INSTITUTO DE MATEMÁTICA PURA E APLICADA

Rio de Janeiro – RJ

# COMBINATORIAL PROPERTIES OF RANDOM GRAPHS AND MATRICES

A dissertation submitted in partial fulfillment of the

requirements for the degree of

DOCTOR OF PHILOSOPHY

in

MATHEMATICS

by

Letícia Dias Mattos

Advisor: Robert Morris

2021

ACKNOWLEDGMENTS

Agradeço à minha família. Silvana, Melissa, Sérgio e Daniel, vocês foram fundamentais na minha caminhada. Ao meu orientador, Rob Morris, que criou um ambiente de pesquisa em Combinatória extremamente amigável. É impossível não se inspirar com a sua empolgação em resolver problemas. Agradeço toda a paciência e o conhecimento compartilhado comigo durante esses anos de doutorado.

Aos meus amigos e co-autores, Pedro Araújo, Marcelo Campos, Simon Griffiths, Anita Liebenau, Taísa Martins, Walner Mendonça, Luiz Moreira, Natasha Morrison, Guilherme Mota e Jozef Skokan. Foi muito gratificante ter trabalhando com todos vocês.

Aos vários amigos que o IMPA me proporcionou, presentes nos momentos bons e ruins. Vou sentir saudades das nossas conversas na hora do café, seja pra discutir matemática ou decidir se xadrez é esporte. Vocês fizeram a minha vida no Rio muito mais feliz.

A Simon Griffiths, Roberto Imbuzeiro, Maurício Collares, Taísa Martins e Guilherme Mota por aceitarem o convite para participar da banca.

A todos os meus amigos e colegas da UFMG, professores de graduação e mestrado que sempre me incentivaram a continuar na Matemática. Aos funcionários do IMPA, por toda ajuda com prazos e processos administrativos. Por último, à OBMEP, por me mostrar que ser matemática era possível.

ABSTRACT

In this thesis we study two of the main objects in probabilistic combinatorics: random matrices and random graphs.

In the first part, joint with Campos, Morris and Morrison, we consider a uniformly-chosen random $n \times n$ symmetric matrix $M_n$ with entries in $\{-1, +1\}$. We show that the probability that $M_n$ is singular is at most $\exp(-\Omega(\sqrt{n}))$. The main new ingredient is an inverse Littlewood–Offord theorem in $\mathbb{Z}_p^n$ whose statement is inspired by the method of hypergraph containers.

In the second part, joint with Griffiths and Morris, we study the size of the maximum $k$-clique packing in $G(n,p)$, denoted by $\nu_p(k)$, for any fixed $p \in (0,1)$. If $k$ is near the size of the largest clique in $G(n,p)$, we show that $\nu_p(k) = \Omega(n^2/k^3)$. To show this result, we follow a random greedy process and use the differential equation method. In particular, this improves the previous lower bound on $\mathbb{E}\left(\nu_p(k)\right)$ obtained by Acan and Kahn.

In the third part, joint with Liebenau, Mendonça and Skokan, we study asymmetric Ramsey properties of $G(n,p)$ for cliques and cycles. For any pair of cliques and cycles $(K_r, C_\ell)$, we determine the threshold for finding a red copy of $K_r$ or a blue copy of $C_\ell$ in every red and blue edge-colouring of $G(n,p)$. The main tool behind the proof is a structural characterisation of Ramsey graphs for the pair $(K_r, C_\ell)$ via a 'container type' argument.

## RESUMO

Nesta tese estudamos dois dos principais objetos em combinatória probabilística: matrizes aleatórias e grafos aleatórios.

Na primeira parte, com Campos, Morris e Morrison, consideramos uma matriz aleatória e simétrica $M_n$, com dimensões $n \times n$ e entradas em $\{-1, +1\}$, escolhida uniformemente ao acaso. Mostramos que a probabilidade de $M_n$ ser singular é no máximo $\exp(-\Omega(\sqrt{n}))$. O principal ingrediente da prova é um teorema inverso de Littlewood–Offord em $\mathbb{Z}_p^n$ cujo enunciado é inspirado pelo método de container para hipergrafos.

Na segunda parte, com Griffiths e Morris, estudamos o tamanho do maior empacotamento de $k$-cliques em $G(n,p)$, denotado por $\nu_p(k)$, para toda constante $p \in (0,1)$. Se $k$ está perto do tamanho do maior clique em $G(n,p)$, mostramos que $\nu_p(k) = \Omega(n^2/k^3)$. Para isso, analisamos um processo aleatório guloso e usamos o método de equações diferenciais. Em particular, esse resultado melhora a cota inferior para $\mathbb{E}\left(\nu_p(k)\right)$, que foi previamente obtida por Acan and Kahn.

Na terceira parte, com Liebenau, Mendonça and Skokan, estudamos propriedades assimétricas de Ramsey em $G(n,p)$ para cliques e ciclos. Para todo par de clique e ciclo $(K_r, C_\ell)$, determinamos o *threshold* para encontrar uma cópia vermelha de $K_r$ ou uma cópia azul de $C_\ell$ em toda coloração das arestas de $G(n,p)$ com vermelho e azul. A principal ferramenta por detrás da prova é uma caracterização estrutural dos grafos Ramsey para o par $(K_r, C_\ell)$ através de um argumento similar ao usado no método de container.

TABLE OF CONTENTS

CHAPTER PAGE

## LIST OF SYMBOLS

| | |
|---|---|
| $[n]$ | the set $\{1, 2, \ldots, n\}$ |
| $2^{[n]}$ | the collection of subsets of $\{1, 2, \ldots, n\}$ |
| $\binom{[n]}{i}$ | the collection of subsets of size $i$ of $\{1, 2, \ldots, n\}$ |
| $O(f(n))$ | a function which is at most a constant multiple of $f$ |
| $\Omega(f(n))$ | a function which is at least a constant multiple of $f$ |
| $o(f(n))$ | a function $g$ such that $\lim_{n\to\infty} g(n)/f(n) = 0$ |
| $\omega(f(n))$ | a function $g$ such that $\lim_{n\to\infty} \lvert g(n)/f(n)\rvert = +\infty$ |
| $E(G)$ | the set of edges of a graph/hypergraph $G$ |
| $e(G)$ | the number of edges of a graph/hypergraph $G$ |
| $V(G)$ | the set of vertices of a graph/hypergraph $G$ |
| $v(G)$ | the number of vertices of a graph/hypergraph $G$ |
| $K_n$ | the complete graph on $n$ vertices |
| $C_\ell$ | the cycle on $\ell$ vertices |

CHAPTER 1

# INTRODUCTION

## 1.1 Random Matrices

The study of random matrices started in the 1950's with Wigner [124], motivated by the analysis of wave functions of quantum mechanical systems. Since then, random matrices have been intensively studied by the physicists to understand the statistical behaviour of chaotic systems. Later, the subject also attracted the interest of the mathematical community. One of the first investigations in this topic was made by Keating [64], who established a connection between the distribution of zeros of the Riemann zeta function and the distribution of eigenvalues of certain random matrices.

The random matrices models are usually classified into discrete and continuous. Surprisingly, the discrete models are the least understood. In Combinatorics, we are typically interested in problems related to singularity, simpleness of spectrum and anti-concentration bounds for the determinant. In this thesis, we address the singularity problem.

### 1.1.1 Singularity of random matrices with independent entries

Let $X$ be a non-constant discrete random variable. Let $M_n = M_n(X)$ denote a random $n \times n$ matrix whose entries are independent copies of $X$. One of the most basic questions one could ask about this model concerns singularity.

**Question 1.1.1.** *What is the asymptotic behaviour of* $\mathbb{P}(\det(M_n) = 0)$*?*

Let $\mathcal{E}_n = \mathcal{E}_n(X)$ be the union of the following events: (a) there are two rows or two columns of $M_n$ which are equal (up to a factor of $\pm 1$).; (b) at least one row is zero, or one

column is zero. An old and notorious conjecture (see, for example, the discussion in [62]) states that the probability that $\det(M_n) = 0$ is asymptotically equal to the probability that the event $\mathcal{E}_n$ occurs.

**Conjecture 1.1.2.** $\mathbb{P}(\det(M_n) = 0) = \mathbb{P}(\mathcal{E}_n)$.

The first progress on this conjecture was made in 1967 by Komlós [69], who considered the model where $X$ is uniformly distributed in $\{-1, 1\}$. By simplicity, let $A_n$ denote the (uniformly-chosen) random $n \times n$ matrix with entries in the set $\{-1, 1\}$. For this particular model, Komlós used Erdős' celebrated solution [21] of the Littlewood–Offord problem to deduce that $A_n$ is singular with probability at most $O(n^{-1/2})$. The Littlewood–Offord problem concerns anti-concentration bounds for the probability that a random walk with possibly different size steps hits a certain value. An introductory discussion about it can be found in subsection 1.1.3.

The first exponential bound on the singularity probability of $A_n$ was only obtained in 1995, by Kahn, Komlós and Szemerédi [62]. They showed that $A_n$ is singular with probability at most $O(0.999^n)$ by applying a Halász-type inequality to the Littlewood–Offord problem. Following improvements in the late 2000s by Tao and Vu [113] and by Bourgain, Vu and Wood [15], a major breakthrough was made recently by Tikhomirov [118].

**Theorem 1.1.3** (Tikhomirov, 2020)**.** $\mathbb{P}\big(\det(A_n) = 0\big) = \left(\frac{1}{2} + o(1)\right)^n$.

Observe that Conjecture 1.1.2 implies that the probability of the event $\det(A_n) = 0$ is asymptotically equal to $n^2 2^{-n+1}$. Although Theorem 1.1.3 gives the correct exponential term, it does not imply Conjecture 1.1.2. The term $(1+o(1))$ in Tikhomirov's theorem grows superpolynomially, while we expect to have only a factor of $n^2$.

Perhaps the second most well-studied model of random matrices with independent entries is the Bernoulli matrix model. For any $p \in [0, 1]$, let $\mathrm{Ber}(p)$ denote a indicator random vari-

able of parameter $p$. Let $B_n(p)$ denote a random $n \times n$ matrix whose entries are independent copies of $\mathrm{Ber}(p)$. The main theorem of Tikhomirov in [118] imply the following bound on the probability that $B_n(p)$ is singular.

**Theorem 1.1.4** (Tikhomirov, 2020)**.** *Let $p \in [0,1]$ be a constant. We have*

$$\mathbb{P}\big(\det(B_n(p)) = 0\big) = \Big(\max\{p, 1-p\} + o(1)\Big)^n.$$

As before, Theorem 1.1.4 does not imply Conjecture 1.1.2. However, there are some ranges of $p$ where this conjecture is known to be true. The first result was obtained very recently by Basak and Rudelson [9] in the sparse setting. They showed that if $pn = \log n + O(\log\log n)$, then Conjecture 1.1.2 holds for $B_n(p)$. A bit later, Litvak and Tikhomirov [74] showed that the conjecture holds whenever $Cn^{-1}\log n \le p \le C^{-1}$, where $C \ge 1$ is some universal constant. In 2020, Han Huang [51] closed the gap between these two results and showed that Conjecture 1.1.2 holds for $B_n(p)$ whenever $n^{-1}\log n \le p \le c$, for some small constant $c > 0$.

Very recently, Jain, Sah and Sawhney [53] proved Conjecture 1.1.2 for Bernoulli random matrices in the case where $p \in (0, 1/2)$.

**Theorem 1.1.5** (Jain, Sah and Sawhney, 2020)**.** *Let $p \in (0,1/2)$ be a constant. We have*

$$\mathbb{P}\big(\det(B_n(p)) = 0\big) = (2 + o(1))n\big(1-p\big)^n.$$

In a subsequent paper (see [54]), their result was also extended for models in which the associated random variable is not uniform outside the support.

### 1.1.2 Singularity of symmetric random matrices

One of the simplest models in which not all the entries are independent from each other is the symmetric random matrix model. In Combinatorics, this model arises naturally from

the adjacency matrices of random graphs. However, the dependencies between the entries makes the problem significantly harder.

Let $M_n$ denote a (uniformly-chosen) random $n \times n$ matrix with entries in the set $\{-1, 1\}$. Apparently, Weiss in the early 1990s (see [19]) asked if $M_n$ is invertible with high probability. Similarly to the non-symmetric case, it is widely believed that the probability of the event $\det(M_n) = 0$ is asymptotically equal to the probability that two of the rows are equal, and hence is of order $n^2 2^{-n}$.

**Conjecture 1.1.6.** $\mathbb{P}(\det(M_n) = 0) = \Theta(n^2 2^{-n})$.

The first result towards solving Conjecture 1.1.6 was obtained in 2005 by Costello, Tao and Vu [19]. The main tool behind their result is a quadratic variant of Littlewood-Offord-type results concerning the concentration of random variables.

**Theorem 1.1.7** (Costello, Tao and Vu, 2005)**.** *Let $X$ be any non-constant discrete random variable. Let $Q_n = (q_{ij})_{i,j}$ be any random $n \times n$ symmetric random matrix whose variables $\{q_{ij} : 1 \leq i < j \leq n\}$ are independent copies of $X$. Then,*

$$\mathbb{P}(\det(Q_n) = 0) \leq n^{-1/8+o(1)}.$$

Observe that in the theorem above no requirements are placed in the diagonal elements. In particular, for any $p \in (0, 1)$ we have that the adjacency matrix of $G(n, p)$ is non-singular with high probability.

The first super-polynomial bound on the probability that $M_n$ is singular, and the first exponential-type bound (i.e., of the form $\exp(-n^c)$ for some $c > 0$), were obtained almost simultaneously, by Nguyen [89] and Vershynin [119], respectively. We remark that the proof in [89] was based on earlier work of Nguyen and Vu [88], which relied on deep results from additive combinatorics, while the proof in [119] built on the earlier breakthroughs of Rudelson and Vershynin [100, 104].

Recently, a new 'combinatorial' approach to studying the invertibility of discrete random matrices was introduced by Ferber, Jain, Luh, and Samotij [31], and applied by Ferber and Jain [30] to prove that

$$\mathbb{P}\big(\det(M_n) = 0\big) \leq \exp\big(-cn^{1/4}\sqrt{\log n}\big)$$

for some $c > 0$. In a joint work with Campos, Morris and Morrison [17], we use a different combinatorial approach (inspired by the method of [31, 30]) to obtain the following bound.

**Theorem 1.1.8** (Campos, M., Morris and Morrison, 2021)**.** *There exists $c > 0$ such that*

$$\mathbb{P}\big(\det(M_n) = 0\big) \leq \exp\big(-c\sqrt{n}\big)$$

*for all sufficiently large $n \in \mathbb{N}$.*

The main new ingredient in our approach is an inverse Littlewood–Offord theorem which applies to vectors $v \in \mathbb{Z}_p^n$ that exhibit a very mild amount of 'structure' and provides just enough information to allow us to deduce Theorem 1.1.8.

In 2020, Jain, Sah and Sawhney [52] improved our bound by a factor of $(\log n)^{1/4}$ in the exponent. The main tool behind their proof is a new notion of arithmetic structure inspired by the Least Common Denominator method introduced by Rudelson and Vershynin [100]. In the same year, Campos, Jenssen, Michelen and Sahasrabudhe [16] improved their bound and attained the natural barrier of $\exp(-\sqrt{n \log n})$.

**Theorem 1.1.9** (Campos, Jenssen, Michelen and Sahasrabudhe, 2021+)**.** *There exists $c > 0$ such that*

$$\mathbb{P}\big(\det(M_n) = 0\big) \leq \exp\big(-c\sqrt{n \log n}\big)$$

*for all sufficiently large $n \in \mathbb{N}$.*

Their method is considerably simple. They developed an inverse Littlewood-Offord result by considering the set of places where a random walk is likely to terminate.

### 1.1.3 The Littlewood–Offord problem

For any abelian group $G$, integer $n \in \mathbb{N}$, and vector $v \in G^n$, define

$$\rho(v) := \max_{a \in G} \mathbb{P}\Big( \sum_{i=1}^{n} \varepsilon_i v_i = a \Big),$$

where $\varepsilon$ is a uniformly-chosen random element of $\{-1, 1\}^n$. The problem of obtaining upper bounds on $\rho(v)$ (and similar functions) was introduced by Littlewood and Offord [73] during their study of random polynomials. Since then, this problem has been known as the 'Littlewood–Offord problem'.

In 1943, Littlewood and Offord [73] showed that $\rho(v) = O\big(|v|^{-1/2} \log |v|\big)$ when $G = \mathbb{Z}$, where $|v| := \big|\big\{i \in [n] : v_i \neq 0\big\}\big|$ denotes the size of the support of $v$. In 1945, Erdős [21] improved this bound to $\rho(v) = O\big(|v|^{-1/2}\big)$ using Sperner's theorem. Observe that Erdős' bound is sharp: if $v = (1, 1, \ldots, 1)$, then $\rho(v) = \Omega(n^{-1/2})$.

**Theorem 1.1.10** (Erdős, 1945)**.** *Let $n \in \mathbb{N}$ and $v \in \mathbb{Z}_p^n$. We have*

$$\rho(v) = O\big(|v|^{-1/2}\big).$$

The Littlewood–Offord problem has been extensively studied over the past several decades, for example by Rogozin [99], Sárkőzy and Szemerédi [107], Esseen [29], Halász [48], and Frankl and Füredi [35]. Under the additional assumption that all the coordinates are distint, Erdős and Moser [24] showed in 1947 that the bound in Theorem 1.1.10 can be improved to $\rho(v) = O(|v|^{-3/2} \log |v|)$. A few years later, Sárkőzy and Szemerédi [107] improved this result by removing the log factor.

**Theorem 1.1.11** (Sárkőzy and Szemerédi, 1965)**.** *Let $n \in \mathbb{N}$ and $v \in \mathbb{Z}_p^n$ be a vector whose coordinates are distinct. We have*

$$\rho(v) = O\big(|v|^{-3/2}\big).$$

In 1977, Halász [48] showed that the bound on $\rho(v)$ can be significantly improved when $v$ does not have much arithmetic structure. For any $\ell \in \mathbb{N}$ and any vector $v \in \mathbb{Z}_p^n$, define

$$R_\ell(v) := |\{(i_1, \dots, i_{2\ell}) \in [n]^{2\ell} : v_{i_1} + \cdots + v_{i_\ell} = v_{i_{\ell+1}} + \cdots + v_{i_{2\ell}}\}|. \tag{1.1}$$

Observe that we allow repetitions on the choices of the sequences. Halász's theorem can be formulated as follows.

**Theorem 1.1.12** (Halász, 1977)**.** *Let $n \in \mathbb{N}$ and $v \in \mathbb{Z}_p^n$ be any vector. We have*

$$\rho(v) = O(n^{-2\ell-1/2} R_\ell).$$

When $\ell = 1$ and all the coordinates of $v$ are distinct, we have $R_1(v) = n$. In particular, we obtain Theorem 1.1.11 as a corollary of Theorem 1.1.12.

An anticoncentration lemma can also be derived from the work of Halász [48] when the abelian group is $\mathbb{Z}_p$, for $p$ prime. In order to state it, we need a little preparation. First, let us define multiplication on $\mathbb{Z}_p$ as follows: if $x, y \in \mathbb{Z}_p$, then the product $x \cdot y \in \mathbb{Z}$ is obtained by projecting $x$ and $y$ onto elements of $\{0, 1, \dots, p-1\}$ in the usual way, and then multiplying in $\mathbb{Z}$. Let $\|\cdot\|$ denote the distance to the nearest integer, and for each $n \in \mathbb{N}$, prime $p$ and vector $v \in \mathbb{Z}_p^n$, define the *level sets* of $v$ to be

$$T_t(v) := \left\{ k \in \mathbb{Z}_p : \sum_{i=1}^{n} \left\| \frac{k \cdot v_i}{p} \right\|^2 \leq t \right\}, \tag{1.2}$$

for each $t \geq 0$.

We can now state the lemma of Halász [48]. We provide a proof in Chapter 2.

**Lemma 1.1.13** (Halász's Anticoncentration Lemma)**.** *Let $n \in \mathbb{N}$ and $p$ be prime, and let $v \in \mathbb{Z}_p^n \setminus \{0\}$. Then*

$$\rho(v) \leq \frac{3}{p} + \frac{6|T_\ell(v)|}{p\sqrt{\ell}} + 3e^{-\ell}$$

*for every $1 \leq \ell \leq 2^{-6}|v|$.*

### 1.1.4 The Inverse Littlewood–Offord problem

One of the major problems in additive combinatorics is to understand the structure of a set with small sumset[1]. The celebrated Freiman's theorem (see, for example, [45]) asserts that in any torsion-free[2] abelian group, sets with 'small' sumset are contained in generalised arithmetic progressions[3] (GAP) of bounded rank. Motivated by this and other inverse theorems from additive combinatorics, Tao and Vu [114] brought a different perspective to the Littlewood–Offord problem.

**Question 1.1.14** (Tao and Vu, 2009)**.** *Does $v$ have some structure when $\rho(v)$ is large?*

Before we address the results regarding this question, let us provide some examples in which $v \in \mathbb{Z}^n$ 'structured' implies $\rho(v)$ polynomially large.

(*A*) $v_i \in [-M, M]$ for all $i \in [n]$. Let $(c_i)_{i=1}^n$ be any sequence of constants such that $|c_i| \leq 1$. By the Central Limit Theorem, we have

$$\mathbb{P}\big(|c_1\varepsilon_1 + \cdots + c_n\varepsilon_n| \leq \sqrt{n}\big) = 1 - o(n^{-1}).$$

Taking $c_i = v_i/M$, we obtain

$$\mathbb{P}\big(|\varepsilon_1 v_1 + \cdots + \varepsilon_n v_n| \leq M\sqrt{n}\big) = 1 - o(n^{-1}).$$

By the Pigeonhole Principle, it follows that

$$\rho(v) = \Omega\left(\frac{1}{M\sqrt{n}}\right).$$

Observe that we obtain the same result when the coordinates of $v$ are contained in an arithmetic progression of size $M$.

[1] For any given set $A$, the set $A + A = \{a_1 + a_2 : a_1, a_2 \in A\}$ is called the *sumset* of $A$.

[2] A abelian group is called *torsion-free* if no element other than the identity is of finite order.

[3] A GAP of rank $d$ is a set of the form $\big\{a + j_1\ell_1 + \cdots + j_d\ell_d : 1 \leq j_i \leq k_i\big\}$ for some $a, \ell_1, \ldots, \ell_d \in \mathbb{Z}_p$ and $k_1, \ldots, k_d \in \mathbb{N}$

(*B*) Let $Q$ be a generalised arithmetic progression of rank $r$ of the form

$$Q = \{\ell_1 d_1 + \cdots + \ell_r d_r : -M \leq \ell_i \leq M\}.$$

By simplicity, assume that $Q$ is *proper*, that is, $|Q| = (2M+1)^r$. Let $v \in \mathbb{Z}^n$ be such that $v_i \in Q$ for all $i \in [n]$. Thus, for each $i \in [n]$, we can write

$$v_i = \sum_{j=1}^{r} \ell_{ij} d_j$$

for some $\ell_{ij} \in [-M, M]$. Now we can write the sum $\varepsilon_1 v_1 + \cdots + \varepsilon_n v_n$ as

$$d_1 \cdot \left( \sum_{k=1}^{n} \ell_{k1} \varepsilon_k \right) + \ldots + d_r \cdot \left( \sum_{k=1}^{n} \ell_{kr} \varepsilon_k \right).$$

By item (A), we have that with high probability each of the sums above is concentrated on $M\sqrt{n}$ values. By the Pigeonhole Principle, it follows that

$$\rho(v) = \Omega\left( \frac{1}{|Q| n^{r/2}} \right).$$

The examples above show that if $v \in \mathbb{Z}^n$ is contained in a small generalised arithmetic progression, then $\rho(v)$ is large. In 2009, Tao and Vu showed that the converse should also be true. That is, if $\rho(v)$ is large, then $v$ must be essentially contained in a generalised arithmetic progression. In 2010, Tao and Vu [116] proved a stronger inverse theorem and obtained better bounds on the volume of the generalised arithmetic progression. Later, Nguyen and Vu [88] improved their bounds combining some Fourier techniques developed by Haláz [48] with Freiman's theorem. Their theorem is referred as the optimal inverse Littlewood-Offord theorem and can be stated as follows.

**Theorem 1.1.15** (Nguyen and Vu, 2010)**.** *Let $\varepsilon \in (0,1)$ and $C > 0$ be constants. Let $v \in \mathbb{Z}^n$ and assume that*

$$\rho(v) \geq n^{-C}.$$

*Then, there exists a proper GAP $Q$ of rank $r = O_{C,\varepsilon}(1)$ such that*

(1) $Q = -Q$;

(2) $|\{i \in [n] : v_i \notin Q\}| \leq \varepsilon n$;

(3) $|Q| = O_{\varepsilon,C}(\rho(v)^{-1} n^{-r/2})$.

In the same paper, Nguyen and Vu left as an exercise to show that the inverse Littlewood–Offord theorem (Theorem 1.1.15) implies Halász theorem (Theorem 1.1.12). By completeness, we now provide a proof of this implication. Let $v = (v_1, \dots, v_n)$ be a vector as in Theorem 1.1.15 and let $Q$ be the GAP given in this theorem. For each $x \in \mathbb{Z}$, define

$$r(x) := |\{(i_1, \dots, i_\ell) \in [n]^\ell : v_{i_1} + \cdots + v_{i_\ell} = x \text{ and } v_{i_j} \in Q\}|.$$

Now, consider the set $S := \{x \in \mathbb{Z} : r(x) \neq 0\}$. By convexity and double-counting, we have

$$R_\ell = \sum_{x \in S} \binom{r(x)}{2} \geq \frac{1}{4|S|} \left( \sum_{x \in S} r(x) \right)^2 = \frac{n^{2\ell}}{4|S|}.$$

As $S$ can also be expressed as $S = \{v_{i_1} + \cdots + v_{i_\ell} : v_{i_j} \in Q\}$, we have $S \subseteq \ell Q$, where the notation $\ell Q$ stands for the $\ell$-sumset of $Q$. It follows that $|S| \leq \ell^r |Q|$ and by the bound on $|Q|$ in Theorem 1.1.15 we obtain

$$R_\ell = \Omega\left(n^{2\ell + r/2} \rho(v)\right).$$

**Inverse Littlewood–Offord in other groups**

Motivated by the problem of invertibility of random matrices, Rudelson and Vershynin [100] and Ferber, Jain, Luh and Samotij [31] developed Inverse Littlewood–Offord theorems in $\mathbb{R}$ and $\mathbb{Z}_p$, respectively. As their statements are quite technical, we do not enunciate them here. Instead, we say a few words about their result.

In 2008, Rudelson and Vershynin [100] gave a sharp estimate to the small ball probability

$$\rho_\varepsilon(v) := \sup_{a \in \mathbb{R}} \mathbb{P}\left( \sum_{i=1}^n \xi_i v_i \in (a - \varepsilon, a + \varepsilon) \right),$$

where $(\xi_i)_i$ are independent and identically distributed centered random variables with variance at least 1 and bounded third moments. Their inverse theorem was obtained as a corollary of the bounds given on $\rho_\varepsilon(v)$, for any vector $v \in \mathbb{R}^n$. The result is stated in terms of what they called *essential least common denominator* of real numbers, which is (roughly speaking) the minimum rescaling needed to make most coordinates of a vector close to an integer. In contrast to Theorem 1.1.15, their inverse theorem guarantees an approximate rather than exact embedding of the coefficients of a vector $v$ with 'large' $\rho_\varepsilon(v)$ into an arithmetic progression. Moreover, such vectors are approximately embedded into one arithmetic progression rather than a GAP.

In 2019, Ferber, Jain, Luh and Samotij [31] studied the counting problem associated with the inverse Littlewood–Offord problem. In typical applications, inverse Littlewood–Offord theorems are only used to obtain estimates on the number of vectors $v$ which have large $\rho(v)$. Motivated by the problem on singularity of random symmetric matrices, they obtained significantly better bounds for the counting problem than those derived from the previous inverse Littlewood–Offord theorems. Roughly speaking, their counting theorem provides an upper bound on the number vectors $v$ for which every 'large' subvector $u \subseteq v$ has 'large' $R_\ell(u)$ (recall the definition of $R_\ell$ in (1.1)). On the other hand, when $v$ has a 'large' subvector $u \subseteq v$ with 'small' $R_\ell(u)$, they used an adaptation of Halász's inequality to show that $\rho(v)$ must be small.

In a joint work with Campos, Morris and Morrison, we developed an inverse Littlewood–Offord theorem in $\mathbb{Z}_p$ which differs from (most of) these earlier results in several important ways: it is designed for $\mathbb{Z}_p$, rather than $\mathbb{Z}$; it gives (weak) structural information about every vector $v \in \mathbb{Z}_p^n$ such that $\rho(v) \geq 4/p$; and it is designed to facilitate iteration. In particular, the method of Nguyen and Vu (see, e.g., [90, Theorem 8.1]) requires that $\rho(v) \geq n^{-C}$, and those of Ferber, Jain, Luh, and Samotij [31, Theorem 1.7] and of Rudelson and Vershynin (see,

e.g., [100, Theorem 1.5]) seem difficult to iterate. Let us note, however, that the powerful results of Rudelson and Vershynin [100, 104] are applicable for $\rho(v) \geq e^{-cn}$, and are moreover valid over the real numbers. We remark that the statement of Theorem 2.1.2 was inspired by the method of hypergraph containers, a technique that was introduced several years ago by Balogh, Morris and Samotij [6] and (independently) Saxton and Thomason [108], and which has turned out to have a large number of applications in extremal and probabilistic combinatorics. We refer the interested reader to the survey [7] for more details.

**Theorem 1.1.16** (Campos, M., Morris, Morrison, 2021)**.** *Let $p$ be a prime. There exists a family $\mathcal{C}$ of subsets of $\mathbb{Z}_p$, with*

$$|\mathcal{C}| \leq \exp\Big(2^{12}\big(\log p\big)^2\Big), \tag{1.3}$$

*such that for each $n \in \mathbb{N}$, and every $v \in \mathbb{Z}_p^n$ with $\rho(v) \geq 4/p$ and $|v| \geq 2^{18}\log p$, there exist sets $B(v) \in \mathcal{C}$ such that*

$$\big|\big\{i \in [n] : v_i \notin B(v)\big\}\big| \leq \frac{n}{4} \qquad \text{and} \qquad |B(v)| \leq \frac{2^{16}}{\rho(v)\sqrt{|v|}}. \tag{1.4}$$

We remark that our inverse theorem used on the singularity problem is slightly more technical than Theorem 1.1.16. See Chapter 2 for more details.

In order to motivate the statement of the theorem above, it is instructive to consider the example of a vector $v \in \mathbb{Z}_p^n$ whose entries are chosen uniformly (and independently) at random from a $d$-dimensional generalised arithmetic progression $Q$. For such a vector, $\rho(v)$ is typically of order $|Q|^{-1}n^{-d/2}$ (see Example (A)), and the $p^{\Theta(d)}$ such progressions are natural 'containers' for these vectors. This example suggests that one might be able to prove a stronger version of Theorem 2.1.2, in which most 'containers' (members of the family $\mathcal{C}$) are significantly smaller than the maximum given in (2.3). However, without significant additional ideas such a strengthening would *not* imply a significant improvement over the bound in Theorem 4.1.1. See the discussion in Chapter 2 for more details.

In 2020, Campos, Jenssen, Michelen and Sahasrabudhe [16] developed an improved and considerably simpler 'rough' inverse Littlewood–Offord theorem which parallels Theorem 2.1.2. The key concept of their proof is to consider the set of places where a random walk is 'likely' to terminate relative to 0. As the main application, they used their inverse Littlewood–Offord theorem to show that the random matrix[4] $M_n$ is singular with probability $O(\exp(-\sqrt{n \log n}))$. This bound represents a natural barrier in all previous approaches to this problem. See the discussion in Chapter 2 for more details.

### 1.1.5 Inverse Littlewood–Offord in random matrix theory

Let $M_n$ be a (uniformly-chosen) random $n \times n$ matrix with entries in the set $\{-1, 1\}$. For each $n \in \mathbb{N}$, $\beta \in [0, 1]$ and prime $p$, define

$$q_n(\beta) := \max_{w \in \mathbb{Z}_p^n} \mathbb{P}\Big(\exists\, v \in \mathbb{Z}_p^n \setminus \{0\} : M_n \cdot v = w \text{ and } \rho(v) \geq \beta\Big). \tag{1.5}$$

Note that the dependence of $q_n(\beta)$ on the prime $p$ is suppressed in the notation.

The problem of bounding the probability that $\det(M_n) = 0$ can be reduced to the problem of bounding the quantity $q_n(\beta)$. This is a consequence of the following lemma, which was proved by Ferber and Jain [30] using techniques developed by Costello, Tao and Vu [19] and Nguyen [89]. A proof of this lemma is provided in Chapter 2.

**Lemma 1.1.17.** *Let $n \in \mathbb{N}$, and let $p > 2$ be prime. For every $\beta > 0$,*

$$\mathbb{P}\big(\det(M_n) = 0\big) \leq 16n \sum_{m=n-1}^{2n-3} \left(\beta^{1/8} + \frac{q_m(\beta)}{\beta}\right).$$

Lemma 2.2.1 establishes a connection between the inverse Littlewood–Offord problem and the singularity problem of random matrices. In fact, inverse Littlewood–Offord theorems say

[4]Recall that we denote by $M_n$ a (uniformly-chosen) random $n \times n$ matrix with entries in the set $\{-1, 1\}$

that if $\rho(v) \geq \beta$, then $v$ must be 'structured' whenever $\beta$ is 'large'. As we expect the number of 'structured' vectors to not be very large, we might deduce that $q_n(\beta)$ is 'small' by simply applying the union bound. In the use of the unioun bound, we group the structured vectors according to a collection of containers given by our inverse Littlewood–Offord theorem. The structured vectors $v$ whose coordinates belong to the same collection of containers will have approximately the same value of $\rho(v)$. As the number of elements in each container is 'small' as well as the number of containers itself, we are able to prove the following bound on $q_n(\beta)$.

**Lemma 1.1.18** (Campos, M., Morris, Morrison, 2021)**.** *Let $n \in \mathbb{N}$, and let $2 < p \leq \exp\left(2^{-10}\sqrt{n}\right)$ be prime. If $\beta \geq 4/p$, then*

$$q_n(\beta) \leq 2^{-n/4}.$$

Theorem 4.1.1 is easily deduced from Lemmas 2.2.1 and 2.2.2. This deduction and the proofs of these Lemmas can be found in Chapter 2.

## 1.2 Random graphs

The theory of random graphs was introduced by Erdős and Rényi [25] in 1959 during their study of properties of the uniform probability distribution on graphs with exactly $m$ edges. Let $G(n, m)$ denote a uniformly-chosen random graph with $m$ edges and $n$ vertices. In [25], Erdős and Rényi addressed a few questions regarding connectivity properties of $G(n, m)$, such as the probability that $G(n, m)$ is connected and the size of the greatest connected component. Nowadays, the $G(n, m)$ model is also referred as the *Erdős-Rényi graph model*.

A similar random graph model was independently introduced by Gilbert [43] in 1959. Let $G(n, p)$ denote a $n$-vertex random subgraph of the complete graph $K_n$, where each edge of $K_n$ is independently included in $G(n, p)$ with probability $p$. This model is known as the

*binomial random graph model* and it has been vastly studied in the past few years (see, for example, [4, 41, 56]). Observe that there is a natural connection between the $G(n,m)$ model and the $G(n,p)$ model. Under certain conditions, $G(n,p)$ and $G(n,m)$ satisfy some similar properties when $p$ is close to $m/\binom{n}{2}$.

In this thesis, we address some properties of the binomial random graph model. In subsection 1.2.1 we state some of the main properties of $G(n,p)$; in subsection 1.2.2 we state some results on packings of small graphs in $G(n,p)$; in subsection 1.2.3 we address packings of sparse graphs in $G(n,p)$; in Subsection 1.2.4, we state our main result, which concerns packings of large cliques in $G(n,p)$.

### 1.2.1 The threshold phenomena

Let $\mathcal{P}$ be any collection of graphs. We refer to $\mathcal{P}$ as a *graph property* and say that any graph contained in $\mathcal{P}$ *has* the property $\mathcal{P}$. In the binomial random graph model, we are generally interested in how likely is for $G(n,p)$ to have the property $\mathcal{P}$.

**Question 1.2.1.** *For which function $p$ and property $\mathcal{P}$ we have* $\lim_{n\to\infty} \mathbb{P}\big(G(n,p(n)) \in \mathcal{P}\big) = 1$*?*

We are generally interested in collections of graphs containing a given subgraph, connected graphs, hamiltonian graphs, graphs with perfect factors such as perfect matchings, their complementary collections and more. When the property $\mathcal{P}$ is *monotone*, an interesting fenomena occurs: the existence of a *threshold* function. This is the content of a theorem of Bollobás and Thomason [14] from 1987. Before we state their result, let us formally define the concepts of *monotone properties* and *threshold functions*.

**Definition 1.2.2.** *Let $\mathcal{P}$ be a collection of graphs. We say that $\mathcal{P}$ is* monotone *if $G \in \mathcal{P}$ implies $G \cup \{e\} \in \mathcal{P}$ for any edge $e$.*

Some examples of monotone graph properties are those listed before: collections of graphs containing a given subgraph, connected graphs, hamiltonian graphs, etc. We now state the definition of a threshold function for a graph property $\mathcal{P}$.

**Definition 1.2.3.** *We say that a function $p^\star$ is a (coarse) threshold function for a property $\mathcal{P}$ if*

$$\lim_{n\to\infty} \mathbb{P}\big(G(n,p(n)) \in \mathcal{P}\big) = \begin{cases} 0, & \text{if } p \ll p^\star, \\ 1, & \text{if } p \gg p^\star. \end{cases}$$

Observe that if $p^\star$ is a threshold function for $\mathcal{P}$, then $Cp^\star$ is also a threshold function for $\mathcal{P}$ for any constant $C > 0$. Although threshold functions are not unique, one can show that they only differ by a multiplicative constant factor. By an abuse of terminology, we refer to any threshold function of a certain property as *the* threshold function.

We are now ready to state the result of Bollobás and Thomason [14] on thresholds of monotone graph properties.

**Theorem 1.2.4** (Bollobás and Thomason, 1987)**.** *Every non-trivial monotone graph property has a threshold.*

One of the simplest graph properties one could consider is the subgraph containment property. Let $H$ be any fixed graph and let $\mathcal{P}_H$ be the collection of all graphs containing $H$ as a subgraph. Observe that $\mathcal{P}_H$ is a monotone graph property, and hence it has a (coarse) threshold. In 1960, Erdős and Rényi [26] determined the threshold for balanced graphs. Many years later, Bollobás [11] determined the threshold for the property $\mathcal{P}_H$ for any graph $H$. Later, a simpler proof was also given by Ruciński and Vince [103].

For each graph $H$, define

$$m(H) := \max\left\{\frac{e(J)}{v(J)} : K_2 \subseteq J \subseteq H\right\}.$$

Bollobás' theorem can be stated as follows.

**Theorem 1.2.5** (Bollobás, 1981)**.** *Let $H$ be a fixed graph with $e(H) > 0$. We have*

$$\lim_{n\to\infty} \mathbb{P}\big(H \subseteq G(n,p)\big) = \begin{cases} 0, & \text{if } p \ll n^{-1/m(H)}, \\ 1, & \text{if } p \gg n^{-1/m(H)}. \end{cases}$$

A natural question which arises from this theorem (and even from the definition of the threshold itself) is what happens when $p$ has the same order as the threshold function. In 1981, Bollobás [11] and, independently, Karoński and Ruciński [63] addressed this question and determined the asymptotic behaviour of $\mathbb{P}\big(H \subseteq G(n,p)\big)$ when $p \sim cn^{-1/m(H)}$. Before we state their theorem, we need a little notation. For any graph $H$, let $\mathrm{aut}(H)$ be the number of automorphisms of $H$ and denote by $H_B$ the largest subgraph of $H$ for which

$$m(H) = \frac{e(H_B)}{v(H_B)}.$$

**Theorem 1.2.6** (Bollobás, Karoński–Ruciński, 1981)**.** *Let $c > 0$ be a constant and $H$ be a fixed graph. If $np^{m(H)} \to c$, then*

$$\lim_{n\to\infty} \mathbb{P}\big(H \not\subseteq G(n,p)\big) = \exp\left(-\frac{c^{v(H_B)}}{\mathrm{aut}(H_B)}\right).$$

More generally, Bollobás [11] and, independently, Karoński and Ruciński [63] have also determined the asymptotic distribution of the random variable which counts the number copies of $H$ in $G(n,p)$. For more details on the subject, see Ruciński's survey in [101].

There exists another concept of threshold function which takes into account the 'abrupt' nature of the appearance and disappearance of certain graph properties. These functions are called *sharp thresholds* and are defined as follows.

**Definition 1.2.7.** *We say that a function $p^\star$ is a sharp threshold function for a property $\mathcal{P}$ if for every $\varepsilon > 0$ we have*

$$\lim_{n\to\infty} \mathbb{P}\big(G(n,p(n)) \in \mathcal{P}\big) = \begin{cases} 0, & \text{if } p \leq (1-\varepsilon)p^\star, \\ 1, & \text{if } p \geq (1+\varepsilon)p^\star. \end{cases}$$

Observe that Theorem 1.2.6 implies that $\mathcal{P}_H$ does not have a sharp threshold for all graphs $H$. However, there are many important graph properties which are known to have a sharp threshold. Erdős and Rényi [25, 27] showed that the property of being connected and the property of containing a perfect matching both have sharp thresholds. Later, Komlós and Szemerédi [70] also showed that the property of containing a hamiltonian cycle has a sharp threshold. For more discussions on sharp thresholds, see [39].

### 1.2.2 Small subgraphs in random graphs

We say that the graphs $H$ and $H'$ are isomorphic, and we denote $H \cong H$, if there exists bijection $\varphi : V(H) \to V(H')$ such that $uv \in E(H) \iff \varphi(u)\varphi(v) \in E(H')$. For each $n \in \mathbb{N}$, $p \in [0,1]$ and graph $H$, define

$$X_H(n,p) := |\{H' \subseteq G(n,p) : H' \cong H\}|.$$

We omit the parameters $n$ and $p$ whenever they are clear from context. From the proof of Theorem 1.2.5, it is possible to deduce the following result. For more details, see [56].

**Theorem 1.2.8** (Janson, Łuczak and Ruciński, 2000)**.** *Let $H$ be a fixed graph with $e(H) > 0$. If $p \gg n^{-1/m(H)}$, then $X_H = \Theta(\mathbb{E}(X_H))$ with high probability.*

Now that we know the asymptotic order of $X_H$ whenever $p \gg n^{-1/m(H)}$, it is natural to ask how many of these copies are vertex-disjoint and how many are edge-disjoint. For each

graph $H$, let $D^v_H(n,p)$ and $D^e_H(n,p)$ denote the largest number of vertex-disjoint copies of $H$ and edge-disjoint copies of $H$ in $G(n,p)$, respectively. Observe that $D^v_H(n,p)$ is upper-bounded by $\min\{n, D^e_H(n,p)\}$ while $D^e_H(n,p)$ is upper-bounded by $X_J$ for any $K_2 \subseteq J \subseteq H$.

From Theorem 1.2.8, one can derive the following implication. If $p \gg n^{-1/m(H)}$, then $X_J = \Theta(\mathbb{E}(X_J))$ for all $K_2 \subseteq J \subseteq H$ with high probability. Thus, $D^e_H(n,p)$ is upper-bounded by the following quantity (up to a constant factor):

$$\Phi^e_H(n,p) := \min\{\mathbb{E}(X_J) : J \subseteq H, e(J) > 0\}.$$

Similarly, we have $D^v_H(n,p) = O\big(\min\{n, \Phi^e_H\}\big)$ with high probability. In 2000, Janson, Łuczak and Ruciński [56] proved that these are in fact the correct order of magnitude of $D^v_H(n,p)$ and $D^e_H(n,p)$.

**Theorem 1.2.9** (Janson, Łuczak and Ruciński, 2000)**.** *Let $H$ be a fixed graph with $e(H) > 0$. If $p \gg n^{-1/m(H)}$, then*

$$D^e_H(n,p) = \Theta(\Phi^e_H(n,p)) \qquad \textit{and} \qquad D^v_H(n,p) = \Theta\big(\min\{n, \Phi^e_H\}\big)$$

*with high probability.*

When $p$ is constant, a sharp bound on $D^e_H(n,p)$ was obtained by Frankl and Rödl [36] in 1985. As $e(G(n,p))$ is highly concentrated on $p\binom{n}{2}$, we have $D^e_H \le (1+o(1))p\binom{n}{2}/e(H)$ with high probability. By applying the well-known Rödl Nibble technique (see [94]), Frankl and Rödl [36] showed a lower bound on $D^e_H$ which matches the upper bounded.

**Theorem 1.2.10** (Frankl and Rödl, 1985)**.** *Let $p \in (0,1)$ and $H$ be a fixed graph with $e(H) > 0$. We have*

$$D^e_H(n,p) = (1+o(1))\frac{p\binom{n}{2}}{e(H)}$$

*with high probability.*

A related type of question one could ask for $D_H^v(n,p)$ is the following: when does $D_H^v(n,p) = n$ with high probability? This is equivalent to $G(n,p)$ having $n/v(H)$ vertex-disjoint copies of $H$. A set of vertex-disjoint copies of $H$ which covers all the vertices of a graph $G$ is usually referred as an *$H$-factor of $G$*. Clearly, the first requirement $G(n,p)$ must satisfy in order to have an $H$-factor is to have $n$ divisible by $v(H)$. In all the results stated below, we shall assume that this divisibility condition holds.

In the case when $H = K_2$, an $H$-factor is equal to a perfect matching. The problem of finding perfect matchings in $G(n,p)$ was already studied by Erdős and Rényi [27].

**Theorem 1.2.11** (Erdős and Rényi, 1966)**.** *For every $\varepsilon > 0$ we have*

$$\lim_{n\to\infty} \mathbb{P}\big(G(n,p) \text{ has a } K_2\text{-factor}\big) = \begin{cases} 0, & \text{if } p \le (1-\varepsilon)\log n/n, \\ 1, & \text{if } p \ge (1+\varepsilon)\log n/n. \end{cases}$$

Besides the divisibility condition in $n$, another requirement that $G(n,p)$ must satisfy in order to have an $H$-factor is the following: every vertex must be contained in a copy of $H$. The threshold for this event was obtained by Ruciński [102] in 1990. As his result is a bit technical, we only state a simple corollary of it.

For any graph $H$ with at least 2 vertices, define

$$d_1(H) := \frac{e(H)}{v(H)-1}.$$

Let $\mathrm{th}_H(n)$ be the threshold for the event that every vertex is contained in a copy of $H$ in $G(n,p)$. The following theorem is due to Ruciński [102].

