Adjacency matrices of random digraphs: singularity and anti-concentration

Alexander E. Litvak Anna Lytova Konstantin Tikhomirov
Nicole Tomczak-Jaegermann Pierre Youssef

Abstract

Let $\mathcal{D}_{n,d}$ be the set of all d-regular directed graphs on n vertices. Let G be a graph chosen uniformly at random from $\mathcal{D}_{n,d}$ and M be its adjacency matrix. We show that M is invertible with probability at least $1 - C \ln^3 d/\sqrt{d}$ for $C \le d \le cn/\ln^2 n$, where c, C are positive absolute constants. To this end, we establish a few properties of d-regular directed graphs. One of them, a Littlewood–Offord type anti-concentration property, is of independent interest. Let J be a subset of vertices of G with $|J| \approx n/d$. Let δ_i be the indicator of the event that the vertex i is connected to J and define $\delta = (\delta_1, \delta_2, ..., \delta_n) \in \{0,1\}^n$. Then for every $v \in \{0,1\}^n$ the probability that $\delta = v$ is exponentially small. This property holds even if a part of the graph is "frozen."

AMS 2010 Classification: 60C05, 60B20, 05C80, 15B52, 46B06.
Keywords: Adjacency matrices, anti-concentration, invertibility, Littlewood–Offord theory, random digraphs, random graphs, random matrices, regular graphs, singular probability, singularity, sparse matrices

Contents

1 Introduction

For $1 \leq d \leq n$ an undirected (resp., directed) graph G is called *d-regular* if every vertex has exactly d neighbors (resp., d in-neighbors and d out-neighbors). In this definition we allow graphs to have loops and, for directed graphs, opposite (anti-parallel) edges, but no multiple edges. Thus directed graphs (*digraphs*) can be viewed as bipartite graphs with both parts of size n. For a digraph G with n vertices its *adjacency matrix* $(\mu_{ij})_{i,j\leq n}$ is defined by

$$\mu_{ij} = \begin{cases} 1, & \text{if there is an edge from } i \text{ to } j; \\ 0, & \text{otherwise.} \end{cases}$$

For an undirected graph G its adjacency matrix is defined in a similar way (in the latter case the matrix is symmetric). We denote the sets of all undirected (resp., directed) d-regular graphs by $\mathcal{G}_{n,d}$ and $\mathcal{D}_{n,d}$, respectively, and the corresponding sets of adjacency matrices by $\mathcal{S}_{n,d}$ and $\mathcal{M}_{n,d}$. Clearly $\mathcal{S}_{n,d} \subset \mathcal{M}_{n,d}$ and $\mathcal{M}_{n,d}$ coincides with the set of $n \times n$ matrices with $0/1$-entries and such that every row and every column has exactly d ones. By the probability on $\mathcal{G}_{n,d}$, $\mathcal{D}_{n,d}$, $\mathcal{S}_{n,d}$, and $\mathcal{M}_{n,d}$ we always mean the normalized counting measure.

Spectral properties of adjacency matrices of random d-regular graphs attracted considerable attention of researchers in the recent years. Among others, we refer the reader to [2], [3], [12], [14], [26], and [35] for results dealing with the eigenvalue distribution. At the same time, much less is known about the singular values of the matrices.

The present work is motivated by related general questions on singular probability. One problem was mentioned by Vu in his survey [37, Problem 8.4] (see also 2014 ICM talks by Frieze and Vu [15, Problem 7], [38, Conjecture 5.8]). It asks if for $3 \leq d \leq n-3$ the probability that a random matrix uniformly distributed on $\mathcal{S}_{n,d}$ is singular goes to zero as n grows to infinity. Note that in the case $d = 1$ the matrix is a permutation matrix, hence non-singular; while in the case $d = 2$ the conjecture fails (see [37] and, for the directed case, [9]). Note also that $M \in \mathcal{M}_{n,d}$ is singular if and only if the "complementary" matrix $M' \in \mathcal{M}_{n,n-d}$ obtained by interchanging zeros and ones is singular, thus the cases $d = d_0$ and $d = n - d_0$ are essentially the same. The corresponding question for non-symmetric adjacency matrices is the following (cf., [9, Conjecture 1.5]):

Is it true that for every $3 \leq d \leq n-3$

$$p_{n,d} := \mathbb{P}_{\mathcal{M}_{n,d}}\left(\{M \in \mathcal{M}_{n,d} : M \textit{ is singular}\}\right) \longrightarrow 0 \quad \textit{as} \quad n \to \infty? \qquad (*)$$

The main difficulty in such singularity questions stems from the restrictions on row- and column-sums, and from possible symmetry constraints for the entries. The question $(*)$ has been recently studied in [9] by Cook who obtained the bound $p_{n,d} \leq d^{-c}$ for a small universal constant $c > 0$ and d satisfying $\omega(\ln^2 n) \leq d \leq n - \omega(\ln^2 n)$, where $f \geq \omega(a_n)$ means $f/a_n \to \infty$ as $n \to \infty$.

The main result of our paper is the following theorem.

Theorem A. *There are absolute positive constants c, C such that for $C \leq d \leq cn/\ln^2 n$ one has*

$$p_{n,d} \leq \frac{C \ln^3 d}{\sqrt{d}}.$$

Thus we proved that $p_{n,d} \to 0$ as $d \to \infty$, which in particular verifies $(*)$ whenever d grows to infinity with n, without any restrictions on the rate of convergence. (Recall that the proof in [9] requires $d \geq \omega(\ln^2 n)$.) We would also like to notice that even for the range $\omega(\ln^2 n) \leq d \leq cn/\ln^2 n$, our bound on probability in Theorem A is better than in [9]. Of course, it would be nice to obtain a bound going to zero with n and not with d for the range $d \geq 3$ as well.

In the remaining part of the introduction we describe methods and techniques used in this paper. We also explain several novel ideas that allow us to drop the restriction $d \geq \omega(\ln^2 n)$ and to treat very sparse matrices. In particular, we introduce the notion of *almost constant* vectors and show how to eliminate matrices having almost constant null vectors; we show a new approximation argument dealing with tails of properly rescaled vectors; we prove an anti-concentration property for graphs, which is of independent interest; and we provide a more delicate version of the so-called "shuffling" technique.

This paper can be naturally split into two distinct parts. In the first one we establish certain properties of random d-regular digraphs. In the second part we use them (or to be more precise, their "matrix" equivalents) to deal with the singularity of adjacency matrices. However in the introduction we reverse this order and discuss first the "matrix" part as it provides a general perspective and motivations for graph results.

Singularity of random square matrices is a subject with a long history and many results. In [21] (see also [22]) Komlós proved that a random $n \times n$ matrix with independent ± 1 entries (*Bernoulli* matrix) is singular with probability tending to zero as $n \to \infty$. Upper bounds for the singular probability of random Bernoulli matrices were successively improved to c^n (for some $c \in (0,1)$) in [18]; to $\big(3/4 + o(1)\big)^n$ in [34]; and to $\big(1/\sqrt{2} + o(1)\big)^n$ in [6]. Recall that the conjectured bound is $\big(1/2 + o(1)\big)^n$. The corresponding problem for symmetric Bernoulli matrices was considered in [11], [27], [36]. Recently, matrices with independent rows and with row-sums constrained to be equal to zero were studied in [28].

In all these works, a fundamental role is played by what is nowadays called *the Littlewood-Offord theory.* In its classical form, established by Erdős [13], the Littlewood-Offord inequality states that for every fixed $z \in \mathbb{R}$, a fixed vector $a = (a_1, a_2, \ldots, a_n) \in \mathbb{R}^n$ with non-zero coordinates, and for independent random signs r_k, $k \leq n$, the probability $\mathbb{P}\left\{\sum_{k=1}^n r_k a_k = z\right\}$

is bounded from above by $n^{-1/2}$. This combinatorial result has been substantially strengthened and generalized in subsequent years, leading to a much better understanding of interrelationship between the law of the sum $\sum_{k=1}^{n} r_k a_k$ and the arithmetic structure of the vector a. For more information and further references, we refer the reader to [32], [33, Section 3], and [29, Section 4]. The use of the Littlewood-Offord theory in context of random matrices can be illustrated as follows. Given an $n \times n$ matrix A with i.i.d. elements, A is non-singular if and only if the inner product of a normal vector to the span of any subset of $n-1$ columns of A with the remaining column is non-zero. Thus, knowing the "typical" arithmetic structure of the random normal vectors and conditioning on their realization, one can estimate the probability that A is singular. Moreover, a variant of this approach allows us to obtain sharp quantitative estimates for the smallest singular value of the matrix with independent subgaussian entries [30].

Similarly to the aforementioned works, the Littlewood-Offord inequality plays a crucial role in the proof of Theorem A. Note that if M is a random matrix uniformly distributed on $\mathcal{M}_{n,d}$ then every two entries/rows/columns of M are probabilistically dependent; moreover, a realization of the first $n-1$ columns uniquely defines the last column of M. This makes a straightforward application of the Littlewood-Offord theory (as illustrated in the previous paragraph) impossible.

In [9], a sophisticated approach based on the "shuffling" of two rows was developed to deal with that problem. The shuffling consists in a random perturbation of two rows of a fixed matrix $M \in \mathcal{M}_{n,d}$ in such a way that the sum of the rows remains unchanged. We discuss this procedure in more details in Section 4.3. It can be also defined in terms of "switching" discussed below. The proof in [9] can be divided into two steps: at the first step, one proves that the event that a random matrix M does not have any (left or right) null vectors with many ($\geq Cnd^{-c}$) equal coordinates has probability close to one, provided that $d \geq \omega(\ln^2 n)$. Then one shows that conditioned on this event, a random matrix M is non-singular with large probability.

In our paper, we expand on some of the techniques developed in [9] by adding new crucial ingredients. On the first step, in Section 4.1, we show that for $C \leq d \leq cn$, with probability going to one with n, a random matrix M does not have any null vectors having at least $n(1 - 1/\ln d)$ equal coordinates, (we call such vectors *almost constant*). Note that we rule out a much smaller set of null vectors. This allows us to drop the lower bound on d, but requires a delicate adjustment of the second step. Key elements of the first step consists of a new *anti-concentration* property of random graphs and their adjacency matrices as well as of using a special form of an ε-net build from the "tails" of appropriately rescaled vectors $x \in \mathbb{R}^n$. Then, conditioning on the event that M does not have almost constant null vectors, we show in Section 4.3 that a random matrix M is non-singular with high probability. This relies on a somewhat modified and simplified version of the shuffling procedure for the matrix rows. As the shuffling involves supports of only two rows we get at this step that probability converges with d and not with n. We would like to emphasize that this is the only step which does not allow to have the convergence to zero with n.

We now turn our attention to Section 2, which deals with the set $\mathcal{D}_{n,d}$ of d-regular digraphs. Our analysis is based on an operation called "the simple switching," which is a standard tool to work with regular graphs. As an illustration, let $G \in \mathcal{D}_{n,d}$ and let $i_1 \neq i_2$ and $j_1 \neq j_2$ be vertices of G such that (i_1, j_1) and (i_2, j_2) are edges of G and (i_1, j_2), (i_2, j_1) are not. Then the simple switching consists in replacing the edges (i_1, j_1), (i_2, j_2) with (i_1, j_2) and (i_2, j_1), while leaving all other edges unchanged. Note that the operation does not destroy d-regularity of the graph. The simple switching was introduced (for general graphs) by Senior [31] (in that paper, it was called "transfusion"); in the context of d-regular graphs it was first applied by McKay [25]. As in [25], we use this operation to compare cardinalities of certain subsets of $\mathcal{D}_{n,d}$. We note that one could use the configuration model, introduced by Bollobàs [4] in the context of random regular graphs, to prove our results for sparse graphs. We prefer to use the switching method in order to have a unified proof for all ranges of d.

As in the matrix counterpart we work with a random graph G uniformly distributed on $\mathcal{D}_{n,d}$. For a finite set S, we denote by $|S|$ its cardinality. For a positive integer n we denote by $[n]$ the set $\{1, 2, \ldots, n\}$. For every subset $S \subset [n]$, let $\mathcal{N}_G^{in}(S)$ be the set of all vertices of G which are in-neighbors to some vertex in S. Further, for every two subsets I, J of $[n]$, we denote by $E_G(I, J)$ the collection of edges of G starting from a vertex in I and ending at a vertex from J. In a simplified form, our first statement about graphs (Theorem 2.2 in Section 2.2) can be formulated as follows:

Let $8 \le d \le n$, $\varepsilon \in (0,1)$, and $k \ge 2$. Assume that $\varepsilon^2 \ge d^{-1} \max\{8, \ln d\}$ and $k \le c\varepsilon n/d$ for a sufficiently small absolute positive constant c. Then

$$\mathbb{P}\big\{\exists S \subseteq [n],\, |S| = k \text{ such that } \big|\mathcal{N}_G^{in}(S)\big| \le (1-\varepsilon) d \big|S\big|\big\} \le \exp\left(-\frac{\varepsilon^2 dk}{8} \ln\left(\frac{3ec\varepsilon n}{kd}\right)\right).$$

Note that $|S| \le \big|\mathcal{N}_G^{in}(S)\big| \le d|S|$. Thus, roughly speaking, our result says that "typically," whenever a set S is not too large, the set of all in-neighbors of S has cardinality close to the maximal possible one. In the case of undirected graphs such results are known (see e.g. [1] and references therein). We note that in fact we prove a more general statement, in which we estimate the probability conditioning on a "partial" realization of a random graph G, when a certain subset of its edges is fixed (see Theorem 2.2).

In our second result, we estimate the probability that $E_G(I, J)$ is empty for large sets I and J (see Theorem 2.6 in Section 2.3):

There exist absolute positive constants c, C such that the following holds. Let $2 \le d \le n/24$ and $Cn \ln d/d \le \ell \le r \le n/4$. Then

$$\mathbb{P}\big\{E_G(I, J) = \emptyset \text{ for some } I, J \subset [n] \text{ with } |I| \ge \ell,\ |J| \ge r\big\} \le \exp\left(-cr\ell d/n\right).$$

Note that the first statement can be reformulated in terms of sets $E_G(I, J)$ (however, the range of cardinalities for I and J will be different compared to the second result). These statements can be seen as manifestations of a general phenomenon that a random graph G with a large probability has good regularity properties. Let us also note that analogous statements for the Erdős–Rényi graphs (in this random model an edge between every two vertices is included/excluded in a graph independently of other edges) follow from standard Bernstein-type inequalities. For related results on d-regular random graphs, we refer the reader to [23] where concentration properties of *co-degrees* were established in the undirected setting, and to [8] for concentration of co-degrees and of the "edge counts" $|E_G(I,J)|$ for digraphs. In paper [8] which serves as a basis for the main theorem of [9] mentioned above, rather strong concentration properties of $|E_G(I,J)|$ are established; however, the results provided in that paper are valid only for $d \geq \omega(\ln n)$. The proof in [9] is based on the method of exchangeable pairs introduced by Stein and developed for concentration inequalities by Chatterjee (see survey [7] for more information and references). On the contrary, our proof of the afore-mentioned statements is simpler, completely self-contained and works for $d \geq C$. As we mentioned above, we use the following Littlewood-Offord type anti-concentration result matching anti-concentration properties of a weighted sum of independent random variables or vectors studied in the Littlewood-Offord theory. This result is of independent interest, and we formulate it here as a theorem (see also Theorem 2.15 in Section 2.4). For every $J \subset [n]$ and $i \in [n]$ we define $\delta_i^J(G) \in \{0,1\}$ as the indicator of the event $\{i \in \mathcal{N}_G^{in}(J)\}$ and denote $\delta^J(G) := (\delta_1^J(G), \ldots, \delta_n^J(G)) \in \{0,1\}^n$.

Theorem B. *There are two positive absolute constants c and c_1 such that the following holds. Let $32 \leq d \leq cn$ and I, J be disjoint subsets of $[n]$ such that $|I| \leq d|J|/32$ and $8 \leq |J| \leq 8cn/d$. Let vectors $a^i \in \{0,1\}^n$, $i \in I$, be such that the event*

$$\mathcal{E} := \{\mathcal{N}_G^{in}(i) = \operatorname{supp} a^i \text{ for all } i \in I\}$$

has non-zero probability (if $I = \emptyset$ we set $\mathcal{E} = \mathcal{D}_{n,d}$). Then for every $v \in \{0,1\}^n$ one has

$$\mathbb{P}\{\delta^J(G) = v \mid \mathcal{E}\} \leq 2 \exp\left(-c_1 d|J| \ln\left(\frac{n}{d|J|}\right)\right).$$

We note that the probability estimate in the previous statement matches the one for the corresponding quantity δ^J in the Erdős–Rényi model.

The paper is organized as follows. Sections 2 deals with all results related to graphs. Section 3 provides links between the graph results of Section 2 and the matrix results used in Section 4. Finally, Section 4 presents the proof of the main theorem, including a number of auxiliary combinatorial lemmas.

In this paper letters c, C, c_0, C_0, c_1, C_1, ... always denote absolute positive constants (i.e. independent of any parameters), whose precise value may be different from line to line.

Main results of this paper were announced in [24].

Aknowledgment. This work was conducted while the second named author was a Research Associate at the University of Alberta, the third named author was a graduate student and held the PIMS Graduate Scholarship, and the last named author was a CNRS/PIMS PDF at the same university. They all would like to thank the Pacific Institute and the University of Alberta for the support. A part of this work was also done when the first four authors took part in activities of the annual program "On Discrete Structures: Analysis and Applications" at the Institute for Mathematics and its Applications (IMA), Minneapolis, MN, USA. These authors would like to thank IMA for the support and excellent working conditions. All authors would like to thank Michael Krivelevich for many helpful comments on the "graph" part of this paper. We would also like to thank Justin Salez for helpful comments.

2 Expansion and anti-concentration for random digraphs

2.1 Notation and preliminaries

For a real number x, we denote by $\lfloor x \rfloor$ the largest integer smaller than or equal to x and by $\lceil x \rceil$ the smallest integer larger than or equal to x. Further, for every $a \geq 1$, we denote by $[a]$ the set $\{i \in \mathbb{N} : \ 1 \leq i \leq \lfloor a \rfloor\}$.

Let $d \leq n$ be positive integers. A *d-regular directed graph* (or *d-regular digraph*) on n (labeled) vertices is a graph in which every vertex has exactly d in-neighbors and d out-neighbors. We allow the graphs to have loops and opposite/anti-parallel edges but do not allow multiple edges. Thus this set coincides with the set of d-regular bipartite graphs with both parts of size n. The set of vertices of such graphs is always identified with $[n]$. The set of all these graphs is denoted by $\mathcal{D}_{n,d}$. When n and d are clear from the context, we will use a one-letter notation $\mathcal{D}$. Note that the set of adjacency matrices for graphs in $\mathcal{D}$ coincides with the set of $n \times n$ matrices with 0/1-entries such that every row and every column has exactly d ones. By a random graph on $\mathcal{D}$ we always mean a graph uniformly distributed on $\mathcal{D}$ (that is, with respect to the normalized counting measure).

Let $G = ([n], E)$ be an element of $\mathcal{D}$, where E is the set of its directed edges. Thus $(i, j) \in E$, $i, j \leq n$, means that there is an edge going from vertex i to vertex j. We will denote the adjacency matrix of G by $M = M(G)$; its rows and columns by $R_i = R_i(M) = R_i(G)$ and $X_i = X_i(M) = X_i(G)$, $i \leq n$, respectively.

Given a graph $G \in \mathcal{D}$ and a subset $S \subset [n]$ of its vertices, let

$$\mathcal{N}^{out}(S) = \mathcal{N}^{out}_G(S) := \big\{v \leq n : \ \exists i \in S \ (i, v) \in E\big\} = \bigcup_{i \in S} \mathrm{supp} R_i,$$
$$\mathcal{N}^{in}(S) = \mathcal{N}^{in}_G(S) := \big\{v \leq n : \ \exists i \in S \ (v, i) \in E\big\} = \bigcup_{i \in S} \mathrm{supp} X_i.$$

Similarly, we define the out-edges and the in-edges as follows

$$E^{out}_G(S) := \big\{e \in E : \ e = (i, j) \text{ for some } i \in S \text{ and } j \leq n\big\},$$
$$E^{in}_G(S) := \big\{e \in E : \ e = (i, j) \text{ for some } i \leq n \text{ and } j \in S\big\}.$$

For one-element subsets of $[n]$ we will use lighter notations $\mathcal{N}^{out}_G(i)$, $\mathcal{N}^{in}_G(i)$, $E^{out}_G(i)$, $E^{in}_G(i)$ instead of $\mathcal{N}^{out}_G(\{i\})$, $\mathcal{N}^{in}_G(\{i\})$, $E^{out}_G(\{i\})$, $E^{in}_G(\{i\})$.

Given a graph $G = ([n], E)$, for every $I, J \subset [n]$ the set of all edges departing from I and landing in J is denoted by

$$E_G(I \times J) = E_G(I, J) = \big\{e \in E : \ e = (i, j) \text{ for some } i \in I \text{ and } j \in J\big\}.$$

Further, we let

$$\mathcal{D}^0(I, J) = \big\{G \in \mathcal{D} : \ E_G(I, J) = \emptyset\big\}.$$

Note that $\mathcal{D}^0(I, J)$ is the set of all graphs whose adjacency matrices have zero $I \times J$-minor, hence the superscript "0".

