The Density of Costas Arrays Decays Exponentially

Lutz Warnke, Bill Correll, Jr., and Christopher N. Swanson

***Abstract*—Costas arrays are useful in radar and sonar engineering, and many other settings in which optimal 2-D autocorrelation is needed: they are permutation matrices in which the vectors joining different pairs of ones are all distinct. We prove that the density of Costas arrays among permutation matrices decays exponentially, solving a core problem in the theory of Costas arrays. The proof combines ideas from random graph theory with tools from probabilistic combinatorics.**

***Index Terms*—Costas arrays, density, permutations, combinatorics, probability, radar, sonar**

I. Introduction

COSTAS ARRAYS are fascinating objects of interdisciplinary interest: they not only have important engineering applications, but also give rise to challenging mathematical problems. Formally, a Costas array is simply a permutation matrix with the additional property that all vectors between any two different ones are distinct, see Figure 1. They were introduced in 1965 by Costas [1], with the goal of improving the target detection performance of frequency hopping sonar systems [2]. Around the same time Gilbert also independently studied them, motivated by the combinatorics of Latin squares [3].

Since the 1960s, engineers and mathematicians alike have been studying Costas arrays. Their optimal 2-D autocorrelation is useful in a variety of different applications, including radar waveforms [4]–[9], computer graphics, communications (particularly cell phones), experimental design, data mining, and a patent [10] that uses Costas arrays to match patterns. Widely studied mathematical questions include existence [11]–[13], constructions [11], [14]–[17], structural properties [18]–[26], and enumeration [27]–[35] of Costas arrays.

From the beginning, the number $C(n)$ of $n\times n$ Costas arrays has been of core theoretical interest. After determining $C(n)$ for $n \leq 13$ by exhaustive search in 1984, Golomb and Taylor compiled a fundamental list of 10 open problems regarding the asymptotic behavior of $C(n)$, see [11, Section V], including the asymptotic enumeration conjecture that

$$\frac{C(n)}{n!} \to 0 \qquad \text{as } n \to \infty, \tag{1}$$

i.e., that the density $C(n)/n!$ of Costas arrays among permutation matrices tends to zero. This conjecture received considerable attention, and three independent proofs emerged in the 1980s: first by Weiss, next by Reiner, and finally by Davies, see [12], [36], [37]. In fact, they each proved that

$$\frac{C(n)}{n!} \leq \frac{O(1)}{n}. \tag{2}$$

Supported by the values of $C(n)$ for small n, in the late 1980s it became a folklore speculation that the density $C(n)/n!$ should in fact decay exponentially, see Table I and [38, p. 119]. It remained a well-known challenge to narrow the gap between the rigorous upper bound (2) and the rate of decay observed in practice, see [12], [39], [40].

In this paper we prove that the density $C(n)/n!$ of Costas arrays among permutation matrices decays exponentially, confirming the above-mentioned speculations from the 1980s. In particular, Theorem I.1 below solves the first part of Problem 4 of Drakakis [40], which in his 2011 update of the Golomb–Taylor open problems list is marked as one of the core theoretical problems for Costas arrays.

Theorem I.1 (Main Result: Exponential Decay)**.** *There is a constant $c > 0$ so that the density $C(n)/n!$ of $n \times n$ Costas arrays among $n \times n$ permutation matrices satisfies*

$$\frac{C(n)}{n!} \leq e^{-cn} \qquad \textit{for all } n \geq 3. \tag{3}$$

The exponential decay of (3) is nearly best possible, since we have the elementary lower bound

$$\frac{C(n)}{n!} \geq e^{-n \log n} \qquad \text{for infinitely many } n, \tag{4}$$

see (38) in Section V. In (3) the restriction to $n \geq 3$ is necessary, since $C(n)/n! = 1$ for $n \in \{1, 2\}$, see Table I. Theorem I.1 significantly improves upon the previously known polynomial decay of $C(n)/n!$, where the smallest implicit constant in (2) is due to Swanson, Correll and Ho [41].

In addition to proving a long-standing open problem in the theory of Costas arrays, a further contribution of this paper lies in the transfer of proof techniques from random graph theory to Costas arrays. Indeed, we will prove (3) by exploiting that $C(n)/n!$ is the probability that a random $n \times n$ permutation matrix is a Costas array. While previous work then used the second moment method to obtain the polynomial decay (2), in this paper we will instead use the bounded differences inequality (Theorem III.1) to obtain the exponential decay (3); see Sections III and IV. A major challenge for obtaining exponential decay from this inequality is that a direct application only gives the trivial upper bound $C(n)/n! \leq 1$, the key obstacle being that the relevant random variables are not sufficiently smooth or Lipschitz; see Section III-B. We will overcome this obstacle by adapting powerful ideas of Bollobás [42] from random graph theory; see Section IV.

Manuscript Date: July 6, 2021; revised June 12, 2022.

L. Warnke is with the Department of Mathematics, University of California, San Diego, La Jolla CA 92093, USA. E-mail: lwarnke@ucsd.edu. Research partially supported by by NSF Grant DMS-1703516, NSF CAREER grant DMS-1945481 and a Sloan Research Fellowship.

B. Correll, Jr. is a Senior IEEE Member and with Maxar Technologies, Ypsilanti, MI 48197, USA. E-mail: bcorrell@ieee.org.

C.N. Swanson is with Ashland University, Ashland, OH 44805, USA. E-mail: cswanson@ashland.edu.

