

Two experimental pearls in Costas arrays

Konstantinos Drakakis, Rod Gow
School of Mathematics and UCD CASL
University College Dublin
Belfield, Dublin 4
Ireland

Email: {Konstantinos.Drakakis, Rod.Gow}@ucd.ie

Abstract—The results of 2 experiments in Costas arrays are presented, for which theoretical explanation is still not available: the number of dots on the main diagonal of exponential Welch arrays, and the parity populations of Golomb arrays generated in fields of characteristic 2.

I. INTRODUCTION

Costas arrays appeared for the first time in 1965 in the context of SONAR detection ([4], and later [5] as a journal publication), when J. P. Costas, disappointed by the poor performance of SONARs, used them to describe a novel frequency hopping pattern for SONARs 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 [9] 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.

Soon it became clear that the mathematical problems related to Costas arrays presented a challenge for our present methodology in Discrete Mathematics (based on Combinatorics, Algebra, and Number Theory), and suggested that novel techniques are desperately needed, perhaps currently lying beyond the frontiers of our knowledge. Indeed, we have so far been unable to settle even the most fundamental question in the field: do Costas arrays exist for all orders?

These insurmountable difficulties the researchers were faced with triggered inevitably an intense activity in computer exploration of Costas arrays (for example [1], [3], [14]), the rationale being that it is easier to prove something on which strong evidence has been gathered, rather than starting completely from scratch. Such evidence led to the formulation of conjectures, some of which subsequently were, at least partially, proved. These successes, however small, helped consolidate the position of the experimental method as an indispensable tool for the study of Costas arrays.

Not all computer experiments have led to conjectures, however, let alone successfully proved conjectures: several experiments, perhaps the most interesting ones, yielded results that still defy any attempt for explanation. In this work we collect our findings in 2 numerical experiments we performed on Costas arrays, whose results appear very interesting, but entirely inexplicable at present, and we present them to the

broader scientific community, hoping to accelerate progress towards their solution. They are:

- The number of dots on the main diagonal of exponential Welch arrays;
- and the parity populations of Golomb arrays generated in fields of characteristic 2.

The reason for choosing these particular 2 experiments is that, having spent lots of time studying them, we can confidently say that a lot more is to be gained than mere deeper understanding of Costas arrays through their successful explanation: in our opinion, such an explanation relies on completely novel, as yet unexplored areas of finite fields, and traditional algebraic and number theoretic methods are totally incapable of making any progress. In other words, these problems, although originating in the relatively unknown field of Costas arrays, reveal new directions in Algebra and Number Theory, and are, consequently, of paramount pure mathematical interest.

II. BASICS

In this section we give precise definitions for all the terms used in the introduction, as well as for everything else needed in the paper.

A. 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.

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):

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

Remark 1. The operations of horizontal flip, vertical flip, and transposition on 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.

B. 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 [6], [9] 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 [6], [10]; in this paper, however, we will focus exclusively on the 2 aforementioned main algorithms.

C. Parity populations

Definition 2. Let $f : [n] \rightarrow [n]$, $n \in \mathbb{N}^*$, be a function; set:

- $ee(f) = |\{i \in [n] : i \bmod 2 = f(i) \bmod 2 = 0\}|$ to be the *even-even population*;
- $oo(f) = |\{i \in [n] : i \bmod 2 = f(i) \bmod 2 = 1\}|$ 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 $f : [n] \rightarrow [n]$, $n \in \mathbb{N}^*$, 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 [8]). 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. ■

III. THE NUMBER OF DOTS ON THE MAIN DIAGONAL OF EXPONENTIAL WELCH ARRAYS

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

$$i \equiv g^{i-1+c} \bmod p \quad (1)$$

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 [15] 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” ([11] and references therein). Observe, though, that this is quite a different problem than the one we are interested in.

Let $S(p, g, c) = |\{i \in [p-1] : i \equiv g^{i-1+c}\}|$, namely the number of solutions of (1) for a given constant c and a primitive root $g \in \mathbb{F}(p)$, p prime. Table I shows $\max_{(g,c)} S(p, g, c)$ for all $p < 5000$: the data do not seem to follow a recognizable pattern, but they roughly seem to behave “logarithmically”. Indeed, $1 + \lceil \ln(p) \rceil$, where $\lceil \cdot \rceil$ 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

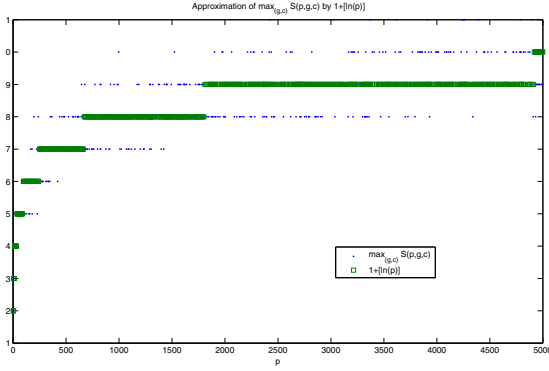


Fig. 1. Plot of $\max_{(g,c)} S(p, g, c)$ for all $p < 5000$, as tabulated in Table I, along with the approximation by $1 + \lfloor \ln(p) \rfloor$. A graph of these results for $p < 1000$ was presented in [7].