Given $G \in \mathcal{D}$, for $u, v \le n$ the sets of common out-neighbors and common in-neighbors will be denoted as

$$\mathrm{C}^{\mathrm{out}}_{\mathrm{G}}(u,v) = \{j \le n \,:\, (u,j),(v,j) \in E\} = \operatorname{supp} R_u \cap \operatorname{supp} R_v,$$
$$\mathrm{C}^{\mathrm{in}}_{\mathrm{G}}(u,v) = \{i \le n \,:\, (i,u),(i,v) \in E\} = \operatorname{supp} X_u \cap \operatorname{supp} X_v.$$

For every $S \subset [n]$ and $F \subset [n] \times [n]$, we define

$$\mathcal{D}(S,F) = \big\{G \in \mathcal{D} :\, E^{in}_G(S) = F\big\}.$$

Informally speaking, $\mathcal{D}(S,F)$ is the subset of d-regular graphs for which the in-edges of S are "frozen" and, as a set, coincide with F. Note that a necessary (but not sufficient) condition for $\mathcal{D}(S,F)$ to be non-empty is

$$\forall i \le n \quad |\{\ell \in [n] :\, (i,\ell) \in F\}| \le d \qquad \text{and} \qquad \forall j \in S \quad |\{\ell \in [n] :\, (\ell,j) \in F\}| = d.$$

For every $\varepsilon \in (0,1)$, denote

$$\mathcal{D}^{co}(\varepsilon) = \big\{G \in \mathcal{D} :\, \forall i \ne j \le n \quad |\mathrm{C}^{\mathrm{out}}_{\mathrm{G}}(i,j)| \le \varepsilon d\big\} = \bigcap_{i<j} \mathcal{D}^{co}_{i,j}(\varepsilon),$$

where

$$\mathcal{D}^{co}_{i,j}(\varepsilon) := \big\{G \in \mathcal{D} :\, |\mathrm{C}^{\mathrm{out}}_{\mathrm{G}}(i,j)| \le \varepsilon d\big\}.$$

Let A, B be sets, and $R \subset A \times B$ be a relation. Given $a \in A$ and $b \in B$, the image of a and preimage of b are defined by

$$R(a) = \{y \in B \,:\, (a,y) \in R\} \qquad \text{and} \qquad R^{-1}(b) = \{x \in A \,:\, (x,b) \in R\}.$$

We also set $R(A) = \cup_{a \in A} R(a)$. Further in this section, we often define relations between sets in order to estimate their cardinality, using the following simple claim.

Claim 2.1. *Let $s, t > 0$. Let R be a relation between two finite sets A and B such that for every $a \in A$ and every $b \in B$ one has $|R(a)| \ge s$ and $|R^{-1}(b)| \le t$. Then*

$$s|A| \le t|B|.$$

Proof. Without loss of generality we assume that $A = [k]$ and $B = [m]$ for some positive integers k and m. For $i \le k$ and $j \le m$, we set $r_{ij} = 1$ if $(i,j) \in R$ and $r_{ij} = 0$ otherwise. Counting the number of ones in every row and every column of the matrix $\{r_{ij}\}_{ij}$ we obtain

$$\sum_{i=1}^{k}\sum_{j=1}^{m} r_{ij} = \sum_{i=1}^{k} |R(i)| \ge sk = s|A| \qquad \text{and} \qquad \sum_{j=1}^{m}\sum_{i=1}^{k} r_{ij} = \sum_{j=1}^{m} |R^{-1}(j)| \le tm = t|B|,$$

which implies the desired estimate. □

2.2 An expansion property of random digraphs

In this section, we establish certain expansion properties of random graphs uniformly distributed on $\mathcal{D}$, which can roughly be described as follows: given a subset $S \subset [n]$ of cardinality $|S| \leq cn/d$, with high probability the number of in-neighbors of S is of order $d|S|$. Beside its own interest, this result is used in the proof of the anti-concentration property for graphs which will be given in Section 2.4. In fact we will need a statement where we control the number of in-neighbors of a subset of vertices while "freezing" (i.e. conditioning on a realization of) a set of edges inside the graph.

Theorem 2.2. *Let $8 \leq d \leq n$, $\varepsilon \in (0,1)$, and $k \geq 2$. Assume that*

$$\varepsilon^2 \geq \frac{\max\{8, \ln d\}}{d} \quad \textit{and} \quad k \leq \frac{c\varepsilon n}{d}$$

for a sufficiently small absolute positive constant c. Let $I \subset [n]$ be of cardinality at most $n/8$. Define

$$\Gamma_k = \left\{G \in \mathcal{D} : \exists S \subseteq I^c,\, |S| = k, \quad \textit{such that } \ \left|\mathcal{N}_G^{in}(S)\right| \leq (1-\varepsilon)d\left|S\right|\right\}$$

and

$$\Gamma = \left\{G \in \mathcal{D} : \exists S \subseteq I^c,\, |S| \leq c\varepsilon n/d, \quad \textit{such that } \ \left|\mathcal{N}_G^{in}(S)\right| \leq (1-\varepsilon)d\left|S\right|\right\} = \bigcup_{\ell=2}^{c\varepsilon n/d} \Gamma_\ell.$$

Then for every $F \subset [n] \times [n]$ with $\mathcal{D}(I,F) \neq \emptyset$ we have

$$\mathbb{P}\left(\Gamma_k \mid \mathcal{D}(I,F)\right) \leq \exp\left(-\frac{\varepsilon^2 dk}{8} \ln\left(\frac{3ec\varepsilon n}{kd}\right)\right).$$

In particular,

$$\mathbb{P}\left(\Gamma \mid \mathcal{D}(I,F)\right) \leq \exp\left(-\frac{\varepsilon^2 d}{8} \ln\left(\frac{ec\varepsilon n}{d}\right)\right).$$

Let us describe the idea of the proof of Theorem 2.2. Suppose we are given a set of vertices S of an appropriate size. Since $|E_G^{in}(S)| = d|S|$, then we always have

$$|S| \leq |\mathcal{N}_G^{in}(S)| \leq d|S|.$$

We want to prove that the number of graphs satisfying $|\mathcal{N}_G^{in}(S)| \leq (1-\varepsilon)d|S|$ is rather small. In order to estimate the number of in-neighbors of S, our strategy is to build S by adding one vertex at a time and trace how the number of in-neighbors is changing. Namely, if $S = \{v_i\}_{i \leq s}$ then to build S we start by setting $S_1 := \{v_1\}$ – a set for which we know that it has exactly d in-neighbors. Now we add the vertex v_2 to S_1 to get $S_2 := \{v_1, v_2\}$. We need to trace how the number of in-neighbors to S_2 changed compared to that of S_1. More precisely, we need to count the number of graphs for which the number of in-neighbors has increased by at most $(1-\varepsilon/2)d$. To this end, we count the number of graphs having the property that the number of common in-neighbors to v_1 and v_2 is at least $\varepsilon d/2$. We count such graphs by applying the simple switching. One should be careful here to switch the edges without interfering with the frozen area of the graph. We continue in a similar manner by adding one vertex at a time and controlling the number of common in-neighbors between the added vertex and the existing ones. Now, note that the condition $|\mathcal{N}_G^{in}(S)| \leq (1-\varepsilon)d|S|$ implies that for a large proportion of the vertices added, the number of common in-neighbors with the existing vertices is at least $\varepsilon d/2$. We use this together with the cardinality estimates obtained via the simple switching at each step to get the required result.

We use the following notation. Given $S \subset [n]$ and $\delta \in (0,1)$, we set $\Gamma(S, \emptyset) = \mathcal{D}$ and for a non-empty $J \subset [n]$, let

$$\Gamma(S,J) = \Gamma(S,J,\delta) = \Big\{ G \in \mathcal{D} \,:\, \forall j \in J \text{ one has } \Big| \bigcup_{i \in S, i<j} \mathrm{C}^{\mathrm{in}}_{\mathrm{G}}(i,j) \Big| \geq \delta d \Big\}$$

(the number δ will always be clear from the context). We also use a simplified notation $\Gamma(S,j) := \Gamma(S, \{j\})$.

Note that $\Gamma(S,J)$ contains all graphs in which every vertex $j \in J$ has many common in-neighbors with the set $\{i \in S \,:\, i<j\}$. In the next lemma, we estimate cardinalities of $\Gamma(S,j)$, conditioning on a "partial" realization of a graph.

Lemma 2.3. *Let $\delta \in (0,1)$, $2 \leq d \leq n/12$, $1 \leq k \leq \delta n/(4ed)$ and $F, H \subset [n] \times [n]$. For every $I \subset [k+d]^c$ satisfying*
$$|I| \leq \frac{n}{8},$$
one has
$$\big|\Gamma([k], k+1) \cap \mathcal{D}([k], F) \cap \mathcal{D}(I,H)\big| \leq \gamma_k \big|\mathcal{D}([k],F) \cap \mathcal{D}(I,H)\big|,$$
where
$$\gamma_k = \left(\frac{2ekd}{\delta n}\right)^{\delta d}.$$

Less formally, the above statement asserts that, considering a subset of $\mathcal{D}$ with prescribed (frozen) sets of in-edges for $[k]$ and I, for a vast majority of such graphs the $(k+1)$-th vertex will have a small number of common in-neighbors with the first k vertices.

Proof. We assume that the intersection $\mathcal{D}([k],F) \cap \mathcal{D}(I,H)$ is non-empty. Then we have $F([n]) = [k]$ and $F^{-1}([k]) = \mathcal{N}_G^{in}([k])$ (recall notation for images and preimages of a relation). Without loss of generality, $\mathcal{N}_G^{in}([k]) = [n_1]^c$ for some $n_1 \leq n$. Note that

$$k \leq \big|\mathcal{N}_G^{in}([k])\big| \leq kd,$$

hence $n - kd \leq n_1 \leq n-k$.

For $0 \leq q \leq d$ denote

$$Q(q) := \Big\{ G \in \mathcal{D}([k],F) \cap \mathcal{D}(I,H) : \, \big|\mathcal{N}_G^{in}([k]) \cap \mathcal{N}_G^{in}(k+1)\big| = q \Big\}.$$

and

$$Q := \Gamma([k], k+1) \cap \mathcal{D}([k], F) \cap \mathcal{D}(I, H) = \bigcup_{q=\lceil \delta d \rceil}^{d} Q(q).$$

We proceed by comparing the cardinalities $Q(q)$ and $Q(q-1)$ for every $1 \leq q \leq d$. To this end, we will define a relation $R_q \subset Q(q) \times Q(q-1)$. Let $G \in Q(q)$. Then there exist $n_1 < i_1 < \ldots < i_q$ such that for every $\ell \leq q$ we have

$$i_\ell \in \mathcal{N}_G^{in}([k]) \cap \mathcal{N}_G^{in}(k+1).$$

For every $\ell \leq q$, there are at most d^2 edges inside $E_G\big([n_1], \mathcal{N}_G^{out}(i_\ell)\big)$. Further, there are $(n_1-(d-q))d$ edges in $E_G^{out}\big([n_1] \setminus \mathcal{N}_G^{in}(k+1)\big)$ and at most $d|I|$ edges in $E_G\big([n_1] \setminus \mathcal{N}_G^{in}(k+1), I\big)$. Therefore, for every $\ell \leq q$, the cardinality of the set

$$E_\ell := E_G\big([n_1] \setminus \mathcal{N}_G^{in}(k+1), I^c \setminus \mathcal{N}_G^{out}(i_\ell)\big)$$

can be estimated as

$$|E_\ell| \geq \big(n_1 - (d-q) - |I|\big)d - d^2 \geq (7n/8 - kd - 2d)d \geq nd/2$$

(here, we used the conditions $|I| \leq n/8$ and $n_1 \geq n - kd$ together with the restrictions on k).

Now, we turn to constructing the relation R_q. We let a pair (G, G') belong to R_q for some $G' \in Q(q-1)$ if G' can be obtained from G in the following way. First we choose $\ell \leq q$ and an edge $(i, j) \in E_\ell$. We destroy the edge $(i_\ell, k+1)$ to form the edge $(i, k+1)$, then destroy the edge (i, j) to form the edge (i_ℓ, j) (in other words, we perform the simple switching on the vertices $i, i_\ell, j, k+1$). Note that the conditions $i \notin \mathcal{N}_G^{in}(k+1)$ and $j \notin \mathcal{N}_G^{out}(i_\ell)$, which are implied by the definition of E_ℓ, guarantee that the simple switching does not create multiple edges, and we obtain a valid graph in $Q(q-1)$.

The definition of R_q implies that for every $G \in Q(q)$ one has

$$|R_q(G)| \geq \sum_{\ell=1}^{q} |E_\ell| \geq \frac{qnd}{2}. \tag{1}$$

Now we estimate the cardinalities of preimages. Let $G' \in R_q\big(Q(q)\big)$. In order to reconstruct a graph G for which $(G, G') \in R_q$, we need to perform a simple switching which

$$\text{destroys an edge from} \quad E_{G'}\big([n_1], k+1\big) \qquad \text{and} \qquad \text{adds an edge to} \quad E_{G'}\big([n_1]^c, k+1\big).$$

There are at most $d - q + 1$ choices to destroy an edge in $E_{G'}\big([n_1], k+1\big)$, and at most $n - n_1 \leq kd$ possibilities to create an edge connecting $[n_1]^c$ with $(k+1)$-st vertex. Assume that we destroyed an edge $(v, k+1)$ and added an edge $(u, k+1)$. The second part of the simple switching is to destroy an excessive out-edge of u and create a corresponding edge (with the same end-point) for v. It is easy to see that we have at most d possibilities for the second part of the switching. Therefore,

$$\big|R_q^{-1}(G')\big| \leq kd^3.$$

Using this bound, Claim 2.1, and (1), we obtain that

$$\big|Q(q)\big| \le \left(\frac{2kd^2}{qn}\right) \cdot \big|Q(q-1)\big|$$

and, applying the estimate successively,

$$\big|Q(q)\big| \le \left(\frac{2kd^2}{n}\right)^q \frac{1}{q!} \, \big|Q(0)\big|.$$

Since $q! \ge 2(q/e)^q$ and $2ekd/(\delta n) \le 1/2$, this implies

$$|Q| = \sum_{q=\lceil \delta d \rceil}^{d} \big|Q(q)\big| \le \frac{1}{2} \sum_{q=\lceil \delta d \rceil}^{d} \left(\frac{2ekd}{\delta n}\right)^q \big|Q(0)\big| \le \left(\frac{2ekd}{\delta n}\right)^{\delta d} \big|Q(0)\big|.$$

Using that $Q(0) \subset \mathcal{D}([k], F) \cap \mathcal{D}(I, H)$, we obtain the desired result. □

Now, we iterate the last lemma to obtain the following statement.

Corollary 2.4. *Let δ, n, d, k and γ_k be as in Lemma 2.3 and let $\ell \le k$. Further, let $I \subset [n]$ satisfy $|I| \le n/8$ and let $H \subset [n] \times [n]$. Then for every subsets $J \subset S \subset I^c$ such that $|S| = k$ and $|J| = \ell$, one has*

$$\big|\Gamma(S, J) \cap \mathcal{D}(I, H)\big| \le {\gamma_k}^{\ell} \, \big|\mathcal{D}(I, H)\big|.$$

Proof. Without loss of generality we assume that the intersection $\Gamma(S, J) \cap \mathcal{D}(I, H)$ is non-empty, that $S = [k]$ and $I \subset [k + d]^c$. Write $J = \{j_1, ..., j_\ell\}$ for some $j_1 < ... < j_\ell$. For $1 \le s \le \ell$ denote $J_s = \{j_1, ..., j_s\}$, $J_0 = \emptyset$ and let $k_s = j_s - 1$. Note that for every $1 \le s \le \ell$, we have

$$\Gamma(S, J_s) = \Gamma([k_s], J_s).$$

Note also that

$$\Gamma(S, J_s) = \Gamma([k_s], k_s + 1) \cap \Gamma(S, J_{s-1}). \tag{2}$$

Clearly,

$$\big|\Gamma(S, J) \cap \mathcal{D}(I, H)\big| = |\mathcal{D}(I, H)| \prod_{s=1}^{\ell} \frac{|\Gamma(S, J_s) \cap \mathcal{D}(I, H)|}{|\Gamma(S, J_{s-1}) \cap \mathcal{D}(I, H)|}. \tag{3}$$

For $1 \le s \le \ell$ define

$$\mathcal{F}_s = \{F \subset [n] \times [n] \, : \, \mathcal{D}([k_s], F) \cap \mathcal{D}(I, H) \subset \Gamma(S, J_{s-1})\}.$$

Then by (2) we have

$$\Gamma(S, J_s) \cap \mathcal{D}(I, H) = \bigsqcup_{F \in \mathcal{F}_s} \Gamma([k_s], k_s + 1) \cap \mathcal{D}([k_s], F) \cap \mathcal{D}(I, H).$$

Applying Lemma 2.3 we obtain

$$\begin{aligned}\big|\Gamma(S,J_s)\cap\mathcal{D}(I,H)\big| &= \sum_{F\in\mathcal{F}_s}|\Gamma([k_s],k_s+1)\cap\mathcal{D}([k_s],F)\cap\mathcal{D}(I,H)|\\ &\le \gamma_{k_s}\sum_{F\in\mathcal{F}_s}|\mathcal{D}([k_s],F)\cap\mathcal{D}(I,H)|\\ &\le \gamma_k|\Gamma(S,J_{s-1})\cap\mathcal{D}(I,H)|,\end{aligned}$$

where the last inequality follows from the definition of $\mathcal{F}_s$ and $k_s\le k$. This and (3) imply the result. $\square$

We are now ready to prove Theorem 2.2. In the proof, we will use Corollary 2.4, together with an easy observation that the condition $|\mathcal{N}_G^{in}(S)|\le(1-\varepsilon)d|S|$ for an (ordered) subset S of vertices implies that proportionally many vertices in S have at least $\varepsilon d/2$ common in-neighbors with the union of the preceeding vertices.

Proof of Theorem 2.2. Let $G\in\Gamma_k$ and S be as in the definition of Γ_k. For $j\in S$ consider

$$A_j=\bigcup_{i\in S,i<j}\mathrm{C}^{\mathrm{in}}_{\mathrm{G}}(i,j)$$

and denote by m_j its cardinality. Note that for $j_0=\min\{j\,:\,j\in S\}$ one has $A_{j_0}=\emptyset$ and $m_{j_0}=0$. Note also

$$\big|\mathcal{N}_G^{in}(S)\big|=\sum_{j\in S}(d-m_j).$$

Let $\delta=\varepsilon/2$ and consider $J':=\{j\in S\,:\,m_j\ge\delta d\}$. Since $m_{j_0}=0$,

$$(1-\varepsilon)\,d\,|S|\ge\big|\mathcal{N}_G^{in}(S)\big|\ge\sum_{j\in S\setminus J'}(d-m_j)>(1-\varepsilon/2)\,d\,(|S|-|J'|),$$

which implies

$$|J'|>\frac{\varepsilon}{2-\varepsilon}\,|S|>\frac{\varepsilon}{2}\,|S|.$$

Hence, for every $G\in\Gamma_k$ there exists $S\subset I^c$ with $|S|=k$, and $J\subset S$ such that

$$|J|=\lceil\varepsilon k/2\rceil:=\ell\quad\text{ and }\quad m_j\ge\delta d\ \text{ for all }\ j\in J.$$

Thus

$$\Gamma_k\subset\bigcup_{|S|=k}\ \bigcup_{J\subset S,|J|=\ell}\Gamma(S,J).$$

By Corollary 2.4 we have

$$\big|\Gamma_k\cap\mathcal{D}(I,F)\big|\le\binom{n}{k}\binom{k}{\ell}{\gamma_k}^{\ell}\,|\mathcal{D}(I,F)|\le\left(\frac{en}{k}\right)^k\left(\frac{ek}{\ell}\right)^{\ell}{\gamma_k}^{\ell}\,|\mathcal{D}(I,F)|.$$

We assume that $\varepsilon k \geq 2$ (the case $\varepsilon k < 2$, in which $\ell = 1$, is treated similarly). Using $\varepsilon \geq \max\{\sqrt{\ln d/d}, \sqrt{8/d}\}$, by direct calculations we observe

$$\left(\frac{en}{k}\right)^k \left(\frac{ek}{\ell}\right)^\ell \left(\frac{4ekd}{\varepsilon n}\right)^{\varepsilon d\ell/2} \leq \left(\frac{en}{k}\right)^k \left(\frac{2e}{\varepsilon}\right)^{\varepsilon k/2} \left(\frac{4ekd}{\varepsilon n}\right)^{\varepsilon^2 dk/4} \leq \left(\frac{C_1 kd}{\varepsilon n}\right)^{\varepsilon^2 dk/8}$$

for a sufficiently large absolute constant $C_1 > 0$. Taking $c \leq 1/(3eC_1)$, we obtain the desired estimate for Γ_k. The second assertion of the theorem regarding Γ follows immediately. □

As we have already noted, Theorem 2.2 essentially postulates that a random d-regular digraph typically has good expansion properties in the sense that every sufficiently small subset S of its vertices has almost $d|S|$ in-neighbors and $d|S|$ out-neighbors. In the undirected setting, expansion properties of graphs are a subject of very intense research (see, in particular, [17] and references therein). As the conclusion for this subsection, we would like to recall some of the known expansion properties of undirected random graphs and compare them with the main result of this part of our paper.

