

CHASING THE  $k$ -COLORABILITY THRESHOLD\*AMIN COJA-OGHLAN<sup>†</sup> AND DAN VILENCHIK

**ABSTRACT.** For a fixed number  $d > 0$  and  $n$  large let  $G(n, d/n)$  be the random graph on  $n$  vertices in which any two vertices are connected with probability  $d/n$  independently. The problem of determining the chromatic number of  $G(n, d/n)$  goes back to the famous 1960 article of Erdős and Rényi that started the theory of random graphs [Magyar Tud. Akad. Mat. Kutató Int. Kozl. **5** (1960) 17–61]. Progress culminated in the landmark paper of Achlioptas and Naor [Ann. Math. **162** (2005) 1333–1349], in which they calculate the chromatic number precisely for all  $d$  in a set  $S \subset (0, \infty)$  of asymptotic density  $\lim_{z \rightarrow \infty} \frac{1}{z} \int_0^z \mathbf{1}_S = \frac{1}{2}$ , and up to an additive error of one for the remaining  $d$ . Here we obtain a near-complete answer by determining the chromatic number of  $G(n, d/n)$  for all  $d$  in a set of asymptotic density 1.

*Mathematics Subject Classification:* 05C80 (primary), 05C15 (secondary)

## 1. INTRODUCTION

Let  $G(n, p)$  denote the random graph on the vertex set  $V = \{1, \dots, n\}$  in which any two vertices are connected with probability  $p \in [0, 1]$  independently, known as the *Erdős-Rényi model*.<sup>1</sup> We write  $p = d/n$  and refer to  $d$  as the *average degree*. As per common practice, we say that  $G(n, d/n)$  has a property *with high probability* (‘w.h.p.’) if the probability that the property holds converges to 1 as  $n \rightarrow \infty$ . We recall that a graph  $G$  is  *$k$ -colorable* if it is possible to assign each vertex one of the colors  $\{1, \dots, k\}$  such that no edge connects two vertices of the same color. Moreover, the *chromatic number*  $\chi(G)$  of a graph  $G$  is the least integer  $k$  such that  $G$  is  $k$ -colorable. Unless specified otherwise, we always consider  $d, k$  fixed as  $n \rightarrow \infty$ .

**1.1. Background and main results.** The theory of random graphs was born with the famous 1960 article by Erdős and Rényi [21], and has grown since into a substantial area of research with hundreds, perhaps thousands of contributions dealing with the  $G(n, p)$  model alone. In their paper, Erdős and Rényi showed that the random graph  $G(n, p)$  undergoes a percolation *phase transition* at  $p = 1/n$ , and phase transitions have been the guiding theme of the theory ever since. In addition, Erdős and Rényi set the agenda for future research by posing a number of intriguing questions, all of which have been answered over the years except for one: for a given  $d > 0$ , what is the typical chromatic number of  $G(n, d/n)$ ?

It is widely conjectured that for any number  $k \geq 3$  of colors there occurs a phase transition for  $k$ -colorability. That is, there exists a number  $d_{k-\text{col}}$  such that  $G(n, d/n)$  is  $k$ -colorable w.h.p. if  $d < d_{k-\text{col}}$ , whereas the random graph fails to be  $k$ -colorable w.h.p. if  $d > d_{k-\text{col}}$ . If true, this would imply that the likely value of the chromatic number, viewed as a function of  $d$ , is a step function that takes the value  $k$  on the interval  $d_{(k-1)-\text{col}} < d < d_{k-\text{col}}$ .

Towards this conjecture, Achlioptas and Friedgut [1] proved that for any fixed  $k \geq 3$  there exists a *sharp threshold sequence*  $d_{k-\text{col}}(n)$ . This sequence is such that for any  $\varepsilon > 0$ ,

- if  $p < (1 - \varepsilon)d_{k-\text{col}}(n)/n$ , then  $G(n, p)$  is  $k$ -colorable with probability tending to 1 as  $n \rightarrow \infty$ .
- if  $p > (1 + \varepsilon)d_{k-\text{col}}(n)/n$ , then  $G(n, p)$  fails to be  $k$ -colorable with probability tending to 1 as  $n \rightarrow \infty$ .

Whether the sequence  $d_{k-\text{col}}(n)$  converges to an actual “uniform” threshold  $d_{k-\text{col}}$  is a well-known open problem.

\*An extended abstract version of this work appeared in the Proceedings of the 54th IEEE Symposium on Foundations of Computer Science (‘FOCS’), 2013.

<sup>†</sup>The research leading to these results has received funding from the European Research Council under the European Union’s Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 278857-PTCC.

<sup>1</sup>Actually this model was introduced by Gilbert [24]. In their seminal paper Erdős and Rényi consider a random graph  $G(n, m)$  in which the number of edges is a fixed integer  $m$  [21]. However, with  $p = m/\binom{n}{2}$  both models are essentially equivalent [26].

Yet [1] is a pure existence result that does not provide any clue as to the location of  $d_{k-\text{col}}$ . In a landmark paper Achlioptas and Naor [6] proved via the “second moment method” that

$$\liminf_{n \rightarrow \infty} d_{k-\text{col}}(n) \geq d_{k,\text{AN}} = 2(k-1) \ln(k-1) = 2k \ln k - 2 \ln k - 2 + o_k(1). \quad (1.1)$$

Here and throughout,  $o_k(1)$  denotes a term that tends to zero in the limit of large  $k$ . By comparison, a naive application of the union bound shows that

$$\limsup_{n \rightarrow \infty} d_{k-\text{col}}(n) \leq d_{k,\text{first}} = 2k \ln k - \ln k. \quad (1.2)$$

Recently [14], a more sophisticated union bound argument was used to prove

$$\limsup_{n \rightarrow \infty} d_{k-\text{col}}(n) \leq d'_{k,\text{first}} = 2k \ln k - \ln k - 1 + o_k(1). \quad (1.3)$$

Thus, the gap between the lower bound (1.1) and the upper bound (1.3) on  $d_{k-\text{col}}(n)$  is about  $\ln k + 1$ , an expression that *diverges* as  $k$  gets large. By improving the lower bound, the following theorem reduces this gap to a small absolute constant of  $2 \ln 2 - 1 + o_k(1) \approx 0.39$ .

**Theorem 1.1.** *The  $k$ -colorability threshold satisfies*

$$\liminf_{n \rightarrow \infty} d_{k-\text{col}}(n) \geq d_{k,\text{cond}} - o_k(1), \quad \text{with} \quad d_{k,\text{cond}} = 2k \ln k - \ln k - 2 \ln 2. \quad (1.4)$$

The bounds (1.1), (1.3) yield an estimate of the chromatic number of  $G(n, d/n)$ . Namely, (1.1) implies that for  $d < d_{k,\text{AN}}$ , the random graph  $G(n, d/n)$  is  $k$ -colorable w.h.p. Moreover, (1.3) shows that for  $d > d_{k-1,\text{first}}$ ,  $G(n, d/n)$  fails to be  $k-1$ -colorable w.h.p. Consequently, for all  $d$  in the interval  $(d'_{k-1,\text{first}}, d_{k,\text{AN}})$  of length about  $\ln k$ , the chromatic number of  $G(n, d/n)$  is precisely  $k$  w.h.p. However, for all  $d$  in the subsequent interval  $(d_{k,\text{AN}}, d'_{k,\text{first}})$  of length about  $\ln k$ , (1.1), (1.3) only imply that the chromatic number is either  $k$  or  $k+1$  w.h.p. Thus, (1.1) and (1.3) yield the typical value of  $\chi(G(n, d/n))$  precisely for “about half” of all  $d$ . Formally, let us say that a (measurable) set  $A \subset \mathbb{R}_{\geq 0}$  has *asymptotic density*  $\alpha$  if  $\lim_{z \rightarrow \infty} \frac{1}{z} \int_0^z \mathbf{1}_A = \alpha$ , where  $\mathbf{1}_A$  is the indicator of  $A$ . Then the set on which (1.1), (1.3) determine  $\chi(G(n, d/n))$  has asymptotic density  $1/2$  [6, Theorem 2].

Theorem 1.1 enables us to pin the chromatic number down precisely on a set of asymptotic density 1, thereby obtaining a near-complete answer to the question of Erdős and Rényi. More precisely, (1.2) and (1.4) imply

**Theorem 1.2.** *There exists a constant  $k_0$  such that the following is true. Let*

$$S_k = (2(k-1) \ln(k-1) - \ln(k-1) - 0.99, 2k \ln k - \ln k - 1.38) \quad \text{and} \quad S = \bigcup_{k \geq k_0} S_k.$$

*Set  $F(d) = k$  for all  $d \in S_k$ . Then  $S$  has asymptotic density 1 and*

$$\lim_{n \rightarrow \infty} \mathbb{P}[\chi(G(n, d/n)) = F(d)] = 1 \quad \text{for any } d \in S.$$

Of course, the constants 0.99 and 1.38 in the definition of  $S_k$  can be replaced by any numbers less than one and  $2 \ln 2$ , respectively. Theorem 1.2 also answers a question of Alon and Krivelevich [8] whether the chromatic number of  $G(n, d/n)$  is concentrated on a single integer for most  $d$  “in an appropriately defined sense”.<sup>2</sup>

Independently of the mathematics literature, the random graph coloring problem has been studied in statistical physics, where it is known as the “diluted mean-field Potts antiferromagnet at zero temperature”. In fact, physicists have developed a generic, ingenious but highly non-rigorous formalism called the “cavity method” for locating phase transitions in random graphs and other discrete structures [35, 36]. The so-called “replica symmetric” variant of the cavity method predicts upper and lower bounds on  $d_{k-\text{col}}$  [30, 39], namely

$$d_{k,\text{cond}} - o_k(1) \leq \liminf_{n \rightarrow \infty} d_{k-\text{col}}(n) \leq \limsup_{n \rightarrow \infty} d_{k-\text{col}}(n) \leq d_{k,\text{first}}. \quad (1.5)$$

Theorem 1.1 establishes the lower bound rigorously.

Additionally, the cavity method yields predictions on the combinatorial nature of the problem, particularly on the geometry of the set of  $k$ -colorings of the random graph. The proof of Theorem 1.1 is based on a “physics-enhanced” second moment argument that exploits this geometrical intuition. In fact, the physics intuition is one of two key ingredients that enable us to improve over the approach of Achlioptas and Naor [6]. The second one is a

<sup>2</sup>A proof that the threshold sequence  $d_{k-\text{col}}(n)$  converges would imply a one-point concentration result for the chromatic number outside a countable set of average degrees. However, the known result [1] does not. Alon and Krivelevich [8] were concerned also with the case that the average degree  $d$  is a growing function of  $n$ . In this paper we deal with  $d$  fixed as  $n \rightarrow \infty$ , the original setting considered by Erdős and Rényi.

novel approach, based on a local variations argument, to the analytical challenge of optimizing a certain (non-convex) function over the Birkhoff polytope. Neither of these ideas seem to depend on particular features of the graph coloring problem, and thus we expect that they will prove vital to tackle a variety of further related problems.

An outline of our physics-enhanced second moment argument follows in Section 2. In addition, in Section 2.5 we will see that the density  $d_{k,\text{cond}}$  in (1.4) matches the *condensation* or *Kauzmann phase transition* predicted by physicists. This implies that the bound obtained in Theorem 1.1 is the best possible one that can be obtained via a second moment-type argument over a certain class of natural random variables (see Section 2.5 for details).

**1.2. Related work.** As witnessed by the notorious “four color problem” first posed by De Morgan in 1852, solved controversially by Appel and Haken in 1976 [9], and re-solved by Robertson, Sanders, Seymour and Thomas [40], the graph coloring problem has been a central subject in (discrete) mathematics for well over a century. Thus, it is unsurprising that the chromatic number problem on  $G(n, p)$  has received a big deal of attention since it was posed by Erdős and Rényi. Indeed, the problem has inspired the development of techniques that are by now widely used in various areas of mathematics, computer science, physics and other disciplines.

For instance, pioneering the use of martingale tail bounds, Shamir and Spencer [41] proved concentration bounds for the chromatic number of  $G(n, p)$ . Their result was enhanced first by Łuczak [33] and then by Alon and Krivelevich [8], who used the Lovász Local Lemma to prove that the chromatic number of  $G(n, p)$  is concentrated on two consecutive integers if  $p \ll n^{-1/2}$ . In a breakthrough contribution, Bollobás [11] determined the asymptotics of the chromatic number of dense random graphs (i.e.,  $G(n, p)$  with  $p > n^{-1/3}$ ). This result improved prior work by Matula [34], whose “merge-and-exposure” technique Łuczak built upon to obtain a similar result for sparser random graphs [32]. However, in the case that  $p = d/n$  for a fixed real  $d > 0$ , the setting originally studied by Erdős and Rényi, Łuczak’s formula is far less precise than (1.1)–(1.2). For a comprehensive literature overview see [12, 26].

The work of Achlioptas and Naor [6], which gave best prior result on the chromatic number of  $G(n, d/n)$ , is based on the *second moment method*. Its use in the context of phase transitions in random discrete structures was pioneered by Achlioptas and Moore [5] and Frieze and Wormald [23]. The techniques of [6] have been used to prove several further important results. For instance, Achlioptas and Moore [4] identified three (and for some  $d$  just two) consecutive integers on which the chromatic number of the random  $d$ -regular is concentrated. This was reduced to two integers for all fixed  $d$  (and one for about half of all  $d$ ) by adding in the small subgraph conditioning technique [27]. Recently, the methods developed in this work have been harnessed to improve this result further still [15]. Moreover, Dyer, Frieze and Greenhill [20] extended the second moment argument from [6] to the problem of  $k$ -coloring  $h$ -uniform random hypergraphs. We expect that our approach can be used to obtain improved results in the hypergraph case. Similarly, it should be possible to improve results of Dani, Moore and Olsen [19] on a “decorated” coloring problem.

In several problems, sophisticated applications of the second moment method gave bounds very close to the predictions made by the physicists’ cavity method [35]. Examples where the physics predictions have (largely) been verified rigorously in this way include the hypergraph 2-coloring problem [16, 18] and the random  $k$ -SAT problem [17]. But thus far a general limitation of the rigorous proof techniques has been that they only apply to *binary* problems where there are only two values available for each variable. By contrast, in random graph coloring each variable (vertex) has  $k$  values (colors) to choose from, where  $k$  can be arbitrarily large. As we will see in Section 2, the large number of available values complicates the problem dramatically. In effect, random graph coloring remained the last among the intensely-studied benchmark problems in which there remained a very substantial gap between the physics predictions and the rigorous results, a situation rectified by the present paper. Thus, we view this paper as an important step towards the long-term goal of providing a mathematical foundation for the cavity method.

In computer science, the *algorithmic* problem of finding a  $k$ -coloring of  $G(n, p)$  in polynomial time is a long-standing challenge, mentioned prominently in several influential survey articles (e.g., [22, 28]). Simple greedy algorithms find a  $k$ -coloring for  $d \leq k \ln k \sim \frac{1}{2}d_{k-\text{col}}$  w.h.p. [3, 25, 29], about half the  $k$ -colorability threshold. However, no efficient algorithm is known to beat the, in the words of Shamir and Spencer [41], “most vexing” factor of two. In fact, it has been suggested changes in the geometry of the set of  $k$ -colorings that occur at  $d \sim \frac{1}{2}d_{k-\text{col}}$  cause the demise of local-search based algorithms [2, 37]. Interestingly, some of the very phenomena that seem to make the algorithmic problem of coloring  $G(n, p)$  difficult will turn out to be extremely helpful in the construction of our random variable and thus in the proof of Theorem 1.1.

**1.3. Notation and preliminaries.** In addition to  $G(n, p)$ , we consider the  $G(n, m)$  model, which is a random graph with vertex set  $V = \{1, \dots, n\}$  and exactly  $m$  edges, chosen uniformly at random amongst all such graphs. Working with  $G(n, m)$  facilitates the second moment argument because the total number of edges is a deterministic quantity. Nonetheless, Lemma 2.1 below shows that any results for  $G(n, m)$  with  $m = \lceil dn/2 \rceil$  extend to  $G(n, d/n)$ . **Thus, throughout the paper we always set  $m = \lceil dn/2 \rceil$ .**

Since our goal is to establish a statement that holds with probability tending to 1 as  $n \rightarrow \infty$ , we are always going to assume tacitly that the number  $n$  of vertices is sufficiently large for the various estimates to hold. Similarly, at the expense of the error term  $o_k(1)$  in Theorem 1.1 we will tacitly assume that  $k \geq k_0$  for a large enough constant  $k_0$ .

We use the standard  $O$ -notation to refer to the limit  $n \rightarrow \infty$ . Thus,  $f(n) = O(g(n))$  means that there exist  $C > 0$ ,  $n_0 > 0$  such that for all  $n > n_0$  we have  $|f(n)| \leq C \cdot |g(n)|$ . In addition, we use the standard symbols  $o(\cdot)$ ,  $\Omega(\cdot)$ ,  $\Theta(\cdot)$ . In particular,  $o(1)$  stands for a term that tends to 0 as  $n \rightarrow \infty$ . Furthermore, we write  $f(n) \sim g(n)$  if  $\lim_{n \rightarrow \infty} f(n)/g(n) = 1$ .

Additionally, we use asymptotic notation in the limit of large  $k$ . To make this explicit, we insert  $k$  as an index. Thus,  $f(k) = O_k(g(k))$  means that there exist  $C > 0$ ,  $k_0 > 0$  such that for all  $k > k_0$  we have  $|f(k)| \leq C \cdot |g(k)|$ . Further, we write  $f(k) = \tilde{O}_k(g(k))$  to indicate that there exist  $C > 0$ ,  $k_0 > 0$  such that for all  $k > k_0$  we have  $|f(k)| \leq (\ln k)^C \cdot |g(k)|$ .

If  $G$  is a graph  $v$  is a vertex of  $G$ , then we denote by  $N_G(v)$  the neighborhood of  $v$  in  $G$ , i.e., the set of all vertices  $w$  that are connected to  $v$  by an edge of  $G$ . Where the graph  $G$  is apparent from the context we just write  $N(v)$ . If  $s \geq 1$  is an integer, we write  $[s]$  for the set  $\{1, 2, \dots, s\}$ . Moreover, throughout the paper we use the conventions that  $0 \ln 0 = 0$  and (consistently) that  $0 \ln \frac{0}{0} = 0$ .

## 2. OUTLINE

In this section we first discuss the second moment method in general and the argument pursued in [6] specifically and investigate why it breaks down beyond the density  $d_{k,AN}$  from (1.1). Then, we see how the physics intuition can be harnessed to overcome this barrier. Finally, we comment on the condensation phase transition.

**2.1. The second moment method.** Suppose that  $Z = Z(G(n, m)) \geq 0$  is a random variable such that  $Z(G) > 0$  implies that  $G$  is  $k$ -colorable. Moreover, suppose that there is a number  $C = C(d, k) > 0$  that may depend on the average degree  $d$  and the number of colors  $k$  but not on  $n$  such that

$$0 < \mathbb{E}[Z^2] \leq C \cdot \mathbb{E}[Z]^2. \quad (2.1)$$

Then the *Paley-Zygmund inequality*

$$\mathbb{P}[Z > 0] \geq \frac{\mathbb{E}[Z]^2}{\mathbb{E}[Z^2]} \quad (2.2)$$

implies that

$$\liminf_{n \rightarrow \infty} \mathbb{P}[G(n, m) \text{ is } k\text{-colorable}] \geq \liminf_{n \rightarrow \infty} \mathbb{P}[Z > 0] \geq (4C)^{-1} > 0.$$

This inequality yields a lower bound on the  $k$ -colorability threshold.

