Three challenges in Costas arrays

Konstantinos Drakakis*
UCD CASL†
Ireland

May 31, 2008

Abstract

We present 3 open challenges in the field of Costas arrays. They are: a) the determination of the number of dots on the main diagonal of a Welch array, and especially the maximal such number for a Welch array of a given order; b) the conjecture that the fraction of Welch arrays without dots on the main diagonal behaves asymptotically as the fraction of permutations without fixed points and hence approaches $1/e$, and c) the determination of the parity populations of Golomb arrays generated in fields of characteristic 2.

1 Introduction

Costas arrays appeared for the first time in 1965 in the context of SONAR detection [5, 6], when J. P. Costas, disappointed by the poor performance of SONAR, used them to describe a novel frequency hopping pattern for SONAR with optimal auto-correlation properties. At that stage their study was entirely empirical and application-oriented. In 1984, however, after the publication by S. Golomb [11] of the 2 main construction methods for Costas arrays (the Welch and the Golomb algorithm) based on finite fields, still the only ones available today, they officially acquired their present name and they became an object of mathematical interest and study.

Many of the results in the field have been triggered by the exploration of Costas arrays properties through computers (see, for example, [2, 4, 16]).

*The author is also affiliated with the School of Mathematics, University College Dublin, Ireland, as well as with the Claude Shannon Institute (www.shannoninstitute.ie), Ireland.
Address: UCD CASL, University College Dublin, Belfield, Dublin 4, Ireland
Email: Konstantinos.Drakakis@ucd.ie
†http://casl.ucd.ie

ARS COMBINATORIA 89(2008), pp. 167-182

The evidence gathered led to the formulation of conjectures [12, 14], some of which subsequently were, at least partially, proved.

In this work we collect our findings in 3 numerical experiments performed on Costas arrays, whose results are inexplicable at present, and we present them to the broader scientific community, hoping to accelerate progress towards their solution.

- *The determination of the number of dots on the main diagonal of a Welch array, and especially the maximal such number for a Welch array of a given order:* diagonals of Costas arrays form Golomb rulers [1], that have many applications in synchronization, frequency allocation to radio stations, phased array antenna design etc.; they are also related to PPM sequences [10]. Of particular interest is the main diagonal of a Costas array, as it is potentially the longest Golomb ruler within the array; additionally, of particular interest are dense Golomb rulers, so we would like to search for Costas arrays whose main diagonal contains as many dots as possible. A particular subfamily of symmetric Golomb arrays is known to have asymptotically optimally dense main diagonals [8], but what about Welch arrays?

- *The conjecture that the fraction of Welch arrays without dots on the main diagonal behaves asymptotically as the fraction of derangements, namely permutations without fixed points, and hence approaches* $1/e$*:* this observation links Welch arrays to the infamous "problem of the misaddressed letters" in combinatorics.

- *The determination of the parity populations of Golomb arrays generated in fields of characteristic 2:* this is the only as yet unexplained case in parity populations of algebraically constructed Costas arrays, which otherwise are known to involve quite deep mathematical results. For example, parity populations of some Welch arrays are expressible in terms of the Class Number [3, 9].

2 Basics

In this section we give precise definitions for the terms used in the paper.

2.1 Definition of the Costas property

Simply put, a Costas array 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.

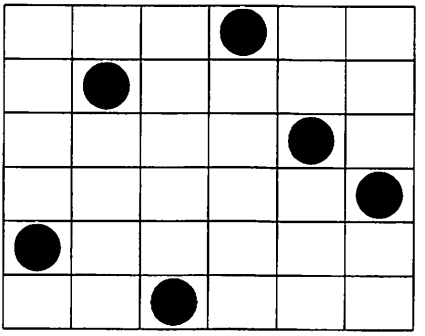

Figure 1: The Costas array of order 6 corresponding to the permutation 526134

Definition 1. Let $f : [n] \to [n]$, where $[n] = \{1, \ldots, n\}$, $n \in \mathbb{N}$, 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):

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

From now on, the terms "array" and "permutation" will be used interchangeably. An example of a Costas array of order 6 and its corresponding permutation is shown in Figure 1.

Remark 1. The horizontal flip, the vertical flip, and the transposition of a Costas array result to a Costas array as well: hence, out of a Costas array 8 can be created, or 4 if the particular Costas array is symmetric.

