Circular automata synchronize with high probability

Christoph Aistleitner [a],[*], Daniele D'Angeli [b],
Abraham Gutierrez [c], Emanuele Rodaro [d], Amnon Rosenmann [c]

[a] *Institute of Analysis and Number Theory, TU Graz, Austria*
[b] *Università Niccolò Cusano, Via don Gnocchi Roma, Italy*
[c] *Institute of Discrete Mathematics, TU Graz, Austria*
[d] *Department of Mathematics, Politecnico di Milano, Italy*

A R T I C L E   I N F O

A B S T R A C T

In this paper we prove that a uniformly distributed random circular automaton $\mathcal{A}_n$ of order n synchronizes with high probability (w.h.p.). More precisely, we prove that

$$\mathbb{P}\left[\mathcal{A}_n \text{ synchronizes}\right] = 1 - O\left(\frac{1}{n}\right).$$

The main idea of the proof is to translate the synchronization problem into a problem concerning properties of a random matrix; these properties are then established with high probability by a careful analysis of the stochastic dependence structure among the random entries of the matrix. Additionally, we provide an upper bound for the probability of synchronization of circular automata in terms of chromatic polynomials of circulant graphs.

© 2020 Elsevier Inc. All rights reserved.

* Corresponding author.
    E-mail addresses: aistleitner@math.tugraz.at (C. Aistleitner), daniele.dangeli@unicusano.it
(D. D'Angeli), a.gutierrez@math.tugraz.at (A. Gutierrez), emanuele.rodaro@polimi.it (E. Rodaro),
rosenmann@math.tugraz.at (A. Rosenmann).

1. Introduction

A *complete deterministic finite automaton* (DFA) is a tuple $\mathcal{A} = (Q, L)$, where $Q := \{q_1, q_2, \ldots, q_n\}$ is a finite set of *states* and $L := \{\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_k}\}$ is a finite set of mappings $\mathbf{a_i} : Q \to Q$, where $\mathbf{a}(q) = q'$ is also written as $q\mathbf{a} = q'$, $q, q' \in Q$, $\mathbf{a} \in L$. The number of states n is the *order* of $\mathcal{A}$. Each $\mathbf{a_i}$ is called a *letter* and a sequence $\mathbf{w} = \mathbf{a_{i_1}}\mathbf{a_{i_2}} \ldots \mathbf{a_{i_r}} \in L^*$ is a *word* of *length* r. The action of L on Q naturally extends to an action of L^* on Q, defined recursively by $q(\mathbf{aw}) = (q\mathbf{a})\mathbf{w}$, $q \in Q$, $\mathbf{a} \in L$, $\mathbf{w} \in L^*$. This action further extends to an action of L^* on subsets of Q by $\{q_{i_1}, q_{i_2}, \ldots, q_{i_k}\}\mathbf{w} = \{q_{i_1}\mathbf{w}, q_{i_2}\mathbf{w}, \ldots, q_{i_k}\mathbf{w}\}$. We say that the subset $S = \{q_{i_1}, q_{i_2}, \ldots, q_{i_k}\} \subseteq Q$ *synchronizes* if there exists a word $\mathbf{w} \in L^*$ such that $q_{i_1}\mathbf{w} = q_{i_2}\mathbf{w} = \ldots = q_{i_k}\mathbf{w}$ (equivalently, we say that $\mathbf{w}$ synchronizes S). If the set Q synchronizes then we say that $\mathcal{A}(Q, L)$ *synchronizes* (or that it is a synchronizing automaton). A word $\mathbf{w} \in L^*$ that synchronizes Q is called a *synchronizing* (or *reset*) word of $\mathcal{A}$.

The following simple criterion for synchronization is well known and plays a crucial role throughout the paper:

Claim 1. $\mathcal{A} = (Q, L)$ *synchronizes* $\iff$ *every pair of states* $q, q' \in Q$ *synchronizes.*

Proof. It is clear that if Q synchronizes by a reset word $\mathbf{w}$ then $\mathbf{w}$ synchronizes every pair of states of Q. Conversely, a reset word for Q can be formed by concatenating words w_i that synchronize pairs of states until we end up with a single state. $\square$

The synchronization property may be described in terms of the graph representation of $\mathcal{A}$. The set Q of states comprises the vertices of the graph and for each pair of states q, q' and a letter $\mathbf{a} \in L$ such that $q\mathbf{a} = q'$ there is an arrow $(q, q')_\mathbf{a}$ labeled with $\mathbf{a} \in L$ and connecting q to q'. Each $q \in Q$ and $w = \mathbf{a_{i_1}}\mathbf{a_{i_2}} \ldots \mathbf{a_{i_k}} \in L^*$ defines a directed path

$$\gamma(q, \mathbf{w}) := ((q, q_{i_1})_{\mathbf{a_{i_1}}}, (q_{i_1}, q_{i_2})_{\mathbf{a_{i_2}}}, \ldots, (q_{i_{k-1}}, q')_{\mathbf{a_{i_k}}})$$

that begins in q and ends in $q' = q\mathbf{w}$. $\mathcal{A}$ then synchronizes if and only if there is a word $\mathbf{w}$, such that the paths $\{\gamma(q, \mathbf{w}) : q \in Q\}$ have a common endpoint q', that is, the word $\mathbf{w}$ acts on Q as the constant mapping.

Synchronizing automata have been intensely studied by theoretical computer scientists as well as pure mathematicians since the 1960's; see [18] for a detailed introduction on synchronization of automata. A driving force in this research field is the Černỳ conjecture.

Conjecture 2 *(The Černỳ conjecture).* A synchronizing automaton $\mathcal{A}$ of order n has a shortest synchronizing word of length at most $(n-1)^2$.

The bound in the Černỳ conjecture is tight: in [6] Černỳ provided a series of synchronizing circular automata $C_2, C_3, \ldots$, such that C_n has order n and its shortest
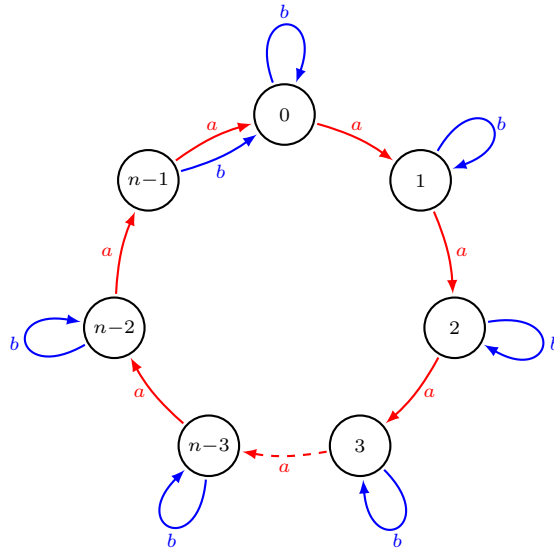
Fig. 1. The automaton C_n.

synchronizing word is of size exactly $(n-1)^2$ (see Fig. 1). Furthermore, the Černỳ series of circular automata $C_2, C_3, \ldots$ is the only known infinite series of automata whose shortest synchronizing words are of length $(n-1)^2$ [1].

The best known general upper bounds for the size of shortest synchronizing words of an automaton with n states are of order $O(n^3)$ [14][17][15]. Nevertheless, there are many classes of automata for which the Černỳ conjecture has been established (see [18] for examples).

In the last decade probabilistic approaches to the synchronization problem have been developed. Typical questions in this setting are: let $\mathcal{A}(\{0, 1, \ldots, n-1\}, L)$ be a uniformly chosen DFA with k letters on a certain probability space, is it true that with high probability the automaton $\mathcal{A}(\{0, 1, \ldots, n-1\}, L)$ is synchronizing? Does the Černỳ conjecture hold with high probability? Here we give a (non-comprehensive) list of recent achievements in this probabilistic setting:

- In [16] the authors study random automata $\mathcal{A}$ where the number of letters k grow together with n. In particular, they prove that $\mathcal{A}$ synchronizes w.h.p. when $k(n)$ grows fast enough;
- In [3] the author proves that $\mathbb{P}\left[\mathcal{A} \text{ synchronizes}\right] = 1 - O(n^{-k/2})$, for arbitrary $k \geq 2$, and $\mathbb{P}\left[\mathcal{A} \text{ synchronizes}\right] = 1 - \Theta(1/n)$ for $k = 2$;
- In [11] the author proves that $\mathcal{A}$ admits w.h.p. a synchronizing word of length $O(n \log^3 n)$ for arbitrary $k \geq 2$;

- In [4] the authors prove that if $\mathcal{A}$ is uniformly chosen among the strongly-connected almost-group automata then $\mathcal{A}$ synchronizes with probability $1 - \Theta((2^{k-1} - 1)n^{-2(k-1)})$ for arbitrary $k \geq 2$.

Since the sequence of circular automata C_n depicted in Fig. 1 is the only known infinite series of synchronizing automata reaching Černỳ's bound $(n-1)^2$, one might suspect that the class of circular automata is somehow difficult to synchronize. However, as we show in the present paper, it turns out that a random circular automaton is synchronizing with high probability.

The rest of the paper is organized as follows: in Section 2 we present the main result together with its proof and the statement of the two key lemmas for the proof. In Section 3 we study the dependence structure among the entries of the random matrix used in the proof of the main result; the result obtained in this section is crucial for the proof of the key lemmas. In Section 4 we prove the first lemma while in Section 5 we prove the second one. In Section 6 we present some interesting connections between synchronization of circular automata and chromatic polynomials of circulant graphs. Finally, in Section 7 we present some possible directions towards generalizing and improving the results presented in this paper.

2. Main result

Let n be a positive integer. An automaton $\mathcal{A}(\mathbb{Z}_n, L)$, where $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ is the set of states, is called a *circular automaton* if L contains a permutation that decomposes in exactly one cycle. Let $(i)_n := i \mod n$. Let $\mathcal{M}_n$ denote the set of all mappings from $\mathbb{Z}_n$ to itself, and let $\mathbb{P}$ denote the uniform probability measure on $\mathcal{M}_n$. We will write the elements of $\mathcal{M}_n$ as vectors by identifying the mapping $\mathbf{b}(i) = b_i$, $i = 0, \ldots, n-1$ with the vector $\mathbf{b} = (b_0, \ldots, b_{n-1})$.

In what follows, we denote by $\mathcal{A}_n(\mathbf{b}) := (\mathbb{Z}_n, \{\mathbf{a}, \mathbf{b}\})$ a circular automaton of order $n \in \mathbb{N}$, with $\mathbf{a} : \mathbb{Z}_n \to \mathbb{Z}_n$ being the circular right shift permutation $a(i) = (i+1)_n$ and $\mathbf{b} := (b_0, ..., b_{n-1})$ being an element of $\mathcal{M}_n$. We will understand that $\mathbf{b}$ is "randomly" chosen from $\mathcal{M}_n$ according to the uniform probability measure $\mathbb{P}$, making $\mathcal{A}_n(\mathbf{b})$ a random circular automaton.

It follows from work of Perrin [12] that a circular automaton $\mathcal{A}(Q, L)$ of prime order synchronizes if and only if L contains a non-permutation. Pin [13] proved with combinatorial methods that a circular automaton $\mathcal{A}(Q, L)$ of prime order which has a letter of rank $\frac{n-1}{2} \leq k \leq n$ has a minimal word of size at most $(n-k)^2$. For the probability of synchronization of $\mathcal{A}_p(\mathbf{b})$ a very precise result is known.

Theorem 3 *([12][13]). Let p be a prime number. Then*

$$\mathbb{P}\left[\{\mathbf{b} \in \mathcal{M}_p : \ \mathcal{A}_p(\mathbf{b}) \ synchronizes\}\right] = 1 - \frac{p!}{p^p} = 1 - \Theta\left(\frac{\sqrt{p}}{e^p}\right).$$

Thus, a uniformly distributed random circular automaton of prime order p with $k \geq 2$ letters synchronizes with high probability (w.h.p.).

Theorem 3 is not explicitly stated in [12], but it is observed in [13] that Perrin's work implies the theorem.

It is known that the Černỳ conjecture holds true for the class of circular automata [8]. In a closely related work, Béal, Berlinkov and Perrin [2] gave an $O\left(n^2\right)$ upper bound for the shortest words of synchronizing automata with a single cluster.

A natural question arises: do random circular automata of order n (not necessarily prime) synchronize with high probability? We give a positive answer to this question in the following:

Theorem 4 *(**Main result**). The following holds:*

$$\mathbb{P}\left[\{\mathbf{b} \in \mathcal{M}_n: \ \mathcal{A}_n(\mathbf{b}) \ synchronizes\}\right] = 1 - O\left(\frac{1}{n}\right)$$

as $n \to \infty$. Thus, a randomly chosen $\mathcal{A}_n(\mathbf{b})$ synchronizes w.h.p. as $n \to \infty$.

Remark 5. Theorem 4 does not follow from the results of Berlinkov or Nicaud. In their models, they use a random automaton $\mathcal{A}(Q, L)$ of order n where L is a collection of k mappings from Q to Q i.i.d. uniformly chosen. For a fixed k, the probability of randomly chosen k mappings to contain a permutation with exactly one cycle is bounded from above by $k \cdot \frac{n!}{n^n} \xrightarrow{n \to \infty} 0$.