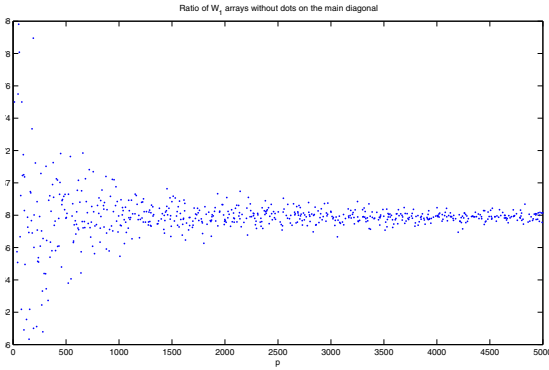


Fig. 2. Plot of the ratio of W_1 arrays with no dots on the main diagonal over the total number of W_1 arrays generated in $\mathbb{F}(p)$ as a function of p .

an error margin of ± 1 . Figure 1 plots the data of Table I and their logarithmic approximation.

Finally, here is an interesting additional side observation we made during our experiments: it is a well known result in Combinatorics (“The problem of the misaddressed letters”) that the ratio of permutations of order n without fixed points over the total $n!$ permutations approaches $e^{-1} = 0.3678794\dots$ as $n \rightarrow \infty$. What can be said about the ratio of the population of W_1 permutations with no fixed points at all generated in $\mathbb{F}(p)$ over the totality of $(p-1)\phi(p-1)$ W_1 arrays? It is plotted in Fig. 2 and seems to approach e^{-1} as well, although the data shows still some fluctuation in the given range of p .

IV. 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 [8]:

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

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

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

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

where $h(-p)$ is the Class Number for discriminant $-p$.

For $p > 3$, $h(-p) = -\frac{1}{p} \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) i$, where $\left(\frac{\cdot}{\cdot}\right)$ denotes the

Legendre symbol [13].

Although the proofs (omitted here, but see [8] for details) are not necessarily easy (in particular the parity populations of Welch arrays involve the quite advanced concept of the Class Number [2]), 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 uniformity holds no longer true for G_2 arrays generated in fields of characteristic 2: here, the parity populations can take many different values, 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 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 , $m = 3, \dots, 11$ are shown in detail in Table II; due to the symmetry we just mentioned, only (the top) half of the array is shown.

Table II shows only the simplest instance of a general phenomenon: consider $k \in \mathbb{N}^*$ and consider the generalized parity populations modulo k . If k happens to be a prime, then the G_2 arrays generated in fields of characteristic k exhibit similar behavior. Clearly, Table II corresponds to the first case $k = 2$. As we have not experimented extensively with $k > 2$, however, we avoid presenting any results at this time.

V. SUMMARY AND FUTURE WORK

In this work we have presented the results of some of our numerical experiments on Costas arrays that we have hitherto been unable to account for, or even formulate relevant conjectures on; in that sense, the entire paper is a plan for future work. We chose the 2 most complex and intriguing experiments we have encountered so far, and presented all of the evidence we have gathered. 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