The analog of a Costas array in one dimension is a Golomb ruler, which has already appeared above in connection with the first challenge:

Definition 2. Let $A = \{a_i\}$, $i \in [m]$ be a sequence of m distinct integers in $[n]$, $n, m \in \mathbb{N}$, $m < n$; A is set to be a *Golomb ruler* iff all differences $\{a_i - a_j : 1 \leq j < i \leq m\}$ are distinct; equivalently, if A describes the numbers in $[n]$ where $f : [n] \to \{0, 1\}$ is equal to 1, f is also called a Golomb ruler.

2.2 Construction algorithms

There are 2 known algorithms for the construction of Costas arrays. We state them below omitting the proofs (which can be found in [7, 11] in full detail):

Algorithm 1 (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 $f(i) = g^{i-1+c} \bmod p,\ i \in [p-1]$.

Remark 2. Given a W_1 permutation, it is well known that its horizontal and vertical flips also correspond to W_1 permutations; its transpose, however, does not: it is what we define as a *logarithmic Welch permutation*. The distinction is well defined as, for $p > 5$, there are no symmetric W_2 arrays. We will no further consider logarithmic Welch permutations in this work, so "Welch" will henceforth be synonymous to "exponential Welch".

Algorithm 2 (Golomb construction $G_2(p, m, a, b)$). Let $q = p^m$, where p prime and $m \in \mathbb{N}^*$, and let a, b be primitive roots of the finite field $\mathbb{F}(q)$; the Golomb permutation corresponding to a and b is defined through the equation $a^i + b^{f(i)} = 1,\ i \in [q-2]$.

Remark 3. The horizontal and vertical flips of a G_2 permutation are themselves G_2 permutations, just like in the Welch case; this time, however, the same holds true for transpositions as well.

Remark 4. The indices in W_1 and G_2 have the significance that the algorithms produce permutations of orders 1 and 2 smaller than the size of the finite field they get applied in, respectively. It is well known that both algorithms can be extended to yield a wide range of sub-algorithms [7, 12]; in this paper, however, we will focus exclusively on the 2 aforementioned main algorithms.

2.3 Parity populations

Definition 3. Let $f : [n] \to [n]$, $n \in \mathbb{N}^*$, be a function; set:

- $ee(f) = |\{i \in [n] : i \bmod 2 = 0,\ f(i) \bmod 2 = 0\}|$ to be the *even-even population*;
- $oo(f) = |\{i \in [n] : i \bmod 2 = 1,\ f(i) \bmod 2 = 1\}|$ to be the *odd-odd population*;
- $eo(f) = |\{i \in [n] : i \bmod 2 = 1,\ f(i) \bmod 2 = 0\}|$ to be the *even-odd population*;

- $oe(f) = |\{i \in [n] : i \bmod 2 = 0,\ f(i) \bmod 2 = 1\}|$ to be the *odd-even population*;

If f is a permutation, the parity populations are closely connected:

Theorem 1. Let $f : [n] \to [n]$, $n \in \mathbb{N}^*$, be a permutation; then

- $ee(f) + oo(f) + eo(f) + oe(f) = n$;
- $oe(f) = eo(f)$;
- $oo(f) - ee(f) = n \bmod 2$.

Proof. This is actually a very simple, almost obvious result (also appearing in [9]). Clearly, $ee + eo = ee + oe$, as both sums equal the number of even integers in $[n]$; hence, $eo = oe$. Further, $oo + oe$ is the number of odd integers in $[n]$, whence:

$$oo + oe - (ee + eo) = oo - ee = \begin{cases} 1 \text{ if } n \bmod 2 \equiv 1 \\ 0 \text{ if } n \bmod 2 \equiv 0 = n \bmod 2 \end{cases}$$

□

There is then only one degree of freedom: if one of the populations is given, all 4 can be determined.

3 First challenge: the number of dots on the main diagonal of a Welch array

Golomb rulers (see Definition 2) have many important applications (in synchronization, frequency allocation to radio stations, phased array antenna design etc. [1]), and are also related to PPM sequences [10]. Although any diagonal of a Costas array is a Golomb ruler by definition, the main diagonal is potentially the longest one within the array, and a further desirable property is that it be "dense", namely have as many dots as possible. Do W_1 arrays yield dense Golomb rulers?

In accordance with Algorithm 1, given a prime p, we are interested in the number of solutions of

$$i \equiv g^{i-1+c} \bmod p \tag{1}$$

with respect to i, where g is a primitive root of the field $\mathbb{F}(p)$ and $c \in [p-1]-1$ is a constant.

