# On the mixing time of the Diaconis-Gangolli random walk on contingency tables over $\mathbb{Z} / q \mathbb{Z}$ 

Evita Nestoridi * Oanh Nguyen *


#### Abstract

The Diaconis-Gangolli random walk is an algorithm that generates an almost uniform random graph with prescribed degrees. In this paper, we study the mixing time of the DiaconisGangolli random walk restricted on $n \times n$ contingency tables over $\mathbb{Z} / q \mathbb{Z}$. We prove that the random walk exhibits cutoff at $\frac{n^{2}}{4\left(1-\cos \frac{2 \pi}{q}\right)} \log n$, when $\log q=o\left(\frac{\sqrt{\log n}}{\log \log n}\right)$.


## 1 Introduction

Random graphs are an important object of study in Combinatorics, Computer Science, and Probability. An $(n, n)$ bipartite graph is a graph with a left vertex set $V=\left\{v_{1}, \ldots, v_{n}\right\}$ and a right vertex set $U=\left\{u_{1}, \ldots, u_{n}\right\}$ and the only edges are the edges that connect a vertex in $V$ with a vertex in $U$. Consider the problem of generating a random bipartite graph with prescribed degrees. How do we choose uniformly at random such an $(n, n)$ bipartite graph?
Diaconis and Gangolli 30 proposed the following randomized algorithm. Start with a bipartite graph $G_{0}$ that has the desired vertex degrees at time $t=0$. At time $t$, from the graph $G_{t-1}$, choose two pairs of vertices $v_{i} \neq v_{j}$ in $V$ and $u_{k} \neq u_{l}$ in $U$ uniformly at random. We delete the already existing edges between $v_{i}, v_{j}$ and $u_{k}, u_{l}$ and we draw the remaining edges between them to get $G_{t}^{\prime}$. If the result is not a graph with the prescribed degrees, then $G_{t}$ is set to be $G_{t-1}$. Otherwise, $G_{t}:=G_{t}^{\prime}$. In the language of random graphs, such a procedure is also known as the simple switching method developed by McKay and Wormald and many others (see, for example, the survey [46] and the references therein).


Two main questions concerning random bipartite graph with prescribed degrees are: what is their number and how long does the Diaconis-Gangolli algorithm take to produce such a random bipartite graph?

[^0]In this paper we consider a more specialized version of the Diaconis-Gangolli algorithm. To start with a simple example, on $\mathbb{Z} / 2 \mathbb{Z}$, consider the problem of generating a random bipartite graph in which every vertex has an even degree. At time $t=0$, we start with the empty graph $G_{0}$. At time $t$, the Diaconis-Gangolli algorithm suggests that from the graph $G_{t-1}$, choose two pairs of vertices $v_{i} \neq v_{j}$ in $V$ and $u_{k} \neq u_{l}$ in $U$ uniformly at random. Then, replace the subgraph induced by restricting $G_{t-1}$ on these four vertices by its complement.


Our main theorem below asserts that at time $t \geq \frac{n^{2}}{8} \log n+10 c n^{2} \sqrt{\log n} \log \log n$, the (random) graph $G_{t}$ is distributed almost uniformly: the $L^{1}$ distance between the distribution of $G_{t}$ and the uniform distribution on the bipartite graphs whose all degrees are even is at most $e^{-c}$.

Similarly, one can use the same algorithm to generate a uniform bipartite graph with prescribed degree parities, say, the vertices in $A \subset V$ and $B \subset U$ have odd degrees and the rest have even degrees. The only difference is in choosing the starting point $G_{0}$. Instead of starting at the empty graph, one can start at any graph that satisfies the prescribed degree parities.
Associate each bipartite graph with its adjacency matrix $A$, which is an $n \times n$ matrix whose $(i, j)$ entry is 1 if $\left(v_{i}, u_{j}\right)$ is an edge and 0 otherwise. The requirement that each vertex has a specific degree parity means that we require $A$ to have given row sums and column sums in $\mathbb{Z} / 2 \mathbb{Z}$.
More generally, we consider matrices with prescribed row and column sums in $\mathbb{Z} / q \mathbb{Z}$ for positive integers $q$.
Definition 1.1. A contingency table over $\mathbb{Z} / q \mathbb{Z}$ is an $n \times n$ matrix with entries in $\mathbb{Z} / q \mathbb{Z}$, with fixed row sums $\left(r_{1}, \ldots, r_{n}\right) \in(\mathbb{Z} / q \mathbb{Z})^{n}$ and fixed column sums $\left(c_{1}, \ldots, c_{n}\right) \in(\mathbb{Z} / q \mathbb{Z})^{n}$. Note that for the existence of such matrices, we need that $\sum_{i=1}^{n} r_{i}=\sum_{j=1}^{n} c_{j}$.

The Diaconis-Gangolli random walk on $n \times n$ contingency tables over $\mathbb{Z} / q \mathbb{Z}$ goes as follows. Pick two distinct rows and two distinct columns at random. Then, we look at the equilateral that these rows and columns form. We flip a fair coin. If heads we add

$$
T=\left(\begin{array}{cc}
-1 & 1 \\
1 & -1
\end{array}\right)
$$

to the corners of the equilateral. If tails, then we add $-T$ to the corners of the equilateral.
Let $\Omega$ be the set of all contingency tables with the prescribed degrees in $\mathbb{Z} / q \mathbb{Z}$ and let $A_{t}$ be the contingency table after $t$ steps of the process. For $A, B \in \Omega$, let $P_{A}^{t}(B)$ be the probability of moving from $A$ to $B$ after $t$ steps. The sequence of probability measures $P_{A}^{t}$ converges to the uniform measure $\pi$ on $\Omega$, as $t \rightarrow \infty$, with respect to the total variation distance

$$
\begin{equation*}
d(t):=\max _{A \in \Omega}\left\|P_{A}^{t}-\pi\right\|_{T . V .}=\max _{A \in \Omega}\left\{\frac{1}{2} \sum_{B \in \Omega}\left|P_{A}^{t}(B)-\pi(B)\right|\right\} \tag{1}
\end{equation*}
$$

A question which arises naturally is to determine the rate of convergence to stationarity of the random walk, which is quantified by the mixing time

$$
\begin{equation*}
t_{m i x}(\varepsilon)=\min \{t \in \mathbb{N}: d(t) \leq \varepsilon\} \tag{2}
\end{equation*}
$$

Our main result is the following.
Theorem 1.2. Let $n \geq 4$ and $q \geq 2$. For the Diaconis-Gangolli walk on $n \times n$ contingency tables with entries in $\mathbb{Z} / q \mathbb{Z}$, with row sums $\left(r_{1}, \ldots, r_{n}\right) \bmod q$ and column sums $\left(c_{1}, \ldots, c_{n}\right) \bmod q$, we have that
(a) (Upper bound) If $t \geq \frac{n^{2}}{4\left(1-\cos \frac{2 \pi}{q}\right)} \log n+\frac{n^{2}}{\left(1-\cos \frac{2 \pi}{q}\right)} c \log \log (16 n) \sqrt{\log n} \log q$, then

$$
d(t) \leq q^{-c},
$$

for all $c \geq \frac{640}{\log \log (16 n)}$.
(b) (Lower bound) If $t \leq \frac{n^{2}}{4\left(1-\cos \frac{2 \pi}{q}\right)} \log n-\frac{n^{2}}{4\left(1-\cos \frac{2 \pi}{q}\right)}(c+12) \log q$, then

$$
d(t) \geq 1-q^{-c},
$$

for all $c \geq 0$.
Set $t_{n, q}=\frac{n^{2}}{4\left(1-\cos \frac{2 \pi}{q}\right)} \log n$ and $\Delta_{n, q}=\frac{n^{2}}{\left(1-\cos \frac{2 \pi}{q}\right)} \log \log (16 n) \sqrt{\log n} \log q$. Theorem 1.2 says that over $\mathbb{Z} / q \mathbb{Z}$, the random walk mixes at time $t_{n, q}$ with window of order at most $\Delta_{n, q}$, i.e.

$$
\lim _{c \rightarrow \infty} \lim _{n \rightarrow \infty} d\left(t_{n, q}-c \Delta_{n, q}\right)=1
$$

and

$$
\lim _{c \rightarrow \infty} \lim _{n \rightarrow \infty} d\left(t_{n, q}+c \Delta_{n, q}\right)=0
$$

If $\log q=o\left(\frac{\sqrt{\log n}}{\log \log n}\right)$ then $\Delta_{n, q}=o\left(t_{n, q}\right)$. In other words, the random walk exhibits cutoff, a sharp transition from $d(t) \approx 1$ to $d(t) \approx 0$.
If $n=2$, then the lazy random walk on contingency tables over $\mathbb{Z} / q \mathbb{Z}$ is the same as the lazy random walk on $\mathbb{Z} / q \mathbb{Z}$, which is known to not have cutoff [27].

### 1.1 Literature

Contingency tables are used in statistics, in order to display the results of tests and surveys. Diaconis and Efron ([28], [29]) developed the conditional volume test, which is a method for performing tests of great importance in such tables. The Diaconis-Efron test provides strong motivation for sampling a contingency table with given row and column sums uniformly at random.
Diaconis, Gangolli [30] and Diaconis and Saloff-Coste (see page 373 of [33]) were the first ones to introduce Markov chains for sampling contingency tables, although it is mentioned in [30] that this chain has been used by practitioners. Diaconis and Saloff-Coste proved that if $N=\sum c_{i}=\sum r_{i}$ and the number of rows and columns is fixed then the mixing time is of order $N^{2}$. Hernek [37] considered the case when the table has two rows and proved that the same chain mixes in time polynomial in the number of columns and $N$. Chung, Graham, and Yau [22] proved that a modified version of the Diaconis and Saloff-Coste chain converges in time polynomial in $N$, the number of rows, and the number of columns, given that $N$ is large.

[^1]Dyer, Kannan, and Mount [35] found a new way to sample contingency tables using polytopes which provided the first truly polynomial-time algorithm (polynomial in the number of rows, the number of columns, and the logarithm of $N$ ). Later, Morris [43] refined their answers.

Dyer and Greenhill [34] applied coupling to get pre-cutoff at $n^{2} \log N$ for the case of $2 \times 2$ heat-bath chain, a different Markov chain on $2 \times n$ contingency tables. Matsui, Matsui and Ono [39] extended the result of [34] for $2 \times 2 \times \ldots \times 2 \times J$ contingency tables. Cryan, Dyer, Goldberg, Jerrum, Martin [24] extended the result of [34] for the case where there is a constant number of rows.

A closely related problem to the mixing time is the enumerating problem. It is worth mentioning that there has been a rich literature in enumerating contingency tables ([2], 3], 4], 6], [5] , 9], 7], [10], [1, [25] [19], [36], [44]) and studying algorithms to sample contingency tables or approximate their number ( 17, , 21], [20], [15], [13], [12], [14, [23], [33]). On a different note, Blanchet and Stauffer [16] provide a necessary and sufficient condition so that the configuration model outputs a binary contingency table with probability bounded away from 0 and $N \rightarrow \infty$.