Given $n \in \mathbb{N}$ and $r \in \mathbb{Z}$, we define the *n-cyclic absolute value* of r to be

$$\left|r\right|_n := \min\left\{(r)_n, (-r)_n\right\} \in \left\{0, 1, \ldots, \left\lfloor\frac{n}{2}\right\rfloor\right\}.$$

When $r, s \in \mathbb{Z}$ then $\left|r - s\right|_n$ is the *n-cyclic distance* between r and s. When the numbers $0, 1, \ldots, n-1$ are identified with the vertices of a cycle of length n, the n-cyclic distance between two such numbers is the length of the shortest path between them in the cycle. We now introduce the main tool for the proof of the main theorem.

Definition. Let $\mathcal{A}_n(\mathbf{b}) := (\mathbb{Z}_n, \{\mathbf{a}, \mathbf{b}\})$ be a circular automaton with $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$. Then we define $T_{\mathbf{b}}$ to be the matrix

$$T_{\mathbf{b}} := \begin{bmatrix} \left|b_0 - b_1\right|_n & \left|b_1 - b_2\right|_n & \cdots & \left|b_k - b_{k+1}\right|_n & \cdots & \left|b_{n-1} - b_0\right|_n \\ \left|b_0 - b_2\right|_n & \left|b_1 - b_3\right|_n & \cdots & \left|b_k - b_{(k+2)_n}\right|_n & \cdots & \left|b_{n-1} - b_1\right|_n \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \left|b_0 - b_i\right|_n & \left|b_1 - b_{1+i}\right|_n & \cdots & \left|b_k - b_{(k+i)_n}\right|_n & \cdots & \left|b_{n-1} - b_{i-1}\right|_n \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \left|b_0 - b_{\lfloor\frac{n}{2}\rfloor}\right|_n & \left|b_1 - b_{1+\lfloor\frac{n}{2}\rfloor}\right|_n & \cdots & \left|b_k - b_{(k+\lfloor\frac{n}{2}\rfloor)_n}\right|_n & \cdots & \left|b_{n-1} - b_{\lfloor\frac{n}{2}\rfloor-1}\right|_n \end{bmatrix}$$

which can be shortly written as

$$T_{\mathbf{b}}(i,j) = \left|b_j - b_{(j+i)_n}\right|_n \text{ for } 1 \leq i \leq \left\lfloor \frac{n}{2} \right\rfloor \text{ and } 0 \leq j \leq n-1.$$

As before, $b_i = \mathbf{b}(i)$, i.e., the image of state i under $\mathbf{b}$. To be clear, note that the first row of $T_{\mathbf{b}}$ is formed of the cyclic distances of the images of states r, s such that $\left|r - s\right|_n = 1$; in general, the i-th row of $T_{\mathbf{b}}$ is formed of the cyclic distances of the images of pairs of states r, s of cyclic distance i. Notice that the columns are counted from 0 to $n-1$.

For $\mathbf{b} \in \mathcal{M}_n$ and $i = 1, \ldots, \left\lfloor \frac{n}{2} \right\rfloor$, let $R_i(\mathbf{b})$ denote the number of different entries in row i of $T_{\mathbf{b}}$:

$$R_i(\mathbf{b}) := \# \left\{ \left|b_0 - b_{(0+i)_n}\right|_n, \left|b_1 - b_{(1+i)_n}\right|_n, \ldots, \left|b_{n-1} - b_{i-1}\right|_n \right\}. \tag{1}$$

Set

$$\mathcal{E}_{\mathrm{row}}(\alpha) := \bigcap_{i=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \left\{ \mathbf{b} \in \mathcal{M}_n : \ R_i(\mathbf{b}) \geq \alpha \left\lfloor \frac{n}{2} \right\rfloor \right\}, \tag{2}$$

i.e., $\mathcal{E}_{\mathrm{row}}(\alpha)$ contains those $\mathbf{b}$ for which every row of $T_{\mathbf{b}}$ has at least $\alpha \left\lfloor \frac{n}{2} \right\rfloor$ different elements. Its complement is

$$\mathcal{E}_{\mathrm{row}}^c(\alpha) := \bigcup_{i=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \left\{ \mathbf{b} \in \mathcal{M}_n : \ R_i(\mathbf{b}) < \alpha \left\lfloor \frac{n}{2} \right\rfloor \right\}. \tag{3}$$

We also define

$$\mathcal{E}_{\mathrm{zero}}(\beta) := \left\{ \mathbf{b} \in \mathcal{M}_n : \ D(\mathbf{b}) \geq \beta \left\lfloor \frac{n}{2} \right\rfloor \right\}, \tag{4}$$

and its complement

$$\mathcal{E}_{\mathrm{zero}}^c(\beta) := \left\{ \mathbf{b} \in \mathcal{M}_n : \ D(\mathbf{b}) < \beta \left\lfloor \frac{n}{2} \right\rfloor \right\}, \tag{5}$$

where

$$D_i(\mathbf{b}) := \begin{cases} 1, & \text{if there exist } k, l \in \mathbb{Z}_n \text{ such that } \left|k - l\right|_n = i \text{ and } \left|b_k - b_l\right|_n = 0, \\ 0, & \text{otherwise}, \end{cases}$$

and

$$D(\mathbf{b}) := \sum_{i=1}^{\left\lfloor \frac{n}{2} \right\rfloor} D_i(\mathbf{b}).$$

That is, $\mathcal{E}_{\mathrm{zero}}(\beta)$ is the set of those $\mathbf{b}$ for which the matrix $T_{\mathbf{b}}$ has at least $\beta \left\lfloor \frac{n}{2} \right\rfloor$ rows containing the entry zero.

The proof of Theorem 4 relies on the following two lemmas.

Lemma 6. *Let $\varepsilon > 0$ and let $\alpha = 1 - e^{-1} - \varepsilon$. Then*

$$\mathbb{P}\left[\mathcal{E}_{\mathrm{row}}^c(\alpha)\right] = O\left(\frac{1}{n}\right)$$

as $n \to \infty$.

Lemma 7. *Let $\varepsilon \in (0,1)$ and let $\beta = \frac{1}{2} - \varepsilon$. Then*

$$\mathbb{P}\left[\mathcal{E}_{\mathrm{zero}}^c(\beta)\right] = O\left(\frac{1}{n}\right),$$

as $n \to \infty$.

Proof of Theorem 4. The main idea of the proof is to transform the question of synchronization of $\mathcal{A}_n(\mathbf{b})$ into a question concerning properties of the matrix $T_{\mathbf{b}}$. The functions $T_{\mathbf{b}}(i,j)$ are random variables over $\mathcal{M}_n$, and to obtain our desired probability estimates we will need to understand the joint stochastic dependence structure of these random variables.

Let $\mathbf{b} \in \mathcal{M}_n$ and consider the associated Matrix $T_{\mathbf{b}}$. The first observation is that a zero in row i of $T_{\mathbf{b}}$ means that two states r, s with cyclic distance i synchronize under $\mathbf{b}$ (i.e., $\mathbf{b}(r) = \mathbf{b}(s)$), which implies that any pair r', s' with cyclic distance i can be synchronized with a word of the form $\mathbf{a}^l \mathbf{b}$ because $\{r', s'\}\mathbf{a}^l = \{r, s\}$ for some l. The second observation is that if the i-th row of $T_{\mathbf{b}}$ contains a number $j = |b_k - b_{(k+i)_n}|_n$ and the j-th row contains a zero, then every pair of states (r, s) with cyclic distance i can be synchronized with a word of the form $\mathbf{a}^{l_1} \mathbf{b} \mathbf{a}^{l_2} \mathbf{b}$. Indeed, we can proceed as follows: $\{r, s\} \overset{\mathbf{a}^{l_1}}{\rightarrow} \{k, (k+i)_n\} \overset{\mathbf{b}}{\rightarrow} \{b_k, b_{(k+i)_n}\}$, where this last pair has n-cyclic distance j; then $\{b_k, b_{(k+i)_n}\}$ synchronizes with a word of the form $\mathbf{a}^{l_2} \mathbf{b}$, for some l_2 because the j-th row contains a zero. With these two observations, we establish sufficient conditions on $T_{\mathbf{b}}$ for the synchronization of $\mathcal{A}_n(\mathbf{b})$. The sets $\mathcal{E}_{\mathrm{row}}(\alpha)$ and $\mathcal{E}_{\mathrm{zero}}(\beta)$ which we defined in (2) and (4) play a crucial role.

Let $\mathbf{b} \in \mathcal{M}_n$. If $\mathbf{b}$ is contained in both $\mathcal{E}_{\mathrm{row}}(\alpha)$ and $\mathcal{E}_{\mathrm{zero}}(\beta)$ for some $\alpha, \beta > 0$ such that $\alpha + \beta > 1$, then $\mathcal{A}_n(\mathbf{b})$ synchronizes. This follows from the two previous observations together with the union bound. Indeed, let (r, s) be any pair of different states and let $i = |r - s|_n$. If row i contains a zero, we can synchronize $\{r, s\}$ with a word of the form $\mathbf{a}^l \mathbf{b}$; otherwise, row i contains an entry $j \neq 0$ such that row j contains a zero (because $\alpha + \beta > 1$), which implies that $\{r, s\}$ can be synchronized with a word of the form $\mathbf{a}^{l_1} \mathbf{b} \mathbf{a}^{l_2} \mathbf{b}$. Therefore, every pair of different states synchronizes and $\mathcal{A}_n(\mathbf{b})$ synchronizes by Claim 1. Therefore, for any $\alpha, \beta > 0$ satisfying $\alpha + \beta > 1$, we have the following bound:

$$\mathbb{P}\left[\{\mathbf{b} \in \mathcal{M}_n : \ \mathcal{A}_n(\mathbf{b}) \text{ synchronizes}\}\right] \geq \mathbb{P}\left[\mathcal{E}_{\text{row}}(\alpha) \cap \mathcal{E}_{\text{zero}}(\beta)\right]$$
$$= 1 - \mathbb{P}\left[\mathcal{E}_{\text{row}}^c(\alpha) \cup \mathcal{E}_{\text{zero}}^c(\beta)\right] \qquad (6)$$
$$\geq 1 - \mathbb{P}\left[\mathcal{E}_{\text{row}}^c(\alpha)\right] - \mathbb{P}\left[\mathcal{E}_{\text{zero}}^c(\beta)\right].$$

Now, by the last inequality and by Lemmas 6 and 7 we obtain the bound stated in the main theorem. We can choose, for example, $\varepsilon' = 0.05$, $\alpha^\star = 1 - e^{-1} - \varepsilon' \approx 0.582$ and $\beta^\star = 0.5 - \varepsilon' = 0.45$, so that $\alpha^\star > 0$, $\beta^\star > 0$ and $\alpha^\star + \beta^\star > 1$. Then we have

$$\mathbb{P}\left[\{\mathbf{b} \in \mathcal{M}_n : \ \mathcal{A}_n(\mathbf{b}) \text{ synchronizes}\}\right] \geq 1 - \underbrace{\mathbb{P}\left[\mathcal{E}_{\text{row}}^c(\alpha^\star)\right]}_{=O\left(\frac{1}{n}\right)} - \underbrace{\mathbb{P}\left[\mathcal{E}_{\text{zero}}^c(\beta^\star)\right]}_{=O\left(\frac{1}{n}\right)} = 1 - O\left(\frac{1}{n}\right)$$

as $n \to \infty$. $\quad\square$

3. Independence among the random variables $T_{\mathbf{b}}(i,j)$

For every pair (i,j), $1 \leq i \leq \left\lfloor \frac{n}{2} \right\rfloor$ and $0 \leq j \leq n-1$, the function $T_{\mathbf{b}}(i,j): \ \mathcal{M}_n \mapsto \mathbb{Z}_n$ is a random variable on the space $\mathcal{M}_n$, equipped with the uniform probability measure $\mathbb{P}$ (and with the power set of $\mathcal{M}_n$ as the natural sigma-field). It is crucial for our proof to give a criterion on pairs of indices $(i_1, j_1), \ldots, (i_k, j_k)$ which guarantees that the random variables $T_{\mathbf{b}}(i_1, j_1)$, $\ldots$, $T_{\mathbf{b}}(i_k, j_k)$ are independent. First, notice that not every subset of random variables $T_{\mathbf{b}}(i,j)$ is independent. For example,

$$T_{\mathbf{b}}(1,0) = \left|b_0 - b_1\right|_n, \quad T_{\mathbf{b}}(1,1) = \left|b_1 - b_2\right|_n, \quad T_{\mathbf{b}}(2,0) = \left|b_0 - b_2\right|_n$$

are clearly dependent: if the first two random variables $T_{\mathbf{b}}(1,0)$ and $T_{\mathbf{b}}(1,1)$ are zero, then $b_0 = b_1 = b_2$, which implies that $\left|b_0 - b_2\right|_n = 0$ and so $T_{\mathbf{b}}(2,0)$ necessarily is also zero. This dependence comes from the fact that there is a "cycle" of the form $b_0 \to b_1 \to b_2 \to b_0$ generated by the indices of these three random variables. Generally, it will turn out that a set of random variables $T_{\mathbf{b}}(i,j)$ is independent if and only if the corresponding indices are "acyclic". We formalize this in the following

Definition. Let

$$S = \{(i_1, j_1), (i_2, j_2), \ldots, (i_k, j_k)\}$$

be a multi-set, where $i_l, j_l \in \mathbb{Z}_n$. The *associated (multi-)graph $G(S)$* is the (multi-)graph with vertex set $\mathbb{Z}_n$ and edge (multi-)set

$$\left\{\{j_1, (j_1 + i_1)_n\}, \{j_2, (j_2 + i_2)_n\}, \ldots, \{j_k, (j_k + i_k)_n\}\right\}.$$

We say that S is acyclic if its associated multi-graph $G(S)$ is acyclic. We also say that the edge $\{j, j + i\}$ is associated to the random variable $T_{\mathbf{b}}(i,j)$.