Equation (1) strikes one immediately as "unalgebraic": the i on the RHS is simply an index, and in particular an integer in $[p-1]-1$, based on

Fermat's Little Theorem; the i on the LHS, however, is an element of $\mathbb{F}(p)$, and elements of $\mathbb{F}(p)$ just happen to be representable by integers because $\mathbb{F}(p)$ is a field of prime size and not an extension field (whose elements are routinely represented as polynomials). In other words, algebra traditionally considers the 2 instances of i in (1) as different, non-comparable objects, and these 2 object types happen to coincide in finite fields of prime size; the solution of this equation then needs to exploit properties of these fields not present in extension fields, where this equation is impossible to formulate in the first place, and this probably means that we need to consider $\mathbb{F}(p)$ as something more complex than a field.

The bottom line is that we are left with a transcendental equation over a finite field. Such equations have almost not been studied at all, as opposed to polynomial equations, on which the literature is abundant. The only instance of a relevant problem studied in the literature (that we have been able to trace) has been one proposed by Demetrios Brizolis: is it true that $\forall i \in [p-1],\ \exists g \in [p-1] :\ i \equiv g^i \bmod p$? This was answered in the affirmative by W. P. Zhang [17] for sufficiently large primes, and later C. Pomerance and M. Campbell "*made the value of "sufficiently large" small enough that they were able to use a direct search to affirmatively answer Brizolis' original question*" ([13] and references therein). Observe, though, that this is quite a different problem than the one we are interested in.

Let $S(p,g,c) = \left|\left\{i \in [p-1] : i \equiv g^{i^{-1}+c}\right\}\right|$, namely the number of solutions of (1) for a given constant c and a primitive root $g \in \mathbb{F}(p)$, p prime. Table 1 shows $\max\limits_{(g,c)} S(p,g,c)$ for all $p < 5000$: the data do not seem to follow a recognizable pattern, but they roughly seem to behave "logarithmically". Indeed, $1 + [\ln(p)]$, where $[\cdot]$ is the rounding function, seems to fit the data very well: 402 out of 669 entries (60.1%) are captured exactly, while 652 entries (97.5%) are captured within an error margin of ± 1. Figure 2 plots the data of Table 1 and their logarithmic approximation. Table 2 collects the values of p where a maximal number of solutions $n \in [11]$ occurs in Table 1 for the first time, as well as the (probable) values of p where a maximal number of solutions $n \in [7]$ occurs in Table 1 for the last time.

Table 1: The maximum number of solutions of the equation $i \equiv g^{i^{-1}+c} \bmod p$ over all possible values of c and primitive roots $g \in \mathbb{F}(p)$, $p < 5000$. First occurrences of values are **bold**, while the last ones (up to 7) are ***bold and italic***. The first and (probable) last p for which a certain maximal number of solutions appears is tabulated in Table 2.