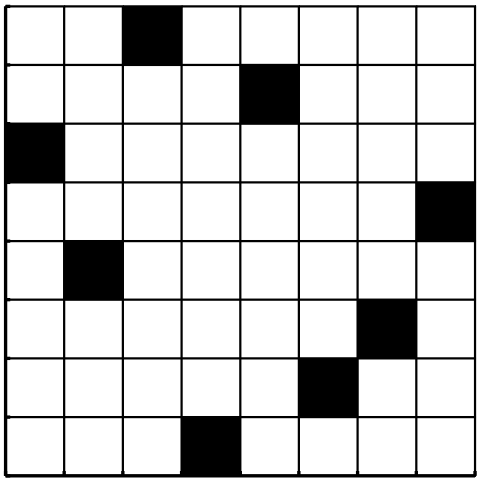

Fig. 1. Example of an 8×8 Costas array, with black squares representing ones (and the remaining squares representing zeros): in this permutation matrix all $\binom{8}{2} = 28$ vectors between pairs of different ones are distinct, i.e., they differ in either length or slope.

II. Background on the numbers of Costas arrays

Definition II.1 (Costas Array)**.** *A Costas array is a permutation matrix with the additional property that all vectors between any two different ones are distinct.*

An example of an 8×8 Costas array is shown in Figure 1, with black squares representing the ones of the permutation matrix. In the frequency-hopping remote sensing applications for which Costas arrays were originally designed, the dimensions of the matrix correspond to transmit time intervals and transmit frequencies. When the frequency hopping pattern is shifted in both time (horizontally) and frequency (vertically), then any one can be brought into coincidence with any other one. The crux of Costas arrays is that no such shift (other than the identity, which is not a shift at all) can bring two different ones into coincidence with any two other ones. This optimal auto-correlation also enables other applications, such as magnetic clamping [10], sub-pixel metrology [43], digital watermarking and steganography [44], [45].

A practical reason to care about the number $C(n)$ of $n \times n$ Costas arrays arises in remote sensing. The tone transmit ordering for a frequency-hopped radar is rapidly changed among a set of Costas arrays of the same order n for two reasons: (i) to simultaneously maintain low probability of intercept operations and target detection performance, and (ii) to control pulse train ambiguities. Selecting the order n to be approximately the time-bandwidth product of the system such that many $n \times n$ Costas arrays exist addresses both needs [46, Section III-IV]. Another reason to care about values of $C(n)$ arises in shared-band communications, for which Costas arrays supply code schemes. In such applications, performance is improved for orders n for which $C(n)$ is large.

In the remainder of this section we shall review further relevant background, which will illustrate that the number $C(n)$ of $n \times n$ Costas arrays has been inspected from various angles since the 1980s.

TABLE I
Number $C(n)$ of $n \times n$ Costas arrays

n	C(n)	n	C(n)	n	C(n)	n	C(n)	n	C(n)
1	1	7	200	13	12828	19	10240	25	88
2	2	8	444	14	17252	20	6464	26	56
3	4	9	760	15	19612	21	3536	27	204
4	12	10	2160	16	21104	22	2052	28	712
5	40	11	4368	17	18276	23	872	29	164
6	116	12	7852	18	15096	24	200	30	??

A. Enumerative Efforts

Many structural insights into Costas arrays were gained by studying $C(n)$ for small orders n via exhaustive enumeration of all possible $n \times n$ Costas arrays. For example, in 1984 Golomb and Taylor [11] reported the complete enumeration for $n \leq 13$ via exhaustive computer search, whose findings underpinned their influential open problems list. During the next three decades the complete enumeration was extended to $n \leq 29$ in sequence of papers [27]–[34], which in turn was instrumental for the 2011 update of the aforementioned fundamental open problems list [40]. The values of $C(17)$ and $C(27)$ are particularly insightful as they reveal that $C(n)$ is neither monotone increasing nor unimodal.

The tabulated values of $C(n)$ in Table I record the results of these massively-distributed backtracking searches for Costas arrays, which for orders $n = 28$ and $n = 29$ took the equivalent of 70 and 366.55 years of single CPU time, respectively [33], [34]. Despite such enormous computational efforts, it remains unknown if Costas arrays exist for order $n = 32$, see [12]. Part of the reason is the 'combinatorial explosion' of the search space: for each increment of order n approximately five times more computational resources are needed according to [31, pp. 530-531] and [47, p. 22]. Interestingly, Correll [35, Equation (3)] found a closed-form sum for $C(n)$ based on the Möbius Inversion Formula, but this expression has proven difficult to evaluate [40, p. 8].

These exhaustive enumeration efforts have been facilitated by an alternate definition of Costas arrays. Namely, for a given permutation π of $[n] := \{1, \ldots, n\}$ the one-line form is

$$\pi = a_1 a_2 \ldots a_n, \tag{5}$$

where $a_j = \pi(j)$. Row r of the difference triangle of π for $1 \leq r \leq n-1$ is then given by the $n - r$ differences

$$a_{r+1} - a_1 \qquad a_{r+2} - a_2 \qquad \cdots \qquad a_n - a_{n-r}. \tag{6}$$

Here the conceptual point is that the permutation π represents an $n \times n$ Costas array if no row of its difference triangle has repeated differences, which in turn can be efficiently verified by a computer with only $O(n^3)$ many difference comparisons [2], [48].

Interest in finding new Costas arrays and additional values of $C(n)$ has spawned research into constraints on difference triangles of Costas arrays, in order to further accelerate backtracking searches. In particular, Chang [49] remarked in 1987 that only differences in rows $r \leq \lfloor \frac{n-1}{2} \rfloor$ need to be computed for verification, and Barker, Drakakis, and Rickard [48, Theorem 4, Section V] showed in 2009 that an isosceles-trapezoidal

region of differences in rows $\frac{n}{3} < r < \lfloor \frac{n-1}{2} \rfloor$ need not be computed. More recently, Correll [19] established constraints on the number of positive differences in the rows $r \leq \lfloor \frac{n}{3} \rfloor$, and additional constraints [20] on first differences ($r = 1$).

