The Rectangle Covering Number
of Random Boolean Matrices

Mozhgan Pourmoradnasseri   Dirk Oliver Theis[*]

Institute of Computer Science
University of Tartu
Ülikooli 17, 51014 Tartu, Estonia

{mozhgan,dotheis}@ut.ee

Abstract

The rectangle covering number of an $n \times n$ Boolean matrix M is the smallest number of 1-rectangles which are needed to cover all the 1-entries of M. Its binary logarithm is the Nondeterministic Communication Complexity, and it equals the chromatic number of a graph $G_{\boxtimes}(M)$ obtained from M by a construction of Lovász and Saks.

We determine the rectangle covering number and related parameters (clique size, independence ratio, fractional chromatic number of $G_{\boxtimes}(M)$) of random Boolean matrices, where each entry is 1 with probability $p = p(n)$, and the entries are independent.

1   Introduction

For a positive integer n, a *rectangle* is a product $R = K \times L \subset [n] \times [n]$ (with $[n] := \{1, \ldots, n\}$). Given an $n \times n$ matrix M with 0/1 entries, a *1-rectangle* is a rectangle R with $M_{k,\ell} = 1$ for all $(k, \ell) \in R$. A *rectangle covering* of M is a collection of 1-rectangles $R^{(1)}, \ldots, R^{(r)}$ such that $\{(k, \ell) \mid M_{k,\ell} = 1\} = \bigcup_r R^{(r)}_{k,\ell}$, i.e., every 1-entry of M is contained in one of the chosen 1-rectangles. The *rectangle covering number* [28, 27], $\mathrm{rc}(M)$, of M is the smallest number of 1-rectangles in a rectangle covering of M. The *nondeterministic communication complexity* [25] of M is $\lceil \log_2(\mathrm{rc}(M)) \rceil$.

Rectangle covering is the same as covering by bicliques the edges of the bipartite graph H_M whose vertex set is the disjoint union $[n] \uplus [n]$, and whose bipartite adjacency matrix

---

equals M. Hence, the term *biclique covering* is often used. In Matrix Theory, the name *Boolean rank* [5, 6, 24] is common. There, the Boolean rank lower bounds the nonnegative rank [15]: Indeed, the rectangle covering number is the best possible lower bound on the nonnegative rank if one considers only zero-nonzero information of the matrix (cf. [26]).

Rectangle covering coincides with the *2-dimension* of certain posets (cf. [8]) and with the strong isometric dimension of certain graphs [13]. It has applications in coding theory [16], and connections to extremal set theory [17].

The rectangle covering number is an important lower bound on the so-called extension complexity [36] of polytopes, a quantity of interest in Combinatorial Optimization: Lower bounds on the rectangle covering number were the techniques which allowed to prove exponential lower bounds for sizes of linear programming formulations for a number of combinatorial optimization problems [9, 10, 3]. While random 01-matrices have high rank, the matrices occurring in Combinatorial Optimization, so-called slack matrices, have arbitrary real (or rational) entries, and their ranks are typically only polylog in their sizes. It is important to realize that, while the rank of the actual slack matrix is a lower bound to the extension complexity, the rank of the 01-matrix (each non-zero entry of the slack matrix is replaced by 1) is not.

As hinted above, the rectangle covering number is the chromatic number of the *(Lovász-Saks) rectangle graph*, $G_{\boxtimes}(M)$, of the matrix M which has as its vertices the 1-entries of M, with two 1-entries being adjacent, if they span a 2×2 rectangle containing a 0-entry of M. More precisely:

$$V(G_{\boxtimes}(M)) = \left\{ (k, \ell) \in [n] \times [n] \mid M_{k,\ell} = 1 \right\}$$
$$E(G_{\boxtimes}(M)) = \left\{ \{(k, \ell), (k', \ell')\} \mid M_{k,\ell} M_{k',\ell'} = 1 \ \& \ M_{k,\ell'} M_{k',\ell} = 0 \right\}.$$

The following is implicit in [27], and implies $\chi(G_{\boxtimes}(M)) = \mathrm{rc}(M)$.

Proposition 1.1 ([27])**.** *The inclusion-wise maximal 1-rectangles of M are precisely the vertex sets of the inclusion-wise maximal independent sets of $G_{\boxtimes}(M)$.*

Other parameters of M and $G_{\boxtimes}$ are used as lower bounds in the application areas: the ratio "number of 1-entries by size of the largest 1-rectangle" is the independence ratio of $G_{\boxtimes}$; so-called fooling sets in M coincide with cliques in $G_{\boxtimes}$; the so-called generalized fooling set bound [7] coincides with the Hall ratio (the supremum of all independence ratios of induced subgraphs) of $G_{\boxtimes}$; fractional rectangle covering [20] is the same as fractional coloring of $G_{\boxtimes}$. (Except for the part about fooling sets, all of these statements follow from Prop. 1.1.) A fooling set (cf., e.g., [25, 11]), is a set of 1-entries of M which, when considered as edges of H_M (see above), form a *cross-free matching,* i.e., a matching no two of whose edges induce a $K_{2,2}$ in H_M.[1] Fooling sets are referred to as sets of *independent* entries in Matrix Theory [4].

---

[1]More precisely, a matching $M \subseteq E \subseteq [n] \times [n]$ is *cross-free* if, for every $(k, \ell), (k', \ell') \in M$ we have $(k, \ell) = (k', \ell')$ or $(k, \ell') \notin E$ or $(k', \ell) \notin E$.

Our results and connections to related work. In this paper we study the rectangle covering number, and the parameters listed above, of a random $n \times n$ Boolean matrix $M^{n,p}$, where each entry is independently 1 with probability $p = p(n)$ and 0 with probability $1 - p$, or, respectively, of the random graph $G_\boxtimes^{n,p} := G_\boxtimes(M^{n,p})$. As usual, we are interested in $n \to \infty$.

In (Communication) Complexity Theory, random objects are usually used for establishing that hard objects exist in the given model of computation. In this spirit, some easy results about the (nondeterministic) communication complexity of random functions and related parameters exist, with p a constant, mostly $p = 1/2$.

For us, part of the motivation for investigating the parameters studied in this paper was to see to which extend random Boolean matrices behave similarly to the difficult families of matrices in Combinatorial Optimization whose rectangle covering number one would like to bound. In these families, the number of zeros per row/column is typically small, i.e., the typical number of 0-entries per row is polylog n. In terms of random matrices, this prompted us to look at these parameters when $p = p(n) \to 1$ with $n \to \infty$ – in the spirit of the study of properties of Erdős-Rényi random graphs. In an analogy to those random graphs, the results become both considerably more interesting and also more difficult that way.

The clique number of $G_\boxtimes^{n,1/2}$ (fooling set size) was shown [7] to be $\Theta(\ln n)$, asymptotically almost surely ("a.a.s.", i.e., the probability of that happening tends to 1 with $n \to \infty$). In the interesting examples from Combinatorial Optimization, the fooling set bound is typically $O(\ln n)$—even worse than the theoretical maximum (from Turán's theorem, cf. [8]) of $O(\text{polylog } n)$ for matrices with $O(\text{polylog } n)$ zeros per row/column. For example, for the Spanning Tree polytope, it was recently shown that the fooling set bound is (almost) useless [22]. This is in line with what we observe in random matrices: We give upper and lower bounds for $\omega(G_\boxtimes^{n,p})$ for $p \to 1$ and also for $p \to 0$, based on matchings in random (binomial) bipartite graphs (Section 5).

Recently, Izhakian, Janson, and Rhodes [18] have determined asymptotically the so-called triangular rank of random Boolean matrices with independent Bernoulli entries. The triangular rank is important in Communication Complexity [27] and in Combinatorial Optimization [26], and it is a lower bound to the size of a fooling set. In Izhakian et al.'s paper, determining the behavior for $p \to 0, 1$ is posed as an open problem.

The size of the largest monochromatic rectangle in a random Bernoulli matrix was determined in [31] when p is bounded away from 1, but their technique fails for $p \to 1$. We determine the asymptotic behaviour of that parameter (the independence number of the Lovász-Saks rectangle graph) for $p \to 1$ (Section 4). The importance of this parameter lies mainly in the fact that the independence ratio (the number of vertices over the independence number) is a lower bound to the chromatic number.

The chromatic number of $G_\boxtimes^{n,1/2}$ is given in Sherstov's lecture notes on Communication Complexity[2]. The rectangle covering number of Clique-vs-Stable-Set (which is important in the context of the extension complexity of the Stable Set polytope) on random graphs

---

[2]http://www.cs.ucla.edu/~sherstov/teaching/2012-winter/

was studied in [3]. We discuss the chromatic number $\chi(G_{\boxtimes}^{n,p})$ and the fractional chromatic number $\chi^*(G_{\boxtimes}^{n,p})$ in Section 6.

Interestingly, the ratio χ/χ^* tends to infinity a.a.s. in a certain range of p. This is not only a notable difference to the situation $p = {}^1\!/_2$, where the chromatic number and the independence ratio (which also lower bounds the fractional chromatic number) coincide a.a.s. It also distinguishes this random graph model from, say, Erdős-Renyi random graphs, where, a.a.s., the independence ratio is within a constant factor of the chromatic number.

Since the fractional chromatic number is today the most sucessfully used (combinatorial) lower bound for extension complexity, it came as a surprise to the authors that random rectangle graphs exhibit a gap between the fractional chromatic number and the cromatic number, at least in some parameter ranges. This phenomenon coincides with observations about some of the matrix families in Combinatorial Optimization, (e.g., related to spanning trees in complete graphs, see, e.g., [35, 23]), where the fractional chromatic number might be a weak lower bound. We refer the reader to the conclusions for a discussion of concrete conjectures on χ-vs-χ^*.

An extended abstract (without proofs) of the results of this paper was accepted to the 13th annual conference on Theory and Applications of Models of Computation, in a form taylored to Complexity Theory audience [32]. (The conference was canceled and accepted papers were presented one year later at the April 2017 TAMC.)

2 Some basic properties of rectangle covering

We summarize some properties of the rectangle covering number in the following remark. All proofs are easy to trivial, and we leave them to the reader as a warm-up.

Remark 2.1.

 (a) Trivial upper bound: If M is an $m \times n$ matrix then $\mathrm{rc}(M) \leqslant \min(n, m)$.

 (b) Redundant rows or columns: If the set of 1s of row k equals the union of the sets of 1s of other rows, then deleting row k does not change the rectangle covering number. A special case is a row with no 1s. Another special case is this: If n' (m', resp.) is the number of distinct, non-0 rows (columns, resp.) of M, then $\mathrm{rc}(M) \leqslant \min(n', m')$.

 (c) The rectangle covering number is not monotone in the set of 1s. Changing a 0 into a 1 can affect the rectangle covering number in both directions.

2.1 Hypergraphs and the Binary Logarithm lower bound

Let $H = (V, E)$ be a hypergraph and $E' \subset 2^V$. We say that E' *generates* H, if every $e \in E$ is a union of $e' \in E'$; in symbols:

$$\text{For all } e \in E: \quad e = \bigcup_{\substack{e' \in E' \\ e' \subseteq e}} e'$$

The *generation number*, gen(H), of H is the smallest number of sets in a E' which generates H. The following is an easy lower bound for the generation number.

Lemma 2.2. *If H is a hypergraph with all edges distinct, then* gen(H) $\geqslant \log_2 |E(H)|$.

Proof. Let E' generate H, and for each $e \in E(H)$ consider the set $E'_e := \{e' \in E(H') \mid e' \subseteq e\}$. Since $e = \bigcup_{e' \in E'_e} e'$, the hyperedge e is uniquely determined by $E'_e \in 2^{E(H')}$. Hence, $2^{|E(H')|} \geqslant E$. $\qquad\square$

We leave the proof of the following proposition to the reader. The trick is use 1-rectangles "generated by" row/column sets (see the definition before Theorem 4.1, p. 7).

Proposition 2.3. *Let H be a hypergraph and M its vertex-hyperedge incidence matrix, i.e., $M_{v,e} = 1$ iff $v \in e$. Then* gen(H) $=$ rc(M).

This means that hypergraph generation and rectangle covering are equivalent concepts, and we obtain the following lower bound on the rectangle covering number.

Remark 2.4 (Log-2-lower-bound). If a Boolean matrix has m' distinct rows and n' distinct columns, then rc(M) $\geqslant \log_2(\max(m', n'))$.

This simple bound has been found independently in Communication Complexity (cf., e.g., [28]), Matrix Theory [1], and Combinatorial Optimization [14].

3 The random graph $G_\boxtimes^{n,p}$

We use the conventions
$$\bar{p} = 1 - p, \text{ and } \lambda = \bar{p}n.$$
E.g., the expected number of zeros in each row of $M^{n,p}$ is λ.

We denote the number of vertices of $G_\boxtimes^{n,p}$ by N. It is a Bin(n^2, p) binomial random variable.