Enumerating the graphs with a given degree sequence also has a vast literature and important applications. See for example, Bender and Canfield [11], Bollobás [18] and Wormald [46]. McKay and Wormald used the method of switchings to obtain in [41] an asymptotic formula for the number of labeled graphs with a given degree sequence in the case where the average degree is $o(\sqrt{n})$. See also [42, [40], 8] for other ranges of the degrees. In a recent breakthrough, Liebenau and Wormald [38] obtained, among other things, the asymptotic number of $d$-regular graphs on $n$ vertices for all d.

### 1.2 There is no Markovian coupling that could give Theorem 1.2

Coupling is a powerful technique to achieve upper bounds on the mixing time. This section is dedicated to proving that there is no Markovian coupling that would give optimal mixing time bounds.

Proposition 1.3. Let $q \geq 2$ and let $T$ be a Markovian coupling time for the Diaconis-Gangolli walk in Theorem 1.2, then

$$
\mathbb{P}\left(T>\frac{n^{3}}{100}\right) \geq \frac{1}{2} .
$$

Proof. Each move of the walk is performed with probability $\frac{1}{2\binom{n}{2}^{2}}$ for $q \geq 3$ and $\frac{1}{\binom{n}{2}^{2}}$ for $q=2$. At each step we change four entries of the matrix. If there are two copies of the Markov chain $\left(C_{t}^{1}\right),\left(C_{t}^{2}\right)$, then we claim that

$$
\begin{equation*}
\mathbb{P}\left(C_{t}^{1}=C_{t}^{2} \mid C_{t-1}^{1} \neq C_{t-1}^{2}\right) \leq \frac{6 n}{\binom{n}{2}^{2}}, \tag{3}
\end{equation*}
$$

for every $t$. Notice that if $C_{t-1}^{1} \neq C_{t-1}^{2}$ then because of the degree restrictions, $C_{t-1}^{1}$ and $C_{t-1}^{2}$ have to differ in at least 4 coordinates.
If $C_{t-1}^{1} \neq C_{t-1}^{2}$ and $C_{t-1}^{1}, C_{t-1}^{2}$ differ in at least 9 entries, then (3) holds because the left hand side of (3) is zero. If $C_{t-1}^{1}, C_{t-1}^{2}$ differ in at least 5 vertices, the above probability is at most $\frac{6}{\binom{n}{2}^{2}}$. If they differ in four entries $a, b, c, d$ (which is the minimum number of entries they can differ by), the only way to resolve these differences, without creating new differences, is if we change $a, b$ in $C_{t-1}^{1}$, and $c, d$ in $C_{t-1}^{2}$ (or any other permutation of these letters). The other side of the box should be the
same on the two chains so that we don't create new mismatched coordinates. The total probability of doing such a move is at most $\frac{\binom{4}{2} n}{\binom{n}{2}^{2}}$, which gives the right hand side term.
We will couple $T$ with a geometric random variable $R$ with probability of success $p=6 n /\binom{n}{2}^{2}$ so that $T \geq R$ always. We have

$$
\mathbb{P}\left(R \geq \frac{1}{3 p}\right)=\sum_{k \geq \frac{1}{3 p}}(1-p)^{k-1} p \geq(1-p)^{1 /(3 p)} \geq \frac{1}{2} .
$$

Thus, $\mathbb{P}\left(T \geq \frac{1}{3 p}\right) \geq \mathbb{P}\left(R \geq \frac{1}{3 p}\right) \geq \frac{1}{2}$ completing the proof of the statement.
If $T$ is a coupling time then

$$
d(t) \leq \mathbb{P}(T>t),
$$

and, therefore Proposition 1.3 says that we cannot hope for a Markovian coupling that will give the upper bound of Theorem 1.2 even for $q=2$.

## 2 The contingency table walk over $\mathbb{Z} / q \mathbb{Z}$ as a random walk on a group

In this section, we explain how linear algebra and representation theory can be used to prove Theorem 1.2 .

Let $A_{i, j, k, l}$ denote the $n \times n$ matrix that has ones on the $(i, k),(j, l)$ positions, -1 on the $(i, l),(j, k)$ positions and zeros else where. If at time $t$ the Markov chain is at a contingency table $B_{t}$, then we choose matrices of the form $A_{i, j, k, l}$ and we add them to $B_{t}$. Let $A_{t+1}$ be the matrix we choose to add to $B_{t}$ at time $t+1$. Then, we have that

$$
B_{t+1}=A_{t+1}+B_{t}=B_{0}+A_{1} \ldots+A_{t+1}
$$

So, instead of studying the Markov chain $\left(B_{t}\right)$, we can equivalently study the process $C_{t}$, where

$$
C_{t}:=A_{1}+\ldots+A_{t+1} .
$$

The advantage of studying $C_{t}$ is that $C_{t}$ is a random walk on the group $G$, which consists of $n \times n$ contingency tables with entries over $\mathbb{Z} / q \mathbb{Z}$ and row sums and column sums zero. This is summarized more formally in the following lemma.

Lemma 2.1. For the processes $\left(B_{t}\right)$ and $\left(C_{t}\right)$, we have that

$$
\left\|\mathbb{P}_{x}\left(B_{t} \in \cdot\right)-\pi\right\|_{T . V .}=\left\|\mathbb{P}_{0}\left(C_{t} \in \cdot\right)-U\right\|_{T . V .},
$$

where $x \in \Omega, \pi$ is the uniform measure on $\Omega$ and $U$ is the uniform measure on $G$.

From now on, we will study the random walk $C_{t}$ on $G$. The next lemma characterizes $G$.
Lemma 2.2. The group $G$ of $n \times n$ contingency tables with entries over $\mathbb{Z} / q \mathbb{Z}$ and row sums and column sums zero, satisfies $G \sim(\mathbb{Z} / q \mathbb{Z})^{(n-1)^{2}}$.

Proof. $G$ is a vector subspace of $(\mathbb{Z} / q \mathbb{Z})^{n \times n}$ over $\mathbb{Z} / q \mathbb{Z}$. In fact, $G \sim(\mathbb{Z} / q \mathbb{Z})^{n \times n} / A$ where $A$ is the subgroup of $(\mathbb{Z} / q \mathbb{Z})^{n \times n}$ generated by $2 n-1$ relations, that are setting $2 n-1$ rows and columns to be equal to zero. Therefore, $\operatorname{dim}_{\mathbb{Z} / q \mathbb{Z}} G=(n-1)^{2}$ and this finishes the proof.

Let $B_{i, j}$ be the matrix that has ones in positions $(i, j),(i+1, j),-1$ in positions $(i, j+1),(i+1, j+1)$ and zero everywhere else. To diagonalize the matrix $P$ we will need the fact that $\left\{B_{i, j}\right\}_{i, j=1}^{n-1}$ is a basis for $G$. We can see that they are a basis, because they are linearly independent and there are $(n-1)^{2}$ of them.

Definition 2.3. Let $\tilde{A}_{i, j, k, l} \in(\mathbb{Z} / q \mathbb{Z})^{(n-1) \times(n-1)}$ be the matrix that has ones on all positions $(a, c)$ that satisfy $i \leq a \leq j$ and $k \leq c \leq l$ and everywhere else zero.

Since

$$
A_{i, j, k, l}=\sum_{a=i}^{j-1} \sum_{c=k}^{l-1} B_{a, c},
$$

the matrix $\tilde{A}_{i, j-1, k, l-1}$ is the coordinates of $A_{i, j, k, l}$ with respect to the basis ( $B_{i, j}$ ) of $G$. Similarly, we associate each element of $G$ with its coordinates with respect to the basis $\left(B_{i j}\right)$.

### 2.1 Fourier Transform and the $\ell^{2}$ bound

Let $X$ be a finite group and let $S$ be a symmetric set of generators.
Definition 2.4. Let $P$ be the uniform measure on $S$. Let $\rho$ be a representation of $X$. Define the Fourier transform of $\rho$ with respect to $P$ to be

$$
\hat{P}(\rho)=\sum_{s \in S} P(s) \rho(s) .
$$

Theorem 6 of [26, Chapter 3E] says that the Fourier transforms of the irreducible representations of $G$ with respect to $P$ give all of the eigenvalues of $P$, each one appearing with multiplicity being the dimension of the corresponding representation. The following lemma explains how to use the irreducible representations of $X$ to bound the mixing time of the Markov chain generated by $P$. It was first used in [31] and the rigorous proof can be found in [26, Chapter 3].

Lemma 2.5 (Upper bound lemma). For the random walk on $X$ generated by $P$, we have that

$$
\begin{equation*}
4\left\|P_{i d}^{t}-\pi\right\|_{T . V .}^{2} \leq \sum^{*} d_{\rho}\left(\hat{P}(\rho) \hat{P}^{*}(\rho)\right)^{t}, \tag{4}
\end{equation*}
$$

where $d_{\rho}$ is the dimension of a representation $\rho$ and the sum is over all irreducible representations $\rho$ of $X$, but the trivial one.

Apply these results to $X=G$ and $S$ being the set of all $\pm A_{i, j, k, l}$; or equivalently, $X=(\mathbb{Z} / q \mathbb{Z})^{(n-1)^{2}}$ and $S$ being the set of all $\pm \tilde{A}_{i, j, k, l}$. Let $y, g \in(\mathbb{Z} / q \mathbb{Z})^{(n-1)^{2}}$, define

$$
\rho_{y}(g)=e^{\frac{2 \pi i<g, y>}{q}},
$$

where $\langle g, y\rangle=\sum_{i=1}^{(n-1)^{2}} g_{i} y_{i}$ is the inner product of $y, g$. Each $\rho_{y}$ is one dimensional, therefore it is irreducible. As explained in Lemma 2 of [26], we have that

$$
\sum d_{i}^{2}=q^{(n-1)^{2}}
$$

where the sum is taken over all irreducible representations and $d_{i}$ is the dimension of each irreducible representation. Therefore, the set $\left\{\rho_{y}, y \in(\mathbb{Z} / q \mathbb{Z})^{(n-1)^{2}}\right\}$ consists of all irreducible representations of $G$.