**Lemma 2.1 ([1]).** *If  $d > 0$  is such that  $\liminf_{n \rightarrow \infty} \mathbb{P}[G(n, m) \text{ is } k\text{-colorable}] > 0$ , then  $\liminf_{n \rightarrow \infty} d_{k\text{-col}}(n) \geq d$ .*

Thus, in order to obtain a lower bound on  $d_{k\text{-col}}$ , we need to define an appropriate random variable  $Z$  and verify (2.1). Both of these steps turn out to be non-trivial.

**2.2. Balanced colorings and the Birkhoff polytope.** The most obvious choice of random variable seems to be the total number  $Z_k$  of  $k$ -colorings of  $G(n, m)$ . But to simplify the calculations, we confine ourselves to a particular type of colorings. Namely, a map  $\sigma : [n] \rightarrow [k]$  is **balanced** if  $|\sigma^{-1}(i) - \frac{n}{k}| \leq \sqrt{n}$  for  $i = 1, \dots, k$ . Let  $\mathcal{B} = \mathcal{B}_{n,k}$  denote the set of all balanced maps. Moreover, let  $Z_{k,\text{bal}}$  be the number of balanced  $k$ -colorings of  $G(n, m)$ . This is the random variable that Achlioptas and Naor [6] work with. As it happens, (2.1) does not hold for either  $Z_k$  or  $Z_{k,\text{bal}}$  in the entire range  $0 < d < d_{k,\text{cond}}$ . We need to understand why.

To get started, we compute the first moment. By Stirling's formula the number of balanced maps is  $|\mathcal{B}| = \Theta(k^n)$ . Furthermore, for  $\sigma$  to be a  $k$ -coloring, the random graph  $G(n, m)$  must not contain any of the

$$\mathcal{F}(\sigma) = \sum_{i=1}^k \binom{|\sigma^{-1}(i)|}{2}$$

“forbidden” edges that join two vertices with the same color under  $\sigma$ . If  $\sigma$  is balanced, we easily check that  $\mathcal{F}(\sigma) = (1 - 1/k) \binom{n}{2} + O(n)$ . Thus, letting  $N = \binom{n}{2}$  and using Stirling's formula, we find that the probability that  $\sigma$  is a  $k$ -coloring of  $G(n, m)$  comes to

$$\binom{N - \mathcal{F}(\sigma)}{m} / \binom{N}{m} = \Theta((1 - 1/k)^m).$$

Hence, by the linearity of expectation,

$$\mathbb{E}[Z_{k,\text{bal}}] = \Theta(k^n (1 - 1/k)^{dn/2}). \quad (2.3)$$

Working out the second moment is not quite so easy. Since  $\mathbb{E}[Z_{k,\text{bal}}^2]$  is the expected number of *pairs* of balanced  $k$ -colorings, we need to compute the probability that  $\sigma, \tau \in \mathcal{B}$  *simultaneously* happen to be  $k$ -colorings of  $G(n, m)$ . Of course, this probability depends on how “similar”  $\sigma, \tau$  are. To quantify this, we define the  $k \times k$  **overlap matrix**  $\rho(\sigma, \tau)$  whose entries

$$\rho_{ij}(\sigma, \tau) = \frac{k}{n} \cdot |\sigma^{-1}(i) \cap \tau^{-1}(j)| \quad (i, j = 1, \dots, k) \quad (2.4)$$

represent the proportion of vertices with color  $i$  under  $\sigma$  and color  $j$  under  $\tau$ .

While in *binary* problems the relevant overlap parameter is just a 1-dimensional (e.g., in random  $k$ -SAT, the Hamming distance of two truth assignments), here the high-dimensional overlap matrix is required. The need for this high-dimensional overlap parameter is what makes the  $k$ -colorability problem so difficult.

The upshot is that  $\rho(\sigma, \tau)$  contains all the information necessary to determine the probability that both  $\sigma, \tau$  are  $k$ -colorings. In fact, let  $Z_{\rho,\text{bal}}$  be the number of pairs of balanced  $k$ -colorings with overlap  $\rho$ , and let  $\mathcal{R}$  denote the set of all possible overlap matrices of maps  $\sigma, \tau \in \mathcal{B}$ . For a  $k \times k$  matrix  $\rho$  we denote the Frobenius norm by

$$\|\rho\|_2 = \left( \sum_{i,j=1}^k \rho_{ij}^2 \right)^{1/2}.$$

**Fact 2.2** ([6]). *Uniformly for  $\rho \in \mathcal{R}$  we have*

$$\mathbb{E}[Z_{\rho,\text{bal}}] = O(n^{(1-k^2)/2}) \cdot \exp[n \cdot f(\rho)], \quad \text{where} \quad (2.5)$$

$$f(\rho) = f_{d,k}(\rho) = \ln k - \frac{1}{k} \left[ \sum_{i,j=1}^k \rho_{ij} \ln \rho_{ij} \right] + \frac{d}{2} \ln \left[ 1 - \frac{2}{k} + \frac{1}{k^2} \|\rho\|_2^2 \right].$$

*Proof.* Since the function  $f$  turns out to be the key object in this paper, we include the simple proof to explain where it comes from combinatorially. By Stirling's formula, the total number of  $\sigma, \tau \in \mathcal{B}$  with overlap  $\rho$  equals

$$\binom{n}{\rho_{11} \frac{n}{k}, \dots, \rho_{kk} \frac{n}{k}} = O(n^{(1-k^2)/2}) \cdot \exp \left[ - \sum_{i,j=1}^k n \cdot \frac{\rho_{ij}}{k} \ln \frac{\rho_{ij}}{k} \right]. \quad (2.6)$$

Now, suppose that  $\sigma, \tau$  have overlap  $\rho$ . By inclusion/exclusion, the number of “forbidden” edges joining two vertices with the same color under either  $\sigma$  or  $\tau$  equals

$$\mathcal{F}(\sigma, \tau) = \sum_{i=1}^k \binom{\sum_j \rho_{ij} \frac{n}{k}}{2} + \sum_{j=1}^k \binom{\sum_i \rho_{ij} \frac{n}{k}}{2} - \sum_{i,j=1}^k \binom{\rho_{ij} \frac{n}{k}}{2} \geq 2k \binom{n/k}{2} - \sum_{i,j=1}^k \binom{\rho_{ij} \frac{n}{k}}{2}.$$

Let  $N = \binom{n}{2}$ . Then Stirling's formula yields

$$\mathbb{P}[\sigma, \tau \text{ are } k\text{-colorings of } G(n, m)] = \frac{\binom{N - \mathcal{F}(\sigma, \tau)}{m}}{\binom{N}{m}} = O(1) \cdot \exp \left[ m \left( 1 - \frac{2}{k} + \sum_{i,j=1}^k \left( \frac{\rho_{ij}}{k} \right)^2 \right) \right]. \quad (2.7)$$

The assertion follows from (2.6), (2.7) and the linearity of expectation.  $\square$



The bound (2.5) is essentially tight as similar calculations show that

$$\mathbb{E}[Z_{\rho, \text{bal}}] = \exp(n \cdot f(\rho) + o(n)). \quad (2.8)$$

Moreover, by the linearity of expectation we can express the second moment as

$$\mathbb{E}[Z_{k, \text{bal}}^2] = \sum_{\rho \in \mathcal{R}} \mathbb{E}[Z_{\rho, \text{bal}}]. \quad (2.9)$$

As the total number of summands is  $|\mathcal{R}| \leq n^{k^2}$ , we obtain from (2.8) and (2.9) that

$$\frac{1}{n} \ln \mathbb{E}[Z_{k, \text{bal}}^2] \sim \max_{\rho \in \mathcal{R}} \frac{1}{n} \ln \mathbb{E}[Z_{\rho, \text{bal}}] \sim \max_{\rho \in \mathcal{R}} f(\rho). \quad (2.10)$$

Further, because we work with balanced colorings, the row and column sums of any  $\rho \in \mathcal{R}$  are  $1 + O(n^{-\frac{1}{2}})$ . Thus, let  $\mathcal{D}$  be the set of all doubly-stochastic  $k \times k$  matrices, the **Birkhoff polytope**. Together with the continuity of  $f$  and the observation that  $\mathcal{R} \cap \mathcal{D}$  becomes a dense subset of  $\mathcal{D}$  as  $n \rightarrow \infty$ , (2.10) implies that

$$\frac{1}{n} \ln \mathbb{E}[Z_{k, \text{bal}}^2] \sim \max_{\rho \in \mathcal{D}} f(\rho). \quad (2.11)$$

In summary, following [6], we have transformed the calculation of the second moment into the problem of optimizing  $f$  over the Birkhoff polytope  $\mathcal{D}$ . Let  $\bar{\rho}$  be the matrix with all entries equal to  $\frac{1}{k}$ , the barycenter of  $\mathcal{D}$ . A glimpse at (2.3) reveals that  $f(\bar{\rho}) \sim \frac{2}{n} \ln \mathbb{E}[Z_{k, \text{bal}}]$  corresponds to the square of the first moment. Therefore, a *necessary* condition for the success of the second moment method is that the maximum (2.11) is attained at  $\bar{\rho}$ . Indeed, if  $f(\rho) > f(\bar{\rho})$  for some  $\rho \in \mathcal{D}$ , then  $\mathbb{E}[Z_{k, \text{bal}}^2]$  exceeds  $\mathbb{E}[Z_{k, \text{bal}}]^2$  by an *exponential* factor  $\exp(\Omega(n))$ . It is not difficult to show that this necessary condition is also sufficient. Combinatorially, the condition that  $\bar{\rho}$  is the maximizer of  $f$  indicates that pairs  $\sigma, \tau$  that, judging by their overlap, look completely uncorrelated make up the lion's share of  $\mathbb{E}[Z_{k, \text{bal}}^2]$ .

**2.3. The singly-stochastic bound.** Yet solving the optimization problem (2.11) proves seriously difficult. Achlioptas and Naor resort to a relaxation: with  $\mathcal{S} \supset \mathcal{D}$  the set of all  $k \times k$  *singly* stochastic matrices, they study

$$\max_{\rho \in \mathcal{S}} f(\rho). \quad (2.12)$$

Because  $\mathcal{S}$  is just a product of simplices, (2.12) turns out to be much more amenable than (2.11). Achlioptas and Naor solve (2.12) completely. More precisely, they optimize  $f$  over the sets  $\{\rho \in \mathcal{S} : \|\rho\|_2 = s\}$  for each  $s$ , i.e., over the intersection of  $\mathcal{S}$  with a sphere. Their argument relies on the product structure of  $\mathcal{S}$  and a sophisticated global analysis (going to the *sixth* derivative). The result is that the maximum of (2.12) and therefore also of (2.11) is attained at the doubly-stochastic  $\bar{\rho}$  for  $d \leq d_{k, \text{AN}}$ .

However, for  $d > d_{k, \text{AN}}$ , the maximum (2.12) is attained elsewhere. For instance, the matrix  $\rho_{\text{half}}$  whose first  $k/2$  rows coincide with those of the identity matrix  $\text{id}$  (with ones on the diagonal and zeros elsewhere) and whose last  $k/2$  rows have all entries equal to  $1/k$  yields a larger function value than  $\bar{\rho}$  for  $d > d_{k, \text{AN}} + o_k(1)$ . Of course, this matrix fails to be doubly-stochastic.

Hence, one might hope that  $\bar{\rho}$  remains the maximizer of (2.11) for  $d$  up to  $d_{k, \text{cond}}$ . That is, however, not the case. Indeed, consider the doubly-stochastic

$$\rho_{\text{stable}} = (1 - 1/k)\text{id} + k^{-2}\mathbf{1}, \quad (2.13)$$

where  $\mathbf{1}$  denotes the matrix with all entries equal to one. A simple calculation reveals that  $f(\rho_{\text{stable}}) > f(\bar{\rho})$ , and thus that the second moment argument for  $Z_{k, \text{bal}}$  fails, for  $d$  well below  $d_{k, \text{cond}}$ .

**2.4. A physics-enhanced random variable.** Therefore, to prove Theorem 1.1 we need to work with a different random variable. The key observation behind its definition is that the second moment (2.11) is driven up by certain “wild”  $k$ -colorings  $\sigma$ . Their number behaves like a lottery: while the random graph typically has no wild coloring, a tiny fraction of graphs have an abundance, boosting the second moment. To avoid this heavily-tailed random variable, we define a notion of “tame” colorings. This induces a decomposition  $Z_{k, \text{bal}} = Z_{k, \text{tame}} + Z_{k, \text{wild}}$  such that  $\mathbb{E}[Z_{k, \text{tame}}] \sim \mathbb{E}[Z_{k, \text{bal}}]$ . The second moment bound (2.1) turns out to hold for  $Z_{k, \text{tame}}$  if  $d \leq d_{k, \text{cond}} - o_k(1)$ .

The notion of “tame” is inspired by statistical physics predictions on the geometry of the set of  $k$ -colorings. More precisely, according to the physicists’ cavity method [30, 42], for  $(1 + o_k(1))k \ln k < d < d_{k, \text{cond}}$  the set of all

$k$ -colorings, viewed as a subset of  $[k]^n$ , decomposes into “tiny clusters” that are “well-separated” from each other. Formally, we define the **cluster** of a balanced  $k$ -coloring  $\sigma$  of  $G(n, m)$  as the set

$$\mathcal{C}(\sigma) = \{\tau \in \mathcal{B} : \tau \text{ is a } k\text{-coloring and } \rho_{ii}(\sigma, \tau) > 0.51 \text{ for all } i \in [k]\}. \quad (2.14)$$

In words,  $\mathcal{C}(\sigma)$  contains all balanced  $k$ -colorings  $\tau$  where more than 51% of the vertices in each color class of  $\sigma$  retain their color. According to the cavity method, for  $d < d_{k,\text{cond}}$  each cluster contains only an exponentially small fraction of all  $k$ -colorings of  $G(n, m)$  w.h.p. But for our purposes it suffices to formalize “tiny” by just requiring that  $|\mathcal{C}(\sigma)| \leq \mathbb{E}[Z_k]$ .

Further, to formalize the notion that the clusters are “well-separated”, we call a balanced  $k$ -coloring  $\sigma$  **separable** if for any other balanced  $k$ -coloring  $\tau$  and any  $i, j \in [k]$  such that  $\rho_{ij}(\sigma, \tau) > 0.51$  we indeed have  $\rho_{ij}(\sigma, \tau) \geq 1 - \kappa$ , where  $\kappa = \ln^{20} k/k$ . (2.15)

In other words, the overlap matrix  $\rho(\sigma, \tau)$  does not have entries in the interval  $(0.51, 1 - \kappa)$ . Hence, if two color classes have an overlap of more than 51%, then they must, in fact, be nearly identical. This definition ensures that the clusters of two separable colorings  $\sigma, \tau$  are either disjoint or identical. We thus arrive at the following definition.

**Definition 2.3.** Let  $G$  be a graph with  $n$  vertices and  $m$  edges. A  $k$ -coloring  $\sigma$  of  $G$  is **tame** if

- T1:**  $\sigma$  is balanced,
- T2:**  $\sigma$  is separable, and
- T3:**  $|\mathcal{C}(\sigma)| \leq \mathbb{E}[Z_k(G(n, m))]$ .

In Section 3 we show that a typical  $k$ -coloring of  $G(n, m)$  is indeed tame, which implies that the expected number of tame  $k$ -colorings satisfies the following.

**Proposition 2.4.** There exists a sequence  $\varepsilon_k \rightarrow 0$  such that for  $d = d_{k,\text{cond}} - \varepsilon_k$  we have

$$\mathbb{E}[Z_{k,\text{tame}}] \sim \mathbb{E}[Z_{k,\text{bal}}] = \Theta(\exp(\frac{n}{2} \cdot f(\bar{\rho}))) \quad \text{and} \quad f(\bar{\rho}) = \frac{2 \ln 2}{k} + o_k(k^{-1}) > 0.$$

Thus, going from balanced to tame colorings has no discernible effect on the first moment, which remains exponentially large in  $n$  up to at least  $d = d_{k,\text{cond}} - \varepsilon_k$ .

Working with tame colorings has a substantial impact on the second moment. As before, computing the second moment boils down to a continuous optimization problem. But in comparison to (2.11), this problem is over a *significantly* reduced domain  $\mathcal{D}_{\text{tame}} \subset \mathcal{D}$ . Indeed, let us call a  $k \times k$ -matrix  $\rho$  **separable** if  $\rho_{ij} \notin (0.51, 1 - \kappa)$  for all  $i, j \in [k]$ . Further, call  $\rho$   **$k$ -stable** if for any  $i$  there is  $j$  such that  $\rho_{ij} > 0.51$ . Let  $\mathcal{D}_{\text{tame}}$  be the set of all  $\rho \in \mathcal{D}$  that are separable but not  $k$ -stable. In particular, the matrix  $\rho_{\text{stable}}$  from (2.13) does *not* belong to  $\mathcal{D}_{\text{tame}}$ . Geometrically, one can think of  $\mathcal{D}_{\text{tame}}$  as being obtained by cutting out (huge) cylinders from the Birkhoff polytope. In Section 4 we will see that the second moment calculation for  $Z_{k,\text{tame}}$  boils down to showing that

$$\max_{\rho \in \mathcal{D}_{\text{tame}}} f(\rho) \quad (2.16)$$

is attained at  $\bar{\rho}$ . Indeed, that (2.16) mirrors the second moment calculation seems reasonable: for any two tame colorings  $\sigma, \tau$  the overlap matrix  $\rho(\sigma, \tau)$  is separable by **T2**. Moreover, if  $\rho(\sigma, \tau)$  is  $k$ -stable, then  $\tau \in \mathcal{C}(\sigma)$  by the very definition of  $\mathcal{C}(\sigma)$ , and **T3** provides an *a priori* bound on the number of such  $\tau$ .

Thus, in a sense the proof strategy that we pursue is the opposite of the one from [6]. While Achlioptas and Naor *relax* the optimization problem (by working with a rather significantly larger domain: singly rather than doubly-stochastic matrices), here we *restrict* the domain by imposing further physics-inspired constraints. This approach, carried out in Section 4, yields

**Proposition 2.5.** Assume that  $k$  is sufficiently large and that  $d = (2k - 1) \ln k - c$  for some number  $c = O_k(1)$ . If  $\mathbb{E}[Z_{k,\text{tame}}] = \Omega(\mathbb{E}[Z_{k,\text{bal}}])$ , then  $0 < \mathbb{E}[Z_{k,\text{tame}}^2] \leq C(k) \cdot \mathbb{E}[Z_{k,\text{tame}}]^2$ .

The proof of Proposition 2.5 essentially comes down to showing that the maximum (2.16) is attained at  $\bar{\rho}$ . Even though we work with the reduced domain  $\mathcal{D}_{\text{tame}}$ , this is anything but straightforward. Indeed, to solve this analytical problem, we develop a novel local variations argument based on properties of the entropy function (among other things). We expect that this argument will prove useful to tackle many related optimisation problems that come up in second moment arguments.

