A stochastic model for the number of fixed points of a Welch Costas permutation

Konstantinos Drakakis*
UCD CASL
University College Dublin
Ireland
Email: Konstantinos.Drakakis@ucd.ie

February 24, 2009

Abstract

Exploiting the empirical observation that the probability of k fixed points in a Welch Costas permutation is approximately the same as in a random permutation of the same order, we propose a stochastic model for the most probable maximal number of fixed points in a Welch Costas permutation.

1 Introduction

Costas arrays are square arrangements of dots and blanks with exactly one dot per row and column (a permutation array), such that no 4 dots form a parallelogram and so that no 3 dots lying on a straight line are equidistant. They appeared for the first time in 1965 in the context of SONAR detection [6, 7], 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. Having found examples of Costas permutations up to order 12 using pencil and paper, but unable to continue, let alone to find a general construction technique himself, he approached Prof. S. Golomb (after approaching several other mathematicians without success), who developed two generation techniques [10, 15, 16] for Costas permutations, both based on the theory of finite fields, known as the Welch and the Golomb method, respectively.

*The author is also affiliated with the School of Mathematics, University College Dublin, Ireland

These arc still the only general construction methods for Costas permutations available today.

One analog of a Costas permutation in one dimension (note that there is no obvious generalization of the concept of permutation in an odd number of dimensions) is the Golomb ruler: a linear arrangement of dots and blanks lying on multiples of a unit distance such that all pairwisc distances between dots are distinct. It has also important applications in engineering, for example in radio-frequency allocation for avoiding third-order interference [1], in generating convolutional self-orthogonal codes [20], in the formation of optimal linear telescope arrays in radio-astronomy [2] etc. Of great interest, in particular, are (asymptotically) optimal Golomb rulers, which, in a given length, pack the maximal possible number of points.

Though Golomb rulers appeared in the engineering literature in the 1950s, the same combinatorial object under an equivalent definition (and a different name) had appeared in the mathematical literature quite earlier, in the 1930s, as a Sidon set (a set of integers whcre all pairwise sums are distinct) [13]. This observation took some time, and in thc mcantime the 2 communities had been working separately, unaware of each other's work [8].

Clearly any diagonal of a Costas array yields a Golomb ruler; of particular intcrest is the main diagonal, being potentially the longest Golomb ruler. We previously demonstrated that the main diagonal of a special sub-family of Golomb Costas arrays yields asymptotically optimal Golomb rulers [12]. What about Welch Costas arrays though? Although we offered simulation results for various orders [11, 12], we were unable to suggest a formula.

In this work we take a step further by building an approximate probabilistic model for the number of fixed points of a Welch Costas permutation and using it to estimate the most probable value of the maximum of this quantity.

2 Basics

In this section we collect a set of properties and results used throughout the paper. For $n \in \mathbb{N}$, we set for brevity $[n] := \{1,\dots,n\}$, as this will be appearing quite often, along with some self-explicable variants, such as $[n]-1 := \{0,1,\dots,n-1\}$ etc.

2.1 Costas permutations

Let us begin with the definition of a Costas function/permutation [6, 7, 10]:

Definition 1. Consider a bijection $f : [n] \to [n]$; f is a Costas permutation iff:

$$\forall i, j, k \text{ such that } 1 \leq i, j, i+k, j+k \leq n : \\ f(i+k) - f(i) = f(j+k) - f(j) \Rightarrow i = j \text{ or } k = 0.$$

A permutation f corresponds to a permutation array $A_f = [a^f_{i,j}]$ 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: $a^f_{f(i),i} = 1$. 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^o, 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.

There exist algebraic generation techniques for Costas arrays; we will specifically need the exponential Welch construction:

Theorem 1 (Exponential Welch construction $W_1^{\exp}(q, g, c)$). *Let q be a prime, let g be a primitive root of the finite field $\mathbb{F}(q)$ of q elements, and let $c \in [q-1]-1$ be a constant; then, the function $f : [q-1] \to [q-1]$ where $f(i) = g^{i-1+c} \bmod q$ is a bijection with the Costas property.*

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*, which we will not be considering any further here, as the main diagonal remains invariant under transposition. The two families are disjoint for $p > 5$ [12], which implies that there are exactly $2(q-1)\phi(q-1)$ Welch permutations (both exponential and logarithmic) of order $q-1$.

2.2 Golomb rulers

Definition 2. Let $m, n \in \mathbb{N}$, and let $f : [m]-1 \to [n+1]-1$ be injective with $f(0) = 0$, $f(m-1) = n$ (whence $m \leq n$); f is a Golomb ruler of length n with m marks iff

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

In other words, consider a ruler of length n with marks on integer points; we need to select m marks (including 0 and n) so that no distance between pairs of points is repeated twice. Two important questions arise:

1. What is the maximal m possible for given n?
2. What is the minimal n possible for given m?

A Golomb ruler is optimal iff it satisfies either of the 2 conditions above; for neither case, however, do we have closed form answers, although several estimates exist: the simplest one is that a Golomb ruler of length n defines at most n possible distances, and, in order to have m points, the $\binom{m}{2}$ distances they define will need to be unique. It follows that

$$\binom{m}{2} = \frac{m(m-1)}{2} \leq n \Rightarrow m \leq \sqrt{2n} \text{ asymptotically.} \tag{1}$$

This turns out to be a very generous upper bound: improved arguments show that $m < \sqrt{n} + O(n^{1/4})$ [13] and even better that $m < \sqrt{n} + n^{1/4} + 1$ [17]. Furthermore, the maximal m for a given n satisfies asymptotically $m > \sqrt{n} - O(n^{5/16})$ [13], but it is conjectured to satisfy $m > \sqrt{n}$.