**Theorem 1.2.12** (Ruciński, 1990)**.** *For any fixed graph $H$, we have*

$$\mathrm{th}_H(n) = \Omega\big(n^{-1/d_1(H)}(\log n)^{1/e(H)}\big).$$

Let us briefly explain why this bound on $\mathrm{th}_H(n)$ is natural. For any given vertex $v$, let $N_v$ be the random variable which counts the number of copies of $H$ in $G(n,p)$ containing $v$. Observe that the expected value of $N_v$ is of order $n^{v(H)-1}p^{e(H)}$. Using concentration inequalities, one might also expect to have $\mathbb{P}(N_v = 0) \approx \exp(-\Theta(\mathbb{E}(N_v))$. Thus, if $\mathbb{E}(N_v) \leq \log n$, we would expect to have at least one vertex $v$ for which $N_v = 0$. It follows that we expect to have at least one vertex not covered by a copy on $H$ when

$$n^{v(H)-1}p^{e(H)} \leq \log n.$$

Let $\mathrm{thf}_H(n)$ be the threshold for the event that $G(n,p)$ contains an $H$-factor. As $\mathrm{thf}_H(n) \geq \mathrm{th}_H(n)$, it follows from Theorem 1.2.12 that

$$\mathrm{thf}_H(n) = \Omega\big(n^{-1/d_1(H)}(\log n)^{1/e(H)}\big). \tag{1.6}$$

In 2008, a major breakthrough was made by Johansson, Kahn and Vu [59], who showed that the upper bound in (1.6) represents the correct order of magnitude of $\mathrm{thf}_H(n)$ whenever $H$ is *strictly balanced*. We say that a graph $H$ is strictly $d_1$-balanced if for every subgraph $J \subsetneq H$ we have

$$d_1(H) < \frac{e(J)}{v(J)-1}.$$

**Theorem 1.2.13** (Johansson, Kahn and Vu, 2008)**.** *Let $H$ be a strictly balanced graph. We have*

$$\mathrm{thf}_H(n) = \Theta\big(n^{-1/d_1(H)}(\log n)^{1/e(H)}\big).$$

When $H$ is not strictly balanced, Johansson, Kanh and Vu [59] also obtained sharp bounds on $\mathrm{thf}_H(n)$ up to a factor of $n^{o(1)}$. The exact order of $\mathrm{thf}_H(n)$ is still not known, and it is conjectured to depend on other parameters rather than $d(H)$ and $e(H)$. For more details see [59].

### 1.2.3 Packing large sparse subgraphs in random graphs

For each graph $H$ and each $p \in (0,1)$, we have already seen that $G(n,p)$ has

$$(1+o(1))\frac{p\binom{n}{2}}{e(H)}.$$

edge-disjoint copies of $H$ (see [36]). A natural extension of this problem is the following:

**Question 1.2.14.** *Let $p \in (0,1)$ be a constant. Given a sequence of graphs $(H_n)_{n\in\mathbb{N}}$, when do we have*

$$(1+o(1))\frac{p\binom{n}{2}}{e(H_n)}$$

*edge disjoint copies of $H_n$ in $G(n,p)$? More generally, given a sequence of graphs $H_1,\dots,H_s$, when can we find edge-disjoint copies of $H_1,\dots,H_s$ in $G(n,p)$?*

Since the work of Frankl and Rödl [36], packing problems of large graphs have been extensively studied in the past few years. In 2004, Frieze and Krivelevich [42] studied packings of hamiltonian cycles in quasirandom graphs. As a corollary, they obtained the following result for random graphs.

**Theorem 1.2.15** (Frieze and Krivelevich, 2005)**.** *Let $p \in (0,1)$ be a constant. With high probability, we have at least*

$$\frac{np}{2} - O(n^{5/6}(\log n)^{1/6})$$

*edge-disjoint copies of a hamiltonian cycle in $G(n,p)$.*

A few years later, a more general decomposition theorem was obtained by Kim, Kühn, Osthus and Tyomkyn [66] in the context of graphs with bounded degree.

**Theorem 1.2.16** (Kim, Kühn, Osthus and Tyomkyn, 2019)**.** *Let $\Delta \in \mathbb{N}$ and $p, \alpha \in (0,1)$ be fixed constants. Let $H_1, \dots, H_s$ be graphs on $n$ vertices with maximum degree at most $\Delta$ and such that*

$$\sum_{i=1}^{s} e(H_i) \leq (1-\alpha)p\binom{n}{2}.$$

*With high probability, there exists edge-disjoint copies of $H_1, \dots, H_s$ in $G(n,p)$.*

We remark that Theorem was stated in a more general form, where a similar statement holds for quasirandom graphs instead of random graphs.

In 2018, Ferber and Samotij [33] addressed the problem of packing large tree in $G(n,p)$. In contrast with [66], the trees are allowed to have maximum degree depending on $n$ and $p$ can be as small as $(\log n)^{36}/n$.

**Theorem 1.2.17** (Ferber and Samotij, 2018)**.** *Let $p \geq (\log n)^{36}/n$ and $N \leq (1-\varepsilon)np/2$, for some constant $\varepsilon > 0$. Let $T_1, \dots, T_N$ be trees on $n$ vertices with maximum degree at most $(np)^{1/6}/(\log n)^6$. With high probability, there exist edge-disjoint copies of $T_1, \dots, T_N$ in $G(n,p)$.*

Very recently, Keevash and Staden [65] obtained a sharp result for tree packings in quasirandom graphs. As a corollary, they established Ringel's conjecture[5] for all large $n$, which was independently obtained by Montgomery, Pokrovskiy and Sudakov [85] using different methods.

**Theorem 1.2.18** (Keevash and Staden, 2021+)**.** *For all $p \in (0,1]$ there exists $n_0 = n_0(p)$ such that the following holds for all $n \geq n_0$. Let $T_n$ be a tree of size $p(n-1)/2 \in \mathbb{N}$. With high probability, there exists a set of edge-disjoint copies of $T_n$ in $G(n,p)$ which covers all the edges of $G(n,p)$.*

[5]Ringel's conjecture states that for any tree $T$ with $n$ edges, the complete graph $K_{2n+1}$ can be decomposed into $2n+1$ disjoint copies of $T$.

Observe that all the results listed above concern packings of large sparse subgraphs in random graphs. For large dense graphs, not much is known apart from cliques. We shall address the packing clique problem in the next subsection.

### 1.2.4 Packings of large cliques in random graphs

Let $p \in (0,1)$ be a constant. One of the most basic questions concerning the binomial random graph model is the following.

**Question 1.2.19.** *What is the size of the largest clique in $G(n,p)$?*

Let $k_0 = k_0(n,p)$ be the minimum $k$ such that

$$\binom{n}{k} p^{\binom{k}{2}} < 1.$$

In the 1970s, Matula [82, 83] and independently Bollobás and Erdős [13] showed that the largest clique in $G(n,p)$ has either $k_0$ of $k_0 - 1$ vertices with high probability. Using Stirling expansions as in [13], we obtain that $k_0$ is of the form $\lceil \eta_0 + o(1) \rceil$, where

$$\eta_0 := 2\log_{1/p} n - 2\log_{1/p}\log_{1/p} n + 2\log_{1/p} e + 1.$$

In 1988, motivated by the study of the chromatic number of random graphs, Bollobás [12] used a random set of cliques to show the following result.

**Theorem 1.2.20** (Bollobás, 1988)**.** *There are $\Omega(n^2/k^4)$ edge-disjoint $k$-cliques in $G(n,1/2)$ with high probability, for $k = k_0(n) - 4$.*

Let us denote by $\nu_p(k)$ the maximum number of edge-disjoint copies of $k$-cliques in $G(n,p)$. Clearly, we have $\nu_p(k) \leq n^2/k^2$ for all values of $k$. For $k = k_0 - 4$, which is the same value of $k$ stated in Theorem 1.2.20, a 1992 conjecture of Alon and Spencer [4] states that the trivial upper bound should be the truth.

**Conjecture 1.2.21** (Alon and Spencer, 1992)**.** *We have* $\mathbb{E}(\nu_{1/2}(k)) = \Theta(n^2/k^2)$ *for* $k = k_0(n) - 4$.

At first, this conjecture sounds plausible because, with high probability, each edge must lie in many $k$-cliques. However, this conjecture turns out to be false: it was disproved by Acan and Kahn [3].

**Theorem 1.2.22** (Acan and Kahn, 2019)**.** *Let* $p \in (0,1)$ *and* $C > 0$ *be constants. For* $k = k_0(n) - C$ *we have*

$$\nu_p(k) = O\left(\frac{n^2}{k^3}\right)$$

*with high probability.*

In the same paper, they also obtained a lower bound on the expectation of $\mathbb{E}(\nu_p(k))$ for the same values of $k$ using a result of Ajtai, Komlós and Szemerédi [1, 2]. More precisely, they showed the following result.

**Theorem 1.2.23** (Acan and Kahn, 2019)**.** *Let* $p \in (0,1)$ *and* $C > 0$ *be constants. For* $k = k_0(n) - C$ *we have*

$$\mathbb{E}(\nu_p(k)) = \Omega\left(\frac{n^2 \log k}{k^4}\right).$$

In a joint work with Griffiths and Morris [46], we obtained a lower bound on $\nu_p(k)$ of the same order of magnitude as the upper bound on $\nu_p(k)$ obtained by Acan and Kahn [3].

**Theorem 1.2.24** (Griffiths, M. and Morris, 2021+)**.** *Let* $p \in (0,1)$ *and* $C \geq 4$ *be constants and* $k = k_0(n) - C$*. With high probability, we have*

$$\nu_p(k) \geq \frac{pn^2}{40k^3}.$$

We may even prove a similar result with $k = k_0(n) - 3$. However, in this case the constant is not universal. When thinking of near-maximal cliques, an important role is played by the real number $\gamma$ such that the expected number of $k$-cliques is of the form $n^{\gamma+o(1)}$.

We formally define the function $\gamma = \gamma(n,k)$ as $\gamma = \gamma(n,k) = \eta_0 - k$, where

$$\eta_0 := 2\log_{1/p} n - 2\log_{1/p}\log_{1/p} n + 2\log_{1/p} e + 1.$$

Recall that $k_0$ is of the form $\lceil \eta_0 + o(1) \rceil$. One can easily verify that the expected number of $k$-cliques is $n^{\gamma+o(1)}$. Moreover, note that if $k = k_0 - C$ for some constant $C > 0$, then $C = \lceil \gamma \rceil$. Thus, to prove a result which includes the case $k = k_0 - 3$ we must prove a result for $\gamma > 2$. This is done in our next theorem, whose statement also includes Theorem 1.2.24.

**Theorem 1.2.25** (Griffiths, M. and Morris, 2021+)**.** *Let $\gamma > 2$ and $p \in (0,1)$ be constants and let $k = \eta_0 - \gamma$. With high probability, we have*

$$\nu_p(k) \geq \frac{\min\{\gamma - 2, 1\}}{40} \cdot \frac{pn^2 \log n}{k^4}.$$

We remark that the dependence on $\gamma$ is correct, as the approach of Acan and Kahn [3] applied for $\gamma \in (2,3)$ and $k = \eta_0 - \gamma$ gives an upper bound of the form $O((\gamma-2)n^2 \log n/k^4)$. For $\gamma < 2$, $\nu_p(k)$ should have the same order as the expectation, as we have only a few pairs of $k$-cliques which intersect each other.

To prove this result, we analyse random process which starts with $G_0 \sim G(n,p)$ and at each step removes a $k$-clique uniformly at random. Let $G_m$ denote the graph obtained after $m$ such $k$-cliques have been removed and let $Q(G_m)$ denote the number of $k$-cliques in $G_m$. The average number of $k$-cliques per edge in $G_m$ is roughly $\frac{k^2 Q(G_m)}{pn^2}$, and hence we expect to destroy roughly

$$\frac{k^4 Q(G_m)}{pn^2}$$

$k$-cliques after removing the $m$-th clique in the random process. It follows that the number of $k$-cliques in $G_m$ should be close to

$$\left(1 - \frac{k^4}{pn^2}\right)^m Q(G_0).$$

If the expected number of $k$-cliques is $n^{\gamma+o(1)}$, then we expect the process to last at least

$$(\gamma - 2)\frac{pn^2 \log n}{k^4}.$$

We conjecture that this gives the correct order of magnitude of $\nu_p(k)$ as long as this quantity is smaller than $n^2p/k^2$.

**Conjecture 1.2.26** (Griffiths, M. and Morris)**.** *Let $p \in (0,1)$ and $k \leq k_0 - 4$. Let $\gamma = \gamma(n,k)$ be such that the expected number of $k$-cliques in $G(n,p)$ is $n^{\gamma+o(1)}$. With high probability, we have*

$$\nu_p(k) = \Theta\left(\min\left\{\frac{pn^2}{k^2}, \frac{\gamma pn^2 \log n}{k^4}\right\}\right).$$

## 1.3 Ramsey theory

Ramsey Theory is a branch of combinatorics which studies the existence of monochromatic structures in coloured objects. We say that a graph $G$ is a *Ramsey graph for the pair of graphs* $(F,H)$ if, in every edge colouring $c : E(G) \to \{\text{red, blue}\}$, we can find either a red coloured copy of $F$ or a blue coloured copy of $H$. We write $G \to (F,H)$ if $G$ is Ramsey for $(F,H)$, and $G \not\to (F,H)$ otherwise.

### 1.3.1 Classical Ramsey theory

Motivated by the study of a regular procedure to determine the truth or falsity of any given logical formula, Ramsey [93] proved the following theorem which is considered the starting point of Ramsey Theory.

**Theorem 1.3.1** (Ramsey, 1930)**.** *For any $s, t \in \mathbb{N}$, let $R(s,t)$ be the minimum $n$ such that any red and blue edge-colouring of $K_n$ contains a red copy of $K_s$ or a blue copy of $K_t$. For all $s, t \in \mathbb{N}$, we have $R(s,t) < +\infty$.*

Motivated by a problem in combinatorial geometry concerning the existence of $n$ points forming a convex polygon in any set of $N = N(n)$ points in general position, Erdős and Szekeres [28] gave an explicit upper bound for $R(s,t)$. The main step to show their bound is to note that if $n \geq R(s,t+1) + R(s+1,t)$, then every vertex of $K_n$ has either $R(s,t+1)$ red neighbours or $R(s+1,t)$ blue neighbours.

**Theorem 1.3.2** (Erdős and Szekeres, 1935)**.** *For all $s, t \in \mathbb{N}$, we have*

$$R(s+1,t+1) \leq \binom{s+t}{t}.$$

In the past few years, some improvements on the upper bound of $R(s,t)$ were obtained by Graham and Rödl [44], Thomason [117], Conlon [18] and Sah [106]. For the *diagonal case*, that is, when $s = t$, the best upper bound is due to Sah [106], which developed tools for effective quasirandomness to prove the following result.

**Theorem 1.3.3** (Sah, 2021+)**.** *There exists an absolute constant $c > 0$ such that for all $t \geq 3$,*

$$R(t+1) \leq t^{-c \log t} \binom{2t}{t}.$$

The first lower bound for $R(t)$ was obtained by Erdős [22] in 1947 using the probabilistic method. In 1977, Spencer [109] used the Lovász Local Lemma to improve Erdős' bound by a factor of 2, which is the best lower bound until today.

**Theorem 1.3.4** (Spencer, 1977)**.** *We have*

$$R(t) \geq \left( \frac{\sqrt{2}}{e} + o(1) \right) t 2^{t/2}$$

*as* $t \to +\infty$.

Observe that there is a large difference between the upper bound and the lower bound of $R(t)$. As $t$ increases, we have

$$\sqrt{2} + o(1) \leq R(t)^{1/t} \leq 4 + o(1).$$

The major open problem in Ramsey theory is to show that the limit $R(t)^{1/t}$ exists.

**Conjecture 1.3.5.** *The limit* $\lim_{t \to +\infty} R(t)^{1/t}$ *exists.*

### 1.3.2 Sparse Ramsey theory

The definition of $R(t,t)$ can also be rephrased as follows. The Ramsey number $R(t,t)$ is equal to the minimum number of vertices in a graph $G$ for which $G \to K_t$. In 1967, Erdős and Hajnal [23] raised the following question, which can be seen as an analogue version of the classical Ramsey question for graphs which are sparser than the complete graph.

**Question 1.3.6.** *For any* $t \geq 3$*, does there exist a graph* $G$ *which is* $K_{t+1}$*-free but* $G \to (K_t, K_t)$*?*

In 1970, Folkman [34] answered this question affirmatively through explicit constructions for every $t \geq 3$. A few years later, Nešetřil and Rödl [87] also gave different explicit

constructions for such graphs. We say that a graph $G$ is $t$-Folkman if $G$ is $K_{t+1}$ free and $G \to (K_t, K_t)$. Similarly as in the classical Ramsey theory, the Folkman number $f(t)$ is defined as

$$f(t) := \min\{n \in \mathbb{N} : \exists\, G\, t\text{-Folkman with } v(G) = n\}.$$

In 1986, Frankl and Rödl [37] analysed Ramsey properties of sparse random graphs to show that

$$f(3) \leq 7 \cdot 10^{11}.$$

One year later, refining the method of Frankl and Rödl [37], Spencer [110] showed that $f(3) \leq 3 \cdot 10^8$. These results established a bridge between random graphs and Ramsey properties. We discuss more about this connection in the next subsection.

Let us briefly mention what it is known about the asymptotic behaviour of $f(t)$. As $f(t) \geq R(t)$, we have that the lower bound on $f(t)$ is at least exponential in $t$. On the other hand, the first upper bounds obtained for $f(t)$ were far from exponential. The upper bounds on $f(t)$ obtained by Folkman [34] and Nešetřil and Rödl [87] were an exponential tower of height polynomial in $t$. In 2017, Rödl, Ruciński and Schacht [98] improved this result considerably by showing that $f(t)$ is an exponential in a polynomial function in $t$. Their proof is build upon the so called hypergraph container method, developed independently by Balogh, Morris and Samotij [6], and Saxton and Thomason [108]. In 2020, using an efficient version of the hypergraph container theorem, Balogh and Samotij [8] proved the best known upper bound on Folkman numbers.

**Theorem 1.3.7.** *There exists an absolute constant $c > 0$ such that for all $t \geq 3$,*

$$f(t) \leq 2^{ct^3}.$$

### 1.3.3 Symmetric Ramsey theory in random graphs

For any $n \in \mathbb{N}$ and any function $p : \mathbb{N} \to [0,1]$, let $G(n,p)$ be the random graph on $[n]$ where each edge $\{i,j\} \in \binom{[n]}{2}$ is included in $G(n,p)$ with probability $p$. The study of Ramsey properties of random graphs was initiated by Frankl and Rödl [37]. In 1986, they showed that $G(n,p(n)) \to (K_3,K_3)$ with high probability, as long as $p(n) \geq n^{-1/2+\varepsilon}$ for some $\varepsilon > 0$. This result was used by them to give an upper bound on the Folkman number $f(3)$.

Let $F$ be any graph. Having the result of Frankl and Rödl [37] in mind, it is natural to ask the following question. When does $G(n,p) \to (F,F)$? In 1987, Bollobás and Thomason [14] proved that every *increasing graph property* has a *threshold*. Now, the question of weather $G(n,p) \to (F,F)$ can be rephrased as follows.

**Question 1.3.8.** *What is a threshold function for $G(n,p) \to (F,F)$?*

In 1992, Łuczak, Ruciński and Voigt [79] showed that the probability threshold for having $G(n,p) \to (K_3,K_3)$ is of order $n^{-1/2}$. In 1995, Rödl and Ruciński [95, 97] determined the probability threshold for $G(n,p) \to (F,F)$ for almost all non-empty graphs $F$. Before showing their result, we need the following definition.

**Definition 1.3.9.** *For any graph $F$ with at least 3 vertices, define the $m_2$-density of $F$ to be*

$$m_2(F) := \max\left\{\frac{e(J)-1}{v(J)-2} : J \subseteq F, v(J) \geq 3\right\}.$$

With this definition in hand, we can state the result of Rödl and Ruciński as follows.

**Theorem 1.3.10.** *Let $F$ be a non-empty graph with at least 3 vertices where at least one of its components is neither a star nor a path of length 3. Then, there exist $C, c > 0$ such that*

$$\lim_{n\to\infty} \mathbb{P}\big(G(n,p) \to (F,F)\big) = \begin{cases} 0, & \text{if } p \leq cn^{-1/m_2(F)} \\ 1, & \text{if } p \geq Cn^{-1/m_2(F)}. \end{cases}$$

In order to have a threshold of order $n^{-1/m_2(F)}$ for the event $G(n,p) \to (F,F)$, one can check that the assumptions of Theorem 1.3.10 are indeed necessary. For more details, see [86]. The remaining cases were addressed subsequently by Friedgut and Krivelevich [40].

Now let us briefly explain the intuition of why $n^{-1/m_2(F)}$ should be the right threshold for the property $G(n,p) \to (F,F)$ for most graphs $F$. For each edge $e \in G(n,p)$, let $X_e$ denote the number of copies of $F$ containing $e$. In order to have $G(n,p) \to (F,F)$, we would need the expected value of $X_e$ to be at least a constant. As $\mathbb{E}(X_e) = \Theta(n^{v(F)-2}p^{e(F)-1})$, we would have $G(n,p) \to (F,F)$ if

$$n^{v(F)-2}p^{e(F)-1} = \Omega(1),$$

which gives the bound $p = \Omega\big(n^{-\frac{v(F)-2}{e(F)-1}}\big)$. This already gives us some intuition in the case where $F$ is $m_2$-*balanced*, that is, when

$$m_2(F) = \frac{e(F)-1}{v(F)-2}.$$

In general, if $G(n,p) \to (F,F)$ then we expect to have 'many' copies of $F$ in $G(n,p)$. That is, it is reasonable to expect that if $G(n,p)$ is a Ramsey graph for $F$ then $\Omega(n^2p)$ edges are covered by some copy of $F$. This implies that the number of copies of $F$ in $G(n,p)$ must be at least $\Omega(n^2p)$. In particular, the number of copies of any subgraph of $F$ should also be at least $\Omega(n^2p)$. Therefore,

$$n^{v(H)}p^{e(H)} = \Omega(n^2p), \text{ for every } H \subseteq F,$$

which gives the bound $p = \Omega(n^{-1/m_2(F)})$.

### 1.3.4 Asymmetric Ramsey theory in random graphs

A natural generalisation of the symmetric Ramsey problem in random graphs is to determine a threshold function $p(F,H)$ for the property $G(n,p) \to (F,H)$ for any asymmetric pair of graphs $(F,H)$.

**Question 1.3.11.** *What is a threshold function for $G(n,p) \to (F,H)$?*

This problem was posed in 1997 by Kohayakawa and Kreuter [67], who found the threshold function for any pair of cycles $(C_\ell, C_k)$ with $k \geq \ell \geq 3$.

**Theorem 1.3.12** (Kohayakawa and Kreuter, 1997)**.** *For any pair of cycles $(C_\ell, C_k)$ with $k \geq \ell \geq 3$, we have*

$$p(C_k, C_\ell) = \Theta(n^{1-\frac{\ell}{(\ell-1)k}}).$$

In the same paper, they conjectured what should be the correct threshold for the general case. Before stating their conjecture, we need a generalisation of the $m_2$-density for pairs of graphs.

**Definition 1.3.13.** *For any pair of graphs such that $m_2(F) \geq m_2(H) \geq 1$, define the $m_2$-density of the pair $(F,H)$ to be*

$$m_2(F,H) := \max\left\{\frac{e(J)}{v(J)-2+1/m_2(H)} : J \subseteq F, e(J) \geq 1\right\}.$$

Now the Kohayakawa–Kreuter conjecture can be stated as follows.

**Conjecture 1.3.14** (Kohayakawa–Kreuter)**.** *Let $F$ and $H$ be any graphs such that $m_2(F) \geq m_2(H) > 1$. Then, there exist $C, c > 0$ such that*

$$\lim_{n\to\infty} \mathbb{P}\big(G(n,p) \to (F,H)\big) = \begin{cases} 0, & \text{if } p \leq cn^{-1/m_2(F,H)} \\ 1, & \text{if } p \geq Cn^{-1/m_2(F,H)}. \end{cases}$$

The assertion of Conjecture 1.3.14 for $p = O(n^{-1/m_2(F,H)})$ is usually refered as the *0-statement* while the assertion for $p = \Omega(Cn^{-1/m_2(F,H)})$ is usually refered as the *1-statement*.

Now let us briefly explain the intuition of why $n^{-1/m_2(F,H)}$ should be the right threshold for the property $G(n,p) \to (F,H)$ for any pair of graphs $(F,H)$ such that $m_2(F) \geq m_2(H) > 1$. Let $c : E(G(n,p)) \to \{\text{red, blue}\}$ be a colouring of $G(n,p)$ with no red copy of $F$. That is, every copy of $F$ in $G(n,p)$ must have a blue edge under $c$. Let

$$m(F) := \max\left\{\frac{e(J)}{v(J)} : J \subseteq F\right\}$$

be the $m$-density of $F$. If $n^{-1/m(F)} \leq p \leq n^{-1/m_2(F)}$, then we expect a constant proportion of the copies of $F$ to be roughly disjoint. One can check that $p = n^{-1/m_2(F,H)}$ is in fact between these bounds. As the copies of $F$ are randomly distributed in $G(n,p)$ and roughly edge-disjoint, we expect that edges contained in some copy of $F$ are roughly distributed as in $G(n,q)$, where $q = \Theta(n^{v(F)-2}p^{e(F)})$. In particular, the blue edges contained in the copies of $F$ under $c$ are also distributed as in $G(n,q)$. By Theorem 1.3.10, we would have a blue copy of $H$ only if $q \geq n^{-1/m_2(H)}$. It follows that if $G(n,p) \to (F,H)$, then $n^{v(F)-2}p^{e(F)} = \Omega(n^{-1/m_2(H)})$. This implies that $p = \Omega(n^{-1/m_F})$, where $m_F$ is given by

$$m_F = \frac{e(F)}{v(F) - 2 + 1/m_2(H)}.$$

One can check that the same reasoning naturally applies to subgraphs $J \subseteq F$ in place of $F$, and hence we obtain $m_2(F,H)$ instead of $m_F$. This explains why the Kohayakawa–Kreuter conjecture should hold.

Since the Kohayakawa–Kreuter conjecture was posed, there have been many attempts to solve it. The first result towards the 1-statement was obtained by Kohayakawa, Schacht and Spöhel [68] in 2012.

They showed that the 1-statement holds under some density balancedness conditions on the graphs. In the same year, Gugelmann, Nenadov, Person, Skoric, Steger and Thomas [47]

showed the 1-statement for any pair of graphs $(F, H)$ but under the stronger assumption $p \geq n^{-1/m_2(F,H)} \log n$. In a recent breakthrough, Mousset, Nenadov and Samotij [86] proved the 1-statement whenever $m_2(F) \geq m_2(H) \geq 1$.

**Theorem 1.3.15** (Mousset, Nenadov and Samotij, 2020)**.** *Let $F$ and $H$ be any graphs such that $m_2(F) \geq m_2(H) \geq 1$. There exist $C > 0$ such that, if $p \geq Cn^{-1/m_2(F,H)}$, then*

$$\lim_{n\to\infty} \mathbb{P}\big(G(n,p) \to (F,H)\big) = 1.$$

In contrast, much less is known about the 0-*statement*, that is, the statement that $p(F,H) = \Omega(n^{-1/m_2(F,H)})$ whenever $m_2(F) \geq m_2(H) \geq 1$. As far as we know, the 0-statement is only proved for two types of pairs of graphs. In 1997 Kohayakawa and Kreuter [67] established the 0-statement for all pairs of cycles while only in 2009 Marciniszyn, Skokan, Spöhel and Steger [81] addressed all pairs of cliques.

**Theorem 1.3.16** (Marciniszyn, Skokan, Spöhel and Steger, 2009)**.** *For any pair of cliques $(K_s, K_t)$ with $t \geq s \geq 3$, we have*

$$\lim_{n\to\infty} \mathbb{P}\big(G(n,p) \to (K_s,K_t)\big) = \begin{cases} 0, & \text{if } p \leq cn^{-1/m_2(K_s,K_t)} \\ 1, & \text{if } p \geq Cn^{-1/m_2(K_s,K_t)}. \end{cases}$$

In Chapter 3, which is joint work with Liebenau, Mendonça and Skokan [72], we show the 0-statement of the Kohayakawa-Kreuter conjecture for any pairs of cliques and cycles. This is the unique 0-statement result for different types of graphs.

**Theorem 1.3.17** (Liebenau, M., Mendonça and Skokan, 2021+)**.** *For all $\ell, r \geq 4$ there exists $c > 0$ such that, if $p = p(n) \leq cn^{-1/m_2(K_r,C_\ell)}$, then*

$$\lim_{n\to\infty} \mathbb{P}\big(G(n,p) \to (K_r,C_\ell)\big) = 0.$$

Combining Theorem 1.3.17 with the results of [67], [81] and [86], we establish the Kohayakawa–Kreuter conjecture for any pair of cycles and cliques with at least 3 vertices. The main tool behind the proof of Theorem 1.3.17 is a structural characterisation of Ramsey graphs for the pair $(K_r, C_\ell)$ via a 'container type' argument, which is a rephrasing of an idea used in previous works. Roughly speaking, we find a family $\mathcal{I}$ of graphs with the following properties: (a) $|\mathcal{I}|$ is small; (b) for every graph $G$ with $G \to (K_r, C_\ell)$ there exists $I \in \mathcal{I}$ such that $I \subseteq G$; and (c) for each $I \in \mathcal{I}$, either $I$ is small and dense or very structured. We provide the details in Chapter 3.

For any graph $G$, set

$$d(G) = \frac{e(G)}{v(G)}.$$

Our structural characterisation of Ramsey graphs passes through a slightly more technical version of the following lemma.

**Lemma 1.3.18** (Liebenau, M., Mendonça and Skokan, 2021+)**.** *Let $r, \ell \geq 4$ be integers. There exists $\varepsilon = \varepsilon(r, \ell) > 0$ such that the following holds. If $G \to (K_r, C_\ell)$, then*

$$d(G) \geq m_2(K_r, C_\ell) + \varepsilon.$$

This is one of the difficulties in dealing with the 0-statement for other pairs of graphs. In order to prove the 0-statement, we believe that we would need a version of Lemma 1.3.18 for all pairs of graphs.

**Conjecture 1.3.19.** *For every pair of graphs $(F, H)$, there exists $\varepsilon = \varepsilon(F, H)$ such that the following holds. If $G \to (F, H)$, then*

$$d(G) \geq m_2(F, H) + \varepsilon.$$

This conjecture was proved in 1995 by Rödl and Ruciński [95, 97] for symmetric pairs of graphs. Not much is known apart from pairs of graphs which are combinations of cycles and cliques. It is worth noting that the Kohayakawa–Kreuter conjecture implies $d(G) > m_2(F, H)$ for any graph $G$ such that $G \to (F, H)$. Otherwise, the presence of $G$ in $G(n, p)$ will not be unlikely for $p = \Omega(n^{-1/m_2(F,H)})$.

## 1.4 Organisation of the thesis

The rest of this thesis is organised as follows:

- In Chapter 2, which is joint work with Campos, Morris and Morrison, we prove Theorem 1.1.8, which bounds the probability that a symmetric random matrix is singular, and we prove Theorem 1.1.16, which is an inverse Littlewood–Offord theorem in $\mathbb{Z}_p$.
- In Chapter 3, which is joint work with Griffiths and Morris, we prove Theorems 1.2.24 and 1.2.25, which determines a lower bound for the $k$-clique packing number in $G(n, p)$ when $k$ is close to the maximum clique size.
- In Chapter 4, which is joint with Liebenau, Mendonça and Skokan, we prove Theorem 1.3.17, which establishes the 0-statement for the property $G(n, p) \to (K_r, C_\ell)$ for all pair of cliques and cycles. This is a particular case of the Kohayakawa–Kreuter conjecture.

CHAPTER 2

# SINGULARITY OF SYMMETRIC RANDOM MATRICES

The work in this chapter is joint with Campos, Morris and Morrison. It is adapted from the article [17] which will appear in *Duke Mathematical Journal*.

## 2.1 Introduction

Let $M_n$ denote a (uniformly-chosen) symmetric random $n \times n$ matrix with entries in the set $\{-1, 1\}$. An old and notorious conjecture (see, for example, the discussion in [62]) states that the probability that $\det(M_n) = 0$ is asymptotically equal to the probability that two of the rows or columns of $M_n$ are equal (up to a factor of $\pm 1$), and hence is of order $n^2 2^{-n}$.

In this chapter we use a combinatorial approach (inspired by the method of [31, 30]) to obtain the following bound on the probability that $M_n$ is singular.

**Theorem 2.1.1.** *There exists $c > 0$ such that*

$$\mathbb{P}\big(\det(M_n) = 0\big) \leq \exp\big(-c\sqrt{n}\big) \tag{2.1}$$

*for all sufficiently large $n \in \mathbb{N}$.*

The main new ingredient in our approach is an inverse Littlewood–Offord theorem (see Theorem 2.1.2, below) which applies to vectors $v \in \mathbb{Z}_p^n$ that exhibit a very mild amount of 'structure'.

For any integers $n, p \in \mathbb{N}$ and vector $v \in \mathbb{Z}_p^n$, define

$$\rho(v) := \max_{a \in G} \mathbb{P}\bigg(\sum_{i=1}^{n} u_i v_i = a\bigg),$$

where $u$ is a uniformly-chosen random element of $\{-1, 1\}^n$. For each subset $Y \subset [n]$, let us write $v_Y$ for the restriction of $v$ to the coordinates of $Y$. Our inverse Littlewood–Offord theorem is as follows.

**Theorem 2.1.2.** *Let $p$ be a prime. There exists a family $\mathcal{C}$ of subsets of $\mathbb{Z}_p$, with*

$$|\mathcal{C}| \leq \exp\Big(2^{12}\big(\log p\big)^2\Big), \tag{2.2}$$

*such that for each $n \in \mathbb{N}$, and every $v \in \mathbb{Z}_p^n$ with $\rho(v) \geq 4/p$ and $|v| \geq 2^{18}\log p$, there exist sets $B(v) \in \mathcal{C}$ and $Y = Y(v) \subset [n]$, with $n/4 \leq |Y| \leq n/2$, such that*

$$\big|\big\{i \in [n] : v_i \notin B(v)\big\}\big| \leq \frac{n}{4} \qquad \text{and} \qquad |B(v)| \leq \frac{2^{16}}{\rho(v_Y)\sqrt{|v|}}. \tag{2.3}$$

One might be able to prove a stronger version of Theorem 2.1.2, in which most 'containers' (members of the family $\mathcal{C}$) are significantly smaller than the maximum given in (2.3). However, without significant additional ideas such a strengthening would *not* imply a significant improvement over the bound in Theorem 4.1.1, see the discussion in Section 2.2.2 for more details.

We remark that the sets $Y(v)$, whose appearance in Theorem 2.1.2 might appear somewhat unnatural at first sight, will play a vital role in our application of the theorem to prove Theorem 4.1.1. More precisely, we will use the sets $Y(v)$ to maintain independence as we reveal various rows and columns of the matrix, see Section 2.2.1 for more details. Let us also mention here that the family of containers $\mathcal{C}$ will be defined explicitly (see (3.22), below), but we will only need the properties stated in the theorem. The proof of Theorem 2.1.2 uses the probabilistic method (for those readers familiar with the container method, we choose the 'fingerprint' randomly), and a classical 'anticoncentration lemma' proved by Halász [48] (Lemma 2.2.3, below), see Section 2.2.3 for more details.

The rest of the chapter is organised as follows: in Section 2.2 we give an overview of the proof, in Section 2.3 we prove Theorem 2.1.2, in Section 2.4 we deduce Theorem 4.1.1, in Sections 2.5 and 2.6 we provide (for completeness) proofs of a 'reduction lemma' of Ferber and Jain [30] (whose proof was based on the method of [19, 89]) and of Halász's lemma.

## 2.2 An overview of the proof

In this section we will outline the proof of our inverse Littlewood–Offord theorem, and the deduction of Theorem 4.1.1. The first step is to apply the method of [19, 30, 89] to reduce the problem to bounding the quantity

$$q_n(\beta) := \max_{w \in \mathbb{Z}_p^n} \mathbb{P}\Big(\exists\, v \in \mathbb{Z}_p^n \setminus \{0\} : M_n \cdot v = w \text{ and } \rho(v) \geq \beta\Big), \tag{2.4}$$

for some suitable $\beta = \exp\big(-\Theta(\sqrt{n})\big)$ and a prime $p = \Theta\big(1/\beta\big)$. To be precise, we will use the following lemma, which was proved by Ferber and Jain [30] using techniques developed by Costello, Tao and Vu [19] and Nguyen [89]. Note that the dependence of $q_n(\beta)$ on the prime $p$ is suppressed in the notation.

**Lemma 2.2.1.** *Let $n \in \mathbb{N}$, and let $p > 2$ be prime. For every $\beta > 0$,*

$$\mathbb{P}\big(\det(M_n) = 0\big) \leq 16n \sum_{m=n-1}^{2n-3} \left(\beta^{1/8} + \frac{q_m(\beta)}{\beta}\right).$$

Since Lemma 2.2.1 was not stated explicitly in [30], for the reader's convenience we provide a proof in Appendix 2.5 (see also [17, Appendix A] for an extended version). Using our inverse Littlewood–Offord theorem (Theorem 2.1.2), we will prove the following bound on $q_n(\beta)$.

**Lemma 2.2.2.** *Let $n \in \mathbb{N}$ be sufficiently large, and let $p \leq \exp\big(2^{-10}\sqrt{n}\big)$ be prime. Then*

$$q_n(\beta) \leq 2^{-n/4}$$

*for every $\beta \geq 4/p$.*

Theorem 4.1.1 is easily deduced from Lemmas 2.2.1 and 2.2.2.

*Proof.* [Proof of Theorem 4.1.1, assuming Lemmas 2.2.1 and 2.2.2] Let $n \in \mathbb{N}$ be sufficiently large, let $\exp\big(2^{-11}\sqrt{n}\big) \leq p \leq 2\cdot\exp\big(2^{-11}\sqrt{n}\big)$ be prime, and set $\beta := 4/p$. By Lemmas 2.2.1 and 2.2.2, it follows that

$$\mathbb{P}\big(\det(M_n) = 0\big) \leq 16n \sum_{m=n-1}^{2n-3} \left( \big(4/p\big)^{1/8} + \frac{p}{2^{m/4+2}} \right) \leq \exp\big(-c\sqrt{n}\big)$$

for some $c > 2^{-15}$, as required. □

We will prove Theorem 2.1.2 in Section 2.3, and deduce Lemma 2.2.2 in Section 2.4. Although the proofs are not especially technical, some of the definitions may initially seem somewhat surprising. In order to motivate these definitions, we will now provide a brief outline of the argument, beginning with the deduction of Lemma 2.2.2 from Theorem 2.1.2.

### 2.2.1 An outline of the proof of Lemma 2.2.2

We will bound $q_n(\beta)$ using the first moment method: for each $w \in \mathbb{Z}_p^n$, we will bound the expected number of vectors $v \in \mathbb{Z}_p^n \setminus \{0\}$ with $\rho(v) \geq \beta$ such that $M_n \cdot v = w$. In order to do so, we will use Theorem 2.1.2 to partition the collection of vectors $v \in \mathbb{Z}_p^n$ with $\rho(v) \geq \beta$ and $|v| \geq \lambda\sqrt{n}$ into a collection $\mathcal{U}$ of at most $n^{cn}$ 'fibres' (for some $\lambda > 0$ and $c > 0$); we will then apply the union bound inside each fibre. The bound we obtain on the probability that $M_n \cdot v = w$ will depend on the fibre containing $v$, and the partition is chosen so that (for each $S \in \mathcal{U}$ and $w \in \mathbb{Z}_p^n$) the expected number of vectors $v \in S$ with $M_n \cdot v = w$ is at most $n^{-c'n}$ (for some $c' > c$). The claimed bound then follows by summing over fibres, and then dealing with the vectors with small support separately via a simple counting argument (see Lemma 2.4.1).

To construct the partition, we need to map each vector $v \in \mathbb{Z}_p^n \setminus \{0\}$ to a fibre containing $v$. To do so, we repeatedly apply Theorem 2.1.2 to vectors of the form $v_Z$, for some set

$Z \subset [n]$ given by the earlier steps of the process. The theorem provides us with a container $B(v_Z)$ for $v_Z$, and (large) disjoint sets $X, Y \subset Z$ such that $v_i \in B(v_Z)$ for each $i \in X$, and (2.3) holds. Revealing the rows of $M_n$ corresponding to $X$, we will be able to use the probability that $M_{X\times[n]} \cdot v = w_X$ to 'beat' the number of choices for $v_X$, using the bound on $|B(v_Z)|$ in (2.3). We continue this iteration until we have chosen all but $O(\sqrt{n})$ of the non-zero entries of $v$.

To describe a single step of this iteration, assume that we have already revealed a subset of the rows of $M_n$, and let $Z \subset [n]$ denote the set of rows that have not yet been revealed. By Theorem 2.1.2, we may associate, to each vector $v \in \mathbb{Z}_p^n \setminus \{0\}$ with $\rho(v_Z) \geq \rho(v) \geq \beta \geq 4/p$ (see Observation 2.3.1, below) and $|v_Z| \geq 2^{18} \log p$, sets

$$Y(v_Z) \subset Z, \quad B(v_Z) \subset \mathbb{Z}_p \quad \text{and} \quad X(v_Z) := \big\{ i \in Z \setminus Y(v_Z) : v_i \in B(v_Z) \big\}.$$

In this step we will 'reveal' the rows of $M_n$ corresponding to $X = X(v_Z)$, and sum over the choices for $v_i \in B(v_Z)$ for each $i \in X$. We claim that

$$\mathbb{P}\big(M_{X\times[n]} \cdot v = w_X\big) \leq \rho(v_Y)^{|X|}. \tag{2.5}$$

Indeed, since $X$ and $Y = Y(v_Z)$ are disjoint subsets of $Z$, the entries of $M_{X\times Y}$ are all independent (of each other, and of the previously revealed entries of $M_n$), so the claimed bound holds by the definition of $\rho$ (see the proof of Lemma 2.4.3, below, for the details).

Each fibre will be the set of vectors that have the same sequence of sets $X$, $Y$ and $B(v_Z)$, and therefore to count the fibres we just need to count the number of choices for these sets. We have at most $2^{|Z|}$ choices each for $X$ and $Y$, and at most

$$\exp\Big(2^{12}\big(\log p\big)^2\Big) \leq \exp\big(2^{-8}n\big)$$

choices for the set $B(v_Z)$, by (2.2) and our choice of $p$. Now, it follows from (2.3) and our bounds on $|Y|$ that $|X| \geq |Z|/4$, and hence the total number of choices for these sets (over all steps of the process) is at most $\exp\big(2^{-6}n\log n\big)$, see Lemma 2.4.2, below.

Finally, we have at most $|B(v_Z)|^{|X|}$ choices for the vector $v_X$. Multiplying this by the probability bound (2.5), and using the bound on $|B(v_Z)|$ given by (2.3), we obtain

$$|B(v_Z)|^{|X|}\rho(v_Y)^{|X|} \leq \left(\frac{2^{16}}{\sqrt{|v_Z|}}\right)^{|X|} \leq n^{-|X|/4},$$

since $|v_Z| \geq \lambda\sqrt{n}$. Since $|X| \geq n/4$ in the first step, this will be sufficient to prove the claimed bound on the expected number of vectors $v \in C$ with $M_n \cdot v = w$.

Before continuing, let us briefly discuss why we are unable to use Theorem 2.1.2 to prove a stronger bound than that in Theorem 4.1.1. Recall that our probability bound for a given fibre is of the form $n^{-cn}$, and the number of fibres is roughly $\exp\big((\log p)^2\log n\big)$, since we need to iterate the process described above $\log n$ times. (We remark that for this reason we also cannot deduce a stronger bound for the probability that $\det(A_n) = 0$ from Theorem 2.1.2.) In order to improve our bound further, one would therefore need to either find a smaller set of containers, or find a set of containers that covers much more of the vector than those in Theorem 2.1.2. It is possible that an improvement of this type could be used to prove a bound of the form $\mathbb{P}\big(\det(M_n) = 0\big) \leq \exp\big(-c\sqrt{n\log n}\big)$; however, as we will show next, in order to obtain any further improvement significant new ideas would be needed.

### 2.2.2 A natural barrier at $\exp\big(-\sqrt{n\log n}\big)$

In this section we explain why a simple union bound (like that described in Section 2.2.1) cannot be used to prove a significantly stronger bound than that in Theorem 4.1.1, without 'reusing' some of the randomness in $M_n$. Let $m \leq n$, and consider the family of vectors $v \in \mathbb{Z}^n$ whose entries are chosen from the set $\{-N, \dots, N\}$, where $N = cn^{-1/2}2^m$ (for some

small $c > 0$). For any such $v$, we have

$$\rho(v_{[k]}) \geq \rho(v) \geq 2^{-m}$$

for every $k \geq m$, since a random walk with step sizes at most $N$ ends in the interval $[-2^{m-2}, 2^{m-2}]$ with probability at least $1/2$. Note also that $\rho(v_{[k]}) \geq 2^{-k}$ for every $k < m$.

Now, it follows that the natural bound[1]

$$\mathbb{P}\big(M_n \cdot v = 0\big) \leq \prod_{k=1}^{n} \rho(v_{[k]}),$$

which uses all of the randomness in $M_n$, cannot give a stronger bound than

$$\mathbb{P}\big(M_n \cdot v = 0\big) \leq 2^{-m(n-m)} \prod_{k=1}^{m} 2^{-k} = 2^{-mn+m^2/2+O(n)}.$$

Since there are $(2N+1)^n \geq c^n 2^{mn} n^{-n/2}$ choices for the vector $v$, a union bound (over these vectors) gives (at best) a bound of $n^{-n/2} 2^{m^2/2+O(n)}$, which is small only if $m \leq \sqrt{n \log n}$.

It follows that our proof method only has a chance of working if $p \leq \exp\big(\sqrt{n \log n}\big)$. However, if we are working over $\mathbb{Z}_p$ then we cannot hope to prove a much stronger bound on the singularity probability than $1/p$. Indeed, let $M_{n-1}$ be the matrix obtained by removing the first row and column of $M_n$, and let $u \in \{-1, 1\}^{n-1}$ be obtained from the first row of $M_n$ by deleting the entry $m_{11}$. Now, if $\det(M_{n-1}) \neq 0$ and $\langle u, M_{n-1}^{-1} \cdot u \rangle = m_{11}$, then there exists a vector $w := (1, -M_{n-1}^{-1} \cdot u) \in \mathbb{Z}_p^n \setminus \{0\}$ with $M \cdot w = 0$, and hence $\det(M_n) = 0$. It follows that the event that $\det(M_n) = 0$ is (up to a constant factor) at least as likely as the event that $\langle u, M_{n-1}^{-1} \cdot u \rangle \in \{-1, 1\}$, and it seems reasonable to expect that this latter event occurs with probability at least $\Omega(1/p)$.

