception in mind. It follows that, for the values of  $i$  corresponding to a fixed  $k$ :

$$f(i+1) - f(i) = (g-1)f(i) - kp \in \left\{ (g-1) \left( \left\lfloor \frac{kp-1}{g} \right\rfloor + 1 \right) - kp, \dots, (g-1) \left\lfloor \frac{(k+1)p-1}{g} \right\rfloor - kp \right\},$$

whence, for this fixed  $k$ ,

$$|f(i+1) - f(i)| \leq \max \left\{ \left| (g-1) \left( \left\lfloor \frac{kp-1}{g} \right\rfloor + 1 \right) - kp \right|, \left| (g-1) \left\lfloor \frac{(k+1)p-1}{g} \right\rfloor - kp \right| \right\}.$$

Using now the decomposition  $p = gu + v$ ,  $v \in [g] - 1 - \{0\}$  (note that  $v = 0$  is impossible),

$$|f(i+1) - f(i)| \leq \max \left\{ \left| (g-1) \left( \left\lfloor \frac{kv-1}{g} \right\rfloor + 1 \right) - k(u+v) \right|, \left| (g-1) \left( \left\lfloor \frac{(k+1)v-1}{g} \right\rfloor + u \right) - k(u+v) \right| \right\},$$

whence  $\|f\|_\infty = \max_{k \in [g]-1} \max\{|a_k|, |b_k|\}$  where

$$a_k = (g-1) \left( \left\lfloor \frac{kv-1}{g} \right\rfloor + 1 \right) - k(u+v),$$

$$b_k = (g-1) \left( \left\lfloor \frac{(k+1)v-1}{g} \right\rfloor + u \right) - k(u+v).$$

A direct comparison between  $a_{k+1}$  and  $b_k$  shows that  $b_k = a_{k+1} + p - (g-1)$  and this formula has some important consequences: if  $a_{k+1} > 0$ ,  $b_k > |a_{k+1}|$ ; and if  $b_k < 0$ ,  $|a_{k+1}| > |b_k|$ . Hence,  $\|f\|_\infty$  must be sought among the positive  $b_k$  and the negative  $a_{k+1}$  (but note that  $a_0$  and  $b_{g-1}$  have to be taken into account separately, as they are not covered by the range of  $k$  for which the formula is valid). A further simplification occurs by taking into account the anti-reflective symmetry of Welch permutations, whereby a hop of length  $x$  takes place iff a hop of length  $-x$  takes place. Hence, it is enough to focus on the positive  $b_k$  (for a suitable  $c$ ).

- Assume that either  $g \leq u+v+1$  or  $v=1$ : in the former case,  $g-1-(u+v) \leq 0$ , and, observing that either  $a_{k+1} = a_k - (u+v)$  or  $a_{k+1} = a_k + g - 1 - (u+v)$ , and similarly that either  $b_{k+1} = b_k - (u+v)$  or  $b_{k+1} = b_k + g - 1 - (u+v)$ , it follows that both  $\{a_k\}$  and  $\{b_k\}$ ,  $k \in [g]-1$  are decreasing sequences. This implies that  $\|f\|_\infty = b_0 = (g-1)u$ . In the latter case,

$$\left\lfloor \frac{kv-1}{g} \right\rfloor = \left\lfloor \frac{k-1}{g} \right\rfloor = 0 \text{ for all } k \in [g]-1$$

(remember the exception for  $k=0$ ), whence  $a_{k+1} - a_k = -(u+1) \Rightarrow a_{k+1} < a_k$ , and similarly  $b_{k+1} < b_k$ : the conclusion is the same.

- Assume that  $g > u+v+1$  and  $v > 1$ : then  $\{b_k\}$  starts out as an increasing sequence, for all values of  $k$  such that  $(k+1)v-1 \geq kg \Leftrightarrow v-1 \geq k(g-v)$ , because, while this condition is true,  $b_{k+1} - b_k = g-1-(u+v) > 0$ . The largest value of  $k$  before  $\{b_k\}$  decreases for the first time is then  $k = \left\lfloor \frac{v-1}{g-v} \right\rfloor$ , and therefore this corresponds to a local maximum of  $\{b_k\}$ . Is it a global maximum? As every time  $k$  increases,  $b_k$  increases by  $g-1-(u+v)$ , for the particular value of  $k$  we found we need to check that  $g-1+k(g-1-u-v) - (u+v) \leq g-1$ . But this implies that  $k \leq \frac{u+v}{g-1-(u+v)}$  which is obviously true, as  $v-1 < u+v$  and  $g-v > g-1-u-v$ . The result now follows.