The following proposition computes the Fourier transform of each irreducible $\rho_{y}$ with respect to $P$.
Lemma 2.6. Let $y \in(\mathbb{Z} / q \mathbb{Z})^{(n-1)^{2}}$, then

$$
\hat{P}\left(\rho_{y}\right)=\frac{1}{\binom{n}{2}^{2}} \sum_{i, j, k, l} \cos \frac{2 \pi<y, \tilde{A}_{i, j, k, l}>}{q}
$$

where $\tilde{A}_{i, j, k, l}$ is defined in Definition 2.3.
Proof. The proof of the lemma follows from the definition of $\rho_{y}$ and the fact that

$$
\exp \left(\frac{2 \pi i<\tilde{A}_{i, j, k, l}, y>}{q}\right)+\exp \left(\frac{-2 \pi i<\tilde{A}_{i, j, k, l}, y>}{q}\right)=2 \cos \frac{2 \pi<y, \tilde{A}_{i, j, k, l}>}{q} .
$$

Applying Lemmas 2.5 and 2.6, we obtain the following bound for the random walk $\left(C_{t}\right)$ on $G$ and the uniform measure $U$ on $G$ as in Lemma 2.1.

$$
\begin{equation*}
\left\|P_{0}\left(C_{t} \in \cdot\right)-U\right\|_{T . V .}^{2} \leq \sum_{y \in G \backslash\{0\}} \hat{P}\left(\rho_{y}\right)^{2 t}=\sum_{y \in G \backslash\{0\}}\left(\frac{1}{\binom{n}{2}^{2}} \sum_{i, j, k, l} \cos \frac{2 \pi<y, \tilde{A}_{i, j, k, l}>}{q}\right)^{2 t} . \tag{5}
\end{equation*}
$$

### 2.2 Bounding negative eigenvalues

In this section, we show that the negative eigenvalues are bounded away from minus one and, therefore, the don't contribute much to the right hand side of (4).
Let $S=\left\{ \pm A_{i, j, k, l}: 1 \leq i<j \leq n, 1 \leq k<l \leq n\right\}$ denote the set of generators of the DiaconisGangolli random walk of interest over $\mathbb{Z} / q \mathbb{Z}$. Let $P$ be the transition matrix and $Q=\frac{1}{2}(I+P)$ where $I$ is the identity matrix. Notice that since all the eigenvalues $\hat{P}\left(\rho_{y}\right)$ of $P$ lie in $[-1,1]$, we have that all the eigenvalues of $Q$ are non-negative, real numbers.
Let $f: G \rightarrow \mathbb{R}$ be a function and let

$$
\begin{equation*}
\mathcal{F}(f, f)=\sum_{x, y \in G}(f(x)+f(y))^{2} P(x, y) \text { and } \tilde{\mathcal{F}}(f, f)=\sum_{x, y \in G}(f(x)+f(y))^{2} Q(x, y) . \tag{6}
\end{equation*}
$$

We are going to use Lemma 4 of [31] to bound the negative eigenvalues of $P$ from below. For completeness, we rewrite the statement of Lemma 4 of [31] for our case.
Lemma 2.7 ([31], Lemma 4). If $\tilde{\mathcal{F}}(f, f) \leq A_{*} \mathcal{F}(f, f)$ for every $f: G \rightarrow \mathbb{R}$, then

$$
\hat{P}\left(\rho_{y}\right) \geq-1+\frac{1}{A_{*}}
$$

for every $y \in(\mathbb{Z} / q \mathbb{Z})^{(n-1)^{2}}$.

We are going to use Lemma 2.7 to prove the following bound on the eigenvalues of $P$.
Lemma 2.8. For the Diaconis-Gangolli random walk on contingency tables over $\mathbb{Z} / q \mathbb{Z}$, we have that

$$
\hat{P}\left(\rho_{y}\right) \geq-\frac{28}{29},
$$

for every $y \in(\mathbb{Z} / q \mathbb{Z})^{(n-1)^{2}}$.
Proof. The proof is based on the technique of "flows" as presented in Theorem 2.3 of [32]. For completion, we explain how this method works.
Notice that for every $f: G \rightarrow \mathbb{R}$, we have that

$$
\begin{align*}
\tilde{\mathcal{F}}(f, f) & =2 \sum_{x \in G} f(x)^{2}+\frac{1}{2} \sum_{x \neq y \in G}(f(x)+f(y))^{2} P(x, y) \\
& =2 \sum_{x \in G} f(x)^{2}+\frac{1}{2} \mathcal{F}(f, f) . \tag{7}
\end{align*}
$$

To bound the term $\sum_{x \in G} f(x)^{2}$, we observe that for $n \geq 3$ and for any $k<b<l$ and $i<j$,

$$
\begin{equation*}
A_{i, j, k, l}=A_{i, j, k, b}+A_{i, j, b, l}, \tag{8}
\end{equation*}
$$

which can be illustrated for the case $i=1=k, j=2=b$ and $l=3$ as

$$
\left[\begin{array}{ccc}
1 & 0 & -1 \\
-1 & 0 & 1 \\
& \cdots &
\end{array}\right]=\left[\begin{array}{ccc}
1 & -1 & 0 \\
-1 & 1 & 0 \\
& \cdots &
\end{array}\right]+\left[\begin{array}{ccc}
0 & 1 & -1 \\
0 & -1 & 1 \\
& \ldots &
\end{array}\right] .
$$

Let $x \in G$ and let $f: G \rightarrow \mathbb{R}$. Using equation (8), we have
$2 f(x)=\left[f(x)+f\left(x+A_{i, j, k, b}\right)\right]-\left[f\left(x+A_{i, j, k, b}\right)+f\left(x+A_{i, j, k, b}+A_{i, j, b, l}\right)\right]+\left[f\left(x+A_{i, j, k, l}\right)+f(x)\right]$.
Applying Cauchy-Schwartz gives
$\frac{4}{3} f(x)^{2} \leq\left[f(x)+f\left(x+A_{i, j, k, b}\right)\right]^{2}+\left[f\left(x+A_{i, j, k, b}\right)+f\left(x+A_{i, j, k, b}+A_{i, j, b, l}\right)\right]^{2}+\left[f\left(x+A_{i, j, k, l}\right)+f(x)\right]^{2}$.
Thus, by averaging,

$$
\begin{aligned}
& f(x)^{2} \leq \frac{3}{4\binom{n}{2}\binom{n}{3}} \sum_{i<j ; k<b<l}\left\{\left[f(x)+f\left(x+A_{i, j, k, b}\right)\right]^{2}+\left[f\left(x+A_{i, j, k, b}\right)+f\left(x+A_{i, j, k, b}+A_{i, j, b, l}\right)\right]^{2}\right. \\
&\left.+\left[f\left(x+A_{i, j, k, l}\right)+f(x)\right]^{2}\right\} .
\end{aligned}
$$

Using the identities $P(x, x+g)=\frac{1}{|S|} \mathbf{1}_{g \in S},|S|=\binom{n}{2}^{2}$ if $q=2$ and $|S|=2\binom{n}{2}^{2}$ if $q>2$, we get

$$
\begin{align*}
& \sum_{x \in G} f(x)^{2} \leq \frac{3}{4\binom{n}{2}\binom{n}{3}} \sum_{x \in G} \sum_{i<j ; k<b<l}\left\{\left[f(x)+f\left(x+A_{i, j, k, b}\right)\right]^{2}\right. \\
&\left.\quad+\left[f\left(x+A_{i, j, k, b}\right)+f\left(x+A_{i, j, k, b}+A_{i, j, b, l}\right)\right]^{2}+\left[f\left(x+A_{i, j, k, l}\right)+f(x)\right]^{2}\right\} \\
& \leq \frac{9 n}{4\binom{n}{2}\binom{n}{3}} \sum_{x \in G, g \in S}(f(x)+f(x+g))^{2} \leq \frac{18 n\binom{n}{2}}{4\binom{n}{3}} \sum_{x \in G, g \in S}(f(x)+f(x+g))^{2} P(x, x+g) \\
& \leq 14 \sum_{x \in G, g \in S}(f(x)+f(x+g))^{2} P(x, x+g) . \tag{9}
\end{align*}
$$

Equation (7) and (9) give that

$$
\tilde{\mathcal{F}}(f, f) \leq 28 \mathcal{F}(f, f)+\frac{1}{2} \mathcal{F}(f, f) \leq 29 \mathcal{F}(f, f)
$$

and then, Lemma 2.7 for $A_{*}=29$ gives that

$$
\hat{P}\left(\rho_{y}\right) \geq-\frac{28}{29}
$$

for every $y \in(\mathbb{Z} / q \mathbb{Z})^{(n-1)^{2}}$.

## 3 Proof of Theorem 1.2

### 3.1 Proof of the lower bound

For the proof of the lower bound, we will use Wilson's lemma.
Lemma 3.1 (Lemma 5, 45]). Let $\varepsilon, R$ be positive numbers and $0<\gamma<2-\sqrt{2}$. Let $F: X \rightarrow \mathbb{R}$ be a function on the state space $X$ of a Markov chain $\left(C_{t}\right)$ such that

$$
\left.\mathbb{E}\left[F\left(C_{t+1}\right) \mid C_{t}\right)\right]=(1-\gamma) F\left(C_{t}\right), \quad \mathbb{E}\left[\left[F\left(C_{t}\right)-F\left(C_{t-1}\right)\right]^{2} \mid C_{t}\right] \leq R
$$

and

$$
t \leq \frac{\log \max _{x \in X} F(x)+\frac{1}{2} \log (\gamma \varepsilon /(4 R))}{-\log (1-\gamma)}
$$

Then the total variation distance from stationarity at time $t$ is at least $1-\varepsilon$.

Proof of the lower bound of Theorem 1.2. As in Definition 2.3 and the discussion that follows, we represent each element of $G$ as an $(n-1) \times(n-1)$ matrix which is its coordinates with respect to the basis $\left(B_{i j}\right)$ of $G$.

Let $D_{a, b}$ be the $(n-1) \times(n-1)$ matrix with entries at $(2 a-1,2 b-1),(2 a, 2 b)$ equal to 1 and at $(2 a, 2 b-1),(2 a-1,2 b)$ equal to -1 , while all the other entries are zero. Theorem 6 of Chapter 3 E of [26] says that the functions $G_{a, b}(x)=\cos \left(\frac{\left.2 \pi<x, D_{a, b}\right\rangle}{q}\right)$ are eigenfunctions of the transition $\operatorname{matrix} P$. To see this, consider

$$
D_{1,1}=\left(\begin{array}{cccc}
1 & -1 & 0 & \ldots \\
-1 & 1 & 0 & \ldots \\
0 & 0 & 0 & \ldots \\
& \ldots & & \ldots
\end{array}\right)
$$

We have that

$$
G_{1,1}(C)=\cos \left(\frac{2 \pi(C(1,1)-C(1,2)-C(2,1)+C(2,2))}{q}\right)
$$

We can only change the value of $G_{1,1}\left(C_{t}\right)$ if we do a move that affects exactly one of the following entries $C_{t}(1,1), C_{t}(1,2), C_{t}(2,1)$ and $C_{t}(2,2)$. For example, the moves that change only the entry $C_{t}(2,2)$ correspond to $\tilde{A}_{i, j, k, l}$, as defined in Definition 2.3, for which the $(2,2)$ entry is the left corner
of the rectangle formed by ones. There are $(n-2)^{2}$ such $\tilde{A}_{i, j, k, l}$. Using this observation, direct calculation gives

$$
\mathbb{E}\left[G_{1,1}\left(C_{t}\right) \mid C_{t-1}\right]=\left(1-\frac{4}{n^{2}}+\frac{4}{n^{2}} \cos \left(\frac{2 \pi}{q}\right)\right) G_{1,1}\left(C_{t-1}\right) .
$$