[1]Note that we are losing something here, since the already-revealed part of the matrix may map $v_{[k+1,n]}$ to a non-maximiser of $\rho$. Controlling this (and using an anticoncentration inequality that is sensitive to the choice of the maximiser) may be a way to overcome the barrier described in this section.

### 2.2.3 Halász's inequality, and the inverse Littlewood–Offord theorem

In this section we will state the main tool we will use in the proof of Theorem 2.1.2, a classical Littlewood–Offord theorem due to Halász [48]. We will also prepare the reader for the proof in the next section by providing some motivation for the way we define our family of containers.

In order to state Halász's inequality, we need a little preparation. First, let us define multiplication on $\mathbb{Z}_p$ as follows: if $x, y \in \mathbb{Z}_p$, then the product $x \cdot y \in \mathbb{Z}$ is obtained by projecting $x$ and $y$ onto elements of $\{0, 1, \dots, p-1\}$ in the usual way, and then multiplying in $\mathbb{Z}$. Let $\|\cdot\|$ denote the distance to the nearest integer, and for each $n \in \mathbb{N}$, prime $p$ and vector $v \in \mathbb{Z}_p^n$, define the *level sets* of $v$ to be

$$T_t(v) := \left\{ k \in \mathbb{Z}_p \,:\, \sum_{i=1}^{n} \left\| \frac{k \cdot v_i}{p} \right\|^2 \leq t \right\}, \tag{2.6}$$

for each $t \geq 0$.

We can now state the lemma of Halász [48]; since we use a slightly different form than is usually stated, for completeness we provide a proof in [17, Appendix B].

**Lemma 2.2.3** (Halász's Anticoncentration Lemma)**.** *Let $n \in \mathbb{N}$ and $p$ be prime, and let $v \in \mathbb{Z}_p^n \setminus \{0\}$. Then*

$$\rho(v) \leq \frac{3}{p} + \frac{4|T_\ell(v)|}{p\sqrt{\ell}} + e^{-\ell}$$

*for every $1 \leq \ell \leq 2^{-6}|v|$.*

Let us now motivate the way we choose our family of containers, see (3.22), below. The basic intuition, first suggested by Tao and Vu [113, 114], is that if $\rho(v)$ is large, then $v$ should have some arithmetic structure. We think of the elements of the level sets $T_t(v)$ as

'frequencies' that correlate with the entries of $v$, and thus encode this arithmetic structure. Following the strategy of Tao and Vu [113] and Nguyen and Vu [88], we would therefore like to define the container of each 'structured' vector using its level sets.

The problem is that we would like a relatively small family of containers, whereas the number of level sets could potentially be very large. The solution is very simple: we consider a random subset $U$ of the coordinates of $v$. We will show that if $|U| \geq 2^{12} \log p$, then $v_U$ still correlates with the frequencies of the level sets of $v$, and we will choose the container of $v$ to be (roughly speaking) the elements of $\mathbb{Z}_p$ that correlate with these frequencies. We then choose $U$ as small as possible (subject to the above argument working), which implies that there are few choices for the vector $v_U$, and hence few containers.

## 2.3 Proof of the inverse Littlewood–Offord theorem

In this section we will prove Theorem 2.1.2. Let $n \in \mathbb{N}$ and a prime $p$ be fixed throughout the section, and assume that $p > 3$ and $n \geq 2^{18} \log p$ (since otherwise there are no vectors $v \in \mathbb{Z}_p^n$ with $\rho(v) \geq 4/p$ and $|v| \geq 2^{18} \log p$, so the statement holds vacuously with $\mathcal{C} = \emptyset$).

For each $m \in \mathbb{N}$ and $w \in \mathbb{Z}_p^m$, define (cf. [113, Section 7] and [88, Section 5]) the set of 'frequencies' of $w$ to be

$$F(w) := \left\{ k \in \mathbb{Z}_p \,:\, \sum_{i=1}^{m} \left\| \frac{k \cdot w_i}{p} \right\|^2 \leq \log p \right\},$$

and note (recalling (2.6)) that $F(w) = T_{\log p}(w)$. Now, for each $S \subset \mathbb{Z}_p$, define

$$C(S) := \left\{ a \in \mathbb{Z}_p \,:\, \sum_{k \in S} \left\| \frac{a \cdot k}{p} \right\|^2 \leq \frac{|S|}{2^5} \right\}. \tag{2.7}$$

Now set $m := \lfloor 2^{12} \log p \rfloor$, and define

$$\mathcal{C} := \big\{ C\big(F(w)\big) : w \in \mathbb{Z}_p^m \big\}, \tag{2.8}$$

and observe that $|\mathcal{C}| \leq p^m$, as required. We will show that $\mathcal{C}$ has the desired properties.

The following simple lemma motivates our choice of containers (cf. [88, Section 5]).

**Lemma 2.3.1.** *Let $v \in \mathbb{Z}_p^n$, and let $t \leq 2^{-7}n$. If $S \subset T_t(v)$, then*

$$\big|\big\{i \in [n] : v_i \notin C(S)\big\}\big| \leq \frac{n}{4}.$$

*Proof.* Let $R = \big\{i \in [n] : v_i \notin C(S)\big\}$, and observe that, by (2.6) and (2.7),

$$\frac{|R||S|}{2^5} \leq \sum_{i \in R} \sum_{k \in S} \left\| \frac{k \cdot v_i}{p} \right\|^2 \leq \sum_{k \in S} \sum_{i=1}^{n} \left\| \frac{k \cdot v_i}{p} \right\|^2 \leq t|S| \leq \frac{n|S|}{2^7},$$

so $|R| \leq n/4$, as required. □

Later in the proof, we will define $B(v) := C\big(F(v_U)\big)$ for some set $U \subset [n]$ with $|U| \leq m$ such that $F(v_U) \subset T_t(v)$ for $t = 2^{-7}n$ (see Lemma 2.3.5, below). We next turn to bounding the size of our containers; the following lemma (cf. [88, Section 5]) provides a first step.

**Lemma 2.3.2.** *For any set $S \subset \mathbb{Z}_p$, we have*

$$|C(S)| \leq \frac{4p}{|S|}. \tag{2.9}$$

*Proof.* We will instead bound the size of the larger set

$$C'(S) := \left\{ a \in \mathbb{Z}_p \,:\, \sum_{k \in S} \cos\left(\frac{2\pi a k}{p}\right) \geq \frac{|S|}{2} \right\}.$$

Indeed, observe that $C(S) \subset C'(S)$, since we have $1 - 2^4\|x\|^2 \leq \cos(2\pi x)$ for every $x \in \mathcal{R}$.

Now, let $a$ be a uniformly-chosen random element of $\mathbb{Z}_p$, and observe that, by Markov's inequality,

$$\begin{aligned} \mathbb{P}\big(a \in C'(S)\big) \;&=\; \mathbb{P}\left( \left( \sum_{k \in S} \cos\left(\frac{2\pi a k}{p}\right) \right)^2 \geq \frac{|S|^2}{4} \right) \\ &\leq\; \frac{4}{|S|^2} \cdot \frac{1}{p} \sum_{a \in \mathbb{Z}_p} \left( \sum_{k \in S} \cos\left(\frac{2\pi a k}{p}\right) \right)^2, \end{aligned}$$

Now, since $2\cos(x) = e^{ix} + e^{-ix}$, we have

$$4\sum_{a\in\mathbb{Z}_p}\left(\sum_{k\in S}\cos\left(\frac{2\pi ak}{p}\right)\right)^2 = \sum_{k_1\in\pm S}\sum_{k_2\in\pm S}\sum_{a\in\mathbb{Z}_p}\exp\left(\frac{2\pi ia(k_1+k_2)}{p}\right) \le 4p|S|,$$

where $\pm S$ is the multi-set obtained by taking the union of $S$ and $-S$, counting elements in both twice. For the second step, simply note that the roots of unity sum to zero, so the only terms that contribute are those with $k_1 + k_2 = 0$. It follows that

$$\frac{4}{|S|^2}\cdot\frac{1}{p}\sum_{a\in\mathbb{Z}_p}\left(\sum_{k\in S}\cos\left(\frac{2\pi ak}{p}\right)\right)^2 \le \frac{4}{|S|},$$

and hence $|C(S)| \le |C'(S)| \le 4p/|S|$, as claimed. □

We will use Halász's Anticoncentration Lemma (Lemma 2.2.3) to bound the right-hand side of (2.9) in terms of $\rho(v_Y)$ (for some set $Y$ that will be chosen in Lemma 2.3.4, below). The following lemma is a straightforward application of Lemma 2.2.3.

**Lemma 2.3.3.** *Let $v \in \mathbb{Z}_p^n$ with $\rho(v) \ge 4/p$ and $|v| \ge 2^{18}\log p$, and let $Y \subset [n]$ be such that $|v_Y| \ge |v|/4$. Then*

$$\rho(v_Y) \le \frac{2^{13}|T_\ell(v_Y)|}{p\sqrt{|v|}},$$

*where $\ell := 2^{-16}|v|$.*

In the proof of Lemma 2.3.3, and also later in the section, we will need the following simple observation (see [30, Lemma 2.8] or [17, Lemma A.10]).

**Observation 2.3.1** (Lemma 2.8 of [30])**.** *$\rho(v_Y) \ge \rho(v)$ for every $v \in \mathbb{Z}_p^n$ and every $Y \subset [n]$.*

*Proof.* [Proof of Lemma 2.3.3] Applying Lemma 2.2.3 to $v_Y$, with $\ell = 2^{-16}|v| \le 2^{-14}|v_Y|$, gives

$$\rho(v_Y) \le \frac{3}{p} + \frac{4|T_\ell(v_Y)|}{p\sqrt{\ell}} + e^{-\ell}.$$

Now, by Observation 2.3.1 and our assumption on $\rho(v)$, we have $\rho(v_Y) \geq \rho(v) \geq 4/p$. Since $\ell \geq 4 \log p$, it follows that

$$\rho(v_Y) \leq \frac{2^5 |T_\ell(v_Y)|}{p\sqrt{\ell}} = \frac{2^{13} |T_\ell(v_Y)|}{p\sqrt{|v|}},$$

as claimed. □

To complete the proof, it will now suffice to choose sets $Y \subset [n]$, with $n/4 \leq |Y| \leq n/2$, and $U \subset [n]$, with $|U| \leq m$, such that

$$F(v_U) \subset T_t(v), \qquad |v_Y| \geq \frac{|v|}{4} \qquad \text{and} \qquad |T_\ell(v_Y)| \leq 2 \cdot |F(v_U)|, \tag{2.10}$$

where $\ell = 2^{-16}|v|$ and $t = 2^{-7}n$. Indeed, for any such sets we have, by Lemmas 2.3.2 and 2.3.3,

$$\big|C\big(F(v_U)\big)\big| \leq \frac{4p}{|F(v_U)|} \leq \frac{2^{15}}{\rho(v_Y)\sqrt{|v|}} \cdot \frac{|T_\ell(v_Y)|}{|F(v_U)|} \leq \frac{2^{16}}{\rho(v_Y)\sqrt{|v|}},$$

and, by Lemma 2.3.1, we have

$$\big|\big\{i \in [n] : v_i \notin C\big(F(v_U)\big)\big\}\big| \leq \frac{n}{4}.$$

Thus, setting $B(v) := C\big(F(v_U)\big)$, we obtain a set in $\mathcal{C}$ for which the properties (2.3) hold.

We will choose the sets $Y$ and $U$ in the next two lemmas. In each case we simply choose a random set of the correct density. We will say that $R$ is a *$q$-random* subset of a set $S$ if each element of $S$ is included in $R$ independently at random with probability $q$.

**Lemma 2.3.4.** *Let $v \in \mathbb{Z}_p^n$ with $|v| \geq 2^{18} \log p$. There exists $Y \subset [n]$, with $n/4 \leq |Y| \leq n/2$, such that*

$$|v_Y| \geq \frac{|v|}{4} \qquad \textit{and} \qquad T_\ell(v_Y) \subset T_{8\ell}(v),$$

*where $\ell = 2^{-16}|v|$.*

*Proof.* Let $Y$ be a (3/8)-random subset of $[n]$; we will prove that with positive probability $Y$ has all of the required properties. Since $n \geq |v| \geq 2^{18} \log p \geq 2^{18}$, the properties

$$\frac{n}{4} \leq |Y| \leq \frac{n}{2} \qquad \text{and} \qquad |v_Y| \geq \frac{|v|}{4}$$

each hold with probability at least 3/4, by Chernoff's inequality. To bound the probability that $T_\ell(v_Y) \setminus T_{8\ell}(v)$ is non-empty, define a random variable

$$W(k) := \sum_{i \in Y} \left\| \frac{k \cdot v_i}{p} \right\|^2$$

for each $k \in \mathbb{Z}_p$, and observe that, by (2.6),

$$k \in T_\ell(v_Y) \;\Leftrightarrow\; W(k) \leq \ell \qquad \text{and} \qquad k \notin T_{8\ell}(v) \;\Rightarrow\; \mathbb{E}[W(k)] \geq 3\ell.$$

Moreover, by Chernoff's inequality,[2]

$$\mathbb{P}\big(k \in T_\ell(v_Y)\big) = \mathbb{P}\big(W(k) \leq \ell\big) \leq e^{-\ell/2} \leq \frac{1}{p^2}$$

for every $k \notin T_{8\ell}(v)$, since $\ell \geq 4 \log p$. It follows that

$$\mathbb{E}\left[|T_\ell(v_Y) \setminus T_{8\ell}(v)|\right] \leq \frac{1}{p},$$

and hence $T_\ell(v_Y) \subset T_{8\ell}(v)$ with probability at least 3/4, as required. □

Finally, we need to show that a suitable set $U$ exists.

**Lemma 2.3.5.** *Let $v \in \mathbb{Z}_p^n$. There exists $U \subset [n]$, with $|U| \leq m$, such that*

$$|T_{8\ell}(v)| \leq 2 \cdot |F(v_U)| \qquad \textit{and} \qquad F(v_U) \subset T_t(v),$$

*where $\ell = 2^{-16}|v|$ and $t = 2^{-7}n$.*

[2]Here we use the following variant of the standard Chernoff inequality: if $X_1, \dots, X_N$ are iid Bernoulli random variables, and $t_1, \dots, t_N \in [0,1]$, then $\mathbb{P}\big(\sum_{i=1}^N t_i X_i \leq s\big) \leq \exp\big(-\mathbb{E}[X]/2 + s\big)$.

*Proof.* Let $U$ be a $(m/2n)$-random subset of $[n]$. We will prove that the claimed properties hold simultaneously with positive probability. Note first that $|U| \leq m$ with probability at least $3/4$, by Chernoff's inequality, since $m = \lfloor 2^{12} \log p \rfloor \geq 2^{12}$.

Next, we show that $|T_{8\ell}(v) \setminus F(v_U)| \leq |T_{8\ell}(v)|/2$ with probability at least $1/2$. Observe first that, for every $k \in \mathbb{Z}_p$,

$$\mathbb{P}\big(k \notin F(v_U)\big) = \mathbb{P}\left(\sum_{i \in U} \left\| \frac{k \cdot v_i}{p} \right\|^2 > \log p\right) \leq \frac{1}{\log p} \cdot \mathbb{E}\left[\sum_{i \in U} \left\| \frac{k \cdot v_i}{p} \right\|^2\right],$$

by Markov's inequality. Now, if $k \in T_{8\ell}(v)$, then

$$\frac{1}{\log p} \cdot \mathbb{E}\left[\sum_{i \in U} \left\| \frac{k \cdot v_i}{p} \right\|^2\right] = \frac{m}{2n \log p} \sum_{i=1}^{n} \left\| \frac{k \cdot v_i}{p} \right\|^2 \leq \frac{8m\ell}{2n \log p} \leq \frac{1}{4},$$

since $m \leq 2^{12} \log p$ and $\ell = 2^{-16}|v| \leq 2^{-16} n$. It follows that

$$\mathbb{P}\left(|T_{8\ell}(v) \setminus F(v_U)| \geq \frac{|T_{8\ell}(v)|}{2}\right) \leq \frac{2}{|T_{8\ell}(v)|} \cdot \mathbb{E}\left[|T_{8\ell}(v) \setminus F(v_U)|\right] \leq \frac{1}{2},$$

by Markov's inequality, as claimed.

Finally, to bound the probability that $F(v_U) \setminus T_t(v)$ is non-empty, we repeat the argument used in the proof of Lemma 2.3.4. To be precise, we define a random variable

$$W(k) := \sum_{i \in U} \left\| \frac{k \cdot v_i}{p} \right\|^2$$

for each $k \in \mathbb{Z}_p$, and observe that, by (2.6),

$$k \in F(v_U) \;\Leftrightarrow\; W(k) \leq \log p \qquad \text{and} \qquad k \notin T_t(v) \;\Rightarrow\; \mathbb{E}[W(k)] \geq 2^{-8} m.$$

Recalling that $m = \lfloor 2^{12} \log p \rfloor$, it follows by Chernoff's inequality that

$$\mathbb{P}\big(k \in F(v_U)\big) = \mathbb{P}\big(W(k) \leq \log p\big) \leq \frac{1}{p^2}$$

for every $k \notin T_t(v)$, and hence

$$\mathbb{P}\big(F(v_U) \not\subset T_t(v)\big) \leq \mathbb{E}\left[|F(v_U) \setminus T_t(v)|\right] \leq \frac{1}{p}.$$

It follows that, with positive probability, the random set $U$ satisfies

$$|U| \leq m, \qquad |T_{8\ell}(v)| \leq 2 \cdot |F(v_U)| \qquad \text{and} \qquad F(v_U) \subset T_t(v),$$

as required. □

As observed above, it is now straightforward to complete the proof of Theorem 2.1.2.

*Proof.* [Proof of Theorem 2.1.2] Let $\mathcal{C}$ be as defined in (3.22), and note that

$$|\mathcal{C}| \leq p^m \leq \exp\big(2^{12}(\log p)^2\big).$$

For each $v \in \mathbb{Z}_p^n$ with $\rho(v) \geq 4/p$ and $|v| \geq 2^{18} \log p$, let $Y$ and $U$ be the sets given by Lemmas 2.3.4 and 2.3.5 respectively, and define $B(v) := C\big(F(v_U)\big)$.

Now, we have $n/4 \leq |Y| \leq n/2$, by Lemma 2.3.4, and

$$\big|\big\{i \in [n] : v_i \notin B(v)\big\}\big| \leq \frac{n}{4},$$

by Lemma 2.3.1, since $F(v_U) \subset T_t(v)$, where $t = 2^{-7}n$, by Lemma 2.3.5. Finally, we have

$$|B(v)| \leq \frac{4p}{|F(v_U)|} \leq \frac{2^{15}}{\rho(v_Y)\sqrt{|v|}} \cdot \frac{|T_\ell(v_Y)|}{|F(v_U)|} \leq \frac{2^{16}}{\rho(v_Y)\sqrt{|v|}},$$

by Lemmas 2.3.2–2.3.5, since $|T_\ell(v_Y)| \leq |T_{8\ell}(v)| \leq 2 \cdot |F(v_U)|$. This completes the proof of the inverse Littlewood–Offord theorem. □

## 2.4 Applying the inverse Littlewood–Offord theorem

In this section we will use our inverse Littlewood–Offord theorem to prove Lemma 2.2.2. Let us fix a sufficiently large integer $n \in \mathbb{N}$ and a prime $3 < p \leq \exp\big(2^{-10}\sqrt{n}\big)$ throughout the section. Recall that $\beta \geq 4/p$, that

$$q_n(\beta) = \max_{w \in \mathbb{Z}_p^n} \mathbb{P}\big(\exists\, v \in \mathbb{Z}_p^n \setminus \{0\} \,:\, M_n \cdot v = w \text{ and } \rho(v) \geq \beta\big),$$

and that our aim is to prove that $q_n(\beta) \leq 2^{-n/4}$. We shall do so by using Theorem 2.1.2 to partition the vectors $v \in \mathbb{Z}_p^n$ with $\rho(v) \geq \beta$ and $|v| \geq 2^8\sqrt{n}$ into a collection of 'fibres', and then applying a simple first moment argument inside each fibre. Vectors with small support will require a separate (and much simpler) argument, so let us begin by dealing with those. For each $w \in \mathbb{Z}_p^n$, define

$$Q(w) := \big|\big\{v \in \mathbb{Z}_p^n \setminus \{0\} \,:\, M_n \cdot v = w \text{ and } |v| < 2^8\sqrt{n}\big\}\big|.$$

Our first lemma bounds the expected size of $Q(w)$.

**Lemma 2.4.1.** *For every $w \in \mathbb{Z}_p^n$,*

$$\mathbb{E}\big[Q(w)\big] \leq 2^{-n/2}.$$

*Proof.* Fix $w \in \mathbb{Z}_p^n$; the lemma is an easy consequence of the following claim.

**Claim:** If $v \in \mathbb{Z}_p^n \setminus \{0\}$, then $\mathbb{P}\big(M_n \cdot v = w\big) \leq 2^{-n}$.

*Proof.* [Proof of Claim] Choose $k \in [n]$ such that $v_k \neq 0$, and reveal the entire matrix $M_n$ except for the $k$th row and the $k$th column. Observe that if $M_n \cdot v = w$, then

$$m_{ik}v_k = w_i - \sum_{j \neq k} m_{ij}v_j \tag{2.11}$$

for each $i \in [n]$, where $m_{ij}$ are the entries of $M_n$. Now, for any choice of the entries $m_{ij}$ with $j \neq k$, the event (2.11) has probability at most $1/2$, and these events are independent for different values of $i \neq k$. Finally, having revealed the entire matrix except for $m_{kk}$, the event (2.11) for $i = k$ has probability at most $1/2$, so $\mathbb{P}\big(M_n \cdot v = w\big) \leq 2^{-n}$, as claimed. □

Now, since there are at most $\binom{n}{k}p^k$ vectors $v \in \mathbb{Z}_p^n \setminus \{0\}$ with $|v| < k$, and recalling that $p \leq \exp\big(2^{-10}\sqrt{n}\big)$ and $n$ is sufficiently large, the claim implies that

$$\mathbb{E}\big[Q(w)\big] \leq \binom{n}{2^8\sqrt{n}} p^{2^8\sqrt{n}} \cdot 2^{-n} \leq 2^{-n/2}$$

as required. □

From now on, we will therefore restrict our attention to the vectors with large support:

$$\mathcal{V} := \big\{v \in \mathbb{Z}_p^n : \rho(v) \geq \beta,\, |v| \geq 2^8\sqrt{n}\big\}.$$

To deal with these vectors, we will define a function

$$f\colon \mathcal{V} \to \mathcal{X} := \Big\{\big(X_i, Y_i, B_i\big)_{i=1}^{\infty} : X_i, Y_i \subset [n] \text{ and } B_i \subset \mathbb{Z}_p \text{ for each } i \in \mathbb{N}\Big\},$$

using Theorem 2.1.2; the 'fibres' forming our partition of $\mathcal{V}$ will be exactly the fibres $f^{-1}(S)$ of the function $f$. We will define $f$ using the following algorithm, which takes as its input a vector $v \in \mathcal{V}$, and outputs an element of $\mathcal{X}$.

**Algorithm 2.4.1.** *Let $v \in \mathcal{V}$. At the $k$th step, if the process has not yet ended, we will have constructed a sequence $(X_i, Y_i, B_i)_{i=1}^{k-1}$ with $X_i, Y_i \subset [n]$ and $B_i \subset \mathbb{Z}_p$ for each $i \in [k-1]$. In this case, set*

$$Z_k := [n] \setminus \bigcup_{i=1}^{k-1} X_i,$$

*and do the following:*

1. *If $|v_{Z_k}| \geq 2^8\sqrt{n}$ then we apply Theorem 2.1.2, and set $Y_k := Y(v_{Z_k})$, $B_k := B(v_{Z_k})$, and*

$$X_k := \big\{i \in Z_k \setminus Y_k \,:\, v_i \in B_k\big\}. \tag{2.12}$$

   *Set $k \to k+1$ and repeat the process.*

2. *If $|v_{Z_k}| < 2^8\sqrt{n}$, then we set $k^* = k^*(v) := k-1$ and*

$$X_j = Y_j = B_j = \emptyset$$

   *for every $j \geq k$. The process terminates, and we set $f(v) := \big(X_i, Y_i, B_i\big)_{i=1}^{\infty}$.*

Define $\mathcal{U} := \big\{f(v) : v \in \mathcal{V}\big\}$. Theorem 2.1.2 implies the following upper bound on $|\mathcal{U}|$.

**Lemma 2.4.2.**

$$|\mathcal{U}| \leq n^{n/64}.$$

*Proof.* We claim first that, for each $k \in \mathbb{N}$, either $|v_{Z_k}| < 2^8\sqrt{n}$, or

$$|Z_k| \leq \left(\frac{3}{4}\right)^{k-1} n. \tag{2.13}$$

Indeed, by Observation 2.3.1 we have $\rho(v_{Z_k}) \geq \rho(v) \geq \beta \geq 4/p$ for every $v \in \mathcal{V}$, and therefore, if $|v_{Z_k}| \geq 2^8\sqrt{n} \geq 2^{18}\log p$, it follows from Theorem 2.1.2 that $|Y_k| \leq |Z_k|/2$ and

$$\big|Z_k \setminus \big(X_k \cup Y_k\big)\big| \leq \big|\big\{i \in Z_k : v_i \notin B_k\big\}\big| \leq \frac{|Z_k|}{4}. \tag{2.14}$$

Hence $|X_k| \geq |Z_k|/4$, and (2.13) follows. In particular, this implies that $k^*(v) \leq 2\log n$.

Now, given $(X_i, Y_i, B_i)_{i=1}^{k-1}$, there are at most $2^{|Z_k|}$ choices for each of the sets $X_k$ and $Y_k$ (since they are subsets of $Z_k$), and by (2.2) there are at most

$$\exp\Big(2^{12}\big(\log p\big)^2\Big) \leq \exp\big(2^{-8}n\big)$$

choices for $B_k$. It follows that the total number of choices for $f(v)$ is at most

$$\exp\left(2^{-7}n\log n + 2\sum_{k=1}^{\infty}\left(\frac{3}{4}\right)^{k-1} n\right) \leq \exp\big(2^{-6}n\log n\big) = n^{n/64},$$

as required, since $n$ is sufficiently large. □

We will bound, for each sequence $S \in \mathcal{U}$, the probability that some vector $v \in \mathcal{V}$ with $f(v) = S$ satisfies $M_n \cdot v = w$, and then sum over $S \in \mathcal{U}$. To do so, for each $S \in \mathcal{U}$ and $w \in \mathbb{Z}_p^n$, let us define a random variable

$$Q(S, w) := \big|\big\{v \in \mathcal{V} \,:\, f(v) = S \text{ and } M_n \cdot v = w\big\}\big|.$$

The next lemma bounds the expected size of $Q(S, w)$.

**Lemma 2.4.3.** *If $S = \big(X_i, Y_i, B_i\big)_{i=1}^{\infty} \in \mathcal{U}$ and $w \in \mathbb{Z}_p^n$, then*

$$\mathbb{E}\big[Q(S,w)\big] \;\leq\; \left(\frac{2^{56}}{n}\right)^{n/16}. \tag{2.15}$$

*Proof.* If $f(v) = S$, then we have $v_j \in B_i$ for every $j \in X_i$, and $|v_{Z_{k^*+1}}| < 2^8\sqrt{n}$. There are therefore at most

$$\binom{n}{2^8\sqrt{n}} \cdot p^{2^8\sqrt{n}} \cdot \prod_{i=1}^{k^*} |B_i|^{|X_i|}$$

vectors $v \in \mathcal{V}$ with $f(v) = S$. We claim that, for each such vector $v$,

$$\mathbb{P}\big(M_n \cdot v = w\big) \leq \prod_{i=1}^{k^*} \max_{u(i) \in \mathbb{Z}_p^{|X_i|}} \mathbb{P}\big(M_{X_i \times Y_i} \cdot v_{Y_i} = u(i)\big) = \prod_{i=1}^{k^*} \rho(v_{Y_i})^{|X_i|}. \tag{2.16}$$

To prove (2.16), recall from (2.12) that

$$X_i \cap Y_i = \emptyset \qquad \text{and} \qquad X_i \cap X_j = Y_i \cap X_j = \emptyset$$

for every $i \in [k^*]$ and every $1 \leq j < i$, since $X_i, Y_i \subset Z_i$. It follows that

$$\mathbb{P}\bigg(M_{X_i \times [n]} \cdot v = w_{X_i} \;\Big|\; \bigcap_{j=1}^{i-1} M_{X_j \times [n]} \cdot v = w_{X_j}\bigg) \leq \max_{u(i) \in \mathbb{Z}_p^{|X_i|}} \mathbb{P}\big(M_{X_i \times Y_i} \cdot v_{Y_i} = u(i)\big)$$

for every $i \in [k^*]$, and moreover the entries of $M_{X_i \times Y_i}$ are all independent. This proves (2.16), and summing over $v \in \mathcal{V}$ with $f(v) = S$ gives

$$\mathbb{E}\big[Q(S,w)\big] \;\leq\; \max_{v \in \mathcal{V}\colon f(v) = S} \binom{n}{2^8\sqrt{n}} \cdot p^{2^8\sqrt{n}} \cdot \prod_{i=1}^{k^*} \Big(|B_i| \cdot \rho(v_{Y_i})\Big)^{|X_i|}.$$

To deduce (2.15), recall from Theorem 2.1.2 and Algorithm 2.4.1 that, for every $v \in \mathcal{V}$ such that $f(v) = S$,

$$|B_i| \leq \frac{2^{16}}{\rho(v_{Y_i})\sqrt{|v_{Z_i}|}} \leq \frac{2^{12}}{\rho(v_{Y_i}) n^{1/4}}$$

for each $i \in [k^*]$, since $|v_{Z_i}| \geq 2^8\sqrt{n}$. Since $p \leq \exp\big(2^{-10}\sqrt{n}\big)$ and $n$ is sufficiently large, and recalling from (2.14) that we have $|X_1| \geq n/4$ (since $|v| \geq 2^8\sqrt{n}$ for every $v \in \mathcal{V}$), it follows that

$$\mathbb{E}\big[Q(S,w)\big] \;\leq\; \binom{n}{2^8\sqrt{n}} \cdot p^{2^8\sqrt{n}} \cdot \left(\frac{2^{12}}{n^{1/4}}\right)^{\sum_i |X_i|} \leq \left(\frac{2^{14}}{n^{1/4}}\right)^{n/4} = \left(\frac{2^{56}}{n}\right)^{n/16},$$

as required. □

Completing the proof of Lemma 2.2.2, and hence of Theorem 4.1.1, is now straightforward.

*Proof.* [Proof of Lemma 2.2.2] By Lemma 2.4.1, for each $w \in \mathbb{Z}_p^n$ the probability that there exists $v \in \mathbb{Z}_p^n \setminus \{0\}$ such that $|v| < 2^8\sqrt{n}$ and $M_n \cdot v = w$ is at most $2^{-n/2}$, and hence

$$q_n(\beta) \leq 2^{-n/2} + \sum_{S \in \mathcal{U}} \max_{w \in \mathbb{Z}_p^n} \mathbb{P}\Big(\exists\, v \in \mathcal{V} \,:\, f(v) = S \text{ and } M_n \cdot v = w\Big).$$

Now, by Lemma 2.4.3, we have

$$\mathbb{P}\Big(\exists\, v \in \mathcal{V} \,:\, f(v) = S \text{ and } M_n \cdot v = w\Big) \,\leq\, \left(\frac{2^{56}}{n}\right)^{n/16}$$

for every $S \in \mathcal{U}$ and $w \in \mathbb{Z}_p^n$, and hence, by Lemma 2.4.2,

$$q_n(\beta) \leq 2^{-n/2} + n^{n/64}\left(\frac{2^{56}}{n}\right)^{n/16} \,\leq\, 2^{-n/4}$$

since $n$ is sufficiently large. This completes the proof of the lemma. □

As observed in Section 2.2, Lemmas 2.2.1 and 2.2.2 together imply Theorem 4.1.1.

## 2.5 The proof of Lemma 2.2.1

In this section we will provide, for the reader's convenience, a proof of Lemma 2.2.1. We emphasize that the proof given below is essentially contained in the paper of Ferber and Jain [30], and that several of the key lemmas in the proof appeared in the papers of Costello, Tao and Vu [19] and Nguyen [89].

It will be convenient to work over $\mathcal{F}_p$, so let us write $\mathrm{rk}(M)$ for the rank of a matrix $M$ over $\mathcal{F}_p$, and $M_{n-1}$ for the random symmetric matrix obtained by removing the first row and

column from $M_n$. The following lemma of Nguyen (see [89, Section 2]), allows us to restrict our attention to matrices $M_n$ such that $\mathrm{rk}(M_n) = n-1$ and $\mathrm{rk}(M_{n-1}) \in \{n-2, n-1\}$.

**Lemma 2.5.1.** *For every $n \in \mathbb{N}$ and prime $p > 2$,*

$$\mathbb{P}\big(\det(M_n) = 0\big) \leq 4n \sum_{m=n}^{2n-2} \mathbb{P}\Big(\big\{\mathrm{rk}(M_m) = m-1\big\} \cap \big\{\mathrm{rk}(M_{m-1}) \in \{m-2, m-1\}\big\}\Big).$$

We deal with the cases $\mathrm{rk}(M_{n-1}) = n-2$ and $\mathrm{rk}(M_{n-1}) = n-1$ in Lemmas 2.5.2 and 2.5.4, respectively; the first of these (cf. [30, Section 2.2]) is more straightforward.

**Lemma 2.5.2.** *For every $n \in \mathbb{N}$, prime $p > 2$, and $\beta > 0$,*

$$\mathbb{P}\Big(\big\{\mathrm{rk}(M_n) = n-1\big\} \cap \big\{\mathrm{rk}(M_{n-1}) = n-2\big\}\Big) \leq \beta + q_{n-1}(\beta).$$

Let us write $\mathrm{adj}(M)$ for the *adjugate* of a matrix $M$ over $\mathcal{F}_p$. We will need the following lemma of Nguyen [89], see also [30, Lemma 2.5].

**Lemma 2.5.3.** *If $\mathrm{rk}(M_{n-1}) = n-2$, then there exists a non-trivial column $a \in \mathcal{F}_p^{n-1}$ of $\mathrm{adj}(M_{n-1})$ such that*

(*a*) *$M_{n-1} \cdot a = 0$, and*

(*b*) *if $\det(M_n) = 0$, then $\sum_{i=2}^{n} a_i x_i = 0$,*

*where $a = (a_2, \ldots, a_n)$, and $(x_1, \ldots, x_n)$ is the first row of $M_n$.*

*Proof.* [Proof of Lemma 2.5.2] By Lemma 2.5.3, it follows that in order to bound the probability that $\mathrm{rk}(M_n) = n-1$ and $\mathrm{rk}(M_{n-1}) = n-2$, it suffices to bound the probability that there exists a vector $a \in \mathcal{F}_p^{n-1} \setminus \{0\}$ (unique up to a constant factor) with $M_{n-1} \cdot a = 0$ and $a \cdot x = 0$, where $x \in \{-1, 1\}^{n-1}$ is a random vector chosen uniformly and independent of $M_{n-1}$.

We will partition this event into 'structured' and 'unstructured' cases, using the event

$$\mathcal{U}_\beta := \big\{\rho(v) \le \beta \text{ for every vector } v \in \mathcal{F}_p^{n-1} \setminus \{0\} \text{ with } M_{n-1} \cdot v = 0\big\}.$$

Observe first that, for any $M_{n-1} \in \mathcal{U}_\beta$, and any $a \in \mathcal{F}_p^{n-1} \setminus \{0\}$ with $M_{n-1} \cdot a = 0$, we have

$$\mathbb{P}\big(a \cdot x = 0 \,\big|\, M_{n-1}\big) \le \beta,$$

and hence

$$\mathbb{P}\Big(\big\{\mathrm{rk}(M_n) = n-1\big\} \cap \big\{\mathrm{rk}(M_{n-1}) = n-2\big\} \cap \mathcal{U}_\beta\Big) \le \beta.$$

On the other hand, by the definition of $q_n(\beta)$, we have

$$\mathbb{P}\big(\mathcal{U}_\beta^c\big) = \mathbb{P}\big(\exists\, v \in \mathcal{F}_p^{n-1} \setminus \{0\} : M_{n-1} \cdot v = 0 \text{ and } \rho(v) > \beta\big) \le q_{n-1}(\beta).$$

It follows that

$$\mathbb{P}\Big(\big\{\mathrm{rk}(M_n) = n-1\big\} \cap \big\{\mathrm{rk}(M_{n-1}) = n-2\big\}\Big) \le \beta + q_{n-1}(\beta),$$

as required. □

Finally, the following lemma deals with the case $\mathrm{rk}(M_{n-1}) = n-1$ (cf. [30, Section 2.3]).

**Lemma 2.5.4.** *For every $n \in \mathbb{N}$, prime $p > 2$, $\beta > 0$, and integer $1 \le k \le n-2$, we have*

$$\mathbb{P}\Big(\mathrm{rk}(M_n) = \mathrm{rk}(M_{n-1}) = n-1\Big) \le 2 \cdot \big(2^k\beta + 2^{-k}\big)^{1/4} + 3^{k+1} q_{n-1}(\beta).$$

The proof strategy for Lemma 2.5.4 is similar to that of Lemma 2.5.2 (in particular, we will split the event into 'structured' and 'unstructured' cases), but now it is trickier to relate our event to $q_n(\beta)$, as we do not have a result corresponding to Lemma 2.5.3 for this case. Instead, we will use the following 'decoupling' lemma of Costello, Tao and Vu [19].

**Lemma 2.5.5** (Lemma 4.7 of [19])**.** *Let $X$ and $Y$ be independent random variables, and let $\mathcal{E}(X,Y)$ be an event that depends on $X$ and $Y$. Then*

$$\mathbb{P}\big(\mathcal{E}(X,Y)\big) \leq \Big(\mathbb{P}\big(\mathcal{E}(X,Y)\cap\mathcal{E}(X',Y)\cap\mathcal{E}(X,Y')\cap\mathcal{E}(X',Y')\big)\Big)^{1/4},$$

*where $X'$ and $Y'$ are independent copies of $X$ and $Y$.*

It was remarked in [19] that Lemma 2.5.5 is equivalent to the classical fact (which was essentially proved by Erdős [20] in 1938) that a bipartite graph with parts of size $m$ and $n$ and $cmn$ edges contains at least $c^4m^2n^2$ (possibly degenerate) copies of $C_4$. Indeed, to deduce Lemma 2.5.5 from this theorem, simply define a bipartite graph, each of whose vertices represents an element of the range of $X$ or $Y$, and whose edges encode the event $\mathcal{E}$.

In order to state the technical lemma that we will use to prove Lemma 2.5.4, we need a little notation. Given a vector $v \in \mathcal{F}_p^m$ and a set $J \subset [m]$, let $v_J \in \mathcal{F}_p^{|J|}$ denote the restriction of $v$ to the coordinates of $J$, and let $v_J^*$ be the vector in $\mathcal{F}_p^m$ whose $i$th coordinate is $v_i \cdot \mathbb{1}[i \in J]$. Moreover, let $u, u' \in \{-1,1\}^{n-1}$ be chosen uniformly and independently at random, and define $w \in \{-2,0,2\}^{n-1}$ by setting $w_i := u_i - u'_i$ for each $i \in [n-1]$.

Costello, Tao and Vu [19] used Lemma 2.5.5 to prove the following key bound (for the details, see either [19, Section 4.6], [30, Section 2.3] or [17, Appendix A]).

**Lemma 2.5.6.** *For any non-trivial partition $I \cup J = [n-1]$, we have*

$$\mathbb{P}\big(\mathrm{rk}(M_n) = \mathrm{rk}(M_{n-1}) = n-1\big) \leq 2 \cdot \mathbb{E}\Big[\max_{a\in\mathcal{F}_p} \mathbb{P}\big(z_I \cdot w_I = a \,\big|\, M_{n-1}\big)^{1/4} \mathbb{1}\big[\mathrm{rk}(M_{n-1}) = n-1\big]\Big],$$

*where $z := M_{n-1}^{-1} \cdot w_J^*$, and the expectation is over the choice of $M_{n-1}$.*

In the proof of Lemma 2.5.4 we will need the following variant of $\rho(v)$. For any $n \in \mathbb{N}$ and $v \in \mathcal{F}_p^n$, define

$$\rho_{1/2}(v) := \max_{a\in\mathcal{F}_p} \mathbb{P}\big(u_1v_1 + \cdots + u_nv_n = a\big),$$

where $u_1, \dots, u_n$ are iid random variables taking the value 0 with probability 1/2, and the values $\pm 1$ each with probability 1/4. We will need the following simple inequalities.

**Lemma 2.5.7** (Lemmas 2.8 and 2.9 of [30]). *For any $v \in \mathcal{F}_p^n$, and any partition $I \cup J = [n]$,*

$$\rho_{1/2}(v) \le \rho(v) \qquad \text{and} \qquad \rho(v) \le \rho(v_I) \le 2^{|J|}\rho(v).$$

We are now ready to prove Lemma 2.5.4.

*Proof.* [Proof of Lemma 2.5.4] Recall that $1 \le k \le n-2$, and let $J \subset [n-1]$ with $|J| = k$. By Lemma 2.5.6, it will suffice to show that

$$\mathbb{E}\left[\max_{a \in \mathcal{F}_p} \mathbb{P}\big(z_I \cdot w_I = a \,\big|\, M_{n-1}\big)^{1/4} \mathbb{1}\big[\mathrm{rk}(M_{n-1}) = n-1\big]\right] \le \left(2^{|J|}\beta + 2^{-|J|}\right)^{1/4} + 3^{|J|} q_{n-1}(\beta),$$

where $I = [n] \setminus J$ and $z = M_{n-1}^{-1} \cdot w_J^*$ is defined whenever $\mathrm{rk}(M_{n-1}) = n-1$. Recall that $w \in \{-2, 0, 2\}^{n-1}$, and observe that therefore $M_{n-1} \cdot z = w_J^* \in W(J)$, where

$$W(J) := \big\{v \in \{-2,0,2\}^{n-1} : v_j = 0 \text{ for all } j \notin J\big\}.$$

We will use the following event to partition into cases:

$$\mathcal{U}_\beta^{(J)} := \Big\{\rho(v) \le \beta \text{ for every vector } v \in \mathcal{F}_p^{n-1} \setminus \{0\} \text{ such that } M_{n-1} \cdot v \in W(J)\Big\}.$$

We will bound the expectation above using the following three claims.

**Claim 1:** $\mathbb{P}\big(M_{n-1} \notin \mathcal{U}_\beta^{(J)}\big) \le 3^{|J|} q_{n-1}(\beta)$.

*Proof.* [Proof of Claim 1] If $\mathcal{U}_\beta^{(J)}$ does not hold for $M_{n-1}$, then there exists a vector $v \in \mathcal{F}_p^{n-1} \setminus \{0\}$ such that $M_{n-1} \cdot v \in W(J)$ and $\rho(v) > \beta$. For each individual vector $w \in W(J)$, the probability that this holds with $M_{n-1} \cdot v = w$ is at most $q_{n-1}(\beta)$, by (2.4). Hence, summing over $w \in W(J)$, and noting that $|W(J)| = 3^{|J|}$, the claim follows. $\square$

**Claim 2:** If $\mathrm{rk}(M_{n-1}) = n-1$, then $\mathbb{P}\big(z = 0 \,\big|\, M_{n-1}\big) \leq 2^{-|J|}$.

*Proof.* [Proof of Claim 2] If $z = 0$ then $w_J^* = M_{n-1} \cdot z = 0$. Since $w_i = 0$ occurs with probability $1/2$ for each $i \in J$, and these events are independent, the claim follows immediately. □

**Claim 3:** If $M_{n-1} \in \mathcal{U}_\beta^{(J)}$ and $\mathrm{rk}(M_{n-1}) = n-1$, then

$$\max_{a \in \mathcal{F}_p} \mathbb{P}\Big(\big\{z_I \cdot w_I = a\big\} \cap \big\{z \neq 0\big\} \;\big|\; M_{n-1}\Big) \leq 2^{|J|}\beta.$$

*Proof.* [Proof of Claim 3] Recall that $w_J$ and $M_{n-1}$ together determine $z$, and that the entries of $w_I$ are independent of $w_J$, and observe that $\rho_{1/2}(z_I) = \max_{a \in \mathcal{F}_p} \mathbb{P}\big(z_I \cdot w_I = a\big)$. Therefore

$$\mathbb{P}\Big(\big\{z_I \cdot w_I = a\big\} \cap \big\{z \neq 0\big\} \,\big|\, M_{n-1}\Big) \leq \mathbb{E}\left[\rho_{1/2}(z_I)\mathbb{1}\big[z \neq 0\big] \;\middle|\; M_{n-1}\right]$$

for every $a \in \mathcal{F}_p$, where the expectation is over the choice of $w_J$. Now, by Lemma 2.5.7,

$$\rho_{1/2}(z_I) \leq \rho(z_I) \leq 2^{|J|}\rho(z).$$

Since $M_{n-1} \in \mathcal{U}_\beta^{(J)}$ and $M_{n-1} \cdot z = w_J^* \in W(J)$, if $z \neq 0$ then $\rho(z) \leq \beta$. It follows that

$$\mathbb{E}\left[\rho_{1/2}(z_I)\mathbb{1}\big[z \neq 0\big] \;\middle|\; M_{n-1}\right] \leq 2^{|J|}\beta,$$

as claimed. □

By Claims 1, 2 and 3, it follows that

$$\mathbb{E}\left[\max_{a \in \mathcal{F}_p} \mathbb{P}\big(z_I \cdot w_I = a \,\big|\, M_{n-1}\big)^{1/4} \mathbb{1}\big[\mathrm{rk}(M_{n-1}) = n-1\big]\right] \leq \left(2^{|J|}\beta + 2^{-|J|}\right)^{1/4} + 3^{|J|} q_{n-1}(\beta),$$

and, as noted above, this completes the proof of Lemma 2.5.4. □

Combining Lemmas 2.5.1, 2.5.2 and 2.5.4, we obtain Lemma 2.2.1.