Finally, Theorem 1.1 is an immediate consequence of Propositions 2.4 and 2.5 combined with Lemma 2.1.

**2.5. The condensation phase transition.** Finally, what would it take to close the (small) remaining gap between the new lower bound (1.4) on  $d_{k-\text{col}}$  and the upper bound (1.3)? According to the physicists' cavity method, this gap is due to a further phase transition, the so-called *condensation* or *Kauzmann transition*, that occurs at  $d_{k,\text{cond}} + o_k(1)$ , i.e., the lower bound established in Theorem 1.1. In fact, the existence and precise location of this phase transition (including the term hidden in the  $o_k(1)$ ) can be established rigorously [10].

According to the cavity method [30], the geometry of the set of  $k$ -colorings changes significantly at  $d_{k,\text{cond}}$ . More precisely, for  $d < d_{k,\text{cond}} - o_k(1)$  the set of  $k$ -colorings decomposes into clusters that each contain only an exponentially small fraction of all  $k$ -colorings of  $G(n, d/n)$  w.h.p. By contrast, for  $d > d_{k,\text{cond}} + o_k(1)$ , the size of the largest cluster is conjectured to contain a *constant* fraction of all  $k$ -colorings. As a result, two random  $k$ -colorings are heavily correlated, as there is a non-vanishing probability that they belong to the same cluster. This explains intuitively why the condensation threshold poses an obstacle to the second moment method, as we saw that a necessary condition for the success of the second moment method is that random pairs of  $k$ -colorings decorrelate.

More formally, we prove in [10] that for  $d > d_{k,\text{cond}} + o_k(1)$  there does not exist a random variable  $Z = Z(G(n, m))$  with the following properties. First,  $Z(G) > 0$  only if  $G$  is  $k$ -colorable. Second,

$$\mathbb{E}[Z(G(n, m))]^{1/n} \sim k(1 - 1/k)^{d/2} \quad \text{and} \quad \mathbb{E}[Z(G(n, m))^2] \leq O(\mathbb{E}[Z(G(n, m))]^2).$$

By contrast, Propositions 2.4 and 2.5 show that  $Z_{k,\text{tame}}$  has these two properties if  $d < d_{k,\text{cond}} - o_k(1)$ . Hence, in this sense the approach (and random variable) put forward in the present paper is best possible.

A refined version of the cavity method, the so-called *1-step replica symmetry breaking* (“*1RSB*”) *ansatz* [30, 31, 38, 42], yields a precise prediction as to the value of  $d_{k-\text{col}} = \lim_{n \rightarrow \infty} d_{k-\text{col}}(n)$  (of course, the existence of the limit is taken for granted in the physics work). However, this prediction is not explicit; for instance, it involves the solution to a seriously complicated fixed point problem on the set of probability distributions on the  $k + 1$ -simplex. Yet it is possible to obtain an expansion in the limit of large  $k$ , according to which  $d_{k-\text{col}} = 2k \ln k - \ln k - 1 + o_k(1)$ . Proving the 1RSB prediction for  $d_{k-\text{col}}$  remains an open problem. In a very few binary problems, asymptotic versions of the 1RSB prediction have been proved rigorously (e.g., [16]). However, it seems anything but straightforward to extend these arguments to the random graph coloring problem. That said, we expect that any attempt at determining  $d_{k-\text{col}}$  precisely would have to build upon the insights gained in this paper and very possibly its techniques.

### 3. THE FIRST MOMENT

*Throughout this section we keep the assumptions of Proposition 2.4 and the notation introduced in Section 2.*

The following lemma is the key step towards proving Proposition 2.4.

**Lemma 3.1.** *There exists a sequence  $\varepsilon_k \rightarrow 0$  such that for  $d = d_{k,\text{cond}} - \varepsilon_k$  we have*

$$\begin{aligned} \mathbb{P}[\sigma \text{ is tame} | \sigma \text{ is a } k\text{-coloring of } G(n, m)] &\sim 1 \text{ for any } \sigma \in \mathcal{B} \quad \text{and} \\ f(\bar{\rho}) &= 2 \ln k + d \ln(1 - 1/k) = \frac{2 \ln 2}{k} + o_k(k^{-1}) > 0. \end{aligned}$$

In fact, once we have Lemma 3.1, Proposition 2.4 readily follows from the linearity of expectation, Bayes' formula and the formula (2.3) for  $\mathbb{E}[Z_{k,\text{bal}}]$ .

To establish Lemma 3.1, we denote by  $G(n, m, \sigma)$  the random graph  $G(n, m)$  conditional on the event that  $\sigma \in \mathcal{B}$  is a  $k$ -coloring. Thus,  $G(n, m, \sigma)$  consists of  $m$  edges drawn uniformly at random without replacement out of those edges that are bichromatic under  $\sigma$ . This probability distribution is also known as the “planted model”.

To establish the bound **T3** on the cluster size, we show that w.h.p.  $G(n, m, \sigma)$  contains a vast “core” comprising of vertices that have several neighbors of each color other than their own that also belong to the core. Formally, if  $G = (V, E)$  is a graph on the vertex set  $V = \{1, \dots, n\}$  and  $\sigma \in \mathcal{B}$ , we define the *core* of  $(G, \sigma)$  as the largest subset  $V' \subset V$  such that

$$|\{w \in N(v) \cap V' : \sigma(w) = i\}| \geq 100 \quad \text{for all } v \in V' \text{ and all } i \neq \sigma(v). \quad (3.1)$$

The core is well-defined: if  $V', V''$  satisfy (3.1), then so does  $V' \cup V''$ . (Of course, the constant 100 is a bit arbitrary.)



As we will see, due to expansion properties no vertex in the core of  $G(n, m, \sigma)$  can be recolored without leaving the cluster  $\mathcal{C}(\sigma)$  w.h.p. The basic reason is that recoloring any vertex  $v$  in the core sets off an avalanche of recolorings: to give  $v$  another color, we will have to recolor at least 100 vertices that also belong to the core, and so on.

In addition, if a vertex  $v$  outside the core is such that for each color other than its own,  $v$  has a neighbor in the core of that color, then it should be impossible to recolor  $v$  without leaving  $\mathcal{C}(\sigma)$  as well. For to assign  $v$  some color  $i \neq \sigma(v)$  we will have to recolor at least one vertex in the core. Guided by this observation, we call a vertex  $v$   **$\sigma$ -complete**, if for each color  $i \neq \sigma(v)$ ,  $v$  has a neighbor  $w$  in the core with  $\sigma(w) = i$ .

If  $\sigma$ -complete vertices do not contribute to  $|\mathcal{C}(\sigma)|$ , then the cluster size stems from recoloring vertices  $v$  that fail to have a neighbor in the core of some color  $i \neq \sigma(v)$ . As we shall see, most of these vertices miss out on exactly one color  $i \neq \sigma(v)$  and hence have precisely two colors to choose from. Formally, we call a vertex  $v$   **$a$ -free** in  $(G, \sigma)$  if, with  $V'$  denoting the core, we have  $|\{i \in [k] : N(v) \cap V' \cap \sigma^{-1}(i) = \emptyset\}| \geq a + 1$ .

The following lemma summarizes the expansion properties of  $G(n, m, \sigma)$  that the proof of Lemma 3.1 builds upon.

**Lemma 3.2.** *Let  $\sigma \in \mathcal{B}$  and assume that  $2k \ln k - \ln k - 2 \leq d \leq 2k \ln k$ . Let  $V_i = \sigma^{-1}(i)$  for  $i = 1, \dots, k$ . Then w.h.p. the random graph  $G(n, m, \sigma)$  has the following four properties.*

- P1:** *Let  $i \in [k]$ . For any subset  $S \subset V_i$  of size  $0.509 \cdot \frac{n}{k} \leq |S| \leq (1 - k^{-0.499}) \frac{n}{k}$ , the number of vertices  $v \in V \setminus V_i$  that do not have a neighbor in  $S$  is less than  $\frac{n}{k} - |S| - n^{2/3}$ .*
- P2:** *Let  $i \in [k]$ . No more than  $\frac{\kappa n}{3k}$  vertices  $v \notin V_i$  have less than 15 neighbors in  $V_i$ , where  $\kappa = \ln^{20} k/k$ .*
- P3:** *There is no set  $S \subset V$  of size  $|S| \leq k^{-4/3}n$  that spans more than  $5|S|$  edges.*
- P4:** *At most  $\frac{n}{k}(1 + \tilde{O}_k(1/k))$  vertices are 1-free, and at most  $\tilde{O}_k(k^{-2})n$  vertices are 2-free.*

The proof of Lemma 3.2 is based on arguments that are, by now, fairly standard; in particular, the “core” has, tweaked in various ways, become a standard tool [2, 7, 13, 37]. For the sake of completeness, we give a full proof of Lemma 3.2 in Appendix A. Here we proceed to show how Lemma 3.2 implies Lemma 3.1.

**Lemma 3.3.** *Assume that  $2k \ln k - \ln k - 2 \leq d \leq 2k \ln k$  and let  $\sigma \in \mathcal{B}$ . Then  $\sigma$  is separable in  $G(n, m, \sigma)$  w.h.p.*

*Proof.* By Lemma 3.2 we may assume that the random graph  $G(n, m, \sigma)$  has the properties **P1–P3**. Suppose that  $\tau \in \mathcal{B}$  is another  $k$ -coloring of this random graph and that  $i, j \in [k]$  are such that  $\rho_{ij}(\sigma, \tau) \geq 0.51$ . Our aim is to show that  $\rho_{ij}(\sigma, \tau) > 1 - \kappa$ . Without loss of generality we may assume that  $i = j = 1$ .

Let  $R = \sigma^{-1}(1) \setminus \tau^{-1}(1)$ ,  $S = \tau^{-1}(1) \cap \sigma^{-1}(1)$  and  $T = \tau^{-1}(1) \setminus \sigma^{-1}(1)$ . Because  $\tau$  is a  $k$ -coloring, none of the vertices in  $T$  has a neighbor in  $S$ . Furthermore, because  $\tau$  is balanced we have  $|S \cup T| \geq \frac{n}{k} - \sqrt{n}$ , and thus  $|T| \geq \frac{n}{k} - |S| - \sqrt{n}$ . Since  $|S| = \frac{n}{k} \rho_{11}(\sigma, \tau) > 0.509 \frac{n}{k}$ , **P1** implies that

$$|S| \geq (1 - k^{-0.49}) \frac{n}{k}. \quad (3.2)$$

Now, let  $U$  be the set of all  $v \in T$  that have at least 15 neighbors in  $\sigma^{-1}(1)$ . Then all of these neighbors lie in  $R$ , because  $\tau$  is a  $k$ -coloring. Further, as  $\sigma, \tau$  are asymptotically balanced we obtain from (3.2)

$$|R \cup U| \leq |\sigma^{-1}(1)| - |S| + |T| \leq 2 \left( \frac{n}{k^{1.49}} + \sqrt{n} \right) \leq n/k^{4/3}.$$

Hence, **P3** applies to  $R \cup U$ . By the definition of  $U$  and **P3**, the number  $e(R \cup U)$  of edges spanned by  $R \cup U$  satisfies

$$15|U| \leq e(R \cup U) \leq 5|R \cup U|, \quad \text{whence } |U| \leq |R|/2. \quad (3.3)$$

Let  $W = T \setminus U$ . Because  $W$  consists of vertices with fewer than 15 neighbors in  $\sigma^{-1}(1)$ , **P2** yields

$$|W| \leq \frac{\kappa n}{3k}. \quad (3.4)$$

Since  $\sigma, \tau$  are balanced, we have

$$|S| + |R| = |\sigma^{-1}(1)| \sim \frac{n}{k} \sim |\tau^{-1}(1)| = |S| + |U| + |W|. \quad (3.5)$$

Hence, by (3.3) and (3.4)

$$|R| = |U| + |W| + o(n) \leq \frac{|R|}{2} + |W| + o(n) \leq \frac{|R|}{2} + \frac{\kappa n}{3k} + o(n), \quad \text{whence } |R| \leq \frac{2\kappa n}{3k} + o(n). \quad (3.6)$$

Finally, (3.5) and (3.6) imply that  $\rho_{11}(\sigma, \tau) = \frac{k}{n} \cdot |S| = 1 + o(1) - \frac{k}{n} \cdot |R| > 1 - \kappa$ , as desired.  $\square$

As a next step, we are going to verify that the  $\sigma$ -complete vertices take the same color in all the colorings in  $\mathcal{C}(\sigma)$  w.h.p.; a similar argument was used in [2].

**Lemma 3.4.** *Assume that  $2k \ln k - \ln k - 2 \leq d \leq 2k \ln k$  and let  $\sigma \in \mathcal{B}$ . W.h.p. the random graph  $G(n, m, \sigma)$  has the following property.*

*If  $\tau \in \mathcal{C}(\sigma)$ , then for all  $\sigma$ -complete vertices  $v$  we have  $\sigma(v) = \tau(v)$  w.h.p.*

*Proof.* By Lemmas 3.2 and 3.3 we may assume that **P3** holds and that  $\sigma$  is separable in  $G(n, m, \sigma)$ . Let  $V'$  be the core of this random graph. Moreover, set

$$\Delta_i^+ = \{v \in V' : \tau(v) = i \neq \sigma(v)\}, \quad \Delta_i^- = \{v \in V' : \tau(v) \neq i = \sigma(v)\} \quad \text{for } i \in [k], \text{ so that}$$

$$\sum_{i=1}^k |\Delta_i^+| = |\{v \in V' : \sigma(v) \neq \tau(v)\}| = \sum_{i=1}^k |\Delta_i^-|. \quad (3.7)$$

The assumptions that  $\sigma$  is separable and that both  $\sigma, \tau$  are asymptotically balanced imply that

$$\max_{i \in [k]} |\Delta_i^+| \leq (\kappa + o(1)) \frac{n}{k}, \quad \max_{i \in [k]} |\Delta_i^-| \leq (\kappa + o(1)) \frac{n}{k}. \quad (3.8)$$

We are going to show that

$$\{v \in V' : \sigma(v) \neq \tau(v)\} = \emptyset. \quad (3.9)$$

By construction, this implies that  $\sigma(v) = \tau(v)$  for all  $\sigma$ -complete vertices.

To establish (3.9), let  $S_i = \Delta_i^+ \cup \Delta_i^-$  for  $i = 1, \dots, k$ . Because  $\Delta_i^+$  is contained in the core, each  $v \in \Delta_i^+$  has at least 100 neighbors in  $\sigma^{-1}(i)$ . Since  $\tau$  is a  $k$ -coloring, all of these neighbors lie in the set  $\Delta_i^-$ . Hence, the number  $e(S_i)$  of edges spanned by  $S_i$  is at least  $100|\Delta_i^+|$ . On the other hand, (3.8) implies that  $|S_i| \leq k^{-4/3}n$  for all  $i$ . Therefore, **P3** entails that  $e(S_i) \leq 5|S_i|$  for all  $i$ . Thus, we obtain  $100|\Delta_i^+| \leq e(S_i) \leq 5|S_i| \leq 5(|\Delta_i^+| + |\Delta_i^-|)$ . Consequently,  $|\Delta_i^-| \geq 2|\Delta_i^+|$  for all  $i$ . Thus, (3.7) shows that  $\Delta_i^+ = \Delta_i^- = \emptyset$  for all  $i$ , whence (3.9) follows.  $\square$

*Proof of Lemma 3.1.* Let  $\sigma \in \mathcal{B}$ . We need to show that  $G(n, m, \sigma)$  enjoys the properties **T2–T3** from Definition 2.3 w.h.p. The fact that **T2** holds w.h.p. follows directly from Lemma 3.3.

With respect to **T3**, by Lemma 3.4 we may assume that for all  $\sigma$ -complete  $v$  and all  $\tau \in \mathcal{C}(\sigma)$  we have  $\tau(v) = \sigma(v)$ . Let  $F_j$  be the set of  $j$ -free vertices for  $j = 1, 2$ . By Lemma 3.2 we may assume that

$$|F_1| \leq \frac{n}{k}(1 + \tilde{O}_k(1/k)), \quad |F_2| \leq \tilde{O}_k(k^{-2})n. \quad (3.10)$$

By construction, for any vertex  $v \in F_1 \setminus F_2$  there is a set  $C_v \subset [k]$  of at most two colors such that  $\tau(v) \in C_v$  for all  $\tau \in \mathcal{C}(\sigma)$ . Hence,

$$|\mathcal{C}(\sigma)| \leq 2^{F_1 \setminus F_2} \cdot k^{F_2}. \quad (3.11)$$

Combining (3.10) and (3.11), we see that w.h.p. in  $G(n, m, \sigma)$ ,

$$\frac{1}{n} \ln \mathcal{C}(\sigma) \leq \frac{\ln 2}{k} + \tilde{O}_k(k^{-2}). \quad (3.12)$$

We need to compare the r.h.s. of (3.12) with  $\frac{1}{n} \ln \mathbb{E}[Z_{k, \text{bal}}]$ . By (2.3) and Taylor expansion,

$$\frac{1}{n} \ln \mathbb{E}[Z_{k, \text{bal}}] = \ln k + \frac{d}{2} \ln(1 - 1/k) = \ln k - \frac{d}{2} \left( \frac{1}{k} + \frac{1}{2k^2} + O_k(k^{-3}) \right).$$

Writing  $d = d_{k, \text{cond}} - \varepsilon_k = 2k \ln k - \ln k - 2 \ln 2 - \varepsilon_k$ , we obtain

$$\frac{1}{n} \ln \mathbb{E}[Z_{k, \text{bal}}] = \ln k + \frac{d}{2} \ln(1 - 1/k) = \ln k - \frac{d}{2} \left( \frac{1}{k} + \frac{1}{2k^2} + O_k(k^{-3}) \right) = \frac{\varepsilon_k + \ln 2}{k} + O_k\left(\frac{\ln k}{k^2}\right). \quad (3.13)$$

Letting, say,  $\varepsilon_k = \Theta_k(k^{-1/2})$ , we obtain from (3.12) and (3.13) that  $|\mathcal{C}(\sigma)| \leq \mathbb{E}[Z_{k, \text{bal}}]$  w.h.p. Hence, **T3** holds in  $G(n, m, \sigma)$  w.h.p.

Finally, upon direct inspection we find  $f(\bar{\rho}) = 2 \ln k + d \ln(1 - 1/k)$ . Thus, (3.13) shows that for  $d = d_{k, \text{cond}} - \varepsilon_k = 2k \ln k - \ln k - 2 \ln 2 - \varepsilon_k$  we have  $k \cdot f(\bar{\rho}) = 2 \ln 2 + o_k(1) > 0$ , as claimed.  $\square$

## 4. THE SECOND MOMENT

In this section we keep the assumptions of Proposition 2.5 and the notation introduced in Section 2.

**4.1. Overview.** The goal is to prove Proposition 2.5. As we already hinted at in Section 2, this boils down to maximizing  $f(\rho)$  over  $\rho \in \mathcal{D}_{\text{tame}}$ . Formally, we have

**Proposition 4.1.** *If  $f(\rho) < f(\bar{\rho})$  for any  $\rho \in \mathcal{D}_{\text{tame}} \setminus \{\bar{\rho}\}$ , then  $\mathbb{E}[Z_{k,\text{tame}}^2] \leq O(\mathbb{E}[Z_{k,\text{tame}}]^2)$ .*

The proof of Proposition 4.1, based on the Laplace method, is a mere technical exercise, which we put off to Section 5.