Similarly, it holds for any $G_{a, b}$ that

$$
\begin{equation*}
\mathbb{E}\left[G_{a, b}\left(C_{t}\right) \mid C_{t-1}\right]=\left(1-\frac{4}{n^{2}}+\frac{4}{n^{2}} \cos \left(\frac{2 \pi}{q}\right)\right) G_{a, b}\left(C_{t-1}\right) . \tag{10}
\end{equation*}
$$

Let

$$
F(x)=\sum_{a, b=0}^{\left\lfloor\frac{n-1}{2}\right\rfloor} G_{a, b} .
$$

Then, we have that $\max F=F(0)=\left\lfloor\frac{n-1}{2}\right\rfloor^{2}$ and (10) gives that

$$
\begin{equation*}
\mathbb{E}\left[F\left(C_{t}\right) \mid C_{t-1}\right]=\left(1-\frac{4}{n^{2}}+\frac{4}{n^{2}} \cos \left(\frac{2 \pi}{q}\right)\right) F\left(C_{t-1}\right) . \tag{11}
\end{equation*}
$$

Finally, we have that

$$
\begin{equation*}
\mathbb{E}\left[\left(F\left(C_{t}\right)-F\left(C_{t-1}\right)\right)^{2} \mid C_{t-1}\right] \leq 64 \tag{12}
\end{equation*}
$$

This is because every move $\tilde{A}_{i, j, k, l}$ that we might choose to make, affects the $G_{a, b}$ who share a unique one with $\tilde{A}_{i, j, k, l}$. For example,

$$
\tilde{A}=\left(\begin{array}{ccccc}
1 & 1 & 1 & 0 & \ldots \\
1 & 1 & 1 & 0 & \ldots \\
1 & 1 & 1 & 0 & \ldots \\
0 & 0 & 0 & 0 & \ldots \\
& \ldots & & & \ldots
\end{array}\right)
$$

fixes all $G_{a, b}$, but $G_{2,2}$. Therefore, every move that we make can affect at most four $G_{a, b}$. Thus, $\left|F\left(C_{t}\right)-F\left(C_{t-1}\right)\right| \leq 8$ surely and so $\mathbb{E}\left[\left(F\left(C_{t}\right)-F\left(C_{t-1}\right)\right)^{2} \mid C_{t-1}\right] \leq 64$.
Using equations (10) and (12) for $n \geq 4$, we have that $\gamma=\frac{4}{n^{2}}\left(1-\cos \frac{2 \pi}{q}\right) \leq \frac{1}{2}<2-\sqrt{2}$ and $R=64$. Since $\frac{1}{-\log (1-\gamma)} \geq \frac{1}{\gamma}-1$, Lemma 3.1 asserts that if

$$
t \leq\left(\frac{1}{\gamma}-1\right) \log \left(F(0) \gamma^{1 / 2} \varepsilon^{1 / 2} R^{-1 / 2} / 2\right)
$$

then

$$
d(t) \geq 1-\varepsilon
$$

Writing $\varepsilon=q^{-c}$ and performing routine algebraic manipulations, we get that if

$$
t \leq \frac{n^{2}}{4\left(1-\cos \frac{2 \pi}{q}\right)} \log n-\frac{n^{2} \log q}{4\left(1-\cos \frac{2 \pi}{q}\right)}(c+12)
$$

then $d(t) \geq 1-q^{-c}$ as desired.

### 3.2 Proof of the upper bound of Theorem 1.2

By (1) and Lemma 2.1, we get

$$
d(t)^{2} \leq\left\|\mathbb{P}_{0}\left(C_{t} \in \cdot\right)-U\right\|_{T . V}^{2}
$$

where $C_{t}$ and $U$ are as in Lemma 2.1. Combining this with (5), we get

$$
\begin{equation*}
d(t)^{2} \leq \sum_{y} \hat{P}\left(\rho_{y}\right)^{2 t} \tag{13}
\end{equation*}
$$

where the sum runs over all nonzero $(n-1) \times(n-1)$ matrices $y$ and

$$
\hat{P}\left(\rho_{y}\right)=\frac{1}{\binom{n}{2}^{2}} \sum_{i, j, k, l} \cos \frac{\left.2 \pi<y, \tilde{A}_{i, j, k, l}\right\rangle}{q} .
$$

For each $a \in \mathbb{Z} / q \mathbb{Z}$, let $N_{a}(y)$ be the number of quadruples ( $i, j, k, l$ ) with $1 \leq i \leq j \leq n-1$ and $1 \leq k \leq l \leq n-1$ such that $\left\langle y, \tilde{A}_{i, j, k, l}\right\rangle=a$. Then,

$$
\begin{equation*}
\hat{P}\left(\rho_{y}\right)=\frac{1}{\binom{n}{2}^{2}} \sum_{a \in \mathbb{Z} / q \mathbb{Z}} N_{a}(y) \cos \frac{2 \pi a}{q} . \tag{14}
\end{equation*}
$$

Note that $\sum_{a \neq 0} N_{a}(y)=\binom{n}{2}^{2}-N_{0}(y)$.
We need to show that for $t=\frac{n^{2}}{4\left(1-\cos \frac{2 \pi}{q}\right)} \log n+\frac{n^{2}}{\left(1-\cos \frac{2 \pi}{q}\right)} c \log \log (16 n) \sqrt{\log n} \log q$,

$$
d(t)^{2} \leq q^{-2 c} .
$$

To do so, we decompose the right-hand side of (13) into the sum over all $y$ with $\hat{P}\left(\rho_{y}\right)<0$ and the sum of the rest, and denote the corresponding sums by $d_{1}$ and $d_{2}$.
By Lemma 2.8, each of the $\hat{P}\left(\rho_{y}\right)$ with $\hat{P}\left(\rho_{y}\right)<0$ satisfies $\hat{P}\left(\rho_{y}\right) \geq-\frac{28}{29}$. Thus,

$$
\begin{equation*}
d_{1} \leq q^{(n-1)^{2}}\left(\frac{28}{29}\right)^{2 t} \leq q^{n^{2}} q^{-8 n^{2}-2 c} \leq q^{-2 c} / 2 . \tag{15}
\end{equation*}
$$

where we used the assumption that $c \geq \frac{640}{\log \log (16 n)}$ and $n \geq 3$ to get the estimate

$$
t \geq \frac{n^{2}}{\left(1-\cos \frac{2 \pi}{q}\right)} c \log \log (16 n) \sqrt{\log n} \log q \geq 2 c \log q+120 n^{2} \log q .
$$

For the rest of the proof, we will show that $d_{2} \leq q^{-2 c} / 2$. Assume that it holds, we have $d(t)^{2} \leq$ $d_{1}+d_{2} \leq q^{-2 c}$ as desired.
For each $(n-1) \times(n-1)$ matrix $y$ and each $1 \leq i \leq j \leq n-1$ and $1 \leq k \leq l \leq n-1$, we consider the minor $y_{i, j, k, l}$ obtained by restricting to the rows from $i$ to $j$ and the columns from $k$ to $l$, inclusively. We say that $[i, j] \times[k, l]$ is a nonzero box if the sum of the entries in this minor is nonzero. Denote by $N(y)$ the number of non-zero boxes of $y$. Observe that $\sum_{a \neq 0} N_{a}(y)=N(y)$. When $\hat{P}\left(\rho_{y}\right) \geq 0$, we have from (14) that

$$
0 \leq \hat{P}\left(\rho_{y}\right) \leq \frac{1}{\binom{n}{2}^{2}}\left[N_{0}(y)+\left(\sum_{a \neq 0} N_{a}(y)\right) \cos \frac{2 \pi}{q}\right]=1-\frac{\left(1-\cos \frac{2 \pi}{q}\right) N(y)}{\binom{n}{2}^{2}} .
$$

Thus,

$$
d_{2} \leq \sum_{y: \hat{P}\left(\rho_{y}\right) \geq 0}\left(1-\frac{\left(1-\cos \frac{2 \pi}{q}\right) N(y)}{\binom{n}{2}^{2}}\right)^{2 t} \leq \Sigma
$$

where

$$
\begin{equation*}
\Sigma:=\sum\left(1-\frac{\left(1-\cos \frac{2 \pi}{q}\right) N(y)}{\binom{n}{2}^{2}}\right)^{2 t} \tag{16}
\end{equation*}
$$

where the sum is taken over all matrices $y \neq 0$ with $N(y) \leq \frac{\binom{n}{2}^{2}}{1-\cos \frac{2 \pi}{q}}$.
It remains to show that

$$
\begin{equation*}
\Sigma \leq q^{-2 c} / 2 \tag{17}
\end{equation*}
$$

and for that we need to control the number of matrices $y$ with a prescribed range of $N(y)$.
The number $N(y)$ of nonzero boxes of a matrix $y$ can vary significantly just by changing an entry of $y$. For example, if $y$ is the zero matrix then $N(y)=0$. If we add a single entry 1 at around the middle of the matrix $y$, then $N(y) \approx(n / 2)^{4}$ which is significantly larger. Now, if the single entry 1 is at position $(1,1)$ (for example) instead of at the middle of the matrix, then $N(y) \approx n^{2}$.
It turns out to be useful to look at one dimensional version of the nonzero boxes. Let $u$ be a vector in $(\mathbb{Z} / q \mathbb{Z})^{n-1}$. For any $1 \leq i \leq j \leq n-1$, the interval $[i, j]$ is said to be a nonzero interval of $u$ if the sum of the entries of the vector $[u(i), u(i+1), \ldots, u(j)]$ is nonzero in $\mathbb{Z} / q \mathbb{Z}$. Let $S(u)$ be the number of nonzero intervals in $u$.

In order to control $S(u)$, we introduce the following definition.
Definition 3.2. Let the skeleton of $u$ to be the set $I(u)=\left\{i_{1}, i_{2}, \ldots, i_{s(u)}\right\} \subset[1, n-1]$ with

- $i_{1} \geq 1$ being the smallest index such that $u_{i_{1}} \neq 0$,
- $i_{k}$ being the smallest index such that $i_{k} \geq i_{k-1}+2$ and $u_{i_{k}} \neq 0$, for all $2 \leq k \leq s(u)$,
- $u_{i}=0$ for all $i \geq i_{s(u)}+2$.

For example, if $u$ has nonzero entries at positions $3,4,5,8,9$ and the rest are 0 then $I(u)=\{3,5,8\}$ and $s(u)=3$.

Observe that for any row vector $u$, the skeleton size $s(u)$ is at most $n / 2$ and indices of the nonzero entries of $u$ form a subset of $I(u) \cup(I(u)+1)$. Thus, the number of nonzero elements in $u$ is at most $2 s(u)$.
The number of nonzero intervals $S(u)$ is controlled by the skeleton size $s(u)$ as follows.
Lemma 3.3. Let $u$ be a nonzero $1 \times(n-1)$ vector in $(\mathbb{Z} / q \mathbb{Z})^{n-1}$. Then for every $n \geq 3$ and $q \geq 2$, we have

$$
S(u) \geq s(u)(n-s(u)) .
$$

Furthermore, the number of nonzero intervals with one or both endpoints belonging to $I(u) \cup(I(u) \pm 1)$ is at least $s(u)(n-s(u))$.