p	#	p	#	p	#	p	#	p	#	p	#	p	#	p	#	p	#
2	1	337	6	761	7	1231	7	1723	9	2267	9	2767	8	3331	8	3877	9
3	2	347	6	769	8	1237	7	1733	8	2269	10	2777	9	3343	8	3881	9
5	2	349	7	773	9	1249	8	1741	8	2273	10	2789	8	3347	9	3889	10
7	3	353	8	787	8	1259	8	1747	9	2281	8	2791	9	3359	9	3907	11
11	4	359	7	797	7	1277	8	1753	9	2287	9	2797	8	3361	8	3911	9
13	4	367	8	809	8	1279	8	1759	9	2293	9	2801	9	3371	9	3917	9
17	3	373	7	811	8	1283	8	1777	9	2297	9	2803	9	3373	11	3919	9
19	5	379	7	821	9	1289	9	1783	8	2309	9	2819	10	3389	9	3923	10
23	5	383	7	823	7	1291	7	1787	9	2311	9	2833	9	3391	10	3929	9
29	4	389	7	827	7	1297	9	1789	8	2333	9	2837	9	3407	10	3931	8
31	4	397	7	829	9	1301	8	1801	9	2339	9	2843	9	3413	9	3943	9
37	4	401	7	839	8	1303	7	1811	9	2341	9	2851	8	3433	9	3947	10
41	5	409	7	853	8	1307	8	1823	8	2347	9	2857	8	3449	9	3967	9
43	4	419	7	857	8	1319	9	1831	8	2351	10	2861	8	3457	10	3989	10
47	5	421	6	859	8	1321	8	1847	8	2357	8	2879	8	3461	9	4001	10
53	5	431	7	863	8	1327	8	1861	9	2371	8	2887	9	3463	9	4003	9
59	5	433	7	877	7	1361	8	1867	9	2377	9	2897	9	3467	9	4007	10
61	5	439	8	881	8	1367	8	1871	8	2381	9	2903	8	3469	8	4013	10
67	5	443	7	883	8	1373	9	1873	9	2383	9	2909	9	3491	10	4019	9
71	5	449	7	887	8	1381	9	1877	9	2389	8	2917	8	3499	9	4021	9
73	5	457	7	907	7	1399	7	1879	8	2393	8	2927	9	3511	9	4027	9
79	5	461	8	911	7	1409	8	1889	8	2399	9	2939	9	3517	10	4049	9
83	6	463	7	919	9	1423	7	1901	10	2411	9	2953	9	3527	9	4051	9
89	5	467	7	929	8	1427	9	1907	8	2417	10	2957	9	3529	9	4057	9
97	6	479	8	937	8	1429	8	1913	8	2423	11	2963	9	3533	9	4073	10
101	6	487	8	941	8	1433	8	1931	9	2437	10	2969	9	3539	9	4079	9
103	6	491	7	947	8	1439	8	1933	8	2441	8	2971	9	3541	9	4091	10
107	6	499	7	953	9	1447	9	1949	9	2447	9	2999	9	3547	8	4093	10
109	6	503	7	967	8	1451	9	1951	8	2459	8	3001	9	3557	9	4099	9
113	5	509	7	971	8	1453	9	1973	10	2467	8	3011	9	3559	9	4111	10
127	5	521	7	977	8	1459	8	1979	10	2473	9	3019	9	3571	9	4127	10
131	6	523	8	983	9	1471	8	1987	8	2477	9	3023	11	3581	9	4129	10
137	6	541	7	991	9	1481	8	1993	9	2503	9	3037	8	3583	9	4133	9
139	6	547	7	997	10	1483	8	1997	9	2521	9	3041	9	3593	9	4139	9
149	6	557	7	1009	7	1487	8	1999	8	2531	9	3049	9	3607	10	4153	9
151	5	563	8	1013	8	1489	8	2003	8	2539	9	3061	9	3613	9	4157	9
157	5	569	8	1019	8	1493	9	2011	9	2543	9	3067	9	3617	9	4159	10
163	6	571	7	1021	7	1499	8	2017	9	2549	9	3079	9	3623	11	4177	9
167	7	577	7	1031	8	1511	8	2027	9	2551	8	3083	9	3631	9	4201	9
173	6	587	8	1033	8	1523	10	2029	9	2557	9	3089	9	3637	9	4211	9
179	7	593	7	1039	8	1531	8	2039	9	2579	10	3109	9	3643	10	4217	9
181	5	599	7	1049	8	1543	8	2053	9	2591	9	3119	9	3659	10	4219	9
191	6	601	7	1051	8	1549	8	2063	10	2593	9	3121	9	3671	9	4229	10
193	6	607	8	1061	8	1553	8	2069	9	2609	9	3137	9	3673	9	4231	9
197	8	613	8	1063	8	1559	9	2081	9	2617	10	3163	8	3677	9	4241	9
199	6	617	8	1069	7	1567	9	2083	9	2621	8	3167	10	3691	9	4243	11
211	6	619	8	1087	7	1571	9	2087	9	2633	10	3169	9	3697	9	4253	11
223	7	631	7	1091	8	1579	8	2089	8	2647	9	3181	9	3701	8	4259	11
227	6	641	7	1093	7	1583	9	2099	9	2657	9	3187	9	3709	9	4261	9
229	5	643	8	1097	8	1597	8	2111	8	2659	9	3191	10	3719	9	4271	9
233	6	647	9	1103	8	1601	8	2113	9	2663	9	3203	10	3727	8	4273	9
239	8	653	7	1109	8	1607	8	2129	9	2671	8	3209	8	3733	9	4283	10
241	7	659	7	1117	7	1609	9	2131	9	2677	9	3217	10	3739	9	4289	9
251	6	661	7	1123	8	1613	8	2137	8	2683	9	3221	10	3761	9	4297	9
257	7	673	7	1129	8	1619	9	2141	9	2687	9	3229	9	3767	9	4327	9
263	6	677	9	1151	7	1621	9	2143	8	2689	9	3251	9	3769	10	4337	9
269	7	683	7	1153	8	1627	8	2153	9	2693	9	3253	9	3779	9	4339	8
271	6	691	7	1163	8	1637	9	2161	8	2699	9	3257	10	3793	8	4349	9
277	6	701	7	1171	9	1657	8	2179	8	2707	8	3259	9	3797	9	4357	9
281	7	709	8	1181	8	1663	8	2203	9	2711	9	3271	9	3803	9	4363	9
283	6	719	7	1187	9	1667	8	2207	9	2713	9	3299	8	3821	10	4373	10
293	7	727	8	1193	8	1669	9	2213	10	2719	8	3301	9	3823	9	4391	11
307	7	733	8	1201	7	1693	8	2221	9	2729	9	3307	9	3833	10	4397	9
311	6	739	8	1213	8	1697	8	2237	9	2731	9	3313	9	3847	10	4409	9
313	7	743	7	1217	8	1699	8	2239	8	2741	9	3319	8	3851	10	4421	9
317	6	751	7	1223	8	1709	8	2243	10	2749	9	3323	8	3853	9	4423	9
331	6	757	8	1229	8	1721	8	2251	8	2753	8	3329	10	3863	10	4441	10