Proposition 4.1 reduces the second moment argument to a problem in analysis. Indeed, neither the function  $f$  nor the domain  $\mathcal{D}_{\text{tame}}$  over which we need to maximize are dependent on  $n$  (though both involve the parameters  $d$  and  $k$ ). In the following, we aim to establish

**Proposition 4.2.** *If  $\rho \in \mathcal{D}_{\text{tame}} \setminus \{\bar{\rho}\}$ , then  $f(\rho) < f(\bar{\rho})$ .*

Thus, Proposition 2.5 is immediate from Propositions 4.1 and 4.2.

The proof of Proposition 4.2 is the heart of the second moment argument. Of course, we need to take a closer look at the function  $f$ . As we will see, it consists of two ingredients: an entropy term and a probability term. More specifically, suppose that  $p : \Omega \rightarrow [0, 1]$  is a probability distribution on a finite set  $\Omega$  (i.e.,  $\sum_{x \in \Omega} p(x) = 1$ ). Recalling our convention that  $0 \ln 0 = 0$ , we denote by

$$H(p) = - \sum_{x \in \Omega} p(x) \ln p(x)$$

the *entropy* of  $p$ . Since any  $\rho \in \mathcal{D}$  satisfies  $\sum_{i,j} \rho_{ij} = k$ , we can view  $k^{-1}\rho$  as a probability distribution on  $[k] \times [k]$ . Hence, we can write

$$f(\rho) = H(k^{-1}\rho) + E(\rho), \quad \text{with} \quad E(\rho) = \frac{d}{2} \cdot \ln \left( 1 - \frac{2}{k} + \frac{\|\rho\|_2^2}{k^2} \right).$$

Combinatorially,  $E(\rho)$  corresponds to the (logarithm of the) probability that  $\sigma, \tau \in \mathcal{B}$  with overlap  $\rho$  simultaneously happen to be  $k$ -colorings, cf. the proof of Fact 2.2.

It is clear that the entropy is *maximized* at the barycentre  $\bar{\rho}$  of the Birkhoff polytope, because  $k^{-1}\bar{\rho}$  is the uniform distribution on  $[k] \times [k]$ . Furthermore, among all the matrices  $\rho$  with non-negative entries that sum to  $k$ ,  $\bar{\rho}$  is the one that *minimizes* the Frobenius norm and hence  $E(\rho)$ . This shows that  $\bar{\rho}$  is a stationary point of  $f(\rho)$ . But how do we prove that  $\bar{\rho}$  is the global maximizer of  $f$ ?

The domain  $\mathcal{D}_{\text{tame}}$  admits a natural decomposition into several subsets. Let us call  $\rho \in \mathcal{D}$   *$s$ -stable* if the matrix has precisely  $s$  entries that are greater than 0.51. Let  $\mathcal{D}_{s,\text{tame}}$  denote the set of all  $s$ -stable  $\rho \in \mathcal{D}_{\text{tame}}$ . Geometrically, any  $\rho \in \mathcal{D}_{s,\text{tame}}$  is close to a  $k - s$ -dimensional face of the Birkhoff polytope. For if  $\rho$  has  $s$  entries greater than 0.51, then by separability these entries are in fact at least  $1 - \kappa$  (with  $\kappa = \ln^{20} k/k$  as in (2.15)). Hence,  $\rho$  is close to the face where these  $s$  entries are equal to 1. Indeed, as all other entries of  $\rho$  are smaller than 0.51,  $\rho$  is near a point “deep inside” that face. Consequently, for any  $1 \leq s < k$  the set  $\mathcal{D}_{s,\text{tame}}$  is disconnected: it consists of many tiny “splinters” near the  $k - s$ -dimensional faces of  $\mathcal{D}$ . Each of these splinters can be mapped to the component where  $\rho_{11}, \dots, \rho_{ss} > 0.51$  by permuting the rows and columns suitably, which does not affect the function  $f$ .

In the following, we are going to optimize  $f$  separately over  $\mathcal{D}_{s,\text{tame}}$  for each  $0 \leq s < k$ . We are going to argue that for each  $s$ , the point  $\bar{\rho}_{s\text{-stable}}$  whose first  $s$  diagonal entries are 1 and whose  $(i, j)$ -entries are equal to  $(k - s)^{-1}$  for  $i, j > s$  comes close to maximizing  $f$  over  $\mathcal{D}_{s,\text{tame}}$  (up to a negligible error term in each case). Geometrically,  $\bar{\rho}_{s\text{-stable}}$  is the centre of the face defined by  $\rho_{11} = \dots = \rho_{ss} = 1$ . Furthermore, in the case  $s = 0$  we have  $\bar{\rho}_{s\text{-stable}} = \bar{\rho}$ , and we will see that the maximum over  $\mathcal{D}_{0,\text{tame}}$  is attained at this very point.

We start by showing that we may confine ourselves to matrices without an entry in the interval  $(0.15, 1 - \kappa)$ . Recall that  $\mathcal{S}$  is the set of all singly-stochastic  $k \times k$ -matrices.

**Proposition 4.3.** *For all  $\rho \in \mathcal{S}$  such that  $\rho_{ij} \in [0.15, 0.51]$  for some  $(i, j) \in [k] \times [k]$  we have  $f(\rho) < 0$ .*

We will see shortly how Proposition 4.3 implies that  $\bar{\rho}$  is the maximizer of  $f$  over  $\mathcal{D}_{0,\text{tame}}$ . In addition, there are three different ranges of  $1 \leq s < k$  that we deal with separately.

**Proposition 4.4.** Suppose that  $1 \leq s \leq k^{0.999}$ . Then for all  $\rho \in \mathcal{D}_{s,\text{tame}}$  we have  $f(\rho) < f(\bar{\rho})$ .

**Proposition 4.5.** Suppose that  $k^{0.999} < s < k - k^{0.49}$ . Then for all  $\rho \in \mathcal{D}_{s,\text{tame}}$  we have  $f(\rho) < f(\bar{\rho})$ .

**Proposition 4.6.** Suppose that  $k - k^{0.49} \leq s < k$ . Then for all  $\rho \in \mathcal{D}_{s,\text{tame}}$  we have  $f(\rho) < f(\bar{\rho})$ .

The proofs of Propositions 4.3 and 4.4–4.5 are based on a local variations argument. Roughly speaking, we are going to argue that if  $\rho \in \mathcal{D}_{s,\text{tame}}$  is “far” from  $\bar{\rho}_{s\text{-stable}}$ , then a higher function value can be attained by moving slightly in the direction of  $\bar{\rho}_{s\text{-stable}}$ . We expect that this argument can be adapted to perform second moment arguments in other problems in probabilistic combinatorics. Indeed, in such arguments the function that needs to be optimized is typically similar in nature to our  $f$ : an entropy term maximised at  $\bar{\rho}$  plus a probability term minimized at  $\bar{\rho}$ .

More precisely, the following fact is the cornerstone of the local variations argument. Let  $\rho \in \mathcal{S}$ , let  $i \in [k]$  be a row index, and let  $\emptyset \neq J \subset [k]$  be a set of column indices. Obtain  $\hat{\rho} \in \mathcal{S}$  from  $\rho$  by letting

$$\hat{\rho}_{ab} = \rho_{ab} \text{ for all } (a, b) \notin \{i\} \times J \text{ and } \hat{\rho}_{ib} = \frac{1}{|J|} \sum_{j \in J} \rho_{ij} \text{ for all } b \in J. \quad (4.1)$$

That is,  $\hat{\rho}$  is obtained by redistributing in row  $i$  the total mass of the columns in  $J$  equally over these columns. Clearly, the entropy satisfies  $H(k^{-1}\hat{\rho}) \geq H(k^{-1}\rho)$ . In fact, this inequality is strict unless  $\hat{\rho} = \rho$ . However, it may well be that for the probability term we have  $E(\hat{\rho}) < E(\rho)$ . The following proposition trades the increase in entropy against the drop in the probability term and shows that  $f(\hat{\rho}) \geq f(\rho)$  if  $J$  is “not too small” and  $\max_{j \in J} \rho_{ij}$  is “not too big”.

**Proposition 4.7.** Suppose that  $\rho \in \mathcal{S}$ . Let  $i \in [k]$  and  $J \subset [k]$  be such that for some number  $3 \ln \ln k / \ln k \leq \lambda \leq 1$  we have  $|J| \geq k^\lambda$ . Moreover, assume that  $\max_{j \in J} \rho_{ij} < \lambda/2 - \ln \ln k / \ln k$ . Then the matrix  $\hat{\rho}$  from (4.1) satisfies  $f(\hat{\rho}) \geq f(\rho)$ . In fact, if  $\rho \neq \hat{\rho}$ , then  $f(\hat{\rho}) > f(\rho)$ .

Let us illustrate the use of Proposition 4.7 by proving

**Corollary 4.8.** If  $\rho \in \mathcal{D}_{0,\text{tame}} \setminus \{\bar{\rho}\}$ , then  $f(\rho) < f(\bar{\rho})$ .

*Proof.* Let  $\rho \in \mathcal{D}_{0,\text{tame}}$ . Then  $\rho_{ij} \leq 0.51$  for all  $i, j$  (as  $\rho$  is 0-stable). In fact, if there are  $i, j$  such that  $\rho_{ij} > 0.15$ , then Proposition 4.3 implies that  $f(\rho) < 0$ , while  $f(\bar{\rho}) > 0$  by Proposition 2.4. Hence, we may assume that  $\rho_{ij} \leq 0.15$  for all  $i, j$ . Let  $\rho[l]$  be the matrix whose first  $l$  rows are identical to those of  $\bar{\rho}$ , and whose last  $k - l$  rows are identical to those of  $\rho$ . Thus,  $\rho[0] = \rho$  and  $\rho[k] = \bar{\rho}$ . We claim that

$$f(\rho[i - 1]) \leq f(\rho[i]) \quad \text{for all } i = 1, \dots, k. \quad (4.2)$$

To obtain (4.2), we apply Proposition 4.7 to the  $i$ th row of  $\rho[i - 1]$  with  $J = [k]$  and  $\lambda = 1$ . This is possible because  $\max_j \rho_{ij}[i - 1] = \max_j \rho_{ij} \leq 0.15$ . The resulting matrix  $\hat{\rho}$  is precisely  $\rho[i]$ . Thus, (4.2) follows from Proposition 4.7. Indeed, Proposition 4.7 shows that one of the inequalities (4.2) is strict (as  $\rho \neq \bar{\rho}$ ). Hence,  $f(\rho) < f(\bar{\rho})$ .  $\square$

Proposition 4.2 is immediate from Propositions 4.4–4.6 and Corollary 4.8. Thus, we are left to prove Propositions 4.3–4.7. In the Section 4.3 we prove Proposition 4.7. Building upon that estimate, we then proceed to prove Propositions 4.3–4.6. But before we start, we introduce a few pieces of notation and some basic facts.

**4.2. Preliminaries.** For  $x \in \mathbb{R}$  we denote by  $\text{sign}(x) \in \{-1, 0, 1\}$  the sign of  $x$ . Moreover, if  $\rho$  is matrix, then  $\rho_i$  denotes the  $i$ th row of  $\rho$  and  $\rho_{ij}$  the  $j$ th entry of  $\rho_i$ . We let  $\|\rho\|_\infty = \max_{i,j} |\rho_{ij}|$ . Further,

$$h : [0, 1] \rightarrow \mathbb{R}_{\geq 0}, \quad z \mapsto -z \ln z - (1 - z) \ln(1 - z)$$

denotes the entropy function. We recall the elementary inequality  $h(z) \leq z(1 - \ln z)$ . In addition, we note that

$$\max_{0 < z < 1} h(z) - z \ln k \leq 1/k. \quad (4.3)$$

Indeed, we have  $h(z) - z \ln k \leq z(1 - \ln z - \ln k)$  and differentiating twice, we see that  $z \mapsto z(1 - \ln z - \ln k)$  takes its global maximum  $1/k$  at  $z = 1/k$ .

We need the following well-known fact about the entropy.

**Fact 4.9.** Let  $p \in [0, 1]^k$  be such that  $\sum_{i=1}^k p_i = 1$ . Then  $H(p) \geq 0$  and the following two statements hold.

**H1:** If  $p$  is supported on a set of size  $s$ , then  $H(p) \leq \ln s$ .

**H2:** Let  $\mathcal{I} \subset [k]$  and suppose that  $q = \sum_{i \in \mathcal{I}} p_i \in (0, 1)$ . Let  $p^\mathcal{I}$  be the vector with entries

$$p_i^\mathcal{I} = p_i \cdot \mathbf{1}_{i \in \mathcal{I}} \quad \text{for } i \in [k].$$

$$\text{Then } H(p) = h(q) + qH(q^{-1}p^\mathcal{I}) + (1-q)H((1-q)^{-1}(p - p^\mathcal{I})).$$

As an immediate consequence of Fact 4.9, we have

**Corollary 4.10.** Let  $p \in [0, 1]^k$  be such that  $\sum_{i=1}^k p_i = 1$ .

- (i) Let  $\mathcal{I} \subset [k]$  and set  $q = \sum_{i \in \mathcal{I}} p_i$ . Then  $H(p) \leq h(q) + q \ln |\mathcal{I}| + (1-q) \ln(k - |\mathcal{I}|)$ .
- (ii) Let  $\mathcal{I} \subset \{2, \dots, k\}$  be a set of size  $0 < |\mathcal{I}| < k - 1$ . Set  $q = \sum_{i \in \mathcal{I}} p_i$ . If  $p_1 < 1$ , then

$$H(p) \leq h(p_1) + (1 - p_1)h(q/(1 - p_1)) + q \ln(|\mathcal{I}|) + (1 - q - p_1) \ln(k - |\mathcal{I}| - 1).$$

*Proof.* The first claim follows simply by first using **H2** and then applying **H1** to  $q^{-1}p^\mathcal{I}$  and  $(1-q)^{-1}(p - p^\mathcal{I})$ . To obtain the second assertion, use **H2** with  $\mathcal{I} = \{1\}$  and then apply (i) to the probability distribution  $q^{-1}p^\mathcal{I}$ .  $\square$

Let  $\rho \in \mathcal{S}$  be a singly-stochastic matrix. We can view each row  $\rho_i$  as a probability distribution on  $[k]$ . With this interpretation, we see that

$$H(k^{-1}\rho) = \ln k + \frac{1}{k} \sum_{i=1}^k H(\rho_i). \quad (4.4)$$

To facilitate the following calculations, we note that

$$\frac{\partial}{\partial p} - p \ln p = -1 - \ln p. \quad (4.5)$$

Moreover, differentiating  $E(\rho)$  by  $y = \|\rho\|_2^2$  and recalling that  $d = 2k \ln k + O_k(\ln k)$ , we obtain

$$\frac{\partial}{\partial y} \frac{d}{2} \ln(1 - 2/k + y/k^2) = \frac{d}{2k^2(1 - 2/k + y/k^2)} = \frac{\ln k}{k} (1 + \tilde{O}_k(1/k)). \quad (4.6)$$

Further, using the expansion  $\ln(1+z) = z + z^2/2 + O(z^3)$ , we obtain the approximation

$$E(\rho) = \frac{d}{2k^2} \left[ -2k + \|\rho\|_2^2 - 2 \left( 1 - \frac{\|\rho\|_2^2}{2k} \right)^2 \right] + o_k(1/k). \quad (4.7)$$

Finally, we calculate the function values  $f(\bar{\rho}_{s\text{-stable}})$  explicitly; recall that  $\bar{\rho}_{s\text{-stable}}$  is the barycentre of the face of  $\mathcal{D}$  defined by the equations  $\rho_{11} = \dots = \rho_{ss} = 1$ . Let  $1 \leq s \leq k - 1$ . The first  $s$  rows of  $\bar{\rho}_{s\text{-stable}}$  have entropy 0, while the last  $k - s$  rows have entropy  $\ln(k - s)$ . Hence, (4.4) yields

$$H(k^{-1}\bar{\rho}_{s\text{-stable}}) = \ln k + \frac{k-s}{k} \ln(k-s) = 2 \ln k + (1 - s/k) \ln(1 - s/k) - \frac{s}{k} \ln k. \quad (4.8)$$

Moreover,  $\|\bar{\rho}_{s\text{-stable}}\|_2^2 = s + 1$ . Thus, using (4.7) and plugging in  $d = 2k \ln k - \ln k - c$  for some bounded  $c$ , we get

$$\begin{aligned} E(\bar{\rho}_{s\text{-stable}}) &= \frac{d}{2k^2} \left[ -2k + s + 1 - 2 \left( 1 - \frac{s+1}{2k} \right)^2 \right] + o_k(1/k) \\ &= -2 \ln k + \frac{c}{k} + \frac{s \ln k}{k} \left( 1 + \frac{3}{2k} - \frac{s}{2k^2} \right) - \frac{cs}{2k^2} + o_k(1/k). \end{aligned} \quad (4.9)$$

Since  $f(\rho) = H(k^{-1}\rho) + E(\rho)$ , (4.8) and (4.9) yield

$$f(\bar{\rho}_{s\text{-stable}}) = \frac{c}{k} + (1 - s/k) \ln(1 - s/k) + \frac{s \ln k}{2k^2} \left( 3 - \frac{s}{k} \right) - \frac{cs}{2k^2} + o_k(1/k). \quad (4.10)$$



**4.3. Proof of Proposition 4.7.** We pursue the following strategy. Suppose that  $a, b \in J$  are such that  $\rho_{ia} = \min_{j \in J} \rho_{ij}$  and  $\rho_{ib} = \max_{j \in J} \rho_{ij}$ . If  $\rho_{ia} = \rho_{ib}$ , then  $\rho = \hat{\rho}$  and there is nothing to prove. Otherwise, we are going to argue that increasing  $\rho_{ia}$  slightly at the expense of  $\rho_{ib}$  yields a matrix  $\rho'$  with  $f(\rho') > f(\rho)$ . We start by calculating the partial derivatives of  $f$ .

**Lemma 4.11.** *Let  $\rho \in \mathcal{S}$ . Let  $i, j, l \in [k]$  and set  $\delta = \rho_{il} - \rho_{ij}$ . Suppose that  $\rho_{ij}, \rho_{il} > 0$ . Then*

$$\text{sign} \left\{ \frac{\partial f}{\partial \rho_{ij}} - \frac{\partial f}{\partial \rho_{il}} \right\} = \text{sign} \left\{ 1 + \frac{\delta}{\rho_{ij}} - \exp \left( \frac{d \cdot \delta}{k - 2 + \frac{1}{k} \|\rho\|_2^2} \right) \right\}. \quad (4.11)$$

*Proof.* Using (4.5), (4.6) and the chain rule, we obtain

$$\frac{\partial f}{\partial \rho_{ij}} - \frac{\partial f}{\partial \rho_{il}} = \frac{1}{k} \left[ \ln \left( \frac{\rho_{il}}{\rho_{ij}} \right) - \frac{d}{k} \cdot \frac{\rho_{il} - \rho_{ij}}{1 - \frac{2}{k} + \frac{1}{k^2} \|\rho\|_2^2} \right].$$

Substituting  $\delta = \rho_{il} - \rho_{ij}$ , we find

$$\ln \left( \frac{\rho_{il}}{\rho_{ij}} \right) - \frac{d}{k} \cdot \frac{\rho_{il} - \rho_{ij}}{1 - \frac{2}{k} + \frac{1}{k^2} \|\rho\|_2^2} = \ln(1 + \delta/\rho_{ij}) - \frac{d \cdot \delta}{k(1 - \frac{2}{k} + \frac{1}{k^2} \|\rho\|_2^2)}.$$

Taking exponentials completes the proof.  $\square$

As a next step, we take a closer look at the right hand side of (4.11).