Drakakis [39] quantified the overall restrictiveness of the various structural constraints by defining the degrees of freedom $L(n)$ of an $n \times n$ Costas array to be the minimal number of integers from the domain $[n]$ whose images need to be specified in order to uniquely determine a Costas array. Based on computational data he conjectured [39, Conjecture 2] that $L(n) \leq 3$ for $n \geq 24$, and he proved that $L(n) = o(n)$ in fact already suffices [39, Section IV] to establish exponential decay of the density $C(n)/n!$ of Costas arrays.

B. Constructions of Costas Arrays and Beard's Database

Costas arrays can be constructed using finite field techniques. For example, Welch (within [14]) gave a construction involving a single primitive element. Golomb also gave a generalization of a construction due to Lempel to two distinct primitive elements [15]. Unfortunately, such explicit constructions (and variants thereof) do not work for all orders n, and it remains open if Costas arrays exist for all n; see [12], [17], [40]. However, the Welch and Lempel-Golomb constructions and the infinitude of primes show that $n \times n$ Costas arrays exist for infinitely many orders n, and even establish that $\limsup C(n) = \infty$ as $n \to \infty$ [11, p. 1158].

All known Costas arrays up to order 1030 are in Beard's database [50]. Figure 2 displays the number of Costas arrays of each order n in the database on logarithmic axes. The exact values of Table I show up in the left-hand part of the figure. The explicit constructions that account for the right-hand side of Figure 2 are explained in more detail in [46, p. 1047].

C. Heuristic Prediction of $C(n)$ and a Density Conjecture

In an effort towards understanding the asymptotic behavior of the number $C(n)$ of $n \times n$ Costas arrays, in 1988 Silverman, Vickers and Mooney [27] accurately predicted the shape of the left-hand hump in Figure 2, based on a probabilistic model in which the entries of the difference triangle (see Section II-A) associated with a random permutation matrix are independent [12], [40]. Their heuristic predicts that

$$\frac{C(n)}{n!} \approx \left(1 - \frac{K}{n+1}\right)^{\mathrm{IP}(n)}, \tag{7}$$

where the constant $K \approx 1.111$ was fit to the values of $C(n)$ for $n \leq 17$ (all known values around 1988) and the parameter

$$\mathrm{IP}(n) := \begin{cases} n(n-2)(2n+1)/24 & \text{if } n \text{ odd,} \\ (n+1)(n-1)(2n-3)/24 & \text{if } n \text{ even.} \end{cases} \tag{8}$$

In 2007, Beard et al. [31] fit K to the values of $C(n)$ for $n \leq 26$, and the resulting constant $K \approx 1.10784$ is nearly unchanged.

A more recent density prediction of Swanson, Correll, and Ho [41] is based on the heuristic that, in a random permutation matrix, the occurrences of the minimal configurations of ones that violate the definition of a Costas array are independent. This probabilistic heuristic leads to the conjecture that

$$\frac{C(n)}{n!} = O\left(e^{-n^2/18 - n/8}\right). \tag{9}$$

As it turns out, inequality (38) in Section V shows that the two heuristic density predictions (7) and (9) are both false for large n. The crux is that both formulas are not useful for large n, as they predict that $\limsup C(n) = 0$ as $n \to \infty$.

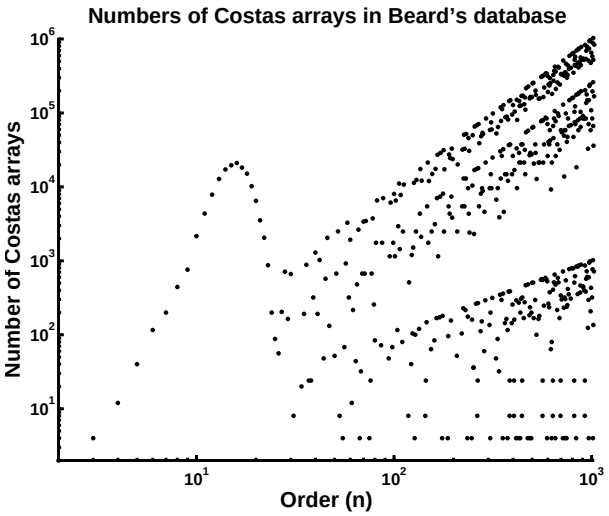

Fig. 2. Numbers of $n \times n$ Costas arrays in Beard's database [50]: for $n \leq 29$ these equal $C(n)$, and for $n \geq 30$ these are lower bounds for $C(n)$. Our main result (Theorem I.1) shows that $C(n)/n!$ decays exponentially with n.

III. Density of Costas Arrays: Key Challenges of Probabilistic Approach

Our upcoming proof of Theorem I.1 in Section IV will use probabilistic techniques to bound the density $C(n)/n!$ of Costas arrays from above. To this end we define S_n as the set of all permutations of $[n] = \{1, \ldots, n\}$, and write M_π for the $n \times n$ permutation matrix representing $\pi \in S_n$ (i.e., $M_\pi = (m_{ij})_{i,j \in [n]}$ with $m_{ij} = 1$ if $\pi(i) = j$ and $m_{ij} = 0$ otherwise). Choosing the permutation $\pi \in S_n$ uniformly at random, we obtain that

$$\mathbb{P}(M_\pi \text{ is a Costas array}) = \frac{C(n)}{n!}, \tag{10}$$

since M_π equals any given Costas array with probability $1/n!$. A Costas array cannot contain three equally-spaced collinear ones, since otherwise the vector from the left one to the middle one would be the same as the vector from the middle one to the right one. These forbidden sets of three ones are called *L_3-configurations* (there are two other forbidden configurations, see [41], but considering L_3-configurations suffices for our purposes). Writing $X = X(\pi)$ for the number of (unordered) L_3-configurations in the random $n \times n$ permutation matrix M_π, using (10) it follows that

$$\frac{C(n)}{n!} = \mathbb{P}(M_\pi \text{ is a Costas array}) \leq \mathbb{P}(X = 0). \tag{11}$$

A. Second Moment Method

To establish the polynomial decay $C(n)/n! = O(1/n)$ as in previous work [12], [37], [41], in view of inequality (11) it suffices to apply the second moment method to X. Indeed, after carefully estimating the first two moments of X, Chebychev's inequality eventually gives the polynomial bound

$$\mathbb{P}(X = 0) \leq \operatorname{Var} X/(\mathbb{E}X)^2 = O(1/n), \tag{12}$$

see [12, Section 4.2]. It it well-known that such inequalities obtained by estimating moments of small order (like Chebychev's inequality) usually do not give exponential bounds. In other words, the basic moment based proof approach used in previous work is not suitable for proving Theorem I.1.