The relation between acyclic index sets and independent variables is stated in the following

Proposition 8. *The variables* $T_{\mathbf{b}}(i_1, j_1), T_{\mathbf{b}}(i_2, j_2), \ldots, T_{\mathbf{b}}(i_k, j_k)$ *are i.i.d.* $\iff$ *the (multi-)set* $S = \{(i_1, j_1), (i_2, j_2), \ldots, (i_k, j_k)\}$ *is acyclic. Furthermore, if the variables are independent then*

$$\mathbb{P}\left[\bigcap_{w=1}^{k} \{\mathbf{b} \in \mathcal{M}_n : T_{\mathbf{b}}(i_w, j_w) = s_w\}\right] = \frac{\prod_{w=1}^{k} m_{s_w}}{n^k}, \quad \forall k \geq 1, \tag{7}$$

where $s_1, s_2, \ldots, s_k$ *are arbitrary integers and*

$$m_s = \#\{d \in \mathbb{Z}_n : |d|_n = s\} = \begin{cases} 2, & \text{if } 0 < s < \frac{n}{2}; \\ 1, & \text{if } s = 0; \\ 1, & \text{if } s = \frac{n}{2} \text{ and } \frac{n}{2} \in \mathbb{N}; \\ 0, & \text{otherwise}. \end{cases}$$

Henceforth in the paper we use the concepts "acyclic" and "independent" interchangeably when we refer to a multi-set of independent random variable entries of $T_{\mathbf{b}}$, resp. to random variable entries whose associated multi-graph is acyclic.

Remark 9. Note that different random variables $T_{\mathbf{b}}(i, j)$, $T_{\mathbf{b}}(i', j')$ may be associated with the same edge; since $1 \leq i \leq \lfloor \frac{n}{2} \rfloor$ this only happens when n is even and $i = i' = \frac{n}{2}$ and $j \equiv j'$ mod $\frac{n}{2}$. Thus, for n odd, a pair of different random variables $T_{\mathbf{b}}(i, j)$, $T_{\mathbf{b}}(i', j')$ is always acyclic/independent.

Remark 10. For a vector $\mathbf{b} \in \mathcal{M}_n$, we can write its entries $b_0, \ldots, b_{n-1}$ as functions of $\mathbf{b}$. In other words, $b_0 = b_0(\mathbf{b}), \ldots, b_{n-1} = b_{n-1}(\mathbf{b})$ are random variables on $\mathcal{M}_n$, equipped with the uniform measure $\mathbb{P}$. The random variables $b_0, \ldots, b_{n-1}$ are independent and identically distributed over this space; this follows immediately from the fact that the uniform measure on $\mathcal{M}_n$ is a product of n one-dimensional uniform measures.

Proof of Proposition 8. First note that any two random variables $T_{\mathbf{b}}(i, j) = |b_j - b_{(j+i)_n}|_n$ and $T_{\mathbf{b}}(i', j') = |b_{j'} - b_{(j'+i')_n}|_n$ are always identically distributed since $b_0, b_1, \ldots, b_{n-1}$ are i.i.d. (see Remark 10). Note also that for all s

$$\mathbb{P}\left[\{\mathbf{b} \in \mathcal{M}_n : |b_p - b_{p+q}|_n = s\}\right] = \frac{n \cdot m_s}{n^2} = \frac{m_s}{n},$$

which can seen by an easy counting argument: there are n different possible choices of b_p, and then there are m_s independent different choices of $b_{(p+q)_n}$ such that $|b_p - b_{p+q}|_n =$

s. Thus equation (7) is just a rephrasing of the fact that the random variables are independent. Therefore, what we need to prove is that independence holds if and only if the associated (multi-)graph is acyclic.

$\Rightarrow$) (by contraposition) Let $S = \{(i_1, j_1), (i_2, j_2), \ldots, (i_k, j_k)\}$ be a (multi-)set which contains a cycle. Thus, its associated multi-graph $G(S)$ has a cycle C of length $l \geq 2$. Let this cycle be w.l.o.g.

$$j_1 \to (j_1 + i_1)_n = j_2 \to (j_2 + i_2)_n = j_3 \to \ldots \to (j_{l-1} + i_{l-1}) = j_l \to (j_l + i_l)_n = j_1.$$

Recall that $T_{\mathbf{b}}(i, j) = 0 \iff b_j = b_{(j+i)_n}$. Thus if for some $\mathbf{b} \in \mathcal{M}_n$ we have

$$T_{\mathbf{b}}(i_1, j_1) = T_{\mathbf{b}}(i_2, j_2) = \ldots = T_{\mathbf{b}}(i_{l-1}, j_{l-1}) = 0,$$

then $b_{j_1} = b_{j_2} = \ldots = b_{j_l}$, and so we automatically also have $T_{\mathbf{b}}(i_l, j_l) = \left| b_{j_l} - b_{(j_l + i_l)_n} \right|_n = \left| b_{j_l} - b_{j_1} \right|_n = 0$. Thus, the variables $T_{\mathbf{b}}(i_1, j_1), \ldots, T_{\mathbf{b}}(i_\ell, j_\ell)$ are not independent. We conclude that an independent multi-set must be acyclic.

$\Leftarrow$) (by induction on k) Let $k \geq 2$. Assume that the multi-set $S_k = \{(i_1, j_1), (i_2, j_2), \ldots, (i_k, j_k)\}$ is acyclic. We want to show that $T_{\mathbf{b}}(i_k, j_k)$ is independent of $T_{\mathbf{b}}(i_1, j_1), \ldots, T_{\mathbf{b}}(i_{k-1}, j_{k-1})$. This will allow us to factor out the k-th factor on the left-hand side of (7), leading (by induction) to the formula on the right-hand side of (7), which is equivalent to independence.

We distinguish two cases: The first case is when the edge $\{j_k, (j_k + i_k)_n\}$ is a connected component by itself in $G(S)$. This means that the sets $S_1 := \{j_1, (j_1 + i_1)_n, j_2, (j_2 + i_2)_n, \ldots, j_k, (j_{k-1} + i_{k-1})_n\}$ and $S_2 := \{j_k, (j_k + i_k)_n\}$ are disjoint. By construction, the random variables $T_{\mathbf{b}}(i_1, j_1), \ldots, T_{\mathbf{b}}(i_{k-1}, j_{k-1})$ depend only on b_s with $s \in S_1$, while $T_{\mathbf{b}}(i_k, j_k)$ depends only on b_s with $s \in S_2$. Since $b_0, \ldots, b_{n-1}$ are independent by Remark 10, this implies that $T_{\mathbf{b}}(i_k, j_k)$ is independent of $T_{\mathbf{b}}(i_1, j_1), \ldots, T_{\mathbf{b}}(i_{k-1}, j_{k-1})$, as desired.

For the second case, the edge $\{j_k, (j_k + i_k)_n\}$ is not a connected component by itself in $G(S)$. Since it is also not part of a cycle by assumption, we can assume that $(j_k + i_k)_n$ is a leaf vertex in $G(S)$. In principle, $T_{\mathbf{b}}(i_k, j_k)$ depends on b_{j_k} as well as on $b_{(j_k+i_k)_n}$. However, since $T_{\mathbf{b}}(i_k, j_k)$ is defined as a cyclic distance, the conditional distribution of $T_{\mathbf{b}}(i_k, j_k)$ given b_{j_k} is always the same. In formulas, for every s_k we have

$$\mathbb{P}\left[\{\mathbf{b} \in \mathcal{M}_n : T_{\mathbf{b}}(i_k, j_k) = s_k\}\right] = \mathbb{P}\left[\{\mathbf{b} \in \mathcal{M}_n : T_{\mathbf{b}}(i_k, j_k) = s_k \text{ and } b_{j_k} = r\}\right] \quad (8)$$

for every $r \in \{0, \ldots, n-1\}$. This fact can be simply established by counting the possible configurations of b_{j_k} and $b_{(j_k+i_k)_n}$. By definition, $T_{\mathbf{b}}(i_k, j_k)$ is independent of all b_ℓ with $\ell \neq j_k, (j_k + i_k)_n$. Thus for every numbers $s_1, \ldots, s_k$ we have, using the independence of $b_0, \ldots, b_{n-1}$ and (8), that

$$\mathbb{P}\left[\bigcap_{w=1}^{k}\{\mathbf{b}:\ T_{\mathbf{b}}(i_w, j_w) = s_w\}\right]$$

$$=\sum_{r=0}^{n-1}\mathbb{P}\left[\bigcap_{w=1}^{k}\{\mathbf{b}:\ T_{\mathbf{b}}(i_w, j_w) = s_w \text{ and } b_{j_k} = r\}\right]$$

$$=\sum_{r=0}^{n-1}\mathbb{P}\left[\underbrace{\left(\bigcap_{w=1}^{k-1}\{\mathbf{b}:\ T_{\mathbf{b}}(i_w, j_w) = s_w \text{ and } b_{j_k} = r\}\right)}_{\text{depends only on } b_\ell \text{ with } \ell \neq j_k,\ (j_k + i_k)_n \text{ when } b_{j_k} \text{ is fixed}}\right.$$

$$\left. \cap \underbrace{\{\mathbf{b}:\ T_{\mathbf{b}}(i_k, j_k) = s_k \text{ and } b_{j_k} = r\}}_{\text{depends only on } b_{(j_k + i_k)_n} \text{ when } b_{j_k} \text{ is fixed}}\right]$$

$$=\sum_{r=0}^{n-1}\left(\mathbb{P}\left[\left(\bigcap_{w=1}^{k-1}\{\mathbf{b}:\ T_{\mathbf{b}}(i_w, j_w) = s_w \text{ and } b_{j_k} = r\}\right)\right]\right.$$

$$\left. \times\ \mathbb{P}\left[\{\mathbf{b}:\ T_{\mathbf{b}}(i_k, j_k) = s_k \text{ and } b_{j_k} = r\}\right]\right)$$

$$=\sum_{r=0}^{n-1}\left(\mathbb{P}\left[\left(\bigcap_{w=1}^{k-1}\{\mathbf{b}:\ T_{\mathbf{b}}(i_w, j_w) = s_w \text{ and } b_{j_k} = r\}\right)\right]\mathbb{P}\left[\{\mathbf{b}:\ T_{\mathbf{b}}(i_k, j_k) = s_k\}\right]\right)$$

$$=\mathbb{P}\left[\left(\bigcap_{w=1}^{k-1}\{\mathbf{b}:\ T_{\mathbf{b}}(i_w, j_w) = s_w\}\right)\right]\mathbb{P}\left[\{\mathbf{b}:\ T_{\mathbf{b}}(i_k, j_k) = s_k\}\right].$$

This is exactly the independence property that we wanted to establish. □

4. Proof of Lemma 6

The overview of the proof is as follows. Recall that we understand the entries of the matrix $T_{\mathbf{b}}$ as random variables. We will prove that every row of $T_{\mathbf{b}}$ contains a "large" number of independent random variables. Then we give a lower bound for the expected value of the number of different elements in each row. Then we apply McDiarmid's inequality to each row and finally we use the union bound together with the exponential decay delivered by McDiarmid's inequality to guarantee that w.h.p. every row of $T_{\mathbf{b}}$ has at least $\sim (1 - e^{-1})\left\lfloor\frac{n}{2}\right\rfloor$ different elements. We denote by $C_n(i)$ the *circulant graph* on n vertices, i.e., the graph with vertex set $\mathbb{Z}_n$ where two vertices r, s are adjacent if and only if $\left|r - s\right|_n = i$.

We need the following property.