*Proof.* [Proof of Lemma 2.2.1] Observe first that $q_n(\beta) \geq 2^{-n}$ for every $\beta < 1/2$ (to see this, set $v = (1, 0, \ldots, 0)$), so the claimed bound holds trivially if $\beta > n^{-1}$ or $\beta < 2^{-n}$. We may therefore assume that $k := \lfloor \log_4(1/\beta) \rfloor$ satisfies $1 \leq k \leq n-2$, and therefore, by Lemmas 2.5.1, 2.5.2 and 2.5.4, we obtain

$$\begin{aligned}\mathbb{P}\big(\det(A_n) = 0\big) &\leq 4n \sum_{m=n}^{2n-2} \Big(\beta + q_{m-1}(\beta) + 2 \cdot \big(3\beta^{1/2}\big)^{1/4} + \beta^{-1} q_{m-1}(\beta)\Big) \\ &\leq 16n \sum_{m=n-1}^{2n-3} \left(\beta^{1/8} + \frac{q_m(\beta)}{\beta}\right).\end{aligned}$$

as required. □

## 2.6 Halász's Anticoncentration Lemma

In this section we will provide, for completeness, a proof of Lemma 2.2.3, which is due to Halász [48]. Let us fix a prime $p > 3$ and an integer $n \in \mathbb{N}$; the first step is the following bound on $\rho(v)$. Recall that $\|\cdot\|$ denotes the distance to the nearest integer.

**Lemma 2.6.1.** *For every $v \in \mathbb{Z}_p^n$,*

$$\rho(v) \leq \frac{1}{p} \cdot \sum_{k \in \mathbb{Z}_p} \exp\left(-\sum_{j=1}^{n} \left\| \frac{k \cdot v_j}{p} \right\|^2\right). \tag{2.17}$$

*Proof.* We need to bound, for each $a \in \mathbb{Z}_p$, the probability that $u \cdot v = a$, where $u$ is chosen uniformly at random from $\{-1, 1\}^n$. The first step is to rewrite this probability as

$$\mathbb{P}\big(u \cdot v = a\big) = \frac{1}{p} \cdot \sum_{k \in \mathbb{Z}_p} \mathbb{E}\left[\exp\left(\frac{2\pi i \cdot (u \cdot v - a)k}{p}\right)\right],$$

using the fact that $\sum_{k \in \mathbb{Z}_p} \exp\big(2\pi i \cdot xk/p\big) = 0$ for every $x \in \mathbb{Z}_p \setminus \{0\}$. Now, noting that

$$\mathbb{E}\left[\exp\left(\frac{2\pi i \cdot u_j v_j k}{p}\right)\right] = \frac{1}{2}\Big(e^{2\pi i k v_j/p} + e^{-2\pi i k v_j/p}\Big) = \cos\left(\frac{2\pi k \cdot v_j}{p}\right)$$

for each $k \in \mathbb{Z}_p$ and $j \in [n]$, and recalling that the $u_j$ are independent, it follows that

$$\begin{aligned}\mathbb{P}\big(u \cdot v = a\big) \;&=\; \frac{1}{p} \cdot \sum_{k \in \mathbb{Z}_p} \exp\bigg(-\frac{2\pi i \cdot a \cdot k}{p}\bigg) \prod_{j=1}^{n} \cos\bigg(\frac{2\pi k \cdot v_j}{p}\bigg) \\ &\leq\; \frac{1}{p} \cdot \sum_{k \in \mathbb{Z}_p} \prod_{j=1}^{n} \bigg|\cos\bigg(\frac{\pi k \cdot v_j}{p}\bigg)\bigg|,\end{aligned}$$

where we used the fact that $\{2k : k \in \mathbb{Z}_p\} = \mathbb{Z}_p$.

Finally, using the inequality $\big|\cos(\pi x/p)\big| \leq \exp\big(-\|x/p\|^2\big)$, we obtain

$$\rho(v) = \max_{a \in \mathbb{Z}_p} \mathbb{P}\big(u \cdot v = a\big) \leq \frac{1}{p} \cdot \sum_{k \in \mathbb{Z}_p} \exp\bigg(-\sum_{j=1}^{n} \bigg\|\frac{k \cdot v_j}{p}\bigg\|^2\bigg),$$

as claimed. □

We next rewrite the right-hand side of (2.17) in terms of the level sets $T_t(v)$.

**Lemma 2.6.2.** *For every $v \in \mathbb{Z}_p^n \setminus \{0\}$ and $\ell \geq 1$,*

$$\rho(v) \leq \frac{1}{p} + \frac{e}{p} \sum_{t=1}^{\lceil \ell \rceil} e^{-t} \big|T_t(v)\big| + e^{-\ell}. \tag{2.18}$$

*Proof.* By Lemma 2.6.1 and the definition (2.6) of $T_t(v)$, we have

$$\rho(v) \leq \frac{1}{p}\bigg(|T_0(v)| + \sum_{t=1}^{n} \big|T_t(v) \setminus T_{t-1}(v)\big| \cdot e^{-(t-1)}\bigg).$$

Now observe that $T_0(v) = \{0\}$, since $v \neq 0$, and therefore

$$\rho(v) \;\leq\; \frac{1}{p} + \frac{e}{p} \sum_{t=1}^{\lceil \ell \rceil} e^{-t} \big|T_t(v)\big| + e^{-\ell}$$

for any $\ell \geq 1$, as required. □

In order to deduce Lemma 2.2.3 from Lemma 2.6.2, we will need the following simple lemma.

**Lemma 2.6.3.** *For any $m \in \mathbb{N}$ and $t \geq 0$, and any vector $v \in \mathbb{Z}_p^n$,*

$$m \cdot T_t(v) \subset T_{m^2 t}(v)$$

*where $m \cdot T$ denotes the $m$-fold sumset of a set $T$.*

*Proof.* For each $a_1, \dots a_m \in T_t(v)$, we have

$$\sum_{k=1}^{n} \left\| \sum_{j=1}^{m} \frac{a_j \cdot v_k}{p} \right\|^2 \leq \sum_{k=1}^{n} \left( \sum_{j=1}^{m} \left\| \frac{a_j \cdot v_k}{p} \right\| \right)^2 \leq m \sum_{j=1}^{m} \sum_{k=1}^{n} \left\| \frac{a_j \cdot v_k}{p} \right\|^2 \leq m^2 t$$

by the triangle inequality for $\| \cdot \|$, convexity, and the definition of $T_t(v)$. $\square$

Finally, we will need the Cauchy–Davenport theorem.

**Lemma 2.6.4.** *Let $m \in \mathbb{N}$, let $p$ be a prime, and let $A \subset \mathbb{Z}_p$ be such that $m \cdot A \neq \mathbb{Z}_p$. Then*

$$|m \cdot A| \geq m|A| - m + 1.$$

We are now ready to prove Halász's Anticoncentration Lemma.

*Proof.* [Proof of Lemma 2.2.3] Let $v \in \mathbb{Z}_p^n \setminus \{0\}$, and let $1 \leq t \leq \ell \leq 2^{-6}|v|$. We claim first that $|T_\ell(v)| < p$. To see this, let $a$ be a uniformly-chosen random element of $\mathbb{Z}_p$, and note that for each fixed $k \in \mathbb{Z}_p \setminus \{0\}$ we have $\mathbb{P}\big(\|a \cdot k/p\| \geq 1/4\big) > 1/4$, and therefore

$$\mathbb{E}\left[ \sum_{i=1}^{n} \left\| \frac{a \cdot v_i}{p} \right\|^2 \right] > \frac{|v|}{2^6}. \tag{2.19}$$

Since $\ell \leq 2^{-6}|v|$, it follows that there exists $k \in \mathbb{Z}_p$ with $k \notin T_\ell(v)$, as claimed.

Now, by Lemma 2.6.3, applied with $m := \lfloor \sqrt{\ell/t} \rfloor \geq \sqrt{\ell}/(2\sqrt{t})$, and by the definitions of $T_t(v)$ and $|v|$, we have

$$|m \cdot T_t(v)| \leq |T_{m^2 t}(v)| \leq |T_\ell(v)|.$$

By the Cauchy–Davenport theorem, it follows that $|m \cdot T_t(v)| \geq m\big(|T_t(v)| - 1\big)$, and hence

$$|T_t(v)| \leq 1 + \frac{|T_\ell(v)|}{m} \leq 1 + 2\sqrt{\frac{t}{\ell}} \cdot |T_\ell(v)|.$$

Combining this with Lemma 2.6.2, we obtain

$$\rho(v) \leq \frac{3}{p} + \frac{2e}{p} \cdot \frac{|T_\ell(v)|}{\sqrt{\ell}} \sum_{t=1}^{\lceil \ell \rceil} \sqrt{t} e^{-t} + e^{-\ell} \leq \frac{3}{p} + \frac{4|T_\ell(v)|}{p\sqrt{\ell}} + e^{-\ell},$$

as claimed. $\square$

CHAPTER 3

# CLIQUE PACKINGS IN RANDOM GRAPHS

The work in this chapter is joint with Griffiths and Morris. It represents a work in progress.

## 3.1 Introduction

For any $n \in \mathbb{N}$ and $p \in (0,1)$, let $k_0 = k_0(n,p)$ be the minimum $k$ such that

$$\binom{n}{k} p^{\binom{k}{2}} < 1.$$

Using Stirling expansions as in [13], we obtain that $k_0$ is of the form $\lceil \eta_0 + o(1) \rceil$, where

$$\eta_0 := 2\log_{1/p} n - 2\log_{1/p}\log_{1/p} n + 2\log_{1/p} e + 1.$$

It is known that the largest clique in $G(n,p)$ has size either $k_0$ or $k_0 - 1$ with high probability (see [82, 83, 13]).

In this chapter, we are interested in *packings* of nearly maximum cliques in $G(n,p)$. We say that a collection of cliques forms a *packing* if all the cliques in this collection are edge-disjoint. Let $\nu_p(k)$ be the maximum number of edge-disjoint copies of $k$-cliques in $G(n,p)$, that is, the maximum size of a $k$-clique packing in $G(n,p)$. In the analysis of the quantity $\nu_p(k)$, an important role is played by the real number $\gamma = \gamma(n,p,k)$ such that the expected number of $k$-cliques is of the form $n^{\gamma + o(1)}$. Formally, $\gamma$ is defined as

$$\gamma(n,p,k) := \eta_0 - k.$$

For this definition of $\gamma$, we can check that the expected number of $k$-cliques in $G(n,p)$ is $n^{\gamma+o(1)}$.

Our main result in this chapter is a lower bound on $\nu_p(k)$ of the same order of magnitude as the upper bound on $\nu_p(k)$ obtained by Acan and Kahn [3].

**Theorem 3.1.1.** *Let $\gamma > 2$ and $p \in (0,1)$ be constants and $k = \eta_0 - \gamma$. With high probability, we have*

$$\nu_p(k) \geq \frac{\min\{\gamma - 2, 1\} p n^2 \log n}{40 k^4}.$$

The bulk of this chapter is devoted to prove Theorem 3.1.1. We consider a random process which starts with $G(n,p)$ and at each step we remove an uniformly random $k$-clique. It suffices to prove that the $k$-clique process lasts at least $\min\{\gamma - 2, 1\} p n^2 \log n / 40 k^4$ steps with high probability. To prove this, we track the number of $k$-cliques remaining in the graph and the number of $k$-cliques containing each edge. To control these variables, we apply the differential equations method.

We also establish a general upper bound on $\nu_p(k)$ using a technique which is simple and completely different from that of Acan and Kahn [3]. Moreover, our upper bound on $\nu_p(k)$ improves Acan and Kahn's result for some ranges of $k$ and $p$, and also disproves the Alon–Spencer packing conjecture.

**Theorem 3.1.2.** *Let $p \in (0,1)$ be a constant, $\gamma > 2$ and $k = \eta_0 - \gamma$. With high probability, we have*

$$\nu_p(k) \leq \frac{5(\gamma - 2)}{1 - p} \cdot \frac{p n^2 \log n}{k^4}.$$

When $\gamma \in (2,3)$, Theorem 3.1.2 almost confirms that Theorem 3.1.1 is best possible up to an absolute constant. However, $(1-p)^{-1}$ blows up as $p$ approaches 1. Our next theorem removes the factor of $(1-p)^{-1}$ from the upper bound in Theorem 3.1.2 in the case where $\gamma \in (2,3)$. The proof combines Theorem 3.1.2 with a theorem of Acan and Kahn [3].

**Theorem 3.1.3.** *Let $p \in (0,1)$ and $\gamma \in (2,3)$ be constants and $k = \eta_0 - \gamma$. There exists an absolute constant $C > 0$ for which*

$$\nu_p(k) \leq C(\gamma - 2) \cdot \frac{p n^2 \log n}{k^4}$$

*with high probability.*

The rest of this chapter is divided as follows: in Section 3.2, we give an overview of the proof of Theorem 3.1.1, in Section 3.3 we establish some concentration inequalities for the number of $k$-cliques in $G(n,p)$ and related quantities, in Sections 3.4 and 3.5 we track the number of cliques and the number of cliques per edge in the random process, respectively. Finally, in Section 3.6 we prove Theorems 3.1.2 and 3.1.3, which concerns the upper bounds on $\nu_p(k)$.

## 3.2 Overview of the proof

Consider a random process which starts with $G_0 \sim G(n,p)$ and at each step removes a uniformly random $k$-clique. We write $G_m$ for the graph obtained after $m$ such $k$-cliques have been removed. The key to the proof is to keep track of $Q(G_m)$, which we define to be the number of $k$-cliques remaining in the graph $G_m$. As long as $Q(G_m)$ is positive the process may continue. We shall in fact prove that $Q(G_m)$ stays close to

$$\exp\left(-\frac{k^4 m}{2pn^2}\right)\mathbb{E}(Q(0)).$$

To control the behaviour of $Q(G_m)$ and see why $Q(G_m)$ should to be close to the expression above, we must understand how many cliques are destroyed at each step. This leads us to consider for each edge $e \in E(G_m)$ the number of cliques which contain this edge. More generally, for any edge $e \in E(K_n)$ we define $Y_e(G_m)$ to be the number of $k$-cliques in $G_m \cup \{e\}$ containing the edge $e$. By a double-counting argument, we can see that the average value of $Y_e(G_m)$ over $e \in G_m$ is

$$\binom{k}{2}\frac{Q(G_m)}{e(G_m)}.$$

We shall prove that for all $e \in G_m$ the variable $Y_e(G_m)$ stays close to the average value. In particular, this implies that we expect to destroy

$$\binom{k}{2}^2 \frac{Q(G_m)}{e(G_m)} \approx \frac{k^4}{2pn^2} \cdot Q(G_m)$$

$k$-cliques when we remove the $(m+1)$-th clique of the process, and hence

$$\begin{aligned} Q(G_{m+1}) &\approx \left(1 - \frac{k^4}{2pn^2}\right) \cdot Q(G_m) \\ &\approx \exp\left(-\frac{k^4 m}{2pn^2}\right) \mathbb{E}(Q(G_0)). \end{aligned}$$

As we expect the process to continue as long as $k^4 m/(2pn^2) < (\gamma - 2)\log n$ (recall that $\mathbb{E}(Q(G_0)) = n^{\gamma + o(1)}$), we obtain a collection of roughly $\Theta(\gamma p n^2 (\log n)/k^4)$ edge-disjoint $k$-cliques.

We now formalise our idea via the differential equations method. Define

$$\delta := \min\{\gamma - 2, 1\}/10 \qquad \text{and} \qquad m_* := \lfloor \delta p n^2 \log n / 4k^4 \rfloor. \tag{3.1}$$

By simplicity, we omit the dependencies of these variables on $\gamma$, $p$ and $k$. For every $m \le m_*$, we expect to destroy about $\binom{k}{2}^2 Q(G_m)/e(G_m)$ cliques of size $k$ in $G_m$. This motivates the following definition of the expected trajectory of $Q$:

$$\widetilde{Q}(m) \;:=\; \widetilde{Q}(0) \prod_{i=0}^{m-1} \left(1 \,-\, \frac{\binom{k}{2}^2}{e(G_0) - i\binom{k}{2}}\right) \;\approx\; \widetilde{Q}(0) \exp\left(-\binom{k}{2}^2 \sum_{i=0}^{m-1} \frac{1}{e(G_0) - i\binom{k}{2}}\right), \tag{3.2}$$

where $\widetilde{Q}(0) \coloneqq \mathbb{E}(Q(0))$. We remark that $e(G_m) = e(G_0) - m\binom{k}{2}$. The allowed relative error for $Q(G_m)$ is defined as

$$g_Q(m) \;:=\; 2n^{-\delta} \prod_{i=0}^{m-1} \left(1 \,+\, \frac{\binom{k}{2}^2}{e(G_0) - i\binom{k}{2}}\right) \;\approx\; 2n^{-\delta} \exp\left(\binom{k}{2}^2 \sum_{i=0}^{m-1} \frac{1}{e(G_0) - i\binom{k}{2}}\right). \tag{3.3}$$

Our next theorem shows that $Q(G_m)$ is very close to its expected trajectory for all $m \le m_*$. Below, the notation $x = a \pm b$ stands for $x \in [a - b, a + b]$.

**Theorem 3.2.1.** *Let $\gamma > 2$ and $p \in (0,1)$ be constants and $k = \eta_0 - \gamma$. Consider the $k$-clique removal process $(G_m)_{m\geq 0}$ with random initial graph $G_0 \sim G(n,p)$. With high probability, we have*

$$Q(G_m) \,\in\, \widetilde{Q}(m)\,\big(1 \pm g_Q(m)\big)$$

*for all $m \leq m_*$.*

Theorem 3.1.1 is easily deduced from Theorem 3.2.1.

*Proof.* [Proof of Theorem 3.1.1, assuming Theorem 3.2.1] The $k$-cliques which are removed in the random process are all edge-disjoint. Thus, it suffices to show that

$$\widetilde{Q}(m_*)(1 - g_Q(m_*)) > 0. \tag{3.4}$$

To see why (3.4) holds, first note that $e(G_0) = pn^2 \pm n^{3/2}$ with high probability, by Chernoff's inequality[1]. This implies that the error $g_Q(m_*)$ is bounded by

$$\begin{aligned} g_Q(m_*) &\leq 2n^{-\delta} \exp\left(\frac{k^4 m_*}{pn^2}\right) \\ &\leq 2n^{-3\delta/4} \end{aligned} \tag{3.5}$$

with high probability. By (3.2), we also have

$$\begin{aligned} \widetilde{Q}(m_*) &\geq n^{\gamma + o(1)} \exp\left(-\frac{k^4 m_*}{pn^2}\right) \\ &\geq n^{\gamma - \delta/4 + o(1)}. \end{aligned} \tag{3.6}$$

Combining (3.5) and (3.6) we have (3.4). □

[1]Let $X$ be the sum of independent and identically distributed Bernoulli random variables. Chernoff's inequality states that $\mathbb{P}\big(|X - \mathbb{E}(X)| > \varepsilon\,\mathbb{E}(X)\big) \leq \exp\big(-\varepsilon^2\,\mathbb{E}(X)/4\big)$ for all $\varepsilon \in (0,1)$.

To show that $Q(G_m)$ stays close to its expected trajectory $\widetilde{Q}(m)$, we need to understand the behaviour of $Y_e(G_m)$ for each $e \in E(K_n)$. Recall that $Y_e(G_m)$ is the number of $k$-cliques in $G_m \cup \{e\}$ containing the edge $e$. The expected trajectory of these variables is defined as

$$\widetilde{Y}(m) := \binom{k}{2} \frac{\widetilde{Q}(m)}{e(G_m)}, \tag{3.7}$$

and the allowed relative error for each $Y_e(G_m)$ is given by

$$g_Y(m) \,:=\, 10n^{-\delta} \prod_{i=0}^{m-1} \left(1 \,+\, \frac{2\binom{k}{2}^2}{e(G_0) - i\binom{k}{2}}\right) \,\approx\, 10n^{-\delta} \exp\left(2\binom{k}{2}^2 \sum_{i=0}^{m-1} \frac{1}{e(G_0) - i\binom{k}{2}}\right). \tag{3.8}$$

Similarly to Theorem 3.2.1, we show that the trajectory of $Y_e(G_m)$ stays very close to its expected trajectory $\widetilde{Y}(m)$ for all $e \in E(K_n)$ and $m \le m_*$.

**Theorem 3.2.2.** *Let $\gamma > 2$ and $p \in (0,1)$ be constants and $k = \eta_0 - \gamma$. Consider the $k$-clique removal process $(G_m)_{m \ge 0}$ with random initial graph $G_0 \sim G(n,p)$. With high probability, we have*

$$Y_e(G_m) \,\in\, \widetilde{Y}(m)\big(1 \pm g_Y(m)\big)$$

*for all $e \in E(K_n)$ and $m \le m_*$.*

### 3.2.1 An outline of the proofs of Theorems 3.2.1 and 3.2.2

The first step to prove Theorems 3.2.1 and 3.2.2 is to control the initial random variables $e(G_0)$, $Q(G_0)$ and $Y_e(G_0)$ for all $e \in E(K_n)$. To do so, we also need to bound for each set $S$ of size 3 the number of $k$-cliques in $G_0 \cup \binom{S}{2}$ containing $S$, which we denote by $Y_S(G_0)$.

In the table below, we place in the first column the variables we need to control in the first step; in the second column we place the bounds we shall prove on the initial behaviour;

| Random variable | Required initial behaviour | Failure event |
|---|---|---|
| $Q(G_0)$ | $Q(G_0) \in \widetilde{Q}(0)(1 \pm n^{-\delta})$ | $F_0^Q$ |
| $Y_e(G_0)$ | $Y_e(G_0) \in \widetilde{Y}(0)(1 \pm n^{-\delta})$ | $F_0^{Y_e}$ |
| $Y_S(G_0)$ | $Y_S(G_0) \leq n^{\delta} \max\{1, \mathbb{E}(Y_S(G_0))\}$ | $F_0^{Y_S}$ |
| $e(G_0)$ | $e(G_0) \in p\binom{n}{2} \pm n^{3/2}$ | $F^{edge}$ |

Table 3.1: Table of failure events

and in the third column we place the notation used for the complementary event of the required initial behaviour.

Note that there is a failure event $F_0^{Y_e}$ for each $e \in E(K_n)$ and a failure event $F_0^{Y_S}$ for each set $S$ of three vertices. In each case, the *failure event* is the event that the required behaviour is *not* satisfied. Let

$$F_0 := F_0^Q \cup \bigcup_{e \in E(K_n)} F_0^{Y_e} \cup \bigcup_{S \subseteq [n] : |S| = 3} F_0^{Y_S} \cup F^{edge} \tag{3.9}$$

be the event that some initial random variable does not satisfy its required initial behaviour. We prove the following Lemma in Section 3.3.

**Lemma 3.2.3.** $\mathbb{P}(F_0) = O(n^{-1})$.

Once we have controlled the initial random variables, we consider the task of showing that the variables $Q(G_m)$ and $Y_e(G_m)$ remain in their respective allowed intervals for all $m = 1, \ldots, m_*$. To accomplish this task, it is convenient to define some stopping times. Define

$$\tau_Q := \min\Big\{m \,:\, Q(G_m) \notin \widetilde{Q}(m)\big(1 \pm g_Q(m)\big)\Big\} \tag{3.10}$$

and for each $e \in E(K_n)$, define

$$\tau_{Y_e} := \min\Big\{m \,:\, Y_e(G_m) \notin \widetilde{Y}(m)\big(1 \pm g_Y(m)\big)\Big\}. \tag{3.11}$$

It is also useful to set

$$\tau_Y := \min\big\{\tau_{Y_e} : e \in E(K_n)\big\} \qquad \text{and} \qquad \tau := \min\big\{\tau_Q, \tau_Y, m_*\big\}. \tag{3.12}$$

To prove both Theorems 3.2.1 and 3.2.2, it suffices to show that $\tau = m_*$ with high probability. As $\tau > 0$ with high probability (by Lemma 3.2.3), it remains to show that both events

$$0 < \tau = \tau_Q < m_* \qquad \text{and} \qquad 0 < \tau = \tau_Y < m_*$$

are very unlikely. Section 3.4 is devoted to prove the following lemma.

**Lemma 3.2.4.** $\mathbb{P}\big(0 < \tau = \tau_Q < m_*\big) \to 0$

In Section 3.5, we prove the corresponding lemma for the stopping time $\tau_Y$.

**Lemma 3.2.5.** $\mathbb{P}\big(0 < \tau = \tau_Y < m_*\big) \to 0\,.$

The proofs of Theorems 3.2.1 and 3.2.2 can be easily deduced from Lemmas 3.2.3, 3.2.4 and 3.2.5. We omit the details.

### 3.2.2 The method of proof and concentration inequalities

Now that we have given an overview of the structure of the proof, let us say something about the methods used. In Section 3.3, we must prove inequalities related to the random variables $Q(G_0), Y_e(G_0)$ and $Y_S(G_0)$ in the random graph $G_0 \sim G(n,p)$. We begin by proving rough bounds on these variables up to a factor of $n^\delta$ using the moment method (effectively Markov's inequality applied to a large power of the random variable). These rough bounds are already sufficient for $Y_S(G_0)$, for all sets $S$ of size 3. To bound the upper tails of $Q(G_0)$ and $Y_e(G_0)$, we use the deletion method [57, 58] together with our rough bounds. For the lower tail, we simply use Janson's inequality.

For the convenience of the reader, we state here the bound on the upper tail derived from the deletion method [57, 58]. Before that, we need a little notation. For each set $S \subseteq [n]$ and each graph $G$, define $Z_S(G)$ to be the number of $k$-cliques in $G$ containing $S$. Note that $Z_S\big(G_0 \cup \binom{S}{2}\big) = Y_S(G_0)$, where $\binom{S}{2}$ denotes the family of sets of size 2 in $S$. Set

$$Y_S^*(G_0) := \max_{v \in [n]\setminus S} Z_{S\cup\{v\}}\left(G_0 \cup \binom{S}{2}\right).$$

In our setting, the deletion lemma can be stated as follows.

**Lemma 3.2.6.** *Let $p \in (0,1)$, $G_0 \sim G(n,p)$ and $S \subseteq [n]$. For every $\varepsilon \in (0,1)$ and every $a, k > 0$ we have*

$$\mathbb{P}\Big(Y_S(G_0) \geq (1+\varepsilon)\,\mathbb{E}\left(Y_S(G_0)\right)\Big) \leq \exp\left(-\frac{\varepsilon a}{3k^2}\right) + \mathbb{P}\left(Y_S^*(G_0) > \frac{\varepsilon\,\mathbb{E}\left(Y_S(G_0)\right)}{2a}\right).$$

Janson's inequality can be stated as follows.

**Lemma 3.2.7** (Janson's inequality)**.** *Let $p \in (0,1)$ and $(E_i)_{i\in[\ell]}$ be a sequence of increasing events in $G(n,p)$. Let*

$$X = \sum_{i\in[\ell]} 1_{E_i} \qquad \text{and} \qquad \Delta = \sum_{(i,j):\, i\sim j} \mathbb{P}\big(E_i \cap E_j\big),$$

*where the sum in $\Delta$ is over ordered pairs of distinct dependent events. For any $0 \leq t \leq \mathbb{E}(X)$, we have*

$$\mathbb{P}\big(X \leq \mathbb{E}(X) - t\big) \leq \exp\left(-\frac{t^2}{2(\mathbb{E}(X)+\Delta)}\right).$$

To prove Lemmas 3.2.4 and Lemma 3.2.5, we need to show that the probability that the variables $Q(G_m)$ and $Y_e(G_m)$ deviate from their expected trajectories goes to zero. We shall control these probabilities using supermartingales[2] and related inequalities. In particular, we

[2] $(X_i)_{i=0}^m$ is a supermartingale with respect to a filtration $(\mathcal{F}_i)_{i=0}^m$ if $\mathbb{E}(X_i|\mathcal{F}_{i-1}) \leq X_{i-1}$ for all $i \in [m]$. A filtration is a sequence of $\sigma$-algebras $(\mathcal{F}_i)_{i=0}^m$ such that $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \ldots \subseteq F_m$.

use the well-known Hoeffding–Azuma inequality [5, 49] to control the trajectory of $Q(G_m)$. To control $Y_e(G_m)$ we shall need Freedman's inequality, which is slightly more refined.

Let $(X_i, \mathcal{F}_i)_{i=0}^m$ be a random discrete process. We say that $(X_i, \mathcal{F}_i)_{i=0}^m$ is a *supermartingale under an event* $A$ if $\mathbb{E}\big(X_i \,|\, \mathcal{F}_{i-1}\big)1_A \leq X_{i-1}1_A$ for every $i \in [m]$. A slightly more general version of Hoeffding–Azuma inequality can be stated as follows.

**Lemma 3.2.8** (Hoeffding–Azuma inequality)**.** *Let $(X_i, \mathcal{F}_i)_{i=0}^m$ be a supermartingale under an event $A$, with bounded increments. That is, for every $i \in [m]$ we have $|X_i - X_{i-1}|1_A \leq c_i$ for some real number $c_i$. Then, for every $t \geq 0$ we have*

$$\mathbb{P}\big(\big\{X_m - X_0 \,\geq\, t\big\} \cap A\big) \,\leq\, \exp\left(\frac{-t^2}{2\sum_{i=1}^m c_i^2}\right).$$

When the deterministic bounds on the increments of a supermartingale are very rough, Hoeffding–Azuma inequality gives a weak bound. However, when a supermartingale $(X_i)_{i=0}^m$ has increments $|X_i - X_{i-1}|$ which are typically much smaller than $\|X_i - X_{i-1}\|_\infty$, Freedman's inequality [38] gives a better bound. This will be exactly the case when we deal with the supermartingales associated with the variables $Y_e(G_m)$.

**Lemma 3.2.9** (Freedman's inequality)**.** *Let $(X_i, \mathcal{F}_i)_{i=0}^m$ be a supermartingale under an event $A$. Let $R \in \mathbb{R}$ be such that $\max_i |X_i - X_{i-1}|1_A \leq R$. Let $V(m)$ be the quadratic variation of the process under $A$ until step $m$, that is,*

$$V(m) \,:=\, \sum_{i=1}^m \mathbb{E}\left((X_i - X_{i-1})^2 \big| \mathcal{F}_{i-1}\right)1_A.$$

*Then, for every $t, s > 0$ we have*

$$\mathbb{P}\Big(X_m - X_0 \geq t,\, V(m) \leq s \text{ and } A\Big) \,\leq\, \exp\left(\frac{-t^2}{2(s + Rt)}\right).$$

There are then two main challenges involved in applying Hoeffding–Azuma and Freedman's inequality to the random variables we wish to track:

(i) We must encode failure events as deviation event for supermartingales;

(ii) We must control the quadratic variation and give an almost sure bound for the magnitude of the increments of these supermartingales.

These details are covered in Sections 3.4 and 3.5. We remark that (i) is related to the (conditional) expected change of the random variable in question, and it is for this reason that some control of the $Y_e(G_m)$ is necessary to control $Q(G_m)$. In (ii) the maximum increments are again related to the one-step change in our random variables. This is why some control of $Y_S(G_m)$ for sets of size 3 is necessary to understand the evolution of the $Y_e(G_m)$. We do not do anything special to control the quadratic variation, we simply use information about the expected change and the maximum change to obtain a bound.

## 3.3 Initial values of the random variables

The main goal of this section is to prove Lemma 3.2.3, which states that the failure event

$$F_0 = F_0^Q \cup \bigcup_{e\in E(K_n)} F_0^{Y_e} \cup \bigcup_{S\subseteq[n]:|S|=3} F_0^{Y_S} \cup F^{edge}$$

occurs with probability at most $n^{-1}$. Recall the notation used for the failure events in Table 3.1. The failure event $F^{edge} = \left\{e(G_0) \notin p\binom{n}{2} \pm n^{3/2}\right\}$ is easy to bound: it is just a simple application of Chernoff's inequality. On the other hand, showing that none of the events $F_0^Q$, $F_0^{Y_e}$ and $F^{Y_S}$ occur is much more involved.

To bound the probability of the events $F_0^Q$, $F_0^{Y_e}$ and $F^{Y_S}$, we start by first bounding the moments of the random variables $Y_S(G_0)$ for every set $S$ of constant size. These bounds will be used together with Markov's inequality to a give rough bound on $Y_S(G_0)$. This will already allow us to bound $\mathbb{P}(F_0^{Y_S})$ effectively for all sets $S$ of size 3.

**Lemma 3.3.1.** *Let $\gamma > 2$, $p \in (0,1)$ and $\ell \in \mathbb{N}$ be constants, and $k = \eta_0 - \gamma$. For $G_0 \sim G(n,p)$ and $S \subseteq [n]$ of constant size, we have*

$$\mathbb{E}\left(Y_S(G_0)^\ell\right) \leq k^{O(1)}\Big(\max\Big\{\mathbb{E}\left(Y_S(G_0)\right), 1\Big\}\Big)^\ell.$$

For $|S| \in \{0,2\}$, Lemma 3.3.1 bounds the moments of the random variables $Q(G_0)$ and $Y_e(G_0)$. However, to prove that these variables are concentrated, and hence show that the events $F_0^Q$ and $F_0^{Y_e}$ are unlikely, we need a bit more. To bound the upper tails of $Q(G_0)$ and $Y_e(G_0)$ we shall use Lemma 3.3.1 combined with the deletion method (see Lemma 3.2.6). For the lower tails, we simply use Janson's inequality (see Lemm 3.2.7).

**Lemma 3.3.2.** *Let $\gamma > 2$ and $p \in (0,1)$ be constants, $k = \eta_0 - \gamma$ and $G_0 \sim G(n,p)$. Then, with probability at least $1 - n^{-2}$, we have*

$$Q(G_0) \in \left(1 \pm \frac{1}{n^\delta}\right)\mathbb{E}\left(Q(G_0)\right) \qquad \text{and} \qquad Y_e(G_0) \in \left(1 \pm \frac{1}{n^\delta}\right)\mathbb{E}\left(Y_e(G_0)\right)$$

*for all $e \in E(K_n)$.*

Lemma 3.2.3 is easily deduced from Lemmas 3.3.1 and 3.3.2.

*Proof.* [Proof of Lemma 3.2.3, assuming Lemmas 3.3.1 and 3.3.2] Let $S \subseteq [n]$ be any set of size 3. We first bound the probability that $Y_S > n^\delta \max\big\{\mathbb{E}(Y_S), 1\big\}$, which is the event $F_0^{Y_S}$. Set $\ell = \lceil 7\delta^{-1} \rceil$. By Markov's inequality combined with Lemma 3.3.1 we have

$$\begin{aligned}\mathbb{P}\big(F_0^{Y_S}\big) &\leq k^{O(1)} n^{-\delta\ell} \\ &\leq n^{-6}.\end{aligned}$$

From the last inequality it follows that

$$\mathbb{P}\left(\bigcup_{S:\,|S|=3} F_0^{Y_S}\right) \leq n^{-3}. \tag{3.13}$$

It is straightforward to bound the remaining failure events. Lemma 3.3.2 directly implies

$$\mathbb{P}\left(F_0^Q \cup \bigcup_{e\in E(K_n)} F_0^{Y_e}\right) \leq n^{-2}, \tag{3.14}$$

as $\mathbb{E}\left(Y_e(G_0)\right) = p^{\binom{k}{2}-1}\binom{n}{k-2} = \widetilde{Y}(0)$. Chernoff's inequality implies

$$\mathbb{P}\Big(\left|e(G_0) - \mathbb{E}\left(e(G_0)\right)\right| > n^{3/2}\Big) \leq \exp(-2^{-3}n). \tag{3.15}$$

Together, equations (3.13), (3.14) and (3.15) prove Lemma 3.2.3. □

The rest of this section is divided as follows. In Subsection 3.3.1 we prove Lemma 3.3.1 and in Subsection 3.3.2 we prove Lemma 3.3.2.

### 3.3.1 Proof of Lemma 3.3.1

Let $\gamma > 2$, $p \in (0,1)$ and $\ell \in \mathbb{N}$ be constants and $k = \eta_0 - \gamma$. Let $G_0 \sim G(n,p)$ and $S \subseteq [n]$ be a set of constant size. These parameters are fixed throughout the proof. By simplicity, we denote $s = |S|$ and $G_0^S = G_0 \cup \binom{S}{2}$.

First, we need a little preparation. Observe that we may express $Y_S = Y_S(G_0)$ a sum of indicator functions. We have $Y_S = \sum_K 1_{S\subseteq K\subseteq G_0^S}$, where the sum is over $k$-cliques in $K_n$ containing $S$. It follows that, for every $\ell \in \mathbb{N}$, we have

$$Y_S^\ell = \sum_{(K^1,\ldots,K^\ell)} 1_{\bigcup_{i=1}^\ell K^i \subseteq G_0^S},$$

where the sum is over $\ell$-sequences of $k$-cliques containing $S$. Taking the expectation on both sides of the equation above, and noting that each multi-set may be represented at most $\ell!$ times as a sequence, we also have that

$$\mathbb{E}\left(Y_S^\ell\right) \leq \ell! \sum_{\{K^1,\ldots,K^\ell\}} \mathbb{P}\left(\bigcup_{i=1}^\ell K^i \subseteq G_0^S\right), \tag{3.16}$$

where again the sum is over multi-sets of $k$-cliques containing $S$.

It is useful to have some control on the effect of adding a single $k$-clique to the multi-set, as stated in our next proposition. As we shall see, Proposition 3.3.3 will be sufficient to prove Lemma 3.3.1 in the case were $\gamma$ is a large constant depending on $p$, $s$ and $\ell$.

**Proposition 3.3.3.** *Let $\mathcal{K}$ be a multi-set of $k$-cliques containing the set $S$. If $|\mathcal{K}| = t$, then*

$$\sum_{K\colon S\subseteq K} \mathbb{P}\left(\bigcup \mathcal{K} \cup K \subseteq G_0^S\right) \leq 2\left(\binom{kt}{k} + \mathbb{E}\left(Y_S\right)\right)\mathbb{P}\left(\bigcup \mathcal{K} \subseteq G_0^S\right).$$

*Proof.* Let $F = \bigcup \mathcal{K}$ be the set of edges of the cliques in $\mathcal{K}$. Clearly, proving our lemma is equivalent to showing that

$$\sum_{K\colon S\subseteq K} \mathbb{P}\left(K \subseteq G_0^S \,\middle|\, F \subseteq G_0^S\right) \leq 2\binom{kt}{k} + 2\,\mathbb{E}\left(Y_S\right). \tag{3.17}$$

Observe that $F$ contains $S$ and is contained in a copy of the clique $K_{kt}$, as $v(F) \leq kt$. Without loss of generality, assume that the set of vertices in this copy of $K_{kt}$ is $\{1, 2, \ldots, kt\}$ and that $S = \{1, 2, \ldots, s\}$. Let $G_0^S(kt)$ be the subgraph of $G_0^S$ induced by the vertices $\{1, 2, \ldots, kt\}$. Now, instead of dealing with probabilities conditioned on the event $F \subseteq G_0^S$, we would like to condition on $G_0^S(kt) = K_{kt}$. This is possible because the events are increasing.

As the events $K \subseteq G_0^S$, $F \subseteq G_0^S$ and $G_0^S(kt) = K_{kt}$ are increasing, we have

$$\mathbb{P}\left(K \subseteq G_0^S \,\middle|\, F \subseteq G_0^S\right) \leq \mathbb{P}\left(K \subseteq G_0^S \,\middle|\, G_0^S(kt) = K_{kt}\right).$$

We then reduce the problem to bounding the quantity

$$B := \sum_{K\colon S\subseteq K} \mathbb{P}\left(K \subseteq G_0^S \,\middle|\, G_0^S(kt) = K_{kt}\right). \tag{3.18}$$

Grouping the sum in (3.18) according to the intersection of $K$ with $\{1, \ldots, kt\}$, we obtain

$$B \leq \sum_{i=s}^{k} \binom{kt}{i-s}\binom{n}{k-i} p^{\binom{k}{2}-\binom{i}{2}}.$$

By simplicity, denote by $a_i$ the $i$-th term in the sum above. Note that

$$\frac{a_{i+1}}{a_i} = \frac{kt-i+s}{i+1-s} \cdot \frac{k-i}{n-k+i+1} \cdot p^{-i}. \tag{3.19}$$

Next, we shall use (3.19) to conclude that $a_j = o(a_s + a_k)$ for all $s < j < k$.

Performing the multiplication of the quotients in (3.19) from $i$ going from $s$ to $j-1$, we obtain

$$\frac{a_j}{a_s} = O\left(\left(\frac{tk^2}{n}\right)^{j-s} \frac{p^{-\binom{j}{2}}}{(j-s)!}\right). \tag{3.20}$$

From (3.20), we can see that $a_j a_s^{-1} = O(k^2/n)$ whenever $j = O(1)$. When $2^4 s \le j \le k_0/4$, we have $p^{-\binom{j}{2}} \le n^{j/2}$ and, since $j$ is large, we obtain $a_j a_s^{-1} = O(k^2/n)$. When $j > k_0/4$, we have $(j-s)! \ge (2^{-5}k)^{j-s}$, and hence

$$\frac{a_j}{a_s} \le \left(\frac{Ck}{np^{j/2}}\right)^{j-s}, \tag{3.21}$$

where $C$ is some constant depending on $p, s$ and $t$. From (3.21), we obtain that $a_j a_s^{-1} = O(n^{-1/8})$ whenever $j > k_0/4$ and $p^{-j/2} \le n/(2Ck)$. It follows that $a_j a_s^{-1} = O(n^{-1/8})$ for all $k_0/4 \le j \le k_0 - D$, where $D$ is some constant depending on $p, s$ and $t$. Finally, when $k_0 - D \le j < k$, we can easily see from (3.19) that $a_j a_k^{-1} = O(n^{-1/2})$. Putting all the pieces together we obtain $a_j = o(a_s + a_k)$ for all $s < j < k$, and hence

$$Q \le 2a_s + 2a_k.$$

As $a_s = \mathbb{E}(Y_S)$ and $a_k = \binom{k\ell}{k-s}$, this proves our proposition. $\square$

If $\mathbb{E}(Y_S) = \Omega(\binom{k\ell}{k})$, then by inductively applying Proposition 3.3.3, we obtain $\mathbb{E}\left(Y_S^\ell\right) = O\big(\mathbb{E}(Y_S)\big)^\ell$, which is sufficient to complete the proof of Lemma 3.3.1. We indeed have $\mathbb{E}(Y_S) = \Omega(\binom{k\ell}{k})$ when $k$ is 'small'. As $\binom{k\ell}{k} \le n^{O_{p,\ell}(1)}$ and $\mathbb{E}(Y_S) = \Omega(n^C)$ whenever $k <$

$k_0-s-2C$, there exists a constant $D = D(p, s, \ell)$ such that $\mathbb{E}(Y_S) = \Omega(\binom{k\ell}{k})$ for all $k \leq k_0-D$. We may now assume that $k > k_0 - D$.

For $k$ 'large', the idea of the proof of Lemma 3.3.1 is as follows. We will consider two cases depending on the intersections between $k$-cliques in a multi-set. In one case we win enough in one step that we may use Proposition 3.3.3 for the remaining steps. In the other case we have extra information that allows us to argue more efficiently.

For each multi-set $\mathcal{K} = \{K^1, \dots K^t\}$ of $k$-cliques, we assume that its elements are ordered algorithmically as follows. In the $j$-th step, the intersection of $K^j$ with $K^1 \cup \cdots \cup K^{j-1}$ is maximal over the possible choices at that step. Given such ordering, we define the intersection sizes $(I_j)_{j=2}^t$ to be

$$I_j := \left| K^j \cap \bigcup_{i<j} K^i \right|.$$

Clearly $(I_j)_{j=2}^t$ depends on the multiset and its ordering, but we omit these dependencies to simplify the notation.

It is useful to classify a multi-set of $k$-cliques according to how 'clustered' their cliques are. Before doing so, it is convenient to define the following constant:

$$C := \frac{3\ell \log \ell}{\log(1/p)} + s. \tag{3.22}$$

This value of $C$ was taken just to guarantee that $\binom{k\ell}{\ell}^\ell \leq n^{C-s}$.

**Definition 3.3.4.** *A sequence $(I_2, \dots, I_j)$ is complex if $I_i \in \{C, \dots, k - C\}$, for some $i \in \{1, \dots, j\}$. Otherwise, we call it simple. Moreover, when a multi-set has a complex sequence of intersection sizes, we call it complex. Otherwise, we call it simple.*

We bound contributions to (3.16) from simple and complex multi-sets separately. When a multi-set $\mathcal{K}$ is complex, it means that there is some clique which is 'far' from being contained

in or disjoint from the union of previous cliques. This will allows us to win by a large factor on that step and hence conclude that the sum in (3.16) restricted over complex multi-sets is much smaller than $(\mathbb{E}(Y_S))^\ell$. When $\mathcal{K}$ is simple, every entry of $I_2, \dots, I_\ell$ is either *small* ($I_j < C$) or *large* ($I_j > k - C$). In this case, we gain due to the ordering we fixed on the multisets, which maximises the intersection sizes.

Given $\mathcal{I} = (I_2, \dots, I_j)$, we define $F(\mathcal{I})$ to be the family of multi-sets $\{K^1, \dots, K^j\}$ for which $S \subseteq V(K^i)$, for every $i \leq j$, and the sequence of intersection sizes is equal to $\mathcal{I}$. To bound the expected value of the number of multi-sets in $F(\mathcal{I})$ contained in $G_0$, we need the following two observations.

(i) Let $\mathcal{K} = \{K^1, \dots, K^j\}$ be a multi-set such that $I_j < C$. Then, at most $O(1)$ edges of $K^j$ are covered by previous cliques.

(ii) Let $(I_2, \dots, I_{j-1})$ be a simple sequence. Then,

$$\frac{F(I_2, \dots, I_j)}{F(I_2, \dots, I_{j-1})} \leq k^{O(1)} \binom{k + O(1)}{I_j} \binom{n}{k - I_j}.$$

While (i) is obvious, it takes a little thought to confirm (ii). Fix any sequence $(I_2, \dots, I_j)$ and define $j_-$ to be the largest index less than $j$ for which $I_{j_-} < C$. If such index does not exist, we simply set $j_- = 2$. We remark that $(I_2, \dots, I_{j-1})$ is simple but $(I_2, \dots, I_j)$ might not be, as we do not have any restrictions on $I_j$. Now, let $\mathcal{K} = \{K^1, \dots, K^j\}$ be any multi-set in $F(I_2, \dots, I_j)$. If $j_- > 2$, then the ordering guarantees that for all $t > j_-$ the clique $K^t$ has only $O(1)$ vertices in $\bigcup_{i<j_-} K^i$. In any case, we have at most $\binom{k\ell}{O(1)} = k^{O(1)}$ choices for the vertices of $K^j$ contained in this set. Moreover, as $(I_2, \dots, I_{j-1})$ is simple, we must have $I_t > k - C$ for all $j_- < t < j$. This implies that $|K^t \cap K^{j_-}| = k + O(1)$ for every $j_- \leq t < j$, and hence we deduce that $\bigcup_{j_- \leq i < j} K^i$ has cardinality $k + O(1)$. From this we obtain that there are at most $\binom{k+O(1)}{I_j}$ choices for the vertices of $K^j$ which are in $\bigcup_{j_- \leq i < j} K^i$. Since there

are at most $\binom{n}{k-I_j}$ choices for the vertices of $K^j$ outside the previous cliques, this proves item (ii).