p	#	p	#	p	#	p	#	p	#	p	#
2	***1***	617	8	1427	9	2269	10	3169	9	4073	10

continued on next page

Table 1: *continued*

p	#	p	#	p	#	p	#	p	#	p	#
3	**2**	619	8	1429	8	2273	10	3181	9	4079	9
5	***2***	631	7	1433	8	2281	8	3187	9	4091	10
7	**3**	641	7	1439	8	2287	9	3191	10	4093	10
11	4	643	8	1447	9	2293	9	3203	10	4099	9
13	4	**647**	**9**	1451	9	2297	9	3209	8	4111	10
17	3	653	7	1453	9	2309	9	3217	10	4127	10
19	5	659	7	1459	8	2311	9	3221	10	4129	10
23	5	661	7	1471	8	2333	9	3229	9	4133	9
29	4	673	7	1481	8	2339	9	3251	9	4139	9
31	4	677	9	1483	8	2341	9	3253	9	4153	9
37	***4***	683	7	1487	8	2347	9	3257	10	4157	9
41	5	691	7	1489	8	2351	10	3259	9	4159	10
43	4	701	7	1493	9	2357	8	3271	9	4177	9
47	5	709	8	1499	8	2371	8	3299	8	4201	9
53	5	719	7	1511	8	2377	9	3301	9	4211	9
59	5	727	8	1523	10	2381	9	3307	9	4217	9
61	5	733	8	1531	8	2383	9	3313	9	4219	9
67	5	739	8	1543	8	2389	8	3319	8	4229	10
71	5	743	7	1549	8	2393	8	3323	8	4231	9
73	5	751	7	1553	8	2399	9	3329	10	4241	9
79	5	757	8	1559	9	2411	9	3331	8	4243	11
83	**6**	761	7	1567	9	2417	10	3343	8	4253	11
89	5	769	8	1571	9	**2423**	**11**	3347	9	4259	11
97	6	773	9	1579	8	2437	10	3359	9	4261	9
101	6	787	8	1583	9	2441	8	3361	8	4271	9
103	6	797	7	1597	8	2447	9	3371	9	4273	9
107	6	809	8	1601	8	2459	8	3373	11	4283	10
109	6	811	8	1607	8	2467	8	3389	9	4289	9
113	5	821	9	1609	9	2473	9	3391	10	4297	9
127	5	823	7	1613	8	2477	9	3407	10	4327	9
131	6	827	7	1619	9	2503	9	3413	9	4337	9
137	6	829	9	1621	9	2521	9	3433	9	4339	8
139	6	839	8	1627	8	2531	9	3449	9	4349	9
149	6	853	8	1637	9	2539	9	3457	10	4357	9
151	5	857	8	1657	8	2543	9	3461	9	4363	9
157	5	859	8	1663	8	2549	9	3463	9	4373	10
163	6	863	8	1667	8	2551	8	3467	9	4391	11
167	**7**	877	7	1669	9	2557	9	3469	8	4397	9

continued on next page

Table 1: *continued*

p	#	p	#	p	#	p	#	p	#	p	#
173	6	881	8	1693	8	2579	10	3491	10	4409	9
179	7	883	8	1697	8	2591	9	3499	9	4421	9
181	5	887	8	1699	8	2593	9	3511	9	4423	9
191	6	907	7	1709	8	2609	9	3517	10	4441	10
193	6	911	7	1721	8	2617	10	3527	9	4447	9
197	**8**	919	9	1723	9	2621	8	3529	9	4451	10
199	6	929	8	1733	8	2633	10	3533	9	4457	9
211	6	937	8	1741	8	2647	9	3539	9	4463	9
223	7	941	8	1747	9	2657	9	3541	9	4481	10
227	6	947	8	1753	9	2659	9	3547	8	4483	9
229	***5***	953	9	1759	9	2663	9	3557	9	4493	9
233	6	967	8	1777	9	2671	8	3559	9	4507	9
239	8	971	8	1783	8	2677	9	3571	9	4513	10
241	7	977	8	1787	9	2683	9	3581	9	4517	9
251	6	983	9	1789	8	2687	9	3583	9	4519	9
257	7	991	9	1801	9	2689	9	3593	9	4523	9
263	6	**997**	**10**	1811	9	2693	9	3607	10	4547	9
269	7	1009	7	1823	8	2699	9	3613	9	4549	9
271	6	1013	8	1831	8	2707	8	3617	9	4561	9
277	6	1019	8	1847	8	2711	9	3623	11	4567	10
281	7	1021	7	1861	9	2713	9	3631	9	4583	9
283	6	1031	8	1867	9	2719	8	3637	9	4591	9
293	7	1033	8	1871	8	2729	9	3643	10	4597	9
307	7	1039	8	1873	9	2731	9	3659	10	4603	9
311	6	1049	8	1877	9	2741	9	3671	9	4621	9
313	7	1051	8	1879	8	2749	9	3673	9	4637	9
317	6	1061	8	1889	8	2753	8	3677	9	4639	9
331	6	1063	8	1901	10	2767	8	3691	9	4643	10
337	6	1069	7	1907	8	2777	9	3697	9	4649	10
347	6	1087	7	1913	8	2789	8	3701	8	4651	9
349	7	1091	8	1931	9	2791	9	3709	9	4657	9
353	8	1093	7	1933	8	2797	8	3719	9	4663	9
359	7	1097	8	1949	9	2801	9	3727	8	4673	9
367	8	1103	8	1951	8	2803	9	3733	9	4679	9
373	7	1109	8	1973	10	2819	10	3739	9	4691	9
379	7	1117	7	1979	10	2833	9	3761	9	4703	9
383	7	1123	8	1987	8	2837	9	3767	9	4721	10
389	7	1129	8	1993	9	2843	9	3769	10	4723	10