3.1 The cases when p tends to 0 or 1 very fast

When p tends to 0 or 1 quickly, the graph is nearly deterministic, and there is nothing much to study in terms of random properties.

Denote by $G_{(r)}$ the graph whose vertices are all pairs $(k, \ell) \in \{1, \ldots, r\} \times \{1, \ldots, n\} \cup \{1, \ldots, n\} \times \{1, \ldots, r\}$ with $k \neq \ell$, and let (k, ℓ) be adjacent to (k', ℓ') iff $k = \ell'$ or $\ell = k'$.

Proposition 3.1.

(a) *For $p = o(n^{-3/2})$, $G_\boxtimes^{n,p}$ is a clique with $pn^2 + O(\sqrt{p}n) = o(\sqrt{n})$ vertices.*

(b) *for $p = 1 - o(n^{-3/2})$, the graph $G_\boxtimes^{n,p}$ is, a.a.s., isomorphic to a disjoint union of $(n - R)^2$ isolated vertices with $G_{(R)}$, for $R := (n^2 - N) = \bar{p}n^2 + O(\sqrt{\bar{p}}n) = o(\sqrt{n})$.*

Proof (sketch). For (a), by, say, Chebyshev's inequality, we have, a.a.s., $N = pn^2 + O(\sqrt{p}n) = o(sqrtn)$, since the standard deviation of N is at most $\sqrt{p}n$. Moreover, the probability that a fixed row (or column) of $M^{n,p}$ contains two or more ones is at most $p^2 \binom{n}{2} = o(1/n)$, so that, by the union bound, a.a.s., there is no row (or column) which contains two or more ones. Thus, $G_{\boxtimes}^{n,p}$ is a clique of $o(\sqrt{n})$ vertices.

For (b), the same argument shows that the number $R := n^2 - N$ of zero-entries of $M^{n,p}$ is $o(\sqrt{n})$ a.a.s., and that, a.a.s., no two of them are in the same row or column. Hence, after permuting rows and columns, can transform $M^{n,p}$ into a matrix all of whose entries are 1, except for the entries $(1,1), \dots, (R,R)$, which are 0. So there are $(n-R)^2$ isolated vertices (bottom right part of the matrix), and the top R rows and leftmost R columns form a $G_{(R)}$. The same application of Chebyshev as above completes the proof. $\square$

Hence, the smallest interesting p is $\Omega(n^{-3/2})$, and the largest interesting p is $1 - \Omega(n^{-3/2})$.

3.2 The cases when p tends to 0 or 1 not too fast

If pn^2 tends to infinity sufficiently fast, then the number of vertices of $G_{\boxtimes}^{n,p}$ is concentrated near pn^2

Denote the number of edges of $G_{\boxtimes}^{n,p}$ by N'. For two potential vertices $u, v \in \{1, \dots, n\}^2$, we have $\mathbf{P}(u \sim v \mid u, v \in V(G_{\boxtimes}^{n,p})) = 1 - p^2 =: \delta$. We fix this meaning of δ for the remainder of the paper. Now

$$\mathbf{E}\, N' = p^2(1-p^2)\frac{n^2(n-1)^2}{2} = \delta\binom{pn^2}{2} + O(p^2 n^3) = \delta\binom{\mathbf{E}\, N}{2} + O(p^2 n^3),$$

so that the expected density of $G_{\boxtimes}^{n,p}$ is asymptotic to δ if N is concentrated. Changing a single matrix entry can affect the number of edges, N', by up to $2n - 1$, so we do not expect very good concentration. But, if p is $\Omega(1/n)$ and $1 - \Omega(1/n)$, then, an application of Chebyshev's inequality shows that we have, a.a.s.,

$$N' = \delta\binom{pn^2}{2} + O\big(pn^2\sqrt{\delta}\big). \tag{1}$$

This is a special case of the concentration of the number of r-cliques, which we discuss in Section 5.

Let us take a more precise look at the number of edges, conditioned on the number of vertices. With $\pi := N/n^2$, we find that the probability, conditioned on N, that a fixed 2-by-2 submatrix of $M^{n,p}$ gives an edge of $G_{\boxtimes}^{n,p}$ equals[3]

$$\frac{2\binom{n^2-4}{N-2} + 4\binom{n^2-4}{N-3}/2}{\binom{n^2}{N}}$$

$$= 2\frac{(n^2 - N)N(N-1)}{(n^2)_4}\left(n^2 - N - 1 + 2(N-2)\right)$$

---

[3]As usual, we denote by $(a)_b := a(a-1)\dots,(a-b+1)$ the falling factorial.

$$= 2 \frac{(n^2 - N)N(N-1)}{(n^2)_4} (n^2 + N - 3)$$
$$= 2\pi^2(1 - \pi^2) + O(1/n^2),$$

and hence,

$$\mathbf{E}(N' \mid N) = \binom{n}{2}^2 \cdot 2\pi^2(1-\pi^2) = (1-\pi^2)\binom{\pi n^2}{2} + O(\pi^2 n^3) = (1-\pi^2)\binom{N}{2} + O(N^2/n) \quad (2)$$

3.3 Concentration of clique number and chromatic number

The clique size (fooling set size) and the chromatic number (corresponding to the nondeterministic communication complexity) are concentrated: Changing one row (or column) of the matrix can change each of these numbers by at most 1, so a standard application of McDiarmid's inequality [29] yields the following.

Proposition 3.2. *(a) The size, $\omega(G_{\boxtimes}^{n,p})$, of the largest clique in $G_{\boxtimes}^{n,p}$ is within t from its mean with probability at least $1 - 2e^{2t^2/n}$.*

(b) The chromatic number, $\chi(G_{\boxtimes}^{n,p})$, of $G_{\boxtimes}^{n,p}$ is within t from its mean with probability at least $1 - 2e^{2t^2/n}$.

The bounds are only useful when ω and χ are larger than $\sqrt{n}$. However, we will see in Sections 5 and 6 that for $p = 1 - o(1)$, ω becomes small (even $O(1)$ ultimately) and χ becomes $O(\text{polylog } n)$.

For the clique number, in that region of p, we can give upper and lower bounds differing by a small constant factor, but for the chromatic number, we do not know any similarly strong concentration results.

4 Independence number (largest 1-rectangle)

Let $\alpha(\cdot)$ denote the independence number of a graph. We extend the results of Park et al. [31] from $p = \Theta(1)$ to $p = 1 - o(1)$.

For $K \subseteq \{1, \ldots, n\}$, the *1-rectangle generated by the row-set K in M* is the largest 1-rectangle R in M with row set K, i.e., $R = K \times L$ with

$$L := \left\{ \ell \in \{1, \ldots, n\} \mid \forall \, k \in K \colon \ M_{k,\ell} = 1 \right\}.$$

The 1-rectangle generated by a set of columns is defined similarly. Note that every inclusion-wise maximal 1-rectangle is generated by its row-set and also by its column set.

Theorem 4.1.

(a) If $5/n \leqslant p \leqslant 1/e$, then a.a.s., the largest 1-rectangle is generated by a single row or column, and if $p \gg (\ln n)/n$, its size is $(1 + o(1))pn$.

(b) Define

$$a_- := \lfloor \log_{1/p} e \rfloor,$$
$$a_+ := \lceil \log_{1/p} e \rceil, \quad \text{and} \tag{3}$$
$$a := \operatorname{argmax}_{b \in \{a_-, a_+\}} b p^b = \operatorname{argmax}_{b \in \{1,2,3,\dots\}} b p^b.$$

There exists a constant λ_0, such that if $1/e \leqslant p \leqslant 1 - \lambda_0/n$, then, a.a.s., a largest 1-rectangle is generated by a rows or columns and its size is $(1 + o(1))ap^a n$.

The result is important for Section 6. In the proof, we first get rid of rectangles which are squares, using a simple union bound, and then use Chernoff-style concentration for non-square rectangles.

Before we present the proof in §§4.1–4.2, we discuss the result. First of all, note that $\log_{1/p} e = 1/\ln(1/p)$. The following helps compare the quantities.

Remark 4.2. (a) If $p \geqslant 1/e$, then

$$1/e^2 \leqslant \frac{p}{e} \leqslant p \cdot p^{\log_{1/p} e} \leqslant p^a \leqslant \frac{1}{p} \cdot p^{\log_{1/p} e} \leqslant \frac{1}{pe} \leqslant 1/e, \tag{4}$$

i.e., $p^a \approx 1/e$, more accurately $p^a = (1 - o_{p \to 1}(1))/e$.

(b) With $p = 1 - \bar{p} = 1 - \lambda/n$, the following makes the range of $\alpha(G_{\boxtimes}^{n,p})$ clearer: Since $\bar{p} \leqslant \ln(1/(1-\bar{p})) \leqslant \bar{p} + \bar{p}^2$ holds when $\bar{p} \leqslant 1 - 1/e$, we have

$$\frac{1}{e\bar{p}} = \frac{n}{e\lambda} \leqslant p\frac{n}{\lambda} = \frac{p}{\bar{p}} \leqslant \frac{1}{1+\bar{p}} \cdot \frac{1}{\bar{p}} \leqslant \log_{1/p} e \leqslant \frac{1}{\bar{p}} = \frac{n}{\lambda} \tag{5}$$

Corollary 4.3. *For $p = 1 - \frac{\lambda}{n}$ with $\lambda_0 \leqslant \lambda = o(n)$, we have $\alpha(G_{\boxtimes}^{n,p}) = \dfrac{n^2}{e\lambda} + O(n)$.*

Proof of the corollary from Theorem 4.1. For the given $p = 1 - \bar{p}$, if $1/e = p^a$, we have

$$ap^a = (1 + O(\bar{p}))\frac{\log_{1/p} e}{e} = \frac{1 + O(\bar{p})}{e \ln \frac{1}{1-\bar{p}}}$$

$$= \frac{1 + O(\bar{p})}{e\left(\bar{p} + \bar{p}^2/2 + \bar{p}^3/3 + \dots\right)} \underset{(*)}{=} \frac{1 + O(\bar{p})}{e\bar{p}} = \frac{1}{e\bar{p}} + O(1) = \frac{n}{e\lambda} + O(1),$$

where equation $(*)$ uses $\bar{p} = o(1)$. Multiplying by n and invoking Theorem 4.1(b), we obtain the desired bound. $\qquad \square$

4.1 Small p: Proof of Theorem 4.1 (a)

Theorem 4.1 (a) occurs in a weaker form in [31], with the additional condition that $p = \Omega(1)$: Their proof does not cover the case $p \to 0$; the following one does.

We say that a rectangle is *bulky*, if it extends over at least 2 rows and also over at least 2 columns. The proof of Theorem 4.1 proceeds by considering three types of rectangles:

1. those consisting of exactly one row or column (they give the bound in the theorem);

2. square bulky rectanges;

3. bulky rectangles which are not square.

Let us start with the easiest type (1). The size of such a rectangle is the number of 1s in the chosen row.

Lemma 4.4. *For all p, n, a.a.s., there exists a row in $M^{n,p}$ containing at least pn 1s. If $p \gg (\ln n)/n$, for every constant $\varepsilon \in \,]0, 1]$, a.a.s., no row or column has more than $(1 + \varepsilon)pn$ 1s.*

Proof. For the first statement, note that the probability that number of 1s in a fixed row is less than pn is at most $1/2$ (median of a binomial distribution). Since the rows are independent, the probability that all rows have fewer than pn 1s is at most 2^{-n}.

For the second statement, we use an easy Chernoff-type bound (Theorem 4.4(2) in [30]). Denote by X the number of 1s in a fixed row of $M^{n,p}$. Then

$$\mathbf{P}(X \geqslant (1 + \varepsilon)pn) \leqslant e^{-\varepsilon^2 pn/3} \leqslant e^{-2\ln n} = n^{-2},$$

where the last inequality holds for large enough n, because $pn \gg \ln n$ implies $pn > 6\varepsilon^{-2} \ln n$ for n sufficiently large. Hence, the probability that a row (or a column) exists which has at least $(1 + \varepsilon)pn$ 1s is $o(1)$. $\qquad \square$

We now deal with rectangles of type (2).