Claim 11. *For every i, the i-th row of $T_{\mathbf{b}}$ contains a set of at least $n - \gcd(n, i)$ random variables which are i.i.d.*

Proof. The variables in row i are given by the multi-set

$$E_i(\mathbf{b}) := \{\big|b_0 - b_i\big|_n, \ldots, \big|b_k - b_{(k+i)_n}\big|_n, \ldots, \big|b_{n-1} - b_{i-1}\big|_n\}. \tag{9}$$

Let $i \neq \frac{n}{2}$. By Remark 9, the corresponding multi-set $E_i(\mathbf{b})$ does not have repeated elements and the associated multi-graph $G(E_i(\mathbf{b}))$ is isomorphic to the circulant graph $C_n(i)$. It is well known and easy to show that $C_n(i)$ is a disjoint union of $\gcd(n, i)$ cycles of length $\frac{n}{\gcd(n, i)}$ [5]. We can then obtain an acyclic set of variables by removing one edge from each of the cycles of $G(S_i)$. The resulting set of variables is i.i.d. by Proposition 8. In the case $i = \frac{n}{2}$, the first $\frac{n}{2}$ variables in row $\frac{n}{2}$

$$E_{\frac{n}{2}}(\mathbf{b}) = \{\big|b_0 - b_{\frac{n}{2}}\big|_n, \ldots, \big|b_k - b_{(k+\frac{n}{2})_n}\big|_n, \ldots, \big|b_{\frac{n}{2}-1} - b_{n-1}\big|_n\}$$

have an associated multi-graph that is isomorphic to the circulant graph $C_n(\frac{n}{2})$, which is a disjoint union of $\frac{n}{2} = \gcd(n, \frac{n}{2})$ edges. This last graph is acyclic, thus the variables are i.i.d. by Proposition 8. $\square$

We prove the following lower bound

Claim 12. *We have $\mathbb{E}[R_i] \geq \lfloor \frac{n}{2} \rfloor (1 - e^{-1}) - 1$, where for all $\mathbf{b} \in \mathcal{M}_n$*

$$R_i(\mathbf{b}) = \#\{\big|b_0 - b_{(0+i)_n}\big|_n, \ldots, \big|b_k - b_{(k+i)_n}\big|_n, \ldots, \big|b_{n-1} - b_{i-1}\big|_n\}$$

(see (1)) is the cardinality of different elements in row i of $T_{\mathbf{b}}$.

Proof. First, for every $d \in \{0, \ldots, \lfloor \frac{n}{2} \rfloor\}$, we define the random variables

$$\delta_j^{(i)}(\mathbf{b}, d) := 1 - \mathbb{1}\{\big|b_j - b_{(j+i)_n}\big|_n = d\} = \begin{cases} 0, & \text{if } \big|b_j - b_{(j+i)_n}\big|_n = d; \\ 1, & \text{otherwise}, \end{cases}$$

and

$$r_d^{(i)}(\mathbf{b}) := \prod_{j \in \mathbb{Z}_n} \delta_j^{(i)}(\mathbf{b}, d) = \begin{cases} 0 & \text{if } \exists p, q \in \mathbb{Z}_n \text{ such that } \big|p, q\big|_n = i \text{ and } \big|b_p, b_q\big|_n = d; \\ 1, & \text{otherwise}. \end{cases}$$

Note that $r_d^{(i)}(\mathbf{b})$ is zero if the number d is included in the i-th row of $T_{\mathbf{b}}$, and that it is one otherwise. Recalling that the entries of $T_{\mathbf{b}}$ can only have values in $\{0, 1, \ldots, \lfloor \frac{n}{2} \rfloor\}$, we write the number of distinct elements in row i as

$$R_i(\mathbf{b}) = \left(\left\lfloor \frac{n}{2} \right\rfloor + 1 \right) - \sum_{d=0}^{\lfloor \frac{n}{2} \rfloor} r_d^{(i)}(\mathbf{b}). \tag{10}$$

By Claim 11, there is a subset I of $\mathbb{Z}_n$ of cardinality $n - \gcd(n, i)$ such that the variables $\{\delta_w^{(i)} : w \in I\}$ are i.i.d., and thus

$$\mathbb{E}\left[r_d^{(i)} \right] = \mathbb{E}\left[\prod_{j \in \mathbb{Z}_n} \delta_j^{(i)}(\mathbf{b}, d) \right] \le \mathbb{E}\left[\prod_{w \in I} \delta_w^{(i)}(\mathbf{b}, d) \right] = \mathbb{E}\left[\delta_0^{(i)}(\mathbf{b}, d) \right]^{n - \gcd(n, i)}.$$

Furthermore, by Proposition 8, we have $\mathbb{E}\left[\delta_0^{(i)}(\mathbf{b}, d) \right] = 1 - \frac{m_d}{n}$, and thus

$$\mathbb{E}\left[r_d^{(i)} \right] \le \left(1 - \frac{m_d}{n} \right)^{n - \gcd(n, i)} \le \left(1 - \frac{m_d}{n} \right)^{\frac{n}{2}} = \begin{cases} \left(1 - \frac{2}{n} \right)^{\frac{n}{2}}, & \text{if } d \neq 0, \frac{n}{2}; \\ \left(1 - \frac{1}{n} \right)^{\frac{n}{2}}, & \text{otherwise}, \end{cases}$$

for $d \in \{0, 1, \ldots, \lfloor \frac{n}{2} \rfloor\}$. Using the inequality $1 - x \le e^{-x}$, which is valid for any real number x, we obtain

$$\mathbb{E}\left[\sum_{d=0}^{\lfloor \frac{n}{2} \rfloor} r_d^{(i)} \right] \le \left\lfloor \frac{n}{2} \right\rfloor \underbrace{\left(1 - \frac{2}{n} \right)^{\frac{n}{2}}}_{\le e^{-1}} + 2 \underbrace{\left(1 - \frac{1}{n} \right)^{\frac{n}{2}}}_{\le e^{-\frac{1}{2}}} \le \left\lfloor \frac{n}{2} \right\rfloor e^{-1} + 2.$$

Plugging this inequality into (10) yields

$$\mathbb{E}\left[R_i \right] = \left(\left\lfloor \frac{n}{2} \right\rfloor + 1 \right) - \mathbb{E}\left[\sum_{d=0}^{\lfloor \frac{n}{2} \rfloor} r_d^{(i)} \right] \ge \left\lfloor \frac{n}{2} \right\rfloor (1 - e^{-1}) - 1.$$

This proves Claim 12. $\square$

We introduce McDiarmid's inequality to prove Claim 14.

Definition. Let $L : (\mathbb{Z}_n)^n \to \mathbb{R}$ be a function. We say that L has *Lipschitz coefficient* $r \in \mathbb{R}^+$ if

$$|L(\overrightarrow{v}) - L(\overrightarrow{w})| \le r$$

for every $\overrightarrow{v}, \overrightarrow{w} \in (\mathbb{Z}_n)^n$ such that $\overrightarrow{v}(j) = \overrightarrow{w}(j)$ for all j except for at most one index.

Proposition 13 *(McDiarmid's Inequality [10]).* *Let $\bar{X} := (X_1, X_2, \ldots, X_n) \in (\mathbb{Z}_n)^n$ be a random vector, where the variables $X_1, X_2, \ldots, X_n$ are independent, and let $L : (\mathbb{Z}_n)^n \to \mathbb{R}$ be a function with bounded Lipschitz coefficient r. Then*

$$\text{(lower tail)} \qquad \mathbb{P}\left[L(\bar{X}) \leq \mathbb{E}\left[L(\bar{X})\right] - r\sqrt{\lambda n}\right] \leq e^{-2\lambda},$$

for all $\lambda \geq 0$.

Remark. This is just a special case of the general form of McDiarmid's inequality. The general inequality also bounds the upper tail, and allows different Lipschitz coefficients in the respective components.

In the following claim we use Proposition 13 to estimate the probability that row i of $T_{\mathbf{b}}$ has less than $\sim (1 - e^{-1})\left\lfloor\frac{n}{2}\right\rfloor$ different elements.

Claim 14. *Let $\varepsilon > 0$. Then*

$$\mathbb{P}\left[\mathbf{b} \in \mathcal{M}_n : \ R_i(\mathbf{b}) < \left\lfloor\frac{n}{2}\right\rfloor\left(1 - e^{-1} - \varepsilon\right)\right] \leq e^{-\Theta(n)},$$

for $i = 1, 2, \ldots, \left\lfloor\frac{n}{2}\right\rfloor$.

Proof. Let $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$. Let $E_i(\mathbf{b})$ be defined as in (9). The function $R_i(\mathbf{b}) := \#E_i(\mathbf{b})$ has Lipschitz coefficient 2: changing one b_j affects at most two entries, namely $\left|b_j - b_{(j+i)_n}\right|_n$ and $\left|b_{(j-i)_n} - b_j\right|_n$. Using McDiarmid's inequality, we deduce that

$$\mathbb{P}\left[\mathbf{b} \in \mathcal{M}_n : \ R_i(\mathbf{b}) \leq \mathbb{E}\left[R_i\right] - 2\sqrt{\lambda n}\right] \leq e^{-2\lambda}, \quad \forall \lambda \geq 0.$$

Using the lower bound $\mathbb{E}\left[R_i\right] \geq \left\lfloor\frac{n}{2}\right\rfloor\left(1 - e^{-1}\right) - 1$ of Claim 12 we obtain

$$\mathbb{P}\left[\mathbf{b} \in \mathcal{M}_n : \ R_i(\mathbf{b}) < \left(\left\lfloor\frac{n}{2}\right\rfloor\left(1 - e^{-1}\right) - 1\right) - 2\sqrt{\lambda n}\right]$$

$$\leq \mathbb{P}\left[\mathbf{b} \in \mathcal{M}_n : \ R_i(\mathbf{b}) \leq \mathbb{E}\left[R_i\right] - 2\sqrt{\lambda n}\right]$$

$$\leq e^{-2\lambda}, \quad \forall \lambda \geq 0.$$

Let $\varepsilon > 0$ and let

$$\lambda_\varepsilon(n) := \frac{1}{4n}\left(\varepsilon\left\lfloor\frac{n}{2}\right\rfloor - 1\right)^2 = \Theta(n); \tag{11}$$

we observe that $\lambda_\varepsilon(n)$ is independent of i. Let $n > \frac{2}{\varepsilon}$, then plugging $\lambda = \lambda_\varepsilon(n)$ into the previous inequality yields

$$\mathbb{P}\left[\mathbf{b} \in \mathcal{M}_n : \ R_i(\mathbf{b}) < \left\lfloor\frac{n}{2}\right\rfloor\left(1 - e^{-1} - \varepsilon\right)\right] \leq e^{-2\lambda_\varepsilon(n)} = e^{-\Theta(n)}. \quad \square \tag{12}$$

Recall that $\mathcal{E}_{\text{row}}(\alpha)$ contains those $\mathbf{b} \in \mathcal{M}_n$ for which every row of $T_{\mathbf{b}}$ has at least $\alpha\left\lfloor\frac{n}{2}\right\rfloor$ different elements, so that

$$\mathcal{E}_{\text{row}}^c(\alpha) = \bigcup_{i=0}^{\lfloor \frac{n}{2} \rfloor} \left\{ \mathbf{b} \in \mathcal{M}_n : \ R_i(\mathbf{b}) < \alpha \left\lfloor \frac{n}{2} \right\rfloor \right\}.$$

Let $\varepsilon > 0$ be arbitrary and let $\alpha^* = 1 - e^{-1} - \varepsilon$. Then

$$\mathbb{P}\left[\mathcal{E}_{\text{row}}^c(\alpha^\star)\right] = \mathbb{P}\left[\bigcup_{i=1}^{\lfloor \frac{n}{2} \rfloor} \left\{ \mathbf{b} \in \mathcal{M}_n : \ R_i(\mathbf{b}) < \alpha^\star \left\lfloor \frac{n}{2} \right\rfloor \right\}\right]$$

$$\leq \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \mathbb{P}\left[\mathbf{b} \in \mathcal{M}_n : \ R_i(\mathbf{b}) < \alpha^\star \left\lfloor \frac{n}{2} \right\rfloor\right]$$

$$\leq ne^{-\Theta(n)}, \tag{13}$$

where we use Claim 14 for the second inequality. The proof of Lemma 6 then follows by noticing that

$$ne^{-\Theta(n)} = O\left(\frac{1}{n}\right).$$

5. Proof of Lemma 7

The overview of the proof is as follows. We will define two random variables $\mathcal{Z}_0(\mathbf{b})$ and $\mathcal{Z}_1(\mathbf{b})$ such that

- $D(\mathbf{b}) \geq \mathcal{Z}_0(\mathbf{b}) - \mathcal{Z}_1(\mathbf{b}), \quad \forall \mathbf{b} : \mathbb{Z}_n \to \mathbb{Z}_n;$
- $\mathbb{E}\left[\mathcal{Z}_0 - \mathcal{Z}_1\right] \sim \dfrac{n}{2}.$

Then we will show that $\mathcal{Z}_0$ and $\mathcal{Z}_1$ concentrate around their respective means, and use this fact to give an upper bound on the probability that D is small. For this purpose, we note the following property.