B. Bounded Differences Inequality

To obtain the stronger exponential decay $C(n)/n! \leq e^{-cn}$ claimed by Theorem I.1, we will estimate $\mathbb{P}(X = 0)$ via a more powerful tool from probabilistic combinatorics, namely the following *bounded differences inequality* for random permutations (which follows from Azuma-Hoeffding type martingale arguments, see [51, Section 11.1] or [52, Section 1.1.4]).

Theorem III.1 (Bounded Differences Inequality)**.** *Let $f : S_n \to \mathbb{R}$ be a function with discrete Lipschitz coefficient D, i.e., such that $|f(\sigma) - f(\sigma')| \leq D$ whenever σ' arises from σ via a transposition. Choosing $\pi \in S_n$ uniformly at random, the random variable $Z := f(\pi)$ satisfies, for all $t \geq 0$,*

$$\mathbb{P}\big(Z \leq \mathbb{E}Z - t\big) \leq \exp\left(-\frac{t^2}{2nD^2}\right). \tag{13}$$

Applying the bounded differences inequality (13) to the number $Z = X(\pi)$ of L_3-configurations in the random $n \times n$ permutation matrix M_π, using $X = X(\pi) \geq 0$ it follows that

$$\mathbb{P}(X = 0) = \mathbb{P}(X \leq \mathbb{E}X - \mathbb{E}X) \leq \exp\left(-\frac{(\mathbb{E}X)^2}{2nD^2}\right), \tag{14}$$

where $D = D_X$ is the discrete Lipschitz coefficient from Theorem III.1 associated with the random variable $X = X(\pi)$. As we shall see in Equation (30) of Section IV-B, the expected number of L_3-configurations satisfies $\mathbb{E}X \sim n/8$ as $n \to \infty$. The key challenge is that the Lipschitz coefficient $D = D_X$ is too large for inequality (14) to be useful. Indeed, we shall below prove that $D = D_X \geq n - 2$, which in view of

$$0 \leq \frac{(\mathbb{E}X)^2}{2nD^2} \leq \frac{O(1)}{n} \tag{15}$$

implies that the right-hand side of inequality (14) tends to one as $n \to \infty$ (and not to zero as one might hope). Using (11) this means that the bounded differences inequality only gives the trivial density bound $C(n)/n! \leq 1$ for large n.

For the interested reader we now prove that the discrete Lipschitz coefficient of X indeed satisfies $D = D_X \geq n-2$, as claimed above. To this end we consider the identity permutation $\sigma \in S_n$, and the permutation $\sigma' \in S_n$ which arises from σ by transposing $n - 1$ and n. Recalling that $X(\sigma)$ counts the number of (unordered) L_3-configurations in the permutation matrix M_σ representing σ, by observing that the two bottom right-hand ones in $M_{\sigma'}$ are not a part of any L_3-configuration, it follows that the above-defined permutations σ, σ' satisfy

$$X(\sigma) - X(\sigma') = \mathrm{Idl}_3(n) - \mathrm{Idl}_3(n-2), \tag{16}$$

where $\mathrm{Idl}_3(n)$ denotes the number of (unordered) L_3-configurations in the $n \times n$ identity permutation matrix. The formula

$$\mathrm{Idl}_3(n) = \begin{cases} \frac{1}{4}n(n-2) & \text{if } n \text{ even}, \\ \frac{1}{4}(n-1)^2 & \text{if } n \text{ odd}, \end{cases} \tag{17}$$

appearing in [41, Theorem 4] then implies that

$$D = D_X \geq |X(\sigma) - X(\sigma')| = n - 2, \tag{18}$$

i.e., that the discrete Lipschitz coefficient of X is very large.

IV. Density of Costas Arrays: Proof of Theorem I.1

In this section we prove Theorem I.1, by estimating the density $C(n)/n!$ of Costas arrays using the bounded differences inequality (13). We will overcome the technical challenge of large Lipschitz coefficients (discussed in Section III) by transferring proof ideas from random graph theory to Costas arrays.

More concretely, we shall adapt a 'disjoint approximation' technique that can be traced back to a random graphs breakthrough of Bollobás [42] from 1988. This powerful proof technique consists of the following two key steps:

Step 1: Using the combinatorial idea of counting 'disjoint' objects, define an auxiliary random variable $X' = X'(\pi)$ which (i) satisfies $0 \leq X' \leq X$, and (ii) has a small discrete Lipschitz coefficient $D = D_{X'}$.

Step 2: Using a random sampling approach, bound the expected value $\mathbb{E}X'$ from below.