Let $G = (V, E)$ be an undirected graph on n vertices. Given a subset $U \subset V$, by $\partial_V U$ we denote a set of all vertices adjacent to the set U but not in U, i.e.

$$\partial_V U := \{i \notin U : \exists j \in U\, (i,j) \in E\} = \mathcal{N}_G^{in}(U) \setminus U.$$

Similarly, let $\partial_E U$ be the set of all edges of G with exactly one endpoint in U. For every $\lambda \in (0, 1]$, we define *the λ-vertex isoperimetric number*

$$i_{\lambda,V}(G) := \min_{|U| \leq \lambda n} \frac{|\partial_V U|}{|U|},$$

and, for every $\lambda \in (0, 1/2]$, *the λ-edge isoperimetric number*

$$i_{\lambda,E}(G) := \min_{|U| \leq \lambda n} \frac{|\partial_E U|}{|U|}.$$

For $\lambda = 1/2$, the above quantities are simply called the vertex and the edge isoperimetric numbers, denoted by $i_V(G)$ and $i_E(G)$. Since $|\partial_V U| \leq |\partial_E U| \leq d|\partial_V U|$, for every $\lambda \in (0, 1/2]$ we have

$$i_{\lambda,V}(G) \leq i_{\lambda,E}(G) \leq d\, i_{\lambda,V}(G). \tag{4}$$

Now, let G be a d-regular graph uniformly distributed on the set $\mathcal{G}_{n,d}$. In [5] it was shown that for large enough fixed d

$$i_E(G) \geq d/2 - \sqrt{d \ln 2}, \tag{5}$$

with probability going to one with n. This result was generalized in [20], where is was shown that

$$i_{\lambda,E}(G) \geq d(1 - \lambda + o(1))$$

with probability going to one with n, where $o(1)$ depends on d and can be made arbitrarily small by increasing d. Note that the relation (4) together with results from [5, 20] immediately implies

$$i_{\lambda,V}(G) \geq 1 - \lambda + o(1)$$

(where the bound should be interpreted in the same way as before), however the bound is far from being optimal. An estimate for the second eigenvalue of G proved in [14] implies that for a fixed d with large probability (going to one with n)

$$i_V(G) \geq 1 - 8/d + O(1/d^2).$$

Moreover, for every d and $\delta > 0$ for small enough $\lambda = \lambda(d, \delta) > 0$ the parameter $i_{\lambda,V}$ (corresponding to expansions of small subsets of V) can be estimated as

$$i_{\lambda,V}(G) \geq d - 2 - \delta$$

(see [17, Theorem 4.16]).

Our main result of this subsection can be interpreted as an expansion property of regular digraphs for small vertex subsets. We define the vertex isoperimetric number $i_{\lambda,V}$ for digraphs by the same formula as for undirected graphs. Theorem 2.2 has the following consequence, which, in particular, provides quantitative estimates of $i_{\lambda,V}$ for d growing together with n to infinity.

Corollary 2.5. *Let $8 \leq d \leq n$ and $\varepsilon \in (0,1)$. Assume that*

$$\varepsilon^2 \geq \frac{\max\{8, \ln d\}}{d}, \quad d \leq \frac{c\varepsilon n}{2} \quad \text{and} \quad \lambda(\varepsilon) := \frac{c\varepsilon}{d}.$$

Further, let G be uniformly distributed on $\mathcal{D}$. Then

$$i_{\lambda(\varepsilon),V}(G) \geq (1-\varepsilon)d - 1$$

with probability at least

$$1 - \exp\left(-\frac{\varepsilon^2 d}{8} \ln\left(\frac{ec\varepsilon n}{d}\right)\right).$$

2.3 On existence of edges connecting large vertex subsets

In this part, we consider the following problem. Let G be uniformly distributed on $\mathcal{D}$ and let I and J be two (large enough) subsets of $[n]$. We want to estimate the probability that G has no edges connecting a vertex from I to a vertex from J. The main result of the subsection is the following theorem.

Theorem 2.6. *There exist absolute constants $c > 0$ and $C, C_1 \geq 1$ such that the following holds. Let $C_1 \leq d \leq n/24$ and let natural numbers ℓ and r satisfy*

$$\frac{n}{4} \geq r \geq \ell \geq \frac{Cn\ln(en/r)}{d}.$$

Then

$$\mathbb{P}\left\{\bigcup \mathcal{D}^0(I,J)\right\} \leq \exp\left(-\frac{cr\ell d}{n}\right),$$

where the union is taken over all $I, J \subset [n]$ with $|I| \geq \ell$ and $|J| \geq r$.

Remark 2.7. Obviously, the roles of ℓ and r in this theorem are interchangeable and the assumptions on ℓ and r imply that $\ell \geq Cn/d$ and $r \geq C_1 n \ln d/d$.

Remark 2.8. We would like to notice that adding an assumption $\ell \geq 4d^2$ in this theorem, we could simplify its proof (we would not need quite technical Lemma 2.12 below)

Remark 2.9. The statement of the theorem can be related to known results on the independence number of random undirected graphs. Recall that the independence number $\alpha(G)$ of a graph G is the cardinality of the largest subset of its vertices such that no two vertices of the subset are adjacent. Suppose now that G is uniformly distributed on $\mathcal{G}_{n,d}$. For $d \to \infty$ with $d \leq n^\theta$ for some fixed $\theta < 1$, it was shown in [16] and [10] that, as n goes to infinity, the ratio $\alpha(G)/\big(2nd^{-1}\ln d\big)$ converges to 1 in probability. Moreover, in [23] it was verified that in the range $n^\theta \leq d \leq 0.9n$ (for a sufficiently large $\theta < 1$), the asymptotic value of $\alpha(G)$ is $2\ln d/\ln(n/(n-d))$, which is equivalent to $2n\ln d/d$ when d/n is small. Taking $I = J$ in Theorem 2.6, we observe a bound of the same order for random digraphs, which can be interpreted as a large deviation estimate for the independence number as follows.

Corollary 2.10. *There exist absolute positive constants c, C such that for every $2 \leq d \leq n/24$ and a random digraph G uniformly distributed on $\mathcal{D}$ one has*

$$\mathbb{P}\left\{\alpha(G) > C\,\frac{n\ln d}{d}\right\} \leq \exp\left(-\frac{cn\ln^2 d}{d}\right).$$

We first give an idea of the proof of Theorem 2.6. Fix two sets of vertices I and J of sizes ℓ and r. Our strategy is to start with two small subsets of I, J and to arrive to I, J by adding one vertex at a time. Suppose that $I_1 \subset I$ and $J_1 \subset J$ and S is a subset of graphs from $\mathcal{D}$ with no edges departing from I_1 and landing in J_1. We add a vertex from $J \setminus J_1$ to J_1 to form a set J_2 and check whether the property of having no edges connecting I_1 to J_2 is preserved, using the simple switching. More precisely, when conditioning on the set of graphs S, we estimate the proportion of graphs in S such that there are no edges departing from I_1 to the vertex added. We perform an analogous procedure by adding a vertex to I_1 and continue until the whole sets I and J are reconstructed.

Note that a similar argument can be applied in the undirected setting to estimate probability of large deviation for the independence number (the sets I and J shall be equal in this situation). We omit the proof of the undirected case as it is a simple adaptation of the argument of Theorem 2.6 and is not of interest in the present paper.

We start with a lemma which can be described as follows: given two sets of vertices $[p]$ and $[k]$, among graphs having no edges departing from $[p]$ to $[k]$, we count how many have no departing edges from $[p]$ to the vertex $k+1$. The proof of Theorem 2.6 will then follow by iterating this lemma.

Lemma 2.11. *Let $20 \leq d \leq n/24$ and $4e^2 n/d \leq p, k \leq n/4$. Then*

$$\max\big\{|\mathcal{D}^0([p],[k+1])|,\ |\mathcal{D}^0([p+1],[k])|\big\} \leq \exp\left(-\frac{pd}{4e^2 n}\right)\,|\mathcal{D}^0([p],[k])|.$$

To prove this lemma we need the following rather technical statement, which shows that for most graphs under consideration every two vertices have a relatively small number of common out-neighbors. For reader's convenience we postpone its proof to the end of this section.

Lemma 2.12. *Let $\varepsilon \in (0,1)$, $0 \le k \le n/4$, $0 \le p \le n$, and $d \le \varepsilon n/12$. Then*

$$\left|\mathcal{D}^0([p],[k]) \setminus \mathcal{D}^{co}(\varepsilon)\right| \le \frac{n^2}{2}\left(\frac{2ed}{\varepsilon n}\right)^{\varepsilon d} \left|\mathcal{D}^0([p],[k])\right|,$$

where $\mathcal{D}^0([p],[k]) = \mathcal{D}$ if $p=0$ or $k=0$.

Proof of Lemma 2.11. We prove the bound for $\mathcal{D}^0([p],[k+1])$, the other bound is obtained by passing to the transpose graph.

Fix $q := \lceil pd/(2e^2 n)\rceil$. Denote

$$Q := \mathcal{D}^0([p],[k+1]) \cap \mathcal{D}^{co}(1/2)$$

and

$$Q(q) := \{G \in \mathcal{D}^0([p],[k]) : \ |E_G([p],k+1)| = q\}.$$

To estimate cardinalities we construct a relation R between Q and $Q(q)$. We say that $(G,G') \in R$ for some $G \in Q$ and $G' \in Q(q)$ if G' can be obtained from G using the simple switchings as follows. First choose q vertices $1 \le v_1 < v_2 < \ldots < v_q \le p$. There are $\binom{p}{q}$ such choices. Then choose q edges in $E_G([p]^c, k+1)$, say $(w_i, k+1)$, $i \le q$, with $p < w_1 < w_2 < \ldots < w_q \le n$. There are $\binom{d}{q}$ such choices. Finally for every $i \le q$ choose

$$j(i) \in \mathcal{N}_G^{out}(v_i) \setminus \mathcal{N}_G^{out}(w_i).$$

Since $G \in \mathcal{D}^{co}(1/2)$, for every $i \le q$ there are at least $d/2$ choices of $j(i)$. For every $i \le q$ we destroy edges $(w_i, k+1)$, $(v_i, j(i))$ and create edges $(v_i, k+1)$, $(w_i, j(i))$. We have

$$\left|R(G)\right| \ge \binom{p}{q}\binom{d}{q}\left(\frac{d}{2}\right)^q \ge \left(\frac{pd^2}{2q^2}\right)^q. \tag{6}$$

Now we estimate the cardinalities of preimages. Let $G' \in R(Q)$. We bound $|R^{-1}(G')|$ from above. To reconstruct a possible $G \in Q$ with $(G,G') \in R$, we perform simple switchings as follows. Write $E_{G'}([p],k+1)$ as $(v_1,k+1),\ldots,(v_q,k+1)$ with $1 \le v_1 < \ldots < v_q \le p$. Choose q vertices $p < w_1 < \ldots w_q \le n$ such that

$$w_i \in [p]^c \setminus \mathcal{N}_{G'}^{in}(k+1)$$

for all $i \le q$. There are

$$\binom{n-p-(d-q)}{q} \le \left(\frac{en}{q}\right)^q$$

such choices. For every $i \le q$ find

$$j \in \left(\mathcal{N}_{G'}^{out}(w_i) \cap [k+1]^c\right) \setminus \mathcal{N}_{G'}^{out}(v_i)$$

(there are at most d such choices). For every $i \le q$ we destroy edges $(v_i, k+1)$, $(w_i, j(i))$ and create edges $(w_i, k+1)$, $(v_i, j(i))$. We obtain

$$\left|R^{-1}(G')\right| \le \left(\frac{en}{q}\right)^q d^q.$$

Claim 2.1 together with the last bound and (6) yields

$$\left|Q\right| \le \left(\frac{2enq}{pd}\right)^q \left|Q(q)\right|.$$

By the choice of q, we have $\left|Q\right| \le \exp(-pd/(2e^2n))\left|Q(q)\right|$. This, together with Lemma 2.12, implies

$$\begin{aligned}|\mathcal{D}^0([p],[k])| \ge |Q(q)| &\ge \exp\left(\frac{pd}{2e^2n}\right) |\mathcal{D}^0([p],[k+1]) \cap \mathcal{D}^{co}(1/2)| \\ &= \exp\left(\frac{pd}{2e^2n}\right) \left(|\mathcal{D}^0([p],[k+1])| - |\mathcal{D}^0([p],[k+1]) \setminus \mathcal{D}^{co}(1/2)|\right) \\ &\ge \exp\left(\frac{pd}{2e^2n}\right) \left(1 - \frac{n^2}{2}\left(\frac{4ed}{n}\right)^{d/2}\right) |\mathcal{D}^0([p],[k+1])|,\end{aligned}$$

which implies the desired result. □

Proof of Theorem 2.6. It is enough to prove the theorem for the union over all $|I| = \ell$ and $|J| = r$. By the union bound, we have

$$\mathbb{P}\left\{\bigcup \mathcal{D}^0(I,J)\right\} \le \binom{n}{\ell}\binom{n}{r} \frac{\left|\mathcal{D}^0([\ell],[r])\right|}{\left|\mathcal{D}\right|} \le \left(\frac{en}{r}\right)^{2r} \frac{\left|\mathcal{D}^0([\ell],[r])\right|}{\left|\mathcal{D}\right|}. \tag{7}$$

Setting $\mathcal{D}^0([0],[0]) = \mathcal{D}$ and using $\mathcal{D}^0([k],[k]) \supset \mathcal{D}^0([k+1],[k+1])$, we get

$$\begin{aligned}\frac{\left|\mathcal{D}^0([\ell],[r])\right|}{\left|\mathcal{D}\right|} &= \prod_{k=0}^{\ell-1} \frac{\left|\mathcal{D}^0([k+1],[k+1])\right|}{\left|\mathcal{D}^0([k],[k])\right|} \prod_{k=\ell}^{r-1} \frac{\left|\mathcal{D}^0([\ell],[k+1])\right|}{\left|\mathcal{D}^0([\ell],[k])\right|} \\ &\le \prod_{k=\lceil \ell/2\rceil}^{\ell-1} \frac{\left|\mathcal{D}^0([k+1],[k+1])\right|}{\left|\mathcal{D}^0([k],[k])\right|} \prod_{k=\ell}^{r-1} \frac{\left|\mathcal{D}^0([\ell],[k+1])\right|}{\left|\mathcal{D}^0([\ell],[k])\right|}.\end{aligned} \tag{8}$$

Further, we write

$$\frac{\left|\mathcal{D}^0([k+1],[k+1])\right|}{\left|\mathcal{D}^0([k],[k])\right|} = \frac{\left|\mathcal{D}^0([k+1],[k+1])\right|}{\left|\mathcal{D}^0([k],[k+1])\right|} \cdot \frac{\left|\mathcal{D}^0([k],[k+1])\right|}{\left|\mathcal{D}^0([k],[k])\right|},$$

and applying Lemma 2.11, for every $\lceil \ell/2 \rceil \le k \le \ell - 1$ we observe

$$\frac{\big|\mathcal{D}^0([k+1],[k+1])\big|}{\big|\mathcal{D}^0([k],[k])\big|} \le \exp\left(-\frac{kd}{2e^2 n}\right),$$

and for every $\ell \le k \le r-1$,

$$\frac{\big|\mathcal{D}^0([\ell],[k+1])\big|}{\big|\mathcal{D}^0([\ell],[k])\big|} \le \exp\left(-\frac{\ell d}{4e^2 n}\right).$$

Thus (8) implies

$$\frac{\big|\mathcal{D}^0([\ell],[r])\big|}{\big|\mathcal{D}\big|} \le \exp\left(-\frac{\ell r d}{8e^2 n}\right).$$

Combining this bound and (7) and using that $\ell \ge Cn\ln(en/r)/d$ we complete the proof. □

Proof of Lemma 2.12. Clearly,

$$\big|\mathcal{D}^0([p],[k]) \setminus \mathcal{D}^{co}(\varepsilon)\big| \le \sum_{i<j} \big|\mathcal{D}^0([p],[k]) \setminus \mathcal{D}^{co}_{i,j}(\varepsilon)\big|.$$

Fix $1 \le i < j \le n$. For $0 \le q \le d$, denote

$$Q(q) := \big\{G \in \mathcal{D}^0([p],[k]) :\ |\mathrm{C}^{\mathrm{out}}_{\mathrm{G}}(i,j)| = q\big\}$$

and

$$Q := \mathcal{D}^0([p],[k]) \setminus \mathcal{D}^{co}_{i,j}(\varepsilon) = \bigsqcup_{q=\lfloor \varepsilon d \rfloor + 1}^{d} Q(q).$$

First, for every $1 \le q \le d$ we will compare the cardinalities of $Q(q)$ and $Q(q-1)$. To this end, we will define a relation R_q between the sets $Q(q)$ and $Q(q-1)$ in the following way.

Let $G \in Q(q)$. Then there exist $j_1 < \dots < j_q$ such that for every $\ell \le q$

$$j_\ell \in \mathcal{N}^{out}_G(i) \cap \mathcal{N}^{out}_G(j).$$

Note that for every $\ell \le q$, there are d^2 edges inside $E^{out}_G\big(\mathcal{N}^{in}_G(j_\ell)\big)$. Also, there are at least $(n-k-(2d-q))d$ edges in $E^{in}_G\big([k]^c \setminus \mathcal{N}^{out}_G(\{i,j\})\big)$. Therefore, for $\ell \le q$, the set

$$E_\ell := E_G\big([n] \setminus \mathcal{N}^{in}_G(j_\ell), [k]^c \setminus \mathcal{N}^{out}_G(\{i,j\})\big)$$

is of cardinality at least

$$|E_\ell| \ge (n-k-(2d-q))d - d^2 \ge nd/2.$$

We say that $(G,G') \in R_q$ for some $G' \in Q(q-1)$ if G' can be obtained from G in the following way. First we choose $\ell \le q$ and an edge $(u,v) \in E_\ell$. Note $v \in [k]^c$ and $u \ne i$. Since $v \notin \mathcal{N}^{out}_G(j)$ then we can destroy the edge (j, j_ℓ) and create the edge (j,v). Since $u \notin \mathcal{N}^{in}_G(j_\ell)$

then we can destroy the edge (u, v) and create the edge (u, j_ℓ). Thus, we obtain G' by the simple switching on vertices u, v, j, j_ℓ. It is not difficult to see that we have not created any edges between $[p]$ and $[k]$, hence G' indeed belongs to $Q(q-1)$. Counting the admissible simple switchings, we get for every $G \in Q(q)$,

$$|R_q(G)| \geq \frac{qnd}{2}. \tag{9}$$

Now we estimate the cardinalities of preimages. Let $G' \in R_q\big(Q(q)\big)$. In order to reconstruct a possible G for which $(G, G') \in R_q$, we need to perform the simple switching which removes an edge (j, v) with $v \notin \mathcal{N}_{G'}^{out}(i)$ and recreates an edge (j, w) for some

$$w \in \mathcal{N}_{G'}^{out}(i) \setminus \mathcal{N}_{G'}^{out}(j).$$

There are at most $d - q + 1$ choices for such v and at most $d - q + 1$ choices for such w. For the second part of the switching, we have at most d possible choices. Therefore,

$$\big|R_q^{-1}(G')\big| \leq d(d-q+1)^2 \leq d^3.$$

Using this bound, (9), and Claim 2.1, we obtain that

$$\big|Q(q)\big| \leq \left(\frac{2d^2}{qn}\right) \cdot \big|Q(q-1)\big|$$

and, applying this successively,

$$\big|Q(q)\big| \leq \left(\frac{2d^2}{n}\right)^q \frac{1}{q!} \big|Q(0)\big|.$$

Since $q! \geq 2(q/e)^q$ and $2ed/(\varepsilon n) \leq 1/2$, this implies

$$|Q| = \sum_{q=\lfloor \varepsilon d \rfloor + 1}^{d} \big|Q(q)\big| \leq \frac{1}{2} \sum_{q=\lfloor \varepsilon d \rfloor + 1}^{d} \left(\frac{2ed}{\varepsilon n}\right)^q \big|Q(0)\big| \leq \left(\frac{2ed}{\varepsilon n}\right)^{\varepsilon d} \big|Q(0)\big|.$$

Using that $Q(0) \subset \mathcal{D}^0([p], [k])$ and that there are $n(n-1)/2$ pairs $i < j$, we obtain the desired result. $\square$

2.4 An anti-concentration property for random digraphs

For every $G \in \mathcal{D}$, $J \subset [n]$ and $i \in [n]$, we define $\delta_i^J \in \{0, 1\}$ by

$$\delta_i^J = \delta_i^J(G) := \begin{cases} 1 & \text{if } i \in \mathcal{N}_G^{in}(J), \\ 0 & \text{otherwise.} \end{cases}$$

Denote $\delta^J := (\delta_1^J, \ldots, \delta_n^J) \in \{0, 1\}^n$. The vector δ^J can be regarded as an indicator of the vertices that are connected to J, without specifying how many edges connect a vertex to J.