Our next proposition bounds the contributions to (3.16) coming from simple multi-sets. Recall that we always assume that a multiset is ordered in a way that maximises the intersection sizes.

**Proposition 3.3.5.** *Let $\mathcal{F}_S$ be the family of simple multi-sets $\mathcal{K}$ satisfying $S \subset V(K^j)$, for every $K^j \in \mathcal{K}$, and $|\mathcal{K}| = \ell$. Then,*

$$\sum_{\mathcal{K}\in\mathcal{F}_S} \mathbb{P}\left(\bigcup \mathcal{K} \subseteq G_0^S\right) \le k^{O(1)}\Big(\max\big\{\mathbb{E}(Y_S),\, 1\big\}\Big)^{\ell}.$$

*Proof.* For each simple sequence $\mathcal{I} = (I_1, \dots, I_\ell)$, we define

$$t(\mathcal{I}) := |\{j : I_j < C\}| \qquad \text{and} \qquad q(\mathcal{I}) = \sum_{j:\, I_j > k-C} (k - I_j).$$

By (ii), it follows that

$$|F(\mathcal{I})| \le \binom{n}{k-s}^{t(\mathcal{I})} k^{O(1)} n^{q(\mathcal{I})}. \tag{3.23}$$

Let $\mathcal{K} = \{K^1, \dots, K^\ell\}$ be any multiset in $F(\mathcal{I})$. Let us now bound the probability that $\cup\mathcal{K} \subseteq G_0^S$. If $I_j > k - C$, then $K^j$ has at least $(k - I_j)(k - C)$ edges which are not in previous cliques. On the other hand, if $I_j < C$, then $K^j$ must contain at least $\binom{k}{2} - O(1)$ edges outside previous cliques. It follows that

$$\mathbb{P}\Big(\cup\,\mathcal{K} \subseteq G_0^S\Big) \le p^{t(\mathcal{I})\binom{k}{2} - O(1) + (k-C)q(\mathcal{I})}. \tag{3.24}$$

As the number of sequences $(I_2, \dots, I_\ell)$ is $O(1)$, it follows from (3.23) and (3.24) that

$$\sum_{\mathcal{K}\in\mathcal{F}_S} \mathbb{P}\left(\bigcup \mathcal{K} \subseteq G_0^S\right) \le k^{O(1)}\big(\mathbb{E}(Y_S)\big)^{t(\mathcal{I})} \cdot (np^{k-C})^{q(\mathcal{I})}.$$

As $np^k = o(n^{-1/2})$ and $\big(\mathbb{E}(Y_S)\big)^{t(\mathcal{I})} \le \big(\max\{\mathbb{E}(Y_S),\, 1\}\big)^{\ell}$, this proves our claim. $\square$

Now, it remains to bound the contributions to (3.16) coming from complex multi-sets (recall Definition 3.3.4). This is done in our next proposition.

**Proposition 3.3.6.** *Let $\mathcal{F}_C$ be the family of complex multi-sets $\mathcal{K}$ for which $S \subset V(K^j)$, for every $K^j \in \mathcal{K}$, and $|\mathcal{K}| = \ell$. Then,*

$$\sum_{\mathcal{K}\in\mathcal{F}_C} \mathbb{P}\left(\bigcup \mathcal{K} \subseteq G_0^S\right) \leq k^{O(1)}\Big(\max\big\{\,\mathbb{E}(Y_S),\,1\big\}\Big)^{\ell}.$$

*Proof.* For each complex multiset $\mathcal{K} \in \mathcal{F}_C$, let $j_0(\mathcal{K})$ be the first step $j$ for which $I_j \in \{C, \dots, k-C\}$. In order to bound the expected number of $\mathcal{K} \in F(\mathcal{I})$ such that $\cup\mathcal{K} \subseteq G_0^S$, we argue as in Proposition 3.3.5 (the simple case) when $j < j_0$, and as in Proposition 3.3.3 when $j > j_0$. Although they are not tight, these bounds are sufficient because we win a lot in step $j_0$.

Fix $j_0 \in [\ell]$. For each multiset $\mathcal{L}$ of size $j_0$, let $\mathcal{F}_C(\mathcal{L})$ be the set of complex multisets $\{K^1, \dots, K^\ell\}$ for which $\{K^1, \dots, K^{j_0}\} = \mathcal{L}$ (this also includes the ordering). By Proposition 3.3.3, we have

$$\sum_{\mathcal{K}\in\mathcal{F}_C(\mathcal{L})} \mathbb{P}\left(\bigcup \mathcal{K} \subseteq G_0^S\right) \leq \left(2\binom{kt}{k} + 2\,\mathbb{E}\left(Y_S\right)\right)^{\ell-j_0} \mathbb{P}\left(\mathcal{L} \subseteq G_0^S\right). \tag{3.25}$$

Now our aim is to bound $\sum_{\mathcal{L}} \mathbb{P}\left(\mathcal{L} \subseteq G_0^S\right)$, where the sum is over multisets $\mathcal{L} = \{K^1, \dots, K^{j_0}\}$ such that $\{K^1, \dots, K^{j_0-1}\}$ is simple. To do so, we group this sum according to sequences $(I_j)_{j\in[j_0]}$ of intersection sizes.

Let $\mathcal{I} = (I_j)_{j\in[j_0]}$ be a sequence such that $(I_j)_{j\in[j_0-1]}$ is simple. By (ii), we have

$$F(\mathcal{I}) \leq k^{O(1)}\binom{k+O(1)}{I_{j_0}}\binom{n}{k-I_{j_0}}F(I_2, \dots, I_{j_0-1}). \tag{3.26}$$

Now we observe that for any $\{K^1, \dots, K^{j_0}\} \in F(\mathcal{I})$, the clique $K^{j_0}$ has at least $\binom{k}{2} - \binom{I_j}{2}$ edges not included in previous cliques. Set

$$A(I_j) := k^{O(1)}\binom{k+O(1)}{I_j}\binom{n}{k-I_j}p^{\binom{k}{2}-\binom{I_j}{2}}.$$

Combining (3.26) and Proposition 3.3.5, it follows that

$$\sum_{\mathcal{K}\in F(\mathcal{I})} \mathbb{P}\left(\bigcup \mathcal{K} \subseteq G_0^S\right) \leq A(I_{j_0})\Big(\max\big\{\mathbb{E}(Y_S),\, 1\big\}\Big)^{j_0-1}. \tag{3.27}$$

Let us bound $\max_j A(I_j)$. Similarly as the analysis done in (3.19), (3.20) and (3.21), we infer that the maximum value of $A(I_j)$ in the range $I_j \in \{C, \ldots, k-C\}$ is achieved by $I_j = C$ or $I_j = k - C$. In either case, we obtain $\max_j A(I_j) \leq k^{O(1)} n^{-C+s}\, \mathbb{E}(Y_S)$.

Now we are ready to finish the proof. Let $\mathcal{F}_C^{j_0}$ be the set of complex multisets $\mathcal{K} \in \mathcal{F}_C$ for which $j_0(\mathcal{K}) = j_0$. As the number of intersection sequences $(I_1, \ldots, I_\ell)$ is $k^{O(1)}$, by (3.25) and (3.27) and the bound on $\max_j A(I_j)$ we have

$$\sum_{\mathcal{K}\in\mathcal{F}_C^{j_0}} \mathbb{P}\left(\bigcup \mathcal{K} \subseteq G_0^S\right) \;\leq\; \left(2\binom{kt}{k} + 2\,\mathbb{E}\left(Y_S\right)\right)^{\ell-j_0} n^{-C+s} k^{O(1)}\Big(\max\big\{\mathbb{E}(Y_S),\, 1\big\}\Big)^{j_0}.$$

Recall the definition of $C$ from (3.22). As $n^{C-s} \geq \binom{k\ell}{k}^{\ell}$, we obtain

$$\sum_{\mathcal{K}\in\mathcal{F}_C^{j_0}} \mathbb{P}\left(\bigcup \mathcal{K} \subseteq G_0^S\right) \;\leq\; k^{O(1)}\Big(\max\big\{\mathbb{E}(Y_S),\, 1\big\}\Big)^{\ell}.$$

We finish the proof by summing over $j_0 \in [\ell]$. $\square$

The sum of all the contributions from simple and complex multi-sets gives the total value of $\mathbb{E}\left(Y_S^\ell\right)$, which is at most $k^{O(1)}\Big(\max\big\{\mathbb{E}(Y_S),\, 1\big\}\Big)^{\ell}$. This finishes the proof Lemma 3.3.1.

### 3.3.2 Proof of Lemma 3.3.2

Let $\gamma > 2$ and $p \in (0,1)$ be constants, $k = \eta_0 - \gamma$ and $G_0 \sim G(n,p)$. If we prove that $Y_e(G_0)$ is concentrated for all $e \in E(K_n)$, then we automatically prove that $Q(G_0)$ is concentrated. In fact, we can write

$$\sum_{e\in E(G_0)} Y_e(G_0) = \binom{k}{2} Q(G_0).$$

If $Y_e(G_0) = (1 \pm n^{-2\delta})\,\mathbb{E}\big(Y_e(G_0)\big)$ for all $e \in E(K_n)$ and $e(G_0) = p\binom{n}{2} \pm n^{3/2}$, then we have

$$Q(G_0) = \left(1 \pm \frac{1}{n^{\delta}}\right) \mathbb{E}\big(Q(G_0)\big).$$

The last equality follows from the identity $\mathbb{E}\big(Q(G_0)\big)/\,\mathbb{E}\big(Y_e(G_0)\big) = p\binom{n}{2}/\binom{k}{2}$. Moreover, we do not lose much in assuming that $e(G_0) = p\binom{n}{2} \pm n^{3/2}$. By Chernoff's inequality, this event holds with probability at least $1 - \exp(-2^{-3}n)$.

First, let us fix $e \in E(K_n)$ and bound the lower tail of $Y_e(G_0)$ via Janson's inequality (see Lemma 3.2.7). Let $G_0^e = G_0 \cup \{e\}$ and, for each $k$-clique $K$ in $K_n$, let $I_K$ denote the indicator function of the event $K \subseteq G_0^e$. The variable $Y_e(G_0)$ can be written as

$$Y_e(G_0) = \sum_{K\colon e \subseteq K} I_K.$$

As these indicators are not all pairwise independent, we also need to consider

$$\Delta := \sum_{K \sim K'} \mathbb{E}(I_K I_{K'}),$$

where the sum is over ordered pairs of distinct $k$-cliques containing $e$ which share at least 3 vertices. By Janson's inequality (see Lemma 3.2.7), we have

$$\mathbb{P}\Big(Y_e \le \mathbb{E}(Y_e) - t\Big) \le \exp\left(-\frac{t^2}{2\big(\mathbb{E}(Y_e) + \Delta\big)}\right), \tag{3.28}$$

for all $t > 0$.

The first step to bound the right-hand side of (3.28) is to bound $\Delta$. Grouping the ordered pairs of $k$-cliques according to the size of their vertex intersection, we obtain

$$\Delta = \binom{n}{k-2} p^{2\binom{k}{2}-1} \sum_{i=3}^{k-1} \binom{k-2}{i-2}\binom{n-k}{k-i} p^{-\binom{i}{2}}. \tag{3.29}$$

Our goal is to show that $\Delta = o(n^{-\delta}(\mathbb{E}(Y_e))^2)$. To do so, define

$$a_i := \binom{k-2}{i-2}\binom{n-k}{k-i} p^{-\binom{i}{2}}$$

and note that

$$\frac{a_{i+1}}{a_i} = \frac{k-i}{i-1} \cdot \frac{k-i}{n-2k+i+1} \cdot p^{-i}. \tag{3.30}$$

We shall use (3.30) to conclude that $a_j = o(a_3 + a_{k-1})$ for all $3 < j < k-1$.

Performing the multiplication of the quotients in (3.30) from $i$ going from $s$ to $j-1$, we obtain

$$\frac{a_j}{a_3} = O_p\left(\left(\frac{k^2}{n}\right)^{j-3} \frac{p^{-\binom{j}{2}}}{(j-2)!}\right). \tag{3.31}$$

From (3.31), we can see that $a_j a_3^{-1} = O(k^2/n)$ whenever $j = O(1)$. When $2^6 \le j \le k_0/4$, we have $p^{-\binom{j}{2}} \le n^{j/2}$ and, since $j$ is large, we obtain $a_j a_3^{-1} = O(k^2/n)$. When $j > k_0/4$, we have $(j-2)! \ge (2^{-5}k)^{j-3}$, and hence

$$\frac{a_j}{a_3} \le \left(\frac{Ck}{np^{j/2}}\right)^{j-3}, \tag{3.32}$$

where $C$ is some constant depending on $p$. From (3.32), we obtain $a_j a_3^{-1} = O(n^{-1/8})$ whenever $j > k_0/4$ and $p^{-j/2} \le n/(2Ck)$. From this, we conclude that $a_j a_3^{-1} = O(n^{-1/8})$ for all $k_0/4 \le j \le k_0 - D$, where $D$ is some constant depending on $p$. Finally, when $k-1 > j \ge k_0 - D$, we can easily see from (3.30) that $a_j a_{k-1}^{-1} = O(n^{-1/2})$. Putting all the pieces together we obtain $a_j = o(a_3 + a_{k-1})$ for all $3 < j < k-1$, and hence

$$\begin{aligned}\Delta &\le 2\binom{n}{k-2} p^{2\binom{k}{2}-1}\big(a_3 + a_{k-1}\big) \\ &\le n^{-1/2}\big(\mathbb{E}(Y_e)\big)^2. \end{aligned} \tag{3.33}$$

Recall that $\delta = \min\{\gamma - 2, 1\}/10$ and $\mathbb{E}(Y_e) = n^{\gamma-2+o(1)}$. Choosing $t = n^{-2\delta}\,\mathbb{E}(Y_e)$ in Janson's inequality (3.28) and using the bound (3.33) for $\Delta$ we obtain

$$\mathbb{P}\left(Y_e \le \left(1 - \frac{1}{n^{2\delta}}\right)\mathbb{E}(Y_e)\right) \le \exp(-n^{\delta}).$$

This proves the first part of our lemma.

To bound the upper tail of $Y_e$ we shall use the deletion method (see Lemma 3.2.6). For any vertex $v \in [n]$, let $Z_{v,e}(G_0^e)$ be the number of $k$-cliques in $G_0^e$ containing $e \cup \{v\}$ and set

$$Y_e^\star(G_0) := \max_{v \in [n] \setminus e} Z_{v,e}\left(G_0^e\right).$$

By the deletion method, for every $\varepsilon \in (0,1)$ and $a > 0$, we have

$$\mathbb{P}\Big(Y_e \geq (1+\varepsilon)\,\mathbb{E}\left(Y_e\right)\Big) \leq \exp\left(-\frac{\varepsilon a}{3k^2}\right) + \mathbb{P}\left(Y_e^\star > \frac{\varepsilon\,\mathbb{E}\left(Y_e\right)}{2a}\right).$$

Take $\varepsilon = n^{-2\delta}$ and $a = n^{3\delta}$ in the inequality above. We obtain

$$\mathbb{P}\left(Y_e \geq \left(1 + \frac{1}{n^{2\delta}}\right)\mathbb{E}(Y_e)\right) \leq \exp(-n^{\delta/2}) + \mathbb{P}\Big(Y_e^\star > n^{\gamma-2-5\delta+o(1)}\Big). \tag{3.34}$$

To bound the probability that $Y_e^\star$ is 'large', we first bound $Z_{v,e}(G_0^e)$ using Lemma 3.3.1 together with Markov's inequality. Although the variables considered in Lemma 3.3.1 are slightly different from $Z_{v,e}(G_0^e)$, we can easily show that Lemma 3.3.1 directly implies that

$$\mathbb{E}\left(\left(Z_{v,e}\big(G_0^e\big)\right)^\ell\right) \leq k^{O(1)}\Big(\max\left\{\,\mathbb{E}\left(Z_{v,e}\big(G_0^e\big)\right),\,1\right\}\Big)^\ell$$

for all $\ell \in \mathbb{N}$. by Markov's inequality, it easily follows that

$$\mathbb{P}\Big(Z_{v,e} > n^\delta \max\left\{\,\mathbb{E}\left(Z_{v,e}\right),\,1\right\}\Big) \leq n^{-7}. \tag{3.35}$$

As $\mathbb{E}\left(Z_{v,e}\big(G_0^e\big)\right) = n^{\gamma-3+o(1)}$ and $\gamma - 2 - 5\delta > \max\{\delta, \gamma-3\}$, it follows from (3.35) and the union bound over $v \in [n]$ that

$$\mathbb{P}\Big(Y_e^\star > n^{\gamma-2-5\delta+o(1)}\Big) \leq n^{-4}. \tag{3.36}$$

Combining (3.34) with (3.36) and applying the union bound over $e \in E(K_n)$, we obtain that $Y_e \leq (1+n^{-2\delta})\,\mathbb{E}(Y_e)$ for all $e \in E(K_n)$ with probability at least $1 - n^{-2}$.

## 3.4 Controlling the evolution of $Q(G_m)$

In this section, we prove Lemma 3.2.4. That is, our goal is to show that

$$\mathbb{P}\big(0 < \tau = \tau_Q < m_*\big) = o(1).$$

Recall that $m_* = \lfloor \delta p n^2 \log n / 4k^4 \rfloor$ and recall the definitions of the stopping times from equations (3.10), (3.11) and (3.12).

We already have some information about the first step. By Lemma 3.2.3, the following holds with probability at least $1 - n^{-1}$:

(a) $e(G_0) = p\binom{n}{2} \pm n^{3/2}$.

(b) $Y_S(G_0) \le n^{\delta} \max\{1, \mathbb{E}\left(Y_S(G_0)\right)\}$ for every set $S$ of size 3.

(c) $Q(G_0) = (1 \pm n^{-\delta})\widetilde{Q}(0)$ and $Y_e(G_0) = (1 \pm n^{-\delta})\widetilde{Y}(0)$ for all $e \in E(K_n)$.

For the rest of this section, we fix $G_0$ to be any graph satisfying conditions (a), (b) and (c). Our goal is to analyse how the random process evolves from $G_0$. Note that we automatically have $\tau > 0$. Moreover, the event $\tau = \tau_Q < m_*$ occurs if and only if there exists $m^\dagger \in \{1, \dots, m_* - 1\}$ for which the following holds:

(i) $Q(G_m) = (1 \pm g_Q(m))\widetilde{Q}(m)$ and $Y_e(G_m) = (1 \pm g(m))\widetilde{Y}(m)$ for all $e \in E(K_n)$ and $0 \le m < m^\dagger$.

(ii) $Q(G_{m^\dagger}) \neq (1 \pm g_Q(m))\widetilde{Q}(m^\dagger)$.

We now encode the event $Q(G_m) > (1 + g_Q(m))\widetilde{Q}(m)$ as a deviation event for a random process. We omit the analysis of the event $Q(G_m) < (1 - g_Q(m))\widetilde{Q}(m)$ as it is essentially identical. Let $(X_i)_i$ be defined as

$$X_i := \begin{cases} Q(G_i) - (1 + g_Q(i))\widetilde{Q}(i) & i \le \tau \\ Q(G_\tau) - (1 + g_Q(\tau))\widetilde{Q}(\tau) & i > \tau\,. \end{cases}$$

Observe that the event $Q(G_m) > (1 + g_Q(m))\widetilde{Q}(m)$ is equivalent to $X_m > 0$. Since $G_0$ is a fixed graph satisfying $(c)$, we deterministically have $X_0 \leq -n^{-\delta}\widetilde{Q}(0)$ (recall that $g_Q(0) = 2n^{-\delta}$). Then, the only chance that $X_m$ has to be positive is if $X_m - X_0 > n^{-\delta}\widetilde{Q}(0)$. At this point it is natural to think about the following proof strategy. If we could show that $(X_i)_i$ is a supermartingale, then Azuma's inequality would imply that the event $X_m - X_0 > -n^{-\delta}\widetilde{Q}(0)$ is very unlikely, and so it is $X_m > 0$. By the union bound, we would conclude that the event $\tau = \tau_Q^+ < m_*$ would also be very unlikely, where

$$\tau_Q^+ := \min\Big\{m : Q(G_m) > (1 + g_Q(m))\widetilde{Q}(m)\Big\}.$$

This strategy indeed works for 'small' values of $k$, namely when $k \leq k_0 - 5$. However, for $k$ larger, we need a finer control on the increments $X_m - X_{m-1}$.

In order to have a better control over the increments $X_m - X_{m-1}$, we use in our favor the fact that they tend to be smaller over time. Thus, instead of analysing the whole process since its first step, we only focus on a small time interval near $\tau$. Let $m_-$ be the last step $m \leq \tau$ such that $Q(G_m) \notin (1 \pm g_Q(m)/2)\widetilde{Q}(m)$. If this step does not exist, we simply set $m_- = \tau$. As $Q(G_0) \in (1 \pm g_Q(0)/2)\widetilde{Q}(0)$, we note that $m_- > 0$.

Let $\mathcal{F}_m$ be the natural filtration generated by the sequence $(G_0, G_1, \ldots, G_m)$. Our next lemma shows that $\{(X_m, \mathcal{F}_m) : m \geq m_-\}$ is a supermartingale under the event $\tau_Q^+ = \tau$. In what follows, we denote by $A(i, j)$ the event $m_- = i$ and $\tau = \tau_Q^+ = j$.

**Lemma 3.4.1.** *Let $0 < i \leq j \leq m_*$. The process $\{(X_m, \mathcal{F}_m) : m \geq i\}$ is a supermartingale under the event $A(i, j)$.*

We shall prove Lemma 3.4.1 in the next subsection. As $X_m$ freezes at the stopping time $\tau$, the event $0 < \tau = \tau_Q^+ < m_*$ implies $X_{m_*} > 0$. We would like to use Azuma's inequality to bound the probability of the latter event. To do so, we control the increments $X_m - X_{m-1}$ for every $m > m_-$.

**Lemma 3.4.2.** *We have* $|X_{m+1} - X_m| = O\big(k^4\widetilde{Q}(m_-)/pn^2\big)$ *for all* $m \geq m_-$.

We shall prove Lemma 3.4.2 in the next subsection. We can easily deduce from Lemmas 3.4.1 and 3.4.2 that $\mathbb{P}\big(0 < \tau = \tau_Q^+ < m_*\big) \to 0$. To finish the proof of Lemma 3.2.4, we also need to consider the supermartingale which encodes the event $Q(G_m) < (1 - g_Q(m))\widetilde{Q}(m)$ and prove lemmas which are analogous to Lemmas 3.4.1 and 3.4.2. Similarly, we can show that $\mathbb{P}\big(0 < \tau = \tau_Q^- < m_*\big) \to 0$, where $\tau^-$ denotes the minimum $m$ such that $Q(G_m) < (1 - g_Q(m))\widetilde{Q}(m)$.

*Proof.* [Proof of Lemma 3.2.4, assuming Lemmas 3.4.1 and 3.4.2.] By Lemma 3.2.3, $G(n,p)$ does not satisfy $F_0$ with probability at least $1 - n^{-1}$. If the event $F_0^c$ holds, then $\tau > 0$ and hence

$$\mathbb{P}\big(0 < \tau = \tau_Q^+ < m_*\big) \leq n^{-1} + \mathbb{P}\big(\tau = \tau_Q^+ < m_* \,\big|\, F_0^c\big).$$

Thus, it suffices to show that the event $\{\tau = \tau_Q^+ < m_*\}^c$ holds with high probability whenever the process starts from a graph $G_0$ which satisfies (a), (b) and (c). From now on, we fix any graph $G_0$ satisfying these items and, to facilitate the notation, we omit any dependencies on $G_0$.

The event $\tau = \tau_Q^+ < m_*$ can be written as

$$\big\{\tau = \tau_Q^+ < m_*\big\} = \bigcup_{0<i\leq j<m^*} A(i,j).$$

We now bound each of the probabilities $\mathbb{P}(A(i,j))$ individually. If $A(i,j)$ holds, then we have $X_i \leq -(g_Q \cdot \widetilde{Q})(i)/4$. Indeed, as $Q(G_i) \leq Q(G_{i-1})$, we have

$$Q(G_i) \leq \widetilde{Q}(i-1) + (g_Q\widetilde{Q})(i-1)/2.$$

Subtracting $\widetilde{Q}(i) + (g_Q\widetilde{Q})(i)/2$ on both sides, we obtain

$$X_i + (g_Q\widetilde{Q})(i)/2 \leq -\Delta\widetilde{Q}(i-1) - \Delta(g_Q\widetilde{Q})(i-1)/2.$$

An easy calculation shows that $|\Delta\widetilde{Q}(i-1)+\Delta(g_Q\widetilde{Q})(i-1)/2| \leq (g_Q\widetilde{Q})(i)/4$ (cf. Claim 3.4.3). As $A(i,j)$ implies that $X_i \leq -(g_Q \cdot \widetilde{Q})(i)/4$ and $X_j > 0$, we have

$$\mathbb{P}\big(A(i,j)\big) \;=\; \mathbb{P}\Big(\big\{X_j - X_i > (g_Q \cdot \widetilde{Q})(i)/4\big\} \cap A(i,j)\Big).$$

Our goal is to bound the probability on the right-hand side above via Azuma's inequality. By Lemma 3.4.1, $\big\{(X_m, \mathcal{F}_m) : m \in [i,j]\big\}$ is a supermartingale under the event $A(i,j)$. Let $\Delta$ be maximum increment $|X_m - X_{m-1}|$ of this supermartingale under $A(i,j)$. As $j - i \leq m_* \leq n^2$, by Azuma's inequality we obtain that

$$\mathbb{P}\big(A(i,j)\big) \leq \exp\left(-O\left(\frac{(g_Q \cdot \widetilde{Q})^2(i)}{\Delta^2 n^2}\right)\right). \tag{3.37}$$

By Lemma 3.4.2, $\Delta$ is bounded by $O\big(k^4\widetilde{Q}(i)/n^2\big)$. It follows from (3.37) that

$$\begin{aligned}\mathbb{P}\big(A(i,j)\big) &\leq \exp\left(-O\left(\frac{g_Q(i)^2 n^2}{k^8}\right)\right)\\ &\leq \exp(-n).\end{aligned}$$

Applying the union bound over all $0 < i \leq j < m_*$ we obtain

$$\mathbb{P}\big(\tau = \tau_Q^+ < m_* \,\big|\, F_0^c\big) \leq n^4 \exp(-n).$$

□

### 3.4.1 Proof of Lemmas 3.4.1 an 3.4.2

For any function $f$, we denote $\Delta f(m) = f(m+1) - f(m)$. For the proofs of both lemmas, we need a bound on the increments which compose the 'deterministic' part of $X_m$, namely $\Delta\widetilde{Q}(m)$ and $\Delta(g_Q \cdot \widetilde{Q})(m)$. This is done in our next claim.

**Claim 3.4.3.** *Let $m \in \mathbb{N}$ be such that $m \leq m_*$. We have*

$$\Delta\widetilde{Q}(m) = -\binom{k}{2}\widetilde{Y}(m) \qquad \textit{and} \qquad \Delta(g_Q\widetilde{Q})(m) = -\binom{k}{2}^4 \frac{(g_Q \cdot \widetilde{Q})(m)}{e(G_m)^2}.$$

*Proof.* By definition (see (3.2) and (3.3)), we have

$$\widetilde{Q}(m+1) = \left(1 - \frac{\binom{k}{2}^2}{e(G_m)}\right)\widetilde{Q}(m) \qquad \text{and} \qquad g_Q(m+1) = \left(1 + \frac{\binom{k}{2}^2}{e(G_m)}\right) g_Q(m). \quad (3.38)$$

From (3.38), it follows that

$$\Delta\widetilde{Q}(m) = -\binom{k}{2}^2 \frac{\widetilde{Q}(m)}{e(G_m)} \qquad \text{and} \qquad \Delta(g_Q \cdot \widetilde{Q})(m) = -\binom{k}{2}^4 \frac{(g_Q \cdot \widetilde{Q})(m)}{e(G_m)^2}. \quad (3.39)$$

As $\widetilde{Y}(m) = \binom{k}{2}\widetilde{Q}(m)/e(G_m)$, it follows from (3.39) that $\Delta\widetilde{Q}(m) = -\binom{k}{2}\widetilde{Y}(m)$. This proves our claim. □

We are now ready to prove Lemma 3.4.1.

*Proof.* [Proof of Lemma 3.4.1]

Let $0 < i \leq j \leq m_*$ and suppose that the event $A(i,j)$ holds. Our aim is to show that $\mathbb{E}(\Delta X_m | \mathcal{F}_m) \leq 0$ for every $m \in [i,j)$. To do so, we first analyse the one-step change $\Delta Q(G_m)$. At step $m$ of the process, recall that a $k$-clique is uniformly chosen among those in $G_{m-1}$, and its edges are removed. Denote this clique by $K$. Note that the $k$-cliques that are destroyed at step $m$ are precisely those that share an edge with $K$. It follows that the number of $k$-cliques removed in total is at most

$$\sum_{e \in K} Y_e(G_m).$$

This might be a slight overcount, as cliques that have intersection at least 3 with $K$ may be counted more than once. As $G_m \subseteq G_0$ and $Y_S(G_0) \leq n^\delta \max\{1, \mathbb{E}(Y_S(G_0))\}$ for every set $S$ of size 3, the overcount is at most

$$\sum_{S \subseteq K : |S| = 3} Y_S(G_m) \leq k^3 n^\delta \max\left\{1, \mathbb{E}(Y_S(G_0))\right\}$$

for every $m \in [i, j)$. It follows that

$$\Delta Q(G_m) \;=\; -\sum_{e \in K} Y_e(G_m) \;\pm\; E_1\,, \tag{3.40}$$

where $E_1 := k^3 n^\delta \max\{1, \mathbb{E}(Y_S(G_0))\}$. Taking the conditional expectation in (3.40), we have

$$\begin{aligned}\mathbb{E}\left(\Delta Q(G_m)\Big|\mathcal{F}_m\right) \;&=\; \frac{-1}{Q(G_m)} \sum_{K} \sum_{e \in K} Y_e(G_m) \;\pm\; E_1 \\ &=\; \frac{-1}{Q(G_m)} \sum_{e \in G_m} Y_e(G_m)^2 \;\pm\; E_1. \end{aligned} \tag{3.41}$$

Now, define

$$\overline{Y}(G_m) \;:=\; \frac{1}{e(G_m)} \sum_{e \in E(G_m)} Y_e(G_m).$$

This variable quantifies the average value of $Y_e(G_m)$ over $e \in G_m$. As each $k$-clique is being counted $\binom{k}{2}$ times in the sum above, we can also write

$$\overline{Y}(G_m) \;=\; \frac{\binom{k}{2} Q(G_m)}{e(G_m)}.$$

We may now write each $Y_e(G_m)$ as $(1 + \eta_e)\overline{Y}(G_m)$, where $\sum_e \eta_e = 0$. From (3.41), it follows that

$$\begin{aligned}\mathbb{E}\left(\Delta Q(G_m)\Big|\mathcal{F}_m\right) \;&=\; -\frac{\overline{Y}(G_m)^2}{Q(G_m)} \sum_{e \in G_m} (1 + \eta_e)^2 \;\pm E_1. \\ &=\; -\frac{\overline{Y}(G_m)^2 e(G_m)}{Q(G_m)} \;\pm\; E_1 \;\pm\; E_2,\,. \end{aligned} \tag{3.42}$$

where the error $E_2$ is defined as

$$E_2 := \frac{\overline{Y}(G_m)^2}{Q(G_m)} \sum_{e \in G_m} \eta_e^2.$$

From (3.42), it follows that

$$\mathbb{E}\left(\Delta Q(G_m)\Big|\mathcal{F}_m\right) \;=\; -\binom{k}{2}\overline{Y}(G_m) \;\pm\; E_1 \;\pm\; E_2. \tag{3.43}$$

Now let us bound $\eta_e^2$. As $m < j = \tau$, we have

$$\begin{aligned} Y_e(G_m) &= (1 \pm g_Y(m))\widetilde{Y}(G_m) \\ &= (1+\eta_e)\overline{Y}(G_m), \end{aligned}$$

and hence $|\eta_e| \le 4g_Y(m)$. It follows that

$$\begin{aligned} E_2 &\le 4g_Y^2(m) \cdot \frac{k^4 Q(G_m)}{e(G_m)} \\ &\le 8g_Y^2(m) \cdot \frac{k^4 \widetilde{Q}(m)}{e(G_m)}. \end{aligned} \tag{3.44}$$

for every $m \in [i,j)$. In the last inequality we used that $Q(G_m) \le 2\widetilde{Q}(m)$, as $m < j = \tau$.

We are now nearly ready to complete our proof. To make the notation shorter, let us set $E = E_1 + E_2$. By Claim 3.4.3 and (3.43), we obtain

$$\mathbb{E}\left(\Delta X(m)\middle|\mathcal{F}_m\right) \;=\; -\binom{k}{2}\left(\overline{Y}(G_m) - \widetilde{Y}(m)\right) \;-\Delta(g_Q\widetilde{Q})(m) \;\pm\; E, \tag{3.45}$$

for every $m \in [i,j)$. Up to now, we have not completely used the assumption that the event $A(i,j)$ holds. This will be important now, to lower bound the increment $\overline{Y} - \widetilde{Y}$. To do so, first note that

$$\overline{Y}(G_m) - \widetilde{Y}(m) = \binom{k}{2}\frac{Q(G_m) - \widetilde{Q}(m)}{e(G_m)}. \tag{3.46}$$

Under the event $A(i,j)$, we have $Q(G_m) \ge (1 + g_Q(m)/2)\widetilde{Q}(m)$ for all $m \in [i,j)$. Then, it follows from (3.46) that

$$\overline{Y}(G_m) - \widetilde{Y}(m) \ge \binom{k}{2}\frac{(g_Q\widetilde{Q})(m)}{2e(G_m)} \tag{3.47}$$

if the event $A(i,j)$ holds. By (3.44) and (3.46), we can see that $E_2 = o\big(\overline{Y}(G_m) - \widetilde{Y}(m)\big)$. By Claim 3.4.3, we can also see that $\Delta(g_Q\widetilde{Q})(m) = o\big(\overline{Y}(G_m) - \widetilde{Y}(m)\big)$. For the error $E_1$, we claim that

$$E_1 \le \binom{k}{2}\frac{(g_Q\widetilde{Q})(m)}{4e(G_m)}. \tag{3.48}$$

In fact, by definition of $\widetilde{Q}$ and $g_Q$, we can see that $(g_Q\widetilde{Q})(m) \geq n^{-\delta}\widetilde{Q}(0)$. As $e(G_m) = \Theta(n^2)$, (3.48) clearly holds if $\mathbb{E}(Y_S(G_0)) > 1$. On the other hand, if $\mathbb{E}(Y_S(G_0)) < 1$, then $E_1 = k^3 n^\delta$. As $(g_Q\widetilde{Q})(m) \geq n^{-\delta}\widetilde{Q}(0) \geq n^{\gamma-\delta+o(1)}$, the inequality follows from the choice of $\delta$ (recall that $\delta = \min\{\gamma - 2, 1\}/10$). We conclude that

$$\mathbb{E}\left(\Delta X(m)\middle|\mathcal{F}_m\right) \leq -\binom{k}{2}\frac{(g_Q\widetilde{Q})(m)}{10e(G_m)}$$

for all $m \in [i, j)$ when the event $A(i, j)$ holds. This finishes the proof of the lemma. □

We now prove Lemma 3.4.2, which bounds the absolute value of the increment $\Delta X_m$.

*Proof.* [Proof of Lemma 3.4.2] Fix any $m \in [m_-, \tau)$. The absolute value $|\Delta X_m|$ is at most the maximum of

$$\left|\Delta Q(G_m)\right| \qquad \text{and} \qquad \left|\Delta\widetilde{Q}(m) + \Delta(g_Q \cdot \widetilde{Q})(m)\right|.$$

Thus, it suffices to prove that each of these terms is at most $O\big(k^4\widetilde{Q}(m_-)/pn^2\big)$. By Claim 3.4.3, we already know that this is the case for the second expression. For the first expression, recall that $\left|\Delta Q(G_m)\right|$ is exactly the number of $k$-cliques removed from $G_m$ when we remove a randomly selected $k$-clique $K$. For any choice of $K$, this is at most

$$\sum_{e\in K} Y_e(G_m) \leq 2\binom{k}{2}\widetilde{Y}(m) = O\left(\frac{k^4\widetilde{Q}(m_-)}{pn^2}\right).$$

as required. □

## 3.5 Controlling the evolution of $Y_e(G_m)$ for all $e \in E(K_n)$

In this section, our aim is to prove Lemma 3.2.5. That is, our goal is to show that

$$\mathbb{P}\big(0 < \tau = \tau_Y < m_*\big) \to 0.$$

Recall that $m_* = \lfloor \delta p n^2 \log n / 4k^4 \rfloor$ and recall the definitions of the stopping times from equations (3.10), (3.11) and (3.12).

For each $e \in E(K_n)$, we denote by $\tau_{Y_e}$ the first time $m$ for which $Y_e(G_m)$ leaves the interval $(1 \pm g_Y(m))\widetilde{Y}(m)$. To prove Lemma 3.2.5 it suffices to show that, for each edge $e \in E(K_n)$, we have

$$\mathbb{P}\big(0 < \tau = \tau_{Y_e} < m_*\big) \leq n^{-3}.$$

To do so, let us first recall the information we have on the first step of the process. By Lemma 3.2.3, the following holds with probability at least $1 - n^{-1}$:

(a) $e(G_0) = p\binom{n}{2} \pm n^{3/2}$.

(b) $Y_S(G_0) \leq n^{\delta} \max\{1, \mathbb{E}(Y_S(G_0))\}$ for every set $S$ of size 3.

(c) $Q(G_0) = (1 \pm n^{-\delta})\widetilde{Q}(0)$ and $Y_e(G_0) = (1 \pm n^{-\delta})\widetilde{Y}(0)$ for all $e \in E(K_n)$.

For the rest of this section, we fix $G_0$ to be any graph satisfying conditions (a), (b) and (c). Under this assumption, note that we automatically have $\tau > 0$.

We now encode the event $Y_e(G_m) > (1 + g_Q(m))\widetilde{Y}(m)$ as a deviation event for a supermartingale. We omit the analysis of the event $Y_e(G_m) < (1 - g_Q(m))\widetilde{Y}(m)$ as it is essentially identical. For each $e \in E(K_n)$, let $(Z_m^e)_m$ be defined as

$$Z_m^e := \begin{cases} Y_e(G_m) \; - \; (1 + g_Y(m))\widetilde{Y}(m) & m \leq \tau \\ Y_e(G_\tau) \; - \; (1 + g_Y(\tau))\widetilde{Y}(\tau) & m > \tau \,. \end{cases}$$

Observe that the event $Y_e(G_m) > (1 + g_Q(m))\widetilde{Y}(m)$ is equivalent to $Z_m^e > 0$. Our goal is to bound the probability that $Z_m^e > 0$ using Freedman's inequality. To do so, we proceed as in the previous section, analysing a small time interval of the process before its stopping time $\tau$.

For each $e \in E(K_n)$, let $\tau_-^e$ be the last step $m \leq \tau$ such that $Y_e(G_m) \in (1 \pm g_Y(m)/2)\widetilde{Y}(m)$. If this step does not exist, we simply set $\tau_-^e = \tau$. As $Y_e(G_0) \in (1 \pm g_Y(0)/2)\widetilde{Y}(0)$, we observe that $\tau_-^e > 0$. Now, define

$$\tau_{Y_e}^+ := \min\Big\{m : Y_e(G_m) > (1 + g_Y(m))\widetilde{Y}(m)\Big\}.$$

Our next lemma shows that if $\tau_{Y_e}^+ = \tau$ holds, then $\{Z_m^e : m \geq \tau_-^e\}$ is a supermartingale with respect to the filtration $(\mathcal{F}_m)_{m\geq 0}$. We recall that $\mathcal{F}_m$ denotes the natural filtration generated by the sequence $(G_0, G_1, \ldots, G_m)$.

In what follows, we denote by $A_e(i,j)$ the event $\tau_-^e = i$ and $\tau = \tau_{Y_e}^+ = j$.

**Lemma 3.5.1.** *Let $0 < i \leq j \leq m_*$ and $e \in E(K_n)$. The process $\{(Z_m^e, \mathcal{F}_m) : m \geq i\}$ is a supermartingale under the event $A_e(i,j)$.*

We shall prove Lemma 3.5.1 in the next subsection. As $Z_m^e$ freezes at the stopping time $\tau$, the event $0 < \tau = \tau_{Y_e}^+ < m_*$ implies $Z_{m_*}^e > 0$. We would like to use Freedman's inequality to bound the probability of the latter event. To do so, we control the absolute value of the increments $Z_m^e - Z_{m-1}^e$ and its expected change, for every $m > \tau_-^e$.

**Lemma 3.5.2.** *Let $e \in E(K_n)$ and $S \subseteq [n]$ be a set of size 3. For every $m \geq \tau_-^e$, the increment $\Delta Z_m^e$ satisfy*

*(i)* $|\Delta Z_m^e| = O(1)k^2 n^\delta \max\{1, \mathbb{E}(Y_S(G_0))\}$;

*(ii)* $\mathbb{E}\left(|\Delta Z_m^e| \middle| \mathcal{F}_m\right) = O\left(\dfrac{k^4 \widetilde{Y}(\tau_-^e)}{pn^2}\right)$.

We shall prove Lemma 3.5.2 in the next subsection. For now, let us assume that Lemmas 3.5.1 and 3.5.2 hold and let us prove Lemma 3.2.5. Our approach is similar to that of the previous section except we now use Freedman's inequality (see Lemma 3.2.9).

*Proof.* [Proof of Lemma 3.2.5, assuming Lemmas 3.5.1 and 3.5.2 ] By Lemma 3.2.3, $G(n,p)$ does not satisfy $F_0$ with probability at least $1-n^{-1}$. If the event $F_0^c$ holds, then $\tau > 0$ and hence

$$\mathbb{P}\big(0 < \tau = \tau_Y < m_*\big) \leq n^{-1} + \mathbb{P}\big(\tau = \tau_Y < m_* \,\big|\, F_0^c\big).$$

Thus, it suffices to show that the event $\{\tau = \tau_Y < m_*\}^c$ holds with high probability whenever the process starts from a graph $G_0$ which satisfies (a), (b) and (c). From now on, we fix any graph $G_0$ satisfying these items and, to facilitate the notation, we omit any dependencies on $G_0$.

Let $e \in E(K_n)$ be any edge. We now bound the probability that $\tau = \tau^+_{Y_e} < m_*$ holds. This event can be written as

$$\big\{\tau = \tau^+_{Y_e} < m_*\big\} = \bigcup_{0<i\leq j<m_*} A_e(i,j).$$

Moreover, if $A_e(i,j)$ holds, then we have $Z_i^e \leq -(g_Y\widetilde{Y})(i)/4$. Indeed, as $Y_e(G_i) \leq Y_e(G_{i-1})$, we have

$$Y_e(G_i) \leq \widetilde{Y}(i-1) + (g_Y\widetilde{Y})(i-1)/2.$$

Subtracting $\widetilde{Y}(i) + (g_Y\widetilde{Y})(i)/2$ on both sides, we obtain

$$Z_i^e + (g_Y\widetilde{Y})(i)/2 \leq -\Delta\widetilde{Y}(i-1) - \Delta(g_Y\widetilde{Y})(i-1)/2.$$

An easy calculation shows that $|\Delta\widetilde{Y}(i-1)+\Delta(g_Y\widetilde{Y})(i-1)/2| \leq (g_Y\widetilde{Y})(i)/4$ (cf. Claim 3.5.3). As $A_e(i,j)$ implies that $Z_i^e \leq -(g_Y\widetilde{Y})(i)/4$ and $Z_j^e > 0$, we have

$$\mathbb{P}\big(A_e(i,j)\big) \;=\; \mathbb{P}\Big(\big\{Z_j^e - Z_i^e > (g_Y\widetilde{Y})(i)/4\big\} \cap A_e(i,j)\Big).$$

Our goal is to bound the probability on the right-hand side of the inequality above via Freedman's inequality. By Lemma 3.5.1, $\{(Z_m^e, \mathcal{F}_m) : m \in [i,j]\}$ is a supermartingale under

the event $A_e(i,j)$. In order to apply Freedman's inequality, we need to bound the quadratic variation of this supermartingale, which is defined as

$$V_e(i,j) := \sum_{m=i}^{j-1} \mathbb{E}\left((\Delta Z_m^e)^2 \middle| \mathcal{F}_m\right).$$

By Lemma 3.5.2, if the event $A_e(i,j)$ holds, then for each $m \in [i,j)$ we have

$$\begin{aligned}\mathbb{E}\left((\Delta Z_m^e)^2 \middle| \mathcal{F}_m\right) &\leq \|\Delta Z_m^e\|_\infty \, \mathbb{E}\left(|\Delta Z_m^e| \,\middle|\, \mathcal{F}_m\right) \\ &= O\left(\frac{k^6 \widetilde{Y}(i)}{n^{2-\delta}}\right) \cdot \max\{1, \mathbb{E}(Y_S(G_0))\}. \end{aligned} \tag{3.49}$$

As $j < n^2$, we obtain from (3.49) that

$$V_e(i,j) = O\left(k^6 n^\delta \widetilde{Y}(i)\right) \cdot \max\{1, \mathbb{E}(Y_S(G_0))\} \tag{3.50}$$

when the event $A_e(i,j)$ holds.

We are now ready to apply Freedman's inequality. Let $W$ denote the quantity in the right-hand side of (3.50), up to a constant. By Lemma 3.5.2, we have $|\Delta Z_m^e| \cdot (g_Y \widetilde{Y})(i) = o\big(W\big)$ for all $m \in [i,j)$, and hence

$$\mathbb{P}\Big(\big\{Z_j^e - Z_i^e > (g_Y \widetilde{Y})(i)/2\big\} \cap A_e(i,j)\Big) \leq \exp\left(-O\left(\frac{(g_Y \widetilde{Y})^2(i)}{W}\right)\right), \tag{3.51}$$

by Freedman's inequality. It remains to compare the expressions $(g_Y \widetilde{Y})^2(i)$ and $W$.