To see why the auxiliary random variable $X' = X'(\pi)$ is useful, note that $0 \leq X' \leq X$ implies

$$\mathbb{P}(X = 0) \leq \mathbb{P}(X' = 0). \tag{19}$$

Applying the bounded differences inequality (Theorem III.1) to $Z = X'(\pi)$ similarly to (14), it follows from (11) that

$$\frac{C(n)}{n!} \leq \exp\left(-\frac{(\mathbb{E}X')^2}{2nD^2}\right), \tag{20}$$

where $D = D_{X'}$ is the discrete Lipschitz coefficient from Theorem III.1 associated with the random variable $X' = X'(\pi)$. Adapting the above-mentioned two key steps to Costas arrays, in Equations (23) and (37) of Sections IV-A and IV-B we will show that for all $n \geq 3$ our auxiliary random variable X' satisfies $D = D_{X'} = 2$ and $\mathbb{E}X' \geq an$ for a suitable constant $a > 0$. Inserting these estimates into (20) then gives

$$\frac{C(n)}{n!} \leq \exp\left(-\frac{a^2 n}{8}\right) \qquad \text{for all } n \geq 3, \tag{21}$$

establishing the desired exponential Costas array density (3) of Theorem I.1 with constant $c := a^2/8$.

To complete the proof of Theorem I.1 it remains to adapt the two key steps of the disjoint approximation technique to Costas arrays, i.e., to define suitable $X' = X'(\pi)$ which satisfies $0 \leq X' \leq X$ and $D = D_{X'} = 2$ as well as $\mathbb{E}X' \geq an$.

A. Step 1: Define X' with Small Lipschitz Coefficient

The first step of the disjoint approximation technique addresses the key challenge that the number $X = X(\pi)$ of L_3-configurations in M_π has a large discrete Lipschitz coefficient. In the context of random graphs Bollobás [42] realized that, by artificially limiting 'overlaps' between the objects of interest, one can often replace X by an auxiliary random variable that (i) behaves similarly to X, and (ii) has a small discrete Lipschitz coefficient. Adapting this combinatorial insight to Costas arrays, we define $X' = X'(\pi)$ as the maximum number of (unordered) L_3-configurations in the random $n \times n$ permutation matrix M_π which are pairwise disjoint, i.e., which share no ones. Note that

$$0 \leq X' \leq X. \tag{22}$$

Recall that the discrete Lipschitz coefficient $D = D_{X'}$ from Theorem III.1 is an upper bound on the maximum change of $X'(\sigma)$ that can result from applying a transposition τ to $\sigma \in S_n$. Since each one in the permutation matrix M_σ is contained in at most one L_3-configuration counted by $X'(\sigma)$, for any permutation $\sigma \in S_n$ and transposition τ it follows that

$$|X'(\sigma) - X'(\tau\sigma)| \leq 2. \tag{23}$$

Hence $D = D_{X'} := 2$ is a valid choice for the discrete Lipschitz coefficient of X'.

B. Step 2: Lower Bound on the Expectation $\mathbb{E}X'$

In the second step of the disjoint approximation technique it remains to show that the expected value $\mathbb{E}X'$ of the auxiliary random variable $X' = X'(\pi)$ is large. Here our main tool is a random sampling technique from probabilistic combinatorics (cf. [53, Theorem 3.2.1 and Lemma 7.3.1]), which uses randomness to construct a set of disjoint L_3-configurations.

Turning to the details, let $\mathcal{L} = \mathcal{L}(\pi)$ denote the collection of all (unordered) L_3-configurations in the $n \times n$ permutation matrix M_π representing the random permutation $\pi \in S_n$, so that $|\mathcal{L}| = X$. Let $\mathcal{O} = \mathcal{O}(\pi)$ denote the collection of all unordered pairs $\{L, L'\} \subseteq \mathcal{L}$ which overlap in exactly one or two ones (note that this implies $L \neq L'$). Let $\mathcal{L}_q = \mathcal{L}_q(\pi)$ be a random subset of $\mathcal{L}$ defined by including each $L \in \mathcal{L}$ independently with probability q, where $q \in [0,1]$ is determined later. Let $\mathcal{O}_q = \mathcal{O}_q(\pi)$ contain all pairs $\{L, L'\} \in \mathcal{O}$ with $L, L' \in \mathcal{L}_q$. Since each $L \in \mathcal{L}$ is included in $\mathcal{L}_q$ independently with probability q, it follows that

$$\mathbb{E}|\mathcal{L}_q| = q\mathbb{E}|\mathcal{L}| \quad \text{and} \quad \mathbb{E}|\mathcal{O}_q| = q^2\mathbb{E}|\mathcal{O}|. \tag{24}$$

Deleting from $\mathcal{L}_q$ one element from each pair in $\mathcal{O}_q$, we obtain a collection $\mathcal{L}_q^*$ of pairwise disjoint L_3-configurations in M_π. Noting $X' \geq |\mathcal{L}_q^*| \geq |\mathcal{L}_q| - |\mathcal{O}_q|$, using the linearity of the expectation together with (24) and $|\mathcal{L}| = X$ we infer that

$$\mathbb{E}X' \geq \mathbb{E}|\mathcal{L}_q| - \mathbb{E}|\mathcal{O}_q| = q\mathbb{E}X - q^2\mathbb{E}|\mathcal{O}|. \tag{25}$$

To establish our desired lower bound $\mathbb{E}X' \geq an$, it remains to estimate the expectations $\mathbb{E}X$ and $\mathbb{E}|\mathcal{O}|$, and then choose the inclusion probability $q \in [0,1]$ which maximizes (25).

