

Costas arrays and the extension of Lambert's function on finite fields

Konstantinos Drakakis*

January 26, 2009

Abstract

Motivated by a problem in Costas arrays, we suggest a generalization of Lambert's W -function in finite fields and study some of its properties.

Mathematics Subject Classification: 11B50, 11B75, 32A05, 32A20, 33E30, 33E50

Keywords: Lambert function, Costas arrays, Golomb rulers

1 Introduction

An interesting feature of Welch Costas arrays that has proved to be extremely hard to compute is the number of dots on their main diagonal. The only results available today on this subject have been obtained through exhaustive search, while the existence of analytical solutions is still under investigation [8]. Our interest in the diagonals of Costas arrays is motivated by the fact that they form Golomb rulers, the main diagonal being potentially the longest of them. Golomb rulers have many practical applications in engineering, in particular in sensor placement of any kind (e.g. in astronomy [2] etc.), as well as in the optimal allocation of transmission frequencies to radio stations in order to minimize cross-interference due to harmonics [1].

A possible course of action towards the derivation of a closed form solution is to “lift” the problem into the corresponding one in non-finite fields (specifically \mathbb{R} and \mathbb{C}), where the solution is known. The necessary second step then involves mapping the solution back to finite fields. This procedure has proved to be very fruitful in countless other occasions. In our case, the solution in \mathbb{C}

***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 & Mechanical Engineering, University College Dublin.

will be seen to be given by Lambert's W -function; hence, what we really seek is a suitable generalization of Lambert's function in finite fields. To the best of our knowledge, this is something that has not been attempted before, so we take a first step here and derive a few simple properties.

2 Costas and Welch arrays

Simply put, a Costas array [5, 6, 7] is a square arrangement of dots and blanks, such that there is exactly one dot per row and column, and such that all vectors between dots are distinct.

Definition 1. Let $f : [n] \rightarrow [n]$, where $[n] = \{1, \dots, n\}$, $n \in \mathbb{N}$, be a bijection; then f has the *Costas property* iff the collection of vectors $\{(i-j, f(i) - f(j)) : 1 \leq j < i \leq n\}$, called *the distance vectors*, are all distinct, in which case f is called a *Costas permutation*. The corresponding *Costas array* A_f is the square array $n \times n$ where the elements at $(f(i), i)$, $i \in [n]$ are equal to 1 (dots), while the remaining elements are equal to 0 (blanks):

$$A_f = [a_{ij}] = \begin{cases} 1 & \text{if } i = f(j) \\ 0 & \text{otherwise} \end{cases}, \quad j \in [n]$$

There are 2 known construction algorithms for Costas arrays: the Welch method, whose definition we now give, and the Golomb method, which is of no further interest to us in this work [7, 9].

Definition 2 (Exponential Welch construction $W_1(p, g, c)$). Let p be a prime, g a primitive root of the finite field $\mathbb{F}(p)$, and $c \in [p-1]-1$; the *exponential Welch permutation* corresponding to g and c is defined by $f(i) = g^{i-1+c} \bmod p$, $i \in [p-1]$.

A Golomb ruler is a set of integers where differences between pairs are distinct:

Definition 3. Let $f : [m] \rightarrow [n]$, $m, n \in \mathbb{N}$ be an injection such that $f(1) = 1$, $f(m) = n$ (clearly $m \leq n$). f is a *Golomb ruler* iff

$$\forall i, j, k, l \in [m] : f(i) - f(j) = f(k) - f(l) \Leftrightarrow \{i, j\} = \{k, l\}.$$

3 Dots on the main diagonal of Welch arrays

It is clear that, in order to find the dots on the main diagonal of $W_1(p, g, c)$, we need to find the solutions in i of:

$$i \equiv g^{i-1+c} \bmod p, \quad i \in [p-1] \tag{1}$$

which can be rewritten as

$$-ig^{-i} \equiv -g^{c-1} \pmod{p}; \quad (2)$$

setting $u = -i$, $k = -g^{c-1}$, we obtain

$$ug^u \equiv k \pmod{p}. \quad (3)$$

We denote the solution of this equation as $u = W_g(k)$, leaving aside for the moment the (important) question of existence and uniqueness of this value. We focus rather on finding the effective range of u so that all possible k in (3) can be spanned: it is clear that all u' such that both $u' \equiv u \pmod{p-1}$ and $u' \equiv u \pmod{p}$ result to the same k . Since $(p-1, p) = 1$, we obtain $u' \equiv u \pmod{p(p-1)}$, hence we need to consider $p(p-1)$ values for u .