Clearly, the main diagonal of a Costas array of order n forms a Golomb ruler of length at most $n-1$; the maximal length is achieved whenever the array has dots at both $(1,1)$ and (n,n). Any diagonal of a Costas array is a Golomb ruler, but the main diagonal is potentially the longest one.

An excellent source of information about Golomb rulers/Sidon sets is A. Dimitromanolakis' diploma thesis [8].

2.3 Lambert's function

Lambert's function will play a key role in the construction of the two probabilistic models for the number of fixed points of a Welch permutation presented in later sections. We therefore summarize some basic facts about it here.

Lambert's function W [3, 5] is the inverse of $f(x) = xe^x$, $x \in \mathbb{R}$; $x \in \mathbb{C}$ can also be considered, but this extension will not be needed here. It is therefore defined by the relation

$$W(x)e^{W(x)} = x,\ W : [e^{-1}, \infty) \to [-1, \infty). \tag{2}$$

Note indeed that $\min_{x\in\mathbb{R}} xe^x = -e^{-1}$ at $x = -1$. When $x < 0$, W is multi-valued (with 2 values for every x, except for $x = e^{-1}$), and defining the range as above is one possible way to make it single-valued. Taking logarithms on both sides of (2) (for $x > 0$) we get

$$\ln(W(x)) + W(x) = \ln(x), \tag{3}$$

whence it follows that

$$W(x) \approx \ln(x), \ x \text{ positive and large.} \tag{4}$$

If we are interested in a second order correction too, we can set $W(x) = \ln(x) + w(x)$, whence:

$$w(x) + \ln(\ln(x) + w(x)) = 0 \approx w(x) + \ln(\ln(x)) \Rightarrow w(x) \approx -\ln(\ln(x)). \tag{5}$$

Therefore,

$$W(x) \approx \ln(x) - \ln(\ln(x)), \ x \text{ positive and large.} \tag{6}$$

2.4 The Kolmogorov-Smirnov test

The construction of the probabilistic models presented below relies on the approximation of a certain probability distribution by another. One of the available statistical measures of proximity of two probability distributions (among many others), and the one we choose to use in this work, is the Kolmogorov-Smirnov test, whose theory we now proceed to review.

Let F be a cumulative distribution function (cdf) and let X_i, $i \in [n]$, $n \in \mathbb{N}$ be i.i.d. random variables whose common cdf is F. It is well known that F can then be approximated by the empirical cumulative distribution

$$F_n(x) = \frac{1}{n}|\{i \in [n] : X_i \leq x\}|, \tag{7}$$

which, as $n \to \infty$, converges to F in various senses (almost surely for fixed x, uniformly in x in L^∞ etc.). We are specifically interested in the largest deviation between F_n and F, whose distribution is the subject of the following

Theorem 2 (Kolmogorov-Smirnov test). *Let $D_n = \sup\limits_x |F_n(x) - F(x)|$; then D_n is itself a random variable with the property that the limit random variable $D = \lim \sqrt{n}D_n$ exists and follows the Kolmogorov distribution K:*

$$K(x) = P(D \leq x) = 1 - 2\sum_{i=1}^{\infty}(-1)^{i-1}e^{-2i^2x^2}. \tag{8}$$

The proof is omitted (see [18] and also Wikipedia's entry on the Kolmogorov-Smirnov test); K is plotted in Figure 1. What is really striking about this theorem is that the limit distribution K turns out to be independent of F (see [14] for a simple proof of this fact, without deriving the formula for the distribution K); it is, in other words, a central limit theorem. This property makes this result an excellent goodness-of-fit statistical test: if

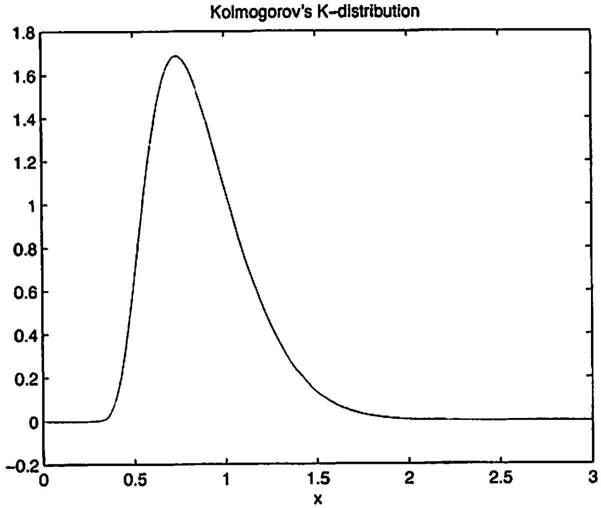

Figure 1: Plot of Kolmogorov's K-distribution

we suspect that some data are generated by n independent trials of a cdf F, we form the empirical distribution and compute $\sqrt{n}D_n$. Agreeing on a tolerated probability of error ϵ, we compute the value K_ϵ so that

$$K(K_\epsilon) = 1 - \epsilon. \tag{9}$$

If then $\sqrt{n}D_n > K_\epsilon$, we reject the hypothesis that our data set comes from F; the probability that we reject it by mistake (while the assumption is actually true, that is) is ϵ (for example, $K_{0.05} = 1.3581$ and $K_{0.01} = 1.6276$).