Claim 15. *Let $\mathcal{Z}_0, \mathcal{Z}_1$ and D be random variables which take non-negative values, such that $D \geq \mathcal{Z}_0 - \mathcal{Z}_1$. Let $\nu > 0$ and let $\delta \leq \mathbb{E}\left[\mathcal{Z}_0 - \mathcal{Z}_1\right] - 2\nu$. Then*

$$\mathbb{P}\left[D < \delta\right] \leq \mathbb{P}\left[\mathcal{Z}_0 < \mathbb{E}\left[\mathcal{Z}_0\right] - \nu\right] + \mathbb{P}\left[\mathcal{Z}_1 > \mathbb{E}\left[\mathcal{Z}_1\right] + \nu\right].$$

Proof. This follows easily from the assumption that $\mathcal{Z}_0 - \mathcal{Z}_1 \leq D$ and the union bound. $\quad\square$

To prove concentration of $\mathcal{Z}_0$ and $\mathcal{Z}_1$ around their respective means, we use Chebyshev's inequality. Notice that $D : \mathbb{Z}_n^n \to \mathbb{Z}_n$ does not have a bounded Lipschitz coefficient, so we cannot use McDiarmid's inequality to guarantee its concentration.

5.1. Lower bound for $D(b)$

Recall that $D(\mathbf{b})$ counts the number of rows of $T_{\mathbf{b}}$ that contain at least one zero. Let

$$z_i = z_i(\mathbf{b}) := \#(\text{Zeros in row } i \text{ of } T_{\mathbf{b}})$$

and

$$\mathcal{Z}_0(\mathbf{b}) := \#(\text{Zeros in } T_{\mathbf{b}}) = \sum_{(i,j) \in [1,\lfloor \frac{n}{2} \rfloor] \times [0, n-1]} \mathbb{1}\{T_{\mathbf{b}}(i,j) = 0\}.$$

Then

$$D(\mathbf{b}) = \mathcal{Z}_0(\mathbf{b}) - \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \max(z_i - 1, 0). \tag{14}$$

It is easy to verify that the number of non-ordered pairs of entries in the i-th row with zero value is

$$\sum_{0 \le j < j' \le n-1} \mathbb{1}\{T_{\mathbf{b}}(i,j) = 0\} \mathbb{1}\{T_{\mathbf{b}}(i,j') = 0\} = \frac{z_i(z_i - 1)}{2} \ge \max(z_i - 1, 0), \quad \forall i,$$

therefore

$$\mathcal{Z}_1(\mathbf{b}) := \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{0 \le j < j' \le n-1} \mathbb{1}\{T_{\mathbf{b}}(i,j) = 0\} \mathbb{1}\{T_{\mathbf{b}}(i,j') = 0\} \ge \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \max(z_i - 1, 0).$$

From this and (14), we conclude that

Claim 16. $D(\mathbf{b}) \ge \mathcal{Z}_0(\mathbf{b}) - \mathcal{Z}_1(\mathbf{b}), \quad \forall \mathbf{b} : \mathbb{Z}_n \to \mathbb{Z}_n.$

5.2. Estimates for $\mathbb{E}[\mathcal{Z}_0]$, $\mathbb{E}[\mathcal{Z}_1]$, $\mathbb{E}[\mathcal{Z}_0 - \mathcal{Z}_1]$, $\mathbb{V}[\mathcal{Z}_0]$, $\mathbb{V}[\mathcal{Z}_1]$

In this subsection we prove that

- $\mathbb{E}[\mathcal{Z}_0 - \mathcal{Z}_1] \sim \frac{n}{2}$,
- $\mathbb{E}[\mathcal{Z}_0] = \Theta(n)$,
- $\mathbb{E}[\mathcal{Z}_1] = \Theta(n)$,
- $\mathbb{V}[\mathcal{Z}_0] = O(n)$, and
- $\mathbb{V}[\mathcal{Z}_1] = O(n)$.

For the rest of this subsection, we use the notation

$$y_{i,j} = y_{i,j}(\mathbf{b}) := \mathbb{1}\{T_{\mathbf{b}}(i,j) = 0\},$$

for $1 \leq i \leq \left\lfloor \frac{n}{2} \right\rfloor$ and $0 \leq j \leq n-1$.

Definition. The variables $y_{i_1,j_1}, y_{i_2,j_2} \ldots, y_{i_k,j_k}$ are called *acyclic* if the multi-set $\bigcup_{w=1}^{k} \{(i_w, j_w)\}$ is acyclic. Let

$$G\left(\{y_{i_1,j_1}, y_{i_2,j_2} \ldots, y_{i_k,j_k}\}\right) = G\left(\bigcup_{w=1}^{k} \{(i_w, j_w)\}\right)$$

be the *associated multi-graph* of the multi-set $\{y_{i_1,j_1}, y_{i_2,j_2} \ldots, y_{i_k,j_k}\}$ and let $e(y_{i,j}) := \{j, (j+i)_n\}$ be the *associated edge* to $y_{i,j}$. The *length* of $e(y_{i,j})$ is $\left|j - (j+i)_n\right|_n = i$.

Remark 17. If the variables $y_{i_1,j_1}, y_{i_2,j_2} \ldots, y_{i_k,j_k}$ are acyclic then they are i.i.d.; this is an immediate consequence of Proposition 8.

We begin with the easy part: the bounds for the expected values.

Claim 18. *Let $n \in \mathbb{N}$. We have $\mathbb{E}\left[\mathcal{Z}_0\right] = \Theta(n)$, $\mathbb{E}\left[\mathcal{Z}_1\right] = \Theta(n)$, and $\mathbb{E}\left[\mathcal{Z}_0 - \mathcal{Z}_1\right] \geq \frac{1}{2}\left\lfloor \frac{n}{2} \right\rfloor - 1$.*

Proof. Using the linearity of the expectation, we get that

$$\mathbb{E}\left[\mathcal{Z}_0\right] = \sum_{(i,j)\in[1,\lfloor \frac{n}{2}\rfloor]\times[0,n-1]} \mathbb{E}\left[y_{i,j}\right] = \left\lfloor \frac{n}{2} \right\rfloor n \frac{1}{n} = \left\lfloor \frac{n}{2} \right\rfloor = \Theta(n), \tag{15}$$

where for the second equality we use that

$$\mathbb{E}\left[y_{i,j}\right] = \mathbb{P}\left[\{\mathbf{b}: \ T_{\mathbf{b}}(i,j) = 0\}\right] = \mathbb{P}\left[\{\mathbf{b}: \ b_j = b_{(j+i)}\}\right] = \frac{1}{n}. \tag{16}$$

Now we calculate an upper bound for $\mathbb{E}\left[\mathcal{Z}_1\right]$, depending on the parity of n.

Case 1: n odd. Every product $y_{i,j}y_{i,j'}$ in the sum

$$\mathcal{Z}_1 = \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{0 \leq j < j' \leq n-1} y_{i,j}y_{i,j'}$$

is formed of independent random variables $y_{i,j}$, $y_{i,j'}$ by Remarks 9, 17. Thus

$$\mathbb{E}\left[\mathcal{Z}_1\right] = \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{0 \leq j < j' \leq n-1} \mathbb{E}\left[y_{i,j}y_{i,j'}\right] = \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \sum_{0 \leq j < j' \leq n-1} \mathbb{E}\left[y_{i,j}\right] \mathbb{E}\left[y_{i,j'}\right]$$

$$\overset{(16)}{=} \left\lfloor \frac{n}{2} \right\rfloor \binom{n}{2} \frac{1}{n^2}$$

$$= \frac{1}{2} \underbrace{\left\lfloor \frac{n}{2} \right\rfloor \left(1 - \frac{1}{n} \right)}_{\leq \frac{1}{2} \lfloor \frac{n}{2} \rfloor} = \Theta(n).$$

Case 2: n even. Using Remark 9, we write $\mathcal{Z}_1$ as

$$\mathcal{Z}_1 = \sum_{\substack{1 \leq i < \frac{n}{2} \\ 0 \leq j < j' \leq n-1}} y_{i,j} y_{i,j'} + \sum_{\substack{0 \leq r < r' \leq n-1 \\ r \not\equiv r' \pmod{n/2}}} y_{n/2,r} y_{n/2,r'} + \sum_{s=0}^{\frac{n}{2}-1} y_{n/2,s}.$$

Every product $y_{i,j} y_{i,j'}$ in the first sum is formed of independent variables $y_{i,j}$, $y_{i,j'}$ by Remark 9 and the same is valid for the products $y_{\frac{n}{2},r} y_{\frac{n}{2},r'}$ in the second sum, therefore

$$\mathbb{E}\left[\mathcal{Z}_1\right] = \sum_{i=1}^{\frac{n}{2}-1} \sum_{0 \leq j < j' \leq n-1} \mathbb{E}\left[y_{i,j}\right] \mathbb{E}\left[y_{i,j'}\right] + \sum_{\substack{0 \leq r < r' \leq n-1 \\ r \not\equiv r' \pmod{n/2}}} \mathbb{E}\left[y_{n/2,r}\right] \mathbb{E}\left[y_{n/2,r'}\right]$$

$$+ \sum_{s=0}^{\frac{n}{2}-1} \mathbb{E}\left[y_{n/2,s}\right]$$

$$= \sum_{i=1}^{\frac{n}{2}-1} \sum_{0 \leq j < j' \leq n-1} \frac{1}{n^2} + \sum_{\substack{0 \leq r < r' \leq n-1 \\ r \not\equiv r' \pmod{n/2}}} \frac{1}{n^2} + \sum_{s=0}^{\frac{n}{2}-1} \frac{1}{n}$$

$$= \left(\frac{n}{2} - 1 \right) \cdot \binom{n}{2} \cdot \frac{1}{n^2} + \left(\binom{n}{2} - \frac{n}{2} \right) \cdot \frac{1}{n^2} + \frac{n}{2} \cdot \frac{1}{n}$$

$$= \underbrace{\frac{1}{2} \cdot \frac{n}{2} \cdot \left(1 - \frac{1}{n} + \left(\frac{2}{n} - \frac{2}{n^2} \right) \right)}_{\leq \frac{1}{2} \cdot \frac{n}{2} + 1} = \Theta(n).$$

We deduce from the previous cases that $\mathbb{E}\left[\mathcal{Z}_1\right] = \Theta(n)$ and $\mathbb{E}\left[\mathcal{Z}_1\right] \leq \frac{1}{2} \left\lfloor \frac{n}{2} \right\rfloor + 1$ for all n. Using this last inequality and (15), we conclude that

$$\mathbb{E}\left[\mathcal{Z}_0\right] - \mathbb{E}\left[\mathcal{Z}_1\right] = \left\lfloor \frac{n}{2} \right\rfloor - \mathbb{E}\left[\mathcal{Z}_1\right] \geq \frac{1}{2} \left\lfloor \frac{n}{2} \right\rfloor - 1.$$

This concludes the proof of Claim 18.   □

Now we estimate the variance of $\mathcal{Z}_0$ and $\mathcal{Z}_1$.

Claim 19. *Let $n \in \mathbb{N}$, then $\mathbb{V}\left[\mathcal{Z}_0\right] = O(n)$ and $\mathbb{V}\left[\mathcal{Z}_1\right] = O(n)$.*

Proof. Here we also divide the calculations according to the parity of n.

Case 1: n odd. We expand the variance of $\mathcal{Z}_0$ to get that

$$\mathbb{V}\left[\mathcal{Z}_0\right] = \sum_{\substack{1 \leq i \leq \lfloor \frac{n}{2} \rfloor \\ 0 \leq j \leq n-1}} \mathbb{V}\left[y_{i,j}\right] + \sum_{\substack{1 \leq i,i' \leq \lfloor \frac{n}{2} \rfloor \\ 0 \leq j,j' \leq n-1 \\ (i,j) \neq (i',j')}} \mathrm{Cov}\left[y_{i,j}, y_{i',j'}\right],$$

where the covariances are calculated among pairs of independent variables $y_{i,j}, y_{i',j'}$ due to Remark 9. Thus

$$\mathbb{V}\left[\mathcal{Z}_0\right] = \sum_{\substack{1 \leq i \leq \lfloor \frac{n}{2} \rfloor \\ 0 \leq j \leq n-1}} \mathbb{V}\left[y_{i,j}\right].$$

We notice that $y_{i,j}^2 = y_{i,j}$ because $y_{i,j} \in \{0,1\}$, therefore

$$\mathbb{V}\left[y_{i,j}\right] = \mathbb{E}\left[y_{i,j}^2\right] - \mathbb{E}\left[y_{i,j}\right]^2 = \frac{1}{n} - \frac{1}{n^2}, \quad \forall n \in \mathbb{N}, \tag{17}$$

where we use (16) in the last equality. Then, for all n odd, we get that

$$\mathbb{V}\left[\mathcal{Z}_0\right] = \left\lfloor \frac{n}{2} \right\rfloor n \left(\frac{1}{n} - \frac{1}{n^2} \right) = \left\lfloor \frac{n}{2} \right\rfloor \left(1 - \frac{1}{n} \right) = O(n). \tag{18}$$

Now we calculate

$$\mathbb{V}\left[\mathcal{Z}_1\right] = \sum_{\substack{1 \leq i \leq \lfloor \frac{n}{2} \rfloor \\ 0 \leq j < j' \leq n-1}} \mathbb{V}\left[y_{i,j}y_{i,j'}\right] + \sum_{\substack{1 \leq i,r \leq \lfloor \frac{n}{2} \rfloor \\ 0 \leq j,j',s,s' \leq n-1 \\ j < j'; \, s < s' \\ (i,j,j') \neq (r,s,s')}} \mathrm{Cov}\left[y_{i,j}y_{i,j'}, y_{r,s}y_{r,s'}\right]; \tag{19}$$