Taking $v \in \{0,1\}^n$ and conditioning on the realization $\delta^J = v$, we obtain a class of graphs with a particular arrangement of the edges. Namely, if a vertex i of a graph in the class is not connected to J then all graphs in the class have the same property. In this section we estimate the cardinalities of such classes generated by vertices of the cube, under additional assumption that a part of the graph is "frozen." We show that if the size of the set J is at most cn/d then a large proportion of such classes are "approximately" of the same size. In other words, we prove that the distribution of δ^J is similar to that of a random vector uniformly distributed on the discrete cube $\{0,1\}^n$ in the sense that for each fixed $v \in \{0,1\}^n$ the probability that $\delta^J = v$ is exponentially small. This makes a link to the anti-concentration results in the Littlewood-Offord theory. We start with a simplified version of this result, when there is no "frozen" part. In this case it is a rather straightforward consequence of Theorem 2.2.

Proposition 2.13. *Let $8 \le d \le n$ and $J \subset [n]$. Let $v \in \{0,1\}^n$ and $m := |\operatorname{supp} v|$. Then*

$$\mathbb{P}\{\delta^J = v\} \le \binom{n}{m}^{-1} \le \exp\left(-m \ln \frac{n}{m}\right).$$

Moreover, if $|J| \le cn/d$, then

$$\mathbb{P}\{\delta^J = v\} \le \exp\left(-cd|J| \ln \frac{cn}{d|J|}\right),$$

where c is an absolute positive constant.

Remark 2.14. Note that $\max\{d, |J|\} \le |\operatorname{supp} \delta^J| \le d|J|$, therefore $\mathbb{P}\{\delta^J = v\} = 0$ unless $\max\{d, |J|\} \le m \le d|J|$.

Proof. Without loss of generality we assume that $\max\{d, |J|\} \le m \le d|J|$. Consider the following subset of the discrete cube

$$T = \{w \in \{0,1\}^n \, : \, |\operatorname{supp} w| = m\}.$$

Clearly, every $w \in T$ can be obtained by a permutation of the coordinates of v. Since the distribution of a random graph is invariant under permutations, $\mathbb{P}\{\delta^J = v\} = \mathbb{P}\{\delta^J = w\}$ for every $w \in T$. Therefore,

$$\mathbb{P}\{\delta^J = v\} \le |T|^{-1} = \binom{n}{m}^{-1} \le \exp\left(-m \ln \frac{n}{m}\right),$$

which proves the first bound and the "moreover" part in the case $m \ge d|J|/2$.

Suppose now that $|J| \le cn/d$ and $m \le d|J|/2$. Applying Theorem 2.2 with $S = J$, $I = \emptyset$, and $\varepsilon = 1/2$, we observe

$$\mathbb{P}\{|\operatorname{supp} \delta^J| \le d|J|/2\} \le \exp\left(-cd|J| \ln \frac{cn}{d|J|}\right),$$

which completes the proof of the "moreover" part. $\square$

Now we turn to the main theorem of this section, which will play a key role in the "matrix" part of our paper. We obtain an anti-concentration property for the vector δ^J even under an assumption that a part of edges is "frozen." It requires a more delicate argument.

Theorem 2.15. *There exist two absolute positive constants $c, \tilde{c}$ such that the following holds. Let $32 \le d \le cn$ and let I, J be disjoint subsets of $[n]$ such that*

$$|I| \le \frac{d|J|}{32} \qquad \text{and} \qquad 8 \le |J| \le \frac{8cn}{d}.$$

Let $F \subset [n] \times [n]$ be such that $\mathcal{D}(I, F) \neq \emptyset$ and let $v \in \{0,1\}^n$. Then

$$\mathbb{P}\{\delta^J = v \mid \mathcal{D}(I,F)\} \le 2\exp\left(-\tilde{c}d|J|\ln\left(\frac{n}{d|J|}\right)\right).$$

To prove this theorem we first estimate the size of the class of graphs given by a realization of a subset of coordinates of δ^J. More precisely, restricted to a subset of graphs with predefined out-edges for the first $i-1$ vertices of δ^J, we count the number of graphs for which the vertex i is connected to J. In other words, conditioning on the realization of the first $i-1$ coordinates of δ^J, we estimate the probability that $\delta^J_i = 1$. In Lemma 2.16 below we show that this probability is of the order $d|J|/n$ for a wide range of i-s. In a sense, this shows that the sets of out-edges restricted on J for different vertices behave like independent. Indeed, in the Erdős–Rényi model, when the edges are distributed independently with probability of having an edge equals d/n, the probability that a vertex i is connected to J is of order $d|J|/n$.

We need the following notation. For $\varepsilon \in (0,1)$ and $J \subset [n]$ let

$$\Lambda(\varepsilon, J) = \left\{G \in \mathcal{D} : \ |\mathcal{N}_G^{in}(J)| \ge (1-\varepsilon)d|J|\right\}.$$

Lemma 2.16. *Let $2 \le d \le n/32$. Let $F \subset [n] \times [n]$ and I, J be disjoint subsets of $[n]$ satisfying*

$$|I| \le \frac{d|J|}{32} \qquad \text{and} \qquad 8 \le |J| \le \frac{n}{4d}. \tag{10}$$

Then there exists a permutation $\sigma \in \Pi_n$ such that for every

$$2|I| \le i_1 < i_2 < \ldots < i_{d|J|/16},$$

every $s \le d|J|/16$ and $\mathcal{H} \subset 2^{[n]\times[n]}$ satisfying

$$\widetilde{\Gamma} := \left\{G \in \mathcal{D}(I,F) \cap \Lambda\left(\tfrac{1}{2}, J\right) \ : \ E_G\big(\sigma([2|I|] \cup \{i_1, \ldots, i_{s-1}\}), I^c\big) \in \mathcal{H}\right\} \neq \emptyset$$

one has

$$\frac{d|J|}{9n} \le \mathbb{P}\left\{\delta^J_{\sigma(i_s)} = 1 \mid \widetilde{\Gamma}\right\} \le \frac{2d|J|}{n}.$$

As the proof of lemma is rather technical, we postpone it to the end of this section.

Proof of Theorem 2.15. Fix $F \subset [n] \times [n]$ with $\mathcal{D}(I,F) \neq \emptyset$ and $v \in \{0,1\}^n$. Let σ be a permutation given by Lemma 2.16.

Denote $B := \mathcal{D}(I,F) \cap \Lambda\left(\frac{1}{2}, J\right)$. Since $J \subset I^c$, applying Theorem 2.2 with $\varepsilon = 1/2$ and $k = |J|$, we get that for some appropriate constant $\tilde{c}$

$$\mathbb{P}\left\{\Lambda\left(\tfrac{1}{2}, J\right) \mid \mathcal{D}(I,F)\right\} \geq 1 - \exp\left(-\tilde{c}d|J|\ln\left(\frac{n}{d|J|}\right)\right),$$

which in particular implies that B is non-empty.

Using this we have

$$\begin{aligned}\mathbb{P}\{\delta^J = v \mid \mathcal{D}(I,F)\} &\leq \mathbb{P}\left\{\delta^J = v \mid \mathcal{D}(I,F) \cap \Lambda\left(\tfrac{1}{2}, J\right)\right\} + \mathbb{P}\left\{\Lambda^c\left(\tfrac{1}{2}, J\right) \mid \mathcal{D}(I,F)\right\} \\ &\leq \mathbb{P}\left\{\delta^J = v \mid B\right\} + \exp\left(-\tilde{c}d|J|\ln\left(\frac{n}{d|J|}\right)\right).\end{aligned}$$

Therefore, it is enough to estimate the first term in the previous inequality. Note that if $|\operatorname{supp} v| < d|J|/2$ then

$$\mathbb{P}\left\{\delta^J = v \mid \mathcal{D}(I,F) \cap \Lambda\left(\tfrac{1}{2}, J\right)\right\} = 0.$$

Assume that $|\operatorname{supp} v| \geq d|J|/2$ and denote $m = d|J|/16$. Since $2|I| \leq m$, there exist

$$2|I| \leq i_1 < i_2 < \ldots < i_m$$

such that for every $s \leq m$ one has $v_{\sigma(i_s)} = 1$. Let $Q_1 = [2|I|]$. For every $2 \leq s \leq m+1$, define $Q_s := Q_1 \cup \{i_1, \ldots, i_{s-1}\}$ and

$$\mathcal{H}_s := \left\{H \subset \sigma(Q_s) \times I^c \,:\, \forall \ell \in Q_s \quad \text{“}v_{\sigma(\ell)} = 0\text{”} \Leftrightarrow \text{“}\forall j \in J \quad (\sigma(\ell), j) \notin H\text{”}\right\}.$$

In words, $\mathcal{H}_s$ is the collection of all possible realizations of configurations of edges connecting $\sigma(Q_s)$ to I^c, such that $\sigma(\ell)$ is not connected to $J \subset I^c$ if and only if $v_{\sigma(\ell)} = 0$ ($\ell \in Q_s$). Note that

$$A_s := \left\{G \in \mathcal{D} \,:\, \forall \ell \in Q_s \quad \delta^J_{\sigma(\ell)} = v_{\sigma(\ell)}\right\} = \left\{G \in \mathcal{D} \,:\, E_G\big(\sigma(Q_s), I^c\big) \in \mathcal{H}_s\right\}.$$

Denote

$$B_s := \left\{G \in \mathcal{D} \,:\, \delta^J_{\sigma(i_s)} = 1\right\}.$$

Since $v_{\sigma(i_s)} = 1$ for every $s \leq m$ then $A_{s+1} = B_s \cap A_s$ and

$$\mathbb{P}\{A_{s+1} \mid B\} = \mathbb{P}\{B_s \cap A_s \mid B\} = \mathbb{P}\{B_s \mid B \cap A_s\}\,\mathbb{P}\{A_s \mid B\}.$$

Therefore,

$$\mathbb{P}\{\delta^J = v \mid B\} \leq \mathbb{P}\{A_{m+1} \mid B\} \leq \prod_{s=1}^{m} \mathbb{P}\{B_s \mid B \cap A_s\}.$$

By the assumptions of the theorem and Lemma 2.16, for every $s \le m$ we have

$$\mathbb{P}\{B_s \mid B \cap A_s\} \le \frac{2d|J|}{n},$$

which implies

$$\mathbb{P}\{\delta^J = v \mid B\} \le \left(\frac{2d|J|}{n}\right)^m \le \exp\left(-\frac{d|J|}{16}\ln\left(\frac{n}{2d|J|}\right)\right).$$

This completes the proof. □

It remains to prove Lemma 2.16. To get the lower bound we employ the simple switching to graphs whose i-th vertex is not connected to J and transform them into graphs with the i-th vertex connected to J. To get the upper bound, we do the opposite trick to transform graphs with only one edge relating vertex i to J to a graph with no connections from i to J. Then we show that if i is connected to J, it is more likely that the number of corresponding out-edges is small. This is very natural if we have in mind the result proven in Theorem 2.2. Indeed, if vertices of a graph had a large number of out-edges connecting them to J, then the number of in-neighbors to J would be small, while Theorem 2.2 states that $\mathcal{N}_G^{in}(J)$ is rather large.

Proof of Lemma 2.16. Let σ be a permutation such that the sequence

$$\left\{|\mathcal{N}_G^{out}\big(\sigma(\ell)\big) \cap I|\right\}_{\ell=1}^n$$

is non-increasing. Note that σ depends only on F when $G \in \mathcal{D}(I, F)$.

First we note that for every $G \in \mathcal{D}(I, F)$

$$\forall i \ge 2|I| \qquad \left|\mathcal{N}_G^{out}\big(\sigma(i)\big) \cap I^c\right| \ge d/2. \tag{11}$$

Indeed, otherwise there would exist $G \in \mathcal{D}(I, F)$ and $i_0 \ge 2|I|$ such that

$$\left|\mathcal{N}_G^{out}\big(\sigma(i_0)\big) \cap I\right| > d/2.$$

Since $\left\{|\mathcal{N}_G^{out}\big(\sigma(\ell)\big) \cap I|\right\}_{\ell \le n}$ is non-increasing, then for every $\ell \le i_0$ we would have

$$\left|\mathcal{N}_G^{out}\big(\sigma(\ell)\big) \cap I\right| > d/2.$$

This would imply

$$\left|E_G(\sigma([i_0]), I)\right| > i_0 d/2 \ge d|I|,$$

which is impossible.

Fix $s \le d|J|/16$. For $0 \le k \le p := \min\{d, |J|\}$ denote

$$\widetilde{\Gamma}_k := \left\{G \in \widetilde{\Gamma} : \ \left|E_G(\sigma(i_s), J)\right| = k\right\}.$$

Clearly, $\widetilde{\Gamma} = \bigsqcup_{k \le p} \widetilde{\Gamma}_k$.

The statement of the lemma is equivalent to the following estimate

$$\frac{d|J|}{9n}\,\big|\widetilde{\Gamma}\big| \le \big|\widetilde{\Gamma}\setminus\widetilde{\Gamma}_0\big| \le \frac{2d|J|}{n}\,\big|\widetilde{\Gamma}\big|. \tag{12}$$

We first show that

$$\big|\widetilde{\Gamma}_0\big| \le \frac{8n}{d|J|}\,\big|\widetilde{\Gamma}_1\big|. \tag{13}$$

Note that (13) implies the left hand side of (12). Indeed, since $\widetilde{\Gamma}_1 \subseteq \widetilde{\Gamma}\setminus\widetilde{\Gamma}_0$, then (13) yields that

$$\big|\widetilde{\Gamma}_0\big| \le \frac{8n}{d|J|}\,\big|\widetilde{\Gamma}\setminus\widetilde{\Gamma}_0\big|.$$

Adding $\big|\widetilde{\Gamma}\setminus\widetilde{\Gamma}_0\big|$ to both sides we obtain the left hand side of (12).

In order to prove (13), we define a relation R between the sets $\widetilde{\Gamma}_0$ and $\widetilde{\Gamma}_1$. Let $G \in \widetilde{\Gamma}_0$. Since $G \in \Lambda\big(\frac{1}{2}, J\big)$ and $2|I| + s \le d|J|/8$, then

$$\big|\mathcal{N}_G^{in}(J)\setminus\sigma([2|I|]\cup\{i_1,\dots,i_{s-1}\})\big| \ge \frac{3d|J|}{8}. \tag{14}$$

Denote

$$T := \big(\mathcal{N}_G^{in}(J)\setminus\sigma([2|I|]\cup\{i_1,\dots,i_{s-1}\})\big)\times\big(\mathcal{N}_G^{out}\big(\sigma(i_s)\big)\cap I^c\big).$$

Since $G \in \widetilde{\Gamma}_0$, that is $\big|E_G(\sigma(i_s), J)\big| = 0$, we have

$$\big|E_G\big(T\big)\big| \le (d-1)\big|\mathcal{N}_G^{out}\big(\sigma(i_s)\big)\cap I^c\big|.$$

This together with (11), (14), and $|J| \ge 8$ implies that the set $S := T\setminus E_G(T)$ satisfies

$$|S| \ge \left(\frac{3d|J|}{8} - d + 1\right)\cdot\big|\mathcal{N}_G^{out}\big(\sigma(i_s)\big)\cap I^c\big| \ge \frac{d^2|J|}{8}. \tag{15}$$

We say that $(G, G') \in R$ for some $G' \in \widetilde{\Gamma}_1$ if G' can be obtained from G in the following way. First choose $(v, j) \in S$. Since $j \in \mathcal{N}_G^{out}\big(\sigma(i_s)\big)\cap I^c$ and $(v, j) \notin E_G(T)$ then we can destroy the edge $(\sigma(i_s), j)$ and create the edge (v, j). Since $v \in \mathcal{N}_G^{in}(J)$, there is $j' \in J$ such that (v, j') is an edge in G. Since $G \in \widetilde{\Gamma}_0$, $(\sigma(i_s), j') \notin G$. Thus we can destroy the edge (v, j') and create the edge $(\sigma(i_s), j')$, completing the simple switching. By (15) we get

$$|R(G)| \ge \frac{d^2|J|}{8}.$$

Note that the above transformation of G does not decrease $|\mathcal{N}_G^{in}(J)|$ which guarantees that $G' \in \Lambda\big(\frac{1}{2}, J\big)$.

Now we estimate the cardinalities of preimages. Let $G' \in R(\widetilde{\Gamma}_0)$. In order to reconstruct a possible G for which $(G, G') \in R$, destroy the only edge $(\sigma(i_s), j')$ in $E_{G'}(\sigma(i_s), J)$ and create an edge (ℓ, j') for $\ell \notin \sigma([2|I|]\cup\{i_1,\dots,i_{s-1}\})$. There are at most $n - 2|I| - (s-1) \le n$ possible choices at this step. To complete the simple switching, we destroy one of the edges in $E_{G'}(\ell, J^c \cap I^c)$ and create an edge connecting $\sigma(i_s)$ to $J^c \cap I^c$. There are at most d possible choices here. Therefore,

$$|R^{-1}(G')| \leq nd.$$

By Claim 2.1, this implies the inequality (13).

We now show that for every $k \in \{1, \dots, p\}$, one has

$$|\widetilde{\Gamma}_k| \leq \frac{2d|J|}{kn} \, |\widetilde{\Gamma}_{k-1}|. \tag{16}$$

Note that (16) implies the right hand side of (12). Indeed, by (16),

$$|\widetilde{\Gamma}_k| \leq \left(\frac{2d|J|}{n}\right)^k \frac{1}{k!} \, |\widetilde{\Gamma}_0|,$$

hence

$$|\widetilde{\Gamma}| = |\widetilde{\Gamma}_0| + \sum_{k=1}^{p} |\widetilde{\Gamma}_k| \leq \exp\left(\frac{2d|J|}{n}\right) |\widetilde{\Gamma}_0|,$$

which implies

$$\left|\widetilde{\Gamma} \setminus \widetilde{\Gamma}_0\right| \leq \left|\widetilde{\Gamma}\right| - \exp\left(-\frac{2d|J|}{n}\right) \left|\widetilde{\Gamma}\right| \leq \frac{2d|J|}{n} \left|\widetilde{\Gamma}\right|.$$

In order to prove (16) for every $k \in \{1, \dots, p\}$, we construct a relation R_k between the sets $\widetilde{\Gamma}_k$ and $\widetilde{\Gamma}_{k-1}$.

Let $G \in \widetilde{\Gamma}_k$. Note that

$$\left|\sigma([2|I|] \cup \{i_1, \dots, i_s\}) \cup \mathcal{N}_G^{in}\big(J\big)\right| \leq 2|I| + s + d|J| \leq \frac{9d|J|}{8}. \tag{17}$$

By (10), we get

$$\left|I^c \cap J^c \setminus \mathcal{N}_G^{out}(\sigma(i))\right| \geq n - \frac{d|J|}{32} - \frac{n}{4d} - d \geq \frac{27n}{32} - \frac{d|J|}{32}. \tag{18}$$

Denote

$$S_k := E_G\big(\sigma([2|I|]^c \setminus \{i_1, \dots, i_s\}) \setminus \mathcal{N}_G^{in}\big(J\big), I^c \cap J^c \setminus \mathcal{N}_G^{out}(\sigma(i_s))\big).$$

Using (17), (18) we observe that

$$|S_k| \geq d\left(\frac{27n}{32} - \frac{d|J|}{32} - \frac{9d|J|}{8}\right) \geq \frac{nd}{2}. \tag{19}$$

We say that $(G, G') \in R_k$ for some $G' \in \widetilde{\Gamma}_{k-1}$ if G' can be obtained from G in the following way. Let $(\sigma(i_s), j_1)$ be one of the k edges in $E_G(\sigma(i_s), J)$. Destroy an edge $(v, j) \in S_k$. Since $j \notin \mathcal{N}_G^{out}\big(\sigma(i_s)\big)$, then we can create the edge $(\sigma(i_s), j)$. Since $v \notin \mathcal{N}_G^{in}(j_1)$, then we can destroy the edge $(\sigma(i_s), j_1)$ and create the edge (v, j_1), thus completing the simple switching. Therefore by (19) we get

$$|R_k(G)| \geq \frac{knd}{2}.$$

Note that the above transformation of G does not decrease $|\mathcal{N}_G^{in}(J)|$ which guarantees that $G' \in \Lambda\big(\frac{1}{2}, J\big)$.

Now we estimate the cardinalities of preimages. Let $G' \in R_k(\widetilde{\Gamma}_k)$. In order to reconstruct a possible G for which $(G, G') \in R_k$, destroy an edge (v, j_1) from $E_{G'}(\sigma([2|I|]^c \setminus \{i_1, \ldots, i_s\}), J)$ to create the edge $(\sigma(i_s), j_1)$ for $j_1 \in J$. There are at most $d|J|$ such choices. To complete the simple switching, we destroy an edge $(\sigma(i_s), j_2)$ in $E_{G'}(\sigma(i_s), I^c \cap J^c)$ and create the edge (v, j_2). There are at most d possible choices here. Therefore

$$|R_k^{-1}(G')| \leq d^2|J|.$$

Claim 2.1 implies the inequality (16), and completes the proof. $\square$

3 Adjacency matrices of random digraphs

In this section we continue to study density properties of random d-regular directed (rrd) graphs. We interpret results obtained in the previous section in terms of adjacency matrices and provide consequences of the anti-concentration property, Theorem 2.15, needed to investigate the invertibility of adjacency matrices.