3 The number of fixed points in a permutation

The material in this section is well known and can be found in several classical references about combinatorics, or even mathematical puzzles. We choose to repeat all relevant derivations here, however, for reasons of completeness, as they are reasonably simple and brief.

3.1 The number of permutations without fixed points

A convenient intermediate result in our derivations is the number d_n of permutations of order n without fixed points. Such permutations are widely known as *derangements of n objects* [21], and determining their number is often referred to as *the problem of the misaddressed letters* [9], where one asks for the probability of placing n letters in n envelopes, so that no letter ends up in the correct envelope (assuming, of course, that to each letter corresponds exactly one envelope and vice versa).

Theorem 3. *The probability that a permutation of n objects contains no fixed points is*

$$f_n = \sum_{k=0}^{n} \frac{(-1)^k}{k!}, \quad n \geq 0;$$

therefore,

$$\lim f_n = \frac{1}{e}$$

Proof. Assume that, in a certain derangement, 1 is mapped on x; there are 2 possibilities:

- x is mapped to 1: then, the remaining $n-2$ objects can themselves be allocated in d_{n-2} ways. Given that x can be chosen in $n-1$ ways, and that all these choices are mutually exclusive, we obtain in total $(n-1)d_{n-2}$ permutations of this type;
- x is not mapped to 1: removing 1 from the domain and x from the range of the permutation, we see that the requirement that x be not mapped to 1 makes 1 the "correct" range value for x. By relabeling x to 1 in the domain, and y to $y-1$ for every $x < y \leq n$ in both the domain and the range, we end up with a derangement on $n-1$ objects. For every particular choice of x and there are exactly d_{n-1} derangements possible, and different choices of x lead to mutually exclusive derangements; since x can again be chosen in $n-1$ ways, we obtain a total of $(n-1)d_{n-1}$ derangements of this type.

It follows that

$$d_n = (n-1)[d_{n-1} + d_{n-2}], \tag{10}$$

along with the initial conditions $d_1 = 0$, $d_2 = 1$, which imply that $d_0 = 1$. Setting $d_n = n!f_n$ we obtain

$$nf_n = (n-1)f_{n-1} + f_{n-2} \Leftrightarrow n(f_n - f_{n-1}) = -(f_{n-1} - f_{n-2}), \tag{11}$$

along with $f_0 = 1$, $f_1 = 0$, and, setting $f_n - f_{n-1} = \frac{(-1)^n}{n!}h_n$, we reach the equation $h_n = h_{n-1}$, whence h_n is a constant h. Back-substitution leads to

$$f_n = h \sum_{k=0}^{n} \frac{(-1)^k}{k!}, \tag{12}$$

and the condition $f(0) = 1$ yields that $h = 1$. This completes the proof.

The well-known power series expansion for the exponential function

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} \tag{13}$$

yields that

$$e^{-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} = f_n + \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!} \Rightarrow \left|e^{-1} - f_n\right| \leq \frac{1}{(n+1)!} \tag{14}$$

which not only proves that

$$\lim f_n = \frac{1}{e}, \tag{15}$$

but also that the convergence is very rapid. □

3.2 The number of permutations with a certain number of fixed points

The expression for the number of permutations with $k > 0$ fixed points relies on the number of permutations without fixed points derived earlier:

Theorem 4. *The probability that a permutation of order n has exactly $0 \leq k \leq n$ fixed points is*

$$p(k,n) = \binom{n}{k} \frac{(n-k)!}{n!} \sum_{i=0}^{n-k} \frac{(-1)^i}{i!} = \frac{1}{k!} \sum_{i=0}^{n-k} \frac{(-1)^i}{i!} = \frac{f_{n-k}}{k!}.$$

Proof. Consider a permutation of order n with $0 \leq k \leq n$ fixed points. Once the fixed points have been chosen, and this can be done in $\binom{n}{k}$ ways, the remaining points must represent a derangement of $n - k$ objects, and there are d_{n-k} of those. Since different choices for the fixed points are mutually exclusive, we find that there are in total $\binom{n}{k}(n-k)! \sum_{i=0}^{n-k} \frac{(-1)^i}{i!}$ permutations with exactly fixed points. This completes the proof. □

Let now $n \to \infty$ for fixed k; Theorem 4 proves

Corollary 1. $\lim_n p(k,n) := p(k) = \frac{e^{-1}}{k!}.$

In other words, when n is large and k is small compared to n, $p(k,n)$ tends to be independent of n and approximated by $p(k)$ of Corollary 1. Note that $\mathcal{P} = \{p(k)\}_{k\in\mathbb{N}}$ is itself a probability distribution, as

$$\sum_{k=0}^{\infty} p(k) = e^{-1} \sum_{k=0}^{\infty} \frac{1}{k!} = e^{-1}e = 1; \tag{16}$$

alternatively we can recognize it directly as a Poisson distribution (whose mean value is equal to 1).