Proof. Let the skeleton of $u$ be $I(u)=\left\{i_{1}, i_{2}, \ldots, i_{s(u)}\right\}$ with $i_{1}<i_{2}<\cdots<i_{s(u)}$. We first claim that the number of nonzero intervals $[i, j]$ with either $j \in\left\{i_{1}-1, i_{1}\right\}$ or $i \in\left\{i_{1}, i_{1}+1\right\}$ or both ${ }^{2}$ is at least $n-1$.


Indeed, let $1 \leq t \leq n-1$ be any index. If $t<i_{1}$ then either $\left[t, i_{1}-1\right]$ or $\left[t, i_{1}\right]$ is a nonzero interval. If $t=i_{1}$ then $\left[t, i_{1}\right]$ is a nonzero interval. If $t>i_{1}$ then $\left[i_{1}, t\right]$ or $\left[i_{1}+1, t\right]$ is a nonzero interval.

Applying the same argument for $i_{2}$ in place of $i_{1}$ and $t$ running from 1 to $n-1$ except for $t=i_{1}, i_{1}+1$ (to avoid double counting), we obtain at least $n-3$ other nonzero intervals $[i, j]$ with either $j \in\left\{i_{2}-1, i_{2}\right\}$ or $i \in\left\{i_{2}, i_{2}+1\right\}$ or both. Keep running this argument for $i_{3}, \ldots, i_{s(u)}$ gives

$$
(n-1)+(n-3)+(n-5)+\cdots+(n-2 s(u)+1)=n s(u)-s(u)^{2}
$$

nonzero intervals as claimed.

Using a similar argument, we can control the number nonzero boxes by the number of nonzero intervals.

Lemma 3.4. Assume that an $(n-1) \times(n-1)$ matrix $y$ has some nonzero rows $i_{1}, i_{2}, \ldots, i_{k}$ with $\left|i_{m}-i_{l}\right| \geq 2$ for all $m \neq l$. Let $S_{m}$ be the number of nonzero intervals of row $i_{m}$. Then for every $n \geq 3$ and $q \geq 2$, we have

$$
N(y) \geq S_{1}(n-1)+S_{2}(n-3)+\cdots+S_{k}(n-2 k+1)
$$

Proof. Consider a nonzero interval $[p, q]$ of row $i_{m}$ for some $1 \leq p \leq q \leq n-1$ and $1 \leq m \leq k$. For each $1 \leq r \leq i_{m}-1$, either the box $\left[r, i_{m}-1\right] \times[p, q]$ or the box $\left[r, i_{m}\right] \times[p, q]$ is a nonzero box. Similarly, for each $i_{m}+1 \leq r \leq n-1$, either the box $\left[i_{m}+1, r\right] \times[p, q]$ or the box $\left[i_{m}, r\right] \times[p, q]$ is a nonzero box. For $r=i_{m}$, the box $\left[i_{m}, r\right] \times[p, q]$ is itself a nonzero box. Thus, each nonzero interval $[p, q]$ contributes at least $n-1$ nonzero boxes that touch $3^{3}$ the columns $p, q$ and either touch the row $i_{m}$ or the row $i_{m}-1$ from above or the row $i_{m}+1$ from below. Taking union over all nonzero intervals of row $i_{m}$, there are at least $S_{m}(n-1)$ nonzero boxes that either touch the row $i_{m}$ or the row $i_{m}-1$ from above or the row $i_{m}+1$ from below. Taking union over $m$ and subtracting the multiple-counted boxes, we conclude that the number of nonzero boxes is at least $S_{1}(n-1)+S_{2}(n-3)+\cdots+S_{k}(n-2 k+1)$.

Now, we give an upper bound on the number of matrices $y$ with $o\left(n^{3}\right)$ nonzero boxes.
Lemma 3.5. Let $0<\varepsilon_{n} \leq \frac{1}{80}$ be any number. Let $w$ be a positive integer satisfying $1 \leq w \leq \varepsilon_{n} n$. Then for every $n \geq 3$ and $q \geq 2$, the number of $(n-1) \times(n-1)$ matrices $y$ in $\mathbb{Z} / q \mathbb{Z}$ with

$$
\begin{equation*}
N(y) \leq\left(w+\frac{1}{2}\right) n^{2} \tag{18}
\end{equation*}
$$

is at most $q^{32 w} n^{2 w+1+60 \varepsilon_{n} w}$.

[^2]Moreover, if $w \leq \min \left\{\frac{1}{100 \varepsilon_{n}}, \varepsilon_{n} n\right\}$, the number of such matrices $y$ is at most $q^{32 w} n^{2 w}$. Also, for such $w$, the number of matrices $y$ with

$$
\begin{equation*}
N(y) \leq\left(w-40 w \varepsilon_{n}\right) n^{2} \tag{19}
\end{equation*}
$$

is at most $q^{16 w} n^{2(w-1)}$.
In the above statement, only the constant 2 in $n^{2 w}$ is important. All of the other constants $16,32,80,100$ are merely for explicitness. Their exact values do not play any significant role. This also holds for other (big) constants in the rest of the proof.

Proof. To prove the first part of the lemma, let $y$ be an $(n-1) \times(n-1)$ matrix satisfying (18). Let $i_{1}<i_{2}<\cdots<i_{p}$ be some nonzero rows of $y$ with $i_{m} \geq i_{m-1}+2$ for each $m$. For each row $i$, let $S_{i}$ be the number of nonzero interval in that row and $0 \leq s_{i} \leq \frac{n}{2}$ be the size of the its skeleton. By Lemma 3.3, $S_{i} \geq s_{i}\left(n-s_{i}\right)$. Note that $s_{i_{j}} \geq 1$ for all $j=1, \ldots, p$ as they are nonzero rows. By applying Lemma 3.4 to the row $i_{j}$, we get

$$
\left(w+\frac{1}{2}\right) n^{2} \geq S_{i_{j}}(n-1)
$$

which together with Lemma 3.3 give

$$
\left(w+\frac{1}{2}\right) n^{2} \geq s_{i_{j}}\left(n-s_{i_{j}}\right)(n-1) .
$$

Thus, for each $j=1, \ldots, p$,

$$
\begin{equation*}
s_{i_{j}} \leq 2 s_{i_{j}}\left(1-\frac{s_{i_{j}}}{n}\right) \leq 4 w \leq 4 \varepsilon_{n} n \tag{20}
\end{equation*}
$$

By applying Lemma 3.4 to the rows $i_{1}, \ldots, i_{p}$, we get

$$
\begin{equation*}
\left(w+\frac{1}{2}\right) n^{2} \geq S_{i_{1}}(n-1)+S_{i_{2}}(n-3)+\cdots+S_{i_{p}}(n-2 p+1) \tag{21}
\end{equation*}
$$

and by Lemma 3.3 ,

$$
\begin{equation*}
\left(w+\frac{1}{2}\right) n^{2} \geq s_{i_{1}}\left(n-s_{i_{1}}\right)(n-1)+s_{i_{2}}\left(n-s_{i_{2}}\right)(n-3)+\cdots+s_{i_{p}}\left(n-s_{i_{p}}\right)(n-2 p+1) . \tag{22}
\end{equation*}
$$

Combining (20) and (22), we obtain

$$
\begin{equation*}
w+\frac{1}{2} \geq \sum_{j=1}^{p} s_{i_{j}}\left(1-\frac{s_{i_{j}}}{n}\right)\left(1-\frac{2 j-1}{n}\right) \geq \sum_{j=1}^{p} s_{i_{j}}\left(1-4 \varepsilon_{n}\right)\left(1-\frac{2 j-1}{n}\right) \tag{23}
\end{equation*}
$$

Thus,

$$
w+\frac{1}{2} \geq\left(1-4 \varepsilon_{n}\right) \sum_{j=1}^{p}\left(1-\frac{2 j-1}{n}\right)=\left(1-4 \varepsilon_{n}\right) p\left(1-\frac{p}{n}\right) \geq p / 4
$$

because $p \leq n / 2$ by the assumption that $i_{m} \geq i_{m-1}+2$ for $m=2, \ldots, p$. So, $p \leq 4 w+2 \leq 6 \varepsilon_{n} n$. Plugging this into (23), we obtain

$$
\begin{equation*}
\left(w+\frac{1}{2}\right)\left(1+20 \varepsilon_{n}\right) \geq\left(w+\frac{1}{2}\right)\left(1-4 \varepsilon_{n}\right)^{-1}\left(1-12 \varepsilon_{n}\right)^{-1} \geq \sum_{j=1}^{p} s_{i_{j}} \geq p \tag{24}
\end{equation*}
$$

We conclude that if there are $p$ nonzero rows whose indices are of distance at least 2 from each other, then $p \leq\left(w+\frac{1}{2}\right)\left(1+20 \varepsilon_{n}\right)$. Let

$$
f(w)=\left\lfloor\left(w+\frac{1}{2}\right)\left(1+20 \varepsilon_{n}\right)\right\rfloor .
$$

Note that $f(w) \leq 2 w \leq n / 2$. Thus, there are at most

$$
\sum_{p=1}^{f(w)}\binom{n}{p} 2^{p} \leq f(w)\binom{n}{f(w)} 2^{f(w)}
$$

ways to choose the indices of the nonzero rows of $y$, and it's always true that there are at most $2 f(w)$ nonzero rows. Similarly, there are at most that many ways to choose the indices of the nonzero columns of $y$. Let $\mathcal{I}$ be the set of the chosen columns. We have $|\mathcal{I}| \leq 2 f(w)$. Applying (24) to the sequence of chosen rows with odd indices $i_{1}, \ldots, i_{p}$, we see that the number of ways to choose the corresponding value $s_{i_{j}}$ for these rows is at most the number of ways to choose a sequence of positive integers $s_{i_{1}}, \ldots, s_{i_{p}}$ satisfying (24) for some value $p$. And that number is at most

$$
\sum_{a=1}^{f(w)} \sum_{p=1}^{a} \left\lvert\,\left\{\left(s_{i_{1}}, \ldots, s_{i_{p}}: s_{i_{1}}+\cdots+s_{i_{p}}=a\right\} \left\lvert\,=\sum_{a=1}^{f(w)} \sum_{p=1}^{a}\binom{a-1}{p-1}=\sum_{a=1}^{f(w)} 2^{a-1} \leq 2^{f(w)} .\right.\right.\right.
$$

Having chosen the $s_{i}$ for the rows with odd indices, by the definition of skeletons and the fact that the nonzero entries lie on the columns in $\mathcal{I}$ and (24), the number of ways to choose these rows in $(\mathbb{Z} / q \mathbb{Z})^{n-1}$ is at most

$$
\begin{equation*}
\prod_{j=1}^{p} q^{2 s_{i}}\binom{|\mathcal{I}|}{s_{i}} \leq \prod_{j=1}^{p} q^{2 s_{i}}|\mathcal{I}|^{s_{i}} \leq q^{2 f(w)}(2 f(w))^{f(w)} \tag{25}
\end{equation*}
$$

Similarly for the rows with even indices.
All in all, the number of choices for $y$ is at most

$$
\left[f(w)\binom{n}{f(w)} 2^{f(w)}\right]^{2}\left[2^{f(w)}\right]^{2}\left[q^{2 f(w)}(2 f(w))^{f(w)}\right]^{2} \leq q^{32 w} n^{2 f(w)} \leq q^{32 w} n^{2 w+1+60 \varepsilon_{n} n}
$$

Now, for the second part of the lemma, if $w \leq \frac{1}{100 \varepsilon_{n}}$ then $f(w) \leq w+\frac{5}{6}$. In that case, $f(w) \leq w$ because both are integers. Thus, the number of matrices $y$ satisfying (18) is at most $q^{32 w} n^{2 w}$ as claimed. To bound the number of matrices $y$ that satisfy (19), we use the same argument, with $w+1 / 2$ being replaced by $w-40 w \varepsilon_{n}$ throughout. We conclude that the number of matrices $y$ satisfying (19) is at most $q^{16 w} n^{2 f(w)}$ where $f(w)$ is the integer part of

$$
\left(w-40 w \varepsilon_{n}\right)\left(1+20 \varepsilon_{n}\right),
$$

which is strictly less than $w$. Therefore, $f(w) \leq w-1$. This completes the proof.
To handle the matrices with a large number of nonzero boxes, we need a stronger version of Lemma 3.4.