continued on next page

Table 1: *continued*

p	#	p	#	p	#	p	#	p	#	p	#
397	7	1151	7	1997	9	2851	8	3779	9	4729	9
401	7	1153	8	1999	8	2857	8	3793	8	4733	9
409	7	1163	8	2003	8	2861	8	3797	9	4751	10
419	7	1171	9	2011	9	2879	8	3803	9	4759	9
421	***6***	1181	8	2017	9	2887	9	3821	10	4783	10
431	7	1187	9	2027	9	2897	9	3823	9	4787	11
433	7	1193	8	2029	9	2903	8	3833	10	4789	10
439	8	1201	7	2039	9	2909	9	3847	10	4793	10
443	7	1213	8	2053	9	2917	8	3851	10	4799	9
449	7	1217	8	2063	10	2927	9	3853	9	4801	9
457	7	1223	8	2069	9	2939	9	3863	10	4813	9
461	8	1229	8	2081	9	2953	9	3877	9	4817	10
463	7	1231	7	2083	9	2957	9	3881	9	4831	10
467	7	1237	7	2087	9	2963	9	3889	10	4861	10
479	8	1249	8	2089	8	2969	9	3907	11	4871	9
487	8	1259	8	2099	9	2971	9	3911	9	4877	10
491	7	1277	8	2111	8	2999	9	3917	9	4889	11
499	7	1279	8	2113	9	3001	9	3919	9	4903	9
503	7	1283	8	2129	9	3011	9	3923	10	4909	8
509	7	1289	9	2131	9	3019	9	3929	9	4919	10
521	7	1291	7	2137	8	3023	11	3931	8	4931	8
523	8	1297	9	2141	9	3037	8	3943	9	4933	9
541	7	1301	8	2143	8	3041	9	3947	10	4937	9
547	7	1303	7	2153	9	3049	9	3967	9	4943	9
557	7	1307	8	2161	8	3061	9	3989	10	4951	9
563	8	1319	9	2179	8	3067	9	4001	10	4957	9
569	8	1321	8	2203	9	3079	9	4003	9	4967	9
571	7	1327	8	2207	9	3083	9	4007	10	4969	9
577	7	1361	8	2213	10	3089	9	4013	10	4973	10
587	8	1367	8	2221	9	3109	9	4019	9	4987	9
593	7	1373	9	2237	9	3119	9	4021	9	4993	9
599	7	1381	9	2239	8	3121	9	4027	9	4999	9
601	7	1399	7	2243	10	3137	9	4049	9		
607	8	1409	8	2251	8	3163	8	4051	9		
613	8	***1423***	***7***	2267	9	3167	10	4057	9		

To summarize:

Challenge 1. For p prime, g a primitive root of $\mathbb{F}(p)$ and $c \in [p-1]-1$,

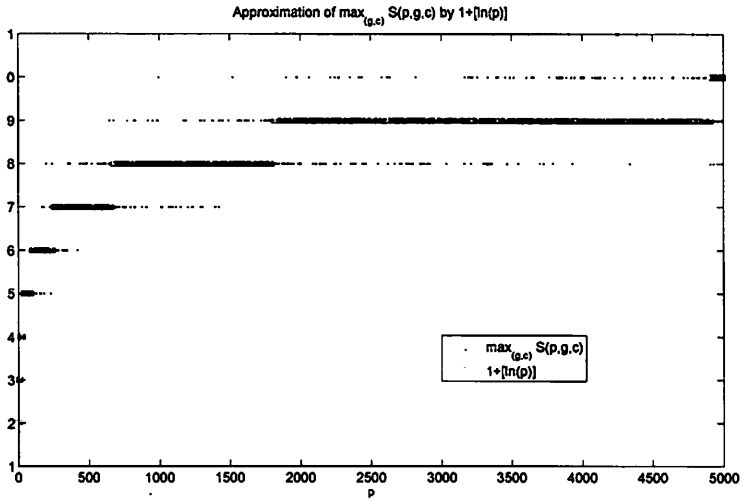

Figure 2: Plot of $\max_{(g,c)} S(p,g,c)$ for all $p < 5000$, as tabulated in Table 1, along with the approximation by $1 + [\ln(p)]$. A graph of these results for $p < 1000$ was presented by the author in a previous paper [8].

n	1	2	3	4	5	6	7	8	9	10	11
First p	2	3	7	11	19	83	167	197	647	997	2423
Last p	2	5	17	37	229	421	1423				

Table 2: The first p for which the maximum number of solutions $n \in [11]$ appears in Table 1, as well as the (probable) last p for which the maximum number of solutions $n \in [7]$ appears in Table 1.

determine the number of solutions of the equation

$$i \equiv g^{i-1+c} \bmod p.$$

In particular, determine the maximal such number of solutions for a given p over all possible g and c, and show that it behaves asymptotically as $\ln(p)$.