Lemma 4.5. *If $p \geqslant 5/n$, then, a.a.s., there is no square 1-rectangle of size $\sqrt{pn} \times \sqrt{pn}$.*

Proof. We abbrevieate $\kappa := pn$. By the union bound, for the probability $q = q(n)$ that there exists a 1-rectangle of size $\sqrt{\kappa} \times \sqrt{\kappa}$, we have

$$q \leqslant \binom{n}{\sqrt{\kappa}}^2 p^\kappa \leqslant \left(\frac{e^2 n}{p}\right)^{\sqrt{\kappa}} p^\kappa;$$

where we used the inequality $\binom{s}{t} \leqslant (es/t)^t$. Applying $\ln$, we find

$$\ln q \leqslant \sqrt{\kappa} \ln n + 2\sqrt{\kappa} + \sqrt{\kappa} \ln(1/p) - \kappa \ln(1/p) = \sqrt{\kappa}\Big(\ln n + 2 - \big(\sqrt{\kappa} - 1\big)\ln(1/p)\Big). \quad (6)$$

Now we distinguish cases. If $(2\ln n)^2/n \leqslant p \leqslant 1/e$, then $\sqrt{\kappa} \geqslant 2\ln n$, and hence we can bound the expression in the parentheses in (6) as follows:

$$\ln n + 2 - \big(\sqrt{\kappa} - 1\big)\ln(1/p) \leqslant \ln n + 2 - 2\ln n + 1 \leqslant -\ln n,$$

for all large enough n. Hence, $q \to 0$ in this region. If, on the other hand, $5/n \leqslant p \leqslant (2\ln n)^2/n$, then

$$\ln q \leqslant \sqrt{5}\Big(\ln n + 2 - \big(\sqrt{5} - 1\big)\big(\ln n - 2\ln(2\ln n)\big)\Big)$$
$$\leqslant -\sqrt{5}\big(\sqrt{5} - 2\big)\ln n + O(\ln \ln n) = -\Omega(\ln n).$$

Hence, $q \to 0$ in this region, too, which completes the proof of the lemma. $\qquad \square$

Finally, we come to rectangles of type (3). Consider the probability, ϱ, that $M^{n,p}$ contains a bulky 1-rectangle of size s. By Lemma 4.5, if such a 1-rectangle has dimensions $a \times b$, we must have $a < \sqrt{pn}$ or $b < \sqrt{pn}$, or else $\varrho = o(1)$. We have $\varrho \leqslant 2\varrho'$, where ϱ' is the probability that $M^{n,p}$ contains a 1-rectangle of size s consisting of at least as many columns than rows. For ϱ', we need to consider only 1-rectangles with $a < \sqrt{pn}$. Moreover, increasing b if necessary, w.l.o.g., we may restrict to rectangles generated by a row-set of size a, with $2 \leqslant a \leqslant n$ (the lower bound $a \geqslant 2$ comes from the condition that the rectangle be bulky).

Lemma 4.6. *With $\kappa = pn$, if $5 \leqslant \kappa = O(\mathrm{polylog}\, n)$, then, a.a.s., there is no bulky rectangle of size at least κ.*

Proof. By the remarks above, we have to bound the probability that there exists a row-set of size $a \in \{2, \dots, \sqrt{\kappa}\}$ which generates a 1-rectangle of size at least κ/a.

Firstly, for a given set K of a rows, we bound the probability that the rectangle it generates has size at least pn. Denote by S the number of columns in the rectangle generated by K. This is a $\mathrm{Bin}(n, p^a)$ r.v. and we find that

$$\mathbf{P}(a \cdot b \geqslant \kappa) = \mathbf{P}(S \geqslant \kappa/a) \leqslant \binom{n}{\kappa/a} p^\kappa = \binom{n}{\kappa/a} \left(\frac{\kappa}{n}\right)^\kappa.$$

Secondly, we sum over all sets K of cardinality a, and compute

$$\binom{n}{a}\binom{n}{\kappa/a} p^\kappa (1 - p^a)^{n-\kappa/a} \quad \leqslant \quad n^{a+\kappa/a-\kappa+\kappa\log_n \kappa} \quad = \quad n^{-\left(\kappa(1-1/a)-a-o(\kappa)\right)},$$

where $\kappa \log_n \kappa = o(\kappa)$ follows from $\kappa = O(\mathrm{polylog}\, n)$.

Now, because $a < \sqrt{\kappa}$, we have that the exponent on $1/n$ is $\kappa(1 - 1/a) - o(\kappa) \geqslant \kappa/3$, as $a \geqslant 2$. Finally, summing over all a, we obtain, as an upper bound for the probability that one of these rectangles has size κ or larger, the expression $n^{-(\kappa/3-1)}$ which is $o(1)$, as $\kappa \geqslant 5$. $\qquad\square$

Now we deal with bulky rectangles.

Lemma 4.7. *With $\kappa := pn$, if $\ln^4 n \leqslant \kappa \leqslant n/e$, then, a.a.s., there is no bulky rectangle of size at least κ.*

Proof. By the remarks above Lemma 4.6, we have to bound the probability that there exists a row-set of size $a \in \{2, \dots, \sqrt{\kappa}\}$ which generates a 1-rectangle of size at least κ/a.

For $2 \leqslant a < \sqrt{\kappa}$, let X_a count the number of columns ℓ with $M_{k,\ell} = 1$ for $k = 1, \dots, a$. We are going to show that

$$P := \sum_{a=2}^{\sqrt{\kappa}} \binom{n}{a} \mathbf{P}\left(X_a \geqslant \kappa/a\right) = o(1).$$

The r.v. X_a has $\mathrm{Bin}(n, p^a)$ distribution. We compute

$$\mathbf{P}\big(X_a \geqslant {}^{\kappa}\!/a\big) \leqslant \binom{n}{{}^{\kappa}\!/a}(p^a)^{\kappa/a} \leqslant \left(\frac{en}{{}^{\kappa}\!/a}\right)^{\kappa/a} (p^a)^{\kappa/a} = \left(\big((ea)^{1/(a-1)}p\big)^{\kappa/a}\right)^{a-1}. \quad (7)$$

Now there exists a constant $\varrho < 1$ such that

$$(ea)^{1/(a-1)} \leqslant \begin{cases} 8\varrho, & \text{for all } a \geqslant 2, \text{ and} \\ e\varrho, & \text{for } a \geqslant 4. \end{cases} \quad (8)$$

Consequently, we distinguish two cases:

(i) $p \leqslant {}^1\!/8$ and

(ii) ${}^1\!/8 < p \leqslant {}^1\!/e$.

Case (i): $\boldsymbol{p \leqslant {}^1\!/8}$. In this case, we compute

$$\begin{aligned}
P &= \sum_{a=2}^{\sqrt{\kappa}} \binom{n}{a} \mathbf{P}\big(X_a \geqslant {}^{\kappa}\!/a\big) \\
&\leqslant \sum_{a=2}^{\sqrt{\kappa}} \binom{n}{a} \left(\big((ea)^{1/(a-1)}p\big)^{\kappa/a}\right)^{a-1} && \text{[by (7)]} \\
&\leqslant \sum_{a=2}^{\sqrt{\kappa}} \binom{n}{a} \left(\varrho^{\kappa/a}\right)^{a-1} && \text{[by (8)]} \\
&\leqslant \sum_{a=2}^{\sqrt{\kappa}} \binom{n}{a} \left(\varrho^{\sqrt{\kappa}}\right)^{a-1} && \text{[since } a \leqslant \sqrt{\kappa} \text{ and } \varrho < 1] \\
&= \varrho^{\sqrt{\kappa}} \sum_{a=2}^{\sqrt{\kappa}} \binom{n}{a} \left(\varrho^{\sqrt{\kappa}}\right)^{a-2} \\
&\leqslant \varrho^{\sqrt{\kappa}}\, n^2 \sum_{a=0}^{\sqrt{\kappa}-2} \binom{n-2}{a} \left(\varrho^{\sqrt{\kappa}}\right)^{a} && \text{[replacing } a \rightsquigarrow a-2] \\
&\leqslant \varrho^{\sqrt{\kappa}}\, n^2 \,(1+\varrho^{\sqrt{\kappa}})^{n-2} && \text{[Binomial theorem]} \\
&\leqslant \varrho^{\sqrt{\kappa}}\, n^2 \, e^{n\varrho^{\sqrt{\kappa}}} \\
&\leqslant \varrho^{\sqrt{\kappa}}\, n^2 \, e^{n\varrho^{\ln^2 n}} && \text{[because } p \geqslant (\ln^4 n)/n \text{ and } \varrho < 1] \\
&= o(1) && \text{[because } \varrho = 1 - \Omega(1).]
\end{aligned}$$

Case (ii): ${}^1\!/8 < p \leqslant {}^1\!/e$. In this case, by (8), the same calculation as in the $p < {}^1\!/8$-case works if the sum is started with $a = 4$. For the first two terms of the sum, $a = 2, 3$, we use a Chernoff bound on X_a. The convenient choice is Corollary 21.9 in [12]: With

$c := ap^{1-a}$ and $\mu := \mathbf{E}\,X_a$, we have

$$
\begin{aligned}
\mathbf{P}(X_a \geqslant \kappa/a) &= \mathbf{P}(X_a \geqslant c\mu) \\
&\leqslant (e^{1-1/c}/c)^{c\mu} \qquad\qquad \text{[Corollary 21.9 in [12]]} \\
&= (e^{1-1/c}/c)^{pn/a} \\
&= (1 + \Omega(1))^{\Omega(n)} = o(n^{-3}) \quad (*),
\end{aligned}
\tag{9}
$$

where $(*)$ follows as $a \geqslant 2$ implies that $c = 1 + \Omega(1)$ (c is greater than and bounded away from 1), which in turn implies that $e^{1-1/c}/c = 1 - \Omega(1)$ (the base of the exponent is less than and bounded away from 1).

We conclude

$$
\begin{aligned}
P &= \sum_{a=2}^{\sqrt{\kappa}} \binom{n}{a} \mathbf{P}(X_a \geqslant \kappa/a) \\
&= \binom{n}{2} \mathbf{P}(X_2 \geqslant \kappa/2) + \binom{n}{3} \mathbf{P}(X_3 \geqslant \kappa/3) + \sum_{a=4}^{\sqrt{\kappa}} \binom{n}{a} \mathbf{P}(X_a \geqslant \kappa/a) \\
&\hspace{8cm} = o(1) + o(1) + o(1),
\end{aligned}
$$

where the first two "$o(1)$"s follow from (9), and the third is the same calculation as in the previous case. $\qquad\square$

This concludes the proof of Theorem 4.1(a).

4.2 Large p: Proof of Theorem 4.1(b)

Now we prove the part of Theorem 4.1 about $p \geqslant 1/e$. Again, we first prove a statement about square rectangles.

Lemma 4.8. *For every $\varepsilon > 0$ there exists a constant λ_0 such that, if $\bar{p}n = \lambda \geqslant \lambda_0$, then, a.a.s., there is no square 1-rectangle of size*

$$
\frac{n}{\lambda^{1-\varepsilon}} \times \frac{n}{\lambda^{1-\varepsilon}}
$$

Proof. This is a direct union bound computation. With $b := \frac{n}{\lambda^{1-\varepsilon}}$, the probability that such a 1-rectangle exists is at most

$$
\binom{n}{b}^2 p^{b^2} = \binom{n}{b}^2 (1 - \bar{p})^{b^2} \leqslant e^{b(2\ln(en/b) - \lambda b/n)} = e^{b \cdot A_b},
$$

where

$$
\begin{aligned}
A_b &= 2\ln(en/b) - \lambda b/n \\
&= 2\ln(e\,\lambda^{1-\varepsilon}) - \lambda^{\varepsilon} \leqslant -1,
\end{aligned}
$$

where the last inequality holds if $\lambda \geqslant \lambda_0$ and λ_0 is large enough. The claim follows because $b \to \infty$ (since $\lambda \leqslant n$. $\qquad\square$

As above, we need the notion of a "bulky" rectangle: Here, we say that a rectangle of dimensions $k \times \ell$ is *bulky,* if $k \leqslant \ell$. By Lemma 4.8, in particular, a.a.s., a bulky rectangle must have $k < n/\lambda^{2/3}$. Again, by exchanging the roles of rows and columns, and multiplying the final probability estimate by 2, we only need to consider 1-rectangles with at least as many columns as rows (i.e., bulky ones).

Proof of Theorem 4.1(b). For every $b \in \{1, \ldots, n\}$, denote by X_b the number of columns of the 1-rectangle generated by the row set $\{1, \ldots, b\}$—a random variable with $\mathrm{Bin}(n, p^b)$ distribution. We prove that, for every $1 < u < 2$,

$$\sum_{b=1}^{n/\lambda^{2/3}} \binom{n}{b} \mathbf{P}(bX_b \geqslant u\, ap^a n) = o(1), \tag{10}$$

which, together with Lemma 4.8, proves Theorem 4.1(b).