4 The number of fixed points in a Welch Costas permutation

In previous work [11] we tabulated the maximal number of fixed points of a $W_1^{\exp}$-permutation of order $q-1$ for all primes $q < 5000$ (see Figure 2), but we were unable to find a closed form solution for this quantity as a function of q; we simply formulated the conjecture that this quantity seems to be proportional to $\ln(q)$, which we justified through fitting. We propose below a more extensive probabilistic model that will allow us to further verify and refine this conjecture.

4.1 The motivating random experiment

We observed in the past [11] that the fraction of $W_1^{\exp}$-permutations without a fixed point approaches $1/e$, which is also asymptotically the fraction of permutations without a fixed point. This led us to conjecture that, as far as fixed points are concerned, $W_1^{\exp}$-permutations behave very much like random permutations, and the latter have the advantage that the distribution of their number of fixed points is known (Theorem 4), as is the asymptotic behavior of this distribution (Corollary 1). We now proceed to establish formally the proximity of the two distributions, using the Kolmogorov-Smirnov test, which will allow us to use the two distributions interchangeably and draw conclusions on the number of fixed points of $W_1^{\exp}$-permutations through the study of the number of fixed points of a randomly chosen permutation, or rather of its asymptotic behavior, as stated in Corollary 1.

As mentioned in Section 2.1, there exist exactly $m = (q-1)\phi(q-1)$ $W_1^{\exp}$-permutations of order $q-1$, when $q > 5$ is a prime. By finding the fixed points of each one, we computed the probability $u(k, q-1)$ for such a permutation to have exactly k fixed points. We then compared the probability distributions $\mathcal{U}_{q-1} = \{u(k, q-1)\}_{0\leq k\leq q-1}$ and $\mathcal{P}$, for all 669 primes $q < 5000$, using the Kolmogorov-Smirnov test (Section 2.4). The

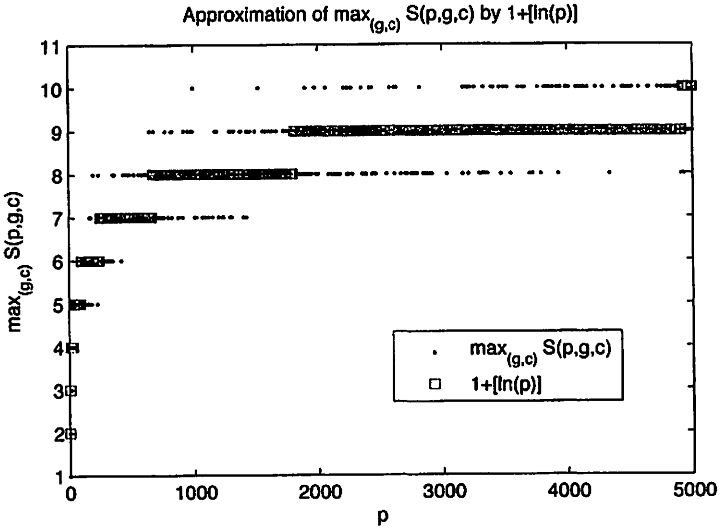

Figure 2: Plot of the maximum over all g and c of the number of fixed points of a $W_1^{\text{exp}}(q, g, c)$-permutation for $p < 5000$, along with the approximation by $1 + [\ln(p)]$.

corresponding values of $\sqrt{m}D_m$ are shown in Figure 3: taking the null hypothesis to be that $\mathcal{U}_{q-1}$ is an empirical distribution corresponding to $\mathcal{P}$, and setting an error level of 5%, we see that in 641 cases the null hypothesis cannot be rejected; on the other hand, 5% of 669 is approximately 33, while the remaining empirical distributions (where the null hypothesis is rejected) are $669 - 641 = 28$: in other words, the number of cases the null hypothesis fails is approximately equal to the number of cases we expect it to fail due to the choice of the error level (and we also need to discount small sample effects occurring for small q). This strengthens our conclusion even further: for large q, $\mathcal{P}$, the asymptotic estimate of the probability distribution of the number of fixed points of a randomly chosen permutation, is an excellent approximation for $\mathcal{U}_{q-1}$, the probability distribution of the number of fixed points of a randomly chosen W_1^{exp}-permutation. We formalize this even further in

Conjecture 1. For each k, $\lim_q \frac{u(k, q-1)}{p(k, q-1)} = 1$, or, equivalently, $\lim_q u(k, q-1) = p(k)$ (see Corollary 1).

This result is intuitively expected: the mechanism of the Welch construction is also known as a reasonably efficient pseudo-random number generator, and therefore W_1^{exp}-permutations are expected to be "randomly"

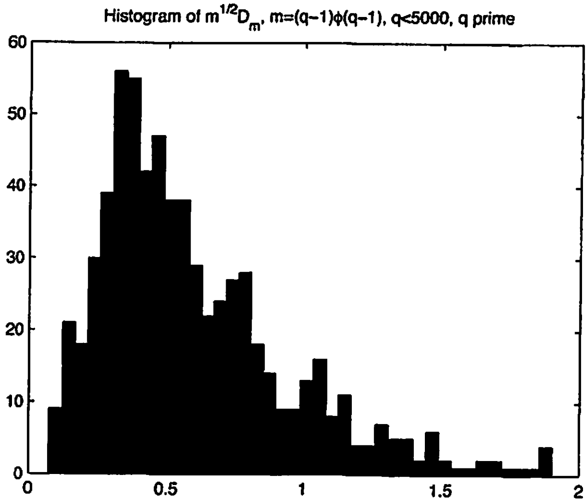

Figure 3: Plot of $\sqrt{m}D_m$, $m = (q-1)\phi(q-1)$, for all prime $q < 5000$.

distributed amongst all permutations, which is precisely what the Kolmogorov-Smirnov test indicates. Note that this result generalizes the result presented in Challenge 2 of [11], which focused exclusively on derangements.