Can we simplify this definition further? In particular, can we express W_g in terms of W_h , where g and h are different primitive roots in $\mathbb{F}(p)$? Let us associate with $\mathbb{F}(p)$ one of its primitive roots (say the smallest one in the usual integer ordering, although this specific choice plays no role in our argument) which we denote by g_p ; then, we can write $g = g_p^r$ for some $r \in [p-2]$ such that $(r, p-1) = 1$. It follows that

$$\begin{aligned} rug_p^{ru} \equiv rk \pmod{p} &\Leftrightarrow ru = W(rk) \pmod{p(p-1)} \Leftrightarrow \\ &u \equiv \frac{W(rk)}{r} \pmod{p(p-1)} \end{aligned} \quad (4)$$

Therefore, we only need to consider W_g for a particular g .

Given $k \in [p] - 1$, how many $u \in [(p-1)p] - 1$ satisfy (3)? Denoting for simplicity $u_1 = u \pmod{p}$, $u_2 = u \pmod{p-1}$, (3) becomes $u_1 g^{u_2} \equiv k \pmod{p}$. We see that, as u spans $[(p-1)p]$, (u_1, u_2) spans all of $([p] - 1) \times ([p-1] - 1)$, hence (3) has exactly $p-1$ solutions for any given value of k .

We collect our observations in the following theorem:

Theorem 1. *Let p be a prime, g a primitive root in $\mathbb{F}(p)$, and $k \in [p] - 1$; the equation*

$$ug^u \equiv k \pmod{p}, \quad u \in [(p-1)p] - 1 \quad (5)$$

has exactly $p-1$ solutions. Therefore, the equation

$$ug^u \equiv k \pmod{p}, \quad u \in [p] - 1 \quad (6)$$

has those solutions of (5) that happen to fall within $[p] - 1$.

What is this function W ? Let us consider it in \mathbb{C} instead of $\mathbb{F}(p)$. Setting without loss of generality $g = e$, Napier's number, (3) becomes

$$W(z)e^{W(z)} = z, \quad z \in \mathbb{C}; \quad (7)$$

we recognize this as Lambert's W -function [4].

4 Lambert's function

We do not intend to give here an exhaustive overview of Lambert's W -function, especially since there exists an excellent overview in the literature already [4]. Our intention is rather to mention the basics only in order to acquaint the reader with it.

Lambert's function is multi-valued on the complex plane, just like the complex logarithm. In the standard way, we can break it into single-valued branches, which turn out to be infinitely many, by defining a branch cut, usually $(-\infty, -e^{-1})$ on the negative real axis. In particular, we denote by W_0 the principal branch that contains the positive real axis in its range. W_0 cannot be expressed in terms of elementary functions, but a Taylor expansion around $z = 0$ is possible, since the function is analytic there. Henceforth, we focus exclusively on the principal branch, and we use the symbol W instead of W_0 , as there is no longer danger of confusion.

There are 2 main methods to derive the formula for W : either directly through implicit differentiation of its defining formula (7), or through the use of a more general tool, namely Lagrange's inversion theorem ([3], p. 61).

Let us see the direct method first: differentiating (7), we get $W'e^W + W'We^W = 1$, whence $W' = \frac{1}{(1+W)e^W}$. It follows that $W(0) = 0$, $W'(0) = 1$. Inductively we can show that

- $W^{(n)} = \frac{e^{-nW} P_n(W)}{(1+W)^{2n-1}}$, where $P_{n+1}(w) = -(nw + 3n - 1)P_n(w) + (1+w)P'_n(w)$, $n \in \mathbb{N}^*$, with $P_1(w) = 1$;
- $W^{(n)}(0) = P_n(0) = (-n)^{n-1}$, $n \geq 1$;
- and $P'_n(0) = (3n - 1)(-n)^{n-1} + (-1)^n(n + 1)^n$, $n \geq 1$.

Hence,

$$W(z) = \sum_{n=0}^{\infty} \frac{W^{(n)}(0)}{n!} z^n = \sum_{n=1}^{\infty} \frac{(-n)^{n-1}}{n!} z^n. \quad (8)$$

The radius of convergence of this series can be found to be e^{-1} .