3.1 Notation

For $1 \leq d \leq n$ we denote by $\mathcal{M}_{n,d}$ the set of $n \times n$ matrices with 0/1-entries and such that every row and every column has exactly d ones. By a random matrix on $\mathcal{M}_{n,d}$ we understand a matrix uniformly distributed on $\mathcal{M}_{n,d}$, in other words the probability on $\mathcal{M}_{n,d}$ is given by the normalized counting measure. Whenever it is clear from the context, we usually use the same letter M for an element of $\mathcal{M}_{n,d}$ and for a random matrix.

For $I \subset [n]$ by P_I we denote the orthogonal projection on the coordinate subspace $\mathbb{R}^I$ and $I^c := [n] \setminus I$. For a matrix $M \in \mathcal{M}_{n,d}$ we say that a non-zero vector x is a null-vector of M if either $Mx = 0$ (a right null-vector) or $x^T M = 0$ (a left null vector).

Let $M = \{\mu_{ij}\} \in \mathcal{M}_{n,d}$. The i'th row of M is denoted by $R_i = R_i(M)$ and the i'th column by $X_i = X_i(M)$, respectively. For $j \leq n$, we denote $\operatorname{supp} X_j = \{i \leq n : \mu_{ij} = 1\}$ and for every subset $J \subset [n]$ we let

$$S_J := \bigcup_{j \in J} \operatorname{supp} X_j,$$

Clearly, $|J| \leq |S_J| \leq d|J|$ and $n - d|J| \leq |(S_J)^c| \leq n - |J|$.

For $x \in \mathbb{R}^n$ we denote its coordinates by x_i, $i \leq n$, its ℓ_∞-norm by $\|x\|_\infty = \max_i |x_i|$ and for a linear operator U from X to Y by $\|U : X \to Y\|$ we denote its operator norm.

3.2 Maximizing columns support

In this section we reformulate Theorem 2.2 in terms of adjacency matrices. It corresponds to bounding from below the number of rows which are non-zero on a given set of columns. More precisely, for every subset $J \subset [n]$ we have $|S_J| \leq d|J|$. We prove that for almost all matrices in $\mathcal{M}_{n,d}$, this inequality is close to being sharp whenever J is of the appropriate size (less than some proportion of n/d). This means that S_J is of almost maximal size.

Theorem 3.1. *Let $8 \leq d \leq n$ and $\varepsilon \in (0,1)$ satisfy*

$$\varepsilon^2 \geq \frac{\max\{8, \ln d\}}{d}.$$

Define

$$\Omega_\varepsilon = \Big\{ M \in \mathcal{M}_{n,d} \,:\, \forall J \subset [n],\, |J| \leq \frac{c_0 \varepsilon n}{d}, \quad \text{one has} \ \ |S_J| \geq (1-\varepsilon) d |J| \Big\},$$

where c_0 is a sufficiently small absolute positive constant. Then

$$\mathbb{P}(\Omega_\varepsilon) \geq 1 - \exp\left(-\frac{\varepsilon^2 d}{8} \ln \left(\frac{e c_0 \varepsilon n}{d} \right) \right).$$

Remark 3.2. In fact Theorem 2.2 gives slightly more, namely the corresponding estimates when $|J| = k$ for a fixed $k \leq c_0 \varepsilon n/d$. However we don't use it below.

The following proposition is a direct consequence of Lemma 2.12 (applied with 2ε instead of ε and with $p = k = 0$). It shows that for a big proportion of matrices in $\mathcal{M}_{n,d}$, every two rows have almost disjoint supports.

Proposition 3.3. *Let $\varepsilon \in (0,1)$ and $8 \leq d \leq \varepsilon n/6$. Define*

$$\Omega^2_\varepsilon = \Big\{ M \in \mathcal{M}_{n,d} : \forall i, j \in [n] \quad |\mathrm{supp}\,(R_i + R_j)| \geq 2(1-\varepsilon) d \Big\}.$$

Then

$$\mathbb{P}(\Omega^2_\varepsilon) \geq 1 - \frac{n^2}{2} \left(\frac{ed}{\varepsilon n} \right)^{\varepsilon d}.$$

3.3 Large zero minors

In this section we reformulate Theorem 2.6 in terms of adjacency matrices. It states that almost all matrices in $\mathcal{M}_{n,d}$ do not contain large zero minors.

Given $0 \leq \alpha, \beta \leq 1$ we define

$$\begin{aligned} \Omega^0(\alpha, \beta) = \{ M \in \mathcal{M}_{n,d} \ : \exists I, J \subset [n] \quad &\text{such that} \quad |I| \geq \alpha n,\, |J| \geq \beta n, \\ &\text{and} \quad \forall i \in I\, \forall j \in J \quad \mu_{ij} = 0 \}. \end{aligned} \tag{20}$$

In other terms, the elements of $\Omega^0(\alpha, \beta)$ are the matrices in $\mathcal{M}_{n,d}$ having a zero submatrix of size at least $\alpha n \times \beta n$. Theorem 2.6, reformulated below, shows that this set is small whenever α and β are not very small.

Theorem 3.4. *There exist absolute positive constants c, C such that the following holds. Let $2 \le d \le n/24$ and $0 < \alpha \le \beta \le 1/4$. Assume that*

$$\alpha \ge \frac{C \ln(e/\beta)}{d}.$$

Then

$$\mathbb{P}\left(\Omega^0(\alpha,\beta)\right) \le \exp\left(-c\alpha\beta dn\right).$$

Remark 3.5. We usually apply this theorem with the following choice of parameters: $\alpha = p/(2q)$, $\beta = p/2$, where $q = c_1 p^2 d$ for a sufficiently small absolute positive constant c_1. Then we have

$$\mathbb{P}\left(\Omega^0\left(\frac{p}{2q}, \frac{p}{2}\right)\right) \le \exp(-c_2 n). \tag{21}$$

We will also need the following simple lemma.

Lemma 3.6. *Let $1 \le d \le n$ and $0 < \alpha, \beta < 1$. Let*

$$\Omega_{\alpha,\beta} = \Big\{M \in \mathcal{M}_{n,d} \,:\, \forall J,\ |J| \ge \beta n, \quad \textit{one has} \quad |\{i \,:\, |\mathrm{supp}\ R_i \cap J| \ge \beta/2\alpha\}| \ge (1-\alpha)n\Big\}.$$

Then provided that αn is an integer, we have

$$\left(\Omega^0(\alpha,\beta/2)\right)^c \subset \Omega_{\alpha,\beta}.$$

Proof. Let $M \in \Omega_{\alpha,\beta}^c$. Then there exist $J \subset [n]$ with $|J| \ge \beta n$ and $I \subset [n]$ with $|I| = \alpha n$ such that

$$\forall i \in I \qquad |\mathrm{supp}\ R_i \cap J| < \beta/2\alpha.$$

This shows that the minor $\{\mu_{ij} \,:\, i \in I,\ j \in J\}$ has strictly less than $\beta n/2$ ones, which means that at least $\beta n/2$ columns of this minor are zero-columns. Thus

$$\exists I \subset [n],\ |I| = \alpha n, \quad \exists J_0 \subset [n],\ |J_0| \ge \beta n/2, \quad \forall i \in I,\ \forall j \in J_0 \,:\, \mu_{ij} = 0.$$

In other words, there is a zero minor of size $\alpha n \times \beta n/2$. This proves the lemma. $\square$

3.4 An anti-concentration property for adjacency matrices

For every $F \subset [n] \times [n]$ and $I \subset [n]$, let

$$\mathcal{M}_{n,d}(I,F) = \left\{M = \{\mu_{ij}\} \in \mathcal{M}_{n,d} \,:\, \mu_{ij} = 1 \text{ if and only if } j \in I,\ (i,j) \in F\right\}.$$

Thus matrices in $\mathcal{M}_{n,d}(I,F)$ have the same columns indexed by I and the places of ones in these columns are given by $F \cap ([n] \times I)$. Of course this set can be empty.

For every $M \in \mathcal{M}_{n,d}$, $J \subset [n]$ and $i \le n$, we define $\delta_i^J \in \{0,1\}$ as follows

$$\delta_i^J = \delta_i^J(M) := \begin{cases} 1 & \text{if } \mathrm{supp}\, R_i \cap J \ne \emptyset, \\ 0 & \text{otherwise.} \end{cases}$$

We also denote $\delta^J := (\delta_1^J, \dots, \delta_n^J) \in \{0,1\}^n$. The quantity δ^J indicates the rows whose supports intersect with J, i.e. the rows that have at least one 1 in columns indexed by J. The following is a reformulation of Theorem 2.15, concerning the anti-concentration property of graphs, in terms of adjacency matrices.

Theorem 3.7. *There are absolute positive constants $c, \tilde{c}$ such that the following holds. Let $32 \le d \le cn$ and I, J be disjoint subsets of $[n]$ such that*

$$|I| \le \frac{d|J|}{32} \qquad \text{and} \qquad 8 \le |J| \le \frac{8cn}{d}. \tag{22}$$

Let $F \subset [n] \times [n]$ be such that $\mathcal{M}_{n,d}(I,F) \neq \emptyset$ and $v \in \{0,1\}^n$. Then

$$\mathbb{P}\{\delta^J = v \mid \mathcal{M}_{n,d}(I,F)\} \le 2\exp\left(-\tilde{c}d|J|\ln\left(\frac{n}{d|J|}\right)\right).$$

This theorem has the following consequence.

Proposition 3.8. *There are absolute positive constants c, c' such that the following holds. Let $32 \le d \le cn$, $\lambda \in \mathbb{R}$, $a > 0$, and I, J, J_λ be a partition of $[n]$ satisfying (22). Let $q \le n/2$ be such that*

$$2^{q+1} \le \exp\left(c'd|J|\ln\left(\frac{n}{d|J|}\right)\right) \tag{23}$$

and y be a vector in $\mathbb{R}^n$ satisfying

$$\forall \ell \in J_\lambda \;\; y_\ell = \lambda \quad \text{and} \quad \forall j \in J \;\; y_j - \lambda \ge 2a. \tag{24}$$

Then for every $S \subset [n]$ with $|S| \ge n - q$, one has

$$\mathbb{P}\{\|P_S M y\|_\infty < a\} \le \exp\left(-c'd|J|\ln\left(\frac{n}{d|J|}\right)\right). \tag{25}$$

Remark 3.9. The above statement with essentially the same proof holds when (24) is replaced by

$$\forall \ell \in J_\lambda \;\; y_\ell = \lambda \quad \text{and} \quad \forall j \in J \;\; \lambda - y_j \ge 2a.$$

To prove Proposition 3.8 we need the following lemma.

Lemma 3.10. *Let $\lambda \in \mathbb{R}$, $a > 0$, and I, J, J_λ be a partition of $[n]$ satisfying (22). Let y be a vector in $\mathbb{R}^n$ satisfying (24). Then for every $i \le n$ and every $F \subset [n] \times [n]$ there exists $v_i \in \{0,1\}$ such that*

$$\{M \in \mathcal{M}_{n,d}(I,F) \mid \delta_i^J(M) = v_i\} \subseteq \{M \in \mathcal{M}_{n,d}(I,F) \mid |(My)_i| \ge a\}.$$

Proof. Fix $i \in [n]$ and $F \subset [n] \times [n]$. We argue by contradiction. Assume that the above inclusion is violated in both cases, $v_i = 0$ and $v_i = 1$. Then there exist two matrices $M_1, M_2 \in \mathcal{M}_{n,d}(I,F)$ such that

$$A_1 := \operatorname{supp} R_i^1 \cap J \neq \emptyset, \quad \operatorname{supp} R_i^2 \cap J = \emptyset, \quad |(M_1 y)_i| < a \quad \text{and} \quad |(M_2 y)_i| < a,$$

where $R_i^j = R_i(M^j)$ denotes the i-th row of M_j, $j = 1, 2$. Note that since $M_1, M_2 \in \mathcal{M}_{n,d}(I, F)$ then

$$\operatorname{supp} R_i^1 \cap I = \operatorname{supp} R_i^2 \cap I := A_2.$$

Let $s_1 := |A_1|$ and $s_2 := |A_2|$. Using (24), we observe

$$(M_1 y)_i = \sum_{j \in A_1} y_j + \sum_{j \in A_2} y_j + \lambda(d - s_1 - s_2) \quad \text{and} \quad (M_2 y)_i = \sum_{j \in A_2} y_j + \lambda(d - s_2).$$

Therefore,

$$(M_1 y)_i - (M_2 y)_i = \sum_{j \in A_1} (y_j - \lambda) \geq 2 s_1 a \geq 2a,$$

which is impossible as $|(M_1 y)_i| < a$ and $|(M_2 y)_i| < a$. $\square$

Proof of Proposition 3.8. Since (24) and (25) are homogeneous in y, without loss of generality we assume that $a = 1$.

Fix $S \subset [n]$ with $|S| \geq n - q$. Let $\mathcal{F}$ be the set of all $F \subset [n] \times [n]$ such that $\mathcal{M}_{n,d}(I, F)$ is not empty. Note that $\{\mathcal{M}_{n,d}(I, F)\}_{F \in \mathcal{F}}$ form a partition of $\mathcal{M}_{n,d}$. Therefore it is enough to prove that for every $F \in \mathcal{F}$,

$$p_0 := \mathbb{P}\{\|P_S M y\|_\infty < 1 \mid \mathcal{M}_{n,d}(I, F)\} \leq \exp\left(-c' d|J| \ln\left(\frac{n}{d|J|}\right)\right).$$

Fix $F \in \mathcal{F}$. Let $v_1, \ldots, v_n \in \{0, 1\}$ be given by Lemma 3.10. Note that

$$\|P_S M y\|_\infty < 1 \qquad \text{iff} \qquad \forall i \in S \quad |(My)_i| < 1,$$

therefore if $\|P_S M y\|_\infty < 1$ then $\{i : \delta_i^J(M) = v_i\} \subset S^c$. Thus

$$p_0 \leq \mathbb{P}\{\{i : \delta_i^J(M) = v_i\} \subseteq S^c \mid \mathcal{M}_{n,d}(I, F)\}.$$

Now for every $K \subset [n]$, define $v^K \in \{0, 1\}^n$ by

$$v_i^K := \begin{cases} v_i & \text{if } i \in K, \\ 1 - v_i & \text{otherwise.} \end{cases}$$

Since $m := |S^c| \leq q$, by Theorem 3.7 we obtain

$$\begin{aligned} p_0 &\leq \sum_{\ell=0}^{m} \mathbb{P}\{\exists K \subset S^c : \ |K| = \ell \text{ and } \delta^J(M) = v^K \mid \mathcal{M}_{n,d}(I, F)\} \\ &\leq \sum_{\ell=0}^{m} \binom{m}{\ell} \max_{|K|=\ell} \mathbb{P}\{\delta^J(M) = v^K \mid \mathcal{M}_{n,d}(I, F)\} \leq 2^{q+1} \exp\left(-\tilde{c} d|J| \ln\left(\frac{n}{d|J|}\right)\right). \end{aligned}$$

Taking $c' = \tilde{c}/2$ and using (23) we complete the proof. $\square$

4 Invertibility of adjacency matrices

In this section we investigate the invertibility of adjacency matrices $M \in \mathcal{M}_{n,d}$ of random d-regular directed graphs and prove Theorem A.

4.1 Almost constant null-vectors

We say that a non-zero vector is "almost constant" if for some $0 < p < 1/2$ at least $(1-p)n$ of its coordinates are equal to each other. Formally, for $0 < p < 1/2$ consider the following set of vectors

$$AC(p) = \{x \in \mathbb{R}^n \setminus \{0\} \, : \, \exists \lambda_x \in \mathbb{R} \quad |\{i \, : \, x_i = \lambda_x\}| \geq (1-p)n\}. \tag{26}$$

In this section we estimate the probability of the event

$$\mathcal{E}^{AC}(p) := \{M \in \mathcal{M}_{n,d} \, : \, \forall x \in AC(p) \quad Mx \neq 0 \quad \text{and} \quad x^T M \neq 0\}, \tag{27}$$

which relates almost constant vectors to null vectors of M. We show that that this probability is close to one, in other words we show that with high probability a matrix $M \in \mathcal{M}_{n,d}$ cannot have almost constant null vectors. This will be used in the proof of the main theorem allowing one to restrict the proof to the event $\mathcal{E}^{AC}(p)$. More precisely, we prove the following theorem.

Theorem 4.1. *There are absolute positive constants C, c such that for $C \leq d \leq cn$ and $p \leq c/\ln d$ one has*

$$\mathbb{P}\big(\mathcal{E}^{AC}(p)\big) \geq 1 - \left(\frac{Cd}{n}\right)^{cd}. \tag{28}$$

We start with some comments on the structure of almost constant vectors. Since $p < 1/2$, if $x \in AC(p)$ then only one real number λ_x satisfies (26). For every $x \in AC(p)$ we fix such $\lambda_x \in \mathbb{R}$. We set

$$AC^+(p) = \{x \in AC(p) \, : \, \lambda_x \geq 0\}.$$

Note that $\lambda_{-x} = -\lambda_x$, therefore

$$\mathcal{E}^{AC}(p) = \{M \in \mathcal{M}_{n,d} \, : \, \forall x \in AC^+(p) \quad Mx \neq 0 \quad \text{and} \quad x^T M \neq 0\}.$$

Moreover, since $(x^T M)^T = M^T x$ and M^T has the same distribution as M then

$$\mathbb{P}(\{M \in \mathcal{M}_{n,d} \, : \, \forall x \in AC^+(p) \quad Mx \neq 0\}) = \mathbb{P}(\{M \in \mathcal{M}_{n,d} \, : \, \forall x \in AC^+(p) \quad x^T M \neq 0\}).$$

Therefore it is enough to consider the event

$$\mathcal{E}^{AC+}(p) = \{M \in \mathcal{M}_{n,d} \, : \, \forall x \in AC^+(p) \quad Mx \neq 0\}$$

and to prove that

$$\mathbb{P}\big(\mathcal{E}^{AC+}(p)\big) \geq 1 - \frac{1}{2}\left(\frac{Cd}{n}\right)^{cd}.$$

To this end we split $AC^+(p)$ into two complementary sets and treat them separately in two lemmas.

For a vector $x = (x_i) \in \mathbb{R}^n$ we define the rearrangement $x^\star = (x_i^\star)_i$ as follows: $x_i^\star = x_{\pi(i)}$, where $\pi : [n] \to [n]$ is a permutation of $[n]$ such that $(|x_i^\star|)_i$ is a decreasing sequence, that is, $|x_{\pi(1)}| \geq |x_{\pi(2)}| \geq \ldots \geq |x_{\pi(n)}|$. Contrary to the usual decreasing rearrangement of absolute values of a sequence, here values $x_i^\star$ can be negative.

In the proof, we choose appropriately a positive integer m_0 and consider a certain subset of $AC^+(p)$. For a vector x in this subset we "ignore" its first m_0 coordinates $x_i^\star$, i.e. we consider $P_I x^\star$ with $I = [m_0]^c$. Then we show that this vector can be split into a sum of two vectors with disjoint supports and such that the second vector has equal coordinates on its support. To approximate such vectors in ℓ_∞-metric we construct a net in the following way.

Let $\eta > 0$ be a reciprocal of an integer. For every $H \subset [n]$ of cardinality $k_1 := pn - m_0$ (we choose p so that pn is an integer) fix an η-net Δ_H in the cube $P_H([-1,1]^n)$. Such Δ_H can be chosen with $|\Delta_H| \leq (1/\eta)^{k_1}$. Given $L \subset [n]$ of cardinality $k_2 := (1-p)n$, consider the one-dimensional space generated by the vector v_L with $\operatorname{supp} v_L = L$ and all coordinates on L equal to one. Fix an η-net Λ_L in the segment $[-v_L, v_L]$. Clearly, Λ_L can be chosen with $|\Lambda_L| = 1/\eta$. Note also that for every $z \in \Lambda_L$ one has $\operatorname{supp} z = L$ and $z_i = z_j$ whenever $i, j \in L$, that is $z \in AC(p)$ and $z_i = \lambda_z$ for $i \in \Lambda$. Given disjoint subsets H, L of $[n]$ of cardinalities k_1 and k_2 respectively, consider $\Delta_H \oplus \Lambda_L = \{w + z \,:\, w \in \Delta_H,\, z \in \Lambda_L\}$. Then

$$\Delta_H \oplus \Lambda_L \subset AC(p) \qquad \text{and} \qquad |\Delta_H \oplus \Lambda_L| \leq (1/\eta)^{k_1+1} \leq (1/\eta)^{pn}.$$

Finally we observe that the vector $P_I x^\star$ can be approximated by the vectors in the union of $\Delta_H \oplus \Lambda_L$ over all such choices of H and L.