We start with the expected number $\mathbb{E}X$ of L_3-configurations in the random permutation matrix M_π. Let $\mathfrak{L}_3(n)$ denote the collection of all possible (unordered) L_3-configurations that can appear in some $n \times n$ permutation matrix. Given $L \in \mathfrak{L}_3(n)$, we denote by $\mathbb{1}_{\{L \subseteq M_\pi\}}$ the indicator variable for the event that $L \subseteq M_\pi$ holds, i.e., that L is contained in M_π. Noting that the number $X = X(\pi)$ of (unordered) L_3-configurations in M_π can be expressed as the sum

$$X = \sum_{L \in \mathfrak{L}_3(n)} \mathbb{1}_{\{L \subseteq M_\pi\}}, \tag{26}$$

using the linearity of the expectation we see that

$$\mathbb{E}X = \sum_{L \in \mathfrak{L}_3(n)} \mathbb{E}(\mathbb{1}_{\{L \subseteq M_\pi\}}) = \sum_{L \in \mathfrak{L}_3(n)} \mathbb{P}(L \subseteq M_\pi). \tag{27}$$

Note that there are exactly $(n-3)!$ permutation matrices of order n which contain a given $L \in \mathfrak{L}_3(n)$. Since M_π equals any such matrix with probability $1/n!$, it follows that

$$\mathbb{E}X = \sum_{L \in \mathfrak{L}_3(n)} \frac{(n-3)!}{n!} = |\mathfrak{L}_3(n)| \cdot \frac{(n-3)!}{n!}. \tag{28}$$

According to [12, Equations (4.4) and (4.5)] the total number of (unordered) potential L_3-configurations is

$$|\mathfrak{L}_3(n)| = \begin{cases} \frac{1}{8}n^2(n-2)^2 & \text{if } n \text{ even}, \\ \frac{1}{8}(n-1)^4 & \text{if } n \text{ odd}, \end{cases} \tag{29}$$

and so we conclude that

$$\mu := \mathbb{E}X = \frac{|\mathfrak{L}_3(n)|}{n(n-1)(n-2)} \sim \frac{n}{8}. \tag{30}$$

We now turn to the expected number $\mathbb{E}|\mathcal{O}|$ of unordered overlapping pairs of L_3-configurations in the random permutation matrix M_π. Given $L, L' \in \mathfrak{L}_3(n)$, let $|L \cap L'|$ denote the number of overlapping ones in these two L_3-configurations. Proceeding similarly to Equations (26) and (27), using the linearity of the expectation it follows that

$$\mathbb{E}|\mathcal{O}| = \tfrac{1}{2} \sum_{\substack{(L,L') \in \mathfrak{L}_3(n) \times \mathfrak{L}_3(n): \\ |L \cap L'| \in \{1,2\}}} \mathbb{P}(L \subseteq M_\pi \text{ and } L' \subseteq M_\pi), \tag{31}$$

where the factor of $1/2$ takes into account that $|\mathcal{O}|$ counts unordered pairs. Writing $\mathfrak{L}_{3,j}(n)$ for the collection of all $(L, L') \in \mathfrak{L}_3(n) \times \mathfrak{L}_3(n)$ with $|L \cap L'| = j$, with analogous counting reasoning as for Equation (28), it then follows that

$$\mathbb{E}|\mathcal{O}| = \frac{|\mathfrak{L}_{3,1}(n)|}{2} \cdot \frac{(n-5)!}{n!} + \frac{|\mathfrak{L}_{3,2}(n)|}{2} \cdot \frac{(n-4)!}{n!}. \tag{32}$$

To bound $|\mathfrak{L}_{3,2}(n)|$ from above, note that there are $|\mathfrak{L}_3(n)|$ choices for $L \in \mathfrak{L}_3(n)$, and then at most $3 \cdot 3 = 9$ choices for $L' \in \mathfrak{L}_3(n)$ with $|L \cap L'| = 2$ (as there are 3 ways to choose the two common ones, and at most 3 ways to choose a third one of L'). It follows that

$$|\mathfrak{L}_{3,2}(n)| \leq |\mathfrak{L}_3(n)| \cdot 9. \tag{33}$$

To bound $|\mathfrak{L}_{3,1}(n)|$ from above, we proceed similarly: note that there are $|\mathfrak{L}_3(n)|$ choices for $L \in \mathfrak{L}_3(n)$, and then at most $3 \cdot n^2 \cdot 3 = 9n^2$ choices for $L' \in \mathfrak{L}_3(n)$ with $|L \cap L'| = 1$ (as there are 3 ways to choose the single common one, at

most n^2 ways to choose a second one of L', and at most 3 ways to choose a third one of L'). It follows that

$$|\mathfrak{L}_{3,1}(n)| \leq |\mathfrak{L}_3(n)| \cdot 9n^2. \tag{34}$$

To clean up border cases, note that $|\mathfrak{L}_{3,1}(n)| = 0$ if $n \leq 4$ and that $|\mathfrak{L}_{3,2}(n)| = 0$ if $n \leq 3$. Inserting the above estimates into (32), using Equation (30) it follows that

$$\mathbb{E}|\mathcal{O}| \leq \frac{9\mu}{2}\left[\frac{\mathbb{1}_{\{n\geq 5\}}n^2}{(n-3)(n-4)} + \frac{\mathbb{1}_{\{n\geq 4\}}}{n-3}\right] =: \Delta, \tag{35}$$

where $\mathbb{1}_{\{n\geq j\}}$ is the indicator function for $n \geq j$, as usual.

We are now ready to derive the desired lower bound on $\mathbb{E}X'$. Namely, after inserting the bounds $\mathbb{E}X = \mu$ and $\mathbb{E}|\mathcal{O}| \leq \Delta$ into inequality (25), we see that the inclusion probability $q := \min\{\mu/(2\Delta), 1\}$ yields

$$\mathbb{E}X' \geq q(\mu - q\Delta) \geq \frac{q\mu}{2} = \frac{\mu}{4} \cdot \min\left\{\frac{\mu}{\Delta},\, 2\right\}. \tag{36}$$

Inspecting (29), (30) and (35), it follows that there is a constant $a > 0$ such that for all $n \geq 3$ we have

$$\mathbb{E}X' \geq an. \tag{37}$$

This concludes the disjoint approximation technique, and thus completes the proof of Theorem I.1, as discussed.