It is known that the optimally dense Golomb ruler of length n contains approximately $\sqrt{n}$ points [8]; the fact that, in the case of W_1 arrays, the number of points depends logarithmically on the length (a much smaller quantity than the square root of the length), shows that they do not lead to dense Golomb rulers after all. Thus, a reformulation of this section's challenge would be to show that Welch arrays lead to sparse Golomb rulers.

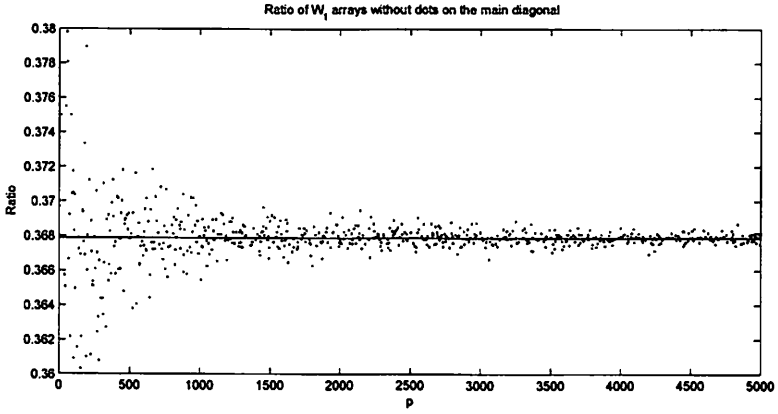

Figure 3: Plot of the ratio of W_1 arrays with no dots on the main diagonal over the total number of W_1 arrays generated in $\mathbb{F}(p)$ as a function of p; the red horizontal line marks $1/e$.

4 Second challenge: the asymptotic behavior of the number of Welch derangements

It is a well known result in combinatorics that the ratio of derangements, i.e. permutations without fixed points, of order n over the total number of permutations ($n!$) approaches $e^{-1} = 0.3678794\ldots$ as $n \to \infty$ (this result is often referred to as *the problem of the misaddressed letters*). What can be said about the ratio of the number of W_1 permutations generated in $\mathbb{F}(p)$ with no fixed points over the totality of $(p-1)\phi(p-1)$ W_1 arrays? It is plotted in Figure 3 and seems to approach e^{-1} as well, although the data shows still some fluctuation in the given range of p.

This conjecture can also be cast in the language of probability. Let N and W be the events that a permutation has no fixed points and that a permutation is W_1, respectively: the conjecture then is equivalent to the statement that $\mathbb{P}(N|W) = \mathbb{P}(N)$, namely that the probability of N given W is equal to the probability of N, at least asymptotically, so the 2 events are independent. This result is an indication of a uniformity of distribution of Welch arrays among the set of all permutations.

To summarize:

Challenge 2. Prove that the fraction of W_1 derangements over the total number of W_1 permutations generated in $\mathbb{F}(p)$, p prime, is asymptotically equal to the fraction of derangements of order $p-1$, as $p \to \infty$, and tends, therefore, to $1/e$.

5 Third challenge: the parity populations of Golomb arrays generated in fields of characteristic 2

The parity populations for both W_1 and G_2 arrays *generated in fields of odd characteristic* have already been completely described [9]: indeed, the 2 theorems below cover all possible Welch and Golomb constructions, except for Golomb constructions in fields of even characteristic, namely of characteristic 2.

Theorem 2. Let a permutation be generated by $G_2(p, m, a, b)$, $p > 2$, $q = p^m$. Then:

- If $q \equiv 1 \bmod 4 \Rightarrow ee = \dfrac{q-5}{4}$, $eo = oe = oo = \dfrac{q-1}{4}$;
- If $q \equiv 3 \bmod 4 \Rightarrow oo = \dfrac{q+1}{4}$, $eo = oe = ee = \dfrac{q-3}{4}$.