We split the proof into two lemmas, dealing with the cases $b \leqslant \log_{1/p} e$ and $b \geqslant \log_{1/p} e$, respectively, stated below. Establishing these lemmas completes the proof of Theorem 4.1(b). $\qquad\square$

Lemma 4.9. *For every $u \in\,]1, 2[$ there exists a constant $\lambda_0 \geqslant 1$ such that, for every $\bar{p} \geqslant \lambda_0/n$, and for every $1 \leqslant b \leqslant \log_{1/p} e$, we have*

$$\binom{n}{b} \mathbf{P}\left(X_b \geqslant u\, \frac{a}{b} p^a n\right) = o_u(1/n).$$

Lemma 4.10. *For every $u \in\,]1, 2[$ there exists a constant λ_0 such that, if $\bar{p}n = \lambda \geqslant \lambda_0$, and $\log_{1/p} e \leqslant b \leqslant n/\lambda^{3/2}$, then*

$$\binom{n}{b} \mathbf{P}\left(X_b \geqslant u\, \frac{a}{b} p^a n\right) = o_u(1/n).$$

Proof of Lemma 4.9. Define

$$\delta := \min\left(u\, \frac{ap^a}{bp^b} - 1,\ 1\right).$$

Note that $\delta \geqslant u - 1 > 0$ by the definition of a in (3). The "1" in the second argument of the mininum is somewhat arbitrary: the particular version of the Chernoff inequality which we refer to, [30, Thm 4.4-2], requires $\delta \leqslant 1$. Using this Chernoff bound in

$$\mathbf{P}(X_b \geqslant u\, ap^a n/b) \leqslant \mathbf{P}(X_b \geqslant (1+\delta)\, \mathbf{E}\, X_b) \leqslant e^{-\delta^2\, \mathbf{E}\, X_b/3},$$

and the inequality $\binom{n}{b} \leqslant (en/b)^b$, we estimate

$$\ln\left(\binom{n}{b} \mathbf{P}\left(X_b \geqslant u\, \frac{a}{b} p^a n\right)\right) \leqslant b \ln\left(\frac{en}{b}\right) - \delta^2 p^b n/3$$

$$\leqslant n\left(\frac{b}{n}\ln\left(\frac{en}{b}\right)-\frac{\delta^2}{3e}\right) \qquad \text{[since } b\leqslant \log_{1/p} e]. \qquad (*)$$

For any real $b\in[1,\log_{1/p}e]$, denote by A_b the term inside the parentheses in $(*)$.

Since $b\mapsto A_b$ is nondecreasing on $[1,n]$, we have, for every $b\in[1,\log_{1/p}e]$,

$$A_b\leqslant A_{\log_{1/p}e}$$
$$\leqslant A_{1/\bar{p}} \qquad \text{[A. nondecreasing and } \log_{1/p}e\leqslant \frac{1}{\bar{p}}\leqslant n, \text{ by (5)]}$$
$$\leqslant A_{n/\lambda_0} \qquad \text{[A. nondecreasing and } 1/\bar{p}\leqslant n/\lambda_0\leqslant n]$$
$$=\frac{\ln(e\lambda_0)}{\lambda_0}-\frac{\delta^2}{3e}$$
$$\leqslant \frac{\ln(e^2\lambda_0)}{\lambda_0}-\frac{(u-1)^2}{3e} \qquad \text{[as } \delta\geqslant u-1]$$

Hence, for sufficiently large λ_0, depending only on u, we have, for all $b\in[1,\log_{1/p}e]$,

$$A_b=-\Omega_u(1),$$

so that

$$\mathbf{P}(X_b\geqslant ap^a n/b)\leqslant e^{-nA_b}=e^{-\Omega_u(n)}=o_u(1/n)$$

which concludes the proof of the lemma. $\qquad\square$

Proof of Lemma 4.10. By Lemma 4.8, we already know that, if a bulky 1-rectangles generated by b rows exists with non-$o(1)$ probability, we must have $b<n/\lambda^{2/3}$.

Define δ as follows, $0<u-1\leqslant\delta:=(u-1)\frac{ap^a}{bp^b}\leqslant u\frac{ap^a}{bp^b}-1$, and let

$$\varepsilon:=\begin{cases} (u-1)^2/3, & \text{if } \delta\leqslant 3/2;\\ \ln 5/2-1+2/5, & \text{otherwise.}\end{cases}$$

We do the case distinction because we use two slightly different versions of Chernoff in our estimate of

$$\varrho:=\mathbf{P}\left(X_b\geqslant u\frac{a}{b}p^a n\right).$$

If $\delta\leqslant 3/2$, then

$$\varrho\leqslant \mathbf{P}\left(X_b\geqslant (1+\delta)\,\mathbf{E}\,X_b\right)$$
$$\leqslant e^{-\delta^2 p^b n/3} \qquad \text{[Chernoff, e.g., [19, Cor. 2.3]]}$$
$$\leqslant e^{-(u-1)(u-1)\frac{a}{b}p^a n/3} \qquad \text{[definition of } \delta, \text{ and } \delta\geqslant u-1]$$
$$=e^{-\varepsilon\frac{a}{b}p^a n}.$$

If, on the other hand, $\delta>3/2$, then

$$u\frac{a}{b}p^a n=u\frac{ap^a}{bp^b}\cdot\mathbf{E}\,X_b\geqslant (\delta+1)\cdot\mathbf{E}\,X_b\geqslant \tfrac{5}{2}\cdot\mathbf{E}\,X_b,$$

and we have, by Eqn. (2.10) in [19, Cor. 2.4],

$$\varrho \leqslant e^{-\varepsilon \frac{a}{b} p^a n}.$$

In both cases, we conclude

$$\ln\left(\binom{n}{b} \mathbf{P}\left(X_b \geqslant u \frac{a}{b} p^a n\right)\right)$$

$$\leqslant b \ln(en/b) - \varepsilon \frac{a}{b} p^a n$$

$$\leqslant b \ln(en/b) - \varepsilon \frac{an}{e^2 b} \qquad [p^a \geqslant 1/e^2 \text{ by (4)}]$$

$$\leqslant b \ln(en/b) - \varepsilon \frac{n^2}{2e^3 \lambda b} \qquad [a \geqslant \lfloor n/e\lambda \rfloor \text{ by (5), \& } \lfloor n/e\lambda \rfloor \geqslant n/2e\lambda \text{ as } \lambda \leqslant n/e]$$

$$\leqslant b \ln(e^2 \lambda) - \varepsilon \frac{n^2}{2e^3 \lambda b} \qquad [\text{as } b \geqslant \log_{1/p} e \geqslant n/e\lambda, \text{ by (5)}]$$

$$\leqslant \frac{n}{\lambda^{2/3}} \ln(e^2 \lambda) - \frac{\varepsilon}{2e^3} \frac{n}{\lambda^{1/3}} \qquad [\text{as } b \leqslant n/(\sqrt{\lambda} \ln \lambda)]$$

$$= \frac{n}{\lambda^{1/3}} \left(-\frac{\varepsilon}{2e^3} + o_{\lambda \to \infty}(1)\right).$$

Hence, if λ is at least a large enough constant, λ_0, then

$$\binom{n}{b} \mathbf{P}\left(X_b \geqslant u \frac{a}{b} p^a n\right) = e^{-\Omega_u(n^{2/3})} = o(1/n),$$

and the lemma is proven. $\square$

5 Clique number (fooling sets)

Recall that H_M is the bipartite graph with bipartite adjacency matrix M, and note that $H_{M^{n,p}}$ is the "usual" Erdős-Renyi random bipartite graph: each edge is picked independently with probability p.

The next lemma, whose easy proof we leave to the reader, gives the relationship between fooling sets in Communication Complexity, cross-free matchings, and cliques in the rectangle graph. Recall that a matching F in a bipartite graph H is called *cross-free*, if for every two edges $e = (u_1, u_2), f = (v_1, v_2) \in F$, none of the "cross edges" (u_1, v_2), (u_2, v_1) is in H.

Lemma 5.1 (Trivial).

Let M be a $n \times n$ matrix, and $F \subseteq \{1, \ldots, n\} \times \{1, \ldots, n\}$. The following are equivalent.

(a) *Fooling set property: for all $(k, \ell) \in F$, $M_{k,\ell} = 1$ and for all $(k', \ell') \in F \setminus \{(k, \ell)\}$ $M_{k,\ell'} M_{k',\ell} = 0$;*

(b) *The set F is a cross-free matching in H_M;*

(c) $F \subseteq V(G_{\boxtimes}(M))$, *and F is a clique in $G_{\boxtimes}(M)$.*

It is known that the decision problem whether a bipartite graph has a cross-free matching of a given size is NP-hard [34].

Recall $\delta = 1 - p^2$, and $\bar{p} = 1 - p$. Denote by $\nu(H)$ the size of the largest matching of a bipartite graph H. Clearly, $\omega(G_{\boxtimes}(M)) \leqslant \nu(H_M)$. Let $a(q)$ be a function with the property that, a.a.s., every Erdős-Renyi random graph $G_{n,q}$ on n vertices with edge-probability q has an independent set of size at least $a(q)$.

Theorem 5.2.

(a) For $n^{-3/2} \leqslant p = o(1/\sqrt{n})$, a.a.s., we have

$$\omega(G_{\boxtimes}^{n,p}) = (1 - o(1))\nu(H_{M^{n,p}}). \tag{11a}$$

In particular, if in addition $p \gg 1/n$, then, a.a.s., $\omega(G_{\boxtimes}^{n,p}) = (1 - o(1))n$.

(b) If $pn - \ln n \to \infty$, then, a.a.s., $\omega(G_{\boxtimes}^{n,p}) \geqslant a(p^2)$.

(c) If $p \gg \sqrt{(\ln n)/n}$ and $\bar{p} \geqslant n^{-o(1)}$, then, a.a.s.,

$$\omega(G_{\boxtimes}^{n,p}) \leqslant 2\log_{1/\delta}(pn^2).$$

(d) If $a \in\,]0, 4[$ is a constant and $\bar{p} = n^{-a}$, then $\omega(G_{\boxtimes}^{n,p}) \leqslant 4/a + 1$. If, in addition, $a < 1$, then $\omega(G_{\boxtimes}^{n,p}) = \lfloor 4/a \rfloor + 1$

The proof of Theorem 5.2 is spread over the remainder of this section. In the first subsection, we study the expected number of cliques of the relevant sizes and obtain Theorem 5.2(c). Subsection 5.2 estimates the variance of the number of cliques of constant size. Finally, in Subsection 5.3, we study the connection to matchings in Erdős-Renyi random bipartite graphs and prove items (a) and (b).

By combining the upper bound in (c) with the lower bound in (b) applied to the classical theorems about independent sets and cliques in Erdős-Renyi random graphs (cf., e.g., [19]), we immediately obtain the following bounds.

Corollary 5.3.

(a) For p in the range $n^{-o(1)} \leqslant p \leqslant 1 - \Omega(1)$, we have, a.a.s.,

$$2\left(\log_{1/\delta} n - \log_{1/\delta} \log_{1/\delta} pn\right) \leqslant \omega(G_{\boxtimes}^{n,p}) \leqslant 2\log_{1/\delta}(pn^2)$$

(b) For p in the range $\sqrt{(\ln n)/n} \ll p \leqslant 1/\ln n$ we have, a.a.s.,

$$\frac{2}{p}\left(\ln pn - \ln\ln pn\right) \leqslant \omega(G_{\boxtimes}^{n,p}) \leqslant 2\log_{1/\delta}(pn^2)$$

In the range given in for (a), the upper bound is within a factor of

$$(1 - o(1))\frac{\ln n + \log_(pn)}{\ln n} \leqslant 2$$

of the lower bound. If p tends to 0 faster, however, the upper bound in (b) is off by a factor of $1/p$ from the lower bound, which leaves "room for improvement"; cf. Section 7.

5.1 Upper bounds: The number of r-cliques

Let the random variable $X = X_r = X_{r,n,p}$ count the number of r-cliques in $G_\boxtimes^{n,p}$. For a set $F \subseteq [n] \times [n]$, denote by A_F the event that F is clique in $G_\boxtimes^{n,p}$. We have

$$X_r = \sum_F \mathbf{I}[A_F], \tag{12}$$

where the sum ranges over all F of the form $F = \{(k_1, \ell_1), \ldots, (k_r, \ell_r)\}$, with all the k_j's distinct, and all the ℓ_j's distinct. There are $r! \binom{n}{r}^2$ of these sets F, and hence

$$\mathbf{E} X_r = r! \binom{n}{r}^2 p^r \, \delta^{\binom{r}{2}}.$$

Elementary calculus shows that, for fixed $r \geqslant 2$, $p \mapsto r! \binom{n}{r}^2 p^r \, \delta^{\binom{r}{2}}$ is increasing on $[0, 1/\sqrt{r}]$ and decreasing on $[1/\sqrt{r}, 1]$ (see the proof of the (a)-part of Lemma 5.4). The following lemma describes for which values of r the expectation $\mathbf{E} X_r$ tends to 0 or infinity, resp., in the relevant range of p.

Lemma 5.4. (a) If $e/n \leqslant p \leqslant n^{-1/2} \sqrt{\ln n}$, then $\mathbf{E} X_n \to \infty$.

(b) For constants $c > 1$, $\varepsilon > 0$ if $p = c\, n^{-1/2} \sqrt{\ln n}$, with $r := (1 + \varepsilon) \frac{n}{c^2}$ we have $\mathbf{E} X_r \to 0$.