**Lemma 4.12.** *Let  $\rho \in \mathcal{S}$ , let  $i, j \in [k]$  and assume that  $\rho_{ij} > 0$ .*

(1) *If*

$$\frac{1}{\rho_{ij}} > \frac{d}{k - 2 + \frac{1}{k} \|\rho\|_2^2}, \quad (4.12)$$

*then there exists a unique  $\delta^* > 0$  such that*

$$1 + \frac{\delta^*}{\rho_{ij}} = \exp \left[ \frac{d \cdot \delta^*}{k - 2 + \frac{1}{k} \|\rho\|_2^2} \right].$$

*Furthermore, for all  $0 < \delta < \delta^*$  we have  $1 + \frac{\delta}{\rho_{ij}} - \exp \left[ \frac{d}{k - 2 + \frac{1}{k} \|\rho\|_2^2} \cdot \delta \right] > 0$ .*

(2) *If (4.12) does not hold, then for all  $\delta > 0$  we have  $1 + \frac{\delta}{\rho_{ij}} < \exp \left[ \frac{d}{k - 2 + \frac{1}{k} \|\rho\|_2^2} \cdot \delta \right]$ .*

*Proof.* There is at most one  $\delta^* > 0$  where the straight line  $\delta \mapsto 1 + \frac{\delta}{\rho_{ij}}$  intersects the strictly convex function

$$\delta \mapsto \exp \left[ \frac{d}{k - 2 + \frac{1}{k} \|\rho\|_2^2} \cdot \delta \right].$$

In fact, there is exactly one such  $\delta^*$  iff the differential of the linear function is greater than that of the exponential function at  $\delta = 0$ , which occurs iff (4.12) holds.  $\square$

*Proof of Proposition 4.7.* If  $\rho_{ij} = 0$  for all  $j \in J$ , then  $\hat{\rho} = \rho$  and there is nothing to show. Thus, assume that  $\sum_{j \in J} \rho_{ij} > 0$ . Suppose that  $\tilde{\rho} \in \mathcal{S}$  maximizes  $f(\tilde{\rho})$  subject to the conditions

- i.  $\tilde{\rho}_{ab} = \rho_{ab}$  for all  $(a, b) \notin \{i\} \times J$  and
- ii.  $\max_{j \in J} \tilde{\rho}_{ij} \leq \max_{j \in J} \rho_{ij}$ .

Such a maximizer  $\tilde{\rho}$  exists because i.–ii. define a compact domain. Because  $\tilde{\rho} \in \mathcal{S}$  we have

$$\sum_{j \in J} \tilde{\rho}_{ij} = \sum_{j \in J} \rho_{ij}. \quad (4.13)$$

We claim that  $\tilde{\rho}_{ij} > 0$  for all  $j \in J$ . Indeed, assume that  $\tilde{\rho}_{ij} = 0$  for  $j \in J$  but  $\tilde{\rho}_{il} > 0$  for some other  $l \in J$ . We recall that  $f(\rho) = H(k^{-1}\rho) + E(\rho)$ . As (4.5) and (4.6) show,  $\partial H(k^{-1}\rho)/\partial \rho_{ij}$  tends to infinity as  $\rho_{ij}$  approaches 0, while  $|\partial E(\rho)/\partial \rho_{ij}|$  remains bounded. Hence, there is  $\xi > 0$  such that the matrix  $\rho'$  obtained from  $\tilde{\rho}$  by replacing  $\tilde{\rho}_{ij}$  by  $\xi$  and  $\tilde{\rho}_{il}$  by  $\tilde{\rho}_{il} - \xi$  satisfied  $f(\rho') > f(\tilde{\rho})$ , in contradiction to the maximality of  $f(\tilde{\rho})$ .

Thus, let  $a$  be such that  $\tilde{\rho}_{ia} = \min_{j \in J} \tilde{\rho}_{ij} > 0$ . Because  $\tilde{\rho}$  is stochastic, we have  $\|\tilde{\rho}\|_2^2 \in [1, k]$  and  $|J|\tilde{\rho}_{ia} \leq \sum_{j \in J} \tilde{\rho}_{ij} \leq 1$ . Therefore, our assumptions  $\lambda \geq 3 \ln \ln k / \ln k$  and  $d \leq 2k \ln k$  imply that

$$\frac{1}{\tilde{\rho}_{ia}} \geq |J| \geq k^\lambda \geq 3 \ln k > \frac{d}{k - 2 + \|\tilde{\rho}\|_2^2 / k}. \quad (4.14)$$

Thus, (4.12) is satisfied. Further, setting  $\hat{\delta} = \lambda/2 - \ln \ln k / \ln k$ , we find

$$\begin{aligned} \exp \left( \frac{d\hat{\delta}}{k(1 - 2/k + k^{-2} \|\tilde{\rho}\|_2^2)} \right) &\leq \exp \left( 2\hat{\delta} \ln k \right) \quad [\text{as } d \leq 2k \ln k \text{ and } \|\tilde{\rho}\|_2^2 \geq 1] \\ &\leq k^\lambda \ln^{-2} k \leq |J| \ln^{-2} k \\ &< 1 + \hat{\delta} / \tilde{\rho}_{ia} \quad [\text{as } \lambda \geq 3 \ln \ln k / \ln k \text{ and } 1/\tilde{\rho}_{ia} \geq |J|]. \end{aligned} \quad (4.15)$$

Now, let  $b \in J$  be such that  $\tilde{\rho}_{ib} = \max_{j \in J} \tilde{\rho}_{ij}$  and assume that  $\delta = \tilde{\rho}_{ib} - \tilde{\rho}_{ia} > 0$ . Moreover, recall that we are assuming that  $\tilde{\rho}_{ib} \leq \max_{j \in J} \rho_{ij} \leq \hat{\delta}$ . Since  $\delta \leq \tilde{\rho}_{ib} \leq \hat{\delta}$ , (4.14) and (4.15) yield in combination with Lemmas 4.11 and 4.12 that

$$\left. \frac{\partial f}{\partial \rho_{ia}} - \frac{\partial f}{\partial \rho_{ib}} \right|_{\tilde{\rho}} > 0.$$

Hence, there is  $\xi > 0$  such that the matrix  $\rho'$  obtained from  $\tilde{\rho}$  by increasing  $\tilde{\rho}_{ia}$  by  $\xi$  and decreasing  $\tilde{\rho}_{ib}$  by  $\xi$  satisfies  $f(\rho') > f(\tilde{\rho})$ . But this contradicts the maximality of  $f(\tilde{\rho})$  subject to i.–ii. Thus, we conclude that  $\min_{j \in J} \tilde{\rho}_{ij} = \tilde{\rho}_{ia} = \tilde{\rho}_{ib} = \max_{j \in J} \tilde{\rho}_{ij}$ . Therefore, (4.13) implies that  $\tilde{\rho} = \hat{\rho}$  is the unique maximizer of  $f$  subject to i.–ii.  $\square$

**4.4. Proof of Proposition 4.3.** To proof is based on two key lemmas. The first one rules out that  $f(\rho)$  takes its maximum over  $\rho \in \mathcal{S}$  at a matrix with an entry close to  $1/2$ .

**Lemma 4.13.** *If  $\rho \in \mathcal{S}$  has an entry  $\rho_{ij} \in [0.49, 0.51]$ , then there is  $\rho' \in \mathcal{S}$  such that  $f(\rho') \geq f(\rho) + \frac{\ln k}{5k}$ .*

*Proof.* Without loss of generality we may assume that  $(i, j) = (1, 1)$  and that  $\rho \in \mathcal{S}$  maximizes  $f$  subject to the condition that  $\rho_{11} \in [0.49, 0.51]$ . There are two cases.

**Case 1:**  $\rho_{1j} < 0.49$  for all  $j \geq 2$ : Applying Proposition 4.7 to the set  $J = \{2, \dots, k\}$  (with  $\lambda = \frac{\ln(k-1)}{\ln k}$ ), we see that  $\rho_{1j} = \frac{1-\rho_{11}}{k-1}$  for all  $j \geq 2$ , due to the maximality of  $f(\rho)$ . Hence, Corollary 4.10 yields

$$H(\rho_1) \leq h(\rho_{11}) + (1 - \rho_{11}) \ln(k-1) \leq \ln 2 + 0.51 \ln k. \quad (4.16)$$

Moreover, because  $\rho_{11} \leq 0.51$  we have

$$\|\rho_1\|_2^2 \leq 0.51^2 + (k-1) \left( \frac{1-\rho_{11}}{k-1} \right)^2 \leq 0.261. \quad (4.17)$$

Let  $\rho'$  be the matrix obtained from  $\rho$  by replacing the first row by  $(1, 0, \dots, 0)$ . Since  $H(1, 0, \dots, 0) = 0$ , (4.4) and (4.16) yield

$$\begin{aligned} f(\rho) - f(\rho') &= H(k^{-1}\rho) - H(k^{-1}\rho') + E(\rho) - E(\rho') \\ &= \frac{H(\rho_1) - H(1, 0, \dots, 0)}{k} + E(\rho) - E(\rho') \leq \frac{\ln 2 + 0.51 \ln k}{k} + E(\rho) - E(\rho'). \end{aligned} \quad (4.18)$$

Furthermore, (4.17) entails  $\|\rho\|_2^2 - \|\rho'\|_2^2 \leq \|\rho_1\|_2^2 - 1 \leq -0.739$ . Hence, (4.6) yields

$$E(\rho) - E(\rho') \leq -(0.739 + \tilde{O}_k(1/k)) \ln k / k \leq -0.73 \ln k / k. \quad (4.19)$$

Combining (4.18) and (4.19), we obtain  $f(\rho) - f(\rho') \leq \frac{1}{k} [\ln 2 - 0.22 \ln k] \leq -\frac{\ln k}{5k}$ .

**Case 2:** there is  $j \geq 2$  such that  $\rho_{1j} > 0.49$ : We may assume that  $j = 2$ . Because  $\sum_j \rho_{1j} = 1$ , we see that  $\max_{j \geq 3} \rho_{1j} \leq 0.02$ . Hence, we can apply Proposition 4.7 to  $J = \{3, \dots, k\}$  (with, say,  $\lambda = 1/2$ ). Due to the maximality of  $f(\rho)$ , we obtain  $\rho_{1j} = (1 - \rho_{11} - \rho_{12}) / (k-2)$  for all  $j \geq 3$ . Hence, Corollary 4.10 yields

$$H(\rho_1) \leq h(\rho_{11}) + h(\rho_{12}) + 0.02 \ln(k-2) \leq 2 \ln 2 + 0.02 \ln k. \quad (4.20)$$

Further, because  $\rho_{11}^2 + \rho_{12}^2 \leq 0.51^2 + 0.49^2$  as  $\rho_{11}, \rho_{12} \in [0.49, 0.51]$  and  $\rho_{11} + \rho_{12} \leq 1$ , we see that

$$\|\rho_1\|_2^2 \leq 0.51^2 + 0.49^2 + (k-2) \left( \frac{1 - \rho_{11} - \rho_{12}}{k-2} \right)^2 \leq 0.501. \quad (4.21)$$

As in the first case, obtain  $\rho'$  from  $\rho$  by replacing the first row by  $(1, 0, \dots, 0)$ . From (4.21) we obtain  $\|\rho\|_2^2 - \|\rho'\|_2^2 \leq 0.501 - 1 = -0.499$ . Hence, (4.6) yields

$$E(\rho) - E(\rho') \leq -0.499(1 + \tilde{O}_k(1/k)) \ln k/k \leq -0.49 \ln k/k. \quad (4.22)$$

Combining (4.20) and (4.22), we find

$$\begin{aligned} f(\rho) - f(\rho') &= H(k^{-1}\rho) - H(k^{-1}\rho') + E(\rho) - E(\rho') \\ &\leq \frac{1}{k} [2 \ln 2 + 0.02 \ln k - 0.49 \ln k] \leq -\frac{\ln k}{5k}. \end{aligned}$$

Hence, in either case we obtain the desired bound.  $\square$

The second key ingredient is

**Lemma 4.14.** *We have  $\max_{\rho \in \mathcal{S}} f(\rho) \leq \frac{\ln k}{8k} + O_k(1/k)$ .*

The proof of Lemma 4.14 requires two intermediate steps. We start with the following exercise in calculus.

**Lemma 4.15.** *Let  $\xi : b \in (0, k/2) \mapsto k^{2b/k}(b^{-1} - k^{-1})$ . Let  $\mu = \frac{k}{2}(1 - \sqrt{1 - 2/\ln k})$ . Then  $\xi$  is decreasing on the interval  $(0, \mu)$  and increasing on  $(\mu, k/2)$ . Furthermore, we have*

$$-1/2 \leq \xi'(b) \leq -3/2 \quad \text{for } b \in (0.99, 1.01). \quad (4.23)$$

*Proof.* The derivatives of  $\xi$  are

$$\xi'(b) = k^{2b/k} \left[ \frac{2 \ln k}{k} \left( \frac{1}{b} - \frac{1}{k} \right) - \frac{1}{b^2} \right], \quad \xi''(b) = 2k^{2b/k} \left[ \frac{2 \ln^2 k}{k^2} \left( \frac{1}{b} - \frac{1}{k} \right) - \frac{2 \ln k}{kb^2} + \frac{1}{b^3} \right].$$

The first derivative vanishes at the two points  $b = \frac{k}{2}(1 \pm \sqrt{1 - 2/\ln k})$  only. Moreover, an elementary calculation shows that  $\mu = \frac{k}{2}(1 - \sqrt{1 - 2/\ln k})$  is a local minimum, while  $\frac{k}{2}(1 + \sqrt{1 - 2/\ln k}) > k/2$  is a local maximum. Hence,  $\xi$  is decreasing on the interval  $(0, \mu)$  and increasing on  $(\mu, k/2)$ . The last assertion follows by direct inspection of the above expression for  $\xi'$ .  $\square$

**Lemma 4.16.** *Let  $\rho \in \mathcal{S}$ . Suppose that  $i \in [k]$  is such that  $\rho_{ij} \notin [0.49, 0.51]$  for all  $j \in [k]$ .*

(1) *Suppose that  $\rho_{ij} \leq 0.49$  for all  $j \in [k]$ . Let  $\rho'$  be the stochastic matrix with entries*

$$\rho'_{hj} = \rho_{hj} \text{ and } \rho'_{ij} = 1/k \quad \text{for all } j \in [k], h \in [k] \setminus \{i\}.$$

*Then  $f(\rho) \leq f(\rho')$ .*

(2) *Suppose that  $\rho_{ij} \geq 0.51$  for some  $j \in [k]$ . Then there is a number  $\alpha = 1/k + \tilde{O}_k(1/k^2)$  such that for the stochastic matrix  $\rho''$  with entries*

$$\rho''_{hj} = \rho_{hj} \text{ and } \rho''_{ii} = 1 - \alpha, \rho''_{ih} = \frac{1 - \alpha}{k - 1} \quad \text{for all } j \in [k], h \in [k] \setminus \{i\}$$

*we have  $f(\rho) \leq f(\rho'')$ .*

*Proof.* To obtain the first assertion, we simply apply Proposition 4.7 to row  $i$  and  $J = [k]$  (with  $\lambda = 1$ ). With respect to the second claim, we may assume without loss that  $i = j = 1$  and  $\rho_{11} \geq 0.51$ . Let  $\hat{\rho} \in \mathcal{S}$  be the matrix that maximizes  $f$  subject to the conditions

- i.  $\hat{\rho}_{11} \geq 0.51$ .
- ii.  $\hat{\rho}_a = \rho_a$  for all  $a \in \{2, \dots, k\}$ . (In words, the last  $k - 1$  rows of  $\hat{\rho}$  and  $\rho$  coincide.)

Since  $\hat{\rho}_{1j} \leq 1 - \hat{\rho}_{11} \leq 0.49$  for all  $j \geq 2$ , Proposition 4.7 applies to  $J = \{2, \dots, k\}$  (with  $\lambda = \frac{\ln(k-1)}{\ln k}$ ) and yields

$$\hat{\rho}_{12} = \dots = \hat{\rho}_{1k} = \frac{1 - \hat{\rho}_{11}}{k - 1}. \quad (4.24)$$

Let  $\delta = \hat{\rho}_{11} - \hat{\rho}_{12}$ , let  $0 \leq \beta \leq 0.49k$  be such that  $\hat{\rho}_{11} = 1 - \beta/k$  and let  $Q = 1 - 1/k + \|\hat{\rho}\|_2^2/k^2$ .

Because  $\hat{\rho}$  is the maximizer of  $f$  subject to i. and ii., Lemma 4.11 implies that

$$\text{either } \beta \in \{0, 0.49k\}, \text{ or } 1 + \frac{\delta}{\hat{\rho}_{12}} = \exp\left(\frac{\delta d}{kQ}\right). \quad (4.25)$$

We are going to argue that (4.25) entails that  $\beta = 1 + \tilde{O}_k(1/k)$ .

First, we observe that  $\beta > 0$ . For (4.5) shows that the derivative  $\partial H(\rho_1)/\partial \rho_{11}$  of the entropy of row  $\rho_1$  tends to  $-\infty$  as  $\rho_{11}$  approaches 1, while (4.6) implies that the derivative  $\partial E(\rho)/\partial \rho_{11}$  remains bounded in absolute value. Hence, the maximality of  $f(\rho)$  implies that  $\beta > 0$ .