We first note that

$$\mathbb{V}\left[y_{i,j}y_{i,j'}\right] = \mathbb{E}\left[y_{i,j}^2 y_{i,j'}^2\right] - \mathbb{E}\left[y_{i,j}y_{i,j'}\right]^2 = \frac{1}{n^2} - \frac{1}{n^4}, \quad \text{for } n \text{ odd and } \forall i \text{ and } j \neq j'; \tag{20}$$

this follows since the variables $y_{i,j}$ and $y_{i,j'}$ are different and therefore independent (see Remark 9). Thus

$$\sum_{\substack{1 \leq i \leq \lfloor \frac{n}{2} \rfloor \\ 0 \leq j < j' \leq n-1}} \mathbb{V}\left[y_{i,j}y_{i,j'}\right] = \left\lfloor \frac{n}{2} \right\rfloor \binom{n}{2} \frac{1}{n^2} \left(1 - \frac{1}{n^2} \right) = O(n). \tag{21}$$

For the sum of the covariances, we proceed as follows: if the variables $y_{i,j}, y_{i,j'}, y_{r,s}, y_{r,s'}$ are acyclic then they are independent (see Proposition 8), therefore

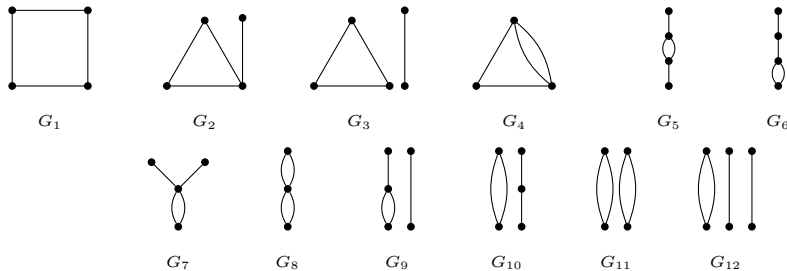$$\mathrm{Cov}\left[y_{i,j}y_{i,j'}, y_{r,s}y_{r,s'}\right] = 0.$$

Fig. 2. Possible non-acyclic multi-graphs for n odd.

On the other hand, if the variables $y_{i,j}, y_{i,j'}, y_{r,s}, y_{r,s'}$ are not acyclic, let

$$\mathcal{Y} := \{\{y_{i,j}, y_{i,j'}, y_{r,s}, y_{r,s'}\} : (i,j,j') \neq (r,s,s'), \, j < j', \, s < s'\},$$

and let

$$Y = \{y_{i,j}, y_{i,j'}, y_{r,s}, y_{r,s'}\} \in \mathcal{Y}.$$

Then $G(Y)$ is a multi-graph with four edges $e(y_{i,j}), e(y_{i,j'}), e(y_{r,s}), e(y_{r,s'})$ such that $e(y_{i,j}) \neq e(y_{i,j'})$ and $e(y_{r,s}) \neq e(y_{r,s'})$ (see Remark 9). In particular, there cannot be 3 equal edges. If $G(Y)$ has at least one cycle, it is isomorphic to one of the multi-graphs in Fig. 2.

We will now estimate the contribution of each of these possible non-acyclic multi-graphs.

Claim 20. *Let $n \in \mathbb{N}$, then*

$$\#\{Y \in \mathcal{Y} : G(Y) \cong G_c\} = \begin{cases} O(n^4), & \text{if } c = 1, 2, 3, 5, 6, 7, 12; \\ O(n^3), & \text{if } c = 4, 8, 9, 10, 11. \end{cases}$$

Proof. The cases $c = 1, 2, 5, 6, 7$ can be bounded by the trivial bound $O(n^4)$, and the same for the cases $c = 4, 8$ with the bound $O(n^3)$. The remaining cases $c = 3, 9, 10, 11, 12$ require better estimates than their respective trivial bounds.

First, notice that for all cases, the four edges of the multi-graph $G(\{y_{i,j}, y_{i,j'}, y_{r,s}, y_{r,s'}\})$ are divided into two pairs: $e(y_{i,j}), e(y_{i,j'})$ of length i and $e(y_{r,s}), e(y_{r,s'})$ of length r. The case G_3 is bounded by $\binom{n}{3} * 2n = O(n^4)$ because three vertices can be chosen freely to form a triangle whose edges have at most two different lengths i, r, then we choose a vertex v for the free edge and finally we choose v' such that $|v - v'|_n = i$ or $|v - v'|_n = r$ depending on the lengths of the edges in the triangle, therefore v' has only two choices.

The case G_{12} is also bounded by $O(n^4)$. To show this, we distinguish between two subcases. In the first subcase, the multi-edge is formed of the associated edges of the same pair, w.l.o.g. $e(y_{i,j}) = e(y_{i,j'})$ (this can only happen in the case n even). Then the free edges are formed of the edges $e(y_{r,s}), e(y_{r,s'})$, which have length r; we choose

two vertices for the multi-edge and two more vertices v_1, v_2 (one for each of the free edges), but then the two missing vertices v'_1, v'_2 have at most two options each, because $\left|v - v_1\right|_n = \left|v_2 - v'_2\right|_n = r$. Thus this subcase is bounded by $O(n^4)$. The second subcase is when $e(y_{i,j}) \neq e(y_{i,j'})$ and $e(y_{r,s}) \neq e(y_{r,s'})$. Then w.l.o.g. the multi-edge is formed of the $e(y_{i,j}) = e(y_{r,s})$ then $i = r$, thus all edges have the same length; we choose two vertices v, v' for the multi-edge and two more vertices v_1, v_2 (one for each of the free edges). The missing vertices v'_1, v'_2 have at most two choices each because $\left|v_1 - v'_1\right|_n = \left|v_2 - v'_2\right|_n = \left|v - v'\right|_n$, which gives again a $O(n^4)$ bound.

For G_9, if we are in the case n odd, then the multi-edge is formed of edges of different groups, w.l.o.g. $e(y_{i,j}) = e(y_{r,s})$ and $i = r$. Therefore the edge attached to the multi-edge is uniquely defined because its length is determined, and the isolated edge is almost uniquely defined once one of the end points is chosen, because the other end has at most two choices. Overall, this gives the $O(n^3)$ bound. In the case n even, it can happen that w.l.o.g. $e(y_{i,j}) = e(y_{i,j'})$ but this can only happen when $i = n/2$. Then the multi-edge is uniquely defined by choosing one end, the isolated edge is defined by choosing two end points, and the last edge has at most four options since its length is already determined by the length of the isolated edge. This gives again a $O(n^3)$ bound.

For G_{10}, in the case n odd we can assume as before $e(y_{i,j}) = e(y_{r,s})$. Then $i = r$, and the multi-edge is determined by choosing two vertices and the remaining two edges are uniquely defined by the central vertex. This yields the bound $O(n^3)$. In the other case, w.l.o.g. $e(y_{i,j}) = e(y_{i,j'})$, and $i = n/2$. The multi-edge can be defined by choosing only one vertex, and the isolated path can be defined by choosing two vertices for one edge, while the remaining edge will have at most two options. This yields again a $O(n^3)$ bound.

For G_{11}, if $e(y_{i,j}) = e(y_{r,s})$, then all edges have the same length $i = r$, we can choose two vertices for the first multi-edge and one vertices for the second multi-edge, while the remaining vertex has at most two options. This yields a $O(n^3)$ bound. In the case when $e(y_{i,j}) = e(y_{i,j'})$ then $e(y_{r,s}) = e(y_{r,s'})$ and $i = r = n/2$. In this case we can choose two vertices (one for each multi-edge), and the remaining two vertices are automatically determined. This yields a $O(n^2) = O(n^3)$ bound. Thus we have established Claim 20. □

We continue with the proof of Claim 19 in the case when n is odd. We observe that

$$\mathbb{E}\left[y_{i,j}y_{i,j'}y_{r,s}y_{r,s'}\right] = \mathbb{P}\left[y_{i,j}y_{i,j'}y_{r,s}y_{r,s'} = 1\right]$$
$$= \mathbb{P}\left[\{\mathbf{b}:\ T_{\mathbf{b}}(i,j) = T_{\mathbf{b}}(i,j') = T_{\mathbf{b}}(r,s) = T_{\mathbf{b}}(r,s') = 0\}\right],$$

and thus for $Y = \{y_{i,j}, y_{i,j'}, y_{r,s}, y_{r,s'}\} \in \mathcal{Y}$, we have that

$$\mathbb{E}\left[y_{i,j}y_{i,j'}y_{r,s}y_{r,s'}\right] = \begin{cases} \frac{1}{n^3}, & \text{if } G(Y) \cong G_{1,2,3,5,6,7,9,10,12}; \\ \frac{1}{n^2}, & \text{if } G(Y) \cong G_{4,8,11}. \end{cases} \tag{22}$$

The last equation, combined with Claim 20, implies that

$$\sum_{\substack{1\leq i,r\leq\lfloor\frac{n}{2}\rfloor\\0\leq j,j',s,s'\leq n-1\\j<j';\,s<s'\\(i,j,j')\neq(r,s,s')}}\text{Cov}\left[y_{i,j}y_{i,j'},y_{r,s}y_{r,s'}\right]\leq\sum_{\substack{1\leq i,r\leq\lfloor\frac{n}{2}\rfloor\\0\leq j,j',s,s'\leq n-1\\j<j';\,s<s'\\(i,j,j')\neq(r,s,s')}}\mathbb{E}\left[y_{i,j}y_{i,j'}y_{r,s}y_{r,s'}\right]$$

$$\leq 7\cdot O(n^4)\frac{1}{n^3}+3\cdot O(n^3)\frac{1}{n^2}+2\cdot O(n^3)\frac{1}{n^3}$$

$$= O(n).$$

Using the previous inequality and (21) we get that

$$\mathbb{V}\left[\mathcal{Z}_1\right]=\sum_{\substack{1\leq i\leq\lfloor\frac{n}{2}\rfloor\\0\leq j<j'\leq n-1}}\mathbb{V}\left[y_{i,j}y_{i,j'}\right]+\sum_{\substack{1\leq i,r\leq\lfloor\frac{n}{2}\rfloor\\0\leq j,j',s,s'\leq n-1\\j<j';\,s<s'\\(i,j,j')\neq(r,s,s')}}\text{Cov}\left[y_{i,j}y_{i,j'},y_{r,s}y_{r,s'}\right]$$

$$= O(n)+O(n)=O(n). \tag{23}$$

This completes the proof of Claim 19 in the case when n is odd.

Case 2: n even. We estimate the variances of $\mathcal{Z}_0$ and $\mathcal{Z}_1$. For n even, we can write $\mathcal{Z}_0$ as

$$\mathcal{Z}_0=\sum_{\substack{1\leq i<\frac{n}{2}\\0<j\leq n-1}}y_{i,j}+2\sum_{j=0}^{\frac{n}{2}-1}y_{\frac{n}{2},j},$$

where all variables involved in the sums are mutually independent (see Remark 9). Thus

$$\mathbb{V}\left[\mathcal{Z}_0\right]=\sum_{\substack{1\leq i<\frac{n}{2}\\0\leq j\leq n-1}}\mathbb{V}\left[y_{i,j}\right]+4\sum_{j=0}^{\frac{n}{2}-1}\mathbb{V}\left[y_{\frac{n}{2},j}\right].$$

Using (16), we deduce that

$$\mathbb{V}\left[\mathcal{Z}_0\right]=\left(\frac{n}{2}-1\right)n\left(\frac{1}{n}-\frac{1}{n^2}\right)+4\frac{n}{2}\left(\frac{1}{n}-\frac{1}{n^2}\right)=O(n), \tag{24}$$

for all n even. By Remark 9, we can write $\mathcal{Z}_1$ as

$$\mathcal{Z}_1=\sum_{\substack{1\leq i\leq\frac{n}{2}\\0\leq j<j'\leq n-1\\j\not\equiv j'\ (\text{mod }n/2)}}y_{i,j}y_{i,j'}+\sum_{s=0}^{\frac{n}{2}-1}y_{n/2,s}.$$

Therefore

$$
\mathbb{V}\left[\mathcal{Z}_1\right] = \sum_{\substack{1 \leq i \leq \frac{n}{2} \\ 0 \leq j < j' \leq n-1 \\ j \not\equiv j' \pmod{n/2}}} \mathbb{V}\left[y_{i,j} y_{i,j'}\right] + \sum_{s=1}^{\frac{n}{2}-1} \mathbb{V}\left[y_{n/2,s}\right]
$$

$$
+ \sum_{\substack{1 \leq i,r \leq \frac{n}{2} \\ 0 \leq j,j',s,s' \leq n-1 \\ j < j'; s < s' \\ j \not\equiv_{\frac{n}{2}} j'; s \not\equiv_{\frac{n}{2}} s' \\ (i,j,j') \neq (r,s,s')}} \mathrm{Cov}\left[y_{i,j} y_{i,j'}, y_{r,s} y_{r,s'}\right]
$$

$$
+ 2 \sum_{\substack{1 \leq u \leq \frac{n}{2} \\ 0 \leq v < v' \leq n-1 \\ v \not\equiv_{\frac{n}{2}} v' \\ 0 \leq w \leq \frac{n}{2}-1}} \mathrm{Cov}\left[y_{u,v} y_{u,v'}, y_{\frac{n}{2},w}\right] + \underbrace{\sum_{\substack{0 \leq w,w' \leq \frac{n}{2}-1 \\ w \neq w'}} \mathrm{Cov}\left[y_{\frac{n}{2},w}, y_{\frac{n}{2},w'}\right]}_{=\,0 \text{ (by Remark 9)}}. \quad (25)
$$