(c) If $p \gg n^{-1/2} \sqrt{\ln n}$ and $1 - p = \bar{p} \geqslant n^{-o(1)}$, then letting $r_- := 2 \log_{1/\delta}(pn^2) - 2 \log_{1/\delta} \log_{1/\delta}(pn^2)$ and $r_+ := 2 \log_{1/\delta}(pn^2)$ we have $\mathbf{E} X_{r_-} \to \infty$, and $\mathbf{E} X_{r_+} \to 0$.

(d) If $a \in \,]0, 4[$ is a constant and $1 - p = \bar{p} = n^{-a}$, then $\mathbf{E} X_r \to 0$ if $r > \frac{4}{a} + 1$, and $\mathbf{E} X_r \to \infty$ if $r < \frac{4}{a} + 1$.

Proof.
(a). First of all, we prove that for $r \geqslant 2$, the function $p \mapsto \mathbf{E} X_{r,p}$ is non-decreasing $]0, r^{-1/2}]$ and non-increasing on $[r^{-1/2}, 1[$.

Clearly, only the function

$$f : p \mapsto p(1 - p^2)^{(r-1)/2}$$

is of interest. Taking the derivative, we obtain

$$f'(p) = (1 - p^2)^{(r-1)/2} - (r-1)p^2(1 - p^2)^{(r-3)/2}.$$

If $0 < p < 1$, then $f'(p) = 0$ and is equivalent to

$$0 = 1 - p^2 - (r-1)p^2 = 1 - rp^2.$$

For $p < 1/\sqrt{r}$, we have $f'(p) > 0$ and $p > 1/\sqrt{r}$, we have $f'(p) < 0$.

Now, for $p = e/n$, using Stirling's formula, we have

$$\mathbf{E}\, X_n = n! \left(\frac{e}{n}\right)^n \left(1 - \frac{e^2}{n^2}\right)^{\binom{n}{2}} = \Theta(\sqrt{n}),$$

so $\mathbf{E}\, X_n$ tends to infinity with $n \to \infty$.

Finally, let $p = n^{-1/2} \sqrt{\ln n}$. We have

$$\frac{\ln \mathbf{E}\, X_n}{n} = \frac{\ln\!\left(n!\, p^n\, \delta^{\binom{n}{2}}\right)}{n} = -1 + o(1) + \ln n - \ln(1/p) - \tfrac{n-1}{2}\ln(1/\delta)$$

$$\geqslant -1 + o(1) + \ln n - \ln(1/p) - \tfrac{n-1}{2}p^2,$$

where we used $\ln(1/\delta) = \ln(1/(1-p^2)) \leqslant p^2 + O(p^4)$ and $np^4 = o(1)$ in the last inequality. Replacing p, we get

$$\frac{\ln \mathbf{E}\, X_n}{n} \geqslant \tfrac{1}{2}\ln \ln n + O(1),$$

which proves the claim in (a) for this particular value of p.

(b). First of all, note that, for $4 \leqslant r < n$, using the estimates

$$\sqrt{r}\left(\frac{r}{e}\right)^r \leqslant \quad r! \quad \leqslant r\left(\frac{r}{e}\right)^r, \text{ and}$$

$$\tfrac{1}{3\sqrt{r}}\, e^{r - r^2/(n-r)}\left(\frac{n}{r}\right)^r \leqslant \quad \binom{n}{r} \quad \leqslant e^r\left(\frac{n}{r}\right)^r,$$

we have

$$1 - \tfrac{r}{n-r} - O\!\left(\tfrac{\ln r}{r}\right) \leqslant \frac{\ln\!\left(r!\binom{n}{r}^2 p^r \delta^{\binom{r}{2}}\right)}{r} - \left(\ln(n^2) - \ln(1/p) - \tfrac{r-1}{2}\ln(1/\delta) - \ln r\right) \leqslant 1 + \tfrac{\ln r}{r}.$$

$$(*)$$

(We will use this for (c), too.)

Now, with $c > 1$, $p = c\, n^{-1/2} \sqrt{\ln n}$ and $r = (1+\varepsilon)n/c^2 = (1 - \Omega(1))n$, we get

$$\begin{aligned}
\frac{\ln \mathbf{E}\, X_r}{r} &= \ln(n^2) - \ln(1/p) - \tfrac{r-1}{2}\ln(1/\delta) - \ln r + O(1) \\
&= \ln(n^2) - \tfrac{1}{2}\ln(n/\ln n) - \tfrac{r-1}{2}\ln(1/\delta) - \ln n + O(1) \\
&= \tfrac{1}{2}\ln n - \tfrac{r-1}{2}n\ln(1/\delta) + O(\ln \ln n) \\
&= \tfrac{1}{2}\ln n - \tfrac{r-1}{2}\left(p^2 + O(p^4)\right) + O(\ln \ln n) \\
&= -\tfrac{\varepsilon}{2}\ln n + O(\ln \ln \ln n),
\end{aligned}$$

which proves $\mathbf{E}\, X_r \to 0$.

(c). With $r := r_+ = 2\ln(pn^2)/\ln(1/\delta)$, using the upper bound from $(*)$, we get

$$\frac{\ln \mathbf{E}\, X_r}{r} \leqslant \ln(pn^2) - \tfrac{r-1}{2}\ln(1/\delta) - \ln r + 1 + \tfrac{\ln r}{r}$$

$$= \tfrac{1}{2}\ln(1/\delta) - \ln r + 1 + \tfrac{\ln r}{r}$$
$$= -\Omega(1),$$

where the last equation follows from $r \to \infty$ (due to $\bar{p} \geqslant n^{-o(1)}$), which also implies $\mathbf{E}\,X_r \to 0$.

On the other hand, with $r := r_- = 2\log_{1/\delta}(pn^2) - 2\log_{1/\delta}\log_{1/\delta}(pn^2)$, using the upper bound from $(*)$, we get

$$
\begin{aligned}
\frac{\ln \mathbf{E}\,X_r}{r} &\geqslant \ln(pn^2) - \tfrac{r-1}{2}\ln(1/\delta) - \ln r + 1 - O(\tfrac{\ln r}{r}) \\
&\geqslant \left(\log_{1/\delta}\log_{1/\delta}(pn^2)\right)\ln(1/\delta) - \ln r + 1 + O(\tfrac{\ln r}{r}) \\
&= \ln\log_{1/\delta}(pn^2) - \ln r + 1 + O(\tfrac{\ln r}{r}) \\
&\geqslant -\ln 2 + 1 + O(\tfrac{\ln r}{r}) \\
&= \Omega(1).
\end{aligned}
$$

Again, the last equation and the conclusion $\mathbf{E}\,X_r \to \infty$ follows from $r \to \infty$.

(d). Finally, let $0 < a < 4$ be a constant and $1 - p = \bar{p} = n^{-a}$. Noting that $\delta = (1+p)\bar{p} = \Theta(\bar{p})$, if $r = O(1)$, we have

$$
\left(\mathbf{E}\,X_r\right)^{1/r} = \Theta\!\left(n^2\bar{p}^{(r-1)/2}\right) = \Theta\!\left(n^{2-a(r-1)/2}\right),
$$

which implies $\mathbf{E}\,X_r \to \infty$ if $r > 4/a + 1$, and $\mathbf{E}\,X_r \to 0$ if $r < 4/a + 1$. $\qquad\square$

From this lemma, we immediately get the upper bound on ω in Theorem 5.2(c).

Proof of Theorem 5.2(c). Follows from (c). $\qquad\square$

Item (a) of the lemma suggests the question, for which p the value of ω drops from $(1 - o(1))n$ to $(1 - \Omega(1))n$. If the expectation is "right", this happens crossing from $p = \sqrt{(\ln n)/n}$ to $p = (1 + \varepsilon)\sqrt{(\ln n)/n}$. This is supported by the fact that our lower bounds in this region—in the next subsection—appear to be quite simple, in that they only consider one fixed maximal matching in $H_{M^{n,p}}$, and delete edges from it until it becomes cross-free.

5.2 Second moment calculation

Lemma 5.5. *If $r = O(1)$ and $p\delta \gg 1/n$, then $\mathbf{Var}(X_r) = o\!\left(\left(\mathbf{E}\,X_r\right)^2\right)$.*

Proof. With the notations as in equation (12), let $F_0 := \{(1,1), \ldots, (r,r)\}$, and abbreviate $A_0 := A_{F_0}$. We have

$$
\mathbf{E}(X^2) = \mathbf{E}\,X \cdot \sum_F \mathbf{P}(A_F \mid A_0)
$$

where the sum ranges over all F of the form $F = \{(k_1, \ell_1), \ldots, (k_r, \ell_r)\}$, with all the k_j's distinct, and all the ℓ_j's distinct, as in (12).

If $F \subset \{r+1, \ldots, n\} \times \{1, \ldots, n\}$, then the events A_F and A_0 are clearly independent, so that, with the following sum ranging over these F, we have

$$\sum_F \mathbf{P}(A_F \mid A_0) = \frac{(n-r)_r}{(n)_r} \mathbf{E}\, X.$$

Consequently, we have

$$\mathbf{E}(X^2) = \frac{(n-r)_r}{(n)_r} \big(\mathbf{E}\, X\big)^2 + \mathbf{E}\, X \cdot \sum_F \mathbf{P}(A_F \mid A_0),$$

where the last sum ranges over all F with $F \cap \{1, \ldots, r\} \times \{1, \ldots, n\} \neq \emptyset$. For each such F,

$$\mathbf{P}(A_F \mid A_0) = O\left(\frac{1}{p\delta n}\right)^{O(r^2)} \mathbf{P}(A_F),$$

with absolute constants in the big-Os.

Hence, if $r = O(1)$ and $p\delta \gg 1/n$,

$$\mathbf{E}(X^2) = \frac{(n)_r}{(n-r)_r} \big(\mathbf{E}\, X\big)^2 + O\left(\frac{1}{p\delta n}\right)^{O(r^2)} \big(\mathbf{E}\, X\big)^2 = (1 + o(1))\big(\mathbf{E}\, X\big).$$

This proves the statement of the lemma. $\qquad\square$

The lemma proves that the number of edges of $G_\boxtimes^{n,p}$ is a.a.s. as given in equation (1) on page 6.

Proof of Theorem 5.2(d). The upper bound, for general a is in Lemma 5.4(d). The lower bound when $a < 1$ follows from Lemma 5.4(d) and Lemma 5.5. $\qquad\square$

5.3 Lower bounds: Cross-free sub-matchings

Let $\nu^\times(\cdot)$ denote the size largest cross-free matching of a bipartite graph.

Let H be a bipartite graph, and $m = \{e_1, \ldots, e_r\} \subseteq E(H)$ a matching in H. Define the graph $G' = G'(H, m)$ with vertex set $V(G') = \{1, \ldots, r\}$ and $\{k, \ell\} \in E(G')$ if e_k, e_ℓ induce a $K_{2,2}$ in H. Then $\nu^\times(H) \geqslant \alpha(G')$ holds: for any independent set A of G', the set $\{e_j \mid j \in A\}$ is a cross-free matching in H.

Our strategy for obtaining a large cross-free matching will be this: fix a large matching m in $H_{M^{n,p}}$, then bound the independence number of the corresponding random graph $G'_{n,p}(m) := G'(H_{M^{n,p}}, m)$. This random graph behaves similarly to an Erdős-Renyi random graph with $|m|$ vertices and edge-probability p^2. The following technical lemma takes care of the dependency issues which arise.

Let $G_{r,q}$ denote the Erdős-Renyi random graph with r vertices and edge probability q.

Lemma 5.6. *For all positive integers n, r, a, and $p \in [0, 1]$, we have*

$$\mathbf{P}\Big(\nu^\times(H_{M^{n,p}}) < a \quad \& \quad \nu(H_{M^{n,p}}) \geqslant r\Big) \quad \leqslant \quad \mathbf{P}\big(\alpha(G_{r,p^2}) < a\big).$$

Proof. Let $\mathcal{M}$ be the set of matchings of size r of $K_{n,n}$, and for each $m \in \mathcal{M}$ denote by C_m the event that $H_{M^{n,p}}$ contains m. Fix a matching $m \in \mathcal{M}$. For every edge $e \in E(K_{n,n})$, we have

$$\mathbf{P}\big(e \in H_{M^{n,p}} \mid C_m\big) = p,$$

and these events are jointly independent. Hence, for each potential edge e' of $G'_{n,p}(m)$,

$$\mathbf{P}\big(e' \in G'_{n,p}(m) \mid C_m\big) = p^2,$$

again with joint independence of the events.