4.2 A model for the maximal number of fixed points in Welch Costas arrays

What is then the maximal number of fixed points in a W_1^{exp}-permutation of order $q-1$? In Challenge 1 of [11] we conjectured that the answer is well approximated by

$$1 + [\ln(q)], \tag{17}$$

but this formula was determined empirically through fitting and was not based on any mathematical model. We now build such a model in order to test the validity of this formula and derive better approximations.

Given Conjecture 1, we can approximate the answer by a different, but closely related, random experiment, whereby we consider $m = (q-1)\phi(q-1)$ i.i.d. random variables X_i, $i \in [m]$ (as many as the W_1^{exp}-permutations of order $q-1$, that is) following the distribution $\mathcal{P}$ and ask for the probability distribution of their maximum; more precisely, we set

$$X^{(m)} = \max_{i=1,\ldots,m} X_i \tag{18}$$

and ask for the probability that $X^{(m)} = k$ or that $X^{(m)} \leq k$. The latter event is true if and only if $X_i \leq k$ for each i, whence

$$P(X^{(m)} \leq k) = p^m(k) = \frac{1}{e^m}\left(\sum_{i=0}^{k} \frac{1}{i!}\right)^m = \left(1 - \frac{1}{e}\sum_{i=k+1}^{\infty} \frac{1}{i!}\right)^m \qquad (19)$$

It follows that

$$P(X^{(m)} = k) = P(X^{(m)} \leq k) - P(X^{(m)} \leq k-1) =$$
$$= \left(1 - \frac{1}{e}\sum_{i=k+1}^{\infty} \frac{1}{i!}\right)^m - \left(1 - \frac{1}{e}\sum_{i=k}^{\infty} \frac{1}{i!}\right)^m ; \qquad (20)$$

using the differential approximation $x^m - (x-\epsilon)^m \approx m\epsilon x^{m-1}$, as well as the facts that factorials are rapidly increasing and that $1 - x \approx e^{-x}$ whenever $|x| \ll 1$, this can be simplified into

$$P(X^{(m)} = k) \approx \frac{m}{k!e}\left(1 - \frac{1}{e}\sum_{i=k+1}^{\infty} \frac{1}{i!}\right)^{m-1} \approx$$
$$\approx \frac{m}{k!e}\left(1 - \frac{1}{e}\frac{1}{(k+1)!}\right)^{m-1} \approx \frac{m}{k!e}\exp\left(-\frac{m-1}{(k+1)!e}\right). \qquad (21)$$

When k changes, the left factor in the RHS changes by a factor of approximately k, whereas the exponential in the right factor changes also by a factor of approximately k:

- When $m \ll (k+1)!e$, $P(X^{(m)} = k) \approx \frac{m}{k!e}$, which decreases rapidly to 0 as k grows.
- When $m \gg (k+1)!e$, the exponent is very large and dominates the formula's behavior, implying that, for small k, $P(X^{(m)} = k) \approx 0$ and that it is an increasing function of k.

As the probability increases for small k and decreases for large k, we expect it to have a maximum, which, intuitively, should occur when $m \approx (k+1)!e$. To make this more rigorous, set

$$l(k) = \ln(P(X^{(m)} = k)) = -\frac{m-1}{(k+1)!e} + \ln\left(\frac{m}{k!}\right) - 1. \qquad (22)$$

The maximum occurs at the value of k where

$$l(k) - l(k-1) \geq 0, \; l(k) - l(k+1) \geq 0. \qquad (23)$$

The explicit expressions for these differences are

$$l(k) - l(k+1) = -\frac{m-1}{(k+1)!e}\left(1 - \frac{1}{k+2}\right) + \ln(k+1) \geq 0,$$
$$l(k) - l(k-1) = \frac{m-1}{k!e}\left(1 - \frac{1}{k+1}\right) - \ln(k) \geq 0, \quad (24)$$

from which we obtain

$$\frac{k!\ln(k)}{1-\frac{1}{k+1}} \leq \frac{m-1}{e} \leq \frac{(k+1)!\ln(k+1)}{1-\frac{1}{k+2}}. \quad (25)$$