We divide the analysis into three parts: the first two sums, the third sum, and the fourth sum. Using Remark 9, we write the first two sums in (25) as

$$
\sum_{\substack{1 \leq i \leq \frac{n}{2} \\ 0 \leq j < j' \leq n-1 \\ j \not\equiv j' \pmod{n/2}}} \mathbb{V}\left[y_{i,j}\right] \mathbb{V}\left[y_{i,j'}\right] + \sum_{s=1}^{\frac{n}{2}-1} \mathbb{V}\left[y_{n/2,s}\right] \overset{(16)}{\leq} n \cdot n^2 \left(\frac{1}{n} - \frac{1}{n^2}\right)^2 + n\left(\frac{1}{n} - \frac{1}{n^2}\right)
$$

$$
= O(n).
$$

$$(26)$$

The third sum in (25) can be bounded above in the same way as in the odd case: the associated graphs of variables $y_{i,j}, y_{i,j'}, y_{r,s}, y_{r,s'}$ with non-zero covariance in the third sum, are isomorphic to one of the graphs in Fig. 2. Thus we can use Claim 20 and (22) to obtain

$$
\sum_{\substack{1 \leq i,r \leq \frac{n}{2} \\ 0 \leq j,j',s,s' \leq n-1 \\ j < j'; s < s' \\ j \not\equiv_{\frac{n}{2}} j'; s \not\equiv_{\frac{n}{2}} s' \\ (i,j,j') \neq (r,s,s')}} \mathrm{Cov}\left[y_{i,j} y_{i,j'}, y_{r,s} y_{r,s'}\right] = O(n). \quad (27)
$$

In the fourth sum in (25), the variables with non-zero covariance have an associated multi-graph which is isomorphic to one of the following multi-graphs.

$$G_{13} \qquad G_{14} \qquad G_{15}$$
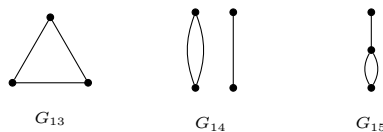
Let $\mathcal{X} := \{\{y_{u,v}, y_{u,v'}, y_{\frac{n}{2},w}\} : 1 \leq u \leq \frac{n}{2}; 0 \leq v < v' \leq n-1; v \not\equiv_{\frac{n}{2}} v'; 0 \leq w \leq \frac{n}{2}-1\}$. In the same way as Claim 20, we can prove that

$$\#\{X \in \mathcal{X} : G(X) \cong G_c\} = O(n^3), \quad c = 13, 14, 15.$$

As in (22), we can prove that $\mathbb{E}\left[y_{u,v}y_{u,v'}y_{\frac{n}{2},w}\right] = \frac{1}{n^2}$ for all $X = \{y_{u,v}, y_{u,v'}, y_{\frac{n}{2},w}\} \in \mathcal{X}$. Thus

$$\sum_{\substack{1 \leq u \leq \frac{n}{2} \\ 0 \leq v < v' \leq n-1 \\ 0 \leq w \leq \frac{n}{2}-1}} \mathrm{Cov}\left[y_{u,v}y_{u,v'}, y_{\frac{n}{2},w}\right] \leq 3 \cdot O(n^3)\frac{1}{n^2} = O(n). \tag{28}$$

Plugging (26), (27), (28) into (25) finally yields

$$\mathbb{V}\left[\mathcal{Z}_1\right] = O(n) + O(n) + 2 \cdot O(n) = O(n), \tag{29}$$

for all n even. Equations (18), (23), (24) and (29) together yield Claim 19 in the case when n is even. Thus we have fully established Claim 19. □

5.3. $\mathcal{E}_{\mathrm{zero}}(\frac{1}{2} - \varepsilon)$ has high probability

Using Chebyshev's inequality, we obtain that

$$\mathbb{P}\left[\left|\mathcal{Z}_0 - \mathbb{E}\left[\mathcal{Z}_0\right]\right| \geq \lambda_0\right] \leq \frac{\mathbb{V}\left[\mathcal{Z}_0\right]}{\lambda_0^2}; \qquad \mathbb{P}\left[\left|\mathcal{Z}_1 - \mathbb{E}\left[\mathcal{Z}_1\right]\right| \geq \lambda_1\right] \leq \frac{\mathbb{V}\left[\mathcal{Z}_1\right]}{\lambda_1^2},$$

for every $\lambda_0, \lambda_1 > 0$. In particular, this implies that

$$\mathbb{P}\left[\mathcal{Z}_0 < \mathbb{E}\left[\mathcal{Z}_0\right] - \lambda_0\right] \leq \frac{\mathbb{V}\left[\mathcal{Z}_0\right]}{\lambda_0^2}; \qquad \mathbb{P}\left[\mathcal{Z}_1 > \mathbb{E}\left[\mathcal{Z}_1\right] + \lambda_1\right] \leq \frac{\mathbb{V}\left[\mathcal{Z}_1\right]}{\lambda_1^2}.$$

Let $\varepsilon \in (0,1)$ be the constant from the statement of Lemma 7, and set $\nu = \varepsilon n/8$. Choosing $\lambda_0 = \lambda_1 = \nu$ and using Claims 18 and 19 we get that

$$\mathbb{P}\left[\mathcal{Z}_0 < \mathbb{E}\left[\mathcal{Z}_0\right] - \nu\right] \leq \frac{\mathbb{V}\left[\mathcal{Z}_0\right]}{\nu^2} = \frac{O(n)}{n^2} = O\left(\frac{1}{n}\right);$$

$$\mathbb{P}\left[\mathcal{Z}_1 > \mathbb{E}\left[\mathcal{Z}_1\right] + \nu\right] \leq \frac{\mathbb{V}\left[\mathcal{Z}_1\right]}{\nu^2} = \frac{O(n)}{n^2} = O\left(\frac{1}{n}\right).$$

By Claim 18 we have

$$\delta := (\frac{1}{2} - \varepsilon)\left\lfloor\frac{n}{2}\right\rfloor \leq \mathbb{E}\left[\mathcal{Z}_0 - \mathcal{Z}_1\right] - 2\nu$$

for n sufficiently large. Thus, using Claim 15 we can conclude that

$$\mathbb{P}\left[\mathcal{E}_{\text{zero}}^c(\tfrac{1}{2} - \varepsilon)\right] = \mathbb{P}\left[\left\{\mathbf{b} \in \mathcal{M}_n : \ D(\mathbf{b}) < (\tfrac{1}{2} - \varepsilon)\left\lfloor\tfrac{n}{2}\right\rfloor\right\}\right]$$

$$\leq \underbrace{\mathbb{P}\left[\mathcal{Z}_0 < \mathbb{E}\left[\mathcal{Z}_0\right] - \nu\right]}_{= O\left(\frac{1}{n}\right)} + \underbrace{\mathbb{P}\left[\mathcal{Z}_1 > \mathbb{E}\left[\mathcal{Z}_1\right] + \nu\right]}_{= O\left(\frac{1}{n}\right)}$$

$$= O\left(\frac{1}{n}\right).$$

This concludes the proof of Lemma 7.

6. Connections with chromatic polynomials of circulant graphs

As we have already seen in the proof of Claim 11, the multi-graph associated with the variables in row $i \neq \frac{n}{2}$ of $T_{\mathbf{b}}$ is the circulant graph $C_n(i)$, and the same holds for the variables in row $n/2$ if we consider the associated graph and not the associated multi-graph. Furthermore, we can express the probability of synchronization of circular automata in terms of chromatic polynomials of circulant graphs: this is a consequence of the close connection of the moments of $D(\mathbf{b})$ to chromatic polynomials of circulant graphs. We formalize this in the following results.

Definition. The *circulant graph* $C_n(i_1, i_2, \ldots, i_k)$ is a graph with vertex set $\mathbb{Z}_n$ where two vertices r, s are adjacent if $\left|r - s\right|_n \in \{i_1, i_2, \ldots, i_k\}$.

Definition. Let G be a graph with vertex set $\{0, 1, \ldots, n-1\}$. The *chromatic polynomial* $P(G; x) : \mathbb{N} \to \mathbb{N}$ of G is defined by

$$P(G; x) := \#\{\mathbf{b} \in \{0, \ldots, x - 1\}^n : \ \mathbf{b} \text{ is a proper coloring of } G\}.$$

Remark 21. Let G be of order n. Then $P(G; x) = \sum_{j=1}^n \lambda_j x^j$, where $\lambda_j \in \mathbb{Z}$ (see, for instance, [9]).

Claim 22. *Let* $D(\mathbf{b})$ *and* $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1}) \in \mathcal{M}_n$ *be as in Lemma 7. Then*

$$\mathbb{E}\left[D\right] = \left\lfloor\frac{n}{2}\right\rfloor - \sum_{i=1}^{\lfloor\frac{n}{2}\rfloor} \frac{P_i(n)}{n^n}$$

and

$$\mathbb{V}\left[D\right] = \sum_{i=1}^{n}\left(\frac{P_i(n)}{n^n} - \frac{P_i^2(n)}{n^{2n}}\right) + 2 \sum_{1 \leq i < j \leq \lfloor\frac{n}{2}\rfloor}\left(\frac{P_{i,j}(n)}{n^n} - \frac{P_i(n)P_j(n)}{n^{2n}}\right),$$

where P_i *is the chromatic polynomial of the circulant graph* $C_n(i)$ *and* $P_{i,j}$ *is the chromatic polynomial of the circulant graph* $C_n(i, j)$.

Remark 23. • It is easy to derive that $P_i(x) = \left((x-1)^{l_i} + (-1)^{l_i}(x-1)\right)^{\frac{n}{l_i}}$ where $l_i = \frac{n}{\gcd(n,i)}$, because $C_n(i)$ is a collection of $\gcd(n,i)$ many disjoint cycles of length $\frac{n}{\gcd(n,i)}$ [5]. With this explicit expression, an easy corollary of Claim 22 is the estimate $\mathbb{E}[D] \sim (1 - e^{-1})\left\lfloor \frac{n}{2} \right\rfloor$.

• We could not find an explicit expression for $P_{i,j}$. The calculation of the chromatic number of circulant graphs with an arbitrary number of parameters is an NP-Hard problem [7]. This implies that the calculation of chromatic polynomials of circulant graphs is also NP-Hard since

$\chi(G) = \operatorname{argmin}_{w \in \mathbb{N}} P(G; w) > 0$ – we believe that our unfruitful attempts to estimate $\mathbb{V}[D]$ are connected to this. To circumvent these issues, the variables $\mathcal{Z}_0$ and $\mathcal{Z}_1$ in Section 5 were introduced.

Proof of Claim 22. Let us recall that $D(\mathbf{b}) = \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} D_i(\mathbf{b})$, where

$$D_i(\mathbf{b}) := \begin{cases} 1, & \text{if there exist } k, l \in \mathbb{Z}_n \text{ such that } |k-l|_n = i \text{ and } |b_k - b_l|_n = 0. \\ 0, & \text{otherwise.} \end{cases}$$

Then $D_i(\mathbf{b}) = 1 - x_i(\mathbf{b})$, where

$$x_i(\mathbf{b}) := \prod_{j=0}^{n} \left(1 - \mathbb{1}\{|b_j - b_{(j+i)_n}|_n = 0\}\right).$$

We observe that $x_i(\mathbf{b}) = 1$ if and only if every two numbers $r, s \in \mathbb{Z}_n$ at cyclic distance i have different images under $\mathbf{b}$ and $x_i(\mathbf{b}) = 0$ otherwise. If we consider $\mathbf{b}$ as a random coloring of $C_n(i)$, then $x_i(\mathbf{b}) = 1$ if and only if $C_n(i)$ is properly colored by $\mathbf{b}$. Thus

$$\mathbb{E}[x_i] = \mathbb{P}[\{\mathbf{b} : x_i(\mathbf{b}) = 1\}] = \frac{P_i(n)}{n^n}.$$

In a similar way

$$\mathbb{E}[x_i x_j] = \mathbb{P}[\{\mathbf{b} : x_i(\mathbf{b}) x_j(\mathbf{b}) = 1\}] = \frac{P_{i,j}(n)}{n^n}.$$

Therefore

$$\mathbb{E}[D] = \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \mathbb{E}[D_i] = \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} (1 - \mathbb{E}[x_i]) = \left\lfloor \frac{n}{2} \right\rfloor - \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \frac{P_i(n)}{n^n},$$

as well as

$$\mathbb{V}[D_i] = \mathbb{E}[D_i^2] - \mathbb{E}[D_i]^2 = \left(1 - \frac{P_i(n)}{n^n}\right) - \left(1 - \frac{P_i(n)}{n^n}\right)^2 = \frac{P_i(n)}{n^n} - \frac{P_i^2(n)}{n^{2n}}$$

and

$$\mathrm{Cov}\left[D_i, D_j\right] = \mathbb{E}\left[D_i D_j\right] - \mathbb{E}\left[D_i\right]\mathbb{E}\left[D_j\right] = \mathbb{E}\left[(1-x_i)(1-x_j)\right] - \mathbb{E}\left[1-x_i\right]\mathbb{E}\left[1-x_j\right]$$
$$= \mathbb{E}\left[x_i x_j\right] - \mathbb{E}\left[x_i\right]\mathbb{E}\left[x_j\right]$$
$$= \frac{P_{i,j}(n)}{n^n} - \frac{P_i(n)P_j(n)}{n^{2n}}.$$

Plugging the two previous equations into

$$\mathbb{V}\left[D\right] = \sum_{i=1}^{\left\lfloor\frac{n}{2}\right\rfloor} \mathbb{V}\left[D_i\right] + 2\sum_{1\leq i<j\leq\left\lfloor\frac{n}{2}\right\rfloor} \mathrm{Cov}\left[D_i, D_j\right]$$

yields Claim 22. □

We get the following relation between chromatic polynomials of circulant graphs and synchronization of circular automata. The number $\frac{1}{2} - e^{-1}$ in the statement of Theorem 24 has the approximate value 0.13.