In fact we will use only a subset of this union. Fix a parameter $a > 0$ and a positive integer r. For H, L as above consider

$$\Gamma(H,L) = \Gamma_{a,r}(H,L) := \{y \in \Delta_H \oplus \Lambda_L \,:\, \exists J \subset H,\, |J| = r, \;\text{ such that }\; \forall i \in J \;\; y_i - \lambda_y \geq 2a\}.$$

Clearly, $|\Gamma(H,L)| \leq (1/\eta)^{pn}$. Finally, set

$$\mathcal{N} = \mathcal{N}_{a,r} := \bigcup_{|L|=k_2, |H|=k_1} \Gamma(H,L),$$

where the union is taken over all disjoints subsets H and L of $[n]$ of cardinalities k_1 and k_2 correspondingly. Then

$$|\mathcal{N}| \leq \binom{n}{k_2} \binom{n-k_2}{k_1} \left(\frac{1}{\eta}\right)^{pn} \leq \binom{n}{pn} \binom{pn}{m_0} \left(\frac{1}{\eta}\right)^{pn} \leq \left(\frac{2e}{\eta p}\right)^{pn}. \tag{29}$$

We are ready now to prove two lemmas needed for Theorem 4.1. In both of them we use the following set associated with $x \in AC^+(p)$ and a given m_0,

$$J_x = J_x(m_0) := \{i > m_0 \,:\, |x_i^\star - \lambda_x| \geq 1/(2d)\}.$$

Lemma 4.2. *There are absolute positive constants c and c_1 such that the following holds. Let $32 \le d \le cn$, $m_0 \ge 1$, and $r \ge 8$ be integers such that $1 \le 2c_1 r \ln(n/(dr))$. Let $p \in (0, 1/2)$ be such that pn is an integer. Assume that*

$$m_0 \le 2c_1 r \ln\left(\frac{n}{dr}\right), \quad r \le \frac{8cn}{d}, \quad p \le \frac{dr}{32n}, \quad \text{and} \;\; p\left(\ln(e/p) + \ln(18d^2)\right) \le \frac{c_1 dr}{n} \ln\left(\frac{n}{dr}\right). \tag{30}$$

Consider the following subset of almost constant vectors

$$T_1 = \{x \in AC^+(p) \, : \, |x^\star_{m_0}| = 1 \quad \text{and} \quad |J_x| \ge 2r\}$$

and the corresponding event

$$\mathcal{E}_{T_1} = \{M \in \mathcal{M}_{n,d} \, : \, \forall x \in T_1 \quad Mx \ne 0\}.$$

Then

$$\mathbb{P}(\mathcal{E}_{T_1}) \ge 1 - 2\exp\left(-c_1 dr \ln\left(\frac{n}{dr}\right)\right).$$

Remark 4.3. We apply this lemma with $r = c_2 n/d$, $m_0 = c_3 n/d$, so that the probability is exponentially (in n) close to one.

Remark 4.4. In fact we show a stronger estimate which could be of independent interest, namely

$$\mathbb{P}\big(\{M \in \mathcal{M}_{n,d} \, : \, \exists x \in T_1 \;\; \text{such that} \;\; \|Mx\|_\infty < 1/(8d)\}\big) \le 2\exp\left(-c_1 dr \ln\left(\frac{n}{dr}\right)\right).$$

Proof of Lemma 4.2. We prove a stronger bound from Remark 4.4. We start by few general comments on the strategy behind the proof. By the construction of T_1, for $x = (x_i)_i \in T_1$ we have

$$\max\Big\{|\{i > m_0 \, : \, x^\star_i - \lambda_x \ge 1/(2d)\}|, \; |\{i > m_0 \, : \, \lambda_x - x^\star_i \ge 1/(2d)\}|\Big\} \ge r.$$

Therefore denoting

$$T_1^+ := \{x \in T_1 \, : \, |\{i > m_0 \, : \, x^\star_i - \lambda_x \ge 1/(2d)\}| \ge r\}$$

and

$$T_1^- := \{x \in T_1 \, : \, |\{i > m_0 \, : \, \lambda_x - x^\star_i \ge 1/(2d)\}| \ge r\},$$

we have $T_1 \subseteq T_1^+ \cup T_1^-$. Thus it is sufficient to show that

$$p_0 := \mathbb{P}\big(\{M \in \mathcal{M}_{n,d} \, : \, \exists x \in T_1^+ \;\; \|Mx\|_\infty < 1/(8d)\}\big) \le \exp\left(-c_1 dr \ln\left(\frac{n}{dr}\right)\right) \tag{31}$$

and similarly for T_1^-. Below we prove (31) only. Its counterpart for T_1^- follows the same lines, one just needs to apply Proposition 3.8 with Remark 3.9 below (with a slight modification of the net constructed above).

To prove (31) we first approximate vectors in T_1^+ by elements of the net $\mathcal{N}$ constructed above. By the union bound, this will reduce (31) to estimates on the net. Then, applying Proposition 3.8, we obtain a probability bound for a fixed vector from the net. As usual, the balance between the probability bound and the size of the net plays the crucial role.

Fix two parameters $\eta := 1/(9d^2)$ and $a = 1/(4d) - \eta$, and take $k_1 = pn - m_0$, $k_2 = (1-p)n$ as in the construction of the net $\mathcal{N}$ above. We start by showing how an element of T_1^+ is approximated by an element from $\mathcal{N}$. Let $x \in T_1^+$ and assume for simplicity that $|x_1| \geq |x_2| \geq \ldots \geq |x_n|$ (that is, $x = x^\star$). Recall that λ_x is the unique real number satisfying (26). By the definition of T_1^+ it is easy to see that there exists a partition J, J_0, I of $[n]$ such that

$$\begin{aligned}
&|J| = r, \quad |J_0| = k_2, \quad |I| = n - r - k_2, \\
&\forall i \in J_0 \quad x_i = \lambda_x \quad \text{with} \quad \lambda_x \geq 0, \\
&\forall j \in J \quad j > m_0 \quad \text{and} \quad x_j \geq \lambda_x + 1/(2d).
\end{aligned}$$

Since $|x_{m_0}| = 1$ and there is $i > m_0$ such that $x_i \geq \lambda_x + 1/(2d)$, we observe that $\lambda_x < 1$. Since for $i \leq m_0$ we have either $x_i \geq 1$ or $x_i \leq -1$, then $J_0 \cap I_0 = \emptyset$, where $I_0 = [m_0]$. Note also that $J \cap I_0 = \emptyset$, hence $I_0 \subset I$. Set $H = J \cup (I \setminus I_0)$ and $L = J_0$. Then $|H| = k_1$, $|L| = k_2$, and $A := I_0^c = H \cup L$. By the definition of Δ_H and Λ_L there exist $y' \in \Delta_H$ and $y'' \in \Lambda_L$ such that

$$\|P_H x - P_H y'\|_\infty \leq \eta \qquad \text{and} \qquad \|P_L x - P_L y''\|_\infty \leq \eta.$$

Therefore $y := y' + y'' \in \Delta_H \oplus \Lambda_L$ satisfies $\|P_A x - P_A y\|_\infty \leq \eta$. Moreover, by the construction of the net $y \in AC(p)$,

$$\forall i \in L \quad y_i = y_i'' = \lambda_y \qquad \text{and} \qquad \forall i \in J \;\; y_i - \lambda_y \geq x_i - \lambda_x - 2\eta \geq (2d)^{-1} - 2\eta = 2a.$$

Thus we showed that for every $x \in T_1^+$ there exist $H, L \subset [n]$ with $|H| = pn - m_0$, $|L| = (1-p)n$, and $y \in \Gamma(H, L) = \Gamma_{a,r}(H, L)$ such that $\|P_A x - P_A y\| \leq \eta$. Note also, that given H and L one can "reconstruct" I_0 as $I_0 = [n] \setminus (H \cup L)$.

Moreover, denoting

$$S := S_{I_0}^c = [n] \setminus \operatorname{supp} \sum_{i \in I_0} X_i.$$

and observing that $P_S M P_{I_0} = 0$ (indeed, for every $i \in S$ and $j \in I_0$ one has $\mu_{ij} = 0$), we get

$$\begin{aligned}
\|P_S M y\|_\infty &= \|P_S M x + P_S M(y - x)\|_\infty = \|P_S M x + P_S M P_A (y - x)\|_\infty \\
&\leq \|P_S M x\|_\infty + \|P_S M P_A (y - x)\|_\infty < \|Mx\|_\infty + \|M \,:\, \ell_\infty \to \ell_\infty\|\, \eta \\
&\leq 1/(8d) + \eta d < a,
\end{aligned}$$

provided that $\|Mx\|_\infty \leq 1/(8d)$. Thus, by the union bound, we obtain

$$p_0 \leq \sum_{y \in \mathcal{N}} \mathbb{P}\big(\{M \in \mathcal{M}_{n,d} \;:\; \|P_S M y\|_\infty < a\}\big),$$

where $S = S(y) = S_{I_0}^c$, $I_0 = I_0(y) = [n] \setminus (H \cup L)$ whenever $y \in \Gamma(H, L)$.

Finally we estimate the probabilities in the sum. Let $H, L \subset [n]$ be such that $|H| = pn - m_0$, $|L| = (1-p)n$, and $y \in \Gamma(H, L)$, J be from the definition $\Gamma(H, L)$ and S be as above. Let $I = [n] \setminus (J \cup L)$. Then I, J, L form a partition of $[n]$ with $|J| = r$ and $|I| = pn - r$. By assumptions of the lemma, this partition satisfies (22). Note also that assumptions on m_0 and r imply $m_0 d < n$, hence $|S| \geq n - m_0 d > 0$, and (23) is satisfied with $q := m_0 d$ (with $c_1 = c'/2$). By the definition of $\Gamma(H, L)$ the vector y satisfies

$$\forall i \in L \quad y_i = \lambda_y \qquad \text{and} \qquad \forall i \in J \;\; y_i - \lambda_y \geq 2a.$$

Applying Proposition 3.8 with the partition $\{I, J, L\}$, the vector y, and the set S, we obtain

$$\mathbb{P}\big(\{M \in \mathcal{M}_{n,d} \, : \, \|P_S M y\|_\infty < a\}\big) \leq \exp\left(-2c_1 dr \ln\left(\frac{n}{dr}\right)\right).$$

Since $\eta = 1/(9d^2)$, by (29) and (30), this implies

$$p_0 \leq |\mathcal{N}| \exp\left(-2c_1 dr \ln\left(\frac{n}{dr}\right)\right) \leq \left(\frac{18d^2 e}{p}\right)^{pn} \exp\left(-2c_1 dr \ln\left(\frac{n}{dr}\right)\right) \leq \exp\left(-c_1 dr \ln\left(\frac{n}{dr}\right)\right),$$

which completes the proof. $\square$

In the next lemma we prove an analogous statement for the set which is complementary to T_1. Recall that Ω_ε was introduced in Theorem 3.1 and let c_0 be the same constant as in that theorem.

Lemma 4.5. *Let $\varepsilon \in (0, 1/4)$. Let m_0, m_1, r be positive integers such that*

$$m_1 = m_0 + 2r < \min\{m_0/(2\varepsilon),\, c_0 \varepsilon n/d\}.$$

Consider the following subset of almost constant vectors

$$T_2 = \{x \in AC^+(p) \, : \, \textit{either} \quad |x^\star_{m_0}| = 0 \quad \textit{or} \quad (|x^\star_{m_0}| = 1 \quad \textit{and} \quad |J_x| < 2r\,)\}.$$

Then

$$\Omega_\varepsilon \subset \mathcal{E}_{T_2} := \{M \in \mathcal{M}_{n,d} \, : \, \forall x \in T_2 \quad Mx \neq 0\}.$$

To prove the lemma we need the following simple observation.

Claim 4.6. *Let $\varepsilon \in (0, 1/2)$, $1 \leq d \leq n$, and $1 \leq m \leq c_0 \varepsilon n/d$, where c_0 is the constant from the definition of Ω_ε. Let $M \in \Omega_\varepsilon$ and I be the set of indices corresponding to rows having exactly one 1 in columns indexed by $[m]$, i.e.*

$$I = \{i \in S_{[m]} \, : \, |\operatorname{supp} R_i \cap [m]| = 1\}.$$

Then $|I| \geq (1 - 2\varepsilon) dm > 0$.

Proof. Since $M \in \Omega_\varepsilon$,

$$|S_{[m]}| \geq (1-\varepsilon)dm.$$

Since rows R_i, $i \in I$, have exactly one 1 on $[m]$, while other rows indexed by $S_{[m]}$ have at least two ones on $[m]$, we observe

$$|I| + 2(|S_{[m]}| - |I|) \leq dm.$$

This implies the desired result. $\square$

Proof of Lemma 4.5. Let $M \in \Omega_\varepsilon$ and $x \in T_2$. For simplicity assume that $x = x^\star$, so that $|x_1| \geq |x_2| \geq ... \geq |x_n|$. Our proof consists of the following three cases.

Case 1: $|x_{m_0}| = 0$. Let $m_x \geq 1$ be the largest integer such that $|x_{m_x}| \neq 0$. Clearly $m_x < m_0$. Let I_x be the set of indices corresponding to rows having exactly one 1 in columns indexed by $[m_x]$. By Claim 4.6, $I_x \neq \emptyset$. Thus there exists a row R_i, $i \in I_x$, and a unique $j \in [m_x]$ such that $\mu_{ij} = 1$. This implies

$$(Mx)_i = \langle R_i, x\rangle = x_j \neq 0.$$

Case 2: $|x_{m_0}| = 1$, $|J_x| < 2r$, and $\lambda_x < 1/(2d)$. In this case the cardinality of the set

$$\{i \geq m_0 \,:\, |x_i| \geq \lambda_x + 1/(2d)\}$$

is less than $2r$. Since $m_1 - m_0 = 2r$, we have $|x_{m_1}| < \lambda_x + 1/(2d) < 1/d$.

Let $J_j = [m_j]$, $j = 0, 1$. We first show that there is a row R_i such that

$$|\operatorname{supp} R_i \cap J_0| = 1 \quad \text{ and } \quad |\operatorname{supp} R_i \cap (J_1 \setminus J_0)| = 0. \tag{32}$$

Let I be the set of indices corresponding to rows having exactly one 1 in J_1. By Claim 4.6, $|I| \geq (1-2\varepsilon)dm_1$. Since the number of nonzero rows on $J_1 \setminus J_0$ is at most $d|J_1 \setminus J_0|$, the number of rows satisfying (32) is at least

$$(1-2\varepsilon)dm_1 - d(m_1 - m_0) = d(m_0 - 2\varepsilon m_1) > 0,$$

that is there exists a row R_i satisfying (32). Denote $j_0 \in J_0$ the only coordinate of $P_{J_1}R_i$ which is equal to one, i.e. $\mu_{ij_0} = 1$ and for every $j \in J_1 \setminus \{j_0\}$, $\mu_{ij} = 0$. Therefore if $j \in \operatorname{supp} R_i$ and $j \neq j_0$ then $j > m_1$ and $|x_j| \leq |x_{m_1}|$. Since $|x_{m_1}| < 1/d$, we observe

$$|(Mx)_i| = |\langle R_i, x\rangle| \geq |x_{j_0}| - \sum_{\substack{j \in \operatorname{supp} R_{i_1} \\ j \neq j_1}} |x_j| \geq |x_{m_0}| - (d-1)|x_{m_1}| \geq 1 - \frac{d-1}{d} > 0.$$

Case 3: $|x_{m_0}| = 1$, $|J_x| < 2r$, and $\lambda_x \geq 1/(2d)$. Consider the set

$$J := \{i \leq n \,:\, 0 < x_i < \lambda_x + 1/(2d)\}.$$

Then $A := J^c \subset [m_0] \cup J_x$. Thus $|S_A| \le (m_0 + 2r)d < n$. Therefore, there exists a row R_j, $j \notin S_A$, such that $\operatorname{supp} R_j \subset J$. This implies

$$(Mx)_j = \langle R_j, x\rangle = \sum_{j\in J} x_j > 0.$$

Thus in all cases $Mx \neq 0$, which completes the proof. $\square$

Proof of Theorem 4.1. Recall that as we mentioned after the theorem it is enough to bound the probability of the event $\mathcal{E}^{AC+}$.

Let c, c_0, c_1 be constants from Lemmas 4.2 and 4.5. We choose $\varepsilon > 0$ to be small enough constant ($\varepsilon = \min\{1/8, c_1c_0/4, 32c/c_0\}$ would work), $m_0 = \lfloor 2c_0\varepsilon^2 n/d\rfloor$ and $r = \lfloor m_0/(8\varepsilon)\rfloor \approx c_0\varepsilon n/(4d)$, so that assumptions of Lemmas 4.2 and 4.5 on m_0 and r are satisfied. Finally, for a sufficiently small absolute positive constant c_2 we choose the biggest $p \le c_2/\ln d$ such that pn is an integer. Then assumptions of Lemma 4.2 on p are also satisfied (note that it is enough to prove the theorem with the biggest possible p). Therefore, applying these lemmas together with Theorem 3.1, we have

$$\mathbb{P}(\mathcal{E}_{T_1}) \ge 1 - 2\exp(-c_3 n) \quad\text{and}\quad \mathbb{P}(\mathcal{E}_{T_2}) \ge \mathbb{P}(\Omega_\varepsilon) \ge 1 - \exp\left(-c_4 d \ln\left(\frac{c_5 n}{d}\right)\right),$$

where T_1, T_2 are events from the lemmas and c_i's are absolute positive constants. Since $\mathcal{E}^{AC+} \supseteq \mathcal{E}_{T_1} \cap \mathcal{E}_{T_2}$ we obtain the desired result by adjusting absolute constants. $\square$

4.2 Auxiliary results

4.2.1 Simple facts

We will need the two following simple facts.

Claim 4.7. *Let $p \in (0, 1/3]$ and $x \in \mathbb{R}^n$. Assume that*

$$\forall \lambda \in \mathbb{R} \quad |\{i : x_i = \lambda\}| \le (1-p)n.$$

Then there exists $J \subset [n]$ such that

$$pn \le |J| \le (1-p)n \quad \text{and} \quad \forall i \in J\ \forall j \notin J \quad x_i \neq x_j.$$

Remark 4.8. We apply this claim twice, once in the following form. Let $m \le n$ and $\ell \le m/3$. Let $S \subset [n]$, $|S| = m$, and let $v \in \mathbb{R}^n$ satisfy $\forall \lambda \in \mathbb{R} \quad |\{i \in S : x_i \neq \lambda\}| \ge \ell$. Then there exists $J \subset S$ such that

$$\ell \le |J| \le m - \ell \quad \text{and} \quad \forall i \in J\ \forall j \in S \setminus J \quad v_i \neq v_j.$$

Proof of Claim 4.7. Let $\{\lambda_1, ..., \lambda_k\}$ be the set of all distinct values of coordinates of x. For $j \le k$, let $I_j = \{i : x_i = \lambda_j\}$ and $m_j = |I_j|$. Clearly, $m_j \le (1-p)n$ for every j. By relabeling assume that $m_1 \ge m_2 \ge ... \ge m_k$. If $m_1 \ge pn$, choose $J = I_1$. Otherwise set $J = I_1 \cup ... \cup I_\ell$, where ℓ is the smallest number satisfying $m := |J| = m_1 + ... + m_\ell \ge pn$. Since $m_j \le m_1 < pn$ for $j \le k$, then $m < 2pn$, and this implies

$$pn \le |J| < 2pn \le (1-p)n.$$

□

Let A, A_1, ..., A_m be sets such that every $x \in A$ belong to at least k of sets A_i's. Then we say that $\{A_i\}_i$ forms a k-fold covering of A.

The proof of the following fact uses a standard argument in measure theory, so we omit it.

Claim 4.9. *Let (X, μ) be a measure space. Let A, A_1, ..., A_m be subsets of X such that $\{A_i\}_i$ forms a k-fold covering of A. Then*

$$k\mu(A) \le \sum_{i=1}^{m} \mu(A_i).$$

4.2.2 Combinatorial results

In this section we prove a Littlewood-Offord type result, which will be one of key steps in the shuffling procedure.

Consider a probability space

$$\Omega_0 = \{B \subset [2d] \, : \, |B| = d\}$$

with the probability given by the normalized counting measure. For a vector $v \in \mathbb{R}^{2d}$ and $B \in \Omega_0$ denote

$$v_B = \sum_{i \in B} v_i.$$

Proposition 4.10. *Let $1 \le k \le d$. Let $v \in \mathbb{R}^{2d}$ and $a \in \mathbb{R}$. Assume there exists $J \subset [2d]$ such that $|J| = k$ and for every $i \in J$ and every $j \notin J$ one has $v_i \ne v_j$. Then*

$$\mathbb{P}(v_B = a) \le \frac{10}{\sqrt{k}}.$$

To prove Proposition 4.10 we need two combinatorial lemmas. We start with so-called anti-concentration Littlewood-Offord type lemma ([13], see also [19]). Usually it is stated for ± 1 Bernoulli random variables, but by shifting and rescaling it holds for any two-valued random variables, where by a two-valued random variable we mean a variable that takes two different values, each with probability half.

Lemma 4.11. *Let ξ_1, ξ_2, ..., ξ_m be independent two-valued random variables. Let $x \in \mathbb{R}^m$. Then*

$$\sup_{a \in \mathbb{R}} \mathbb{P}\Big(\sum_{i=1}^{m} \xi_i x_i = a \Big) \leq |\operatorname{supp} x|^{-1/2}.$$

Let Π_{2d} be the permutation group with a probability given by the normalized counting measure and denoted by $\mathbb{P}_{\Pi_{2d}}$. By π we denote a random permutation. The proof of the next lemma is rather straightforward, we postpone it to the end of the section.