Lemma 3.6. Let $y$ be an $(n-1) \times(n-1)$ matrix. Let $\Psi_{i}$ be a collection of nonzero intervals on each row $i$ such that for every two consecutive rows $i$ and $i+1$, we have that $\Psi_{i} \cap \Psi_{i+1}=\emptyset$. Then for every $n \geq 3$ and $q \geq 2$, it holds that

$$
\begin{equation*}
2 N(y) \geq\left(\left|\Psi_{1}\right|+\left|\Psi_{2}\right|+\cdots+\left|\Psi_{n-1}\right|\right) n . \tag{26}
\end{equation*}
$$

Proof. For each row $i$, let $\mathfrak{P}_{i}$ be the collection of nonzero boxes of the form $[i, j] \times[k, l]$ or $[i+1, j] \times$ $[k, l]$ where $j \geq i+1$ and $[k, l] \in \Psi_{i}$ together with the nonzero boxes $[i, i] \times[k, l]$ (for all $[k, l] \in \Psi_{i}$ ). Note that for each $[k, l] \in \Psi_{i}$, since the interval $[k, l]$ is a nonzero interval in row $i$, either $[i, j] \times[k, l]$ or $[i+1, j] \times[k, l]$ must be a nonzero box. Thus, $\left|\mathfrak{P}_{i}\right| \geq|\{j: j \geq i+1\}|\left|\Psi_{i}\right|+\left|\Psi_{i}\right|=(n-i)\left|\Psi_{i}\right|$. By the hypothesis, the $\left(\mathfrak{P}_{i}\right)_{i=1}^{n-1}$ are disjoint. Thus,

$$
\begin{equation*}
N(y) \geq \sum_{i=1}^{n-1}\left|\mathfrak{P}_{i}\right| \geq \sum_{i=1}^{n-1}(n-i)\left|\Psi_{i}\right| . \tag{27}
\end{equation*}
$$

Likewise, let $\mathfrak{Q}_{j}$ be the collection of nonzero boxes of the form $[j, i] \times[k, l]$ or $[j, i-1] \times[k, l]$ where $j \leq i-1$ and $[k, l] \in \Psi_{i}$ together with the nonzero boxes $[i, i] \times[k, l]$ (for all $[k, l] \in \Psi_{i}$ ). Then the $\mathfrak{Q}_{i}$ are disjoint and $\left|\mathfrak{Q}_{i}\right| \geq i\left|\Psi_{1}\right|$. Therefore,

$$
\begin{equation*}
N(y) \geq \sum_{i=1}^{n-1}\left|\mathfrak{Q}_{i}\right| \geq \sum_{i=1}^{n-1} i\left|\Psi_{i}\right| . \tag{28}
\end{equation*}
$$

Adding up (27) and (28), we obtain the desired bound.

Now, we bound the number of matrices $y$ with a large number of nonzero boxes.
Lemma 3.7. Let $\varepsilon_{n}$ be a positive number satisfying $\frac{1}{\sqrt{\log n}} \leq \varepsilon_{n} \leq \frac{1}{80}$. Let $w \geq \varepsilon_{n} n$ be an integer. For every $n \geq 3$ and $q \geq 2$, the number of $(n-1) \times(n-1)$ matrices $y$ with

$$
\begin{equation*}
N(y) \leq\left(w+\frac{1}{2}\right) n^{2} \tag{29}
\end{equation*}
$$

is at most $n^{2 w+C_{1} \varepsilon_{n} w}$ where $C_{1}=\frac{200 \log q}{\varepsilon_{n} \sqrt{\log n}}+80$.
Proof. We will treat the "big" rows and "small" rows separately.
Step 1: Big rows. A row $i$ is said to be a big row if either $S_{i-1} \geq \varepsilon_{n} n\left(n-\varepsilon_{n} n\right)$ or $S_{i} \geq \varepsilon_{n} n\left(n-\varepsilon_{n} n\right)$ or $S_{i+1} \geq \varepsilon_{n} n\left(n-\varepsilon_{n} n\right)$ where $S_{j}$ is the number of nonzero interval of row $j$. In other words, either row $i$ or $i \pm 1$ has a large number of nonzero intervals.

Let $\mathcal{B}$ be the set of indices $i$ of the big rows in $y$.
Let $M$ be the number of rows $i$ with

$$
\begin{equation*}
S_{i} \geq \varepsilon_{n} n\left(n-\varepsilon_{n} n\right) \geq \varepsilon_{n} n^{2} / 2 . \tag{30}
\end{equation*}
$$

Assume that there is a sequence of rows $i_{1}<i_{2}<\cdots<i_{p}$ satisfying with $i_{m} \geq i_{m-1}+2$. By (21), we get

$$
\left(w+\frac{1}{2}\right) n^{2} \geq \frac{1}{2} \varepsilon_{n} n^{2}[(n-1)+\ldots(n-2 p+1)]=\frac{1}{2} \varepsilon_{n} n^{2} p(n-p) \geq \varepsilon_{n} n^{2} \frac{p n}{4} .
$$

Thus, $p \leq \frac{4\left(w+\frac{1}{2}\right)}{\varepsilon_{n} n} \leq 6 w$. And so,

$$
\begin{equation*}
M \leq 2 p \leq \frac{12 w}{\varepsilon_{n} n} . \tag{31}
\end{equation*}
$$

Since $|\mathcal{B}| \leq 3 M \leq \frac{36 w}{\varepsilon_{n} n}$, the number of ways to choose the set $\mathcal{B}$ and the realizations of the rows with indices belonging to $\mathcal{B}$ is at most

$$
\begin{equation*}
2^{n}\left(q^{n-1}\right)^{36 w /\left(\varepsilon_{n} n\right)} \leq 2^{n} q^{36 w / \varepsilon_{n}} \leq n^{40 w \varepsilon_{n}(\log q) / a^{2}} \leq n^{40 w \varepsilon_{n}(\log q) / a} \tag{32}
\end{equation*}
$$

where $a=\varepsilon_{n} \sqrt{\log n}$ and in the last 2 inequalities, we used the assumption that $a \geq 1$.
Step 2: Small rows. It's left to control the set of small rows $[1, n-1] \backslash \mathcal{B}=: \mathcal{S}$. We will use Lemma 3.6 for which we need to define the $\Psi_{i}$ carefully.

## Step 2.1: Definition of $\Psi_{i}$ and $r_{i}$.

For $i \in \mathcal{B}$, we set $\Psi_{i}=\emptyset$. For $i \in \mathcal{S}$, we consider the cases that $i$ is odd and even separately and define $\Psi_{i}$ (and another quantity denoted by $r_{i}$, which is in essence, the skeleton size of row $i$ ) differently for each case.

Assume that $i \in \mathcal{S}$ is odd. Let $I_{i}$ be the skeleton of row $i$ and $r_{i}:=\left|I_{i}\right|$. Note that by Lemma 3.3, the fact that $r_{i} \leq n / 2$ and the assumption that row $i \in \mathcal{S}, r_{i} \leq \varepsilon_{n} n$. For an odd index $i$, let $\Psi_{i}$ be the collection of nonzero intervals of row $i$ with one or both endpoints belonging to the set $\mathcal{I}_{i}:=I_{i} \cup\left(I_{i} \pm 1\right)$. By Lemma 3.3,

$$
\begin{equation*}
\left|\Psi_{i}\right| \geq r_{i}\left(n-r_{i}\right) \geq r_{i}\left(n-\varepsilon_{n} n\right) . \tag{33}
\end{equation*}
$$

Assume that $i \in \mathcal{S}$ is even. Note that the $\Psi_{i \pm 1}$ are defined in Step 2.1.1. Let $\mathcal{K}_{i}=\mathcal{I}_{i-1}^{c} \cap \mathcal{I}_{i+1}^{c}$. Observe that any interval $\left[h, h^{\prime}\right]$ with $h, h^{\prime} \in \mathcal{K}_{i}$, it holds that $\left[h, h^{\prime}\right]$ does not belong to $\Psi_{i-1} \cup \Psi_{i+1}$. Define $\Psi_{i}$ to be the collection of nonzero intervals with both endpoints in $\mathcal{K}_{i}$. This guarantees that the assumption of Lemma 3.6 is satisfied.
To define $r_{i}$, let $\mathcal{L}_{i}=\mathcal{J}_{i-1}^{c} \cap \mathcal{J}_{i+1}^{c}$, where $\mathcal{J}_{j}:=I_{j} \cup\left(I_{j} \pm 1\right) \cup\left(I_{j} \pm 2\right)$. We have $\mathcal{L}_{i} \subset \mathcal{K}_{i}$ and

$$
\begin{equation*}
\left|\mathcal{K}_{i}\right| \geq\left|\mathcal{L}_{i}\right| \geq n-5\left|I_{i-1}\right|-5\left|I_{i+1}\right| \geq n-5 r_{i-1}-5 r_{i+1} \geq n-10 \varepsilon_{n} n . \tag{34}
\end{equation*}
$$

We consider a version of skeleton $\tilde{\mathcal{I}}_{i}=\left\{i_{1}, i_{2}, \ldots, i_{s}\right\}$ restricted to the set $\mathcal{L}_{i}$ as follows. Let $u=\left(y_{i, 1}, \ldots, y_{i, n-1}\right) \in(\mathbb{Z} / q \mathbb{Z})^{n-1}$ be the vector of row $i$. Let $i_{1}$ be the smallest index in $\mathcal{L}_{i}$ such that $u_{i_{1}} \neq 0$. Let $i_{k}$ be the smallest index such that $i_{k} \in \mathcal{L}_{i}, i_{k} \geq i_{k-1}+2$ and $u_{i_{k}} \neq 0$ for all $2 \leq k \leq s$. Here $s$ is the largest index for which this process has to stop, meaning, $u_{h}=0$ for all $h$ satisfying both $h \geq i_{s}+2$ and $h \in \mathcal{L}_{i}$. Set $r_{i}:=s$. Observe that $r_{i} \leq \varepsilon_{n} n$ because $i \in \mathcal{S}$ and $r_{i}$ is at most the size of the skeleton of row $i$.