As $g_Y(i) \geq g_Y(0) > n^{-\delta}$, we have

$$\frac{(g_Y \widetilde{Y})^2(i)}{W} = \Omega\left(\frac{\widetilde{Y}(i)}{k^6 n^{3\delta} \max\{1, \mathbb{E}(Y_S(G_0))\}}\right).$$

Now, we claim that $\widetilde{Y}(i) \geq n^{4\delta} \max\{1, \mathbb{E}(Y_S(G_0))\}$. Indeed, we as $i \leq m_*$, we have

$$\begin{aligned}\widetilde{Y}(i) &= \Omega\left(\frac{k^2 \widetilde{Q}(0)}{n^{2+4\delta}}\right) \\ &= \Omega\left(n^{\gamma-2-4\delta+o(1)}\right).\end{aligned}$$

where the first equality follows from $i \leq m_*$. By the choice of delta (recall that $\delta = \min\{\gamma - 2, 1\}/10$), we can check that the last expression implies that $\widetilde{Y}(i) \geq n^{4\delta} \max\{1, \mathbb{E}(Y_S(G_0))\}$. From this analysis, we conclude that

$$\frac{(g_Y \widetilde{Y})^2(i)}{W} = \Omega\left(k^{-6} n^{\delta}\right). \tag{3.52}$$

From eqs (3.51) and (3.52), it follows that

$$\mathbb{P}\Big(\left\{Z_j^e - Z_i^e > (g_Y \widetilde{Y})(i)/2\right\} \cap A_e(i,j)\Big) \leq \exp\left(-O\left(k^{-6} n^{\delta}\right)\right).$$

By the union bound over $0 < i \leq j < m_*$ and $e \in E(K_n)$, we obtain

$$\mathbb{P}\left(\bigcup_{e \in E(K_n)} \left\{\tau = \tau_{Y_e}^+ < m_*\right\}\right) = n^4 \exp\left(-O\left(k^{-6} n^{\delta}\right)\right).$$

To finish the proof of Lemma 3.2.4, we also need to consider the supermartingales which encodes the events $Y_e(G_m) < (1 - g_Y(m))\widetilde{Y}(m)$ and prove lemmas which are analogous to Lemmas 3.5.1 and 3.5.2. Similarly, we can show that $\mathbb{P}\big(\tau = \tau_{Y_e}^- < m_*\big) \leq \exp\big(-O(k^{-6} n^{\delta})\big)$, where $\tau_{Y_e}^-$ denotes the minimum $m$ such that $Y_e(G_m) < (1 - g_Y(m))\widetilde{Y}(m)$. We omit the details. $\square$

### 3.5.1 Proof of Lemmas 3.5.1 an 3.5.2

For any function $f$, recall that we denote $\Delta f(m) = f(m+1) - f(m)$. For the proofs of both lemmas, we need a bound on the increments which compose the 'deterministic' part of $Z_m^e$, namely $\Delta\widetilde{Y}(m)$ and $\Delta(g_Y \cdot \widetilde{Y})(m)$. To do so, it is useful to define the following error functions:

$$E_1 := \frac{k^6 \widetilde{Y}(m)}{e(G_m)^2} \qquad \text{and} \qquad E_2 := \frac{k^8 (g_Y \widetilde{Y})(m)}{e(G_{m+1})^2}. \tag{3.53}$$

**Claim 3.5.3.** *For any $m \le \tau$, we have*

$$\Delta\widetilde{Y}(m) = -\binom{k}{2}\left(\binom{k}{2}-1\right)\frac{\widetilde{Y}(m)}{e(G_m)} \pm E_1.$$

*and*

$$\Delta(g_Y\widetilde{Y})(m) = g_Y(m)\left(\binom{k}{2}^2+\binom{k}{2}\right)\frac{\widetilde{Y}(m)}{e(G_m)} \pm E_2.$$

*Proof.* First, let us analyse the one-step difference $\Delta\widetilde{Y}(m)$. Recall from (3.2) and (3.7) that

$$\widetilde{Q}(m+1) = \left(1-\frac{\binom{k}{2}^2}{e(G_m)}\right)\widetilde{Q}(m) \qquad \text{and} \qquad \widetilde{Y}(m) = \binom{k}{2}\frac{\widetilde{Q}(m)}{e(G_m)}.$$

From this, it follows that

$$\begin{aligned}\Delta\widetilde{Y}(m) &= \binom{k}{2}\left(\frac{\widetilde{Q}(m+1)}{e(G_{m+1})}-\frac{\widetilde{Q}(m)}{e(G_m)}\right)\\ &= \binom{k}{2}\widetilde{Q}(m)\left(\frac{1}{e(G_{m+1})}\left(1-\frac{\binom{k}{2}^2}{e(G_m)}\right)-\frac{1}{e(G_m)}\right).\end{aligned}$$

As $e(G_{m+1}) = e(G_m) - \binom{k}{2}$, we obtain from the last equality that

$$\begin{aligned}\Delta\widetilde{Y}(m) &= -\binom{k}{2}^2\left(\binom{k}{2}-1\right)\frac{\widetilde{Q}(m)}{e(G_{m+1})e(G_m)}\\ &= -\binom{k}{2}\left(\binom{k}{2}-1\right)\frac{\widetilde{Y}(m)}{e(G_{m+1})}.\end{aligned}$$

As $e(G_{m+1})^{-1} = e(G_m)^{-1} \pm k^2 e(G_{m+1})^{-2}$ , we obtain the required expression for $\Delta\widetilde{Y}(m)$.

Now, let us analyse the one-step difference $\Delta(g_Y\widetilde{Y})(m)$. From the identity $\Delta(ab)(m) = \Delta a(m)b(m) + a(m+1)\Delta b(m)$, it follows that

$$\Delta(g_Y\widetilde{Y})(m) = g_Y(m)\Delta\widetilde{Y}(m) + \Delta g_Y(m)\widetilde{Y}(m+1). \tag{3.54}$$

We shall analyse each of the terms in the right-hand side of (3.54) separately. From the bound we obtained for $\Delta\widetilde{Y}(m)$, it follows that

$$g_Y(m)\Delta\widetilde{Y}(m) = -\binom{k}{2}\left(\binom{k}{2}-1\right)\frac{(g_Y\widetilde{Y})(m)}{e(G_m)} \pm \frac{E_2}{2}. \tag{3.55}$$

Now it remains to bound the term $\Delta g_Y(m)\widetilde{Y}(m+1)$. From the definition of $g_Y$ (see (3.8)), we have

$$\Delta g_Y(m) = 2\binom{k}{2}^2 \frac{g_Y(m)}{e(G_m)}. \tag{3.56}$$

Moreover, from the definitions of $\widetilde{Q}$ and $\widetilde{Y}$ (see (3.2) and (3.7)), it follows that

$$\widetilde{Y}(m+1) = \binom{k}{2}\left(1 - \frac{\binom{k}{2}^2}{e(G_m)}\right)\frac{\widetilde{Q}(m)}{e(G_{m+1})}. \tag{3.57}$$

Combining (3.56) and (3.57), we obtain

$$\Delta g_Y(m)\widetilde{Y}(m+1) = 2\binom{k}{2}^2\left(1 - \frac{\binom{k}{2}^2}{e(G_m)}\right)\frac{(g_Y\widetilde{Y})(m)}{e(G_{m+1})}.$$

Again because $e(G_{m+1})^{-1} = e(G_m)^{-1} \pm k^2 e(G_{m+1})^{-2}$, we obtain

$$\Delta g_Y(m)\widetilde{Y}(m+1) = 2\binom{k}{2}^2\frac{(g_Y\widetilde{Y})(m)}{e(G_m)} \pm \frac{E_2}{2}. \tag{3.58}$$

The claim follows from combining equations (3.54), (3.55) and (3.58).

□

Our first goal is to show that the process $\{(Z_m^e, \mathcal{F}_m) : m \geq \tau_-^e\}$ is a supermartingale if the event $A_e(i,j)$ holds. To show this, we need a bound on the increment $\mathbb{E}(\Delta Y_e(G_m)|\mathcal{F}_m)$. The first step on this direction is to express this quantity in terms of some variables which only depend on $\mathcal{F}_m$. For each ordered pair of edges $(e,f) \in E(K_n)^2$, define $Y_{e,f}(G_m)$ to be the number of copies of $k$-cliques in $G_m \cup e$ which contain $e$ and $f$. Our next proposition express $\mathbb{E}(\Delta Y_e(G_m)|G_m)$ in terms of these variables. Before stating it, we need to define the following error function:

$$E_3 := \frac{2\widetilde{Y}(m)k^3n^\delta}{\widetilde{Q}(m)} \cdot \max\{1, \mathbb{E}(Y_S(G_0))\}. \tag{3.59}$$

**Proposition 3.5.4.** *If $m < \tau$, then*

$$\mathbb{E}\left(\Delta Y_e(\mathcal{F}_m)\middle|\mathcal{F}_m\right) = -\frac{1}{Q(G_m)}\sum_{f\in E(G_m)\setminus\{e\}} Y_{e,f}(G_m)Y_f(G_m) \pm E_3.$$

*Proof.* In order to analyse the one-step change $\Delta Y_e(G_m)$, we define $P(m)$ to be the number of pairs $(K^1, K^2)$ satisfying

1. $K^1$ is a $k$-clique in $G_m$;
2. $K^2$ is a $k$-clique in $G_m \cup \{e\}$ containing $e$ and at least one edge of $K^1 \setminus \{e\}$.

At step $m$ of the process, recall that a $k$-clique is uniformly chosen among those in $G_{m-1}$. This implies that the conditional expectation $\mathbb{E}(\Delta Y_e(m)|\mathcal{F}_m)$ is precisely

$$\mathbb{E}(\Delta Y_e(m)|\mathcal{F}_m) = -\frac{P(m)}{Q(m)}. \tag{3.60}$$

Let us give an upper bound on $P(m)$. From items 1 and 2 we can easily see that

$$P(m) \le \sum_K \sum_{f\in K\setminus\{e\}} Y_{e,f}(G_m).$$

Inverting the order of the sums above, we obtain

$$P(m) \le \sum_{f\in E(G_m)\setminus\{e\}} Y_{e,f}(G_m)Y_f(G_m). \tag{3.61}$$

We might not have an equality above due to a possible slight overcount. Those pairs of cliques $(K^1, K^2)$ where $K^2$ contains at least 3 vertices in $K^1$ are counted more than once in the sums above. But, we can easily see that the overcount does not exceeds

$$Y_e(G_m)\binom{k}{3}\max\{Y_S(G_m) : |S| = 3\}. \tag{3.62}$$

As $m < \tau$, we have $Y_e(G_m) \leq 2\widetilde{Y}(m)$ and, as $G_m \subseteq G_0$, we have $Y_S(G_m) \leq n^\delta \max\{1, \mathbb{E}(Y_S(G_0))\}$. Thus, the quantity in (3.62) is upper bounded by $\widetilde{Y}(m)k^3n^\delta \max\{1, \mathbb{E}(Y_S(G_0))\}$. From (3.60) and (3.61), it follows that

$$\mathbb{E}\left(\Delta Y_e(m)\middle|\mathcal{F}_m\right) = -\frac{1}{Q(m)} \sum_{f \in E(G_m)\setminus\{e\}} Y_{e,f}(G_m)Y_f(G_m) \pm E_3,$$

where

$$E_3 = \frac{\widetilde{Y}(m)k^3n^\delta}{Q(m)} \cdot \max\{1, \mathbb{E}(Y_S(G_0))\}.$$

This completes the proof. □

With Claim 3.5.3 and Proposition 3.5.4 in our hands, we are ready to prove Lemma 3.5.1. Recall that Lemma 3.5.1 states that $\{(Z^e_m, \mathcal{F}_m) : m \geq \tau^e_-\}$ is a supermartingale if the event $A_e(i,j)$ holds.

*Proof.* [Proof of Lemma 3.5.1] First, observe that

$$\sum_{f \in G_m\setminus\{e\}} Y_{e,f}(G_m) = \sum_{f \in G_m\setminus\{e\}} \sum_{K \ni e,f} 1\{K \subseteq G_m \cup \{e\}\}. \tag{3.63}$$

Exchanging the order of the sums, we obtain

$$\sum_{f \in G_m\setminus\{e\}} Y_{e,f}(G_m) = \sum_{K \ni e} \sum_{f \in K\setminus\{e\}} 1\{K \subseteq G_m \cup \{e\}\} \tag{3.64}$$

$$= \left(\binom{k}{2} - 1\right) Y_e(m). \tag{3.65}$$

Now, recall that we have $Y_f(G_m) \geq (1 - g_Y(m))\widetilde{Y}(m)$ for every $m < \tau$. From Proposition 3.5.4, it follows that

$$\mathbb{E}\left(\Delta Y_e(G_m)\middle|\mathcal{F}_m\right) \leq -(1 - g_Y(m))\left(\binom{k}{2} - 1\right)\frac{\widetilde{Y}(m)Y_e(m)}{Q(G_m)} \pm E_3. \tag{3.66}$$

Moreover, as $Q(G_m) \le (1+g_Q(m))\widetilde{Q}(m)$ and $\widetilde{Y}(m) = \binom{k}{2}\widetilde{Q}(m)/e(G_m)$, it follows that

$$\mathbb{E}\left(\Delta Y_e(G_m)\middle|\mathcal{F}_m\right) \le -(1-g_Y(m)-g_Q(m))\left(\binom{k}{2}^2 - \binom{k}{2}\right)\frac{Y_e(G_m)}{e(G_m)} \pm E_3. \tag{3.67}$$

As the event $A_e(i,j)$ holds, we also have $Y_e(G_m) \ge (1+g_Y(m)/2)\widetilde{Y}(m)$ for all $m \ge i$. Now, we would like to replace $Y_e(G_m)$ in the right-hand side of (3.67) by this lower bound. Before that, let us bound the cumulative error coming from $g_Q$ and $g_Y$. As $g_Q(m) \le g_Y(m)/5$, we have

$$\begin{aligned}\big(1-g_Q(m)-g_Y(m)\big)\big(1+g_Y(m)/2\big) &\ge \big(1-4g_Y(m)/5\big)\big(1+g_Y(m)/2\big)\\ &\ge 1-3g_Y(m)/10-2g_Y(m)^2/5\\ &\ge 1-3g_Y(m)/4.\end{aligned}$$

Finally, replacing $Y_e(G_m)$ by $(1+g_Y(m)/2)\widetilde{Y}(m)$ in the right-hand side of (3.67) and using the last inequality above, we obtain

$$\mathbb{E}\left(\Delta Y_e(G_m)\middle|\mathcal{F}_m\right) \le -(1-3g_Y(m)/4)\left(\binom{k}{2}^2 - \binom{k}{2}\right)\frac{\widetilde{Y}(m)}{e(G_m)} \pm E_3 \tag{3.68}$$

for all $m \ge i$, provided the event $A_e(i,j)$ holds. We remark that this is why we need to use the bound $Y_e(G_m) \ge (1+g_Y(m)/2)\widetilde{Y}(m)$. If we only use the crude bound $Y_e(G_m) \ge (1-g_Y(m))\widetilde{Y}(m)$, the coefficient of $g_Y(m)$ would be bigger than 1. This would not be enough to show that $Z_m$ is a supermartingale.

Recall that $Z_m^e = Y_e(G_m) - (1+g_Y(m))\widetilde{Y}(m)$ if $m \le \tau$. Combining Claim 3.5.3 with (3.68), we obtain

$$\mathbb{E}\left(\Delta Z_m^e\middle|\mathcal{F}_m\right) \le -\frac{g_Y(m)}{4}\left(\binom{k}{2}^2 - \binom{k}{2}\right)\frac{\widetilde{Y}(m)}{e(G_m)} \pm (E_1+E_2+E_3). \tag{3.69}$$

From the definitions of the error functions $E_1$ and $E_2$ (see (3.53)), we can easily see that

$$E_1 + E_2 = o\left(\frac{g_Y(m)\widetilde{Y}(m)}{e(G_m)}\right).$$

For $E_3$, recall that

$$E_3 \le \frac{4\widetilde{Y}(m)k^3n^\delta}{\widetilde{Q}(m)} \cdot \max\{1, \mathbb{E}(Y_S(G_0))\}. \tag{3.70}$$

We claim that

$$k^3n^\delta \max\{1, \mathbb{E}(Y_S(G_0))\} \le \binom{k}{2}\frac{(g_Q\widetilde{Q})(m)}{4e(G_m)}. \tag{3.71}$$

In fact, by definition of $\widetilde{Q}$ and $g_Q$, we can see that $(g_Q\widetilde{Q})(m) \ge n^{-\delta}\widetilde{Q}(0)$. As $e(G_m) = \Theta(n^2)$, (3.71) clearly holds if $\mathbb{E}(Y_S(G_0)) > 1$. On the other hand, if $\mathbb{E}(Y_S(G_0)) < 1$, then the left-hand side of (3.71) is equal to $k^3n^\delta$. As $(g_Q\widetilde{Q})(m) \ge n^{-\delta}\widetilde{Q}(0) \ge n^{\gamma-\delta+o(1)}$, the inequality follows from the choice of $\delta$ in this case. Multiplying both sides of (3.71) by $4\widetilde{Y}(m)/\widetilde{Q}(m)$ and using (3.70), we obtain

$$E_3 \le \binom{k}{2}\frac{(g_Q\widetilde{Y})(m)}{e(G_m)}$$

and hence

$$E_3 \le \frac{1}{8}\binom{k}{2}^2\frac{(g_Y\widetilde{Y})(m)}{e(G_m)}.$$

It follows that the sum of the errors $E_1 + E_2 + E_3$ is very small compared with the leading term of (3.69). Therefore, we conclude that $\{(Z_m^e, \mathcal{F}_m) : m \ge \tau_-^e\}$ is a supermartingale conditioned on the event $A_e(i,j)$. $\square$

Now we proceed to the proof of Lemma 3.5.2.

*Proof.* [Proof of Lemma 3.5.2] We begin with part $(i)$. For any $m < \tau$, it suffices to show that $|\Delta Y_e(G_m)|$ and $|\Delta\widetilde{Y}(m) + \Delta(g_Y\widetilde{Y})(m)|$ are bounded by $k^2n^\delta \max\{1, \mathbb{E}(Y_S(G_0))\}$. Let $K$ denote the $k$-clique chosen at step $m$. Then, we have

$$\begin{aligned}|\Delta Y_e(G_m)| &\le \sum_{f\in K\setminus\{e\}} Y_{e,f}(G_m) \\ &\le \binom{k}{2}\max\big\{Y_S(G_0) : |S| = 3\big\}. \end{aligned}\tag{3.72}$$

As $G_m \subseteq G_0$, we have $Y_S(G_m) \leq Y_S(G_0)$ and hence $Y_S(G_m) \leq n^\delta \max\{1, \mathbb{E}(Y_S(G_0))\}$. This combined with (3.72) provides the required upper bound for $|Y_e(G_m)|$. For the absolute value $|\Delta\widetilde{Y}(m) + \Delta(g_Y\widetilde{Y})(m)|$, we simply use Claim 3.5.3. By this claim, we have

$$|\Delta\widetilde{Y}(m) + \Delta(g_Y\widetilde{Y})(m)| \leq \frac{4k^4\widetilde{Y}(m)}{e(G_m)}. \tag{3.73}$$

By the assumptions on $G_0$ (recall that $G_0$ does not satisfy $F_0$), we have $\widetilde{Y}(m) \leq \widetilde{Y}(0) \leq 2\,\mathbb{E}(Y_e(G_0))$ and $e(G_m) \geq pn^2/4$. These imply that

$$\begin{aligned} |\Delta\widetilde{Y}(m) + \Delta(g_Y\widetilde{Y})(m)| &\leq \frac{2^5k^4\,\mathbb{E}(Y_e(G_0))}{pn^2} \\ &\leq k^2n^\delta \max\{1, \mathbb{E}(Y_S(G_0))\}. \end{aligned}$$

The second inequality follows from the choice of $\delta$.

Now let us prove part $(ii)$. By (3.73), it suffices to show that

$$\mathbb{E}\left(|\Delta Y_e(G_m)|\big|\mathcal{F}_m\right) = O\left(\frac{k^4\widetilde{Y}(\tau_-^e)}{pn^2}\right).$$

Recall that, by Proposition 3.5.4, we have

$$\mathbb{E}\left(|\Delta Y_e(G_m)|\big|\mathcal{F}_m\right) \;=\; \frac{1}{Q(G_m)} \sum_{f \in E(G_m)\setminus\{e\}} Y_{e,f}(G_m)Y_f(G_m) \;\pm\; E_3, \tag{3.74}$$

where the error term $E_3$ is given by

$$E_3 = \frac{2\widetilde{Y}(m)k^3n^\delta}{\widetilde{Q}(m)} \cdot \max\{1, \mathbb{E}(Y_S(G_0))\}. \tag{3.75}$$

In the proof of Lemma 3.5.1, we bounded a quantity similar to the error $E_3$ (see (3.71)). By (3.71), it easily follows that

$$E_3 \leq \frac{k^4\widetilde{Y}(m)}{pn^2}.$$

Now, it remains to bound the leading term of $\mathbb{E}\left(|\Delta Y_e(G_m)|\big|\mathcal{F}_m\right)$ in (3.74).

Observe that

$$\sum_{f \in E(G_m) \setminus \{e\}} Y_{e,f}(G_m) = \left( \binom{k}{2} - 1 \right) Y_e(G_m).$$

Moreover, on the event $m < \tau$ we have $Y_f(G_m) \leq (1 + g_Y(m))\widetilde{Y}(m)$ for all $f \in E(K_n)$. These imply that the leading term of $\mathbb{E}\left(|\Delta Y_e(G_m)| \big| G_m\right)$ in (3.74) is upper bounded by

$$(1 + g_Y(m)) \left( \binom{k}{2} - 1 \right) \frac{Y_e(G_m)\widetilde{Y}(m)}{Q(G_m)}.$$

As $Q(G_m) \geq (1 - g_Q(m))\widetilde{Q}(m)$ and $Y_e(G_m) \leq (1 + g_Y(m))\widetilde{Y}(m)$, combining (3.74) with the bound on the leading term we obtain

$$\begin{aligned} \mathbb{E}\left(|\Delta Y_e(G_m)| \big| G_m\right) &\leq \frac{4k^2(\widetilde{Y}(m))^2}{\widetilde{Q}(m)} \pm E_3. \\ &\leq \frac{8k^4\widetilde{Y}(m)}{pn^2}. \end{aligned}$$

This concludes our proof. □

## 3.6 Upper bounds

In this section we prove Theorems 3.1.2 and 3.1.3. The main idea is to work with $G(n, m)$ instead of $G(n, p)$. The random graph $G(n, m)$ is defined to be a graph uniformly selected from graphs with vertex set $[n]$ which have exactly $m$ edges. Note that if we condition $G(n, p)$ to have exactly $m$ edges then the resulting random graph is distributed as $G(n, m)$.

Let $\mathbb{P}_p$ and $\mathbb{P}_m$ denote the probability distributions of $G(n, p)$ and $G(n, m)$, respectively. For any event $E$ we have

$$\mathbb{P}_p(E) = \sum_{m=0}^{N} \mathbb{P}_p\big(e(G(n,p)) = m\big)\mathbb{P}_m(E),$$

where $N := \binom{n}{2}$. Let $E_t$ be the event that $G(n,p)$ contains $t$ edge-disjoint $k$-cliques. Since $E_t$ is a monotone increasing property, we have

$$\mathbb{P}_p(E_t) \leq \mathbb{P}_m(E_t) + \mathbb{P}_p\big(e(G(n,p)) > m\big) \tag{3.76}$$

for any value of $m$. Now, define

$$m_+(p) := \lfloor pN + n^{3/2} \rfloor.$$

By Chernoff's inequality, we have that $\mathbb{P}_p\big(e(G(n,p)) > m_+\big) \leq \exp(-2^4 np)$. Then, to prove that $\nu_k(p) \leq t$ with high probability it suffices to show that $\mathbb{P}_{m_+(p)}(E_t) = o(1)$. This is done in our next lemma.

**Lemma 3.6.1.** *For all $\gamma > 2$ and $p \in (0,1)$ there is a constant $A = A(\gamma,p) = 5p(\gamma - 2)/(1-p)$ such that with high probability the random graph $G(n, m_+(p))$ does not contain $An^2 \log n/k^4$ edge-disjoint $k$-cliques.*

The proof of Theorem 3.1.2 can be easily deduced from Lemma 3.6.1. We omit the details. Lemma 3.6.1 is proved by a straightforward first moment argument. To do so, we first need an upper bound on the probability that $G(n, m_+(p))$ contains a fixed set of $An^2 \log n/k^4$ edge-disjoint $k$-cliques. This is done in our next proposition.

**Proposition 3.6.2.** *Let $p \in (0,1)$ and $A > 0$ be constants and $t = An^2 \log n/k^4$. Let $F$ be a set with $t\binom{k}{2}$ edges. We have*

$$\mathbb{P}_{m_+}\Big(F \subseteq G(n,m_+)\Big) \leq \exp\left(t\left[\binom{k}{2}\log p - \frac{A(1-p+o(1))\log n}{4p}\right]\right).$$

*Proof.* By simplicity, let us set $\mathbb{P} = \mathbb{P}_{m_+(p)}$ and $G = G(n,m_+)$. Note that the probability $\mathbb{P}(F \subseteq G)$ can be written as

$$\mathbb{P}(F \subseteq G) = \frac{(m_+)_{e(F)}}{(N)_{e(F)}},$$

where $(m)_a$ denotes the falling factorial $m(m-1)\dots(m-a+1)$. We may now use that $e(F) = t\binom{k}{2} = (1+o(1))tk^2/2$ and that $m_+/N \leq p(1+n^{-1/4})$ to deduce that

$$\begin{aligned}
\mathbb{P}(F \subseteq G) &\leq p^{t\binom{k}{2}}(1+n^{-1/4})^{tk^2/2} \prod_{i=0}^{t\binom{k}{2}-1} \frac{1-i/m_+}{1-i/N} \\
&\leq p^{t\binom{k}{2}}(1+n^{-1/4})^{tk^2/2} \exp\left( - \sum_{i=0}^{t\binom{k}{2}-1} \left( \frac{i}{m_+} - \frac{i}{N} - \frac{O(1)i^2}{N^2} \right) \right) \\
&\leq p^{t\binom{k}{2}} \cdot \exp\left( t \left[ - \frac{tk^4}{8} \left( \frac{1}{m_+} - \frac{1}{N} \right) + O(1) \right] \right).
\end{aligned}$$

Recall that $t = An^2 \log n/k^4$. We also have $1/m_+ - 1/N = (2+o(1))(1-p)/pn^2$. Then, it follows that

$$\begin{aligned}
\mathbb{P}(F \subseteq G) &\leq \exp\left( t \left[ \binom{k}{2} \log p - \frac{An^2 \log n}{8} \left( \frac{1}{m_+} - \frac{1}{N} \right) \right] \right) \\
&\leq \exp\left( t \left[ \binom{k}{2} \log p - \frac{A(1-p+o(1)) \log n}{4p} \right] \right),
\end{aligned}$$

as required $\square$

We can now easily deduce Lemma 3.6.1 from Proposition 3.6.2. In what follows, we denote by $\mathcal{K}(n,t,k)$ the family of all sets of $t$ edge-disjoint $k$-cliques in $K_n$.

*Proof.* [Proof of Lemma 3.6.1] Let $G \sim G(n, m_+)$ and $A > 0$ be a constant that we may fix later. Let $X$ be the random variable which counts how many sets of $t = An^2 \log n/k^4$ edge-disjoint $k$-cliques are contained in $G$. It suffices to prove that (for an appropriate choice of $A$) we have $\mathbb{E}(X) \to 0$. Let $F$ be any any set with $t\binom{k}{2}$ edges. We have

$$\begin{aligned}
\mathbb{E}(X) &= |\mathcal{K}(n,t,k)| \mathbb{P}\big(F \subseteq G\big) \\
&\leq \frac{\binom{n}{k}^t}{t!} \cdot \mathbb{P}\big(F \subseteq G\big).
\end{aligned}$$

As $\binom{n}{k}p^{\binom{k}{2}} = n^{\gamma+o(1)}$, by Proposition 3.6.2 we have

$$\mathbb{E}(X) \leq \exp\left(t\left[(\gamma+o(1))\log n - \log t - \frac{A(1-p+o(1))\log n}{4p}\right]\right).$$

As $\log t = (2+o(1))\log n$, the last expression converges to 0 if we choose $A = 5p(\gamma-2)/(1-p)$. This proves our lemma. $\square$

We have now proved Theorem 3.1.2, which gives an upper bound $A(\gamma,p)n^2\log n/k^4$ on the number of edge-disjoint $k$-cliques we may find in $G(n,p)$. As mentioned in the introduction of this chapter, this almost confirms Theorem 3.1.3. However, $A(\gamma,p) = 5p(\gamma-2)/(1-p)$ blows up as $p$ approaches 1. To prove Theorem 3.1.3, we shall need a bound on $|\mathcal{K}(n,t,k)|$ which is better than the trivial bound $\binom{n}{t}^t/t!$ used to prove Lemma 3.6.1.

In [3], Acan and Kahn consider the question of how many ways there are to select $t$-edge-disjoint $k$-cliques in $K_n$. They improve on the trivial upper bound $\binom{n}{k}^t/t!$ by a factor $\zeta(n,k,t)$. More precisely, they showed that there exists $\beta > 0$ such that

$$|\mathcal{K}(n,k,t)| \leq \exp\left(\frac{-\beta t^2k^4}{n^2}\right)\cdot\frac{1}{t!}\binom{n}{k}^t \tag{3.77}$$

for all $t \leq en^2/k^3$.

We are now ready to prove Theorem 3.1.3:

*Proof.* [Proof of Theorem 3.1.3] Let $p' := \max\{2^{-1}, e^{-\beta}\}$, where $\beta > 0$ is such that (3.77) holds for all $t \leq en^2/k^3$. Let $A(p) = 2\beta^{-1}p(\gamma-2)$. We will show that for all $p \in (p',1)$ the following holds: with high probability $G(n,p)$ does not contain $An^2\log n/k^4$ edge-disjoint $k$-cliques. Observe that this together with Theorem 3.1.2 proves Theorem 3.1.3.

For now on, we fix $p \in (p',1)$ and $t = An^2\log n/k^4$. We proceed as in the proof of Theorem 3.6.1 and use the first moment method combined with the bound (3.77). Before we proceed to applying the bound (3.77), we shall first check that $t \leq en^2/k^3$. In fact, as

$p \in (p', 1)$, we have $\log(1/p) < \beta$ and hence

$$k = (2 + o(1)) \log_{1/p} n > 2\beta^{-1} \log n.$$

This implies that $t \leq (\gamma - 2)n^2/k^3$, which is less than $en^2/k^3$.

Let $X$ be the random variable which counts how many sets of $t$ edge-disjoint cliques are contained in $G\big(n, p\big)$. We have

$$\mathbb{E}(X) = |\mathcal{K}(n, k, t)| p^{\binom{k}{2} t}.$$

As $\binom{n}{k} p^{\binom{k}{2}} = n^{\gamma + o(1)}$, by (3.77) it follows that

$$\mathbb{E}(X) \leq \exp\left( t \left[ (\gamma + o(1)) \log n \, - \, \log t \, - \, \frac{\beta t k^4}{n^2} \right] \right).$$

As $t = An^2 \log n / k^4$ and $\log t = (2 + o(1)) \log n$, we have

$$\mathbb{E}(X) \leq \exp\Big( t \log n \Big( \gamma - 2 - A\beta + o(1) \Big) \Big).$$

As $A\beta > \gamma - 2$ we have $\mathbb{E}(X) \to 0$ as required. $\square$

CHAPTER 4

# ASYMMETRIC RAMSEY PROPERTIES OF RANDOM GRAPHS INVOLVING CLIQUES AND CYCLES

The work in this chapter is joint with Liebenau, Mendonça and Skokan. It is adapted from the article [72] which will appear in *Random Structures and Algorithms*.

## 4.1 Introduction

We say that a graph $G$ is a *Ramsey graph for the pair of graphs* $(F, H)$ if, in every edge colouring $c : E(G) \to \{1, 2\}$, we can find either a 1-coloured copy of $F$ or a 2-coloured copy of $H$. We write $G \to (F, H)$ if $G$ is Ramsey for $(F, H)$, and $G \not\to (F, H)$ otherwise. It follows from Ramsey's Theorem [93] that, for each pair of graphs $(F, H)$, there exists a graph $G$ such that $G \to (F, H)$.

In a series of papers [40, 95, 97] it was shown that the probability threshold for $G(n, p) \to (F, F)$ is of order $n^{-1/m_2(F)}$ for almost all non-empty graphs $F$, where

$$m_2(F) := \max\left\{\frac{e(J)-1}{v(J)-2} : J \subseteq F, v(J) \geq 3\right\}.$$

The parameter $m_2(F)$ is called the $m_2$-density of the graph $F$. A natural generalisation of this problem is to determine a threshold function $p(F, H)$ for the property $G(n, p) \to (F, H)$, for any asymmetric pair of graphs $(F, H)$.

The problem of determining the threshold function $p(F, H)$ was posed in 1997 by Kohayakawa and Kreuter [67], who conjectured that $p(F, H) = \Theta(n^{-1/m_2(F,H)})$, where

$$m_2(F, H) := \max\left\{\frac{e(J)}{v(J)-2+1/m_2(H)} : J \subseteq F, e(J) \geq 1\right\},$$

for any pair of graphs such that $m_2(F) \geq m_2(H) \geq 1$. In a recent breakthrough, Mousset, Nenadov and Samotij [86] showed that $p(F, H) = O(n^{-1/m_2(F,H)})$ whenever $m_2(F) \geq$

$m_2(H) \geq 1$, the so-called 1-*statement*. In contrast, much less is known about the 0-*statement*, that is, the statement that $p(F,H) = \Omega(n^{-1/m_2(F,H)})$ whenever $m_2(F) \geq m_2(H) \geq 1$. One possible reason for that is that the 0-statement seems to depend on the structural behaviour of Ramsey graphs.

In this chapter, we show that the 0-*statement* holds for any pair of cliques and cycles. This is the first 0-statement result for different types of graphs.

**Theorem 4.1.1.** *For all $\ell, r \geq 4$ there exists $c > 0$ such that, if $p = p(n) \leq cn^{-1/m_2(K_r,C_\ell)}$, then*

$$\lim_{n\to\infty} \mathbb{P}\big[G(n,p) \to (K_r, C_\ell)\big] = 0.$$

Combining Theorem 4.1.1 with the results of [67], [81] and [86], we establish the Kohayakawa–Kreuter conjecture for any pair of cycles and cliques with at least 3 vertices.

The main tool behind the proof of Theorem 4.1.1 is a structural characterisation of Ramsey graphs for the pair $(K_r, C_\ell)$ via a 'container type' argument (see Theorem 4.2.1), which is a rephrasing of the idea used in previous works. Roughly speaking, we find a family $\mathcal{I}$ of graphs with the following properties: (a) $|\mathcal{I}|$ is small; (b) for every graph $G$ with $G \to (K_r, C_\ell)$ there exists $I \in \mathcal{I}$ such that $I \subseteq G$; and (c) for each $I \in \mathcal{I}$, either $I$ is small and dense or very structured. We provide the details in Section 4.2.

The rest of the chapter is organised as follows. In Section 4.2, we prove Theorem 4.1.1; in Section 4.3, we provide the main technical lemmas of this chapter; in Section 4.4, we prove some structural lemmas about Ramsey graphs; in Section 4.5, we describe the algorithms used to prove our main technical theorem (see Theorem 4.2.1); finally, in Section 4.6, we do a careful analysis of these algorithms. In Section 4.7, we provide some simple calculations involving $m_2$-densities, for completeness.

## 4.2 The main technical result

In this section, we present the main technical result of this paper and deduce Theorem 4.1.1 from it. In order to state this result, we need the following notation. For a graph $G$, define $\lambda(G)$ by

$$\lambda(G) = v(G) - \frac{e(G)}{m_2(K_r, C_\ell)}.$$

This parameter plays an important role in our analysis, as the expected number of copies of $G$ in $G(n,p)$ is of order $c^{e(G)}n^{\lambda(G)}$ when $p = cn^{-1/m_2(K_r,C_\ell)}$. For any positive real numbers $M, \varepsilon$ and any positive integer $n$, define

$$\mathcal{J}_1(\varepsilon) = \{G : \lambda(G) \leq -\varepsilon\} \qquad \text{and} \qquad \mathcal{J}_2(M,n) = \{G : \lambda(G) \leq M \text{ and } e(G) \geq \log n\}, \tag{4.1}$$

where the logarithm is in base 2. Finally, for any natural numbers $r, \ell$ and $n$, let

$$\mathcal{R}_n(K_r, C_\ell) = \big\{G : V(G) = [n] \text{ and } G \to (K_r, C_\ell)\big\},$$

where $[n] := \{1, 2, \cdots, n\}$. When $r$ and $\ell$ are clear from context, we write $\mathcal{R}_n$ for $\mathcal{R}_n(K_r, C_\ell)$. In addition, we set

$$\mathcal{R}(K_r, C_\ell) = \bigcup_{n \in \mathbb{N}} \mathcal{R}_n(K_r, C_\ell).$$

The connection between $\lambda$, $\mathcal{J}_1(\varepsilon)$, $\mathcal{J}_2(M,n)$ and $\mathcal{R}_n$ is contextualised in the next theorem.

**Theorem 4.2.1.** *For any integers $r, \ell \geq 4$, there exist positive constants $M = M(r,\ell)$ and $\varepsilon = \varepsilon(r,\ell)$ such that the following holds. For every positive integer $n$, there exists a function $f : \mathcal{R}_n(K_r, C_\ell) \to \mathcal{J}_1(\varepsilon) \cup \mathcal{J}_2(M,n)$ such that $G$ contains a copy of $f(G)$ as a subgraph, for all $G \in \mathcal{R}_n$, and*

$$|f(\mathcal{R}_n)| \leq (\log n)^M.$$

In the language of hypergraph containers [6, 108], Theorem 4.2.1 provides a relatively small collection $f(\mathcal{R}_n)$ of *fingerprints*. Additionally to $|f(\mathcal{R}_n)|$ being small, each graph $f(G)$ either has a *very* small value of $\lambda$ (negative, and bounded away from 0), or a fairly small (though possibly positive) value of $\lambda$ and is *very* large. To obtain such a collection and the function $f$ in Theorem 4.2.1, we employ an algorithm adapted from [71].

Theorem 4.1.1 is easily deduced from Theorem 4.2.1. The proof of Theorem 4.2.1 is given in the next four sections.

*Proof.* [Proof of Theorem 4.1.1] Given $r, \ell \geq 4$, let $M$ and $\varepsilon$ be positive constants given by Theorem 4.2.1 and set $c = 2^{-2M}$. For each $n \in \mathbb{N}$, let $p = p(n) \leq cn^{-1/m_2(K_r, C_\ell)}$. Let $f$ be the function given by Theorem 4.2.1, let $\Gamma \sim G(n,p)$ and suppose that $\Gamma \in \mathcal{R}_n$. Then, $f(\Gamma) \subseteq \Gamma$ and $f(\Gamma) \in \mathcal{J}_1(\varepsilon) \cup \mathcal{J}_2(M,n)$. Let $\mathcal{I}_1 := f(\mathcal{R}_n) \cap \mathcal{J}_1(\varepsilon)$ and $\mathcal{I}_2 := f(\mathcal{R}_n) \cap \mathcal{J}_2(M,n)$. Thus,

$$\mathbb{P}\big(\Gamma \to (K_r, C_\ell)\big) \leq \mathbb{P}\big(F \subseteq \Gamma \text{ for some } F \in \mathcal{I}_1 \cup \mathcal{I}_2\big). \tag{4.2}$$

Since $\lambda(F) \leq -\varepsilon$ for each $F \in \mathcal{I}_1$ and $c \leq 1$, we have

$$\mathbb{P}(F \subseteq \Gamma) \leq n^{v(F)} p^{e(F)} \leq c^{e(F)} n^{\lambda(F)} \leq n^{-\varepsilon} \tag{4.3}$$

for every $F \in \mathcal{I}_1$. Similarly, we have

$$\mathbb{P}(F \subseteq \Gamma) \leq c^{e(F)} n^{\lambda(F)} \leq n^{-M} \tag{4.4}$$

for every $F \in \mathcal{I}_2$, as $\lambda(F) \leq M$ and $e(F) \geq \log n$ for each $F \in \mathcal{I}_2$, and by our choice of $c$. Applying the union bound to (4.2) and using (4.3) and (4.4), we obtain that

$$\mathbb{P}\big(G(n,p) \to (K_r, C_\ell)\big) \leq (\log n)^M \cdot (n^{-\varepsilon} + n^{-M}),$$

since $|\mathcal{I}_1 \cup \mathcal{I}_2| \leq (\log n)^M$. As the expression on the right hand side tends to 0 as $n \to \infty$, this implies the theorem. $\square$

## 4.3 Proof of Theorem 4.2.1

In this section, we state the main technical lemmas of this paper, and deduce Theorem 4.2.1 from them. We also introduce some notation that we use during the proof.

Let $r, \ell$ be positive integers. We follow the approach by [67] and [71] and bring our problem into the hypergraph setting. Given a graph $G = (V, E)$, let $\mathcal{G}_{r,\ell}(G)$ be the hypergraph on the edge set of $G$ whose hyperedges correspond to the copies of $K_r$ and $C_\ell$ in $G$. We suppress $G$, $r$ and $\ell$ from the notation whenever they are clear from context. Define

$$\mathcal{E}_1(\mathcal{G}) = \{E(F) : F \cong K_r, F \subseteq G\} \text{ and } \mathcal{E}_2(\mathcal{G}) = \{E(F) : F \cong C_\ell, F \subseteq G\}. \tag{4.5}$$

Analogously, if $\mathcal{H} \subseteq \mathcal{G}_{r,\ell}(G)$, then we set $\mathcal{E}_1(\mathcal{H}) := \mathcal{E}_1(\mathcal{G}) \cap E(\mathcal{H})$ and $\mathcal{E}_2(\mathcal{H}) := \mathcal{E}_2(\mathcal{G}) \cap E(\mathcal{H})$.

The reason why we deal with $\mathcal{G}_{r,\ell}(G)$ instead of $G$ is as follows. In order to build our fingerprints algorithmically, we would like to deal with a subgraph $H$ of $G$ which has the two following properties: (1) every edge $e \in E(H)$ is contained in an $\ell$-cycle; (2) for *every* copy $C$ of $C_\ell$ in $H$ end every $e \in C$, there exists a copy $K$ of $K_r$ such that $E(K) \cap E(C) = \{e\}$. These properties would allow us to build the fingerprint of $G$ algorithmically by attaching either a copy of $K_r$ or a copy of $C_\ell$ to the current graph at each step. However, such a graph $H$ might not exist. Even if $H$ is minimal (with respect to subgraph containment) for $H \to (K_r, C_\ell)$, we can only deduce that for every $e \in E(H)$ there exist $K \cong K_r$ and $C \cong C_\ell$ in $H$ such that $E(K) \cap E(C) = \{e\}$. But this does not directly imply that property (2) holds. We can overcome this problem by considering subhypergraphs of $\mathcal{G}_{r,\ell}(G)$ which are $\star$-critical. This property was first considered in [71].

**Definition 4.3.1** ($\star$-critical)**.** *Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be two families of sets on a vertex set. We say that a hypergraph $\mathcal{H} = \mathcal{E}_1 \cup \mathcal{E}_2$ is $\star$-critical with respect to $(\mathcal{E}_1, \mathcal{E}_2)$ if the following two properties hold. For each $e \in V(\mathcal{H})$, there exists a hyperedge $F \in \mathcal{E}_2$ such that $e \in F$; and*

*for each $F \in \mathcal{E}_2$ and each $e \in F$, there exists a hyperedge $E \in \mathcal{E}_1$ such that $E \cap F = \{e\}$. When $\mathcal{E}_1$ and $\mathcal{E}_2$ are clear from context, we say that the hypergraph $\mathcal{H}$ is $\star$-critical.*

Let $\mathrm{Crit}_{r,\ell}(G)$ be the set of all $\star$-critical subhypergraphs of $\mathcal{G}_{r,\ell}(G)$. The next lemma shows that if $G \to (K_r, C_\ell)$, then there are subhypergraphs of $\mathcal{G}_{r,\ell}(G)$ which are $\star$-critical. We prove it in Section 4.4.

**Lemma 4.3.2.** *Let $r, \ell \geq 4$ be integers. If $G \to (K_r, C_\ell)$, then $\mathrm{Crit}_{r,\ell}(G) \neq \emptyset$.*

Given a hypergraph $\mathcal{H} \subseteq \mathcal{G}_{r,\ell}(G)$, we define the *underlying graph of* $\mathcal{H}$, denoted by $\mathbf{G}(\mathcal{H})$, to be the subgraph of $G$ whose edge set is $\bigcup_{E \in E(\mathcal{H})} E$. The following lemma is central to our proof. We prove it in Section 4.4.

**Lemma 4.3.3.** *Let $r, \ell \geq 4$ be integers. There exists $\varepsilon = \varepsilon(r, \ell) > 0$ such that the following holds for any graph $H$. If $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(H)$, then $\lambda\big(\boldsymbol{G}(\mathcal{H})\big) \leq -\varepsilon$.*

In order to find the function $f : \mathcal{R}_n(K_r, C_\ell) \to \mathcal{J}_1(\varepsilon) \cup \mathcal{J}_2(M, n)$ in Theorem 4.2.1, we define an algorithm Hypertree in Section 4.5. For each $G \in \mathcal{R}_n(K_r, C_\ell)$, this algorithm takes some hypergraph $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(G)$ as input and creates a subhypergraph $\mathcal{H}_T \subseteq \mathcal{H}$ as output. The fingerprint $f(G)$ will be a graph isomorphic to $\mathbf{G}(\mathcal{H}_T)$. For the detailed description of Hypertree, we refer the reader to Section 4.5.

Let Hypertree$(\mathcal{H})$ denote the execution of Hypertree on input $\mathcal{H}$. Its basic properties are given by the next lemma.

**Lemma 4.3.4.** *Let $n, r, \ell \geq 4$ be integers and $G$ be a graph on vertex set $[n]$. For any hypergraph $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(G)$,* Hypertree$(\mathcal{H})$ *generates a sequence of hypergraphs $\mathcal{H}_0 \subseteq \ldots \subseteq \mathcal{H}_T \subseteq \mathcal{H}$ for which the following holds.*

(a) *$\mathcal{H}_0 = \{E\}$, for some $E \in \mathcal{E}_1(\mathcal{H})$; that is, the underlying graph of $\mathcal{H}_0$ is a copy of $K_r$ in $G$;*

(*b*) $v(\mathcal{H}_0) < v(\mathcal{H}_1) < \ldots < v(\mathcal{H}_T)$;

(*c*) $T$ *is the smallest integer such that* $\lambda(G_T) \leq -\varepsilon$ *or* $T \geq \log n$, *where* $G_T = \boldsymbol{G}(\mathcal{H}_T)$ *and* $\varepsilon$ *is the constant given by Lemma* 4.3.3;

(*d*) HYPERTREE($\mathcal{H}$) *returns* $\mathcal{H}_T$.