This can be approximately simplified as the largest k for which

$$k!\ln(k) \leq \frac{m}{e} \quad (26)$$

and, therefore, $k = \lfloor x \rfloor$ where

$$\Gamma(x+1)\ln(x) = \frac{m}{e}. \quad (27)$$

Using Stirling's approximation [4], whereby

$$\Gamma(x+1) \approx \sqrt{2\pi x}\left(\frac{x}{e}\right)^x, \quad (28)$$

we obtain

$$\sqrt{2\pi x}\left(\frac{x}{e}\right)^x \ln(x) = \frac{m}{e} \Leftrightarrow$$
$$\frac{1}{2}\ln(2\pi) + \left(x + \frac{1}{2}\right)\ln(x) - x + \ln(\ln(x)) = \ln(m) - 1 \quad (29)$$

and, assuming both m and x to be large,

$$x\ln(x) \approx \ln(m) \Leftrightarrow ue^u \approx \ln(m), \; x = e^u \quad (30)$$

whence

$$u \approx W(\ln(m)) \approx \ln(\ln(m)) - \ln(\ln(\ln(m))) \Leftrightarrow$$
$$x \approx e^{W(\ln(m))} \sim \frac{\ln(m)}{\ln(\ln(m))} \quad (31)$$

where W is Lambert's function (see Section 2.3). This finally leads to

$$k = \lfloor x \rfloor \approx \left\lfloor e^{W(\ln(m))} \right\rfloor \sim \left\lfloor \frac{\ln(m)}{\ln(\ln(m))} \right\rfloor. \quad (32)$$

We have proved

Theorem 5. *Assuming the truth of Conjecture 1, the most probable value of* $X^{(m)}$ *is asymptotically equal to* $\left\lfloor e^{W(\ln(m))} \right\rfloor \sim \left\lfloor \frac{\ln(m)}{\ln(\ln(m))} \right\rfloor$ *for large* m.

Note that we use $\sim$ to denote the fact that this approximation may be off by a multiplicative constant (or even slowly increasing function of m): the asymptotic approximation (6) does not include a constant term, hence, when exponentiated, as in (31), it leads to an ambiguity of a multiplicative constant (at least). Actually, more precise asymptotical analysis [5] shows the constant term in (6) to be 0, hence the multiplicative constant in (31) to be 1, so we could have been careless about this point.

It is evident from the series of the approximations made in the previous derivations that this asymptotic estimate holds for extremely large m, probably much larger than the ones considered for $q < 5000$. In view of this result, the logarithmic approximation (17) is inaccurate for large q (although not completely unjustifiable, and still valid obviously within this specific range): clearly $q < 5000$ does not constitute numbers large enough for the asymptotical analysis above to apply, and this gives us a motive to improve the asymptotical formula.

4.3 An improved model

The approximation expressed in Theorem 5 can be improved by more careful asymptotical analysis. Going back to the RHS equation in (29), we see that we can build up its solution as a sequence of progressively refined approximations, by solving simpler equations that become progressively more complicated through the addition of less and less dominant terms. To be more precise, let us get the crudest approximation possible by discarding all terms except the most dominant one(s): when x is very large, the dominant term is $x\ln(x)$, and we consequently demand that

$$x_1 \ln(x_1) = a := \ln(m) - 1 - \frac{1}{2}\ln(2\pi) \Rightarrow x_1 = \exp(W(a)). \qquad (33)$$

Let us now add the 2 next most dominant terms one by one and consider the equations

$$y\ln(y) - y = a \text{ and } \left(z + \frac{1}{2}\right)\ln(z) - z = a. \qquad (34)$$

Assuming we know the exact solution of the former, we express z as a perturbation of y, namely $z = y + \epsilon$; clearly, for a large, $\epsilon \ll y$. Substitution into the latter equation, using the approximation that $\ln\left(1 + \frac{\epsilon}{y}\right) \approx \frac{\epsilon}{y}$, yields

$$(y+\epsilon+0.5)\ln(y+\epsilon)-y-\epsilon=a \Leftrightarrow$$
$$a \approx y\ln(y)+(\epsilon+0.5)\ln(y)+(y+\epsilon+0.5)\frac{\epsilon}{y}-y-\epsilon, \quad (35)$$

whence it follows that

$$(\epsilon+0.5)\ln(y)+(\epsilon+0.5)\frac{\epsilon}{y} \approx 0 \Rightarrow \epsilon \approx -0.5, \quad (36)$$

as the left term dominates over the right one. In other words, the first order correction resulting by considering the z-equation instead of the y-equation in (34) is just a constant; if we do not demand higher precision from our asymptotic, we can completely forget about the higher order terms induced by $\frac{1}{2}\ln(x)$ and (a fortiori) about $\ln(\ln(x))$ in (29), and focus on the asymptotic expansion of y.

Set $y=(1+\epsilon)x_1$: we get

$$(1+\epsilon)x_1\ln(x_1)+(1+\epsilon)x_1\ln(1+\epsilon)-(1+\epsilon)x_1=a \Leftrightarrow$$
$$\epsilon+(1+\epsilon)\frac{\ln(1+\epsilon)}{w}-\frac{1+\epsilon}{w}=0,\ w=\ln(x_1). \quad (37)$$