By the same argument as in the proof of Lemma 3.3, the number of nonzero intervals with both endpoints belonging to the set $\left\{i_{1}, i_{1} \pm 1, \ldots, i_{r_{i}}, i_{r_{i}} \pm 1\right\}$ or one endpoint in this set and the other in $\mathcal{K}_{i}$ is at least $r_{i}\left(\left|\mathcal{K}_{i}\right|-r_{i}\right)$. By the definition of $\mathcal{L}_{i}$, this set is a subset of $\mathcal{K}_{i}$, and so all such intervals belong to $\Psi_{i}$. Therefore,

$$
\left|\Psi_{i}\right| \geq r_{i}\left(\left|\mathcal{K}_{i}\right|-r_{i}\right) .
$$

From that and (34), we get

$$
\begin{equation*}
\left|\Psi_{i}\right| \geq r_{i}\left(n-10 \varepsilon_{n} n-r_{i}\right) \geq r_{i}\left(n-11 \varepsilon_{n} n\right) . \tag{35}
\end{equation*}
$$

Applying Lemma 3.6 together with the equations (33) and (35), we have

$$
(2 w+1) n^{2} \geq 2 N(y) \geq\left(\left|\Psi_{1}\right|+\cdots+\left|\Psi_{n-1}\right|\right) n \geq \sum_{i \in \mathcal{S}} r_{i}\left(n-11 \varepsilon_{n} n\right) n
$$

which gives that

$$
\begin{equation*}
\sum_{i \in \mathcal{S}} r_{i} \leq \frac{2 w+1}{1-11 \varepsilon_{n}} \leq 2 w+44 w \varepsilon_{n}+2 \tag{36}
\end{equation*}
$$

## Step 2.2: Realizations of small rows.

Choosing the $r_{i}$. The number of sequences $\left(r_{i}\right)_{i \in \mathcal{S}}$ of nonnegative integers satisfying (36) is at most the number of nonnegative integer solutions to $r_{1}+r_{2}+\cdots+r_{n-1}=a$ for some $a \leq$ $2 w+44 w \varepsilon_{n}+2$ and is thus bounded by

$$
\begin{equation*}
\sum_{a=0}^{2 w+44 w \varepsilon_{n}+2}\binom{a+n-2}{n-2} \leq 7 w\binom{6 w+2 n}{n} \leq 7 w\left(\frac{6 e w+2 e n}{n}\right)^{n} \leq n^{24 \varepsilon_{n} w} \tag{37}
\end{equation*}
$$

where we used the assumptions that $a=\varepsilon_{n} \sqrt{\log n} \geq 1$ and $w \geq \varepsilon_{n} n$.
Realizations of odd rows $i$. For each choice of the set $\mathcal{B}$, the realizations of rows $j$ with $j \in \mathcal{B}$, and the sequence $\left(r_{i}\right)_{i \in \mathcal{S}}$, we need to bound the number of realizations of rows $i$ with $i \in \mathcal{S}$.

If $i \in \mathcal{S}$ is odd, then by the definition of skeletons, the number of realizations of row $i$ with a given $r_{i}$, the size of its skeleton, is at most

$$
\begin{equation*}
\binom{n}{r_{i}} q^{2 r_{i}} \tag{38}
\end{equation*}
$$

Realizations of even rows $i$. Having chosen all of the rows $i^{\prime}$ with $i^{\prime}$ being odd, for each even index $i \in \mathcal{S}$, note that the set $\mathcal{L}_{i}$, defined earlier in the proof, is fixed as the rows $i \pm 1$ (odd) have been chosen. The number of choices for the restricted skeleton $\tilde{\mathcal{I}}_{i}$ is at most $\binom{n}{r_{i}}$. The number of realizations of row $i$ inside the set $\mathcal{L}_{i}$ with a given $\tilde{\mathcal{I}}_{i}$ is at most $q^{2 r_{i}}$. The number of realizations of row $i$ inside the set $\mathcal{L}_{i}^{c}$ is at most $q^{\left|\mathcal{L}_{i}^{c}\right|} \leq q^{5 r_{i-1}+5 r_{i+1}}$ by (34). Thus, the number of realizations of row $i$ given $r_{i}, r_{i \pm 1}$ and the rows with odd indices is at most

$$
\begin{equation*}
\binom{n}{r_{i}} q^{2 r_{i}+5 r_{i-1}+5 r_{i+1}} \tag{39}
\end{equation*}
$$

Combining. From (38), and (39), the number of realizations of rows $i$ with $i \in \mathcal{S}$ is at most

$$
\begin{align*}
& \prod_{i \in \mathcal{S}, i=2 k+1}\binom{n}{r_{i}} q^{2 r_{i}} \prod_{i \in \mathcal{S}, i=2 k}\binom{n}{r_{i}} q^{2 r_{i}+5 r_{i-1}+5 r_{i+1}} \leq \\
& \exp \left(\log n \sum_{i \in \mathcal{S}} r_{i}+12 \log q \sum_{i \in \mathcal{S}} r_{i}\right) \leq n^{2 w+45 \varepsilon_{n} w+160 w \varepsilon_{n}(\log q) / a} \tag{40}
\end{align*}
$$

where in the last inequality, we used 36 .
Combining (32), (37) and (40), we obtain the stated lemma.

Finally, we are ready to prove (17) which completes the proof of the upper bound of Theorem 1.2 ,

Lemma 3.8. Let $\alpha_{n}=\log \log (16 n) \sqrt{\log n}$. Let $c$ be any number satisfying $c \geq \frac{640}{\log \log (16 n)}$. Let $t=\frac{n^{2}}{4\left(1-\cos \frac{2 \pi}{q}\right)} \log n+\frac{n^{2}}{\left(1-\cos \frac{2 \pi}{q}\right)} c \alpha_{n} \log q$. We have for all $n \geq 3$ and $q \geq 2$,

$$
\begin{equation*}
\Sigma=\sum\left(1-\frac{(1-\cos 2 \pi / q) N(y)}{\binom{n}{2}^{2}}\right)^{2 t} \leq q^{-2 c} / 2 \tag{41}
\end{equation*}
$$

where the sum is taken over all matrices $y \neq 0$ with $N(y) \leq \frac{\binom{n}{2}^{2}}{1-\cos \frac{2 \pi}{q}}$.
Proof. Let $\varepsilon_{n}=\frac{1}{100 \sqrt{\log n}}$ chosen with foresight. We break up the left-hand side of 411) into sums $T_{1}, T_{2}$ where

- $T_{1}$ is the sum over all $y$ with $1 \leq N(y) \leq \frac{n^{2}}{100 \varepsilon_{n}}$,
- $T_{2}$ is the sum over all $y$ with $\frac{n^{2}}{100 \varepsilon_{n}} \leq N(y) \leq \frac{\binom{n}{2}^{2}}{1-\cos 2 \pi / q}$.

Observe that for these matrices $y$,

$$
0 \leq 1-\frac{(1-\cos 2 \pi / q) N(y)}{\binom{n}{2}^{2}} \leq \exp \left(-\frac{4(1-\cos 2 \pi / q) N(y)}{n^{4}}\right) .
$$

Bound $T_{1}$. Note that by combining Lemmas 3.3 and 3.4, every nonzero matrix $y$ has $N(y) \geq$ $(n-1)^{2} \geq(1-1 / 2) n^{2}$. Thus $T_{1} \leq T_{1,1}+T_{1,2}$ where

$$
\begin{aligned}
& T_{1,1}=\sum_{w=1}^{1 /\left(100 \varepsilon_{n}\right)}\left|\left\{y:\left(w-\frac{1}{2}\right) n^{2}<N(y) \leq\left(w-40 w \varepsilon_{n}\right) n^{2}\right\}\right| \exp \left(-\frac{8(1-\cos 2 \pi / q) t\left(w-\frac{1}{2}\right)}{n^{2}}\right) \\
& T_{1,2}=\sum_{w=1}^{1 /\left(100 \varepsilon_{n}\right)}\left|\left\{y:\left(w-40 w \varepsilon_{n}\right) n^{2}<N(y) \leq\left(w+\frac{1}{2}\right) n^{2}\right\}\right| \exp \left(-\frac{8(1-\cos 2 \pi / q) t\left(w-40 w \varepsilon_{n}\right)}{n^{2}}\right)
\end{aligned}
$$

Since $\varepsilon_{n} \leq \frac{1}{80}$, applying the second part of Lemma 3.5 , we deduce that

$$
T_{1,1} \leq \sum_{w=1}^{1 /\left(100 \varepsilon_{n}\right)} q^{16 w} n^{2 w-2} \exp \left(-\frac{8(1-\cos 2 \pi / q) t\left(w-\frac{1}{2}\right)}{n^{2}}\right) \leq \sum_{w=1}^{\infty} q^{(16-4 c \alpha) w} \leq \frac{q^{-2 c}}{8}
$$

and

$$
T_{1,2} \leq \sum_{w=1}^{1 /\left(100 \varepsilon_{n}\right)} q^{32 w} n^{2 w} \exp \left(-\frac{8(1-\cos 2 \pi / q) t\left(w-40 w \varepsilon_{n}\right)}{n^{2}}\right) \leq \sum_{w=1}^{\infty} q^{(32-c \alpha / 4) w} \leq \frac{q^{-2 c}}{8}
$$

where we use the fact that $\alpha \geq 1$ and $c \alpha \geq 640 \sqrt{\log n}$. Thus, $T_{1} \leq q^{-2 c} / 4$.
Bound $T_{2}$. We have $T_{2} \leq T_{2,1}+T_{2,2}$ where
$T_{2,1}=\sum_{w=1 /\left(100 \varepsilon_{n}\right)}^{\varepsilon_{n} n}\left|\left\{y:\left(w-\frac{1}{2}\right) n^{2}<N(y) \leq\left(w+\frac{1}{2}\right) n^{2}\right\}\right| \exp \left(-\frac{8(1-\cos 2 \pi / q) t\left(w-\frac{1}{2}\right)}{n^{2}}\right)$,

$$
T_{2,2}=\sum_{w=\varepsilon_{n} n}^{\infty}\left|\left\{y:\left(w-\frac{1}{2}\right) n^{2}<N(y) \leq\left(w+\frac{1}{2}\right) n^{2}\right\}\right| \exp \left(-\frac{8(1-\cos 2 \pi / q) t\left(w-\frac{1}{2}\right)}{n^{2}}\right),
$$

Since $\varepsilon_{n} \leq \frac{1}{80}$, applying the first part of Lemma 3.5 to $T_{2,1}$ yields

$$
T_{2,1} \leq \sum_{w=1 /\left(100 \varepsilon_{n}\right)}^{\infty} q^{32 w} n^{2 w+1+60 \varepsilon_{n} w} \exp \left(-\frac{8(1-\cos 2 \pi / q) t\left(w-\frac{1}{2}\right)}{n^{2}}\right) \leq \frac{q^{-2 c}}{8}
$$

where we used the fact that $c \alpha \log q \geq 320 \varepsilon_{n} \log n$.
Applying the first part of Lemma 3.7 to $T_{2,2}$ yields

$$
T_{2,1} \leq \sum_{w=\varepsilon_{n} n}^{\infty} n^{2 w+C_{1} \varepsilon_{n} w} \exp \left(-\frac{8(1-\cos 2 \pi / q) t\left(w-\frac{1}{2}\right)}{n^{2}}\right) \leq \frac{q^{-2 c}}{8} .
$$

where $C_{1}$ is as in Lemma 3.7 and we used the fact that $C_{1} \varepsilon_{n} \leq \frac{300 \log q}{\sqrt{\log n}}$ and that $c \alpha \log q \geq 640 \sqrt{\log n}$. Thus, $T_{2} \leq q^{-2 c} / 4$ which together with the bound on $T_{1}$ complete the proof.