Our next lemma is one of the most important properties of the HYPERTREE algorithm. We shall use it together with Lemma 4.3.4 to deduce that the underlying graph given by the output of HYPERTREE($\mathcal{H}$) belongs to $\mathcal{J}_1(\varepsilon) \cup \mathcal{J}_2(M, n)$ whenever $\mathcal{H}$ is a hypergraph in $\mathrm{Crit}_{r,\ell}(G)$, where $M = M(r, \ell) > 0$. As the underlying graph of the output hypergraph is a subgraph of $G$, this will establish the existence of a function $f : \mathcal{R}_n(K_r, C_\ell) \to \mathcal{J}_1(\varepsilon) \cup \mathcal{J}_2(M, n)$ as required for Theorem 4.2.1.

**Lemma 4.3.5.** *Let* $r, \ell \geq 4$ *be integers,* $G$ *a graph and* $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(G)$. *Let* $(\mathcal{H}_i)_{i=0}^T$ *be the sequence generated by* HYPERTREE($\mathcal{H}$) *and let* $G_i = \boldsymbol{G}(\mathcal{H}_i)$ *for each* $i \in \{0, \ldots, T\}$. *Then we have*

$$\lambda(G_i) \leq \lambda(G_{i-1})$$

*for each* $i \in \{1, \ldots, T\}$.

We prove a stronger version of this lemma (Lemma 4.6.1) in Section 4.6. For each $n, r, \ell \geq 4$, consider the family of possible output graphs of HYPERTREE($\mathcal{H}$)

$$\mathrm{Out}_{r,\ell}(n) = \bigcup_{G\,:\,V(G)=[n]} \big\{\mathbf{G}(\mathcal{H}_T) \;:\; \mathcal{H} \in \mathrm{Crit}_{r,\ell}(G)\big\},$$

where $T = T(\mathcal{H})$ and $\mathcal{H}_T$ are the stopping time and the output given by HYPERTREE($\mathcal{H}$), respectively. The set $\mathrm{Out}_{r,\ell}(n)$ will, of course, be rather large and we cannot hope for $|\mathrm{Out}_{r,\ell}(n)|$ to be bounded by a function that is poly-logarithmic in $n$. Instead, we restrict to

our attention to isomorphism classes. For a set $S$ of graphs, denote by $S/_{\cong}$ a set consisting of exactly one representative graph for every (graph) isomorphism class of $S$. The next lemma bounds the size of $\mathrm{Out}_{r,\ell}(n)/_{\cong}$.

**Lemma 4.3.6.** *For all $r, \ell \geq 4$, there exists $C > 0$ such that $|\mathrm{Out}_{r,\ell}(n)/_{\cong}| \leq (\log n)^C$, for all $n \in \mathbb{N}$.*

We prove this lemma in Section 4.6. Now, we are ready to prove Theorem 4.2.1 assuming all the lemmas stated in this section.

*Proof.* [Proof of Theorem 4.2.1] Fix $n, r, \ell \geq 4$. For each $G \in \mathcal{R}_n(K_r, C_\ell)$, let $\mathcal{H}(G)$ be a $\star$-critical hypergraph in $\mathrm{Crit}_{r,\ell}(G)$. By Lemma 4.3.2, such a hypergraph must exist. Let $(\mathcal{H}_i(G))_{i=0}^T$ be the sequence of hypergraphs generated by HYPERTREE($\mathcal{H}(G)$). By Lemma 4.3.4, the last hypergraph of this sequence, namely $\mathcal{H}_T(G)$, is the hypergraph output by HYPERTREE($\mathcal{H}(G)$).

Define

$$\begin{aligned} f : \mathcal{R}_n &\to \mathrm{Out}_{r,\ell}(n)/_{\cong} \\ G &\mapsto [\mathbf{G}(\mathcal{H}_T(G))], \end{aligned}$$

where by $[\mathbf{G}(\mathcal{H}_T(G))]$ we denote the graph $G' \in \mathrm{Out}_{r,\ell}(n)/_{\cong}$ isomorphic to $\mathbf{G}(\mathcal{H}_T(G))$. As $\mathcal{H}_T(G) \subseteq \mathcal{H}(G)$ by Lemma 4.3.4, and $\mathbf{G}(\mathcal{H}(G)) \subseteq G$ by construction, we have that $G$ contains a copy of $f(G)$ as a subgraph for each $G \in \mathcal{R}_n$. Moreover, by Lemma 4.3.4($c$), we have $\lambda(f(G)) \leq -\varepsilon$ or $T \geq \log n$. In the first case, $f(G)$ belongs to the set of graphs

$$\mathcal{J}_1(\varepsilon) = \{H : \lambda(H) \leq -\varepsilon\}.$$

In the second case, we claim that $f(G) \in \mathcal{J}_2(C, n)$, where $C = \lambda(K_r)$. To see that, first note that the sequence $\big(v(\mathcal{H}_i(G))\big)_{i=0}^T$ is strictly increasing by Lemma 4.3.4($b$). For simplicity, let

$G_i = \mathbf{G}(\mathcal{H}_i(G))$. Since $e(G_i) = v(\mathcal{H}_i(G))$ for every $i \in \{0, \dots, T\}$, we have

$$e(f(G)) = v(\mathcal{H}_T(G)) \geq T \geq \log n. \tag{4.6}$$

Moreover, by Lemma 4.3.5, we have $\lambda(G_i) \leq \lambda(G_{i-1})$ for each $i \in \{0, \dots, T\}$, where $G_0 \cong K_r$ by Lemma 4.3.4 $(a)$. In particular,

$$\lambda(f(G)) = \lambda(G_T) \leq \lambda(G_0) = \lambda(K_r). \tag{4.7}$$

Together, (4.6) and (4.7) imply that $f(G) \in \mathcal{J}_2(C, n)$, where $C = \lambda(K_r)$. This proves our claim.

Now, it only remains to show that $|f(\mathcal{R}_n)| \leq (\log n)^{C_0}$, for some constant $C_0 > 0$. But, this follows directly from Lemma 4.3.6. We finish the proof by setting $M = \max\{C_0, C\}$. □

## 4.4 The structural lemmas

In this section, we obtain some key structural information about Ramsey hypergraphs and prove Lemmas 4.3.2 and 4.3.3.

Given two families of sets $\mathcal{E}_1$ and $\mathcal{E}_2$ on a vertex set and a hypergraph $\mathcal{H}$, define

$$\mathcal{E}_1(\mathcal{H}) = \mathcal{E}_1 \cap E(\mathcal{H}) \qquad \text{and} \qquad \mathcal{E}_2(\mathcal{H}) = \mathcal{E}_2 \cap E(\mathcal{H}).$$

We refer to the hyperedges of $\mathcal{E}_1(\mathcal{H})$ and $\mathcal{E}_2(\mathcal{H})$ as, respectively, hyperedges of type 1 and 2. We say that $\mathcal{H}$ is Ramsey for $(\mathcal{E}_1, \mathcal{E}_2)$, and we write $\mathcal{H} \to (\mathcal{E}_1, \mathcal{E}_2)$, if the following holds. For every 2-colouring $c : V(\mathcal{H}) \to \{1, 2\}$, there exists a hyperedge $E \in \mathcal{E}_i(\mathcal{H})$ such that $c(E) = \{i\}$, for some $i \in \{1, 2\}$. Conversely, we write $\mathcal{H} \not\to (\mathcal{E}_1, \mathcal{E}_2)$ if $\mathcal{H} \to (\mathcal{E}_1, \mathcal{E}_2)$ is not satisfied. Clearly, if $\mathcal{H} \subseteq \mathcal{F}$ and $\mathcal{H} \to (\mathcal{E}_1, \mathcal{E}_2)$, then $\mathcal{F} \to (\mathcal{E}_1, \mathcal{E}_2)$. Therefore, we may concentrate on the minimal hypergraphs $\mathcal{H}$ that satisfy $\mathcal{H} \to (\mathcal{E}_1, \mathcal{E}_2)$.

We call a hypergraph $\mathcal{H}$ *Ramsey minimal* with respect to $(\mathcal{E}_1, \mathcal{E}_2)$ if $\mathcal{H} \to (\mathcal{E}_1, \mathcal{E}_2)$, yet the removal of any hypervertex or hyperedge from $\mathcal{H}$ destroys this property. Minimal Ramsey hypergraphs have the $\star$-critical property, as the next lemma shows. Its proof follows the same steps as the proof of [71, Claim 1]. A particular case of it can be also found in [67, Section 3].

**Lemma 4.4.1.** *Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be two disjoint families of sets on a vertex set. If a hypergraph $\mathcal{H}$ is Ramsey minimal with respect to $(\mathcal{E}_1, \mathcal{E}_2)$, then the following holds. For each $i \in \{1, 2\}$, each hyperedge $E \in \mathcal{E}_i$, and each hypervertex $e \in E$, there exists a hyperedge $F \in \mathcal{E}_{3-i}$ such that $E \cap F = \{e\}$. In particular, $\mathcal{H}$ is $\star$-critical.*

*Proof.* Fix any hyperedge $E \in \mathcal{E}_i(\mathcal{H})$, for some $i \in \{1, 2\}$, and any hypervertex $e \in E$. Let $\mathcal{H} \setminus E$ be the hypergraph with vertex set $V(\mathcal{H})$ and hyperedge set $E(\mathcal{H}) \setminus \{E\}$. Consider any colouring $c : V(\mathcal{H}) \to \{1, 2\}$ for which there is no hyperedge of type $j$ in $\mathcal{H} \setminus E$ coloured $j$ under $c$, for all $j \in \{1, 2\}$. This colouring exists because $\mathcal{H}$ is Ramsey minimal. As $\mathcal{H} \to (\mathcal{E}_1, \mathcal{E}_2)$, all the hypervertices in $E$ must be coloured $i$ under $c$. Moreover, $E$ is the only monochromatic hyperedge under $c$ which has type $j$ and colour $j$, for $j = 1, 2$. Now, let $c' : V(\mathcal{H}) \to \{1, 2\}$ be the colouring such that $c'(f) = c(f) \iff f \neq e$ (recall that $e \in E$). As $\mathcal{H} \to (\mathcal{E}_1, \mathcal{E}_2)$ and $E$ is not monochromatic of colour $i$ under $c'$, there must exist a hyperedge $F \in \mathcal{E}_{3-i}(\mathcal{H})$ such that $c'_E(F) = 3 - i$ and $E \cap F = \{e\}$, as required. □

Now we are ready to prove Lemma 4.3.2.

*Proof.* [Proof of Lemma 4.3.2] If $G \to (K_r, C_\ell)$, then $\mathcal{G}_{r,\ell}(G) \to (\mathcal{E}_1, \mathcal{E}_2)$, where $\mathcal{E}_1$ and $\mathcal{E}_2$ are defined in (4.5). Let $\mathcal{H}$ be an arbitrary Ramsey minimal subhypergraph of $\mathcal{G}_{r,\ell}(G)$. Then $\mathcal{H}$ is $\star$-critical, by Lemma 4.4.1, and therefore $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(G)$, as required. □

We now turn to the proof of Lemma 4.3.3. In order to prove it, we require some structural information about underlying graphs of $\star$-critical hypergraphs. This structural information is obtained in Lemma 4.4.2 and, before stating it, it is worth to point out the following observation.

**Observation 4.4.1.** *Let $r, \ell \geq 3$. For any graph $H$ and any hypergraph $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(H)$, we have $d(v) \geq r$ for all $v \in V(\boldsymbol{G}(\mathcal{H}))$.*

In fact, if $\mathcal{H}$ is $\star$-critical, then for any $e \in E(\mathbf{G}(\mathcal{H}))$ there exists $K \in \mathcal{E}_1(\mathcal{H})$ and $C \in \mathcal{E}_2(\mathcal{H})$ such that $K \cap C = \{e\}$. As $K$ and $C$ are copies of $K_r$ and $C_\ell$ contained in $\mathbf{G}(\mathcal{H})$, respectively, we can easily infer that $d(v) \geq r$ for all $v \in V(\mathbf{G}(\mathcal{H}))$.

Now, we need to set some notation. For each graph $G$, define

$$A = A(G) = \{v \in V(G) : d(v) = r\} \qquad \text{and} \qquad B = B(G) = \{v \in V(G) : d(v) > r\}. \tag{4.8}$$

By Observation 4.4.1, $V(G)$ can be partitioned into $V(G) = A \cup B$ whenever $G$ is the underlying graph of a $\star$-critical hypergraph. Below, we use $N(v)$ to denote the neighbourhood of a vertex $v$ in $G$ and, for each $S \subseteq V(G)$, we write $d_S(v) = |N(v) \cap S|$. Our structural lemma is as follows.

**Lemma 4.4.2.** *Let $r \geq 3$ and $\ell \geq 4$ be integers, and $H$ be a graph. For any hypergraph $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(H)$, we have that*

(1) *$A$ is an independent set in $\boldsymbol{G}(\mathcal{H})$ and*

(2) *$d_B(v) \geq r - 2$, for all $v \in V(\boldsymbol{G}(\mathcal{H}))$.*

*Proof.* [Proof] First, let us prove item (1). Suppose for a contradiction that there are two adjacent vertices $u, v \in V(\mathbf{G}(\mathcal{H}))$ such that $d(u) = d(v) = r$. As $\mathcal{H}$ is $\star$-critical, there exists an $r$-clique $R_1 \in \mathcal{E}_1(\mathcal{H})$ and an $\ell$-cycle $C_1 \in \mathcal{E}_2(\mathcal{H})$ such that $E(R_1) \cap E(C_1) = \{uv\}$. Now,

let $u_c$ be the neighbour of $u$ in $C_1 \setminus \{v\}$ and $v_c$ be the neighbour of $v$ in $C_1 \setminus \{u, v\}$. First, we observe that $u_c \notin N(v)$ and $v_c \notin N(u)$. Indeed, note that $N(v) = (V(R_1) \setminus \{v\}) \cup \{v_c\}$ and $\ell \geq 4$ implies that $u_c \neq v_c$, hence $u_c \notin N(v)$. Similarly, we have $v_c \notin N(u)$. This will be used in the rest of the proof below.

Now, fix any vertex $w \in V(R_1) \setminus \{u, v\}$. We have the following claim.

**Claim 4.4.3.** *There exists an $\ell$-cycle $C_2 \in \mathcal{E}_2(\mathcal{H})$ such that either $\{u_c u, uw\} \subseteq E(C_2)$ or $\{vu, uw\} \subseteq E(C_2)$.*

*Proof.* [Proof of the Claim] As $\mathcal{H}$ is $\star$-critical, there exists an $r$-clique $R_2$ and an $\ell$-cycle $C_2$ such that $E(R_2) \cap E(C_2) = \{uw\}$. If $R_2 = R_1$, then $C_2$ must contain $u_c$, as $d(u) = r$. This settles the first part of the claim. If $R_2 \neq R_1$, then $R_2$ must contain $u_c$, again because $d(u) = r$. As $u_c \in V(R_2)$, we cannot have $v \in R_2$. Otherwise, we would have $u_c \in N(v)$, which is a contradiction. Together, these imply that $V(R_2) = \{u_c\} \cup V(R_1) \setminus \{v\}$. As $v$ is the only vertex in $V(R_1)$ not contained in $R_2$, it follows that $v \in C_2$. This settles the second part. □

Let $C_2$ be the cycle given by the claim above. If $\{u_c u, uw\} \subseteq E(C_2)$, then there exists an $r$-clique $R_2 \in \mathcal{E}_1(\mathcal{H})$ such that $E(R_2) \cap E(C_2) = \{u_c u\}$. As $V(R_2) \subseteq N(u) \cup \{u\} \setminus \{w\}$, $R_2$ has no choice but to contain $v$. In particular, this implies that $v$ is a neighbour of $u_c$, which gives us a contradiction. If $\{vu, uw\} \subseteq E(C_2)$, then there exists an $r$-clique $R_2 \in \mathcal{E}_1(\mathcal{H})$ such that $E(R_2) \cap E(C_2) = \{uv\}$. As $V(R_2) \subseteq N(u) \cup \{u\} \setminus \{w\}$, $R_2$ has no choice but to contain $u_c$. In particular, this implies again that $v$ is a neighbour of $u_c$, which gives us a contradiction. This proves item (1).

To show item (2), we consider two cases: (i) either $d_B(v) = d(v)$, or (ii) $d(v) > d_B(v)$. In the first case, Observation 4.4.1 gives us $d_B(v) = d(v) \geq r$. In the second case, there is a vertex $u \in N(v) \cap A$ and, since $\mathcal{H}$ is $\star$-critical, there is also an $r$-clique $R$ in $\mathbf{G}(\mathcal{H})$ such that

$uv \in E(R)$. As $A$ is an independent set, we must have $V(R) \setminus \{u\} \subseteq B$, which implies that $v$ has least $r-2$ neighbours in $B$. $\square$

Let $m(G) = e(G)/v(G)$ be the edge density of $G$. Now, we are ready to prove Lemma 4.3.3.

*Proof.* [Proof of Lemma 4.3.3] To simplify the notation, set $G = \mathbf{G}(\mathcal{H})$. We show that there exists $\delta > 0$ such that $m(G) > m_2(K_r, C_\ell) + \delta$. Note that this implies that $m(G) - m_2(K_r, C_\ell) \geq \varepsilon m_2(K_r, C_\ell) v(G)^{-1}$ for $\varepsilon = \delta / m_2(K_r, C_\ell)$, as $|v(G)| \geq 1$. This can be seen to be equivalent to $\lambda(G) \leq -\varepsilon$, by definition of $\lambda$.

In order to find $\delta$, we shall first bound $e(G)$ from below. By Observation 4.4.1, the set $V(G)$ can be partitioned into $V(G) = A \cup B$, where $A = A(G)$ and $B = B(G)$ were defined in (4.8). Thus, we can write

$$2e(G) = \sum_{v \in A} d(v) + \sum_{v \in B} d(v).$$

As $d(v) = r$ for all $v \in A$, we have $\sum_{v \in A} d(v) = r|A|$. Now, to bound the sum $S = \sum_{v \in B} d(v)$, observe that this sum counts twice each edge inside the set $B$ and counts once each edge across $A$ and $B$. By Lemma 4.4.2(1), we have $e(A, B) = r|A|$, as $A$ is an independent set and $d(v) = r$ for each $v \in A$. By Lemma 4.4.2(2), $d_B(v) \geq r - 2$ for each $v \in B$. Together, these imply that

$$S \geq r|A| + (r-2)|B|.$$

Furthermore,

$$S \geq (r+1)|B|,$$

as $d(v) \geq r + 1$ for each $v \in B$. Therefore,

$$2e(G) \geq r|A| + \max\Big\{r|A| + (r-2)|B|, (r+1)|B|\Big\}.$$

As $v(G) = |A| + |B|$, we have

$$\begin{aligned} 2m(G) &\geq \max\left\{\frac{2r|A| + (r-2)|B|}{|A| + |B|}, \frac{r|A| + (r+1)|B|}{|A| + |B|}\right\} \\ &= r - 2 + \max\big\{(r+2)x, 3 - x\big\}, \end{aligned}$$

where $x = |A|/v(G)$. The last expression attains its minimum value when $x = 3/(r+3)$, and hence

$$m(G) \geq \frac{r+1}{2} - \frac{3}{2(r+3)}.$$

A straightforward calculation shows that $m_2(K_r, C_\ell) = \frac{\binom{r}{2}(\ell-1)}{(r-1)(\ell-1)-1}$ (see Fact 4.6.2). From this expression, we can see that $\ell \mapsto m_2(K_r, C_\ell)$ is decreasing. Thus, in order to conclude our proof, it suffices to show that

$$\frac{r+1}{2} - \frac{3}{2(r+3)} > m_2(K_r, C_4).$$

Using again the expression we have for $m_2(K_r, C_\ell)$, an easy calculation shows that the last inequality holds for every $r \geq 4$. This completes the proof of the lemma. □

## 4.5 The Algorithms

In this section, we formally describe the algorithm Hypertree and its subroutine Flower, and prove Lemma 4.3.4. Let $n, r, \ell \geq 4$ be fixed integers throughout this section.

First, let us recall some notation from Section 4.3. Given any graph $G$, $\mathrm{Crit}_{r,\ell}(G)$ denotes the set of all $\star$-critical subhypergraphs of $\mathcal{G}_{r,\ell}(G)$, the hypergraph whose hyperedges correspond to the copies of $K_r$ and $C_\ell$ in $G$. We distinguish the hyperedges of $\mathcal{G}_{r,\ell}(G)$ by two types:

$$\mathcal{E}_1(\mathcal{G}_{r,\ell}(G)) = \{E(F) : F \cong K_r, F \subseteq G\} \text{ and } \mathcal{E}_2(\mathcal{G}_{r,\ell}(G)) = \{E(F) : F \cong C_\ell, F \subseteq G\}.$$

For any $\mathcal{H} \subseteq \mathcal{G}_{r,\ell}(G)$, we denote $\mathcal{E}_1(\mathcal{H}) = E(\mathcal{H}) \cap \mathcal{E}_1(\mathcal{G}_{r,\ell}(G))$ and $\mathcal{E}_2(\mathcal{H}) = E(\mathcal{H}) \cap \mathcal{E}_2(\mathcal{G}_{r,\ell}(G))$. The underlying graph of $\mathcal{H}$ is denoted by $\mathbf{G}(\mathcal{H})$.

We find it instructive to first provide an informal overview of Hypertree. This algorithm takes a hypergraph $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(G)$ as input, for some graph $G$ on $n$ vertices, builds a sequence $(\mathcal{H}_i)_{i=0}^{T}$ of subhypergraphs of $\mathcal{H}$ and outputs $\mathcal{H}_T$. The algorithm seeks to find a subhypergraph $\mathcal{F} \subseteq \mathcal{H}$ for which the following holds. The graph $F = \mathbf{G}(\mathcal{F})$, which is a subgraph of $G$, satisfies (1) $\lambda(F) \leq -\varepsilon$ or (2) $\lambda(F) \leq M$ and $e(F) \geq \log n$, for some positive constants $\varepsilon = \varepsilon(r,\ell)$ and $M = M(r,\ell)$.

In the initialisation step, the algorithm picks a hyperedge $E_0 \in \mathcal{E}_1(\mathcal{H})$ and sets $\mathcal{H}_0 = \{E_0\}$. Then, the algorithm enters a while loop. In iteration $i$ of the loop, the algorithm attaches a hyperedge $E_i \in \mathcal{E}_1(\mathcal{H})$ to the current hypergraph $\mathcal{H}_{i-1}$ to build $\mathcal{H}_i$. It is required that such a copy intersects $\mathbf{G}(\mathcal{H}_{i-1})$ in at least two vertices, but is not a subgraph of $\mathbf{G}(\mathcal{H}_{i-1})$. If no such hyperedge exists, then the algorithm runs a subroutine which we call Flower. This algorithm, when called within Hypertree, returns (1) a hyperedge $C \in \mathcal{E}_2(\mathcal{H})$ which intersects $\mathcal{H}_{i-1}$ in at least one hypervertex and it is not contained in $\mathcal{H}_{i-1}$; and (2) a collection of hyperedges in $\mathcal{E}_1(\mathcal{H})$, each intersecting $C$ in exactly one hypervertex. The output of Flower is attached to $\mathcal{H}_{i-1}$ to build $\mathcal{H}_i$. We defer the exact description of Flower until after the description of Hypertree.

A hyperedge $E$ always corresponds to a set of edges of some underlying graph, and so we denote by $V(E)$ the set of vertices of $V(G)$ belonging to some edge in $E$, i.e., $V(E) = \{v \in V(G) : \exists e \in E, v \in e\}$. For a hypergraph $\mathcal{H}$, $V(\mathcal{H})$ denotes the set $\cup_{E \in E(\mathcal{H})}\{e : e \in E\}$, and hence we have $V(\mathcal{H}) = E(\mathbf{G}(\mathcal{H}))$. We switch between these two equivalent perspectives throughout the algorithm and its analysis, whichever is more convenient at that point. Next is the formal description of the Hypertree algorithm. Recall that $\varepsilon = \varepsilon(r,\ell)$ is the small positive constant given by Lemma 4.3.3.

**Algorithm 1:** HYPERTREE

**Input:** A hypergraph $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(G)$, for some graph $G$ with $V(G) = [n]$

**Output:** A pair $(\mathcal{H}_T, D_T)$, where $\mathcal{H}_T \subseteq \mathcal{H}$ and $D_T \subseteq \mathbb{N}$

`/* Initialise: */`

$i = 0$, $D_0 = \emptyset$, $\mathcal{H}_0 = \{E_0\}$ for some $E_0 \in \mathcal{E}_1(\mathcal{H})$

**while** $\lambda(\boldsymbol{G}(\mathcal{H}_i)) > -\varepsilon$ *and* $i < \log n$ **do**

  **if** *there exists* $E \in \mathcal{E}_1(\mathcal{H})$ *such that* $|V(E) \cap V(\boldsymbol{G}(\mathcal{H}_i))| \geq 2$ *and* $E \not\subseteq V(\mathcal{H}_i)$ **then**

    set $\mathcal{H}_{i+1} = \mathcal{H}_i \cup \{E\}$ and $D_{i+1} = D_i \cup \{i+1\}$

  **end**

  **else**

    let $\mathcal{H}_F$ be the output of FLOWER$(\mathcal{H}_i, \mathcal{H})$

    set $\mathcal{H}_{i+1} = \mathcal{H}_i \cup \mathcal{H}_F$

    **if** $|V(\boldsymbol{G}(\mathcal{H}_{i+1})) \setminus V(\boldsymbol{G}(\mathcal{H}_i))| = (r-1)(\ell-1) - 1$ **then** set $D_{i+1} = D_i$

    **else** set $D_{i+1} = D_i \cup \{i+1\}$

  **end**

  $i \mapsto i + 1$

**end**

**return** $(\mathcal{H}_i, D_i)$

The auxiliary set $D_T$ in the output of HYPERTREE will help us to count all the possible outputs given by this algorithm. This set will also help us to ensure that $\mathbf{G}(\mathcal{H}_T)$ belongs to $\mathcal{J}_1 \cup \mathcal{J}_2$ (recall the definition of these sets in (4.1)). From now on, we say that the $i$-th step of HYPERTREE$(\mathcal{H})$ is *degenerate* if $i \in D_T$, and *non-degenerate* otherwise.

Let us now turn to the subroutine FLOWER. The input of FLOWER is a tuple $(\mathcal{H}_i, \mathcal{H})$, where $\mathcal{H}$ is a $\star$-critical subhypergraph of $\mathcal{G}_{r,\ell}(G)$, for some graph $G$, and $\mathcal{H}_i \subseteq \mathcal{H}$. When called

within HYPERTREE, the output is a subhypergraph of $\mathcal{H}$ called a flower. For a hyperedge $C$ of type 2 and hyperedges $P_1, \dots, P_t$ of type 1, we call the hypergraph $\mathcal{H}_F = \{C, P_1, \dots, P_t\}$ a *flower* if $|C \cap P_s| = 1$ and $C \cap P_s \cap P_q = \emptyset$ for all $1 \leq s < q \leq t$. The hyperedges $P_1, \dots, P_t$ are called *petals*. Observe that $\mathbf{G}(\mathcal{H}_F)$ corresponds to a copy of $C_\ell$ and $t$ copies of $K_r$ that intersect $C$ in exactly one edge (and possibly more vertices). Moreover, if we denote the edges in $C$ by $e_0, \dots, e_{\ell-1}$, then the condition $|V(\mathbf{G}(\mathcal{H}_{i+1})) \setminus V(\mathbf{G}(\mathcal{H}_i))| = (r-1)(\ell-1)-1$ in line 7 of HYPERTREE is equivalent to having $t = \ell - 1$ and having (up to a relabelling) $V(C) \cap V(\mathbf{G}(\mathcal{H}_i)) = e_0$, $V(P_s) \cap V(C) = e_s$ and $V(P_s) \cap (V(\mathbf{G}(\mathcal{H}_{i+1})) \setminus V(C)) = \emptyset$ for $1 \leq s < \ell$.

In Section 4.6, we prove that the if condition in line 7 of HYPERTREE is satisfied for all but a constant number of iterations of the while loop. That is, the size of $D_T$ is bounded by a constant. This will be one main ingredient to show that the set of all possible outputs given by HYPERTREE, up to isomorphism, is at most polylogarithmic in $n$ when applied over $\bigcup_{V(G)=[n]} \mathrm{Crit}_{r,\ell}(G)$.

The second main ingredient towards this goal is to make sure that in a non-degenerate step $i$, there is only one way, up to isomorphism, to attach the underlying graph of a flower $\mathcal{H}_F$ to the current graph $\mathbf{G}(\mathcal{H}_i)$, independent of the input hypergraph $\mathcal{H}$. To make this precise, we now introduce some non-standard notation. For each $i \in \mathbb{N}$ and each graph $H$ with $V(H) \subseteq [n]$, let $\mathscr{C}(i, H)$ be the set of all hypergraphs $\mathcal{F}$ with the following properties: (1) $\mathcal{F} \in \mathrm{Crit}_{r,\ell}(G)$ for some graph $G$ with $V(G) = [n]$; (2) $H \cong \mathbf{G}(\mathcal{F}_i)$, where $\mathcal{F}_i$ is the subhypergraph of $\mathcal{F}$ generated after $i$ iterations of the while loop of HYPERTREE($\mathcal{F}$); and (3) HYPERTREE($\mathcal{F}$) enters FLOWER in iteration $i+1$ of the while loop. Let $\sigma_{\mathcal{F}_i} : V(H) \to V(\mathbf{G}(\mathcal{F}_i))$ be a graph isomorphism and, by abuse of notation, denote by $\sigma_{\mathcal{F}_i}(E)$ the set of

edges in $\mathbf{G}(\mathcal{F}_i)$ corresponding to the edges in $E$ under the isomorphism $\sigma_{\mathcal{F}_i}$. Now, define

$$\overline{\mathcal{H}}_{H,i} = \bigcup_{\mathcal{F}\in\mathscr{C}(i,H)} \big\{E \subseteq E(H) : \sigma_{\mathcal{F}_i}(E) \in \mathcal{F}_i\big\}.$$

Observe that if $\mathscr{C}(i,H) \neq \emptyset$, then $H = \mathbf{G}(\overline{\mathcal{H}}_{H,i})$. Finally, we call an edge $e$ of a graph $H$ *suitable (with respect to $H$)* if $e \notin C$ for all $C \in \mathcal{E}_2(\overline{\mathcal{H}}_{H,i})$. Let $S = S(H)$ be the set of suitable edges of $H$. Our next lemma says that if $\mathscr{C}(i,H) \neq \emptyset$, then $S(H) \neq \emptyset$.

**Lemma 4.5.1.** *Let $G$ be a graph on vertex set $[n]$ and let $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(G)$. Suppose that the algorithm* Flower$(\mathcal{H}_i, \mathcal{H})$ *is called in iteration $i+1$ of the while loop of* Hypertree$(\mathcal{H})$. *Then $S(\boldsymbol{G}(\mathcal{H}_i))$ is non-empty.*

We prove the lemma after the description of Flower. Lemma 4.5.1 allows us to make the following definition.

**Definition 4.5.2** (Canonical edge)**.** *For every graph $H$ with $V(H) \subseteq [n]$ and $S(H) \neq \emptyset$, fix an edge $e_0 = e_0(H) \in S(H)$ such that if $H$ and $H'$ are isomorphic then there is a graph isomorphism $\varphi : V(H) \to V(H')$ that maps $e_0(H)$ to $e_0(H')$. Call $e_0(H)$ the* canonical edge of $H$.

We remark that the canonical edge is undefined when $S(H)$ is empty. However, we only need the canonical edge of $H$ when $H \cong \mathbf{G}(\mathcal{H}_i)$ and Flower is called on input $(\mathcal{H}_i, \mathcal{H})$ in Hypertree. In this case, Lemma 4.5.1 guarantees the existence of the canonical edge. We stress that, in the light of bounding the size of $\mathrm{Out}_{r,\ell}(n)/_{\cong}$, it is important that 'the same' edge is fixed for any two isomorphic graphs.

Now we are ready to state the formal description of Flower.

**Algorithm 2:** FLOWER

**Input:** A tuple $(\mathcal{H}_i, \mathcal{H})$, where $\mathcal{H}$ is a hypergraph in $\mathrm{Crit}_{r,\ell}(G)$, for some graph $G$, and $\mathcal{H}_i \subseteq \mathcal{H}$

**Output:** A flower $\mathcal{H}_F = \{C\} \cup \{P_e : e \in C \setminus V(\mathcal{H}_i)\}$, where $C \in \mathcal{E}_2(\mathcal{H})$, $P_e \in \mathcal{E}_1(\mathcal{H})$ for all $e \in C \setminus V(\mathcal{H}_i)$

`/* Find a seed: */`

1 Let $e_0 \in S(\mathbf{G}(\mathcal{H}_i))$ be the canonical edge of $\mathbf{G}(\mathcal{H}_i)$

2 Let $C \in \mathcal{E}_2(\mathcal{H})$ be a hyperedge containing $e_0$ such that $C \not\subseteq V(\mathcal{H}_i)$

**for** *every* $e \in C \setminus V(\mathcal{H}_i)$ **do**

3 | let $P_e \in \mathcal{E}_1(\mathcal{H})$ be such that $C \cap P_e = \{e\}$

**end**

**return** $\{C\} \cup \{P_e : e \in C \setminus V(\mathcal{H}_i)\}$

We remark here that the condition $C \not\subseteq V(\mathcal{H}_i)$ in line 2 is not an additional restriction. That is, if $e_0 \in S(\mathbf{G}(\mathcal{H}_i))$, then $C \not\subseteq V(\mathcal{H}_i)$ for all $C \in \mathcal{E}_2(\mathcal{H})$ containing $e_0$. Indeed, if we had $C \subseteq V(\mathcal{H}_i)$ for some $C \in \mathcal{E}_2(\mathcal{H})$ containing $e_0$, then this would imply that $C \in \mathcal{E}_2(\overline{\mathcal{H}}_{G_i,i})$, where $G_i = \mathbf{G}(\mathcal{H}_i)$ for simplicity. Thus, $e_0$ would not be suitable, a contradiction.

*Proof.* [Proof of Lemma 4.5.1] Let $G_i := \mathbf{G}(\mathcal{H}_i)$ and let $\overline{\mathcal{H}}_i := \overline{\mathcal{H}}_{G_i,i}$. Recall that we have $G_i = \mathbf{G}(\overline{\mathcal{H}}_i)$ as remarked after the definition of $\overline{\mathcal{H}}_i$. We first claim that $\overline{\mathcal{H}}_i$ cannot be $\star$-critical. Otherwise, $\lambda(G_i) \leq -\varepsilon$, by Lemma 4.3.3, and this would imply that HYPERTREE$(\mathcal{H})$ has not entered the while loop in iteration $i+1$. In particular, FLOWER would not be called in iteration $i+1$ of HYPERTREE$(\mathcal{H})$.

Now, we show that for every $C \in \mathcal{E}_2(\overline{\mathcal{H}}_i)$ and every $e \in C$, there exists $K \in \mathcal{E}_1(\overline{\mathcal{H}}_i)$ such that $K \cap C = \{e\}$. Indeed, let $C \in \mathcal{E}_2(\overline{\mathcal{H}}_i)$, and let $\mathcal{F} \in \mathscr{C}(i, G_i)$ be such that $\sigma_{\mathcal{F}_i}(C) \in \mathcal{E}_2(\mathcal{F})$, where $\mathcal{F}_i$ is the subhypergraph of $\mathcal{F}$ generated after $i$ iterations of the while loop of HYPERTREE$(\mathcal{F})$ and where $\sigma_{\mathcal{F}_i} : V(H) \to V(\mathbf{G}(\mathcal{F}_i))$ is a graph isomorphism.

Note that such $\mathcal{F}$ must exist by definition of $\overline{\mathcal{H}_i}$. Let $e \in C$ be arbitrary and let $e'$ be the corresponding copy of $e$ in $\mathbf{G}(\mathcal{F}_i)$. Since $\mathcal{F}$ is $\star$-critical, there must exist $K' \in \mathcal{E}_1(\mathcal{F})$ such that $K' \cap \sigma_{\mathcal{F}_i}(C) = \{e'\}$. However, as HYPERTREE($\mathcal{F}$) has entered the else-statement in iteration $i+1$ (c.f. the definition of $\mathscr{C}(i, G_i)$), the condition of the if statement in line 3 is false. This implies that $K' \subseteq V(\mathcal{F}_i)$, and hence the preimage $K$ of $K'$ under $\sigma_{\mathcal{F}_i}$ is contained in $\mathcal{E}_1(\overline{\mathcal{H}_i})$. In particular, we have $K \cap C = \{e\}$.

It follows that the only reason for which $\overline{\mathcal{H}_i}$ is not $\star$-critical is because there exists an edge $e \in V(\overline{\mathcal{H}_i}) = E(G_i)$ for which there is no hyperedge in $\mathcal{E}_2(\overline{\mathcal{H}_i})$ containing $e$. Or, equivalently, $S(G_i) \neq \emptyset$. $\square$

The following is now immediate.

**Corollary 4.5.3.** *Under the same assumptions as in Lemma* 4.5.1*, the algorithm* FLOWER($\mathcal{H}_i, \mathcal{H}$) *runs without errors and finishes in finite time. Moreover, the edge $e_0$ in line 1 is uniquely determined by the isomorphism class of $\boldsymbol{G}(\mathcal{H}_i)$.*

*Proof.* The existence of the edge $e_0$ in line 1 follows immediately from $S(\mathbf{G}(\mathcal{H}_i)) \neq \emptyset$ proved in the previous lemma. Its uniqueness follows by fixing the canonical edge for every isomorphism type globally. As $\mathcal{H}$ is $\star$-critical, the existence of the cycle $C$ as in line 2 and the petals $P_e$ as in line 3 is straightforward. $\square$

We next pin down important properties of the flower returned by FLOWER($\mathcal{H}_i, \mathcal{H}$) that we need repeatedly in the analysis of the algorithm.

**Lemma 4.5.4.** *Under the same assumptions as in Lemma* 4.5.1*,* FLOWER($\mathcal{H}_i, \mathcal{H}$) *outputs a flower $\mathcal{H}_F = \{C\} \cup \{P_e : e \in C \setminus V(\mathcal{H}_i)\}$ which satisfies the following properties:*

*(F1)* $C \in \mathcal{E}_2(\mathcal{H})$ *but* $C \not\subseteq V(\mathcal{H}_i)$,

*(F2)* $P_e \in \mathcal{E}_1(\mathcal{H})$ *and* $C \cap P_e = \{e\}$ *for every* $e \in C \setminus V(\mathcal{H}_i)$, *and*

*(F3)* $|V(P_e) \cap V(\boldsymbol{G}(\mathcal{H}_i))| \leq 1 \leq |C \cap E(\boldsymbol{G}(\mathcal{H}_i))|$ *for all* $e \in C \setminus V(\mathcal{H}_i)$.

*Proof.* The properties *(F1)* and *(F2)* are immediate from the algorithm description and Corollary 4.5.3. As FLOWER was called in iteration $i+1$ of the while loop of HYPERTREE($\mathcal{H}$), line 3 of HYPERTREE was not executed. This means that for each petal $P_e$ we have $|V(P_e) \cap V(\mathbf{G}(\mathcal{H}_i))| \leq 1$, which proves the first inequality in *(F3)*. The second inequality follows from the existence of $e_0$ in line 1, as $e_0 \in C \cap E(\mathbf{G}(\mathcal{H}_i))$. □

With Corollary 4.5.3 and Lemma 4.5.4 at our hands, we now deduce Lemma 4.3.4.

*Proof.* [Proof of Lemma 4.3.4] In its initialisation, the algorithm HYPERTREE($\mathcal{H}$) sets $D_0 = \emptyset$ and $\mathcal{H}_0 = \{E_0\}$, for some $E_0 \in \mathcal{E}_1(\mathcal{H})$. This already establishes Part $(a)$. Now, for each iteration $i+1$ of the while loop, where $i = 0, 1, \ldots,$ HYPERTREE($\mathcal{H}$) executes one of the following actions. Either it sets $\mathcal{H}_{i+1} = \mathcal{H}_i \cup \{E\}$ for some $E \in \mathcal{E}_1(\mathcal{H})$ (Case 1, cf. line 4), or it sets $\mathcal{H}_{i+1} = \mathcal{H}_i \cup \mathcal{H}_F$, where $\mathcal{H}_F$ is the output of the algorithm FLOWER($\mathcal{H}_i, \mathcal{H}$) (Case 2, cf. line 6). We remark that one of them must be executed because $\mathcal{H}_i \notin \mathrm{Crit}_{r,\ell}(G)$, as $\lambda(\mathbf{G}(\mathcal{H}_i)) > -\varepsilon$ (see Lemma 4.3.3). In either case, $\mathcal{H}_i \subseteq \mathcal{H}_{i+1} \subseteq \mathcal{H}$ (cf. Lemma 4.5.4 for the second case). Similarly, it is easy to see from lines 4, 7 and 8 that $D_i \subseteq D_{i+1} \subseteq \mathbb{N}$.

Let $T$ be the number of iterations of the while loop in line 2 of HYPERTREE($\mathcal{H}$). By the while loop condition and the increase of $i$ by one in every iteration (see line 9), HYPERTREE($\mathcal{H}$) must stop in at most $\log n$ iterations. Moreover, the while loop guarantees that $T$ is the smallest integer such that $\lambda(G_T) \leq -\varepsilon$ or $T \geq \log n$, where $G_T = \mathbf{G}(\mathcal{H}_T)$ and $\varepsilon$ is the constant given by Lemma 4.3.3. This establishes Part $(c)$. Since HYPERTREE($\mathcal{H}$) should return $(\mathcal{H}_T, D_T)$ (see line 10), we also establish Part $(d)$.

Now, it remains to show Part $(b)$. Let $i = 0, 1, \ldots,$ and assume HYPERTREE($\mathcal{H}$) enters the while loop in iteration $i+1$. In Case 1, the hyperedge $E$ satisfies $E \not\subseteq V(\mathcal{H}_i)$ (cf. line 3). In

Case 2, Lemma 4.5.4 implies that the output $\mathcal{H}_F = \{C, P_1, \ldots, P_t\}$ given by FLOWER$(\mathcal{H}_i, \mathcal{H})$ satisfies $C \not\subseteq V(\mathcal{H}_i)$. In both cases, $v(\mathcal{H}_i) < v(\mathcal{H}_{i+1})$. $\square$

## 4.6 The algorithm analysis

In this section, we prove Lemmas 4.3.5 and 4.3.6, and hence complete the proof of Theorem 4.2.1. Let $G_i$ denote the graph $\mathbf{G}(\mathcal{H}_i)$, where $\mathcal{H}_i$ is the hypergraph generated in the $i$-th step of HYPERTREE. Lemma 4.3.5 is easily deduced from our next lemma, which states that $\lambda(\mathbf{G}(\mathcal{H}_i))$ either decreases by an additive constant in a degenerate step or it remains the same in a non-degenerate step. This lemma is proved at the end of this section.

**Lemma 4.6.1.** *For all integers $r, \ell \geq 4$, there exists $\delta = \delta(r, \ell) > 0$ such that the following holds. For any graph $G$ and any hypergraph $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(G)$, the sequence $(\mathcal{H}_i, D_i)_{i=0}^{T}$ generated by* HYPERTREE$(\mathcal{H})$ *satisfies*

(1) $\lambda(G_i) = \lambda(G_{i-1})$ *for all* $i \notin D_T$, *and*

(2) $\lambda(G_i) \leq \lambda(G_{i-1}) - \delta$ *for all* $i \in D_T$,

*where $G_i = \boldsymbol{G}(\mathcal{H}_i)$ for each $i \in \{1, \ldots, T\}$.*

For all $1 \leq i \leq T$, the graph $G_i$ is obtained from $G_{i-1}$ by adding either an $r$-clique or the underlying graph of a flower $\{C, P_1, \ldots, P_t\}$ to it, depending whether HYPERTREE executes the if-clause in lines 3–4 or the else-clause in lines 5–8. In the latter case, we will analyse the change in $\lambda$ by adding first $C$, and then one petal (copy of $K_r$) at a time. Thus, it makes sense to pin down the effect of adding a copy of $K_r$ to an arbitrary graph $F$ first.

For two graphs $F_1$ and $F_2$, we denote by $F_1 \cap F_2$ the subgraph with vertex set $V(F_1) \cap V(F_2)$ and edge set $E(F_1) \cap E(F_2)$. The graph $F_1 \cup F_2$ is defined analogously. For any graph $F$,

recall that $\lambda(F) = v(F) - e(F)/m_2(K_r, C_\ell)$. Then, we can write

$$\begin{aligned}\lambda(F_1 \cup F_2) - \lambda(F_1) &= v(F_1 \cup F_2) - v(F_1) - \frac{e(F_1 \cup F_2) - e(F_1)}{m_2(K_r, C_\ell)} \\ &= v(F_2) - v(F_1 \cap F_2) - \frac{e(F_2) - e(F_1 \cap F_2)}{m_2(K_r, C_\ell)}. \end{aligned} \tag{4.9}$$

Now, define

$$\beta_{r,\ell}(J) = r - v(J) - \frac{\binom{r}{2} - e(J)}{m_2(K_r, C_\ell)}. \tag{4.10}$$

By (4.9), we have

$$\lambda(F_1 \cup F_2) - \lambda(F_1) = \beta_{r,\ell}(J) \tag{4.11}$$

in the case when $F_2 \cong K_r$ and $J = F_1 \cap F_2$. Before stating the lemma which encompasses how $\beta_{r,\ell}(J)$ behaves for various subgraphs $J \subseteq K_r$, we pin down the following fact which provides closed formulas for $m_2(C_\ell)$, $m_2(K_r)$ and $m_2(K_r, C_\ell)$. These follow from standard calculations which we provide in the appendix for completeness.

**Fact 4.6.2.** *Let $r, \ell \geq 4$ be integers. Then,*

$$m_2(C_\ell) = \frac{\ell - 1}{\ell - 2}, \quad m_2(K_r) = \frac{r+1}{2}, \quad \textit{and} \quad m_2(K_r, C_\ell) = \frac{\binom{r}{2}}{r - 2 + (\ell - 2)/(\ell - 1)}.$$

*In particular, $r/2 < m_2(K_r, C_\ell) < m_2(K_r)$.*

In our next lemma, we obtain upper bounds for $\beta_{r,\ell}(J)$ for every subgraph $J \subsetneq K_r$ with at least two vertices.