V. Conclusion

In this paper we proved that the density $C(n)/n!$ of Costas arrays among permutation matrices decays exponentially, narrowing the gap between the theoretical and empirical bounds that had existed since the 1980s. We did this by showing, more generally, that the density of permutation matrices without three equally-spaced collinear ones decays exponentially. A key proof ingredient was an approximation technique from random graph theory, which allowed us to overcome the concentration inequality-related obstacle of large Lipschitz coefficients. This combinatorial technique does not seem to be as widely known in other fields, and we hope that our exposition in Section IV makes it accessible to a wider range of researchers.

Our knowledge of the number $C(n)$ of $n \times n$ Costas arrays remains somewhat incomplete. For orders $n \geq 1$ for which $n \times n$ Costas arrays do exist, note that we trivially have $C(n)/n! \geq 1/n! \geq n^{-n}$. It thus follows from Theorem I.1 and the explicit constructions mentioned in Section II-B that for infinitely many (but not all) n we have

$$e^{-n\log n} \leq \frac{C(n)}{n!} \leq e^{-cn}. \tag{38}$$

In terms of asymptotic enumeration of Costas arrays, the main open problem is to close the gap in (38). As a first step in this direction, we propose the following more modest problem.

Problem V.1 (Exponential Rate of Decay)**.** *Determine the order of magnitude of* $-\log\left(C(n)/n!\right)$ *as* $n \to \infty$.

Acknowledgments

The authors would like to thank James K. Beard and David Bevan for pointing out references, as well as Guillem Perarnau, Michael Simkin and Erlang Surya for discussions about Problem V.1. We also thank the referees for helpful comments.

References

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

[2] ——, "A study of detection waveforms having nearly ideal range-Doppler ambiguity properties," *Proc. IEEE*, vol. 72, pp. 996–1009, 1984.

[3] E. N. Gilbert, "Latin squares which contain no repeated digrams," *SIAM Review*, vol. 7, pp. 189–198, 1965.

[4] J. P. Donohoe and F. M. Ingels, "Ambiguity function properties of frequency-hopped radar / sonar signals," in *IEEE Proceedings - 1989 Southeastcon, Vol. 1*, 1989, pp. 85–89.

[5] N. Levanon and E. Mozeson, *Radar Signals*, 1st ed. ISBN 978-0-471-47378-7: John Wiley & Sons, Inc., 2004.

[6] C.-F. Chang and M. R. Bell, "Frequency-coded waveforms for enhanced delay-doppler resolution," *IEEE Transactions on Information Theory*, vol. 49, no. 11, pp. 2960–2971, November 2003.

[7] P. E. Pace and C. Y. Ng, "Costas CW frequency hopping radar waveform: peak sidelobe improvement using Golay complementary sequences," *Electronics Letters*, vol. 46, no. 2, pp. 169–170, January 2010.

[8] A. Pezeshki, R. Calderbank, and L. L. Scharf, "Sidelobe suppression in a desired range/doppler interval," in *Proceedings of the 2009 IEEE Radar Conference*, 2009, pp. 1–5.

[9] Z. Wagner, D. Garren, and P. E. Pace, "SAR imagery via frequency shift keying Costas coding," in *Proceedings of the 2017 IEEE Radar Conference*, 2017, pp. 1789–1792.

[10] L. W. Fullerton and M. D. Roberts, "Method for assembling a magnetic attachment mechanism," U.S. Patent 10 173 292, January, 2019. [Online]. Available: http://www.freepatentsonline.com/10173292.html

[11] S. Golomb and H. Taylor, "Constructions and properties of Costas arrays," *Proc. IEEE*, vol. 72, pp. 1143–1163, 1984.

[12] K. Drakakis, "A review of Costas arrays," *Journal of Applied Mathematics*, vol. 2006, pp. 1–32, 2006.

[13] B. Correll, Jr., C. N. Swanson, and R. W. Ho, "Costas arrays and the Lovász local lemma," in *Proceedings of the 2015 IEEE Radar Conference*, 2015, pp. 186–191.

[14] S. Golomb and H. Taylor, "Two-dimensional synchronization patterns for minimum ambiguity," *IEEE Trans. Inform. Theory*, vol. 28, no. 4, pp. 600–604, 1982.

[15] S. Golomb, "Algebraic constructions for Costas arrays," *J. Comb. Theory Series A*, vol. 37, pp. 13–21, 1984.

[16] ——, "The T_4 and G_4 constructions for Costas arrays," *IEEE Transactions on Information Theory*, vol. 38, no. 4, pp. 1404–1406, 1992.

[17] S. W. Golomb and G. Gong, "The status of Costas arrays," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4260–4265, November 2007.

[18] K. Drakakis, R. Gow, and L. O'Carroll, "On the symmetry of Welch- and Golomb-constructed Costas arrays," *Discrete Mathematics*, vol. 309, no. 8, pp. 2559–2563, April 2009.

[19] B. Correll, Jr., "A new structural property of Costas arrays," in *Proceedings of the 2018 IEEE Radar Conference*, 2018, pp. 0748–0753.

[20] ——, "More new structural properties of Costas arrays," in *Proceedings of the 2019 IEEE Radar Conference*, 2019.

[21] K. Drakakis, "On the hops present in Costas permutations," *IEEE Transactions on Information Theory*, vol. 56, no. 3, pp. 1271–1277, March 2010.

[22] J. Jedwab and J. Wodlinger, "The deficiency of Costas arrays," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7947–7954, December 2014.

[23] S. V. Maric, I. Seskar, and E. L. Titlebaum, "On cross-ambiguity properties of Welch-Costas arrays," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 30, no. 4, pp. 1063–1071, Oct 1994.

[24] J. Jedwab and L. Yen, "Costas cubes," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 3144–3149, 2018.

[25] D. Gómez-Pérez and A. Winterhof, "A note on the cross-correlation of Costas permutations," *IEEE Transactions on Information Theory*, vol. 66, no. 12, pp. 7724–7727, 2020.