## References

[1] W. Baldoni-Silva, J. A. De Loera, and M. Vergne. Counting integer flows in networks. Found. Comput. Math., 4(3):277-314, 2004.
[2] Alexander Barvinok. Brunn-Minkowski inequalities for contingency tables and integer flows. Adv. Math., 211(1):105-122, 2007.
[3] Alexander Barvinok. Enumerating contingency tables via random permanents. Combin. Probab. Comput., 17(1):1-19, 2008.
[4] Alexander Barvinok. Asymptotic estimates for the number of contingency tables, integer flows, and volumes of transportation polytopes. Int. Math. Res. Not. IMRN, (2):348-385, 2009.
[5] Alexander Barvinok. What does a random contingency table look like? Combin. Probab. Comput., 19(4):517-539, 2010.
[6] Alexander Barvinok and J. A. Hartigan. Maximum entropy Gaussian approximations for the number of integer points and volumes of polytopes. Adv. in Appl. Math., 45(2):252-289, 2010.
[7] Alexander Barvinok and J. A. Hartigan. An asymptotic formula for the number of nonnegative integer matrices with prescribed row and column sums. Trans. Amer. Math. Soc., 364(8):4323-4368, 2012.
[8] Alexander Barvinok and John A Hartigan. The number of graphs and a random graph with a given degree sequence. Random Structures \& Algorithms, 42(3):301-348, 2013.
[9] Alexander Barvinok, Zur Luria, Alex Samorodnitsky, and Alexander Yong. An approximation algorithm for counting contingency tables. Random Structures Algorithms, 37(1):25-66, 2010.
[10] Edward A. Bender. The asymptotic number of non-negative integer matrices with given row and column sums. Discrete Math., 10:217-223, 1974.
[11] Edward A Bender and E Rodney Canfield. The asymptotic number of labeled graphs with given degree sequences. Journal of Combinatorial Theory, Series A, 24(3):296-307, 1978.
[12] Ivona Bezáková, Nayantara Bhatnagar, and Eric Vigoda. Sampling binary contingency tables with a greedy start. In Proceedings of the Seventeenth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 414-423. ACM, New York, 2006.
[13] Ivona Bezáková, Nayantara Bhatnagar, and Eric Vigoda. Sampling binary contingency tables with a greedy start. Random Structures Algorithms, 30(1-2):168-205, 2007.
[14] Ivona Bezáková, Alistair Sinclair, Daniel ` Stefankovi` c, and Eric Vigoda. Negative examples for sequential importance sampling of binary contingency tables. In Algorithms-ESA 2006, volume 4168 of Lecture Notes in Comput. Sci., pages 136-147. Springer, Berlin, 2006.
[15] Ivona Bezáková, Alistair Sinclair, Daniel ` Stefankovi` c, and Eric Vigoda. Negative examples for sequential importance sampling of binary contingency tables. Algorithmica, 64(4):606-620, 2012.
[16] Jose Blanchet and Alexandre Stauffer. Characterizing optimal sampling of binary contingency tables via the configuration model. Random Structures Algorithms, 42(2):159-184, 2013.
[17] Joseph Blitzstein and Persi Diaconis. A sequential importance sampling algorithm for generating random graphs with prescribed degrees. Internet Math., 6(4):489-522, 2010.
[18] Béla Bollobás. A probabilistic proof of an asymptotic formula for the number of labelled regular graphs. European Journal of Combinatorics, 1(4):311-316, 1980.
[19] E. Rodney Canfield, Catherine Greenhill, and Brendan D. McKay. Asymptotic enumeration of dense 0-1 matrices with specified line sums. J. Combin. Theory Ser. A, 115(1):32-66, 2008.
[20] Yuguo Chen, Persi Diaconis, Susan P. Holmes, and Jun S. Liu. Sequential Monte Carlo methods for statistical analysis of tables. J. Amer. Statist. Assoc., 100(469):109-120, 2005.
[21] Yuguo Chen, Ian H. Dinwoodie, and Seth Sullivant. Sequential importance sampling for multiway tables. Ann. Statist., 34(1):523-545, 2006.
[22] F. R. K. Chung, R. L. Graham, and S.-T. Yau. On sampling with Markov chains. In Proceedings of the Seventh International Conference on Random Structures and Algorithms (Atlanta, GA, 1995), volume 9, pages 55-77, 1996.
[23] Mary Cryan and Martin Dyer. A polynomial-time algorithm to approximately count contingency tables when the number of rows is constant. J. Comput. System Sci., 67(2):291-310, 2003. Special issue on STOC2002 (Montreal, QC).
[24] Mary Cryan, Martin Dyer, Leslie Ann Goldberg, Mark Jerrum, and Russell Martin. Rapidly mixing Markov chains for sampling contingency tables with a constant number of rows. SIAM J. Comput., 36(1):247-278, 2006.
[25] Mary Cryan, Martin Dyer, and Dana Randall. Approximately counting integral flows and cell-bounded contingency tables. SIAM J. Comput., 39(7):2683-2703, 2010.
[26] Persi Diaconis. Group representations in probability and statistics, volume 11 of Institute of Mathematical Statistics Lecture Notes - Monograph Series. Institute of Mathematical Statistics, Hayward, CA, 1988.
[27] Persi Diaconis. Threads through group theory. In Character theory of finite groups, volume 524 of Contemp. Math., pages 33-47. Amer. Math. Soc., Providence, RI, 2010.
[28] Persi Diaconis and Bradley Efron. Testing for independence in a two-way table: new interpretations of the chi-square statistic. Ann. Statist., 13(3):845-913, 1985. With discussions and with a reply by the authors.
[29] Persi Diaconis and Bradley Efron. Probabilistic-geometric theorems arising from the analysis of contingency tables. In Contributions to the theory and application of statistics, pages 103-125. Academic Press, Boston, MA, 1987.
[30] Persi Diaconis and Anil Gangolli. Rectangular arrays with fixed margins. In Discrete probability and algorithms (Minneapolis, MN, 1993), volume 72 of IMA Vol. Math. Appl., pages 15-41. Springer, New York, 1995.
[31] Persi Diaconis and Laurent Saloff-Coste. Comparison techniques for random walk on finite groups. Ann. Probab., 21(4):2131-2156, 1993.
[32] Persi Diaconis and Laurent Saloff-Coste. Comparison theorems for reversible Markov chains. Ann. Appl. Probab., 3(3):696-730, 1993.
[33] Persi Diaconis and Bernd Sturmfels. Algebraic algorithms for sampling from conditional distributions. Ann. Statist., 26(1):363-397, 1998.
[34] Martin Dyer and Catherine Greenhill. Polynomial-time counting and sampling of two-rowed contingency tables. Theoret. Comput. Sci., 246(1-2):265-278, 2000.
[35] Martin Dyer, Ravi Kannan, and John Mount. Sampling contingency tables. Random Structures Algorithms, 10(4):487-506, 1997.
[36] Catherine Greenhill and Brendan D. McKay. Asymptotic enumeration of sparse nonnegative integer matrices with specified row and column sums. Adv. in Appl. Math., 41(4):459-481, 2008.
[37] Diane Hernek. Random generation of $2 \times n$ contingency tables. Random Structures Algorithms, 13(1):71-79, 1998.
[38] Anita Liebenau and Nick Wormald. Asymptotic enumeration of graphs by degree sequence, and the degree sequence of a random graph. arXiv preprint arXiv:1702.08373, 2017.
[39] Tomomi Matsui, Yasuko Matsui, and Yoko Ono. Random generation of $2 \times 2 \times \cdots \times 2 \times J$ contingency tables. Theoret. Comput. Sci., 326(1-3):117-135, 2004.
[40] Brendan D McKay and Nicholas C Wormald. Asymptotic enumeration by degree sequence of graphs of high degree. European Journal of Combinatorics, 11(6):565-580, 1990.
[41] Brendan D McKay and Nicholas C Wormald. Asymptotic enumeration by degree sequence of graphs with degrees $o\left(n^{1 / 2}\right)$. Combinatorica, 11(4):369-382, 1991.
[42] Brendan D McKay and Nicholas C Wormald. The degree sequence of a random graph. i. the models. Random Structures and Algorithms, 11(2):97-117, 1997.
[43] Ben Morris. Improved bounds for sampling contingency tables. In Randomization, approximation, and combinatorial optimization (Berkeley, CA, 1999), volume 1671 of Lecture Notes in Comput. Sci., pages 121-129. Springer, Berlin, 1999.
[44] George W. Soules. New permanental upper bounds for nonnegative matrices. Linear Multilinear Algebra, 51(4):319-337, 2003.
[45] David Bruce Wilson. Mixing times of Lozenge tiling and card shuffling Markov chains. Ann. Appl. Probab., 14(1):274-325, 2004.
[46] Nicholas C Wormald. Models of random regular graphs. London Mathematical Society Lecture Note Series, pages 239-298, 1999.


[^0]:    *Department of Mathematics, Princeton University, USA, emails: exn@princeton.edu, onguyen@princeton.edu.

[^1]:    ${ }^{1}$ The lower bound of Theorem 1.2 is in fact stronger than this.

[^2]:    ${ }^{2}$ This guarantees that one or both endpoints of $[i, j]$ belong to the set $\left\{i_{1}, i_{1} \pm 1\right\}$.
    ${ }^{3}$ We say that a box touches a row or a column if it has that row or column as a boundary. In other words, the box $[i, j] \times[k, l]$ touches rows $i, j$ and columns $k, l$.