**Lemma 4.6.3.** *Let $r, \ell \geq 4$ be integers. Let $J \subsetneq K_r$ such that $v(J) \geq 2$. Then,*

(*a*) $\beta_{r,\ell}(J) < 0$,

(*b*) $\beta_{r,\ell}(K_2) = 1/m_2(K_r, C_\ell) - (\ell - 2)/(\ell - 1) > -1$,

(c) $\beta_{r,\ell}(J) \leq \beta_{r,\ell}(K_2)$ *if* $d(v) = 1$ *for some* $v \in V(J)$. *The equality holds if and only if* $J \cong K_2$.

*Proof.* First, let us prove part $(a)$. When $J \subsetneq K_r$ has $r$ vertices, we can easily see from (4.10) that $\beta_{r,\ell}(J) < 0$. Thus, let us assume that $2 \leq v(J) < r$. Observe that $\beta_{r,\ell}(J) < 0$ if the following inequalities are satisfied:

$$m_2(K_r, C_\ell) < m_2(K_r) \leq \frac{\binom{r}{2} - e(J)}{r - v(J)}. \tag{4.12}$$

The first inequality follows from Fact 4.6.2. For the second, simply note that

$$\frac{\binom{r}{2} - e(J)}{r - v(J)} \geq \frac{\binom{r}{2} - \binom{v(J)}{2}}{r - v(J)} \geq \frac{r + j - 1}{2} \geq \frac{r+1}{2}.$$

As $m_2(K_r) = (r+1)/2$ (see Fact 4.6.2), this establishes part $(a)$.

To show part $(c)$, first note that $d(v) = 1$ for some $v \in V(J)$ if and only if $K_2 \subseteq J \subseteq K_{r-1} \cdot K_2$, where $K_{r-1} \cdot K_2$ denotes the graph obtained from $K_{r-1}$ by adding a pendant edge. When $J \cong K_2$, the equality in $(c)$ holds trivially. Thus, let us assume that $v(J) \geq 3$ and $J \subseteq K_{r-1} \cdot K_2$. In this case, the inequality $\beta_{r,\ell}(J) < \beta_{r,\ell}(K_2)$ is equivalent to

$$\frac{e(J) - 1}{v(J) - 2} < m_2(K_r, C_\ell). \tag{4.13}$$

But, for any $J \subseteq K_{r-1} \cdot K_2$ such that $v(J) \geq 3$, we have

$$\frac{e(J) - 1}{v(J) - 2} \leq m_2(K_{r-1} \cdot K_2) = \max\left\{ m_2(K_{r-1}), \frac{e(K_{r-1} \cdot K_2) - 1}{v(K_{r-1} \cdot K_2) - 2} \right\} = \frac{r}{2},$$

by definition of $m_2(\cdot)$ and the identity $m_2(K_{r-1}) = r/2$ (see Fact 4.6.2). As $m_2(K_r, C_\ell) > r/2$ by Fact 4.6.2, this finishes the proof of part $(c)$.

For part $(b)$, the identity $\beta_{r,\ell}(K_2) = 1/m_2(K_r, C_\ell) - (\ell-2)/(\ell-1)$ follows readily from the definition of $\beta_{r,\ell}$ in (4.10) and the identity for $m_2(K_r, C_\ell)$ in Fact 4.6.2. Finally, $m_2(K_r, C_\ell) > 0$ and $(\ell-2)/(\ell-1) < 1$ imply that $\beta_{r,\ell}(K_2) > -1$. $\square$

Now we are ready to prove Lemma 4.6.1. As a consequence, we also prove Lemma 4.3.5.

*Proof.* [Proof of Lemma 4.6.1]

Suppose that HYPERTREE($\mathcal{H}$) executes the if-statement in lines 3–4 in the $i$-th iteration of its while loop. Then, $i \in D_i$ and hence $i \in D_T$. Moreover, $G_i = G_{i-1} \cup K$ for some $K \cong K_r$ such that $|V(G_{i-1}) \cap V(K)| \geq 2$ and $K \not\subseteq G_{i-1}$. Observe that the graph $J = G_{i-1} \cap K$ satisfies the assumptions of Lemma 4.6.3 and hence, by (4.11), $\lambda(G_i) - \lambda(G_{i-1}) = \beta_{r,\ell}(J) < 0$.

Now, suppose that HYPERTREE($\mathcal{H}$) executes the else-statement in lines 5–8 in the $i$-th iteration of its while loop. Let $\mathcal{H}_F = \{C\} \cup \{P_e : e \in C \setminus E(G_{i-1})\}$ be the flower returned by FLOWER($\mathcal{H}_{i-1}, \mathcal{H}$). Recall all the properties of $\mathcal{H}_F$ given by Lemma 4.5.4. In order to bound the difference $\lambda(G_i) - \lambda(G_{i-1})$, we first analyse the increment $\lambda(G_{i-1} \cup C) - \lambda(G_{i-1})$. Let $J_0$ be the graph $G_{i-1} \cap C$. By (4.9), we have

$$\begin{aligned}\lambda(G_{i-1} \cup C) - \lambda(G_{i-1}) &= \ell - v(J_0) - \frac{\ell - e(J_0)}{m_2(K_r, C_\ell)} \\ &\leq \left(\frac{\ell - 2}{\ell - 1} - \frac{1}{m_2(K_r, C_\ell)}\right) \cdot |E(C) \setminus E(G_{i-1})|, \end{aligned} \tag{4.14}$$

where in the inequality we use that $v(J_0) \geq e(J_0)+1 \geq 2$, as $K_2 \subseteq J_0 \subsetneq C_\ell$ (see Lemma 4.5.4). Note that equality holds in (4.14) if and only if $J_0 \cong K_2$.

By Lemma 4.6.3($a$), the contribution of each petal of $\mathcal{H}_F$ to $\lambda$ is negative. But, the contribution of $C$ to $\lambda$, which is bounded by (4.14), may be positive (and large). However, as we shall show, the contribution of $C$ to $\lambda$ is smaller than or equal to the absolute value of the sum of all the contributions of each petal of $\mathcal{H}_F$ to $\lambda$. In order to prove this, we recursively find a subsequence of petals $(P_j)_{j=1}^t$ in $\mathcal{H}_F$ such that the intersection graph $P_j \cap (G_{i-1} \cup C \cup P_1 \cup \cdots \cup P_{j-1})$ has potentially many isolated vertices. These isolated vertices allow us to gain a sufficiently negative contribution to $\lambda$ from each petal in the sequence, and hence 'beat' the contribution given by the cycle in (4.14). This sequence

of petals does not necessarily contain all the petals of $\mathcal{H}_F$, but this is not a problem. By Lemma 4.6.3($a$), all the petals in $\mathcal{H}_F$ give a negative contribution to $\lambda$, and hence we may discard some petals from the analysis (and adding them later will not increase the value of $\lambda$).

We define this sequence of petals iteratively. Let us say that $V(C) = \{u_0, \dots u_{\ell-1}\}$ with $u_{j-1}u_j \in E(C)$, for each $j \in [\ell]$ (assuming that $u_\ell = u_0$), and that the edge $u_0u_{\ell-1}$ belongs to $G_{i-1}$. Now, define $A_0 = E(C) \setminus E(G_{i-1})$ and construct a nested sequence of sets $(A_s)_{s\geq 0}$ in the following recursive way. For each $s \in \mathbb{N}$, if $A_{s-1}$ is empty, then let $A_s = \emptyset$. If $A_{s-1}$ is non-empty, then let

$$m_s = \min\{m : u_m u_{m+1} \in A_{s-1}\}$$

and let $P_s = P_{u_{m_s}u_{m_s+1}}$ be the petal in $\mathcal{H}_F$ which covers the edge $u_{m_s}u_{m_s+1}$. Then, set

$$A_s = A_{s-1} \setminus \{u_m u_{m+1} : u_{m+1} \in V(P_s)\}.$$

Let $t$ be the smallest integer such that $A_t = \emptyset$, and note that $t \leq |A_0| = |E(C) \setminus E(G_{i-1})|$.

For simplicity, denote $G_{i-1}^{(0)} = G_{i-1} \cup C$ and, more generally, for each $1 \leq s \leq t$, let

$$G_{i-1}^{(s)} = G_{i-1} \cup C \cup P_1 \cup \ldots \cup P_s.$$

Now, observe that

$$\lambda(G_i) - \lambda(G_{i-1}) \leq \lambda(G_{i-1}^{(0)}) - \lambda(G_{i-1}) + \sum_{s=1}^{t} \big(\lambda(G_{i-1}^{(s)}) - \lambda(G_{i-1}^{(s-1)})\big). \tag{4.15}$$

Indeed, Lemma 4.6.3($a$) together with (4.11) imply that we can discard the petals in $\{P_e : e \in E(C) \setminus E(G_{i-1})\}$ which do not belong to the chosen sequence $P_1, \dots, P_t$. Moreover, equality holds if and only if $P_1, \dots, P_t$ are all the petals in the flower $\mathcal{H}_F$. To bound each increment in (4.15), we next analyse the structure of the graph $J_s := G_{i-1}^{(s-1)} \cap P_s$. Define

$$I_s = \{u_{m+1} \in V(J_s) \setminus \{u_{m_s+1}\} : u_m u_{m+1} \in A_{s-1}\}.$$

**Claim 4.6.4.** *The degree of $u_{m_s+1}$ in $J_s$ is 1 and $I_s$ is a set of isolated vertices in $J_s$.*

*Proof.* Let $u_m$ be any vertex in $I_s \cup \{u_{m_s+1}\}$ and $w$ be any vertex in $J_s$. We affirm that $u_m$ is adjacent to $w$ inside the graph $J_s$ if and only if $\{u_m w\} = C \cap P_s$. Indeed, we cannot have $u_m w \in E(G_{i-1})$, otherwise $P_s$ would be an $r$-clique which intersects $G_{i-1}$ in at least 2 vertices, contradicting Lemma 4.5.4 (*F3*). If $w \neq u_{m+1}$, we also cannot have $\{u_m w\} \in E(P_1 \cup \cdots \cup P_{s-1})$, otherwise $u_{m-1}u_m \notin A_{s-1}$, and hence $u_m \notin I_s \cup \{u_{m_s+1}\}$.

As $u_{m_s}u_{m_s+1}$ is the only edge in $P_s \cap C$, it follows that $u_{m_s}$ is the only neighbour of $u_{m_s+1}$ in $J_s$, and that $u_m$ is isolated in $J_s$ for any $u_m \in I_s$. $\square$

Let $\widetilde{J}_s$ be the subgraph of $J_s$ induced by the vertex set $V(J_s) \setminus I_s$. By the previous claim, we have $E(\widetilde{J}_s) = E(J_s)$, which implies that $\beta_{r,\ell}(J_s) = \beta_{r,\ell}(\widetilde{J}_s) - |I_s|$ (see (4.10)). By (4.11), we obtain

$$\lambda(G_{i-1}^{(s)}) - \lambda(G_{i-1}^{(s-1)}) = \beta_{r,\ell}(J_s) = \beta_{r,\ell}(\widetilde{J}_s) - |I_s| \leq \beta_{r,\ell}(K_2) - |I_s| \tag{4.16}$$

for every $1 \leq s \leq t$. In the last inequality we use Lemma 4.6.3($c$), as $d(u_{m_s+1}) = 1$ by Claim 4.6.4. Moreover, by Lemma 4.6.3($c$), equality holds if and only if $\widetilde{J}_s \cong K_2$. When $\widetilde{J}_s \cong K_2$, note that we also have $|I_s| = 0$, as the only vertex $u_{m+1} \in V(J_s)$ such that $u_m u_{m+1} \in A_{s-1}$ is $u_{m+1} = u_{m_s+1}$.

Combining (4.14), (4.15) and (4.16), we have

$$\lambda(G_i) - \lambda(G_{i-1}) \leq \left(\frac{\ell-2}{\ell-1} - \frac{1}{m_2(K_r, C_\ell)}\right) \cdot |E(C) \setminus E(G_{i-1})| + t\beta_{r,\ell}(K_2) - \sum_{s=1}^{t} |I_s|. \tag{4.17}$$

From the definitions of $A_s$ and $I_s$, it is easy to see that $\sum_s (|I_s|+1) = |A_0| = |E(C) \setminus E(G_{i-1})|$. And, by Lemma 4.6.3($b$), we have $\beta_{r,\ell}(K_2) = m_2(K_r, C_\ell)^{-1} - (\ell-2)/(\ell-1)$. Then, (4.17) is equivalent to

$$\lambda(G_i) - \lambda(G_{i-1}) \leq (\beta_{r,\ell}(K_2) + 1) \cdot (t - |A_0|). \tag{4.18}$$

By Lemma 4.6.3, $\beta_{r,\ell}(K_2) > -1$ and, as we have $t \leq |A_0|$, it follows that

$$(\beta_{r,\ell}(K_2) + 1) \cdot (t - |A_0|) \leq 0. \tag{4.19}$$

Clearly, equality in (4.19) holds if and only if $t = |A_0|$. We conclude that $\lambda(G_i) - \lambda(G_{i-1}) \leq 0$ in the case when we add the flower $\{C\} \cup \{P_e : e \in C \setminus E(G_{i-1})\}$.

Observe that $\lambda(G_i) - \lambda(G_{i-1}) = 0$ if and only if we have equalities in (4.14)–(4.19). This means that we must have $C \cap G_{i-1} \cong K_2$ (and hence $|A_0| = \ell - 1$), $t = |A_0|$ and

$$P_s \cap (G_{i-1} \cup C \cup P_1 \cup \cdots \cup P_{s-1}) \cong K_2,$$

for each $1 \leq s \leq t$. As $e \in E(P_e \cap C)$, we infer that none of the $\ell - 1$ petals intersect outside the cycle $C$ and that the only petals sharing a vertex are consecutive petals, which share exactly one vertex. This happens if and only if $|V(G_i) \setminus V(G_{i-1})| = (r-1)(\ell-1) - 1$, in which case $i$ is *not* added to $D_i$ (cf. line 7 of HYPERTREE), and then $i \notin D_T$. This proves (1). The existence of $\delta = \delta(r, \ell)$ for (2) readily follows by noting that there are only $C = C(r, \ell)$ non-isomorphic configurations of such flowers and cliques (and how they intersect with $G_{i-1}$). This finishes the proof of the lemma. □

It remains to prove Lemma 4.3.6, which bounds the number of non-isomorphic underlying graphs that HYPERTREE may output. Recall that, for a set of graphs $S$, we denote by $S/_{\cong}$ a set consisting of exactly one representative graph for every (graph) isomorphism class of $S$. In principle, $|\mathrm{Out}_{r,\ell}(n)/_{\cong}|$ could be very large, but this is avoided by two means. Firstly, the number of degenerate steps in HYPERTREE is bounded by a constant. In this case, we bound the number of possible (non-isomorphic) structures that can emerge in one iteration of the while loop of HYPERTREE quite crudely. Secondly, in a non-degenerate step, we ensure that there is only one possible structure emerging from a given $\mathbf{G}(\mathcal{H}_t)$, up to isomorphism. Here,

it is important that we fix the canonical edge of $\mathbf{G}(\mathcal{H}_t)$ in a unique way for the class of graphs isomorphic to $\mathbf{G}(\mathcal{H}_t)$, c.f. Definition 4.5.2.

We first bound how many non-isomorphic graphs $G_t = \mathbf{G}(\mathcal{H}_t)$ the algorithm HYPERTREE can produce in step $t$, for all $t = 1, \dots, \lceil \log n \rceil$. To do so, we need to recall and define some notation. For each $n \in \mathbb{N}$, recall that $\mathrm{Crit}_{r,\ell}(n) = \bigcup_{V(G)=[n]} \mathrm{Crit}_{r,\ell}(G)$. For a hypergraph $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(n)$, let $T(\mathcal{H})$ be the stopping time of HYPERTREE($\mathcal{H}$). For any $t \geq 0$ and any $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(n)$ such that $T(\mathcal{H}) \geq t$, let $\mathcal{H}_t(\mathcal{H})$ be the hypergraph obtained in step $t$ of HYPERTREE($\mathcal{H}$) and let $D_t(\mathcal{H})$ be the accompanying set of integers. Recall that $\mathcal{H}_t$ is a subgraph of $\mathcal{G}_{r,\ell}(G)$ for some graph $G$ with $V(G) = [n]$, so that $V(\mathcal{H}_t) \subseteq \binom{[n]}{2}$ and we can associate with $\mathcal{H}_t$ a graph $\mathbf{G}(\mathcal{H}_t)$, called the underlying graph of $\mathcal{H}_t$, which is a subgraph of $G$. Finally, for each $t, n \in \mathbb{N}$ and each set $D \subseteq \{1, \dots, t\}$, define

$$\mathcal{G}(t, D, n) = \bigcup \Big\{ \mathbf{G}(\mathcal{H}_t) : \mathcal{H}_t = \mathcal{H}_t(\mathcal{H}) \Big\},$$

where the union is over all $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(n)$ such that $D_t(\mathcal{H}) = D$ and $T(\mathcal{H}) \geq t$. Our next lemma gives an upper bound on the size of $\mathcal{G}(t, D, n)/_{\cong}$.

**Lemma 4.6.5.** *For all $r, \ell \geq 4$ there exists $C > 0$ such that $|\mathcal{G}(t, D, n)/_{\cong}| \leq (tr\ell)^{C|D|}$, for all $t, n \in \mathbb{N}$ and $D \subseteq \{1, \dots, t\}$.*

*Proof.* To simplify notation, set $g(t, D, n) := |\mathcal{G}(t, D, n)/_{\cong}|$. First, note that $\mathcal{G}(0, \emptyset, n)$ contains only one graph $G_0$, up to isomorphism, and hence $g(0, \emptyset, n) = 1$. Indeed, for every $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(n)$, the hypergraph $\mathcal{H}_0(\mathcal{H})$ consists of one hyperedge of type 1 (c.f. Lemma 4.3.4($a$)). That is, $G_0$ is a copy of $K_r$.

Now, we claim that for each $t \geq 1$ and each $D \subseteq \{1, \dots, t\}$, we have

$$g(t, D, n) \leq \begin{cases} g(t-1, D, n) & \text{if } t \notin D; \\ g\big(t-1, D \setminus \{t\}, n\big) \cdot (t\ell r)^{4(\ell r)^2} & \text{if } t \in D. \end{cases} \tag{4.20}$$

First, assume that $t \notin D$. Let $G_{t-1} \in \mathcal{G}(t-1, D, n)$. We will show that there is at most one graph $G_t \in \mathcal{G}(t, D, n)$, up to isomorphism, such that if $\mathcal{H}$ is a subgraph with $\mathbf{G}(\mathcal{H}_{t-1}(\mathcal{H})) \cong G_{t-1}$ and $T(\mathcal{H}) \geq t$ then we must have that $\mathbf{G}(\mathcal{H}_t(\mathcal{H})) \cong G_t$. If $t \geq \log n$ or $\lambda(G_{t-1}) \leq -\varepsilon$, then $T(\mathcal{H}) = t-1$ for all $\mathcal{H}$ such that $\mathbf{G}(\mathcal{H}_{t-1}(\mathcal{H})) \cong G_{t-1}$. In this case, the statement is trivially true. So we may assume that $t \leq \log n$ and $\lambda(G_{t-1}) > -\varepsilon$. Let $\mathcal{H}$ be any hypergraph in $\mathrm{Crit}_{r,\ell}(n)$ such that $D_t(\mathcal{H}) = D$ and $\mathbf{G}(\mathcal{H}_{t-1}) \cong G_{t-1}$, where $\mathcal{H}_{t-1} = \mathcal{H}_{t-1}(\mathcal{H})$. As $t \notin D$ and HYPERTREE($\mathcal{H}$) did not stop after iteration $t$, we have $\mathcal{H}_t := \mathcal{H}_t(\mathcal{H}) = \mathcal{H}_{t-1} \cup \mathcal{H}_F$, for some flower $\mathcal{H}_F$ such that

$$|V(\mathbf{G}(\mathcal{H}_t)) \setminus V(\mathbf{G}(\mathcal{H}_{t-1}))| = (r-1)(\ell-1) - 1, \tag{4.21}$$

see line 7 of HYPERTREE. For (4.21) to hold, observe that $\mathbf{G}(\mathcal{H}_F)$ must intersect $\mathbf{G}(\mathcal{H}_{t-1})$ in exactly one edge, the canonical edge $e_0$ of $\mathbf{G}(\mathcal{H}_{t-1})$, see line 1 of FLOWER($\mathcal{H}_{t-1}, \mathcal{H}$). Once we have this edge, we can see that FLOWER generates only one type of flower $\mathbf{G}(\mathcal{H}_F)$ such that (4.21) holds and $\mathbf{G}(\mathcal{H}_F) \cap \mathbf{G}(\mathcal{H}_{t-1})$ is equal to $\{e_0\}$. Moreover, by construction, $e_0$ only depends on the isomorphism class of $\mathbf{G}(\mathcal{H}_{t-1})$, see Definition 4.5.2 and Corollary 4.5.3. Therefore, for any other hypergraph $\widetilde{\mathcal{H}}$ such that $\mathbf{G}(\mathcal{H}_{t-1}(\widetilde{\mathcal{H}})) \cong \mathbf{G}(\mathcal{H}_{t-1}) \cong G_{t-1}$ and $t \notin D_t(\widetilde{\mathcal{H}})$, the flower $\widetilde{\mathcal{H}}_F$ given by the algorithm FLOWER in iteration $t$ of HYPERTREE($\widetilde{\mathcal{H}}$) satisfies $\mathbf{G}(\widetilde{\mathcal{H}}_F) \cap \mathbf{G}(\mathcal{H}_{t-1}(\widetilde{\mathcal{H}})) = \{e_0'\}$, where $e_0'$ is the image of $e_0$ under some graph isomorphism $\varphi : V(\mathbf{G}(\mathcal{H}_{t-1})) \to V(\mathbf{G}(\mathcal{H}_{t-1}(\widetilde{\mathcal{H}})))$. Thus, we conclude that the two graphs $\mathbf{G}(\mathcal{H}_t(\mathcal{H}))$ and $\mathbf{G}(\mathcal{H}_t(\widetilde{\mathcal{H}}))$ produced after $t$ iterations of the while loop by HYPERTREE($\mathcal{H}$) and HYPERTREE($\widetilde{\mathcal{H}}$), respectively, are isomorphic. This implies that $g(t, D, n) \leq g(t-1, D, n)$ when $t \notin D$, which proves the first inequality in (4.20).

Now, suppose that $t \in D$. To show the second inequality in (4.20), note that in step $t$ of HYPERTREE($\mathcal{H}$) one of the following holds: (1) $\mathcal{H}_t = \mathcal{H}_{t-1} \cup \{E\}$, for some $E \in \mathcal{E}_1(\mathcal{H})$; or (2) $\mathcal{H}_t = \mathcal{H}_{t-1} \cup \mathcal{H}_F$, for some flower $\mathcal{H}_F \subseteq \mathcal{H}$. Let $H = \mathbf{G}(E)$ or $H = \mathbf{G}(\mathcal{H}_F)$ be the underlying

graph of the hyperedges that were added in step $t$. In order to count how many choices we have for the graph $\mathbf{G}(\mathcal{H}_{t-1}) \cup H$ it suffices to count how many subgraphs in $\mathbf{G}(\mathcal{H}_{t-1})$ have at most $v(H)$ vertices and how many subgraphs $H$ has. As $v(H) \leq \ell r$ and $v\big(\mathbf{G}(\mathcal{H}_{t-1})\big) \leq t\ell r$, there are at most $(t\ell r)^{\ell r} \cdot 2^{(\ell r)^2}$ subgraphs in $\mathbf{G}(\mathcal{H}_{t-1})$ with at most $\ell r$ vertices. Moreover, we can easily see that there are at most $(\ell r)^{\ell r} \cdot 2^{(\ell r)^2}$ subgraphs in $H$. From these bounds it follows that there are at most $(t\ell r)^{\ell r} 2^{(\ell r)^2} \cdot (\ell r)^{\ell r} 2^{(\ell r)^2} \leq (t\ell r)^{4(\ell r)^2}$ choices for the graph $\mathbf{G}(\mathcal{H}_{t-1}) \cup H$. That is, the graph $\mathbf{G}(\mathcal{H}_t)$ may be obtained from $\mathbf{G}(\mathcal{H}_{t-1})$ in at most $(t\ell r)^{4(\ell r)^2}$ ways, and hence $g(t, D, n) \leq g(t-1, D, n) \cdot (t\ell r)^{4(\ell r)^2}$.

As $g(0, \emptyset, n) = 1$, it follows that $g(t, D, n) \leq (t\ell r)^{4(\ell r)^2 |D|}$ by iterating the inequalities in (4.20). $\square$

Now, we are ready to prove Lemma 4.3.6:

*Proof.* [Proof of Lemma 4.3.6] We first claim that there exists a constant $C_1 = C_1(r, \ell) > 0$ such that $|D_T(\mathcal{H})| \leq C_1$ for all $\mathcal{H} \in \mathrm{Crit}_{r,\ell}(n)$. Recall that $T = T(\mathcal{H})$ denotes the stopping time of HYPERTREE($\mathcal{H}$). Fix any hypergraph $\mathcal{H}$ in $\mathrm{Crit}_{r,\ell}(n)$ and let $G_i = \mathbf{G}(\mathcal{H}_i)$ for $i = 0, \ldots, T$. By Lemma 4.6.1, we have $\lambda(G_i) \leq \lambda(G_{i-1}) - \delta$ if $i \in D_T(\mathcal{H})$, and $\lambda(G_i) = \lambda(G_{i-1})$ if $i \notin D_T(\mathcal{H})$, where $\delta = \delta(r, \ell) > 0$. As $\lambda(G_0) = \lambda(K_r)$ (by Lemma 4.3.4($a$)) and $\lambda(G_{T(\mathcal{H})-1}) > -\varepsilon$ (by Lemma 4.3.4($c$)), it follows that $|D_T(\mathcal{H})| \leq 1 + (\lambda(K_r) + \varepsilon)/\delta$. As $\varepsilon$ only depends on $r$ and $\ell$, this proves our claim.

By Lemma 4.3.4($c$), the stopping time $T$ is bounded from above by $\log n$. Since $|D_T| \leq C_1$, the size of $\mathrm{Out}_{r,\ell}(n)/_{\cong}$ is bounded by the size of

$$\bigcup_{t \leq \log n} \bigcup_{\substack{D \subseteq [t]: \\ |D| \leq C_1}} |\mathcal{G}(t, D, n)/_{\cong}|,$$

where $\mathcal{G}(t, D, n)$ was defined just above Lemma 4.6.5. Using the bound on $|\mathcal{G}(t, D, n)/_{\cong}|$ given by Lemma 4.6.5, we conclude that

$$|\mathrm{Out}_{r,\ell}(n)/_{\cong}| \leq \sum_{t=1}^{\lceil \log n \rceil} \sum_{\substack{D \subseteq [t]: \\ |D| \leq C_1}} (t\ell r)^{C|D|} \leq (\log n)^{C_0},$$

for some $C_0 = C_0(r, \ell) > 0$. $\square$

## 4.7 Proof of Fact 4.6.2

Note that every subgraph $J \subsetneq C_\ell$ is a forest, and so we have $e(J) \leq v(J) - 1$. Thus, for every $J \subsetneq C_\ell$ with $v(J) \geq 3$ this implies that $(e(J) - 1)/(v(J) - 2) \leq 1$. On the other hand,

$$\frac{e(C_\ell) - 1}{v(C_\ell) - 2} = \frac{\ell - 1}{\ell - 2} > 1,$$

which implies $m_2(C_\ell) = (\ell - 1)/(\ell - 2)$. Now, let us analyse subgraphs of $K_r$. For each $J \subseteq K_r$, we have $e(J) \leq \binom{v(J)}{2}$. Thus,

$$\frac{e(J) - 1}{v(J) - 2} \leq \frac{\binom{v(J)}{2} - 1}{v(J) - 2} = \frac{v(J) + 1}{2}$$

for each $J \subseteq K_r$ such that $v(J) \geq 3$. It follows that $m_2(K_r) = (r + 1)/2$. Next, for each $\ell \geq 3$, consider the function $f_\ell : \mathbb{N} \to \mathbb{Q}$ defined by

$$f_\ell(t) = \frac{\binom{t}{2}}{t - 2 + m_2(C_\ell)^{-1}}.$$

It is not hard to check that $(f_\ell(t))_{t \geq 3}$ is monotone increasing (for every given $\ell$). Since $m_2(C_\ell) = (\ell - 1)(\ell - 2)$, we have

$$m_2(K_r, C_\ell) = f_\ell(r) = \frac{\binom{r}{2}}{r - 2 + (\ell - 2)/(\ell - 1)}. \tag{4.22}$$

It follows readily from this identity that $m_2(K_r, C_\ell)$ is strictly decreasing in $\ell$, and thus,

$$m_2(K_r, C_\ell) \leq m_2(K_r, C_3) = \frac{r(r-1)}{2r-3} < \frac{r+1}{2} = m_2(K_r) \tag{4.23}$$

for every $r \geq 4$. Finally, the identity in (4.22) implies that

$$m_2(K_r, C_\ell) = \frac{\binom{r}{2}(\ell-1)}{(r-1)(\ell-1)-1} = \frac{r}{2} \cdot \frac{1}{1-\frac{1}{(r-1)(\ell-1)}} > \frac{r}{2}.$$

BIBLIOGRAPHY


[1] M. Ajtai, J. Komlós and E. Szemerédi, A note on Ramsey numbers, *J. Combinatorial Th. (A)*, **299** (1980), 354–360.

[2] M. Ajtai, J. Komlós and E. Szemerédi, A dense infinite Sidon sequence, *Europ. J. Combinatorics*, **2** (1981), 1–11.

[3] H. Acan, J. Kahn, Disproof of a packing conjecture of Alon and Spencer, *Random Structures Algorithms* **55** (2019), no. 3, 531–544.

[4] N. Alon and J. Spencer, The Probablistic Method, *Wiley, New York, 1992.*

[5] K. Azuma, Weighted sums of certain dependent random variables, *Tohoku Math. J.* **19** (1967), no. 3, 357–367.

[6] J. Balogh, R. Morris and W. Samotij, Independent sets in hypergraphs, *J. Amer. Math. Soc.*, **28** (2015), 669–709.

[7] J. Balogh, R. Morris and W. Samotij, The method of hypergraph containers, *Proc. Int. Cong. Math.*, Rio de Janeiro, 2018, Vol. 3, 3045–3078.

[8] J. Balogh and W. Samotij, An efficient container lemma, *discrete analysis*, **17** (2020), 56pp.

[9] A. Basak and M. Rudelson, Sharp transition of the invertibility of the adjacency matrices of sparse random graphs, *Probab. Theory Relat. Fields* (2021).

[10] S. Ben-Shimon, M. Krivelevich and B. Sudakov, On the Resilience of Hamiltonicity and Optimal Packing of Hamilton Cycles in Random Graphs, **25** (2011), *SIAM J. Discr. Math.*, 173–211.

[11] B. Bollobás, Random Graphs, *In Combinatorics, Proceedings, Swansea* (1981), 80–102.

[12] B. Bollobás, The chromatic number of random graphs, *Combinatorica* **8** (1988) 49–55.

[13] B. Bollobás and P. Erdős, Cliques in random graphs, *Math. Proc. Cam. Phil. Soc.*, **80** (1976), 419–427.

[14] B. Bollobás and A. Thomason, Threshold functions, *Combinatorica*, **7** (1987), 35–38.

[15] J. Bourgain, V. H. Vu and P. M. Wood, On the singularity probability of discrete random matrices, *J. Funct. Anal.*, **258** (2010), 559–603.

[16] M. Campos, M. Jenssen, M. Michelen and J. Sahasrabudhe, Singularity of random symmetric matrices revisited, arXiv:2011.03013 (2020).

[17] M. Campos, L. Mattos, R. Morris and N. Morrison, On the singularity of random symmetric matrices, *Duke Math. J.*, **170** (2021), 881–907.

[18] D. Conlon, A new upper bound for diagonal Ramsey numbers, *Ann. of Math.*, **170** (2009), 941–960.

[19] K. P. Costello, T. Tao and V. Vu, Random symmetric matrices are almost surely non-singular, *Duke Math. J.*, **135** (2006), 395–413.

[20] P. Erdős, On sequences of integers no one of which divides the product of two others and on some related problems, *Mitt. Forsch.-Inst. Math. Mech. Univ. Tomsk*, **2** (1938), 74–82.

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

[22] P. Erdős, Some remarks on the theory of graphs, *Bull. Amer. Math. Soc.*, **53** (1947), 292–294.

[23] P. Erdős and A. Hajnal, Research problems 2–3, *J. Combin. Theory*, **2** (1967), 104–105.

[24] P. Erdős and L. Moser, Elementary problems and solutions, *Amer. Math. Monthly*, **4** (1947), 229–230.

[25] P. Erdős and A. Rényi, On random graphs I, *Publicationes Mathematicae*, **6** (1959), 290–297.

[26] P. Erdős and A. Rényi, On the evolution of random graphs, *Publ. Math. Inst. Hungar. Acad. Sci.*, **5** (1960), 17–61.

[27] P. Erdős and A. Rényi, On the existence of a factor of degree one of a connected random graph, *Acta Mathematica Academiae Scientiarum Hungaricae*, **17** (1966), 359–368.

[28] P. Erdős and G. Szekeres, A combinatorial problem in geometry, *Compositio Math.* **2** (1935), 463—470.

[29] C. Esseen, On the Kolmogorov–Rogozin inequality for the concentration function, *Z. Wahrscheinlichkeitstheorie verw Gebiete*, **5** (1966), 210–216.

[30] A. Ferber and V. Jain, Singularity of random symmetric matrices – a combinatorial approach to improved bounds, *Forum Math., Sigma*, **7** (2019), e22.

[31] A. Ferber, V. Jain, K. Luh, and W. Samotij, On the counting problem in inverse Littlewood–Offord theory, arXiv:1904.10425.

[32] A. Ferber, K. Luh and G. McKinley, Resilience of the Rank of Random Matrices, arXiv:1910.03619 (2019)

[33] A. Ferber and W. Samotij, Packing trees of unbounded degrees in random graphs, *J. of the London Math. Soc.*, **99** (2018), 653–677.

[34] J. Folkman, Graphs with monochromatic complete subgraphs in every edge coloring, *SIAM J. Appl. Math.*, **18** (1970), 19–24.

[35] P. Frankl and Z. Füredi, Solution of the Littlewood–Offord problem in high dimensions, *Ann. Math.*, **128** (1988), 259–270.

[36] P. Frankl and V. Rödl, Near Perfect Coverings in Graphs and Hypergraphs, *Eur. J. of Comb.*, **6** (1985), 317–326.

[37] P. Frankl and V. Rödl, Large triangle-free subgraphs in graphs without $K_4$, *Graphs and Combinatorics*, **2** (1986), 135–144.

[38] D. Freedman, On tail probabilities for martingales, *Ann. Probab.* **3** (1975), 100–118.

[39] E. Friedgut, Sharp threshold of graph properties and the k-SAT problem, *J. of the Amer. Math. Soc.*, **12** (1999), 1017–1054.

[40] E. Friedgut and M. Krivelevich, Sharp thresholds for certain Ramsey properties of random graphs, *Random Struct. Algorithms*, **17** (2000), 1–19.

[41] A. Frieze and M. Karoński, Introduction to random graphs, *Cambridge University Press.*

[42] A. Frieze and M. Krivelevich, On packing Hamilton cycles in $\varepsilon$-regular graphs, *J. of Comb. Theory, Series B*, **94** (2005), 159–172.

[43] E. Gilbert, Random graphs, *Ann. of Math. Stat.*, **30** (1959), 1141–1144.

[44] R. Graham and V. Rödl, Numbers in Ramsey theory, *London Math. Soc. Lecture Note Ser.*, **123** (1987), 111–153.

[45] B. Green and I. Ruzsa, Freiman's theorem in an arbitrary abelian group, *Journal of the London Mathematical Society*, **1** (2007), 163–175.

[46] S. Griffiths, L. Mattos and R. Morris, Clique-packings in random graphs, in preparation.

[47] L. Gugelmann, R. Nenadov, Y. Person, N. Škorić, A. Steger, and H. Thomas, Symmetric and asymmetric Ramsey properties in random hypergraphs, *Forum Math. Sigma*, **5** (2017), p. e28.

[48] G. Halász, Estimates for the concentration function of combinatorial number theory and probability, *Period. Math. Hungar.*, **8** (1977), 197–211.

[49] W. Hoeffding, Probability inequalities for sums of bounded random variables, *J. Amer. Statist. Assoc.* **58** (1963), 13–30.

[50] R. Horn and C. Johnson, Matrix Analysis (second edition), Cambridge University Press, 2013.

[51] H. Huang, Rank of Sparse Bernoulli Matrices, arXiv:2009.13726v2 (2020).

[52] V. Jain, A. Sah, M. Sawhney, On the smallest singular value of symmetric random matrices, arXiv:2011.02344 (2020).

[53] V. Jain, A. Sah, M. Sawhney, Singularity of discrete random matrices I, arXiv:2010.06553 (2020).

[54] V. Jain, A. Sah, M. Sawhney, Singularity of discrete random matrices II, arXiv:2010.06554 (2020).

[55] S. Janson, Poisson approximation for large deviations, *Random Structures Algorithms* **1** (1990), 221–230.

[56] S. Janson, T. Łuczak and A. Ruciński, *Random graphs*, Wiley-Interscience, 2000.

[57] S. Janson and A. Ruciński, The infamous upper tail, *Random Structures Algorithms* **20** (2002), no. 3, 317–342.

[58] S. Janson and A. Ruciński, The Deletion Method For Upper Tail Estimates, *Combinatorica* **24** (2004), 615–640.

[59] A. Johansson, J. Kahn and V. Vu, Factors in random graphs, *Rand. Struc. and Alg.*, **33** (2008), 1–28.

[60] F. Joos, J. Kim, D. Kühn and D. Osthus, Optimal packings of bounded degree trees, **21** (2019), *J. Eur. Math. Soc.*

[61] J. Kahn, J. Komlós and E. Szemerédi, On the probability that a random ±1 matrix is singular, *J. Amer. Math. Soc.*, **8** (1995), 223–240.

[62] J. Kahn, J. Komlós and E. Szemerédi, On the probability that a random ±1 matrix is singular, *J. Amer. Math. Soc.*, **8** (1995), 223–240.

[63] M. Karoński and A. Ruciński, On the number of strictly balanced subgraphs of a random graph, *In: Graph Theory, Proc. Łagów* (1983), 79–83.

[64] J. Keating, The Riemann Zeta-Function and Quantum Chaology, *Quantum Chaos* (1993), 145–185.

[65] P. Keevash and K. Staden, Ringel's tree packing conjecture in quasirandom graphs, arXiv:2004.09947v1 (2020).

[66] J. Kim, D. Kühn, D. Osthus and M. Tyomkyn, A blow-up lemma for approximate decompositions *Trans. Amer. Math. Soc.*, **371** (2019), 4655–4742.

[67] Y. Kohayakawa and B. Kreuter, Threshold functions for asymmetric Ramsey properties involving cycles, *Random Struct. Algorithms*, **11** (1997), 245–276.

[68] Y. Kohayakawa, M. Schacht and R. Spöhel, Upper bounds on probability thresholds for asymmetric Ramsey properties, *Rand. Str. and Alg.*, **44** (2012), 1–28.

[69] J. Komlós, On the determinant of $(0, 1)$ matrices, *Studia Sci. Math. Hungar.*, **2** (1967), 7–22.

[70] J. Komlós and A. Szemerédi, Limit distribution for the existence of hamiltonian cycles in a random graph, *Discr. Math.*, **43** (1983), 55–63.

[71] B. Kreuter, Threshold functions for asymmetric Ramsey properties with respect to vertex colorings, *Random Struct. Algorithms*, **9** (1996), 335–348.

[72] A. Liebenau, L. Mattos, W. Mendonça, and J. Skokan. Asymmetric Ramsey properties of random graphs for cliques and cycles. Submitted to *Random Struct. Algorithms*, arXiv:2010.11933.

[73] J. E. Littlewood and A. C. Offord, On the number of real roots of a random algebraic equation III, Rec. Math. (Mat. Sbornik) N.S., **12** (1943), 277–286.

[74] A. Litvak, K. Tikhomirov, Singularity of sparse Bernoulli matrices, arXiv:2004.03131v1 (2020).

[75] G. Livshyts, K. Tikhomirov and R. Vershynin, The smallest singular value of inhomogeneous square random matrices, *arXiv: 1909.04219*

[76] P. Lopatto and K. Luh, Tail bounds for gaps between eigenvalues of sparse random matrices, arXiv:1901.05948.

[77] L. Lovász and M. Saks, Lattices, Möbius Functions and Communication Complexity. *Annual Symp. Found. Comp. Science* (1988), 81–90.

[78] S. Lovett, Communication is Bounded by Root of Rank, *Assoc. for Comp. Machinery*, **63** (2016), 1–9.

[79] T. Łuczak, A. Ruciński, and B. Voigt, Ramsey properties of random graphs, *J. Combin. Theory Ser. B*, **56** (1992), 55–68.

[80] K. Luh and V. Vu, Sparse Random Matrices have Simple Spectrum, *Annales de l'Institut Henri Poincaré Probabilités et Statistiques*. Forthcoming.

[81] M. Marciniszyn, J. Skokan, R. Spöhel, and A. Steger, Asymmetric Ramsey properties of random graphs involving cliques, *Random Struct. Algorithms*, **34** (2009), 419–453.

[82] D. Matula, On the complete subgraphs of a random graph, *In Proceedings of the 2nd Chapel Hill Conference on Combinatorial Mathematics and its Applications* (1970), 356–369.

[83] D. Matula, The employee party problem, *Notices of the American Mathematical Society*, **19** (1972), A-382.

[84] K. Mehlhorn and E. M Schmidt. Las vegas is better than determinism in vlsi and distributed computing. *Proc. ACM symp. on theory of comp.* (1982), 330–337.

[85] R. Montgomery, A. Pokrovskiy and B. Sudakov, A proof of Ringel's Conjecture, arXiv:2001.02665v2.

[86] F. Mousset, R. Nenadov and W. Samotij, Towards the Kohayakawa–Kreuter conjecture on asymmetric Ramsey properties, arXiv:1808.05070 (2018).

[87] J. Nešetřil and V. Rödl, The Ramsey property for graphs with forbidden complete subgraphs, *J. Combin. Theory Ser. B*, **20** (1976), 243–249.

[88] H. H. Nguyen and V. H. Vu, Optimal inverse Littlewood–Offord theorems, *Adv. Math.*, **226** (2011), 5298–5319.

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

[90] H. H. Nguyen and V. H. Vu, Small ball probability, inverse theorems, and applications, In: Erdős Centennial, pages 409–463. Springer, 2013.

[91] N. Nisan and A. Wigderson, On rank vs. communication complexity, *Combinatorica*, **15** (1995), 557–565.

[92] A. M. Odlyzko, On subspaces spanned by random selections of $\pm 1$ vectors, *J. Combin. Theory Ser. A*, **47** (1988), 124–133.

[93] F. Ramsey, On a problem of formal logic, *Proc. of London Math. Soc.*, **30** (1930), 264–286.

[94] V. Rödl, On a packing and covering problem, *Eur. J. of Comb.*, **6** (1985),69–78.

[95] V. Rödl and A. Ruciński, Lower bounds on probability thresholds for Ramsey properties, *Combinatorics, Paul Erdős is eighty*, **1** (1993), 317–346.

[96] V. Rödl and A. Ruciński, Threshold functions for Ramsey properties, *J. of Amer. Math. Soc.*, **8** (1995), 917–942.

[97] V. Rödl and A. Ruciński, Threshold functions for Ramsey properties, *J. of Amer. Math. Soc.*, **8** (1995), 917–942.

[98] V. Rödl, A. Ruciński and M. Schacht, An exponential-type upper bound for Folkman numbers, *Combinatorica*, **37** (2017), 767–784.

[99] B.A. Rogozin, On the increase of dispersion of sums of independent random variables, *Teor. Verojatnost. i Primenen.*, **6** (1961), 106–108.

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

[101] A. Ruciński, Small subgraphs of random graphs – a survey, *Random graphs*, John Wiley & Sons (1987).

[102] A. Ruciński, Matching and covering the vertices of a random graph by copies of a given graph, *Discrete Mathematics*, **105** (1992), 185–197.

[103] A. Ruciński and A. Vince, Strongly balanced graphs and random graphs, *Journal of Graph Theory*, **10** (1986), 251–264.

[104] M. Rudelson and R. Vershynin, Smallest singular value of a random rectangular matrix, *Comm. Pure Appl. Math.*, **62** (2009), 1707–1739.

[105] M. Rudelson and R. Vershynin, Non-asymptotic theory of random matrices: extreme singular values, *Proc. Int. Cong. Math.*, Hyderabad, 2010, Vol. 3, 1576–1602.

[106] A. Sah, Diagonal Ramsey via effective quasirandomness, arXiv:2005.09251 (2020).

[107] A. Sárkőzy and E. Szemerédi, Uber ein Problem von Erdős und Moser, *Acta Arith.*, **11** (1965), 205–208.

[108] D. Saxton and A. Thomason, Hypergraph containers, *Inv. Math.*, **201** (2015), 1–68.

[109] J. Spencer, Ramsey's theorem – a new lower bound, *J. Combin. Theory Ser. A*, **18** (1975), 108–115.

[110] J. Spencer, Three hundred million points suffice, *J. Combin. Theory Ser. A*, **49** (1988), 210–217.

[111] D. Spielman and S. Teng, Smoothed analysis of algorithms: why the simplex algorithm usually takes polynomial time, *J. of the ACM.*, **51** (2004), 385–463.

[112] T. Tao and V. Vu, On random ± matrices: Singularity Determinant, *Random Struct. Algorithms*, **28** (2006), 1–23.

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

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

[115] 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.*, **46** (2009), 377–396.

[116] T. Tao and V. Vu, A sharp inverse Littlewood-Offord theorem, *Random Str. and Alg.*, **37** (2010), 525–539.

[117] A. Thomason, An upper bound for some Ramsey numbers, *J. Graph Theory*, **12** (1988), 509–517.

[118] K. Tikhomirov, Singularity of random Bernoulli matrices, *Ann. Math.*, **191** (2020), 593–634.

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

[120] V. Vu, Random discrete matrices, *In: Horizons of combinatorics, Bolyai Soc.Math. Stud.*, **17** (2008), 257–280.

[121] V. Vu, Combinatorial problems in random matrix theory, *Proc. Int. Cong. Math.*, Seoul, 2014, Vol. 4, 489–508.

[122] V. Vu, Recent progress in combinatorial random matrix theory, arXiv:2005.02797 (2020).

[123] V. Waerden, Beweis einer Baudetschen Vermutung, *Nieuw. Arch. Wisk. (in German)*, **15** (1927), 212–216.

[124] E. Wigner, Characteristic vectors of bordered matrices with infinite dimensions, *Ann. of Math.*, **62** (1955), 548–564.