Turning now to the alternative method, we use Lagrange's inversion theorem:

Theorem 2. *Let a function f be analytic in the neighborhood of $a \in \mathbb{C}$, where, in addition, $f'(a) \neq 0$. Then,*

1. *there exists a neighborhood of a where f is bijective on its range, hence invertible there;*
2. *its inverse is also analytic;*

3. letting g denote the inverse function in question, its Taylor expansion around $b = f(a)$ is given by the formula:

$$g(z) = a + \sum_{n=1}^{\infty} \frac{d^{n-1}}{dw^{n-1}} \left(\frac{w-a}{f(w)-b} \right)^n \Big|_{w=a} \frac{(z-b)^n}{n!}$$

Proof. See [3], pp.61–62. □

Now, in our case, $f(w) = we^w$, $f(0) = 0$, and $f'(0) = 1 \neq 0$. We use then the theorem above with $a = b = 0$: $\frac{d^{n-1}}{dw^{n-1}} \left(\frac{w-a}{f(w)-b} \right)^n \Big|_{w=a} = \frac{d^{n-1}e^{-nw}}{dw^{n-1}} \Big|_{w=0} = (-n)^{n-1}$, and we reach the same formula as before.

5 Lambert's function on finite fields

We have been unable to locate in the literature any attempts to extend Lambert's function to finite fields, as we defined it in Section 3. It is well known, however, that many functions first defined and studied in \mathbb{C} are subsequently successfully extended in finite fields or groups (e.g. Riemann's ζ -function, elliptic curves etc.), so it is not obvious whether such an extension has never been attempted before or was attempted and failed.

According to our investigation in Sections 3 and 4 then, the following hold true for the generalization of Lambert's function:

- The appropriate defining relation for Lambert's W -function of $\mathbb{F}(p)$, p prime is $W(x)g_p^{W(x)} \equiv x \pmod{p}$, where $W : [p] - 1 \rightarrow [p(p-1)] - 1$, and g_p is the primitive root of $\mathbb{F}(p)$ associated with p , as mentioned in Section 3. In particular, W 's range is a superset of $\mathbb{F}(p)$.
- W is multi-valued: in particular, for any $x \in \mathbb{F}(p)$, $W(x)$ takes exactly $p-1$ values. This is reminiscent of the situation in \mathbb{C} , so we can say here by analogy that W has $p-1$ branches, where branch k may be defined by the relation $W \pmod{p-1} = k$, $k \in [p-1] - 1$.

The definition of the branches above is appropriate in the sense that for each x each branch contains exactly one value of $W(x)$. The solution of the original problem proposed, however, namely (6) in Theorem 1, does not correspond to a particular branch, but rather is a collection of solutions across branches.

6 Conclusion

Motivated by a problem about Costas arrays, namely the determination of the number of dots on the main diagonal of a Welch Costas array, we were led to consider the generalization of Lambert's W function to a finite field $\mathbb{F}(p)$, p prime. We saw that this generalization is multi-valued, just like in \mathbb{C} , in a very regular way, as it assumes $p - 1$ values in $[p(p - 1)] - 1$ for each value in its domain. This is the only "strange" feature of the new definition: the domain and the range of W are not the same.

As far as we have been able to assert by searching the literature, there has never been a previous attempt to define Lambert's function on finite fields. Such a definition is not only useful in applications (in our case Costas arrays and Golomb rulers), but also presents an intrinsic mathematical interest.

Acknowledgements

This material 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.

References

- [1] W. C. Babcock. "Intermodulation interference in radio systems." Bell Systems Technical Journal, 1953, pp. 63–73.
- [2] F. Biraud, E. Blum, and J. Ribes. "On optimum synthetic linear arrays with application to radioastronomy." IEEE Transactions on Antennas and Propagation, Volume 22, Issue 1, 1974, pp. 108–109.
- [3] G. F. Carrier, M. Krook, and C. E. Pearson. "Functions of a Complex Variable: Theory and Technique.", Hod Books, 1983.
- [4] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth. "On the Lambert W Function." Advances in Computational Mathematics, volume 5, 1996, pp. 329–359.
- [5] J. P. Costas. "Medium constraints on sonar design and performance." Technical Report Class 1 Rep. R65EMH33, GE Co., 1965.
- [6] 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.

- [7] K. Drakakis. “A review of Costas arrays.” *Journal of Applied Mathematics*, Volume 2006.
- [8] K. Drakakis. “Three challenges in Costas arrays.” *Ars Combinatoria*, Volume 89, 2008.
- [9] S. Golomb. “Algebraic Constructions For Costas Arrays.” *Journal Of Combinatorial Theory Series A*, Volume 37, Issue. 1, pp. 13–21, 1984.