Lemma 4.12. *Let $1 \leq k \leq d$. Let $x \in \mathbb{R}^{2d}$ and $J \subset [2d]$ be such that $|J| = k$ and for every $i \in J$ and every $j \notin J$ one has $x_i \neq x_j$. For $\pi \in \Pi_{2d}$ let*

$$E = E(\pi) = \big\{ (x_{\pi(i)}, x_{\pi(i+d)}) \, : \, i \leq d, \ x_{\pi(i)} \neq x_{\pi(i+d)} \big\}.$$

Then

$$\mathbb{P}_{\Pi_{2d}} \left(|E| \leq \frac{k}{50} \right) \leq \left(\frac{k}{1.1\, d} \right)^{k/3}.$$

Proof of Proposition 4.10. Let B be a (set-valued) random variable on Ω_0. Let $\delta = (\delta_1, ..., \delta_d)$ be a vector of independent Bernoulli random 0/1 variables ($\mathbb{P}(\delta_i = 1) = 1/2$ for $i \leq d$), and Ω denote the corresponding probability space. Consider a random (on $\Pi_{2d} \times \Omega$) set of indexes

$$A(\delta, \pi) = \{ \pi(i) \, : \, \delta_i = 1 \} \cup \{ \pi(i+d) \, : \, \delta_i = 0 \} \subset [2d].$$

Note that $|A(\delta, \pi)| = d$. It is not difficult to see that for every fixed δ, $A(\delta, \pi)$ has the same distribution as B. Therefore, $A(\delta, \pi)$ on $\Pi_{2d} \times \Omega$ has the same distribution as B on Ω_0. Thus, given $v \in \mathbb{R}^{2d}$, the random variable v_B has the same distribution as $v_{A(\delta,\pi)}$. Now we introduce the following random variables on $\Pi_{2d} \times \Omega$:

$$\xi_i = \xi_i^v = \delta_i v_{\pi(i)} + (1 - \delta_i) v_{\pi(i+d)}.$$

Note that $\mathbb{P}(\xi_i = v_{\pi(i)}) = \mathbb{P}(\xi_i = v_{\pi(i+d)}) = 1/2$ and that

$$v_{A(\delta,\pi)} = \sum_{i \in A(\delta,\pi)} v_i = \sum_{i=1}^{d} \xi_i.$$

Moreover, if we condition on π, the random variables $\bar{\xi}_i = \xi_i|_\pi$ are independent, hence we can apply Lemma 4.11. Denote by $m(\pi)$ the number of two-valued $\bar{\xi}_i$'s. Then

$$\mathbb{P}_\Omega \Big(\sum_{i=1}^{d} \bar{\xi}_i = a \Big) \leq \frac{1}{\sqrt{m(\pi)}}.$$

Finally, we note that by Lemma 4.12 we have many permutations with large $m(\pi)$, namely

$$\mathbb{P}_{\Pi_{2d}} \big(m(\pi) \leq k/50 \big) \leq \left(\frac{k}{1.1d} \right)^{k/3}.$$

Thus

$$\mathbb{P}\Big(\sum_{i=1}^{d} \xi_i = a\Big) \leq \sqrt{\frac{50}{k}} + \left(\frac{k}{1.1d}\right)^{k/3}.$$

This implies the desired result. □

Proof of Lemma 4.12. Without loss of generality we can assume that $x_i = 1$ for $i \leq k$ and $x_i = 0$ for $i > k$. Let π be a random permutation uniformly distributed over Π_{2d}. The basic idea of the proof is to condition on a realization of a set $\{i \leq d : x_{\pi(i)} = 1\}$ and show that the conditional probability of the event $|E| < k/50$ is small regardless of that realization.

Let $A = \{i \leq d : x_{\pi(i)} = 1\}$ be a random subset of $[d]$. Fix a subset $A_0 \subset [d]$ with $|A_0| \leq k$ (then the event $A = A_0$ has a non-zero probability). Denote $m := |A_0|$. Further, define a random subset $E_0 = \{i \in A_0 : x_{\pi(i+d)} = 1\}$. Clearly, we have $|E| = m - |E_0| + (k - m - |E_0|) = k - 2|E_0|$ everywhere on the event $\{A = A_0\}$. Let a parameter $\beta_1 \in (0, 0.1)$ be chosen later. Consider three cases.

Case 1: $m \leq (1-\beta_1)k/2$**.** Then clearly we have $|E| \geq k - 2m \geq \beta_1 k$ everywhere on the event $\{A = A_0\}$.

Case 2: $m \geq (1+\beta_1)k/2$**.** Since $|E_0| + m \leq k$ (deterministically), we have $|E| \geq 2m - k \geq \beta_1 k$ everywhere on $\{A = A_0\}$.

Case 3: $(1-\beta_1)k/2 \leq m \leq (1+\beta_1)k/2$**.** Note that the set $\{\pi(d+1), \pi(d+2), \dots, \pi(2d)\}$ contains $k - m$ ones and $d - k + m$ zeros. Thus, for every $\ell \leq k - m$ we have

$$p_\ell := \mathbb{P}(|E_0| = \ell \,|\, A = A_0) = \frac{1}{d!}\binom{m}{\ell}\binom{d-m}{k-m-\ell}(k-m)!(d-k+m)!,$$

where the second factor is the number of choices of subsets E_0 of A_0 of cardinality ℓ, the third factor is the number of possible choices of the set $\{d+1 \leq i \leq 2d : x_{\pi(i)} = 1 \text{ and } x_{\pi(i-d)} = 0\}$ provided that $|E_0| = \ell$, and the factors $(k-m)!$ and $(d-k+m)!$ are the numbers of all permutations of ones and zeros in the last d positions. Therefore,

$$p_\ell = \binom{d}{m}^{-1}\binom{k-m}{\ell}\binom{d-k+m}{m-\ell}$$

We choose $\beta > 3/4$ from $(1-\beta)(1-\beta_1)/2 = \beta_1$ and set $\beta_2 = 1 - \beta$. Using Chernoff bounds, we observe

$$\sum_{\ell \geq \beta m} \binom{d-k+m}{m-\ell} = \sum_{\ell \leq (1-\beta)m} \binom{d-k+m}{\ell} \leq \left(\frac{e(d-k+m)}{\beta_2 m}\right)^{\beta_2 m} \leq \left(\frac{ed}{\beta_2 m}\right)^{\beta_2 m}.$$

Since $k \leq 2m/(1-\beta_1)$ and $2/(1-\beta_1) - 1 - \beta = 2\beta_2$, then for $\ell \geq \beta m$,

$$\binom{k-m}{\ell} = \binom{k-m}{k-m-\ell} \leq \left(\frac{e(k-m)}{k-m-\beta m}\right)^{k-m-\beta m} \leq \left(\frac{e(1+\beta_1)}{2(1-\beta_1)\beta_2}\right)^{2\beta_2 m} \leq \left(\frac{3}{2\beta_2}\right)^{2\beta_2 m}.$$

Therefore we have

$$\sum_{\ell\geq\beta m} p_\ell \leq \left(\frac{m}{d}\right)^m \left(\frac{3}{2\beta_2}\right)^{2\beta_2 m} \left(\frac{ed}{\beta_2 m}\right)^{\beta_2 m} \leq \left(\frac{m}{d}\right)^{\beta m} \left(\frac{2}{\beta_2}\right)^{3\beta_2 m} \leq \left(\frac{(1+\beta_1)k}{2d} \left(\frac{2}{\beta_2}\right)^{3\beta_2/\beta}\right)^{\beta m}.$$

Choosing $\beta_1 = 1/50$ we obtain

$$\sum_{\ell\geq\beta m} p_\ell \leq \left(\frac{k}{1.1\,d}\right)^{k/3}.$$

On the event $\{A = A_0\}$ we have $|E| \geq m - |E_0|$, hence

$$\mathbb{P}(|E| \leq (1-\beta)m \,|\, A = A_0) \leq \sum_{\ell\geq\beta m} p_\ell.$$

Using that $m \geq (1-\beta_1)k/2$ and that $(1-\beta)(1-\beta_1)/2 = \beta_1$ we obtain

$$\mathbb{P}(|E| \leq \beta_1 k \mid A = A_0) \leq \left(\frac{k}{1.1\,d}\right)^{k/3},$$

which completes the proof. □

4.3 Proof of the main theorem

In this section, we complete the proof of the main result for adjacency matrices. The general scheme is similar to the one in [9, Section 4]. The main idea of the proof of Theorem A can be roughly described as follows: after throwing away all small "bad" events (namely, the existence of almost constant null vectors, big zero minors, and rows with largely overlapping supports) we split the remaining singular matrices from $\mathcal{M}_{n,d}$ into two sets

$$E_1 = \{M \in \mathcal{M}_{n,d} : \operatorname{rk} M = n-1\} \quad \text{and} \quad E_2 = \{M \in \mathcal{M}_{n,d} : \operatorname{rk} M \leq n-2\}.$$

Then, combining linear-algebraic arguments (Lemmas 4.16 and 4.17) with the shuffling procedure (Lemma 4.14), we show that E_1 and E_2 have a small proportion inside the sets $\mathcal{M}_{n,d}$ and $\{M \in \mathcal{M}_{n,d} : \operatorname{rk} M \leq n-1\}$, respectively. This implies that $E_1 \cup E_2$ has small probability.

The argument is rather technical and involves various events and "linear-algebraic" objects. To make the reading more convenient, we first group the notation used in this section.

4.3.1 Notation

For every $k \leq n$, let

$$\mathcal{E}_k = \{M \in \mathcal{M}_{n,d} : \operatorname{rk} M \leq k\}.$$

Our purpose is to estimate the probability of the event $\mathcal{E}_{n-1}$.

Let M be a matrix from $\mathcal{M}_{n,d}$ with rows R_i, $i \leq n$. For every $i \in [n]$, we denote by M^i the $(n-1) \times n$ minor of M obtained by removing the row R_i. Further, take a pair of distinct indices (i,j), $i \neq j \leq n$. By $M^{i,j}$ we denote the $(n-2) \times n$ minor of M obtained by removing the rows R_i, R_j. Additionally, define

$$V_{i,j} = V_{i,j}(M) = \operatorname{span}\{R_k,\, k \neq i,j\} \quad \text{and} \quad F_{i,j} = F_{i,j}(M) = \operatorname{span}\{V_{i,j},\, R_i + R_j\}.$$

In what follows, we write simply $V_{i,j}$ and $F_{i,j}$ instead of $V_{i,j}(M)$ and $F_{i,j}(M)$ as the matrix M will always be clear from the context. Note that the random vector $R_i + R_j$ and the random subspaces $V_{i,j}$ and $F_{i,j}$ are fully determined by the $(n-2) \times n$ matrix $M^{i,j}$.

As we see later, to be able to successfully apply the aforementioned shuffling to a pair of rows R_i, R_j, we will need at our disposal a vector orthogonal to the subspace $F_{i,j}$ such that its restriction to the union of the supports of R_i and R_j has many pairs of distinct coordinates. Of course, such a vector may not exist for some matrices $M \in \mathcal{M}_{n,d}$. We start by defining for every $q \in [n]$ and $i \neq j \leq n$ a "good" subset of $\mathcal{M}_{n,d}$ as follows:

$$\begin{aligned} \mathcal{E}^{i,j}(q) = \{M \in \mathcal{M}_{n,d} : \exists v \perp F_{i,j} \quad &\text{such that} \\ &\forall \lambda \in \mathbb{R} \ \ |\{k \in \operatorname{supp}(R_i + R_j) : \ v_k \neq \lambda\}| \geq q\}. \end{aligned} \tag{33}$$

For a matrix in this set we fix one vector satisfying (33), in fact we define it as a function of the matrix. The crucial fact for our proof is that since $F_{i,j}$ and $R_i + R_j$ are uniquely determined by $M^{i,j}$, we can fix such a vector for the class of matrices "sharing" the same minor $M^{i,j}$.

Definition 4.13. *Given $M \in \mathcal{E}^{i,j}(q)$, consider the equivalence class*

$$\mathcal{H}_M^{i,j}(q) = \{\widetilde{M} \in \mathcal{E}^{i,j}(q) \ : \ \widetilde{M}^{i,j} = M^{i,j}\}.$$

For every equivalence class $\mathcal{H}_M^{i,j}(q)$ fix one vector $v = v(M,q,i,j)$ satisfying

$$v \perp F_{i,j} \ \text{ and } \ \forall \lambda \in \mathbb{R} \ \ |\{k \in \operatorname{supp}(R_i + R_j) : \ v_k \neq \lambda\}| \geq q. \tag{34}$$

Whenever q and the indices i,j are clear from context, we write $v(M)$ instead of $v(M,q,i,j)$. One of the key ideas of the proof of Theorem A is to show that for most matrices M in $\mathcal{H}_M^{1,2}(q)$, the vector $v(M)$ does not belong to the kernel of M. To this end we introduce a subset of $\mathcal{E}^{1,2}(q)$

$$\mathcal{K}^{1,2}(q) = \{M \in \mathcal{E}^{1,2}(q) : \ v(M) \in \ker M\}.$$

In Lemma 4.14 below we will show that the ratio $|\mathcal{K}^{1,2}(q)|/|\mathcal{M}_{n,d}|$ goes to zero as $d \to \infty$.

As we mentioned above, in the proof we essentially restrict ourselves to the set of matrices, which have no almost constant null-vectors, no big zero minors, and no rows with largely overlapping supports. To define this set formally, let $0 < p \leq 1/3$, $2 \leq q \leq d/2$, and $\varepsilon \in (0,1)$. Denote

$$\Theta = \Theta(p,q,\varepsilon) := \mathcal{E}^{AC}(p) \cap \Omega_\varepsilon^2 \setminus \Omega^0\big(p/2q, p/2\big),$$

where Ω^2_ε, $\Omega^0(p/2q, p/2)$, and $\mathcal{E}^{AC}(p)$ were introduced in Proposition 3.3, (20), and (27), respectively. By Proposition 3.3, Theorem 4.1 , and (21) we have

$$\mathbb{P}(\Theta^c) \le \frac{n^2}{2}\left(\frac{ed}{\varepsilon n}\right)^{\varepsilon d} + \left(\frac{Cd}{n}\right)^{cd} + e^{-cn} \le n^2\left(\frac{ed}{\varepsilon n}\right)^{\varepsilon d} \le \left(\frac{ed}{\varepsilon n}\right)^{\varepsilon d/2} \tag{35}$$

provided that $p \le c_1/\ln d$, $q = c_2 p^2 d$, $c_3/\varepsilon^2 \le d \le \varepsilon n/6$ and ε is small enough.

Further we will need two more auxiliary events dealing with the $(n-2)\times n$ minors $M^{i,j}$ of M. For $i \ne j$, introduce

$$\mathcal{E}^{i,j}_{n-2} = \{M \in \mathcal{M}_{n,d} \,:\, \operatorname{rk} M^{i,j} = n-2 \quad \text{and} \quad R_i + R_j \notin V_{i,j}\},$$

and

$$\mathcal{E}^{i,j}_{rk} = \{M \in \mathcal{M}_{n,d} \,:\, R_i, R_j \in V_{i,j}\}.$$

Note that for every $M \in \mathcal{E}^{i,j}_{rk}$ we have $\operatorname{rk} M = \operatorname{rk} M^{i,j}$. In the next section we prove several statements involving events $\mathcal{E}^{i,j}_{n-2}$, $\mathcal{E}^{i,j}_{rk}$, and $\mathcal{K}^{1,2}(q)$.

4.3.2 Proof of Theorem A

The next lemma encapsulates the shuffling procedure. Recall that Ω^2_ε was defined in Proposition 3.3.

Lemma 4.14. *Let $\varepsilon \in (0,1)$ and $2\varepsilon d < q \le 2d/3$. Then*

$$\mathbb{P}\left(\mathcal{K}^{1,2}(q) \,\middle|\, \mathcal{E}^{1,2}(q) \cap \Omega^2_\varepsilon\right) \le \frac{10}{\sqrt{(q-2\varepsilon d)}}.$$

Proof. Note that

$$\mathcal{K}^{1,2}(q) = \{M \in \mathcal{E}^{1,2}(q) :\, \langle v(M), R_1\rangle = 0\}.$$

Let $M \in \mathcal{E}^{1,2}(q) \cap \Omega^2_\varepsilon$. Denote

$$S_{1,2} = S_{1,2}(M) = \operatorname{supp} R_1 \cup \operatorname{supp} R_2, \quad s_{1,2} = s_{1,2}(M) = \operatorname{supp} R_1 \cap \operatorname{supp} R_2$$

and set

$$S = S(M) = S_{1,2} \setminus s_{1,2}, \quad m_1 = |S_{1,2}|, \quad m_2 = |s_{1,2}|, \quad \text{and} \quad m = |S|.$$

Note that $m_1 = 2d - m_2$ and $m = m_1 - m_2 = 2(d - m_2)$. By the definition of Ω^2_ε, we have

$$m_1 \ge 2(1-\varepsilon)d \quad \text{and} \quad m_2 \le 2\varepsilon d.$$

By (34), the vector $v := v(M)$ satisfies $\forall \lambda \in \mathbb{R} \quad |\{i \in S \,:\, x_i \ne \lambda\}| \ge q - m_2$. Since $q - m_2 \le m/3$, by Claim 4.7 (see Remark 4.8) there exists $J \subset S$ such that

$$q - m_2 \le |J| \le m - (q - m_2) \ \text{ and } \ \forall i \in J \ \ \forall j \in S \setminus J \quad v_i \ne v_j. \tag{36}$$

We compute the desired probability as follows. For every (fixed) $M \in \mathcal{E}^{1,2}(q) \cap \Omega_\varepsilon^2$ consider the equivalence class

$$\mathcal{F}_M := \mathcal{H}_M^{1,2}(q) \cap \Omega_\varepsilon^2 = \left\{ \widetilde{M} \in \mathcal{E}^{1,2}(q) \cap \Omega_\varepsilon^2 \ : \ \widetilde{M}^{1,2} = M^{1,2} \right\}.$$

Note that by construction $S_{1,2}(\widetilde{M}) = S_{1,2}(M) = S_{1,2}$, $s_{1,2}(\widetilde{M}) = s_{1,2}(M) = s_{1,2}$ and $v(\widetilde{M}) = v(M) = v$ for every matrix $\widetilde{M}$ in $\mathcal{F}_M$. Therefore it is enough to show that the proportion of matrices $\widetilde{M} \in \mathcal{F}_M$ satisfying $\langle v, R_1(\widetilde{M})\rangle = 0$ is small. Every matrix $\widetilde{M} \in \mathcal{F}_M$ is determined by its minor $M^{1,2}$ (which is fixed on $\mathcal{F}_M$) and its first row $R_1(\widetilde{M})$. Thus to determine a matrix in $\mathcal{F}_M$ it is enough to choose a support of the first row, which is a subset of $S_{1,2}$. Since m_2 elements in $\operatorname{supp} R_1$ are fixed (as $s_{1,2}$ is fixed) then we have to calculate how many $(d - m_2)$-element subsets B of m-element set S exist so that

$$\langle v, R_1\rangle = \sum_{i \in B \cup s_{1,2}} v_i = 0,$$

that is

$$\sum_{i \in B} v_i = a := -\sum_{i \in s_{1,2}} v_i.$$

For vectors $v = v(M)$ satisfying (36) this was calculated in Proposition 4.10 (note that $m = 2(d - m_2)$, a is independent of $B \subset S$ and apply the proposition with $q - m_2$ and $m/2$ instead of k and d). Applying this for all classes $\mathcal{F}_M$, we obtain the desired bound. □

In what follows, we will show that, up to intersection with $\Theta \cap \mathcal{E}^{1,2}(q) \cap \mathcal{E}_{n-2}^{1,2}$ (resp., $\Theta \cap \mathcal{E}^{1,2}(q) \cap \mathcal{E}_{rk}^{1,2}$), the event $E_1 = \mathcal{E}_{n-1} \setminus \mathcal{E}_{n-2}$ (resp., $E_2 = \mathcal{E}_{n-2}$) is a subset of $\mathcal{K}^{1,2}(q)$, hence has a small probability. Our treatment of singular matrices M with $\operatorname{rk} M = n-1$ and $\operatorname{rk} M \le n-2$ is slightly different, although the general idea is the same – at the first step, given a singular matrix M, we fix a left null vector $y = y(M)$ and a right null-vector $x = x(M)$ and choose a row R_i such that $\operatorname{rk} M^i = \operatorname{rk} M$ and x has many distinct coordinates on R_i. On the next step, we choose a second row R_j so that the minor $M^{i,j}$ is of maximal rank, that is $\operatorname{rk} M^{i,j} = n-2$ in the case $\operatorname{rk} M = n-1$ and $\operatorname{rk} M^{i,j} = \operatorname{rk} M$ in the case $\operatorname{rk} M \le n-2$. We also show that there are many choices for such i and j. Finally, using the shuffling, we show, in a sense, that we can increase the rank of a matrix by "playing" with rows i and j only, i.e. that the events $\mathcal{E}_{n-2}$ and $\mathcal{E}_{n-1}$ are small inside $\mathcal{E}_{n-1}$ and $\mathcal{M}_{n,d}$ respectively. The next lemma describes the set of "good" i's for the first step.