Further, since  $\|\hat{\rho}\|_2^2 \in [1, k]$ , we have  $Q \geq (1 - 1/k)^2$ . Moreover, (4.24) implies that  $\delta = \hat{\rho}_{11} - O_k(1/k)$ . Therefore, recalling that  $d = 2k \ln k + O_k(\ln k)$ , we obtain

$$\begin{aligned} \exp\left(\frac{\delta d}{kQ}\right) &= k^{2\hat{\rho}_{11}} \left(1 + \tilde{O}_k(1/k)\right) = k^{2(1-\beta/k)}(1 + O_k(\ln k/k)), \\ 1 + \frac{\delta}{\hat{\rho}_{12}} &= \frac{\hat{\rho}_{11}}{\hat{\rho}_{12}} = \frac{(k-1)\hat{\rho}_{11}}{1 - \hat{\rho}_{11}} = k^2(1/\beta - 1/k)(1 + O_k(1/k)) \quad [\text{as } \rho_{11} = 1 - \beta/k]. \end{aligned}$$

Thus, with  $\xi(b) = k^{2b/k}(b^{-1} - k^{-1})$  the function from Lemma 4.15, we see that for a certain  $\eta = O_k(\ln k/k)$ ,

$$(1 - \eta) \cdot \xi(\beta) \leq \left(1 + \frac{\delta}{\hat{\rho}_{12}}\right) \exp\left(-\frac{\delta d}{kQ}\right) \leq (1 + \eta) \cdot \xi(\beta). \quad (4.26)$$

Let  $\mu = \frac{k}{2}(1 - \sqrt{1 - 2/\ln k}) = (1 + o_k(1))\frac{k}{2\ln k}$ . By Lemma 4.15,  $\xi$  is decreasing on  $(0, \mu)$ . Moreover,  $\xi'(b)$  is negative and bounded away from 0 for  $b$  close to 1. Hence, setting  $\gamma = \ln^2 k/k$ , we find

$$\xi(\beta) \leq \xi(1 + \gamma) < (1 + \eta)^{-1} \quad \text{if } \beta \in [1 + \gamma, \mu].$$

In addition,  $\xi$  is increasing on  $(\mu, k/2)$ . Thus,

$$\xi(\beta) \leq \xi(0.49k) \leq k^{0.98} \left(\frac{1}{0.49k} - \frac{1}{k}\right) < (1 + \eta)^{-1} \quad \text{if } \beta \in [\mu, 0.49k].$$

Plugging these two bounds into (4.26), we get

$$1 + \frac{\delta}{\hat{\rho}_{12}} < \exp\left(\frac{\delta d}{kQ}\right) \quad \text{if } \beta \in [1 + \gamma, 0.49k]. \quad (4.27)$$

Similarly, because  $\mu$  is the unique local minimum of  $\xi$ , we have

$$\xi(\beta) \geq \xi(1 - \gamma) > (1 - \eta)^{-1} \quad \text{if } \beta \in (0, 1 - \gamma).$$

Hence, (4.26) yields

$$1 + \frac{\delta}{\hat{\rho}_{12}} > \exp\left(\frac{\delta d}{kQ}\right) \quad \text{if } \beta \in (0, 1 - \gamma). \quad (4.28)$$

Since we already know that  $\beta > 0$ , (4.25), (4.27) and (4.28) imply  $\beta \in [1 - \gamma, 1 + \gamma]$ . Thus,  $\beta = 1 + \tilde{O}_k(1/k)$  and consequently  $\hat{\rho}_{11} = 1 - \beta/k = 1 - 1/k + \tilde{O}_k(k^{-2})$ , as desired.  $\square$

*Proof of Lemma 4.14.* Lemma 4.13 implies that  $\max_{\rho \in S} f(\rho)$  is attained at a matrix  $\rho$  without entries in  $[0.49, 0.51]$ . Therefore, Lemma 4.16 shows that the maximizer  $\rho$  has the following form for some integer  $0 \leq s \leq k$  and certain  $\alpha_i = 1/k + \tilde{O}_k(1/k^2)$ :

$$\rho_{ij} = \begin{cases} 1 - \alpha_i & \text{if } i = j \in [s], \\ \frac{\alpha_i}{k-1} & \text{if } i \in [s], j \neq i, \\ 1/k & \text{otherwise.} \end{cases} \quad (4.29)$$

Thus, for  $i \in [s]$  we have

$$H(\rho_i) = h(1 - \alpha_i) + \alpha_i \ln(k - 1) \leq h(\alpha_i) + \alpha_i \ln k, \quad (4.30)$$

$$\|\rho_i\|_2^2 = (1 - \alpha_i)^2 + \alpha_i^2/(k - 1). \quad (4.31)$$

Let  $\rho'$  be the matrix obtained from  $\rho$  by replacing the first  $s$  rows by  $(1, 0, \dots, 0)$ . This matrix satisfies

$$H(\rho'_i) = 0, \quad \|\rho'_i\|_2^2 = 1 \quad \text{for } i \in [s]. \quad (4.32)$$

Set  $\alpha = \frac{1}{s} \sum_{i=1}^s \alpha_i = \frac{1}{k} + \tilde{O}_k(k^{-2})$ . Then (4.4), (4.30)–(4.32) and the concavity of  $h$  imply that

$$H(k^{-1}\rho) - H(k^{-1}\rho') = \frac{1}{k} \sum_{i=1}^s H(\rho_i) \leq \frac{s}{k} [h(\alpha) + \alpha \ln k] \leq \frac{\alpha s}{k} [1 - \ln \alpha + \ln k] \leq \frac{2\alpha s}{k} [1 + \ln k], \quad (4.33)$$

$$\begin{aligned} \|\rho\|_2^2 - \|\rho'\|_2^2 &\leq \sum_{i=1}^s \left[ (1 - \alpha_i)^2 + \frac{\alpha_i^2}{k - 1} - 1 \right] = \sum_{i=1}^s \alpha_i [-2 + \alpha_i(1 + 1/(k - 1))] \\ &= \alpha s [-2 + O_k(1/k)]. \end{aligned} \quad (4.34)$$

Plugging (4.34) into (4.6), we obtain

$$E(\rho) - E(\rho') \leq \alpha s [-2 + O_k(1/k)] \cdot (1 + \tilde{O}_k(1/k)) \frac{\ln k}{k} \leq -\frac{2\alpha s}{k} [\ln k + \tilde{O}_k(1/k)]. \quad (4.35)$$

Combining (4.33) and (4.35) and recalling that  $\alpha = 1/k + \tilde{O}_k(1/k^2)$ , we see that

$$f(\rho) - f(\rho') \leq \frac{2\alpha s}{k} [1 + \tilde{O}_k(1/k)] \leq 3/k. \quad (4.36)$$

To complete the proof, we calculate  $f(\rho')$ . Recall that  $d = 2k \ln k - \ln k - c$  with  $c$  bounded. Moreover, (4.32) shows that  $\|\rho'_i\|_2^2 = 1$  for  $i = 1, \dots, s$ . In addition, since  $\rho'_{ij} = 1/k$  for all  $i > s, j \in [k]$ , we get  $\|\rho'_i\|_2^2 = 1/k$  for  $i > s$ . Hence,  $\|\rho'\|_2^2 = 1 + (1 - 1/k)s$ . Thus, using (4.7) and performing an elementary calculation, we get

$$\begin{aligned} E(\rho') &= \frac{d}{2k^2} \left[ -2k + \|\rho'\|_2^2 - 2 \left( 1 - \frac{\|\rho'\|_2^2}{2k} \right)^2 \right] + o_k(1/k) \\ &= -2 \ln k + \frac{c}{k} + \frac{s \ln k}{k} \left( 1 + \frac{1}{2k} - \frac{s}{2k^2} \right) - \frac{cs}{2k^2} + o_k(1/k). \end{aligned}$$

Further,  $H(\rho'_i) = 0$  for  $i \leq s$ , while  $H(\rho'_i) = \ln k$  for  $i > s$ . Hence, (4.4) yields  $H(k^{-1}\rho') = \ln k + (1 - s/k) \ln k = 2 \ln k - \frac{s}{k} \ln k$ . Thus,

$$\begin{aligned} f(\rho') &= H(\rho') + E(\rho') = \frac{c}{k} + \frac{s \ln k}{k} \left( \frac{1}{2k} - \frac{s}{2k^2} \right) - \frac{cs}{2k^2} + o_k(1/k) \\ &= \frac{c}{k} + \frac{s}{k} (1 - s/k) \cdot \frac{\ln k}{2k} - \frac{cs}{2k^2} + o_k(1/k) = \frac{s}{k} (1 - s/k) \cdot \frac{\ln k}{2k} + O_k(1/k). \end{aligned} \quad (4.37)$$

Finally, combining (4.36) and (4.37), we see that  $f(\rho) \leq \frac{s}{k} (1 - s/k) \cdot \frac{\ln k}{2k} + O_k(1/k) \leq \frac{\ln k}{8k} + O_k(1/k)$ , as claimed.  $\square$

*Proof of Proposition 4.3.* Suppose that  $\rho \in \mathcal{S}$  has an entry  $\rho_{ij} \in [0.49, 0.51]$ . We claim that  $f(\rho) < 0$ . Indeed, by Lemmas 4.13 and 4.14

$$f(\rho) \leq \max_{\rho' \in \mathcal{S}} f(\rho') - \frac{\ln k}{5k} \leq \frac{\ln k}{8k} + O_k(1/k) - \frac{\ln k}{5k} < 0.$$

Now, suppose that  $\rho \in \mathcal{S}$  has a row  $i$  such that  $\max_{j \in [k]} \rho_{ij} \in [0.15, 0.49]$ . Without loss of generality, we may assume  $i = 1$  and  $\rho_{11} = \max_{j \in [k]} \rho_{1j}$ . In fact, we may assume that  $\rho$  is the maximizer of  $f$  subject to the condition  $\rho_{11} = \max_j \rho_{1j} \in [0.15, 0.49]$ . Again, we show that  $f(\rho) < 0$ .

What can we say about this maximizer  $\rho$ ? We apply Proposition 4.7 to  $i = 1$  and  $J = \{2, \dots, k\}$ : if we let  $\lambda = \ln(k - 1)/\ln k$ , then  $|J| = k - 1 \geq k^\lambda$ . Moreover,  $\rho_{1j} \leq 0.49 < \lambda/2 - 10/\ln k$  for all  $j \in J$ . Hence, Proposition 4.7 implies that

$$\rho_{12} = \dots = \rho_{1k}. \quad (4.38)$$



Thus, Corollary 4.10 shows that the entropy of  $\rho_1$  is

$$H(\rho_1) \leq h(\rho_{11}) + (1 - \rho_{11}) \ln(k - 1).$$

By comparison, let  $\hat{\rho}$  be the matrix obtained from  $\rho$  by replacing the first row by  $\frac{1}{k}\mathbf{1}$ . Then  $H(\hat{\rho}_1) = \ln k$ . Therefore, (4.4) yields

$$H(k^{-1}\rho) - H(k^{-1}\hat{\rho}) = -\frac{1}{k} [\ln k - h(\rho_{11}) - (1 - \rho_{11}) \ln(k - 1)] \leq -\rho_{11} \frac{\ln k}{k} + O_k(1/k). \quad (4.39)$$

Moreover, (4.38) yields  $\|\rho_1\|_2^2 = \rho_{11}^2 + (1 - \rho_{11})^2/(k - 1)$  and  $\|\hat{\rho}_1\|_2^2 = 1/k$ , whence

$$\|\rho\|_2^2 - \|\hat{\rho}\|_2^2 \leq \rho_{11}^2 + \frac{(1 - \rho_{11})^2}{k - 1} - 1/k \leq \rho_{11}^2.$$

Hence, (4.6) implies  $E(\rho) - E(\hat{\rho}) \leq \rho_{11}^2 \frac{\ln k}{k} + \tilde{O}_k(1/k^2)$ . Combining this estimate with (4.39), we get

$$f(\rho) - f(\hat{\rho}) = H(k^{-1}\rho) - H(k^{-1}\hat{\rho}) + E(\rho) - E(\hat{\rho}) \leq -\rho_{11}(1 - \rho_{11}) \frac{\ln k}{k} + O_k(1/k). \quad (4.40)$$

Since  $f(\hat{\rho}) \leq \frac{\ln k}{8k} + O_k(1/k)$  by Lemma 4.14, we obtain from (4.40)

$$f(\rho) \leq \left[ \frac{1}{8} - \rho_{11}(1 - \rho_{11}) \right] \frac{\ln k}{k} + O_k(1/k).$$

The assertion follows because  $\rho_{11}(1 - \rho_{11}) > 1/8$  for  $\rho_{11} \in [0.15, 0.49]$ .  $\square$

**4.5. Proof of Proposition 4.4.** Let  $1 \leq s \leq k^{0.999}$  and let  $\rho \in \mathcal{D}_{s, \text{tame}}$  be the maximiser of  $f$ . Without loss of generality we may assume that  $\rho_{ii} \geq 0.51$  for  $i = 1, \dots, s$  and  $f(\rho_{ij}) < 0.51$  for all  $(i, j) \notin \{(1, 1), \dots, (s, s)\}$ . Because  $\rho$  is separable, this implies that in fact  $\rho_{ii} \geq 1 - \kappa$  for  $i = 1, \dots, s$ , with  $\kappa = \ln^{20} k/k$  as in (2.15). Furthermore, if there is a pair  $(i, j) \notin \{(1, 1), \dots, (s, s)\}$  such that  $\rho_{ij} \geq 0.15$ , then Proposition 4.3 implies that  $f(\rho) < 0$ . In this case we are done, because  $f(\bar{\rho}) > 0$  by Proposition 2.4. Thus, assume from now on that  $\rho_{ij} < 0.15$  for all  $(i, j) \notin \{(1, 1), \dots, (s, s)\}$ .

Let  $\hat{\rho}$  be the singly-stochastic matrix with entries

$$\hat{\rho}_{ij} = \begin{cases} \rho_{ij} & \text{if } i \in [k], j \leq s, \\ \frac{1}{k-s} \sum_{l>s} \rho_{il} & \text{if } i \in [k], j > s. \end{cases}$$

Since  $k - s = (1 - o_k(1))k$  and  $\max_{j>s} \rho_{ij} < 0.15$ , we can apply Proposition 4.7 to  $J = [k] \setminus [s]$  for any  $i \in [k]$  (with, say,  $\lambda = 1/2$ ). Hence,

$$f(\rho) \leq f(\hat{\rho}). \quad (4.41)$$

We are going to compare  $f(\hat{\rho})$  with  $f(\bar{\rho}_{s-\text{stable}})$ , the barycentre of the face of  $\mathcal{D}$  where the first  $s$  diagonal entries are equal to one. To this end, we need to estimate  $f(\hat{\rho}) = H(k^{-1}\hat{\rho}) + E(\hat{\rho})$ .

As  $\hat{\rho}$  is stochastic and  $\hat{\rho}_{ii} = \rho_{ii} \geq 1 - \kappa$  for  $i \leq s$ , we find that

$$q_i = \sum_{j \neq i} \hat{\rho}_{ij} = 1 - \rho_{ii} \leq \kappa \quad \text{for } i \leq s. \quad (4.42)$$

Further, let  $q_i = \sum_{j=1}^s \hat{\rho}_{ij}$  for  $i > s$ . Because  $\rho$  is doubly-stochastic and  $\rho_{ii} \geq 1 - \kappa$  for  $i \leq s$ , we see that

$$\sum_{i>s} q_i = \sum_{i>s} \sum_{j=1}^s \hat{\rho}_{ij} = \sum_{i>s} \sum_{j=1}^s \rho_{ij} = \sum_{i=1}^s \sum_{j>s} \rho_{ij} \leq \kappa s. \quad (4.43)$$

Based on (4.42)–(4.43), we obtain the following estimate of the entropy.

**Claim 4.17.** *We have  $H(k^{-1}\hat{\rho}) \leq H(k^{-1}\bar{\rho}_{s-\text{stable}}) + o_k(1/k)$ .*

*Proof.* By Corollary 4.10 and (4.42),

$$H(\hat{\rho}_i) \leq h(q_i) + q_i \ln k \leq h(\kappa) + \kappa \ln k \quad \text{for } i \leq s. \quad (4.44)$$

Once more by Corollary 4.10,

$$H(\hat{\rho}_i) \leq h(q_i) + q_i \ln s + (1 - q_i) \ln(k - s) \leq h(q_i) + q_i \ln s + \ln(k - s) \quad \text{for } i > s. \quad (4.45)$$

Since  $h$  is concave, (4.43) and (4.45) yield

$$\frac{1}{k} \sum_{i>s} H(\hat{\rho}_i) \leq \frac{k-s}{k} \ln(k-s) + \frac{1}{k} \sum_{i>s} (h(q_i) + q_i \ln s) \leq \frac{k-s}{k} \ln(k-s) + h\left(\frac{\kappa s}{k}\right) + \frac{\kappa s}{k} \ln s. \quad (4.46)$$

Plugging the bounds (4.44) and (4.46) into (4.4), we arrive at

$$\begin{aligned} H(k^{-1}\hat{\rho}) &= \ln k + \frac{1}{k} \sum_{i=1}^k H(\hat{\rho}_i) \\ &\leq \ln k + \frac{s}{k} (h(\kappa) + \kappa \ln k) + \frac{k-s}{k} \ln(k-s) + h(\kappa s/k) + \frac{\kappa s}{k} \ln s \\ &\leq \ln k + \frac{k-s}{k} \ln(k-s) + o_k(1/k) && [\text{as } \kappa = \tilde{O}_k(1/k) \text{ and } s \leq k^{0.999}] \\ &= H(k^{-1}\bar{\rho}_{s\text{-stable}}) + o_k(1/k) && [\text{by (4.8)}], \end{aligned}$$

thereby proving the claim.  $\square$

**Claim 4.18.** *We have  $E(\hat{\rho}) \leq E(\bar{\rho}_{s\text{-stable}}) + o_k(1/k)$ .*

*Proof.* As a first step, we show that there is a constant  $\gamma > 0$  such that

$$\|\rho\|_2^2 \leq s + 1 + (\kappa s)^2 \leq s + 1 + k^{-\gamma}. \quad (4.47)$$

Indeed, as  $\hat{\rho}$  is a stochastic matrix, we have

$$\|\hat{\rho}_i\|_2^2 \leq 1 \quad \text{for } i = 1, \dots, s. \quad (4.48)$$

Furthermore, since  $\sum_{j>s} \rho_{ij} \leq 1$  for each  $i \in [k] \setminus [s]$ , we have

$$\sum_{i>s} \sum_{j>s} \hat{\rho}_{ij}^2 = (k-s) \sum_{i>s} \left( \frac{\sum_{j>s} \rho_{ij}}{k-s} \right)^2 \leq 1. \quad (4.49)$$

Moreover, (4.43) shows that  $\sum_{i>s} q_i = \sum_{i>s} \sum_{j \leq s} \hat{\rho}_{ij} \leq \kappa s$ . Hence,

$$\sum_{i>s} \sum_{j \leq s} \hat{\rho}_{ij}^2 \leq \left( \sum_{i>s} \sum_{j \leq s} \hat{\rho}_{ij} \right)^2 \leq (\kappa s)^2. \quad (4.50)$$

As  $s \leq k^{0.999}$  and because  $\kappa = \ln^{20} k/k$ , there is a constant  $\gamma > 0$  such that  $\kappa s \leq k^{-0.001} \ln^{20} k \leq k^{-\gamma/2}$  (provided that  $k$  is sufficiently large). Thus, combining (4.48)–(4.50), we obtain (4.47).