Now, denote by A the event that there does not exists a cross-free matching of size larger than a in $H_{M^{n,p}}$. By the discussion above, A and C_m together imply $\alpha(G'_{n,p}(m)) < a$, so that

$$\mathbf{P}\big(A \mid C_m\big) \leqslant \mathbf{P}\big(\alpha(G'_{n,p}(m)) < a \mid C_m\big) = \mathbf{P}\big(\alpha(G_{r,p^2}) < a\big).$$

It follows that

$$\mathbf{P}\Big(\nu^{\times}(H_{M^{n,p}}) < a \quad \& \quad \nu(H_{M^{n,p}}) \geqslant r\Big) = \mathbf{P}\Big(A \cap \bigcup_m C_m\Big) \leqslant \sum_m \mathbf{P}\big(A \cap C_m\big)$$

$$= \sum_m \mathbf{P}\big(A \mid C_m\big)\mathbf{P}\big(C_m\big) \leqslant \mathbf{P}\big(\alpha(G_{r,p^2}) < a\big),$$

which concludes the proof of the lemma. $\qquad\square$

Remark 5.7. We will use Lemma 5.6 in the following way: If p, r_-, r_+ are such that both

$$\begin{aligned} \mathbf{P}\big(\nu(H_{M^{n,p}}) < r_+\big) &= o(1), \text{ and} \\ \mathbf{P}\big(\alpha(G_{r_+,p^2}) < r_-\big) &= o(1), \end{aligned} \tag{13}$$

then, a.a.s., $G_{\boxtimes}(M^{n,p})$ has a clique of size r_-. Indeed,

$$\begin{aligned} &\mathbf{P}\big(\omega(G_{\boxtimes}(M^{n,p})) < r_-\big) \\ &\leqslant \mathbf{P}\Big(\nu^{\times}(H_{M^{n,p}}) < r_- \quad \& \quad \nu(H_{M^{n,p}}) \geqslant r_+\Big) + \mathbf{P}\big(\nu(H_{M^{n,p}}) < r_+\big) \\ &\leqslant \mathbf{P}\big(\alpha(G_{r_+,p^2}) < r_-\big) + \mathbf{P}\big(\nu(H_{M^{n,p}}) < r_+\big) \qquad\qquad \text{[Lemma 5.6]} \\ &= o(1) + o(1) \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \text{[by (13)].} \end{aligned}$$

We are now ready to prove the first two items of Theorem 5.2. We start with the easiest part.

Proof of Theorem 5.2(b). This is a direct consequence of the remark with $r_- := a(p^2)$ and $r := n$, since, if $pn - \ln n \to \infty$, then $\nu(H_{M^{n,p}}) = n$, a.a.s. (e.g., [19, Thm 4.1]). $\qquad\square$

Proof of Theorem 5.2(a). Let $\varepsilon > 0$ be a constant. Proceeding as in Remark 5.7, with $r_- := r$ and $r_+ := (1+\varepsilon)r$, if both a.a.s. $\nu(H_{M^{n,p}}) \geqslant r$ and a.a.s. $\alpha(G_{r,p^2}) \geqslant (1-\varepsilon)r$, then, a.a.s.,

$$(1-\varepsilon)\nu(H_{M^{n,p}}) \leqslant \omega(G_{\boxtimes}(M^{n,p})) \leqslant \nu(H_{M^{n,p}}).$$

Letting ε tend to 0 then gives the desired result.

For $n^{-3/2} \leqslant p = o(n)$, a.a.s., the number of edges of G_{n,p^2} is $o(1)$, and hence $\alpha(G_{n,p^2}) = (1 - o(1))n$, while easy arguments show that a.a.s. $\nu(H_{M^{n,p}}) = \Omega(n)$ with concentration in a window of size $O(\sqrt{n})$. Hence the conditions (13) are satisfied.

For $p = \Omega(1/n)$, a classical result by Karp & Sipser [21] states that there is a function $h\colon]0, \infty[\to [0, 1]$ with $\lim_{c \to \infty} h(c) = 1$ such that if $p = c/n$, then, a.a.s., $\nu(H_{M^{n,p}}) = (1-o(1))h(c)/n$. Since $p = o(1/\sqrt{n})$, a.a.s., the number of edges of G_{n,p^2} is $o(n)$, and hence $\alpha(G_{n,p^2}) = (1 - o(1))n$. It follows that $\omega(G_{\boxtimes}M^{n,p}) = (1 - o(1))\nu(H_{M^{n,p}})$. In particular, if $p \gg 1/n$, then, a.a.s, $\nu(H_{M^{n,p}}) = (1 - o(1))n$. $\qquad\square$

6 (Fractional) Chromatic number

We start with the easy case $p \leqslant 1/2$.

Corollary 6.1. *In the range $1/n \ll p \leqslant 1/2$, we have $\chi(G_{\boxtimes}^{n,p}) = (1 - o(1))n$.*

Proof. Remark 2.1(a) gives the upper bound. Theorem 5(a) gives the lower bound for small $p = o(1/\sqrt{n})$.

For, say, $1/e \geqslant p = \Omega(n^{-1/4})$ (say), Theorem 4.1(a) plus an easy concentration argument yield $\alpha(G_{\boxtimes}^{n,p}) = (1 + o(1))pn$ a.a.s. and for $1/e \leqslant p \leqslant 1/2$, the value of a in equation (3) of Theorem 4.1(b) is 1, so that $\alpha(G_{\boxtimes}^{n,p}) = (1 + o(1))pn$ there, too.

We conlcude $\chi(G_{\boxtimes}^{n,p}) \geqslant N/\alpha(G_{\boxtimes}^{n,p}) = ((1-o(1))pn^2)/((1-o(1))pn) = (1-o(1))n$. $\quad\square$

The case $p > 1/2$ is more interesting.

6.1 The fractional chromatic number

We briefly review the definition of fractional chromatic number and (equivalently) fractional rectangle covering number.

Let R be a random independent set of G, drawn according to a distribution π, and consider $\gamma(\pi) := \min_{u \in V(G)} \mathbf{P}(u \in R)$. A convenient definition of the fractional chromatic number of G is then $\chi^*(G) := \min_\pi 1/\gamma(\pi)$, where the minimum is taken over all distributions π on the set of independent sets of G. It is OK to restrict the supports of the distributions π to a subset $\mathcal{I}$ of all independent sets of G, as long as $\mathcal{I}$ contains all inclusion-wise maximal independent sets. In particular, for a Lovász-Saks rectangle graph, we can assume w.l.o.g., that R takes values in the 1-rectangles of the corresponding matrix.

Recall the following well-known inequalities:[4]

$$\left.\begin{array}{c} \mathrm{ir}(G) := \dfrac{|V(G)|}{\alpha(G)} \\[2mm] \omega(G) \end{array}\right\} \leqslant \sup_{U \subseteq V(G)} \frac{|U|}{\alpha(G[U])} \leqslant \chi^*(G) \leqslant \chi(G) \underset{(*)}{\leqslant} \bigl(1 + \ln \alpha(G)\bigr) \chi^*(G). \quad (14)$$

---

[4]See [33, Vol. B], Theorem 64.13, for the last inequality.

The number ir(G) is called the *independence ratio.* Theorem 4.1(b) allows us to bound it: With $\lambda/n = \bar{p} = 1 - p$ as always, we have a.a.s.

$$\frac{N}{\alpha(G_{\boxtimes}^{n,p})} \geqslant \frac{(1+o(1))pn^2}{(1+o(1))n/e\ln(1/p)} =$$
$$(1+o(1))\,ep\ln(1/p)\,n = (1+o(1))\,(1 - \bar{p}/2 - \bar{p}^2/3 + O(\bar{p}^3))\,e\lambda, \quad (15)$$

where the last equation is the Taylor expansion

$$\ln(1/p) = \sum_{j=1}^{\infty} \frac{\bar{p}^j}{j} = \frac{\lambda}{n}\left(1 + \bar{p}/2 + \bar{p}^2/3 + \dots\right).$$

For $\bar{p} = o(1)$, this is asymptotic to $e\lambda$. It is worth noting that the first inequality in (15) becomes an asymptotic equality if $\bar{p} = o(1)$.

We now give upper bounds on the $\chi^*(G_{\boxtimes}^{n,p})$. To prove an upper bound b on χ^* for a fixed matrix M, we have to give a distribution π on the 1-rectangles of M such that, if R is sampled according to π, we have, for all (k,ℓ) with $M_{k,\ell} = 1$, we have $\mathbf{P}((k,\ell) \in R) \geqslant 1/b$.

To prove an "a.a.s." upper bound for a random matrix, we have to show that

$$\mathbf{P}\left(\exists (k,\ell)\colon \ \mathbf{P}\big((k,\ell) \in R \mid M^{n,p} \ \& \ M_{k,\ell}^{n,p} = 1\big) < 1/b\right) = o(1). \quad (16)$$

Our random 1-rectangle R within the random matrix $M^{n,p}$ is sampled as follows. Let K be a random subset of $[n]$, by taking each k into K independently, with probability q. Then let $R := K \times L$ be the 1-rectangle generated (p. 7) by the row-set K, i.e., $L := \{\ell \mid \forall k \in K\colon M_{k,\ell}^{n,p} = 1\}$.

Let the random variable Z_ℓ count the number of 0s in column ℓ, and set $Z := \max_\ell Z_\ell$. For $k, \ell \in \{1, \dots, n\}$, conditioned on $M^{n,p}$ and $M_{k,\ell}^{n,p} = 1$, the probability that $(k,\ell) \in R$ equals

$$q(1-q)^{Z_\ell} \geqslant q(1-q)^Z,$$

so that for every positive integer z, using $1/b = q(1-q)^z$ in (16),

$$\mathbf{P}\left(\exists (k,\ell)\colon \ \mathbf{P}\big((k,\ell) \in R \mid M^{n,p} \ \& \ M_{k,\ell}^{n,p} = 1\big) < q(1-q)^z\right) = \mathbf{P}(Z > z). \quad (17)$$

To obtain upper bounds on χ^*, we give a.a.s. upper bounds on Z, and choose q accordingly. The following theorem summarizes the results.

Theorem 6.2. *Let* $p = 1 - \bar{p} = 1 - \lambda/n$ *as usual, and* $\bar{p} < 1/2$.

(a) *If* $\ln n \ll \lambda < n/2$, *then, a.a.s.,* $\chi^*(G_{\boxtimes}^{n,p}) \leqslant (1+o(1))\,e\lambda$

(b) *If* $\lambda = \Theta(\ln n)$, *then, a.a.s.,* $\chi^*(G_{\boxtimes}^{n,p}) = O(\ln n)$.

(c) *If* $1 \ll \lambda = o(\ln n)$, *then, a.a.s.,* $\chi^*(G_{\boxtimes}^{n,p}) \leqslant (1+o(1))\,e\max\left(2\lambda, \dfrac{\ln n}{\ln((\ln n)/\lambda)}\right)$

Proof. The bound in (a). For every constant $t > 0$, let

$$\psi(t) := 1/\big((1+t)\ln(1+t) - t\big).$$

With

$$h(t) = h(t,n) := \frac{\lambda}{\psi(t)\ln n},$$

using the a standard Chernoff estimate (Theorem 2.1, Equation (2.5) in [19]) we find that

$$\mathbf{P}\big(Z_1 \geqslant (1+t)\lambda\big) \leqslant e^{-\lambda/\psi(t)} \leqslant e^{-h(t)}n,$$

so that, by the union bound,

$$\mathbf{P}\big(Z \geqslant (1+t)\lambda\big) \leqslant e^{-h(t)}. \tag{19}$$

For every fixed $t > 0$, $h(t)$ tends to infinity with n, so that the RHS in (19) is $o(1)$. Using that in (17), we obtain

$$\mathbf{P}\bigg(\exists (k,\ell)\colon \ \mathbf{P}\big((k,\ell) \in R \mid M^{n,p} \ \& \ M_{k,\ell}^{n,p} = 1\big) < q(1-q)^{(1+t)\lambda}\bigg) = \mathbf{P}\big(Z > (1+t)\lambda\big) = o(1),$$

and, taking $q := \frac{1}{(1+t)\lambda}$, we obtain, a.a.s.,

$$\chi^* \leqslant \frac{1}{q(1-q)^{(1+t)\lambda}} \leqslant \frac{1+t}{1 + \frac{1}{(1+t)\lambda}} e\lambda,$$

where we used $(1-\varepsilon)^k \geqslant (1 - k\varepsilon^2)e^{-k\varepsilon}$ for $\varepsilon < 1$. Since this is true for every $t > 0$, we conclude that, a.a.s., $\chi^* \leqslant (1 - o(1))e\lambda$.

The bounds in (b), (c). Here we use a slightly different Chernoff bound, Lemma 6.3 below.

For (b), suppose that $\lambda \leqslant C \ln n$ for a constant $C > 1$. Using Lemma 6.3 below with $\alpha = e^2 C \ln n$, we obtain

$$\mathbf{P}\big(Z_1 \geqslant e^2 C \ln n\big) = O\big(1/\sqrt{\ln n}\big)e^{-\lambda}\Big(\frac{eC\ln n}{e^2 C \ln n}\Big)^{\alpha} = O\big(1/\sqrt{\ln n}\big)e^{-\ln n}.$$

and thus

$$\mathbf{P}\big(Z \geqslant e^2 C \ln n\big) = o(1).$$

We conclude similarly as above: with $q := \frac{1}{e^2 C \ln n}$ we obtain, a.a.s., $\chi^* \leqslant e^3 C \ln n$.