Setting $v=\frac{1}{w}$, this can be rewritten as

$$v=-\frac{\epsilon}{(1+\epsilon)(\ln(1+\epsilon)-1)}; \quad (38)$$

the RHS is an analytic function of $1+\epsilon$ in a neighborhood of $\epsilon=0$, where also $v=0$. Invoking the inversion theorem for analytic functions [3], we see that $1+\epsilon$ is an analytic function of v in a neighborhood of $v=0$, as long as the derivative of (38) at $\epsilon=0$ is not 0; this can easily checked to be true (the derivative in question equals -1). In other words, $1+\epsilon=f(v)$, and f admits a Taylor expansion around $v=0$. We have overall shown that

$$x=e^w f\left(\frac{1}{w}\right)-\frac{1}{2}+o(1). \quad (39)$$

What is the form of f? Setting $y=x_1+x_2$, where $x_2 \ll x_1$, and plugging back in (34) we get

$$(x_1+x_2)\ln(x_1+x_2)-x_1-x_2=a. \quad (40)$$

But, as above, $\ln(x_1+x_2)=\ln(x_1)+\ln\left(1+\frac{x_2}{x_1}\right)\approx\ln(x_1)+\frac{x_2}{x_1}$ and therefore we obtain

$$(x_1+x_2)\ln(x_1)+(x_1+x_2)\frac{x_2}{x_1}-x_1-x_2=a, \quad (41)$$

which, in view of (33), simplifies into

$$x_2 \ln(x_1) + \frac{x_2^2}{x_1} - x_1 \approx 0 \tag{42}$$

The dominant terms are the first and the third, as the other 2 choices violate the condition that $x_2 \ll x_1$, whence

$$x_2 = \frac{x_1}{\ln(x_1)} \approx \frac{e^w}{w} \Rightarrow$$
$$y \approx e^w \left(1 + \frac{1}{w}\right), \quad w = W\left(\ln(m) - 1 - \frac{1}{2}\ln(2\pi)\right). \tag{43}$$

The process can continue to yield higher order terms of the approximation: keeping higher order terms in the approximation of the logarithm, according to the well known Taylor expansion $\log(1+t) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{t^n}{n}$, we further find

$$x_3 = -\frac{1}{2}\frac{e^w}{w^3}, \ x_4 = \frac{1}{6}\frac{e^w}{w^4}. \tag{44}$$

An improved version of Theorem 5 is therefore

Theorem 6. *Assuming the truth of Conjecture 1, the most probable value of $X^{(m)}$ is, for large m, asymptotically equal to $\lfloor x \rfloor$, where*

$$x = e^w f\left(\frac{1}{w}\right) - \frac{1}{2} + o(1) = e^w \left(1 + \frac{1}{w} - \frac{1}{2}\frac{1}{w^3} + \frac{1}{6}\frac{1}{w^4} + \ldots\right) - \frac{1}{2} + o(1),$$

and where $w = W\left(\ln(m) - 1 - \frac{1}{2}\ln(2\pi)\right)$. f is analytic at the origin and given by the inversion of (38).

The maximal number of fixed points over all $W_1^{\exp}$-permutations of order $q-1$ as a function of the prime $q < 5000$ (also shown in Figure 2), along with the approximation suggested by Theorem 6, are shown in Figure 4. The results for the first few primes are omitted, as the approximation is not well defined there. For 265 primes (39.6% of the total) the approximation yields an exact result, while for 637 primes (95.2% of the total) the approximation differs from the true value by at most 1.

4.4 A comparison of the various models

So far we have obtained three different approximations to the maximal number of fixed points of a $W_1^{\exp}$-permutation of a given order: the logarithmic approximation (17), and the formulas of Theorems 5 and 6. How

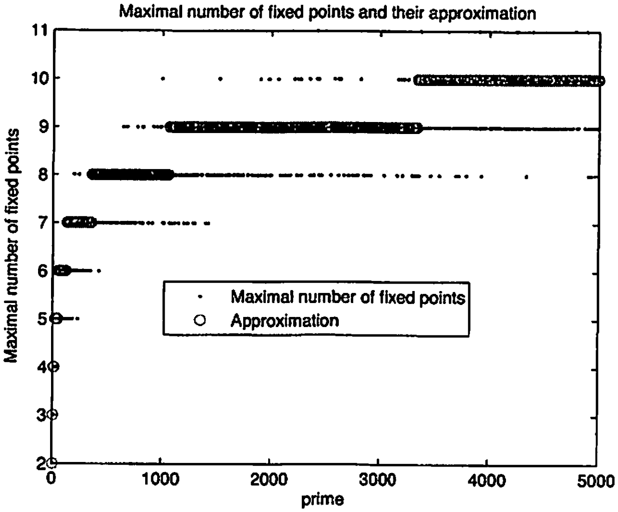

Figure 4: Plot of the maximum over all g and c of the number of fixed points of a $W_1^{\exp}(q, g, c)$-permutation for $q < 5000$, along with the approximation suggested by Theorem 6.

do these formulas compare to each other? A plot of their values over all primes $q < 1,000,000$ is shown in Figure 5. To begin with, we expect that, for large m, Theorems 5 and 6 will give the "same" values (asymptotically differing by the constant 0.5): this does not happen in the given range of q, so even higher values are needed to observe this. More precisely, note that both formulas are functions of $w \approx W(\ln(m)) \approx \ln(\ln(m))$: when q is close to 10^6, w of Theorem 6 is only close to 2.4 which is a small value, hence the higher order corrections in Theorem 6 make a difference compared to the simpler dominant-term only asymptotic approximation of Theorem 5. For example, in order to bring the two formulas within 1% of each other, we would need $w \approx 100$, whence $m \approx e^{e^{100}}$, which is an astronomically large number!