By comparison, we have  $\|\bar{\rho}_{s\text{-stable}}\|_2^2 = s + 1$ . Hence, the bound (4.6) on the derivative of  $E$  and (4.47) yield  $E(\hat{\rho}) \leq E(\bar{\rho}_{s\text{-stable}}) + o_k(1/k)$ , as claimed.  $\square$

Combining Claims 4.17 and 4.18, we see that  $f(\hat{\rho}) \leq f(\bar{\rho}_{s\text{-stable}}) + o_k(1/k)$ . Hence, (4.41) yields

$$\begin{aligned} f(\rho) &\leq f(\hat{\rho}) \leq f(\bar{\rho}_{s\text{-stable}}) + o(1/k) \\ &\leq \frac{c}{k} + (1-s/k) \ln(1-s/k) + \frac{s \ln k}{2k^2} \left( 3 - \frac{s}{k} \right) - \frac{cs}{2k^2} + o_k(1/k) && [\text{due to (4.10)}] \\ &\leq \frac{c}{k} + (1-s/k) \ln(1-s/k) + o_k(1/k) && [\text{because } s \leq k^{0.999}] \\ &\leq \frac{c}{k} - \frac{s}{k} (1-s/k) + o_k(1/k) && [\text{as } \ln(1-x) \leq -x] \\ &= f(\bar{\rho}) - \frac{s}{k} (1-s/k) + o_k(1/k) && [\text{by Proposition 2.4}]. \end{aligned}$$

The last expression is decreasing in  $s$  (for  $1 \leq s \leq k^{0.999}$ ). Thus,  $f(\rho) < f(\bar{\rho}) - 1/k + o_k(1/k)$ . This implies the assertion because we chose  $\rho$  to be the maximizer of  $f$  over  $\mathcal{D}_{s,\text{tame}}$ .  $\square$

**4.6. Proof of Proposition 4.5.** Suppose that  $k^{0.999} < s < k - k^{0.49}$  and let  $\rho \in \mathcal{D}_{s,\text{tame}}$  be the maximizer of  $f$  over  $\mathcal{D}_{s,\text{tame}}$ . We may assume without loss that  $\rho_{ii} \geq 0.51$  for  $i = 1, \dots, s$  and  $\rho_{ij} < 0.51$  for  $(i, j) \notin \{(1, 1), \dots, (s, s)\}$ . Due to separability, we thus have  $\rho_{ii} \geq 1 - \kappa$  for  $i = 1, \dots, s$ . Further, we may assume that  $\rho_{ij} \leq 0.15$  for all  $(i, j) \notin \{(1, 1), \dots, (s, s)\}$  as otherwise Proposition 4.3 yields  $f(\rho) < 0 < f(\bar{\rho})$ .

Let  $\hat{\rho}$  be the stochastic matrix with entries

$$\hat{\rho}_{ij} = \begin{cases} \rho_{ij} & \text{if } i = j \in [s], \\ \frac{1}{s-1} \sum_{l \in [s] \setminus \{i\}} \rho_{il} & \text{if } i, j \leq s, i \neq j, \\ \frac{1}{k-s} \sum_{l > s} \rho_{il} & \text{if } j > s, \\ \frac{1}{s} \sum_{l \leq s} \rho_{il} & \text{if } j \leq s < i. \end{cases}$$

Since  $\max_{i \neq j} \rho_{ij} \leq 0.15$  and  $s, k-s > k^{0.49}$ , we can apply Proposition 4.7 to  $J_i = [k] \setminus [s]$  and to  $J'_i = [s] \setminus \{i\}$  for all  $i \in [k]$  (with, say,  $\lambda = 0.4$ ). We thus obtain

$$f(\rho) \leq f(\hat{\rho}). \quad (4.51)$$

To estimate  $f(\hat{\rho})$ , let

$$q_i = \sum_{j > s} \rho_{ij} = \sum_{j > s} \hat{\rho}_{ij} \text{ for } i \leq s \text{ and } q_i = \sum_{j \leq s} \rho_{ij} = \sum_{j \leq s} \hat{\rho}_{ij} \text{ for } i > s.$$

Since  $\rho$  is doubly-stochastic and  $\rho_{ii} \geq 1 - \kappa$  for  $i \leq s$ , we see that

$$q = \sum_{i > s} q_i = \sum_{i \leq s} q_i \leq \sum_{i=1}^s 1 - \rho_{ii} \leq \kappa s. \quad (4.52)$$

In addition, let

$$t_i = \sum_{j \in [s] \setminus \{i\}} \hat{\rho}_{ij} = \sum_{j \in [s] \setminus \{i\}} \rho_{ij} \leq 1 - \rho_{ii} \leq \kappa \quad \text{for } i \leq s. \quad (4.53)$$

**Claim 4.19.** We have  $H(\hat{\rho}) \leq 2 \ln k + \frac{3q(2 + \ln k)}{k} + (1 - s/k) \ln(1 - s/k) - \frac{s \ln k}{k} + \frac{2 \ln k}{k} \sum_{i=1}^s t_i + O_k(1/k)$ .

*Proof.* Applying Corollary 4.10, we obtain

$$H(\hat{\rho}_i) \leq h(t_i) + t_i \ln s + h(q_i) + q_i \ln(k-s) \quad \text{for } i \leq s. \quad (4.54)$$

Set

$$\tilde{H} = \frac{1}{k} \sum_{i \leq s} h(t_i) + t_i \ln s.$$

Summing (4.54) up, recalling from (4.52) that  $q = \sum_{i \leq s} q_i$ , and using the concavity of  $h$ , we get

$$\frac{1}{k} \sum_{i=1}^s H(\hat{\rho}_i) \leq \tilde{H} + \frac{s}{k} h(q/s) + \frac{q}{k} \ln(k-s). \quad (4.55)$$

Furthermore, again by Corollary 4.10, for  $i > s$  we have

$$H(\hat{\rho}_i) \leq h(q_i) + q_i \ln s + (1 - q_i) \ln(k-s).$$

Once more due to the concavity of  $h$  and as  $q = \sum_{i > s} q_i$ , we see that

$$\frac{1}{k} \sum_{i > s} H(\hat{\rho}_i) \leq \frac{k-s}{k} h(q/(k-s)) + \frac{q}{k} \ln s + \frac{k-s-q}{k} \ln(k-s). \quad (4.56)$$

Combining (4.55) and (4.56), we get

$$H(\hat{\rho}) \leq \tilde{H} + \ln k + \left[ \frac{s}{k} h(q/s) + \frac{q}{k} \ln(k-s) \right] + \left[ \frac{k-s}{k} h(q/(k-s)) + \frac{q}{k} \ln s \right] + \frac{k-s-q}{k} \ln(k-s).$$

Using the elementary inequality  $h(z) \leq z(1 - \ln z)$  to simplify the above, we get

$$\begin{aligned}
H(\hat{\rho}) - \tilde{H} &\leq \ln k + \frac{q}{k} [2 + \ln(s/q) + \ln((k-s)/q) + \ln s + \ln(k-s)] + \frac{k-s-q}{k} \ln(k-s) \\
&\leq \ln k + \frac{q}{k} [2 + 2\ln(s) + \ln(k-s) - 2\ln q] + \frac{k-s}{k} \ln(k-s) \\
&\leq \ln k + \frac{3q(2 + \ln k)}{k} + \frac{k-s}{k} \ln(k-s) + O_k(1/k) \quad [\text{as } -z \ln z \leq 1 \text{ for all } z > 0] \\
&= 2\ln k + \frac{3q(2 + \ln k)}{k} + (1 - s/k) \ln(1 - s/k) - \frac{s \ln k}{k} + O_k(1/k).
\end{aligned} \tag{4.57}$$

Since  $s \leq k$ , we obtain

$$\tilde{H} - \frac{2\ln k}{k} \sum_{i=1}^s t_i = \frac{1}{k} \sum_{i \leq s} h(t_i) + t_i(\ln s - 2\ln k) \leq \frac{1}{k} \sum_{i=1}^s h(t_i) - t_i \ln k \leq \frac{1}{k} \quad [\text{due to (4.3)}]. \tag{4.58}$$

Finally, the assertions follows by combining (4.57) and (4.58).  $\square$

**Claim 4.20.** We have  $E(\hat{\rho}) = -2\ln k + \frac{s \ln k}{k} \left(1 + \frac{3}{2k} - \frac{s}{2k^2}\right) - \frac{2\ln k}{k} \sum_{i=1}^s t_i + \tilde{O}_k(1/k)$ .

*Proof.* As a first step, we show that

$$\|\rho\|_2^2 \leq s + 1 - 2 \sum_{i=1}^s t_i + o_k(1/\ln k). \tag{4.59}$$

Indeed, together with the definition of  $\hat{\rho}$ , equation (4.53) shows that for  $i \in [s]$ ,

$$\hat{\rho}_{ii}^2 \leq (1 - t_i)^2 = 1 - 2t_i + t_i^2 \leq 1 - 2t_i + \kappa^2 \quad \text{and} \tag{4.60}$$

$$\sum_{j \in [s] \setminus \{i\}} \hat{\rho}_{ij}^2 = (s-1) \cdot \left(\frac{t_i}{s-1}\right)^2 \leq \frac{\kappa^2}{s-1} \leq \kappa^2. \tag{4.61}$$

Moreover, since  $\hat{\rho}$  is stochastic and  $\hat{\rho}_{ii} \geq 1 - \kappa$  if  $i \leq s$ , we have

$$\sum_{j \in [k] \setminus [s]} \hat{\rho}_{ij}^2 \leq \kappa^2 \quad \text{for } i \in [s]. \tag{4.62}$$

Combining (4.60)–(4.62) and recalling that  $\kappa = \tilde{O}_k(k^{-1})$ , we obtain

$$\sum_{i=1}^s \|\hat{\rho}_i\|_2^2 \leq s + 3\kappa^2 s - 2 \sum_{i=1}^s t_i = s + o_k(1/\ln k) - 2 \sum_{i=1}^s t_i. \tag{4.63}$$

Further, since  $\rho_{jj} \geq 1 - \kappa$  for  $j \leq s$  and because  $\rho$  is doubly-stochastic, we have  $\rho_{ij} \leq \kappa$  for all  $j \leq s < i$ . By the construction of  $\hat{\rho}$ , this implies that  $\hat{\rho}_{ij} \leq \kappa$  for all  $j \leq s < i$ . Furthermore,  $q = \sum_{i>s} \sum_{j \in [s]} \hat{\rho}_{ij} \leq \kappa s$  by (4.52). As a sum of squares is maximized if the summands are as unequal as possible, we obtain

$$\sum_{i>s} \sum_{j \in [s]} \hat{\rho}_{ij}^2 \leq \kappa^2 s = o_k(1/\ln k). \tag{4.64}$$

In addition, once more by the construction of  $\hat{\rho}$ ,

$$\sum_{i>s} \sum_{j>s} \hat{\rho}_{ij}^2 = \sum_{i>s} (k-s) \left(\frac{\sum_{j>s} \rho_{ij}}{k-s}\right)^2 \leq (k-s)^2 \cdot \left(\frac{1}{k-s}\right)^2 = 1. \tag{4.65}$$

Combining (4.63)–(4.65), we obtain (4.59).

By comparison, we have  $\|\bar{\rho}_{s\text{-stable}}\|_2^2 = s + 1$ . Hence, (4.6) implies together with (4.59) that

$$E(\hat{\rho}) \leq E(\bar{\rho}_{s\text{-stable}}) - \frac{2\ln k}{k} \sum_{i=1}^s t_i + \tilde{O}_k(1/k).$$

Plugging in the expression (4.9) for  $E(\bar{\rho}_{s\text{-stable}})$  yields the assertion.  $\square$

Finally, combining Claims 4.19 and 4.20, we see that

$$\begin{aligned} f(\rho) &\leq f(\bar{\rho}) \leq (1 - s/k) \ln(1 - s/k) + \frac{3q(2 + \ln k)}{k} + \frac{s \ln k}{k} \left( \frac{3}{2k} - \frac{s}{2k^2} \right) + \tilde{O}(1/k) \\ &= (1 - s/k) \ln(1 - s/k) + \tilde{O}(1/k) \leq -\frac{s}{k}(1 - s/k) + \tilde{O}_k(1/k). \end{aligned} \quad (4.66)$$

Our assumption  $k^{0.999} < s < k - k^{0.49}$  ensures that  $-\frac{s}{k}(1 - s/k) + \tilde{O}_k(1/k) < 0$ . Thus, (4.66) and Proposition 2.4 show that  $f(\rho) < 0 < f(\bar{\rho})$ . This completes the proof as  $\rho$  was chosen to be the maximizer of  $f$  over  $\mathcal{D}_{s, \text{tame}}$ .  $\square$

**4.7. Proof of Proposition 4.6.** Suppose that  $k - \sqrt{k} \leq s \leq k - 1$  and that  $\rho \in \mathcal{D}_{s, \text{tame}}$  maximizes  $f$  over  $\mathcal{D}_{s, \text{tame}}$ . As before, we assume without loss that  $\rho_{ii} \geq 0.51$  for  $i = 1, \dots, s$  and  $\rho_{ij} < 0.51$  for  $(i, j) \notin \{(1, 1), \dots, (s, s)\}$ . Thus,  $\rho_{ii} \geq 1 - \kappa$  for  $i = 1, \dots, s$  as  $\rho$  is separable. Further, if  $\rho_{ij} > 0.15$  for some  $(i, j) \in \{(1, 1), \dots, (s, s)\}$ , then  $f(\rho) < 0 < f(\bar{\rho})$  by Proposition 4.3. Hence, we assume  $\rho_{ij} \leq 0.15$  for all  $(i, j) \notin \{(1, 1), \dots, (s, s)\}$ .

Let  $q_i = \sum_{j \neq i} \rho_{ij}$  for  $i \in [s]$ . Because  $\rho$  is doubly-stochastic and  $\rho_{ii} \geq 1 - \kappa$  for  $i \leq s$ , we see that

$$q = \sum_{i=1}^s q_i = \sum_{i=1}^s \sum_{j \neq i} \rho_{ij} = \sum_{i=1}^s 1 - \rho_{ii} \leq \kappa s. \quad (4.67)$$

In addition, let

$$t_i = \sum_{j > s} \rho_{ij}, \quad t = \sum_{i=1}^s t_i.$$

Since  $\rho$  is doubly-stochastic, we have

$$t = \sum_{i=1}^s \sum_{j > s} \rho_{ij} = \sum_{i > s} \sum_{j=1}^s \rho_{ij}. \quad (4.68)$$

We are going to compare  $f(\rho)$  with  $f(\text{id})$ , where  $\text{id}$  is the identity matrix (with ones on the diagonal and zeros elsewhere).

**Claim 4.21.** *With  $\mathcal{H} = \frac{1}{k} \sum_{i=1}^s h(\rho_{ii})$  we have  $H(k^{-1}\rho) \leq \ln k + \mathcal{H} + \frac{q}{k} \ln k + 0.51(k - s) \frac{\ln k}{k}$ .*

*Proof.* Corollary 4.10 implies together with the concavity of  $h$  that

$$\begin{aligned} \frac{1}{k} \sum_{i=1}^s H(\rho_i) &\leq \frac{1}{k} \sum_{i=1}^s h(\rho_{ii}) + q_i h(t_i/q_i) + t_i \ln(k - s) + (q_i - t_i) \ln s \\ &\leq \mathcal{H} + \frac{q}{k} h(t/q) + \frac{t}{k} \ln(k - s) + \frac{q - t}{k} \ln(s) \\ &\leq \mathcal{H} + \frac{t}{k} (1 - \ln t + \ln q) + \frac{t}{k} \ln(k - s) + \frac{q - t}{k} \ln(s) \quad [\text{as } h(z) \leq z(1 - \ln z)]. \end{aligned} \quad (4.69)$$

Because  $-z \ln z \leq 1$  for all  $z > 0$ , we have  $-\frac{t}{k} \ln t \leq 1/k$ . Moreover, as  $\rho$  is doubly-stochastic (4.68) implies that  $t \leq k - s$ . Additionally, (4.67) shows that  $q \leq \kappa s \leq \kappa k = \tilde{O}_k(1)$ , because  $\kappa = \ln^{20} k/k$ . Thus,

$$\frac{t}{k} (1 - \ln t + \ln q) \leq \frac{k - s}{k} \cdot O_k(\ln \ln k).$$

Plugging this last estimate into (4.69), we obtain

$$\frac{1}{k} \sum_{i=1}^s H(\rho_i) \leq \mathcal{H} + \frac{t}{k} \ln(k - s) + \frac{q - t}{k} \ln(s) + \frac{k - s}{k} \cdot O_k(\ln \ln k). \quad (4.70)$$



Furthermore, using Corollary 4.10, (4.68) and the concavity of  $h$ , we see that

$$\begin{aligned}
\frac{1}{k} \sum_{i>s} H(\rho_i) &\leq \frac{1}{k} \sum_{i>s} h \left( \sum_{j=1}^s \rho_{ij} \right) + \sum_{j=1}^s \rho_{ij} \ln(s) + \left( 1 - \sum_{j=1}^s \rho_{ij} \right) \ln(k-s) \\
&\leq \frac{k-s}{k} h \left( \frac{t}{k-s} \right) + \frac{t}{k} \ln s + \frac{k-s-t}{k} \ln(k-s) \\
&\leq \frac{k-s}{k} \ln 2 + \frac{t}{k} \ln s + \frac{k-s-t}{k} \ln(k-s) \quad [\text{as } h(z) \leq \ln 2 \text{ for all } z].
\end{aligned} \tag{4.71}$$

Plugging (4.70) and (4.71) into (4.4), we find

$$\begin{aligned}
H(k^{-1}\rho) &\leq \ln k + \mathcal{H} + \frac{q}{k} \ln k + \frac{k-s}{k} \ln(k-s) + \frac{k-s}{k} \cdot O_k(\ln \ln k) \\
&\leq \ln k + \mathcal{H} + \frac{q}{k} \ln k + \frac{k-s}{2k} \ln k + \frac{k-s}{k} \cdot O_k(\ln \ln k) \quad [\text{as } k-s \leq \sqrt{k}] \\
&\leq \ln k + \mathcal{H} + \frac{q}{k} \ln k + 0.51(k-s) \frac{\ln k}{k},
\end{aligned} \tag{4.72}$$

as claimed.  $\square$

**Claim 4.22.** We have  $E(\rho) \leq E(\text{id}) + (1 + \tilde{O}_k(1/k)) \frac{\ln k}{k} (-0.85(k-s) + \sum_{i=1}^s (\rho_{ii}^2 - 1))$ .