Finally, for (c), if $\lambda = o(\ln n)$, let $\varepsilon > 0$ be a constant, and use Lemma 6.3 again, with

$$\alpha := \max\bigg(2\lambda, \ \frac{(1+\varepsilon)\ln n}{\ln\big(\frac{\ln n}{e\lambda}\big)}\bigg).$$

We find that

$$\mathbf{P}\big(Z_1 \geqslant \alpha\big) = o\big(e^{-\alpha \ln(\alpha/e\lambda)}\big),$$

and the usual calculation (Appendix A.1) shows that $\alpha \ln(\alpha/e\lambda) \geqslant \ln n$, which implies

$$\mathbf{P}\big(Z \geqslant \alpha\big) = o(1).$$

Conclude similarly as above, with $q := \frac{1}{\alpha}$, we obtain, a.a.s.,

$$\chi^* \leqslant e\alpha = e \max\left(2\lambda, (1+\varepsilon)\frac{\ln n}{\ln\big(\frac{\ln n}{e\lambda}\big)}\right).$$

One obtains the statement in the theorem by letting ε tend to 0; the e-factor in the denominator of the ln of the denominator in α is irrelevant as $n \to \infty$. $\qquad\square$

We have no good reference for the following simple Chernoff estimate (it is almost exactly Theorem 5.4 in [30], except that we allow $\lambda \to \infty$ slowly). For the sake of completeness, we include it here (and its proof in Appendix A.2).

Lemma 6.3. *Let $\bar{p} = \lambda/n$ with $1 < \lambda = o(n)$, and $2\lambda \leqslant \alpha \leqslant n/2$. The probability that a $\mathrm{Bin}(n,\bar{p})$ random variable is at least α is at most*

$$O\big(1/\sqrt{\alpha}\big) \cdot e^{-\lambda}\Big(\frac{e\lambda}{\alpha}\Big)^{\alpha}. \tag{20}$$

To summarize, comparing with (15), we can determine the fractional chromatic number accurately in the region $\ln n \ll \lambda \ll n$. For $\lambda = \Theta(\ln n)$ and for $\lambda = \Theta(n)$, we can determine χ^* up to a constant, but for $\lambda = o(\ln n)$, there is a large gap between our upper and lower bounds.

Inequality $(*)$ in (14) gives us corresponding upper bounds on χ:

Corollary 6.4.

(a) *If $\ln n \ll \lambda = O(n/\ln n)$, then, a.a.s., $\chi(G_\boxtimes^{n,p}) = O(\lambda \ln n)$.*

(b) *If $\lambda = \Theta(\ln n)$, then, a.a.s., $\chi(G_\boxtimes^{n,p}) = O(\ln^2 n)$.*

(c) *If $1 \ll \lambda = o(\ln n)$, then, a.a.s., $\chi(G_\boxtimes^{n,p}) = O\Big(\max\Big(\lambda \ln n, \dfrac{\ln^2 n}{\ln((\ln n)/\lambda)}\Big)\Big)$*

6.2 Binary-Logarithm of the number of distinct rows, and the ratio χ/χ^*

The binary logarithm of the number of distinct rows of the matrix (Remark 2.4) is a lower bound on the chromatic number of the rectangle graph. This bound is not generally available for the chromatic number of general graphs. The following proposition shows these bounds.

Proposition 6.5.

(a) *If $1/2 \geqslant \bar{p} = \Omega(1/n)$, then, a.a.s., the 2-Log lower bound on $\chi(G_\boxtimes^{n,p})$ is $(1-o(1))\log_2 n$.*

(b) If $\bar{p} = n^{-\gamma}$ for $1 < \gamma \leqslant {}^3\!/_2$, then a.a.s., the 2-Log lower bound on $\chi(G_{\boxtimes}^{n,p})$ is $(1 - o(1))(2 - \gamma)\log_2 n$.

Proof. Directly from the following Lemma 6.6 about the number of distinct rows, with $\lambda = n^{1-\gamma}$. $\qquad\square$

Lemma 6.6.

(a) If ${}^1\!/_2 \geqslant \bar{p} = \Omega({}^1\!/n)$, then, a.a.s., $M^{n,p}$ has $\Theta(n)$ distinct non-zero rows.

(b) With $\bar{p} = \lambda/n$, if $n^{-1/2} \leqslant \lambda \leqslant {}^1\!/_2$, then, a.a.s., $M^{n,p}$ has $\Omega(\lambda n)$ distinct non-zero rows.

(The constants in the big-Omegas are absolute.)

For the sake of completeness, we sketch the proof in Appendix A.3.

Erdős-Renyi random graphs have the property that the chromatic number is within a small constant factor from the lower bound one obtains from the independence ratio. For random rectangle graphs, this is not the case. Indeed, Theorem 6.2(c), together with Proposition 6.5, shows that, a.a.s.,

$$\frac{\chi(G_{\boxtimes}^{n,p})}{\chi^*(G_{\boxtimes}^{n,p})} \geqslant (1 + o(1)) \frac{\log_2 n}{\frac{\ln n}{\ln\left(\frac{\ln n}{\lambda}\right)}} = \Omega\left(\ln\left(\frac{\ln n}{\lambda}\right)\right),$$

which is $\Omega(\ln\ln n)$ if $\lambda = \ln^{o(1)} n$.

This gap is more pronounced in the (not quite as interesting) situation when $\lambda = o(1)$. Consider, e.g., $\lambda = n^{-\varepsilon}$, for some $\varepsilon = \varepsilon(n) = o(1/\ln\ln n)$, say. Similarly to the proofs of Theorem 6.2, we obtain that $\chi^*(G_{\boxtimes}^{n,p}) \leqslant e\max(10, 2/\varepsilon)$. (The max-term comes from the somewhat arbitrary upper bound $Z \leqslant \max(10, 2/\varepsilon)$.) For the Log-2 lower bound on χ, we have $(1 - \varepsilon)\log_2 n$, by Proposition 6.5, and thus

$$\frac{\chi(G_{\boxtimes}^{n,p})}{\chi^*(G_{\boxtimes}^{n,p})} = \Omega(\varepsilon \ln n).$$

7 Conclusion and open questions

The most important question for future research is to decide whether the gap between χ^* and χ goes away for $\lambda = \Omega(\ln n)$, or is inherent in the random graph model. Recall that the largest possible ratio χ/χ^* is $O(\ln n)$. We conjecture the following.

Conjecture 7.1 (Separation between $\boldsymbol{\chi^*}$ and $\boldsymbol{\chi}$, for $\boldsymbol{p = 1 - o(1)}$). *There are constants c, d such that in the range $\ln^c n \leqslant \lambda \leqslant n^d$, a.a.s.,*

$$\frac{\chi(G_{\boxtimes}^{n,p})}{\chi^*(G_{\boxtimes}^{n,p})} = \Omega\left(\frac{\ln n}{\ln\ln n}\right).$$

Conjecture 7.2 (Separation between χ^* and χ, for constant p). *There is a strictly increasing function $c = c(p)$ such that, for every constant $p \geqslant 1/2$, a.a.s.,*

$$\frac{\chi(G_{\boxtimes}^{n,p})}{\chi^*(G_{\boxtimes}^{n,p})} = (1 + o(1))\, c(p).$$

Our results show that $c(1/2) = 1$ and that, if $c(\cdot)$ exists, then $\lim_{p \to 1} c(p) = \infty$.

In order to tackle these two conjectures, it appears necessary improve the techniques for proving and lower bounds for $\chi(G_{\boxtimes}^{n,p})$. Our upper bounds rely on bounding the fractional chromatic number χ^*, and then using the fact that the chromatic number is at most $O(\ln n)$ from χ^*. It is possible that these can be improved. But our upper bounds for the fractional chromatic number don't appear to be optimal, either, when $\bar{p} = o(\ln n)$. Our lower bound is the fractional chromatic number, which we can determine accurately in the region $\ln n \ll \lambda \ll n$. Obviously, other bounds are needed to prove $\chi > \chi^*$.

Last not least, it would be interesting to know whether χ is concentrated on a small range of values, for some range of p, as is the case for, e.g., both Erdős-Renyi and regular random graphs.

As for the clique number, in the region $p = 1 - \Omega(1)$, it seems to be difficult to understand satisfactorily. The first moment upper bound on the number of fooling sets, Lemma 5.4, suggests that $\omega(G_{\boxtimes}^{n,p}) = (1 - o(1))n$ for $n^{-1/2} \leqslant p \leqslant n^{-1/2}\sqrt{\ln n}$, but it seems plausible that $\omega = (1 - \Omega(1))n$ already for $p > p_0 = o(n^{-1/2}\sqrt{\ln n})$.

Question 7.3. *Is it true that, a.a.s., $\omega(G_{\boxtimes}^{n,p}) = (1 - o(1))n$ for $n^{-1/2} \leqslant p \leqslant n^{-1/2}\sqrt{\ln n}$?*

More poignantly,
$$\omega(G_{\boxtimes}^{n,1/\sqrt{n}}) = ?$$

Answering this would likely require to give better lower bounds on $\omega(G_{\boxtimes}^{n,p})$ than the ones obtained by fixing the diagonal (and then using $\alpha(G_{n,p})$).

Another question about the fooling set size of random matrices presents itself naturally:

Question 7.4. *Is $\omega(p)$ unimodal as a function of p? I.e., is there a $q = q(n)$ such that if, for all n, $p_1(n) < p_2(n) < q(n)$, a.a.s., $\omega(G_{\boxtimes}^{n,p_1}) \leqslant \omega(G_{\boxtimes}^{n,p_2})$, and if, for all n, $q(n) < p_1(n) < p_2(n)$, a.a.s., $\omega(G_{\boxtimes}^{n,p_1}) \geqslant \omega(G_{\boxtimes}^{n,p_2})$?*

It seems plausible that such a q would coincide with the p_0 above.

References

[1] Sergei Bezrukov, Dalibor Fronček, Steven J. Rosenberg, and Petr Kovář, *On biclique coverings*, Discrete Math. **308** (2008), no. 2-3, 319–323. MR 2378030 (2008j:05272)

[2] Béla Bollobás, *Random graphs*, second ed., Cambridge Studies in Advanced Mathematics, vol. 73, Cambridge University Press, Cambridge, 2001. MR 1864966 (2002j:05132)

[3] Gábor Braun, Samuel Fiorini, and Sebastian Pokutta, *Average case polyhedral complexity of the maximum stable set problem*, Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2014, September 4-6, 2014, Barcelona, Spain, 2014, pp. 515–530.

[4] Joel E. Cohen and Uriel G. Rothblum, *Nonnegative ranks, decompositions, and factorizations of nonnegative matrices*, Linear Algebra Appl. **190** (1993), 149–168. MR 1230356 (94i:15015)

[5] D. de Caen, D. A. Gregory, and N. J. Pullman, *The Boolean rank of zero-one matrices*, Proceedings of the Third Caribbean Conference on Combinatorics and Computing (Bridgetown, 1981) (Cave Hill Campus, Barbados), Univ. West Indies, 1981, pp. 169–173. MR 657202 (83f:05009)

[6] ———, *The Boolean rank of zero-one matrices ii*, Proceedings of the Fifth Caribbean Conference on Combinatorics and Computing (Bridgetown, 1988) (Cave Hill Campus, Barbados), Univ. West Indies, 1988, pp. 120–126.

[7] Martin Dietzfelbinger, Juraj Hromkovič, and Georg Schnitger, *A comparison of two lower-bound methods for communication complexity*, Theoret. Comput. Sci. **168** (1996), no. 1, 39–51, 19th International Symposium on Mathematical Foundations of Computer Science (Košice, 1994). MR 1424992 (98a:68068)

[8] Samuel Fiorini, Volker Kaibel, Kanstantin Pashkovich, and Dirk Oliver Theis, *Combinatorial bounds on nonnegative rank and extended formulations*, Discrete Math. **313** (2013), no. 1, 67–83.

[9] Samuel Fiorini, Serge Massar, Sebastian Pokutta, Hans Raj Tiwary, and Ronald de Wolf, *Linear vs. semidefinite extended formulations: Exponential separation and strong lower bounds*, STOC, 2012.

[10] Samuel Fiorini, Serge Massar, Sebastian Pokutta, Hans Raj Tiwary, and Ronald De Wolf, *Exponential lower bounds for polytopes in combinatorial optimization*, Journal of the ACM (JACM) **62** (2015), no. 2, 17.

[11] Mirjam Friesen and Dirk Oliver Theis, *Fooling-sets and rank in nonzero characteristic*, The Seventh European Conference on Combinatorics, Graph Theory and Applications (Jaroslav Nešetřil and Marco Pellegrini, eds.), CRM series, vol. 16, CRM, 2013, pp. 383–390.