On a different note, Theorem 6 (hence eventually Theorem 5 as well) appears to approximate (17) very well; is this to be expected? Combining Theorem 5 with (6) we obtain:

$$e^{W(\ln(m))} \sim \frac{\ln(m)}{\ln(\ln(m))} \approx \frac{\ln(q-1) + \ln(\phi(q-1))}{\ln(\ln(m))}. \tag{45}$$

But $\ln(\ln(m))$ varies very slowly and is practically constant when m (or q) is confined in a narrow range, while $\ln(\phi(q-1))$ is dominated by $\ln(q-1) \approx$

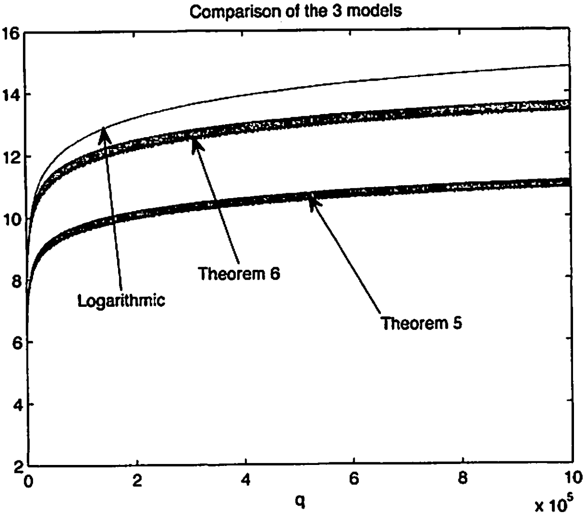

Figure 5: Comparison of the three models for the maximum over all g and c of the number of fixed points of a $W_1^{\exp}(q,g,c)$-permutation for $q < 10^6$.

$\ln(q)$: it follows then that, for q confined in a narrow range of values, $e^{W(\ln(m))} \approx C\ln(q)$ for some $C > 0$, hence Theorem 6 and (17) are indeed compatible. Eventually, however, even under the extremely generous approximation $m \approx q^2$, it can be seen that $\ln(q)$ grows faster than $e^{W(\ln(m))}$, though only slightly so.

5 Conclusion

Though the exact distribution of the number of fixed points of a $W_1^{\exp}$-permutation has still not been found, statistics establishes that, for large orders, a) it behaves similarly to the corresponding distribution for a randomly chosen permutation, and b) it tends to be independent of the order. Exploiting this observation, we approximated the most probable maximal number of fixed points in a W_1^{cxp}-permutation of a given order through asymptotical analysis, by assuming the distribution of this number to be the same as for a randomly chosen permutation. We proposed two models, the second being a more refined version of the first, based on Lambert's W-function.

Comparing the new (stochastic) model to a previously suggested empirically fitted model, we found that the empirical model, though oversimplifying, is compatible with the new model. We also concluded that the more complicated refined version of the new model is meaningful, as the asymptotic approximation proposed becomes valid for extremely large primes, much larger than the ones studied here.

To get back to our original motivating point, do the diagonals of $W_1^{\exp}$-Costas arrays yield dense Golomb rulers? Our results show that they do not, as the number of dots in a diagonal is at best the logarithm of the order (further divided by a slowly varying function), whereas optimal Golomb rulers have asymptotically as many dots as the square root of their length, and the difference between the logarithm and the square root is considerable.

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/frequency of occurrence and control by channel selection." Bell System Technical Journal, Volume 31, pp. 63–73, 1953.

[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, pp. 108–109, 1974.

[3] G.F. Carrier, M. Krook, and C.E. Pearson. "Functions of a Complex Variable: Theory and Technique." Hod Books, 1983.

[4] Ch. Charalambides. "Enumerative combinatorics." Chapman & Hall/CRC (2002).

[5] 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.

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

[7] 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.

[8] A. Dimitromanolakis. "Analysis of the Golomb Ruler and the Sidon set problems, and determination of large, near-optimal Golomb rulers." Diploma thesis, Department of Electronic and Computer Engineering, Technical University of Crete, 2002 (available at `http://www.cs.toronto.edu/ apostol/golomb/`).

[9] H. Dörrie. "100 Great Problems of Elementary Mathematics." Dover (1965).

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

[11] K. Drakakis. "Three challenges in Costas arrays." Ars Combinatoria, Volume 89, pp. 167–182, October 2008.

[12] K. Drakakis, R. Gow, L. O'Carroll. "On the symmetry of Welch- and Golomb-constructed Costas arrays." Discrete Mathematics (to appear).

[13] P. Erdös and P. Turan. "On a problem of Sidon in additive number theory and some related problems." Journal. of the London Mathematical Society, Volume 16, pp. 212–215, 1941 — followed by Addendum (by P. Erdös), ibid. Volume 19, pp. 208, 1944.

[14] W. Feller. "An introduction to probability theory and its applications, Volume 2 (Second edition)." Wiley (1971).

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

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

[17] B. Lindström. "An inequality for b_2-sequences." Journal of Combinatorial Theory, Volume 6, pp. 211–212, 1969.

[18] A.M. Mood, F.A. Graybill, and D.C. Boes. "Introduction to the theory of statistics." McGraw-Hill (1974).

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

[20] J.P. Robinson and A.J. Bernstein "A Class of Binary Recurrent Codes with Limited Error Propagation." IEEE Transactions on Information Theory, Volume 13, pp. 106–113, 1967.

[21] R. Stanley. "Enumerative combinatorics, Volume 1." Cambridge University Press (1997).