Lemma 4.15. *Let $0 < p \le 1/3$, and $q \ge 2$ be such that $pn/2q$ is an integer. Further, let*

$$M \in \mathcal{E}_{n-1} \cap \mathcal{E}^{AC}(p) \setminus \Omega^0\big(p/2q, p/2\big)$$

and $x \in \ker M \setminus \{0\}$, $y \in \ker M^T \setminus \{0\}$. Consider the set of indices

$$I_M(x,y) = \{i \in \operatorname{supp} y : \ \forall \lambda \in \mathbb{R} \ |\{j \in \operatorname{supp} R_i \ : \ x_j \ne \lambda\}| \ge q\}.$$

Then

$$|I_M(x,y)| \ge pn/2.$$

Note that for $y \in \ker M^T$ we have $\sum_i y_i R_i = 0$ and $I_M(x,y) \subset \operatorname{supp} y$. Therefore removing the row R_i, $i \in I_M(x,y)$, we do not decrease the rank of M, that is $\operatorname{rk} M^i = \operatorname{rk} M$.

Proof of Lemma 4.15. Since $x \notin AC(p)$ and $p \le 1/3$, by Claim 4.7 there exists a subset $J_x \subset [n]$ such that

$$pn \le |J_x| \le (1-p)n \quad \text{and} \quad \forall i \in J_x \ \forall j \notin J_x \quad x_i \neq x_j.$$

Now we compute how many rows have more than q ones in J_x and more than q ones in J_x^c. Since $M \notin \Omega^0(p/2q, p/2)$ then applying Lemma 3.6 with $\alpha = p/(2q)$ and $\beta = p$, we get

$$|\{i \ : \ |\operatorname{supp} R_i \cap J_x| \ge q\}| \ge (1-p/2q)n \quad \text{and} \quad |\{i \ : \ |\operatorname{supp} R_i \cap J_x^c| \ge q\}| \ge (1-p/2q)n.$$

Therefore

$$|\{i \ : \ |\operatorname{supp} R_i \cap J_x| \ge q \quad \text{and} \quad |\operatorname{supp} R_i \cap J_x^c| \ge q\}| \ge (1-p/q)n.$$

By the construction of the set J_x this implies that the set

$$I := \{i \ : \ \forall \lambda \in \mathbb{R} \quad |\{j \in \operatorname{supp} R_i \ : \ x_j \neq \lambda\}| \ge q\}$$

has cardinality at least $(1-p/q)n$. Finally, since $y \notin AC(p)$, we have that $|\operatorname{supp} y| \ge pn$, which implies

$$|I_M(x,y)| = |I \cap \operatorname{supp} y| \ge pn - pn/q \ge pn/2,$$

and completes the proof. $\square$

Now we consider the set of matrices $M \in \Theta$ with $\operatorname{rk} M \le n-2$.

Lemma 4.16. *Let p, q satisfy the assumptions of Lemma 4.15, $\varepsilon \in (0,1)$, and let $\mathcal{E} = \mathcal{E}_{n-2} \cap \Theta$ with $\Theta = \Theta(p,q,\varepsilon)$. Then*

$$\mathbb{P}(\mathcal{E}) \le 2p^{-2}\ \mathbb{P}(\mathcal{E}_{rk}^{1,2} \cap \mathcal{E}^{1,2}(q) \cap \mathcal{E}).$$

Proof. Fix $M \in \mathcal{E}$. There exist $x \in \ker M \setminus \{0\}$ and $y \in \ker M^T \setminus \{0\}$, that is

$$\forall i \le n \ \ x \perp R_i \quad \text{and} \quad \sum_{i \in \operatorname{supp} y} y_i R_i = 0.$$

Note that by the definition of Θ we have $x, y \notin AC(p)$. We compute how many ordered pairs (i,j), $i \neq j$, satisfy

$$R_i, R_j \in V_{i,j} \quad \text{and} \quad \forall \lambda \in \mathbb{R}\ |\{k \in \operatorname{supp}(R_i + R_j) : \ x_k \neq \lambda\}| \ge q.$$

By Lemma 4.15, the set $I_M(x,y)$ satisfies $|I_M(x,y)| \ge pn/2$, and for every $i \in I_M(x,y)$ we have $\operatorname{rk} M^i = \operatorname{rk} M$. Next, since $\operatorname{rk} M^i < n-1$, the set $\ker(M^i)^T \setminus \{0\}$ is non-empty, i.e.

$$\exists y^{(i)} \in \mathbb{R}^n \setminus \{0\} \ \text{ such that } \ y^{(i)}_i = 0, \quad \sum_{j=1}^n y^{(i)}_j R_j = 0.$$

Clearly $y^{(i)} \in \ker M^T \setminus \{0\}$, and, since $M \in \mathcal{E}^{AC}(p)$, $y^{(i)}$ has at least pn non-zero coordinates; moreover,

$$\forall j \leq n \quad \text{such that} \quad y_j^{(i)} \neq 0 \quad \text{one has} \quad R_j \in V_{i,j}.$$

This shows that for every $M \in \mathcal{E}$ there are at least $(pn)^2/4$ pairs (i,j) with $i < j$ satisfying $R_i, R_j \in V_{i,j}$. Obviously $x \perp F_{i,j}$ for every $i, j \leq n$. Hence for each pair (i,j) we have

$$R_i, R_j \in V_{i,j}, \quad x \perp F_{i,j} \quad \text{and} \quad \forall \lambda \in \mathbb{R} \; |\{k \in \operatorname{supp}(R_i + R_j) : \; x_k \neq \lambda\}| \geq q,$$

implying that M belongs to at least $(pn)^2/4$ distinct subsets among $\{\mathcal{E}_{rk}^{i,j} \cap \mathcal{E}^{i,j}(q) \cap \mathcal{E}\}_{i<j}$.

Thus, $\{\mathcal{E}_{rk}^{i,j} \cap \mathcal{E}^{i,j}(q) \cap \mathcal{E}\}_{i<j}$ forms a $((pn)^2/4)$-fold covering for $\mathcal{E}$. Since

$$\mathbb{P}\left(\mathcal{E}_{rk}^{i,j} \cap \mathcal{E}^{i,j}(q) \cap \mathcal{E}\right) = \mathbb{P}\left(\mathcal{E}_{rk}^{1,2} \cap \mathcal{E}^{1,2}(q) \cap \mathcal{E}\right)$$

then applying Claim 4.9, we obtain

$$\frac{(pn)^2}{4}\, \mathbb{P}(\mathcal{E}) \leq \sum_{i<j} \mathbb{P}\left(\mathcal{E}_{rk}^{i,j} \cap \mathcal{E}^{i,j}(q) \cap \mathcal{E}\right) = \frac{n(n-1)}{2}\, \mathbb{P}\left(\mathcal{E}_{rk}^{1,2} \cap \mathcal{E}^{1,2}(q) \cap \mathcal{E}\right).$$

This completes the proof of the lemma.

□

Now we treat the case when a matrix has rank $n-1$.

Lemma 4.17. *Let p, q satisfy the conditions of Lemma 4.15, $\varepsilon \in (0,1)$, and let $\mathcal{E} = (\mathcal{E}_{n-1} \setminus \mathcal{E}_{n-2}) \cap \Theta$ with $\Theta = \Theta(p, q, \varepsilon)$. Then*

$$\mathbb{P}\big(\mathcal{E}\big) \leq 2p^{-2}\, \mathbb{P}\big(\mathcal{E}_{n-2}^{1,2} \cap \mathcal{E}^{1,2}(q) \cap \mathcal{E}\big).$$

Proof. Repeating the first step of the proof of Lemma 4.16, we fix $M \in \mathcal{E}$, $x \in \ker M \setminus \{0\}$, $y \in \ker M^T \setminus \{0\}$. Then by Lemma 4.15 the set of indices $I_M(x,y)$ has cardinality $|I_M(x,y)| \geq pn/2$ and for every $i \in I_M(x,y)$ the $(n-1) \times n$ minor M^i satisfies $\operatorname{rk} M^i = \operatorname{rk} M$.

Now, we calculate how many ordered pairs (i,j), $i \neq j$, exist such that

$$\operatorname{rk} M^{i,j} = n-2 \qquad \text{and} \qquad R_i + R_j \notin V_{i,j}.$$

Let $i \in I_M(x,y)$. Since $y \notin AC(p)$, there are at least pn choices of j such that $y_j \neq y_i$. Fix such a j. We claim that then $R_i + R_j \notin V_{i,j}$. Indeed, otherwise

$$R_i + R_j = \sum_{\ell \neq i,j} z_\ell R_\ell$$

for some $z_\ell \in \mathbb{R}$, hence there exists $w \in \ker M^T \setminus \{0\}$ such that $w_i = w_j$. Since the dimension of $\ker M^T$ is one, we have $y = \lambda w$ for some $\lambda \in \mathbb{R}$, which contradicts the condition $y_i \neq y_j$. Therefore, there are at least $(pn)^2/2$ pairs (i,j) with $i \neq j$ satisfying

$$\operatorname{rk} M^{i,j} = n-2, \qquad R_i + R_j \notin V_{i,j},$$

and

$$x \perp F_{i,j}, \qquad \forall \lambda \in \mathbb{R} \ \ |\{k \in \operatorname{supp}(R_i + R_j) \ : \ x_k \neq \lambda\}| \geq q.$$

In other words, the matrix M belongs to at least $(pn)^2/2$ events $\mathcal{E}_{n-2}^{i,j} \cap \mathcal{E}^{i,j}(q) \cap \mathcal{E}$. Thus, we proved that $\{\mathcal{E}_{n-2}^{i,j} \cap \mathcal{E}^{i,j}(q) \cap \mathcal{E}\}_{i<j}$ forms a $((pn)^2/4)$-fold covering of $\mathcal{E}$. Since for every $i < j$,

$$\mathbb{P}\left(\mathcal{E}_{n-2}^{i,j} \cap \mathcal{E}^{i,j}(q) \cap \mathcal{E}\right) = \mathbb{P}\left(\mathcal{E}_{n-2}^{1,2} \cap \mathcal{E}^{1,2}(q) \cap \mathcal{E}\right),$$

then applying Claim 4.9, we obtain

$$\frac{(pn)^2}{4}\, \mathbb{P}(\mathcal{E}) \leq \sum_{i<j} \mathbb{P}\left(\mathcal{E}_{n-2}^{i,j} \cap \mathcal{E}^{i,j}(q) \cap \mathcal{E}\right) = \frac{n(n-1)}{2}\, \mathbb{P}\left(\mathcal{E}_{n-2}^{1,2} \cap \mathcal{E}^{1,2}(q) \cap \mathcal{E}\right),$$

and the proof is complete. $\square$

We now can finish Theorem A.

Proof of Theorem A. Let p, q, ε be chosen later to satisfy assumptions in the corresponding statements. By Lemmas 4.16, 4.17 and (35) we obtain

$$\begin{aligned}\mathbb{P}(\mathcal{E}_{n-1}) &\leq \mathbb{P}\big(\mathcal{E}_{n-2} \cap \Theta\big) + \mathbb{P}\big((\mathcal{E}_{n-1} \setminus \mathcal{E}_{n-2}) \cap \Theta\big) + \left(\frac{ed}{\varepsilon n}\right)^{\varepsilon d/2} \\ &\leq 2p^{-2}\big(\mathbb{P}(A) + \mathbb{P}(B)\big) + \left(\frac{ed}{\varepsilon n}\right)^{\varepsilon d/2},\end{aligned}$$

where

$$A = \mathcal{E}_{rk}^{1,2} \cap \mathcal{E}^{1,2}(q) \cap \mathcal{E}_{n-2} \cap \Theta \quad \text{ and } \quad B = \mathcal{E}_{n-2}^{1,2} \cap \mathcal{E}^{1,2}(q) \cap (\mathcal{E}_{n-1} \setminus \mathcal{E}_{n-2}) \cap \Theta.$$

We show now that

$$A \cup B \subset \mathcal{K}^{1,2}(q) \cap \mathcal{E}^{1,2}(q) \cap \Omega_\varepsilon^2.$$

In other words, we verify that for a matrix $M \in A \cup B$ the vector $v(M) \in F_{1,2}^{\perp}$ (see Definition 4.13) belongs to $\ker M$.

Indeed, if $M \in A$, then $R_1, R_2 \in V_{1,2}$. Using the condition $v(M) \in F_{1,2}^{\perp}$ we immediately get $v(M) \in \ker M$.

If $M \in B$ then $\operatorname{rk} M = n-1$, $\operatorname{rk} M^{1,2} = n-2$, and $R_1 + R_2 \notin V_{1,2}$. Therefore $\dim F_{1,2} = n-1$. Since $\ker M \subseteq F_{1,2}^{\perp}$ and $\dim \ker M = \dim F_{1,2}^{\perp} = 1$ we infer $\ker M = F_{1,2}^{\perp}$ and thus $v(M) \in \ker M$.

Finally note that A and B are disjoint, so $\mathbb{P}(A) + \mathbb{P}(B) = \mathbb{P}(A \cup B)$. Applying Lemma 4.14 we obtain

$$\mathbb{P}(\mathcal{E}_{n-1}) \leq 2p^{-2}\mathbb{P}\left(\mathcal{K}^{1,2}(q) \cap \mathcal{E}^{1,2}(q) \cap \Omega_\varepsilon^2\right) + \left(\frac{ed}{\varepsilon n}\right)^{\varepsilon d/2} = \frac{20}{p^2\sqrt{(q - 2\varepsilon d)}} + \left(\frac{ed}{\varepsilon n}\right)^{\varepsilon d/2}.$$

Finally we choose the parameters. Let c_1, c_2 be sufficiently small positive absolute constants. Choose $p = c_1/\ln d$ and q to be the largest integer not exceeding $c_2 p^2 d = c_1 c_2 d/\ln^2 d$ (we slightly adjust c_1, c_2 so that $pn/2q$ is also an integer). Let $\varepsilon = q/(4d) \approx 1/\ln^2 d$ (note that then the condition $c_3/\varepsilon^2 \le d \le \varepsilon n/6$ needed in (35) is also satisfied). Then we obtain the desired bound. $\square$

Remark 4.18. We could choose $q = -cdp/\ln p \approx d/((\ln\ln d)\ln d)$, then $\varepsilon = q/(4d) \approx 1/((\ln\ln d)\ln d)$. This would lead to the restriction $d \le cn/((\ln\ln n)\ln n)$ instead of $d \le cn/\ln^2 n$ in Theorem A.

References

[1] N. Alon and J.H. Spencer. *The probabilistic method.* Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2008. With an appendix on the life and work of Paul Erdős.

[2] R. Bauerschmidt, J. Huang, A. Knowles, and H.T. Yau. *Bulk eigenvalue statistics for random regular graphs*, arXiv:1505.06700.

[3] R. Bauerschmidt, A. Knowles, and H.T. Yau. *Local semicircle law for random regular graphs,* arXiv:1503.08702.

[4] B. Bollobás. *A probabilistic proof of an asymptotic formula for the number of labelled regular graphs*, European J. Combin., **4** (1980), 311–316.

[5] B. Bollobás. *The isoperimetric number of random regular graphs*, European J. Combin., **9** (1988), 241–244.

[6] J. Bourgain, V.H. Vu and P. M. Wood, *On the singularity probability of discrete random matrices*, J. Funct. Anal. **258** (2010), no. 2, 559–603.

[7] S. Chatterjee, *A short survey of Stein's method*, Proceedings ICM, Vol. 4, 2014, 1–24.

[8] N.A. Cook, *Discrepancy properties for random regular digraphs*, Random Structures Algorithms, to appear.

[9] N.A. Cook, *On the singularity of adjacency matrices for random regular digraphs*, Prob. Th. Rel. Fields, to appear.

[10] C. Cooper, A. Frieze, B. Reed, O. Riordan, *Random regular graphs of non-constant degree: independence and chromatic number*, Combin. Probab. Comput. **11** (2002), 323–341.

[11] K.P. Costello, T. Tao and V. Vu, *Random symmetric matrices are almost surely nonsingular*, Duke Math. J. **135** (2006), no. 2, 395–413.

[12] I. Dumitriu and S. Pal, *Sparse regular random graphs: spectral density and eigenvectors*, Ann. Probab. **40** (2012), 2197–2235.

[13] P. Erdős, *On a lemma of Littlewood and Offord*, Bull. Amer. Math. Soc. **51** (1945), 898–902.

[14] J. Friedman. *A proof of Alon's second eigenvalue conjecture and related problems*, Mem. Amer. Math. Soc., **195** (2008), no. 910.

[15] A. Frieze, *Random structures and algorithms*, Proceedings ICM, Vol. 1, 2014, 311–340.

[16] A.M. Frieze and T. Łuczak. *On the independence and chromatic numbers of random regular graphs*, J. Combin. Theory Ser. B, **54** (1992), 123–132.

[17] S. Hoory, N. Linial and A. Wigderson, *Expander graphs and their applications,* Bull. Amer. Math. Soc. (N.S.) **43** (2006), no. 4, 439–561.

[18] J. Kahn, J. Komlós and E. Szemerédi, *On the probability that a random* ± 1*-matrix is singular*, J. Amer. Math. Soc. **8** (1995), no. 1, 223–240.

[19] D.J. Kleitman, *On a Lemma of Littlewood and Offord on the Distributions of Linear Combinations of Vectors*, Adv. Math., **5** (1970), 155–157.

[20] B. Kolesnik and N. Wormald. *Lower bounds for the isoperimetric numbers of random regular graphs*, SIAM J. Discrete Math., **28** (2014), 553–575.

[21] J. Komlós, *On the determinant of* $(0,1)$ *matrices*, Studia Sci. Math. Hungar **2** (1967), 7–21.

[22] J. Komlós, Circulated Manuscript, Available online at http://math.rutgers.edu/∼komlos/01short.pdf.

[23] M. Krivelevich, B. Sudakov, V.H. Vu, and N. C. Wormald. *Random regular graphs of high degree*, Random Structures Algorithms, **18** (2001), 346–363.

[24] A.E. Litvak, A. Lytova, K. Tikhomirov, N. Tomczak-Jaegermann, P. Youssef, *Anti-concentration property for random digraphs and invertibility of their adjacency matrices*, C.R. Math. Acad. Sci. Paris, **354** (2016), 121–124.

[25] B.D. McKay, *Subgraphs of random graphs with specified degrees*, Congr. Numer. **33** (1981), 213–223.

[26] B.D. McKay, *The expected eigenvalue distribution of a large regular graph*, Linear Algebra Appl. **40** (1981), 203–216.

[27] H.H. Nguyen, *Inverse Littlewood-Offord problems and the singularity of random symmetric matrices*, Duke Math. J. **161** (2012), 545–586.

[28] H.H. Nguyen, *On the singularity of random combinatorial matrices*, SIAM J. Discrete Math. **27** (2013), 447–458.

[29] M. Rudelson and R. Vershynin, *Non-asymptotic theory of random matrices: extreme singular values*, Proceedings ICM, Vol. 3, 2010, 1576–1602.

[30] M. Rudelson and R. Vershynin, *The Littlewood-Offord problem and invertibility of random matrices*, Adv. Math. **218** (2008), 600–633.

[31] J.K. Senior, *Partitions and their representative graphs*, Amer. J. Math. **73** (1951), 663–689.

[32] T. Tao and V. Vu, *Inverse Littlewood-Offord theorems and the condition number of random discrete matrices*, Annals of Math., **169** (2009), 595–632.

[33] T. Tao and V. Vu, *From the Littlewood-Offord problem to the circular law: universality of the spectral distribution of random matrices*, Bull. Amer. Math. Soc. (N.S.) **46** (2009), 377–396.

[34] T. Tao and V. Vu, *On the singularity probability of random Bernoulli matrices*, J. Amer. Math. Soc. **20** (2007), 603–628.

[35] L.V. Tran, V.H. Vu and K. Wang, *Sparse random graphs: eigenvalues and eigenvectors*, Random Structures Algorithms **42** (2013), 110–134.

[36] R. Vershynin, *Invertibility of symmetric random matrices*, Random Structures Algorithms **44** (2014), 135–182.

[37] V. Vu, *Random discrete matrices*, Horizons of combinatorics, Bolyai Soc. Math. Stud., **17**, 257–280, Springer, Berlin, 2008.

[38] V.H. Vu, *Combinatorial problems in random matrix theory*, Proceedings ICM, Vol. 4, 2014, 489–508.

Alexander E. Litvak, Anna Lytova, Konstantin Tikhomirov and Nicole Tomczak-Jaegermann,
Dept. of Math. and Stat. Sciences,
University of Alberta,
Edmonton, Alberta, Canada, T6G 2G1.
e-mail: aelitvak@gmail.com, lytova@ualberta.ca, ktikhomi@ualberta.ca,
nicole.tomczak@ualberta.ca

Pierre Youssef,
Université Paris Diderot,
Laboratoire de Probabilités et de modèles aléatoires,
75013 Paris, France.
e-mail: youssef@math.univ-paris-diderot.fr