[26] J. K. Beard, "Singular value decomposition of a matrix representation of the Costas condition for Costas array selection," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 57, no. 2, pp. 1139–1161, 2021.

[27] J. Silverman, V. E. Vickers, and J. M. Mooney, "On the number of Costas arrays as a function of array size," *Proc. IEEE*, vol. 76, no. 7, pp. 851–853, July 1988.

[28] O. Moreno, P. Pei, and J. G. Ramirez, "A parallel algorithm for the enumeration of Costas sequences," in *Proceedings of the Seventh SIAM Conference on Parallel Processing for Scientific Computing, PPSC 1995, San Francisco, California, USA, February 15-17, 1995*, D. H. Bailey, P. E. Bjørstad, J. R. Gilbert, M. Mascagni, R. S. Schreiber, H. D. Simon, V. Torczon, and L. T. Watson, Eds. SIAM, 1995, pp. 255–260.

[29] O. Moreno, J. Ramírez, D. Bollman, and E. Orozco, "Faster backtracking algorithms for the generation of symmetry-invariant permutations," *Journal of Applied Mathematics*, vol. 2, no. 6, pp. 277–287, 2002.

[30] S. Rickard, E. Connell, F. Duignan, B. Ladendorf, and A. Wade, "The enumeration of costas arrays of size 26," in *2006 40th Annual Conference on Information Sciences and Systems*, 2006, pp. 815–817.

[31] J. K. Beard, J. C. Russo, K. G. Erickson, M. C. Monteleone, and M. T. Wright, "Costas array generation and search methodology," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 43, no. 2, pp. 522–538, 2007.

[32] K. Drakakis, S. Rickard, J. K. Beard, R. Caballero, F. Iorio, G. O'Brien, and J. Walsh, "Results of the enumeration of Costas arrays of order 27," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4684–4687, 2008.

[33] K. Drakakis, F. Iorio, and S. Rickard, "The enumeration of Costas arrays of order 28 and its consequences," *Advances in Mathematics Communications*, vol. 5, no. 1, pp. 69–86, 2011.

[34] K. Drakakis, F. Iorio, S. Rickard, and J. Walsh, "Results of the enumeration of Costas arrays of order 29," *Advances in Mathematics Communications*, vol. 5, pp. 547–553, 2011.

[35] B. Correll, Jr., "A closed form expression for the number of Costas arrays of arbitrary order," in *Proceedings of the Forty-First Asilomar Conference on Signals, Systems, and Computers*, 2007, pp. 2218–2222.

[36] S. W. Golomb, "Discrete Mathematics for Communication Systems," *Final technical report on ONR Contract N00014-84-K-0189*, 1990. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA220430.pdf

[37] V. S. Reiner, "Probabilistic methods for combinatorial problems," Princeton University, Bachelor's thesis, 1986.

[38] P. Grant, J. Dripps, L. O'Carroll, D. Davies, and C. Smyth, "Auto- and cross-ambiguity surface performance for frequency-hop coded waveforms," in *IEEE International Symposium on Spread Spectrum Techniques and Applications*, 1990, pp. 116–122.

[39] K. Drakakis, "Some results on the degrees of freedom of Costas arrays," in *Proceedings of Forty-Fourth Conference on Information Sciences and Systems*, 2010, pp. 1–5.

[40] ——, "Open problems in Costas arrays." [Online]. Available: http://arxiv.org/abs/1102.5727

[41] C. N. Swanson, B. Correll, Jr., and R. W. Ho, "Enumeration of parallelograms in permutation matrices for improved bounds on the density of Costas arrays," *Electronic Journal of Combinatorics*, vol. 23, no. 1, pp. 1–14, 2016.

[42] B. Bollobás, "The chromatic number of random graphs," *Combinatorica*, vol. 8, no. 1, pp. 49–55, 1988.

[43] J. Healy, G. Sweeney, D. Mas, and J. Sheridan, "Use of Costas arrays in subpixel metrology," in *Proceedings of SPIE Vol. 9131, 91311J*, 2014, pp. 0748–0753.

[44] A. Soltanipanah, "Digital watermarking of non-media data stream (applications)," Ph.D. dissertation, RMIT University, Melbourne, June 2017.

[45] M. Sterling, E. Titlebaum, X. Dong, and M. Bocko, "An adaptive spread-spectrum data hiding technique for digital audio," in *Proceedings. (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005*, vol. 5, 2005, pp. V685–V688.

[46] B. Correll, Jr., J. K. Beard, and C. N. Swanson, "Costas array waveforms for closely-spaced target detection," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 2, pp. 1045–1076, April 2020.

[47] K. Taylor, S. Rickard, and K. Drakakis, "Costas arrays: Survey, standardization, and matlab toolbox," *ACM Trans. Math. Softw.*, vol. 37, no. 4, Feb. 2011.

[48] L. Barker, K. Drakakis, and S. Rickard, "On the complexity of the verification of the Costas property," *Proc. IEEE*, vol. 97, no. 3, pp. 586–593, March 2009.

[49] W. Chang, "A remark on the definition of Costas arrays," *Proc. IEEE*, vol. 75, no. 4, pp. 522–523, April 1987.

[50] J. K. Beard, "Costas arrays and enumeration to order 1030," IEEE Dataport, 2017. [Online]. Available: http://dx.doi.org/10.21227/H21P42

[51] M. Molloy and B. Reed, *Graph colouring and the probabilistic method*, ser. Algorithms and Combinatorics. Springer-Verlag, Berlin, 2002, vol. 23.

[52] L. Warnke, "On the method of typical bounded differences," *Combinatorics, Probability and Computing*, vol. 25, no. 2, pp. 269–299, 2016.

[53] N. Alon and J. H. Spencer, *The Probabilistic Method*, 4th ed., ser. Wiley Series in Discrete Mathematics and Optimization. John Wiley & Sons, Inc., Hoboken, NJ, 2016.