This completes the proof.  $\square$

**Corollary 1.** Let  $p$  be a prime and let  $g$  be a primitive root in  $\mathbb{F}(p)$  such that  $g > \sqrt{p} > g^{-1} \pmod{p}$ ; then,

$$\|W_1^{\text{exp}}(p, g, c)\|_\infty = (g^{-1} \pmod{p} - 1) \left\lfloor \frac{p}{g^{-1} \pmod{p}} \right\rfloor.$$

*Proof.* The permutations generated by  $g$  and  $g^{-1} \pmod{p}$  have the same hops.  $\square$

### 3.4 Hops in $W_1^{\text{log}}$ - and $G_2$ -permutations

The treatment of  $W_1^{\text{log}}$ - and  $G_2$ -permutations, unlike  $W_1^{\text{exp}}$ -permutations, presents considerable difficulties; we can still compile tables with this information, however, carrying on the tradition of collection of data on Costas permutations regarding aspects of their behavior not easily explained [4, 9]. Results for  $G_2$ - and  $W_1$ -permutations (exponential and logarithmic) are shown in Figure 1; these results exhibit some regularity, and lead to the formulation of the following conjecture:

**Conjecture 1.** There exist constants  $C_{g,i}, C_{w,i} > 0$ ,  $i = 1, 2$  such that, as  $p \rightarrow \infty$ ,

$$\frac{\min_{g,c} \|W_1^{\text{log}}(p, g, c)\|_\infty}{p} \approx 1 - C_{w1} \sqrt{\frac{\ln(p)}{p}} - C_{w2} \frac{\ln(p)}{p},$$

$$\frac{\min_{a,b} \|G_2(p, a, b)\|_\infty}{p} \approx 1 - C_{g1} \sqrt{\frac{\ln(p)}{p}} - C_{g2} \frac{\ln(p)}{p}.$$

The error in these approximations is a decreasing oscillation around 0. The part of the conjecture regarding  $G_2$ -permutations remains true for extension fields (of size equal to the power of a prime).

The data suggests that  $C_{w1} = C_{g1} \approx 1.25$  and that  $C_{w2} \approx -1$  while  $C_{g2} \approx 0$ . These estimates have also been verified on further data points, of a higher order of magnitude than those appearing in Figure 1; the suggested approximations were found to remain valid in these ranges as well, as well as on extension fields for the case of  $G_2$ -permutations.

Figure 1 shows the quality of the approximation of the data by the above formulas, by looking both at the fraction of the hops over the field size ( $\min_{g,c} \|W_1^{\text{log}}(p, g, c)\|_\infty/p$ ,  $\min_{a,b} \|G_2(p, a, b)\|_\infty/p$ ) and at their difference ( $p - \min_{g,c} \|W_1^{\text{log}}(p, g, c)\|_\infty$ ,  $p - \min_{a,b} \|G_2(p, a, b)\|_\infty$ ): it can be seen that the approximation is excellent, and that, in the case of  $W_1^{\text{log}}$ -permutations, the second order correction does make a difference and gives better results.

The results presented in Figure 1 needed significant computational time, namely about 2.5 weeks of single CPU time on a 2.0 GHz processor using Matlab code.

## 4 Conclusion

The most useful Costas permutations in SONAR/RADAR applications are those whose frequency hops are as small as possible. The maximal hop present in a Costas permutation of order  $n$  is always at least  $n/2$ , and  $W_1^{\text{exp}}$ -permutations generated by the primitive root 2 achieve this lower bound for  $n = p-1$ ,  $p$  prime. Among all algebraically constructible Costas permutations built in a finite field,  $W_1^{\text{exp}}$ -permutations exhibit the smallest maximal hop (except for some small orders), whereas the minimum of the maximal hops over all  $W_1^{\text{log}}$ -permutations and over all  $G_2$ -permutations seem to have the same asymptotical behavior, differing only by a second order correction. Although