[12] Alan Frieze and Michał Karoński, *Introduction to random graphs*, Cambridge University Press, 2015.

[13] Dalibor Froncek, Janja Jerebic, Sandi Klavzar, and Petr Kovár, *Strong isometric dimension, biclique coverings, and sperner's theorem*, Combinatorics, Probability & Computing **16** (2007), no. 2, 271–275.

[14] Michel X. Goemans, *Smallest compact formulation for the permutahedron*, Mathematical Programming **153** (2015), no. 1, 5–11.

[15] D. A. Gregory and N. J. Pullman, *Semiring rank: Boolean rank and nonnegative rank factorizations*, J. Combin. Inform. System Sci. **8** (1983), no. 3, 223–233. MR 783759 (86h:15008)

[16] Hossein Hajiabolhassan and Farokhlagha Moazami, *Secure frameproof code through biclique cover*, Discrete Mathematics & Theoretical Computer Science **14** (2012), no. 2, 261–270.

[17] _____, *Some new bounds for cover-free families through biclique covers*, Discrete Mathematics **312** (2012), no. 24, 3626–3635.

[18] Zur Izhakian, Svante Janson, and John Rhodes, *Superboolean rank and the size of the largest triangular submatrix of a random matrix*, Proceedings of the American Mathematical Society **143** (2015), no. 1, 407–418.

[19] Svante Janson, Tomasz Łuczak, and Andrzej Rucinski, *Random graphs*, Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley-Interscience, New York, 2000. MR 1782847 (2001k:05180)

[20] Mauricio Karchmer, Eyal Kushilevitz, and Noam Nisan, *Fractional covers and communication complexity*, SIAM J. Discrete Math. **8** (1995), no. 1, 76–92. MR 1315960 (96e:68062)

[21] Richard M. Karp and Michael Sipser, *Maximum matchings in sparse random graphs*, FOCS, 1981, pp. 364–375.

[22] Kaveh Khoshkhah and Dirk Oliver Theis, *Fooling sets and the spanning tree polytope*, Preprint `arXiv:1701.00350` (2017).

[23] _____, *On the combinatorial lower bound for the extension complexity of the spanning tree polytope*, Preprint `arXiv:1702.01424` (2017).

[24] Ki Hang Kim, *Boolean matrix theory and applications*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 70, Marcel Dekker Inc., New York, 1982, With a foreword by Gian-Carlo Rota. MR 655414 (84a:15001)

[25] Eyal Kushilevitz and Noam Nisan, *Communication complexity*, Cambridge University Press, Cambridge, 1997. MR 1426129 (98c:68074)

[26] Troy Lee and Dirk Oliver Theis, *Support based bounds for positive semidefinite rank*, Tech. Report `arXiv:1203.3961` (2012).

[27] L. Lovász and M. Saks, *Communication complexity and combinatorial lattice theory*, Journal of Computer and System Sciences **47** (1993), 322–349.

[28] Laszlo Lovász, *Communication complexity: a survey*, Paths, flows, and VLSI-Layout (B. Korte, L. Lovász, H.J. Prömel, and A. Schrijver, eds.), Springer, 1990, pp. 235–265.

[29] Colin McDiarmid, *On the method of bounded differences*, Surveys in combinatorics **141** (1989), no. 1, 148–188.

[30] M. Mitzenmacher and E. Upfal, *Probability and computing — randomized algorithms and probabilistic analysis*, Cambridge, 2006.

[31] Gahyun Park and Wojciech Szpankowski, *Analysis of biclusters with applications to gene expression data*, International Conference on Analysis of Algorithms DMTCS proc. AD, vol. 267, 2005, p. 274.

[32] Mozhgan Pourmoradnasseri and Dirk Oliver Theis, *Nondeterministic communication complexity of random boolean functions (extended abstract)*, Proceedings of the 13th annual conference on Theory and Applications of Models of Computation, 2016.

[33] Alexander Schrijver, *Combinatorial optimization. Polyhedra and efficiency.*, Algorithms and Combinatorics, vol. 24, Springer-Verlag, Berlin, 2003.

[34] Yaroslav Shitov, *On the complexity of Boolean matrix ranks*, Linear Algebra and Its Applications **439** (2013), 2500–2502.

[35] Stefan Weltge, *Sizes of linear descriptions in combinatorial optimization*, Ph.D. thesis, University of Magdeburg, 2016.

[36] Mihalis Yannakakis, *Expressing combinatorial optimization problems by linear programs*, J. Comput. System Sci. **43** (1991), no. 3, 441–466. MR 1135472 (93a:90054)

A   Omitted proofs

A.1   Section 6 (chromatic number): The "usual calculation"

With
$$\alpha := \max\left(2\lambda,\ \frac{(1+\varepsilon)\ln n}{\ln\left(\frac{\ln n}{e\lambda}\right)}\right),$$

we have to show that
$$\alpha\ln(\alpha/e\lambda) \geqslant \ln n.$$

We write it down informally. In the following sequence, each inequality is implied by the next:

$$\alpha\ln(\alpha/e\lambda) \geqslant \ln n \qquad \text{[replace } \alpha \text{ by the 2nd term in the max]}$$

$$(1+\varepsilon)\frac{\ln\left(\frac{\alpha}{e\lambda}\right)}{\ln\left(\frac{\ln n}{e\lambda}\right)} \geqslant 1$$

$$\alpha \geqslant \ln^{1/(1+\varepsilon)} n$$

$$\frac{(1+\varepsilon)\ln n}{\ln\left(\frac{\ln n}{e\lambda}\right)} \geqslant \ln^{1/(1+\varepsilon)} n \qquad \text{[is true.]}$$

A.2   Section 6 (chromatic number): Chernoff

Proof of Lemma 6.3. Using Thm 1.1 in [2] (here we need the $\alpha \geqslant 2\lambda$), and the usual estimates for binomial coefficients, we find that said probability (for n sufficiently large) is at most an absolute constant times

$$\mathbf{P}\Big(\mathrm{Bin}(n,\bar{p}) = \alpha\Big) \leqslant \frac{1.1}{\sqrt{2\pi\alpha(n-\alpha)/n}}\left(\frac{\lambda}{\alpha}\right)^{\alpha}\left(\frac{n-\lambda}{n-\alpha}\right)^{n-\alpha}$$

$$\leqslant \frac{1}{\sqrt{\alpha}}\left(\frac{\lambda}{\alpha}\right)^{\alpha}\left(1 - \frac{\alpha - \lambda}{n - \alpha}\right)^{n-\alpha} \leqslant \frac{1}{\sqrt{\alpha}}\left(\frac{\lambda}{\alpha}\right)^{\alpha} e^{\alpha - \lambda},$$

as promised. □

A.3   Section 6 (chromatic number): Number of distinct rows

Proof of Lemma 6.6. For notational convenience, for $k = 1, \ldots, n$, let

$$S_k := \{\ell \mid M_{k,\ell} = 0\}$$

The S_k are random sets, where the events $\ell \in S_k$ are all independent and have probability $\bar{p}$. For $m \geqslant 0$, with $\mathbf{0} := \{1, \ldots, n\}$, denoting by

$$X_m := |\{S_1, \ldots, S_k\} \setminus \{\mathbf{0}\}|,$$

the number of distinct non-zero rows among the first m rows of $M^{n,p}$, we need to show that $X_n = \Omega(n)$. This is quite easy for $\bar{p} = \Omega(1/n)$, i.e., Item (a). Here, we just prove it in the case that $\bar{p} \leqslant 1/2n$, i.e., Item (b).

Denote by A_{m+1} the event that the $(m+1)$st row is zero or a duplicate of the first m rows, i.e., that

$$S_{m+1} \in \{\mathbf{0}, S_1, \ldots, S_m\}.$$

We enumerate the distinct sets: $\{S_1, \ldots, S_m\} =: \{S_{k_1}, \ldots, S_{k_{X_m}}\}$. Now, for $m \geqslant 1$, we have

$$\mathbf{P}\Big(A_{m+1} \;\Big|\; |S_1|, \ldots, |S_m|, X_m\Big) = \mathbf{P}\Big(S_{m+1} \in \{\mathbf{0}, S_1, \ldots, S_m\} \;\Big|\; |S_1|, \ldots, |S_m|, X_m\Big)$$

$$= \mathbf{P}(S_{m+1} = \mathbf{0}) + \sum_{j=1}^{X_m} \mathbf{P}\Big(S_{m+1} = S_{k_j} \;\Big|\; |S_1|, \ldots, |S_m|, X_m\Big)$$

$$= \bar{p}^n + \sum_{j=1}^{X_m} \bar{p}^{|S_{k_j}|} p^{n-|S_{k_j}|} \leqslant \bar{p}^n + p^n + \max(0, X_m - 1)\bar{p}p^{n-1},$$

where the last inequality comes from the fact that, since the S_{k_j} are all distinct, at most one of them has cardinality 0. Hence, for $m \geqslant 2$,

$$\mathbf{P}\Big(A_{m+1} \mid X_m, X_1 = 1\Big) \leqslant \bar{p}^n + p^n + (X_m - 1)\bar{p}p^{n-1}$$
$$\leqslant \bar{p}^n + p^n - \bar{p}p^{n-1} + \bar{p}p^{n-1}X_m.$$

Now, for $m \geqslant 1$,

$$\mathbf{E}\Big(X_{m+1} \mid X_m, X_1 = 1\Big) = X_m + 1 - \mathbf{P}(A_{m+1} \mid X_m, X_1 = 1),$$
$$\geqslant X_m + 1 - \bar{p}^n - p^n + \bar{p}p^{n-1} - \bar{p}p^{n-1}X_m$$
$$= 1 + \bar{p}p^{n-1} - \bar{p}^n - p^n + (1 - \bar{p}p^{n-1})X_m.$$

Using the law of total probability and solving the recursion[5], we find that

$$\mathbf{E}\big(X_m \mid X_1 = 1\big) \geqslant (1 + \bar{p}p^{n-1} - \bar{p}^n - p^n)\frac{1 - (1 - \bar{p}p^{n-1})^{m-2}}{\bar{p}p^{n-1}} + (1 - \bar{p}p^{n-1})^{m-1}$$

With $\lambda := \bar{p}n$, again, note that, since, by our assumption above, $\lambda \leqslant 1/2$, using the Bernoulli inequalities $1 - tn \leqslant (1 - t)^n \leqslant 1 - tn + t^2\binom{n}{2}$ for $t < 1$, we have

$$\frac{1}{2} \leqslant 1 - \lambda \leqslant p^n \leqslant p^{n-1} \leqslant 1 - \lambda\left(\frac{n-1}{n} + \lambda\frac{n-1}{n}\right) \leqslant 1,$$

so that

$$(1 - \bar{p}p^{n-1})^{m-2} \leqslant (1 - \bar{p}/2)^{m-2} \leqslant 1 - \frac{\lambda}{2}\left(\frac{m-2}{n} + \frac{\lambda}{2}\frac{m-2}{n}\right).$$

We conclude that, for $m = n$,

$$\mathbf{E}\big(X_m \mid X_1 = 1\big) \geqslant (1 - p^n)\frac{1 - (1 - \bar{p}p^{n-1})^{m-2}}{\bar{p}p^{n-1}}$$

$$\geqslant \lambda\left(\frac{n-1}{n} + \lambda\frac{n-1}{n}\right) \cdot \frac{\frac{\lambda}{2}\left(\frac{m-2}{n} + \frac{\lambda}{2}\frac{m-2}{n}\right)}{\lambda/n} \geqslant (1 + o(1))\frac{\lambda n}{2}.$$

Since $\mathbf{P}(X_1 = 1) = \mathbf{P}(S_1 = \mathbf{0}) = (1 - \bar{p}^n) = 1 - o(1)$, this implies $\mathbf{E}\,X_n \geqslant \mathbf{E}(X_n \mid X_1 = 1)\,\mathbf{P}(X_1 = 1) \geqslant (1 - o(1))\lambda n/2$.

To obtain the a.a.s. statement from the one about the expectation, we use Martingale-based concentration bound (Corollary 2.27 in [19]): as changing one row can affect X_n by at most 1, we get

$$\mathbf{P}\big(X_n \leqslant \lambda n/4\big) \leqslant \mathbf{P}\big(X_n \leqslant \mathbf{E}\,X_n - \lambda n/4\big) \leqslant e^{-(\lambda n)^2/32n} = e^{-\Omega(\lambda^2 n)} = o(1),$$

where the last equation follows from the condition $n^{-3/2} = o(\bar{p})$. □

---

[5]The recursion: $\mu_{m+1} = \alpha + \beta\mu_m = \ldots = \alpha\sum_{j=0}^{m-1}\beta^j + \beta^m\mu_1 = \alpha\frac{1 - \beta^m}{1 - \beta} + \beta^m\mu_1.$