TABLE I
 THE MAXIMUM NUMBER OF SOLUTIONS OF THE EQUATION $i \equiv g^{i-1+c} \pmod p$ OVER ALL POSSIBLE VALUES OF c AND PRIMITIVE ROOTS $g \in \mathbb{F}(p)$,
 $p < 5000$.

$m = 3$		
ee	eo	#
1	2	6

$m = 4$		
ee	eo	#
2	5	4
3	4	4

$m = 5$		
ee	eo	#
5	10	10
6	9	40
7	8	40

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

$m = 7$		
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

$m = 8$		
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

$m = 9$		
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

$m = 10$		
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

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

m	Length
3	1
4	2
5	3
6	4
7	8
8	11
9	18
10	27
11	39

TABLE II

THE VARIOUS DIFFERENT PARITY POPULATIONS FOR G_2 ARRAYS GENERATED IN $\mathbb{F}(2^m)$, $m = 3, \dots, 11$: THE THIRD COLUMN OF EACH ARRAY SHOWS THE NUMBER OF G_2 ARRAYS WITH THE GIVEN ee AND eo . THE LAST ARRAY CONTAINS THE NUMBER OF DIFFERENT PARITY POPULATIONS APPEARING FOR EACH GIVEN m , NAMELY THE NUMBER OF ROWS OF THE ARRAY CORRESPONDING TO m . 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.

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.

ACKNOWLEDGEMENTS

The author would like to thank Prof. Rod Gow, Prof. Paul Curran, Dr. Scott Rickard, and John Healy for the long and useful discussions on these experiments.

REFERENCES

- [1] 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.
- [2] Z. I. Borevich and I. R. Shafarevich. "Number Theory." Academic Press, New York and London, 1966.
- [3] C. Brown, M. Cenkci, 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.
- [4] J. P. Costas. "Medium constraints on sonar design and performance." Technical Report Class 1 Rep. R65EMH33, GE Co., 1965.
- [5] 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.
- [6] K. Drakakis. "A review of Costas arrays." Journal of Applied Mathematics, Volume 2006.
- [7] K. Drakakis, R. Gow, L. O'Carroll. "On some properties of Costas arrays generated via finite fields." IEEE CISS 2006.
- [8] K. Drakakis, R. Gow, and S. Rickard. "Parity properties of Costas arrays defined via finite fields." Advances in Mathematics of Communications, Vol. 1, Issue 3, Aug 2007, pp. 323-332.
- [9] S. Golomb. "Algebraic Constructions For Costas Arrays." Journal Of Combinatorial Theory Series A, Volume 37, Issue. 1, pp. 13-21, 1984.
- [10] S. Golomb, H. Taylor. "Constructions and properties of Costas arrays", Proceedings of the IEEE, Vol. 72, pp. 1143-1163, 1984.
- [11] 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.
- [12] S. Maric, I. Seskar, and E. Titlebaum. "On Cross-Ambiguity Properties of Welch-Costas Arrays When Applied in SS/FH Multiuser Radar and Sonar Systems." IEEE Transactions on Aerospace and Electronic Systems, Volume 30, No. 4, pp. 489-493, October 1994.
- [13] D. Shanks. "Solved and Unsolved Problems in Number Theory." 4th Edition, New York: Chelsea, pp. 154-157, 1993.
- [14] J. Silverman, V. Vickers, and J. Mooney. "On the Number of Costas arrays as a function of array size." Proceedings of the IEEE, pp. 851-853, July 1988.
- [15] W. P. Zhang. "On a problem of Brizolis." Pure and Applied Mathematics, Volume 11 (suppl.), pp. 1-3, 1995.