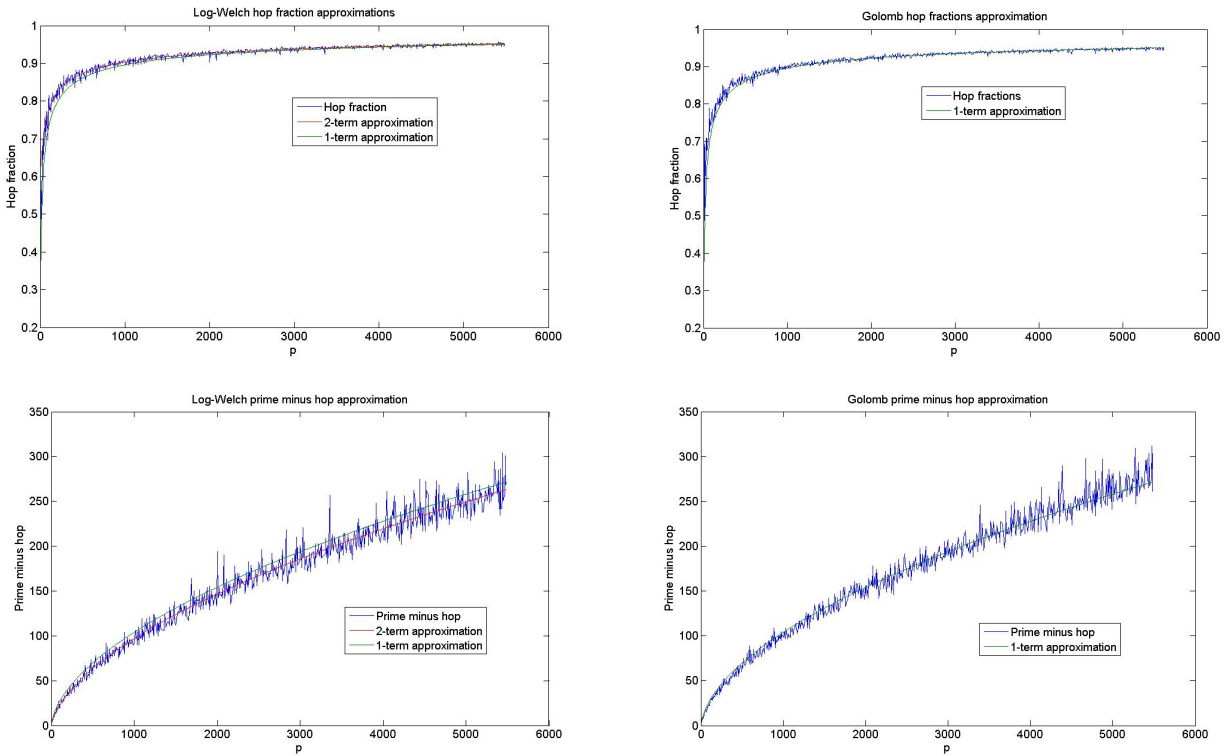


Figure 1: (top left) the approximation of  $\min_{g,c} \|W_1^{\log}(p, g, c)\|_{\infty}/p$  by  $1 - 1.25\sqrt{\ln(p)/p} + \ln(p)/p$  and  $1 - 1.25\sqrt{\ln(p)/p}$ ; (top right) the approximation of  $\min_{a,b} \|G_2(q, a, b)\|_{\infty}/p$  by  $1 - 1.25\sqrt{\ln(p)/p}$ ; (bottom left) the approximation of  $p - \min_{g,c} \|W_1^{\log}(p, g, c)\|_{\infty}$  by  $1.25\sqrt{p \ln(p)} - \ln(p)$  and  $1.25\sqrt{p \ln(p)}$ ; (bottom right) the approximation of  $p - \min_{a,b} \|G_2(q, a, b)\|_{\infty}$  by  $1.25\sqrt{p \ln(p)}$ .

a closed formula for the maximal hop in a specific  $W_1^{\text{exp}}$ -permutation has been established, this has not been possible for the cases of  $W_1^{\log}$ - and  $G_2$ -permutations.

## Acknowledgements

The author is indebted to Masoud Farshchian, a student in Rensselaer Polytechnic Institute's Department of Mathematical Sciences, who introduced him to this problem during the CISS 2006 conference in Princeton University.

## References

- [1] J. P. Costas. "Medium constraints on sonar design and performance." Technical Report Class 1 Rep. R65EMH33, GE Co., 1965
- [2] J. P. Costas. "A study of detection waveforms having nearly ideal range-doppler ambiguity properties." Proceedings of the IEEE, Volume 72, No. 8, pp. 996-1009, August 1984
- [3] K. Drakakis. "A review of Costas arrays." Journal of Applied Mathematics, Volume 2006
- [4] K. Drakakis. "Three challenges in Costas arrays." Ars Combinatoria (to appear)
- [5] K. Drakakis, R. Gow, L. O'Carroll. "On the symmetry of Welch- and Golomb-constructed Costas arrays" Discrete Mathematics (to appear)
- [6] M. Farshchian. Personal communication. IEEE CISS 2006
- [7] S. Golomb. "Algebraic Constructions For Costas Arrays." Journal Of Combinatorial Theory Series A, Volume 37, Issue 1, pp. 13-21, 1984
- [8] S. Golomb and H. Taylor. "Constructions and properties of Costas arrays", Proceedings of the IEEE, Vol. 72, pp. 1143-1163, 1984.
- [9] S. Rickard. "Large sets of frequency hopped waveforms with nearly ideal orthogonality properties." Masters thesis, MIT, 1993