Theorem 24. *Let $\mathcal{A}_n(\mathbf{b})$ be a circulant graph as introduced in Section 2. Let $\varepsilon \in (0, \frac{1}{2} - e^{-1})$, then there exist $n_\epsilon \in \mathbb{N}$ such that for all $n \geq n_\epsilon$ it holds that*

$$\mathbb{P}\left[\{\mathbf{b}\in\mathcal{M}_n:\ \mathcal{A}_n(\mathbf{b})\ synchronizes\}\right] \geq 1 - \left\lfloor\frac{n}{2}\right\rfloor\exp\left\{-\frac{1}{2n}\left(\varepsilon\left\lfloor\frac{n}{2}\right\rfloor - 1\right)^2\right\} - \frac{\mathbb{V}\left[D\right]}{\left(\varepsilon\left\lfloor\frac{n}{2}\right\rfloor - 1\right)^2},$$

where $\mathbb{V}\left[D\right]$ is as given in Claim 22.

Proof. By (11), (13) we know that

$$\mathbb{P}\left[\mathcal{E}^c_{\mathrm{row}}(\alpha^\star)\right] \leq \left\lfloor\frac{n}{2}\right\rfloor\exp\left\{-\frac{1}{2n}\left(\varepsilon\left\lfloor\frac{n}{2}\right\rfloor - 1\right)^2\right\}, \tag{30}$$

for all $\varepsilon > 0$ and n large enough, where $\alpha^\star = 1 - e^{-1} - \varepsilon$. Using the expression for P_i in Remark 23 together with the inequality $1 - x \leq e^{-x}$, $x \in \mathbb{R}$, we bound $P_i(n)/n^n$ from above

$$\frac{P_i(n)}{n^n} = \left(\frac{n-1}{n}\right)^n\left(1 + \frac{(-1)^{\ell_i}}{(n-1)^{\ell_i-1}}\right)^{\frac{n}{\ell_i}}$$
$$\leq e^{-1}\left(1 + \frac{1}{(n-1)^{\ell_i-1}}\right)^{\frac{n}{\ell_i}}$$
$$\leq e^{-1}e^{\frac{n}{\ell_i}\cdot\frac{1}{(n-1)^{\ell_i-1}}}$$
$$= \exp\left\{-1 + \frac{n}{\ell_i\cdot(n-1)^{\ell_i-1}}\right\}$$

and thus

$$
\frac{P_i(n)}{n^n} \leq
\begin{cases}
\exp\left\{-1 + \frac{1}{2} \cdot \left(\frac{n}{n-1}\right)\right\}, & \text{if } i = \frac{n}{2} \text{ i.e. } \ell_i = 2; \\
\exp\left\{-1 + \frac{n}{3(n-1)^2}\right\}, & \text{if } i \neq \frac{n}{2} \text{ i.e. } \ell_i \geq 3.
\end{cases}
\tag{31}
$$

Using Equation (31) and the equation $\mathbb{E}[D] = \lfloor \frac{n}{2} \rfloor - \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \frac{P_i(n)}{n^n}$ from Claim 22 we get that

$$
\mathbb{E}[D] \geq \left\lfloor \frac{n}{2} \right\rfloor \left(1 - \exp\left\{\frac{n}{3(n-1)^2} - 1\right\}\right) - 1 = \eta_\star.
$$

By Chebyshev's inequality and elementary manipulations, we get that

$$
\mathbb{P}\left[\{\mathbf{b} \in \mathcal{M}_n : \ D(\mathbf{b}) < \eta_\star - \lambda\}\right] \leq \frac{\mathbb{V}[D]}{\lambda^2},
$$

for all $\lambda > 0$. Let $\varepsilon > 0$. Setting $\lambda = \lambda'_\varepsilon(n) = \eta_\star - \lfloor \frac{n}{2} \rfloor (1 - e^{-1} - \varepsilon) + 1$ and noting that $\lambda > 0$ for n large enough, we get that

$$
\begin{aligned}
\mathbb{P}\left[\left(\mathcal{E}_{\text{zero}}^{\tilde{\beta}}\right)^c\right] = \mathbb{P}\left[\left\{\mathbf{b} \in \mathcal{M}_n : \ D(\mathbf{b}) < \left\lfloor \frac{n}{2} \right\rfloor (1 - e^{-1} - \varepsilon) - 1\right\}\right] &\leq \frac{\mathbb{V}[D]}{\left(\lambda'_\varepsilon(n)\right)^2} \\
&\leq \frac{\mathbb{V}[D]}{\left(\lfloor \frac{n}{2} \rfloor \varepsilon - 1\right)^2}
\end{aligned}
$$

for n sufficiently large, where $\tilde{\beta} = 1 - e^{-1} - \varepsilon - \frac{1}{\lfloor \frac{n}{2} \rfloor}$. Using the previous inequalities, we conclude that

$$
\begin{aligned}
\mathbb{P}\left[\{\mathbf{b} \in \mathcal{M}_n : \ \mathcal{A}_n(\mathbf{b}) \text{ synchronizes}\}\right] \\
\overset{(6)}{\geq} 1 - \mathbb{P}\left[\mathcal{E}_{\text{row}}^c(\alpha^\star)\right] - \mathbb{P}\left[\mathcal{E}_{\text{zero}}^c(\tilde{\beta})\right] \tag{32} \\
\geq 1 - \left\lfloor \frac{n}{2} \right\rfloor \exp\left\{-\frac{1}{2n}\left(\varepsilon \left\lfloor \frac{n}{2} \right\rfloor - 1\right)^2\right\} - \frac{\mathbb{V}[D]}{\left(\varepsilon \lfloor \frac{n}{2} \rfloor - 1\right)^2} \tag{33}
\end{aligned}
$$

for n large enough where the relations $\alpha^\star, \tilde{\beta} > 0$ and $\alpha^\star + \tilde{\beta} > 1$ are valid when $\varepsilon \in (0, \frac{1}{2} - e^{-1})$ and n is large enough.　□

Actually, we formulate the following conjecture:

Conjecture 25. $\mathbb{V}[D] = O(n)$.

To prove this conjecture it is sufficient to prove that there is $g : \mathbb{N} \to \mathbb{R}$ such that $\left|\frac{P_{i,j}(n)}{n^n} - \frac{P_i(n)P_j(n)}{n^{2n}}\right| \leq g(n) = O(1/n)$ for all i, j. From (31) we see that

$0 \leq P_i(n)/n^n \leq f(n) = O(1)$ for all i, therefore the first part of the sum of $\mathbb{V}[D]$ given in Claim 22 is $|\sum_{i=1}^{n} \left(\frac{P_i(n)}{n^n} - \frac{P_i^2(n)}{n^{2n}} \right)| \leq nf(n) = O(n)$. The second part of the sum $\sum_{1 \leq i < j \leq \lfloor \frac{n}{2} \rfloor} \left(\frac{P_{i,j}(n)}{n^n} - \frac{P_i(n)P_j(n)}{n^{2n}} \right)$ has a quadratic number of elements of the form $\frac{P_{i,j}(n)}{n^n} - \frac{P_i(n)P_j(n)}{n^{2n}}$, and it can be bounded by $O(n^2)g(n) = O(n)$ if the assumption $|\frac{P_{i,j}(n)}{n^n} - \frac{P_i(n)P_j(n)}{n^{2n}}| \leq g(n) = O(1/n)$ for all i,j is true, making $\mathbb{V}[D] = O(n) + O(n) = O(n)$. In particular, a positive answer to this chromatic-polynomial question would give an alternative proof of Theorem 4.

7. Future work

Let $\mathcal{A}_n(\mathbf{a}, \mathbf{b})$ be an automaton where $\mathbf{a} : \mathbb{Z}_n \to \mathbb{Z}_n$ is fixed and $\mathbf{b} \in \mathcal{M}_n$. These are natural lines of research to extend/improve the results in this paper:

• We want to explore in more detail the strengths and limitations in the ideas presented in this paper. For example, we think that these ideas can extend Theorem 4 to the case where $\mathbf{a} : \mathbb{Z}_n \to \mathbb{Z}_n$ is in the form of a finite number of pairwise disjoint cycles of almost-equal length. We also think that (probabilistic) upper bounds for the length of the synchronizing minimal words can be given with our techniques, in the spirit of the results of [11].

• Theorem 3 has a decay rate in $\Theta\left(\frac{\sqrt{p}}{e^p} \right)$. We believe that this can be extended in a weaker form to the case of circular automata of composite order:

Conjecture 26.

$$\mathbb{P}\left[\{\mathbf{b} \in \mathcal{M}_n : \ \mathcal{A}_n(\mathbf{b}) \text{ synchronizes}\}\right] = 1 - O(\alpha^n),$$

for some $0 < \alpha < 1$, as $n \to \infty$.

Acknowledgments

References

[1] D.S. Ananichev, V.V. Gusev, M.V. Volkov, Slowly synchronizing automata and digraphs, CoRR, arXiv:1005.0129 [abs], 2010.

[2] M.-P. Béal, M.V. Berlinkov, D. Perrin, A quadratic upper bound on the size of a synchronizing word in one-cluster automata, Int. J. Found. Comput. Sci. 22 (02) (2011) 277–288.

[3] M.V. Berlinkov, On the probability of being synchronizable, in: Algorithms and Discrete Applied Mathematics, in: Lecture Notes in Comput. Sci., vol. 9602, Springer, Cham, 2016, pp. 73–84.

[4] M.V. Berlinkov, C. Nicaud, Synchronizing random almost-group automata, in: International Conference on Implementation and Application of Automata, Springer, 2018, pp. 84–96.

[5] F. Boesch, R. Tindell, Circulants and their connectivities, J. Graph Theory 8 (4) (1984) 487–499.

[6] J. Cerny, Poznamka k homogenym eksperimentom s konechnymi automatami, Math.-Fyz. Cas 14 (1964) 208–215.

[7] B. Codenotti, I. Gerace, S. Vigna, Hardness results and spectral techniques for combinatorial problems on circulant graphs, Linear Algebra Appl. 285 (1) (1998) 123–142.

[8] L. Dubuc, Sur les automates circulaires et la conjecture de Černỳ, RAIRO Theor. Inform. Appl. 32 (1–3) (1998) 21–34.

[9] D. Fengming, K. Khee-meng, et al., Chromatic Polynomials and Chromaticity of Graphs, World Scientific, 2005.

[10] C. McDiarmid, On the method of bounded differences, Surv. Comb. 141 (1) (1989) 148–188.

[11] C. Nicaud, The Černý conjecture holds with high probability, J. Autom. Lang. Comb. 24 (2–4) (2019) 343–365.

[12] D. Perrin, Codes asynchrones, Bull. Soc. Math. Fr. 105 (1977) 385–404.

[13] J.-E. Pin, Sur un cas particulier de la conjecture de Cerny, in: Automata, Languages and Programming, Fifth Internat. Colloq., Udine, 1978, in: Lecture Notes in Comput. Sci., vol. 62, Springer, Berlin-New York, 1978, pp. 345–352.

[14] J.-E. Pin, On Two Combinatorial Problems Arising from Automata Theory, North-Holland Mathematics Studies, vol. 75, Elsevier, 1983, pp. 535–548.

[15] Y. Shitov, An improvement to a recent upper bound for synchronizing words of finite automata, J. Autom. Lang. Comb. 24 (2019) 367–373.

[16] E. Skvortsov, Y. Zaks, Synchronizing random automata, Discret. Math. Theor. Comput. Sci. 12 (4) (2010) 95–108.

[17] M. Szykuła, Improving the upper bound on the length of the shortest reset words, arXiv preprint arXiv:1702.05455, 2017.

[18] M.V. Volkov, Synchronizing automata and the Černỳ conjecture, in: International Conference on Language and Automata Theory and Applications, Springer, 2008, pp. 11–27.