Theorem 3. Let permutation be generated by $W_1(p, g, 0)$. Then:

- If $p \equiv 1 \bmod 4 \Rightarrow ee = oo = eo = oe$;
- If $p \equiv 3 \bmod 8$, then $eo - ee = -3h(-p)$;
- If $p \equiv 7 \bmod 8$, then $eo - ee = h(-p)$,

where $h(-p)$ is the *Class Number [3] for discriminant* $-p$: for $p > 3$, $h(-p) = -\dfrac{1}{p}\sum_{i=1}^{p-1}\left(\dfrac{i}{p}\right) i$, where $\left(\dfrac{\cdot}{\cdot}\right)$ denotes the Legendre symbol [15].

Although the proofs (omitted here, but see [9] for details) are not necessarily easy (in particular the parity populations of Welch arrays involve the quite advanced concept of the Class Number [3]), the statements certainly are: the parity populations of G_2 arrays generated in $\mathbb{F}(p^m)$, $p > 2$, are independent of the primitive roots a and b used. The same holds essentially true for W_1 arrays, except that changing the value of c by 1 causes ee and eo to swap values; as W_1 arrays are of even order, horizontal or vertical flips have the same effect, changing the parity of the corresponding coordinate of the dots.

This effective independence of the parity populations from the specific primitive roots used for the generation of the array holds no longer true for G_2 arrays generated in fields of characteristic 2: here, the parity populations take many different values, depending on the primitive roots used for the generation of the array, which appear to follow no readily recognizable

pattern. As these arrays have even order, however, the same phenomenon that we observed in W_1 arrays applies here: for each array with parity populations ee and eo, there exists another (its horizontal and vertical flip) with these values swapped; hence, there are as many arrays with $ee = x$ and $eo = y$ as with $ee = y$ and $eo = x$. The different parity populations observed in G_2 arrays generated in the fields of size 2^m, $m = 3, \ldots, 11$ are shown in detail in Table 3; due to the symmetry we just mentioned, only (the top) half of the array is shown.

To summarize:

Challenge 3. Let $f = G_2(2, m, a, b)$ be a G_2 permutation in a field of characteristic 2; determine its parity populations $ee(f)$, $eo(f)$, $oe(f)$, $oo(f)$. Determine also the number of G_2 permutations constructed in $\mathbb{F}(2^m)$ with a given set of parity populations.

6 Summary and future work

In this work we have presented, in the form of challenges, the results of 3 of our numerical experiments on Costas arrays. We chose the 3 most intriguing experiments we have encountered so far, and presented all of the evidence we have gathered. In brief, these 3 challenges are:

1. The determination of the number of fixed points of a W_1 permutation, and in particular the maximal such number among all W_1 arrays generated in a particular field.

2. The proof of the conjecture that the fraction of W_1 arrays without fixed points is asymptotically equal to the fraction of derangements, and in particular that it tends to $1/e$.

3. The determination of the parity populations of G_2 arrays generated in fields of characteristic 2. We should note further here that Table 3 shows only the simplest instance of a general phenomenon: consider $k \in \mathbb{N}^*$ and consider the generalized parity populations modulo k. Whenever k is a prime, the G_2 arrays generated in fields of characteristic k exhibit similar behavior. Clearly, Table 3 corresponds to the first case $k = 2$. As we have not experimented extensively with $k > 2$, however, we avoided presenting any results at this time.

It is our firm belief that these results are instances of as yet unexplored number theoretic or algebraic properties of (some families of) finite fields, so that further study of these matters will greatly benefit both pure mathematics and applications. We can only hope that we will successfully arouse the interest of a reader, perhaps better versed in the relevant techniques than ourselves, who will unravel the mysteries of these experiments.

$m = 3$ (1)		
ee	*eo*	#
1	2	6

$m = 4$ (2)		
ee	*eo*	#
2	5	4
3	4	4

$m = 5$ (3)		
ee	*eo*	#
5	10	10
6	9	40
7	8	40

$m = 6$ (4)		
ee	*eo*	#
12	19	12
13	18	22
14	17	54
15	16	20

$m = 7$ (8)		
ee	*eo*	#
24	39	4
25	38	20
26	37	44
27	36	104
28	35	140
29	34	206
30	33	336
31	32	280

$m = 8$ (11)		
ee	*eo*	#
53	74	10
54	73	4
55	72	12
56	71	36
57	70	62
58	69	106
59	68	156
60	67	116
61	66	166
62	65	178
63	64	178

$m = 9$ (18)		
ee	*eo*	#
110	145	8
111	144	8
112	143	32
113	142	26
114	141	90
115	140	112
116	139	156
117	138	350
118	137	426
119	136	496
120	135	668
121	134	756
122	133	872
123	132	1020
124	131	1232
125	130	1296
126	129	1436
127	128	1384

$m = 10$ (27)		
ee	*eo*	#
229	282	2
230	281	4
231	280	4
232	279	16
233	278	38
234	277	34
235	276	60
236	275	62
237	274	142
238	273	164
239	272	248
240	271	354
241	270	326
242	269	532
243	268	560
244	267	792
245	266	832
246	265	874
247	264	972
248	263	1130
249	262	1276
250	261	1282
251	260	1524
252	259	1620
253	258	1654
254	257	1718
255	256	1780

$m = 11$ (39)					
ee	*eo*	#	*ee*	*eo*	#
472	551	4	493	530	3466
473	550	16	494	529	4062
475	548	4	495	528	4752
476	547	4	496	527	5300
477	546	56	497	526	5774
478	545	72	498	525	6226
479	544	120	499	524	6948
480	543	136	500	523	7232
481	542	224	501	522	7946
482	541	348	502	521	8442
483	540	444	503	520	8932
484	539	488	504	519	9244
485	538	782	505	518	9426
486	537	908	506	517	10180
487	536	1340	507	516	10952
488	535	1400	508	515	10848
489	534	1730	509	514	11790
490	533	2090	510	513	11306
491	532	2732	511	512	11624
492	531	3020			

Table 3: The various different parity populations for G_2 arrays generated in $\mathbb{F}(2^m)$, $m = 3, \ldots, 11$: the third column of each array shows the number of G_2 arrays with the given *ee* and *eo*. The numbers in parentheses next to the value of m denote the number of different parity populations (rows). Note that the bottom half of the arrays, which is the same as the top half but with the values of *ee* and *eo* swapped, is omitted.

Acknowledgements

The author would like to thank Prof. Rod Gow for his coordinated attempts with the author to explain the 2 experiments presented here. He would also like to thank Prof. Paul Curran, Dr. Scott Rickard, and John Healy for the long and useful discussions on these experiments. Finally, he would like to thank the anonymous referee whose detailed comments improved the presentation and the content of the paper.

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] J. Beard, J. Russo, K. Erickson, M. Monteleone, and M. Wright. "Combinatoric Collaboration on Costas Arrays and Radar Applications." IEEE Radar Conference, pp. 260-265, Philadelphia, Pennsylvania, USA, April 2004.

[3] Z. I. Borevich and I. R. Shafarevich. "Number Theory." Academic Press, New York and London, 1966.

[4] C. Brown, M. Cenki, R. Games, J. Rushanan, O. Moreno, and P. Pei. "New enumeration results for Costas arrays." IEEE International Symposium on Information Theory, pp. 405, January 1993.

[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, R. Gow, L. O'Carroll: "On some properties of Costas arrays generated via finite fields." IEEE CISS 2006.

[9] K. Drakakis, R. Gow, and S. Rickard. "Parity properties of Costas arrays defined via finite fields." Advances in Mathematics of Communications, Volume 1, Issue 3, Aug 2007, pp. 323-332.

[10] C. N. Georghiades. "On the synchronizability and detectability of random PPM sequences." IEEE Transactions on Information Theory, Volume 35, No. 1, January 1989, pp. 146-156.

[11] S. Golomb. "Algebraic Constructions For Costas Arrays." Journal Of Combinatorial Theory Series A, Volume 37, Issue. 1, pp. 13-21, 1984.

[12] S. Golomb and H. Taylor. "Constructions and properties of Costas arrays", Proceedings of the IEEE, Vol. 72, pp. 1143-1163, 1984.

[13] J. Holden and P. Moree. "New Conjectures and Results for Small Cycles of the Discrete Logarithm." High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, AMS, 2004, pp. 245-254.

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

[15] D. Shanks. "Solved and Unsolved Problems in Number Theory." 4th Edition, New York: Chelsea, pp. 154-157, 1993.

[16] J. Silverman, V. Vickers, and J. Mooney. "On the Number of Costas arrays as a function of array size." Proceedings of the IEEE, Volume 76, Issue 7, July 1988, pp. 851-853.

[17] W. P. Zhang. "On a problem of Brizolis." Pure and Applied Mathematics, Volume 11 (suppl.), pp. 1-3, 1995.