*Proof.* The Frobenius norm of  $\rho$  can be estimated as follows. Since  $\rho_{ii} \geq 1 - \kappa$  for all  $i \leq s$  and  $\rho$  is stochastic, we have  $\rho_{ij} \leq \kappa$  for all  $i \leq s, j \neq i$ . Hence, the bound (4.67) implies together with the fact that a sum of squares is maximized by having the summands as unequal as possible that

$$\sum_{i=1}^s \|\rho_i\|_2^2 \leq \left\lceil \frac{q}{\kappa} \right\rceil \cdot \kappa^2 + \sum_{i=1}^s \rho_{ii}^2 \leq s\kappa^2 + \sum_{i=1}^s \rho_{ii}^2 \leq \tilde{O}_k(1/k) + \sum_{i=1}^s \rho_{ii}^2 \quad [\text{as } \kappa \leq \ln^{20} k/k]. \tag{4.73}$$

A similar argument applies to the remaining rows. More precisely, if  $i > s$  then  $\rho_{ij} \leq 0.15$  for all  $j$  by our initial assumption on  $\rho$ . Therefore,

$$\sum_{i>s} \|\rho_i\|_2^2 \leq \frac{k-s}{0.15} \cdot (0.15)^2 = 0.15(k-s). \tag{4.74}$$

Combining (4.73) and (4.74), we arrive at

$$\|\rho\|_2^2 \leq \sum_{i=1}^s \rho_{ii}^2 + 0.15(k-s) + \tilde{O}_k(1/k). \tag{4.75}$$

By comparison,  $\|\text{id}\|_2^2 = k$ . Thus, (4.75) yields  $\|\rho\|_2^2 - \|\text{id}\|_2^2 \leq -0.85(k-s) + \sum_{i=1}^s (\rho_{ii}^2 - 1) + \tilde{O}_k(1/k)$ . Combining this estimate with (4.6) completes the proof.  $\square$

Observing that  $H(k^{-1}\text{id}) = \ln k$  and using Claims 4.21 and 4.22, we obtain

$$\begin{aligned}
f(\rho) - f(\text{id}) &= H(k^{-1}\rho) - \ln k + E(\rho) - E(\text{id}) \\
&\leq \mathcal{H} + \frac{q}{k} \ln k - \frac{k-s}{3k} \ln k + (1 + \tilde{O}_k(1/k)) \frac{\ln k}{k} \sum_{i=1}^s (\rho_{ii}^2 - 1).
\end{aligned} \tag{4.76}$$

To complete the proof, let  $r_i = 1 - \rho_{ii}$  for  $i = 1, \dots, s$ . Then (4.67) shows that  $q = \sum_{i=1}^s r_i$ . Moreover,  $\mathcal{H} = \frac{1}{k} \sum_{i=1}^s h(r_i)$ , as  $h(1-z) = h(z)$  for all  $z$ . Since  $r_i \leq \kappa = \tilde{O}_k(1/k)$ , we have

$$\begin{aligned}
\mathcal{H} + \frac{q}{k} \ln k + \frac{\ln k}{k} \sum_{i=1}^s (\rho_{ii}^2 - 1) &= \frac{1}{k} \sum_{i=1}^s [h(r_i) + r_i \ln k + ((1-r_i)^2 - 1) \ln k] \\
&= \frac{1}{k} \sum_{i=1}^s [h(r_i) + r_i \ln k + (r_i^2 - 2r_i) \ln k] \\
&\leq \tilde{O}_k(1/k^2) + \frac{1}{k} \sum_{i=1}^s h(r_i) - r_i \ln k \leq O_k(1/k) \quad [\text{by (4.3)}].
\end{aligned}$$

Plugging this bound into (4.76) and recalling that  $s \leq k - 1$ , we get

$$f(\rho) \leq -\frac{k-s}{3k} \ln k + O_k(1/k) + f(\text{id}) \leq f(\text{id}) - \frac{k-s}{3k} \ln k + O_k(1/k) < f(\text{id}). \quad (4.77)$$

Finally, we calculate  $f(\text{id}) = \ln k + \frac{d}{2} \ln(1 - 1/k) = \frac{1}{2}f(\bar{\rho})$ . Since  $f(\bar{\rho}) > 0$  (by Proposition 2.4), we conclude that  $f(\text{id}) < f(\bar{\rho})$ . Thus, the assertion follows from (4.77).

## 5. THE LAPLACE METHOD

In this section we keep the assumptions of Proposition 2.5 and the notation introduced in Section 2.

In this section we prove Proposition 4.1. Recalling that  $\mathcal{R} = \mathcal{R}_{n,k}$  is the (discrete) set of overlap matrices, let

$$Z_{\rho', \text{tame}} = |\{(\sigma, \tau) \in \mathcal{B} \times \mathcal{B} : \sigma, \tau \text{ are tame } k\text{-colorings of } G(n, m) \text{ and } \rho(\sigma, \tau) = \rho'\}| \quad \text{for } \rho' \in \mathcal{R}.$$

Then we can cast the second moment as

$$\mathbb{E}[Z_{k, \text{tame}}^2] = \sum_{\rho \in \mathcal{R}} \mathbb{E}[Z_{\rho, \text{tame}}]. \quad (5.1)$$

Because any tame  $k$ -coloring is balanced, Fact 2.2 yields

$$\mathbb{E}[Z_{\rho, \text{tame}}] \leq \mathbb{E}[Z_{\rho, \text{bal}}] \leq O(n^{(1-k^2)/2}) \cdot \exp(n \cdot f(\rho)) \quad \text{uniformly for } \rho \in \mathcal{R}. \quad (5.2)$$

By Taylor-expanding  $f$  around  $\bar{\rho}$ , we can estimate the contribution to the sum (5.1) resulting from  $\rho$  near  $\bar{\rho}$ .

**Lemma 5.1.** *There exist  $C = C(k) > 0$  and  $\eta = \eta(k) > 0$  such that with  $\mathcal{R}_0 = \{\rho \in \mathcal{R} : \|\rho - \bar{\rho}\|_2 < \eta\}$  we have*

$$\sum_{\rho \in \mathcal{R}_0} \mathbb{E}[Z_{\rho, \text{tame}}] \leq C \cdot \mathbb{E}[Z_{k, \text{tame}}]^2.$$

*Proof.* By construction, we have  $\sum_{i,j=1}^k \rho_{ij} = k$  for all  $\rho \in \mathcal{R}$ . Therefore, we can parameterize  $\mathcal{R}$  as follows. Let

$$\begin{aligned} \mathcal{L} : [0, 1]^{k^2-1} &\rightarrow [0, 1]^{k^2}, & \hat{\rho} = (\hat{\rho}_{ij})_{(i,j) \in [k]^2 \setminus \{(k,k)\}} &\mapsto \mathcal{L}(\hat{\rho}) = (\mathcal{L}_{ij}(\hat{\rho}))_{i,j \in [k]}, \text{ where} \\ \mathcal{L}_{ij}(\hat{\rho}) &= \hat{\rho}_{ij} \text{ for } (i,j) \neq (k,k) & \text{ and } \mathcal{L}_{kk}(\hat{\rho}) &= k - \sum_{(i,j) \neq (k,k)} \hat{\rho}_{ij}. \end{aligned}$$

Moreover, let  $\hat{\mathcal{R}} = \mathcal{L}^{-1}(\mathcal{R})$  and  $\tilde{\rho} = \mathcal{L}^{-1}(\bar{\rho})$ .

We compute the Hessian of  $f \circ \mathcal{L} = H \circ \mathcal{L} + E \circ \mathcal{L}$  at  $\tilde{\rho}$ . A direct calculation yields for  $(a, b) \neq (i, j)$

$$\frac{\partial}{\partial \hat{\rho}_{ij}} H \circ \mathcal{L}(\hat{\rho}) \Big|_{\hat{\rho}=\tilde{\rho}} = 0, \quad \frac{\partial^2}{\partial \hat{\rho}_{ij}^2} H \circ \mathcal{L}(\hat{\rho}) \Big|_{\hat{\rho}=\tilde{\rho}} = -2, \quad \frac{\partial^2}{\partial \hat{\rho}_{ij} \partial \hat{\rho}_{ab}} H \circ \mathcal{L}(\hat{\rho}) \Big|_{\hat{\rho}=\tilde{\rho}} = -1. \quad (5.3)$$

Furthermore,

$$\frac{\partial}{\partial \hat{\rho}_{ij}} \|\mathcal{L}(\hat{\rho})\|_2^2 \Big|_{\hat{\rho}=\tilde{\rho}} = 0, \quad \frac{\partial^2}{\partial \hat{\rho}_{ij}^2} \|\mathcal{L}(\hat{\rho})\|_2^2 \Big|_{\hat{\rho}=\tilde{\rho}} = 4, \quad \frac{\partial^2}{\partial \hat{\rho}_{ij} \partial \hat{\rho}_{ab}} \|\mathcal{L}(\hat{\rho})\|_2^2 \Big|_{\hat{\rho}=\tilde{\rho}} = 2.$$

Thus, by the chain rule

$$\frac{\partial}{\partial \hat{\rho}_{ij}} E \circ \mathcal{L}(\hat{\rho}) \Big|_{\hat{\rho}=\tilde{\rho}} = 0, \quad \frac{\partial^2}{\partial \hat{\rho}_{ij}^2} E \circ \mathcal{L}(\hat{\rho}) \Big|_{\hat{\rho}=\tilde{\rho}} = \frac{2d}{k^2(1-1/k)^2}, \quad \frac{\partial^2}{\partial \hat{\rho}_{ij} \partial \hat{\rho}_{ab}} E \circ \mathcal{L}(\hat{\rho}) = \frac{d}{k^2(1-1/k)^2}. \quad (5.4)$$

Combining (5.3) and (5.4), we see that the first derivative of  $f \circ \mathcal{L}$  at the point  $\tilde{\rho}$  vanishes, and that the Hessian is

$$D^2 f \circ \mathcal{L}(\hat{\rho}) \Big|_{\hat{\rho}=\tilde{\rho}} = - \left( 1 - \frac{d}{k^2(1-1/k)^2} \right) \cdot (\text{id} + \mathbf{1}), \quad (5.5)$$

where  $\mathbf{1}$  denotes the matrix with all entries equal to one and  $\text{id}$  is the identity matrix.

As  $\text{id}$  is positive definite,  $\mathbf{1}$  is positive semidefinite and  $d/(k^2(1-1/k)^2) = O_k(\ln k/k) < \frac{1}{2}$ , (5.5) shows that the Hessian is negative definite at  $\tilde{\rho}$ . In fact, by continuity there exist numbers  $\tilde{\eta}, \tilde{\xi} > 0$  independent of  $n$  such that the largest eigenvalue of  $D^2 f \circ \mathcal{L}$  is smaller than  $-\tilde{\xi}$  at all points  $\hat{\rho}$  such that  $\|\hat{\rho} - \tilde{\rho}\|_2 < \tilde{\eta}$ . Further, because  $\mathcal{L}$  is linear

there is an  $n$ -independent  $\eta > 0$  such that for all  $\rho \in \mathcal{R}_0 = \{\rho \in \mathcal{R} : \|\rho - \bar{\rho}\|_2 < \eta\}$  we have  $\|\mathcal{L}^{-1}(\rho) - \tilde{\rho}\|_2 < \tilde{\eta}$ . Hence, by Taylor's formula there is a number  $\xi > 0$  that does not depend on  $n$  such that

$$f \circ \mathcal{L}(\hat{\rho}) \leq f(\bar{\rho}) - \xi \sum_{(i,j) \neq (k,k)} (\hat{\rho}_{ij} - 1/k)^2 \quad \text{for all } \hat{\rho} \in \hat{\mathcal{R}}_0 = \mathcal{L}^{-1}(\mathcal{R}_0). \quad (5.6)$$

Combining (5.2) and (5.6), we obtain

$$\begin{aligned} \sum_{\rho \in \mathcal{R}_0} \mathbb{E}[Z_{\rho, \text{tame}}] &\leq \exp(f(\bar{\rho})n) \cdot O(n^{(1-k^2)/2}) \sum_{\hat{\rho} \in \hat{\mathcal{R}}_0} \exp \left[ -n \cdot \xi \sum_{(i,j) \neq (k,k)} (\hat{\rho}_{ij} - 1/k)^2 \right] \\ &\leq \exp(f(\bar{\rho})n) \cdot O(1) \int_{\mathbb{R}^{k^2-1}} \exp \left[ -\xi \sum_{(i,j) \neq (k,k)} (\hat{z}_{ij} - 1/k)^2 \right] d\hat{z} \\ &\leq \exp(f(\bar{\rho})n) \cdot O(1) \left[ \int_{-\infty}^{\infty} \exp[-\xi z^2] dz \right]^{k^2-1} = O(1) \cdot \exp(f(\bar{\rho})n). \end{aligned} \quad (5.7)$$

Finally, a direct calculation shows that  $f(\bar{\rho}) = 2(\ln k + \frac{d}{2} \ln(1 - 1/k))$ , whence  $\exp(f(\bar{\rho})n) = O(k^n(1 - 1/k)^m)^2$  (as  $m = \lceil dn/2 \rceil$ ). Thus, the assertion follows from Proposition 2.4 and (5.7).  $\square$

To estimate the contribution of  $\rho \notin \mathcal{R}_0$ , we decompose  $\mathcal{R} \setminus \mathcal{R}_0$  into three subsets:

$$\begin{aligned} \mathcal{R}_1 &= \{\rho \in \mathcal{R} \setminus \mathcal{R}_0 : \rho \text{ fails to be separable}\}, \\ \mathcal{R}_2 &= \{\rho \in \mathcal{R} \setminus (\mathcal{R}_0 \cup \mathcal{R}_1) : \text{for each } i \text{ there is } j \text{ such that } \rho_{ij} > 0.51\}, \\ \mathcal{R}_3 &= \mathcal{R} \setminus (\mathcal{R}_0 \cup \mathcal{R}_1 \cup \mathcal{R}_2). \end{aligned}$$

Condition **T2** from Definition 2.3 directly implies that

$$\mathbb{E}[Z_{\rho, \text{tame}}] = 0 \quad \text{for all } \rho \in \mathcal{R}_1. \quad (5.8)$$

With respect to  $\mathcal{R}_2$ , we have

**Lemma 5.2.** *There is a number  $C = C(k) > 0$  such that  $\sum_{\rho \in \mathcal{R}_2} \mathbb{E}[Z_{\rho, \text{tame}}] \leq C \cdot \mathbb{E}[Z_{k, \text{tame}}]^2$ .*

*Proof.* Let  $\mathcal{R}'_2$  be the set of all  $k$ -stable  $\rho' \in \mathcal{R}$  (i.e.,  $\rho'_{ii} > 0.51$  for all  $i \in [k]$ ). Because we restrict ourselves to balanced  $k$ -colorings, the row and column sums of each matrix  $\rho \in \mathcal{R}$  are  $1 + O(n^{-1/2})$ . Hence, for any matrix  $\rho \in \mathcal{R}$  there is at most one entry greater than 0.51 in each row or column. Thus, suppose that  $\sigma, \tau$  are tame  $k$ -colorings of  $G(n, m)$  such that  $\rho(\sigma, \tau) \in \mathcal{R}_2$ . Then each row and each column of  $\rho(\sigma, \tau)$  have *exactly* one entry that is greater than 0.51. Therefore, there exists a permutation  $\pi : [k] \rightarrow [k]$  such that  $\sigma, \pi \circ \tau$  are two colorings such that  $\rho(\sigma, \pi \circ \tau) \in \mathcal{R}'_2$ . Consequently,

$$\sum_{\rho \in \mathcal{R}_2} \mathbb{E}[Z_{\rho, \text{tame}}] \leq k! \sum_{\rho \in \mathcal{R}'_2} \mathbb{E}[Z_{\rho, \text{tame}}]. \quad (5.9)$$

Further, if  $\sigma, \tau$  are  $k$ -colorings such that  $\rho(\sigma, \tau) \in \mathcal{R}'_2$ , then  $\tau \in \mathcal{C}(\sigma)$  by the very definition of the cluster  $\mathcal{C}(\sigma)$ . Therefore, by the linearity of expectation and Bayes' formula, we have

$$\sum_{\rho \in \mathcal{R}'_2} \mathbb{E}[Z_{\rho, \text{tame}}] = \sum_{\sigma \in \mathcal{B}} \mathbb{E}[\mathcal{C}(\sigma) | \sigma \text{ is a tame } k\text{-coloring}] \cdot \mathbb{P}[\sigma \text{ is a tame } k\text{-coloring}] \quad (5.10)$$

Now, if  $\sigma$  is a tame  $k$ -coloring, then by **T3** we know that  $\mathcal{C}(\sigma) \leq \mathbb{E}[Z_{k, \text{bal}}]$  with certainty. Thus, (5.9) yields

$$\begin{aligned} \sum_{\rho \in \mathcal{R}'_2} \mathbb{E}[Z_{\rho, \text{tame}}] &\leq \mathbb{E}[Z_{k, \text{bal}}] \sum_{\sigma \in \mathcal{B}} \mathbb{P}[\sigma \text{ is a tame } k\text{-coloring}] \leq \mathbb{E}[Z_{k, \text{bal}}] \cdot \mathbb{E}[Z_{k, \text{tame}}] \\ &\leq (1 + o(1)) \mathbb{E}[Z_{k, \text{tame}}]^2 \quad [\text{by Proposition 2.4}]. \end{aligned} \quad (5.11)$$

Combining (5.9) and (5.11), we get  $\sum_{\rho \in \mathcal{R}_2} \mathbb{E}[Z_{\rho, \text{tame}}] \leq O(\mathbb{E}[Z_{k, \text{tame}}]^2)$ , as claimed.  $\square$

To bound the contribution of  $\rho \in \mathcal{R}_3$ , we need the following observation.

**Lemma 5.3.** *There is a number  $C = C(k) > 0$  such that for any  $\rho \in \mathcal{R}$  there is  $\rho' \in \mathcal{D}$  with  $\|\rho - \rho'\|_2 < C/\sqrt{n}$ .*

*Proof.* Let  $\rho \in \mathcal{R}$ . By construction, we have  $\sum_{i,j} \rho_{ij} = k$ . Hence, while there is  $i \in [k]$  such that the row sum is  $\sum_j \rho_{ij} = 1 + \alpha > 1$ , there must be another row  $l$  such that  $\sum_j \rho_{lj} = 1 - \alpha' < 1$ . Thus, by replacing row  $i$  by  $(1 - \alpha'')\rho_i$  and row  $l$  by  $\rho_l + \alpha''\rho_i$  for some suitable  $\alpha'' \leq 2k/\sqrt{n}$ , we can ensure that at least one of the row sums is one. After at most  $k - 1$  steps, we thus obtain a stochastic matrix  $\rho''$  such that  $\|\rho - \rho''\|_2 = 2k^3/\sqrt{n}$ . Repeating the same operation for the columns yields the desired doubly-stochastic  $\rho'$ .  $\square$

**Lemma 5.4.** *If  $f(\rho) < f(\bar{\rho})$  for any  $\rho \in \mathcal{D}_{\text{tame}} \setminus \{\bar{\rho}\}$ , then  $\sum_{\rho \in \mathcal{R}_3} \mathbb{E}[Z_{\rho, \text{tame}}] \leq \mathbb{E}[Z_{k, \text{tame}}]^2$ .*

*Proof.* Let  $\eta > 0$  be the number from Lemma 5.1 and let  $\mathcal{D}'$  be the set of all  $\rho \in \mathcal{D}_{\text{tame}}$  such that  $\|\rho - \bar{\rho}\|_2 \geq \eta/2$ . The set  $\mathcal{D}'$  is compact. Hence, our assumption that  $f(\rho) < f(\bar{\rho})$  for any  $\rho \in \mathcal{D}_{\text{tame}} \setminus \{\bar{\rho}\}$  implies that there exists a number  $\gamma > 0$  (independent of  $n$ ) such that

$$\max_{\rho \in \mathcal{D}'} f(\rho) < f(\bar{\rho}) - \gamma. \quad (5.12)$$

In fact, because the function  $f$  is uniformly continuous on  $[0, 1]^{k^2}$ , there is  $0 < \delta < \eta/3$  such that

$$\max_{\rho \in \mathcal{D}''} f(\rho) < f(\bar{\rho}) - \gamma/2, \quad \text{where } \mathcal{D}'' = \{\rho \in [0, 1]^{k^2} : \text{there is } \rho' \in \mathcal{D}' \text{ with } \|\rho - \rho'\|_2 < \delta\}. \quad (5.13)$$

We claim that  $\mathcal{R}_3 \subset \mathcal{D}''$ . Indeed, any  $\rho \in \mathcal{R}_3$  satisfies  $\|\rho - \bar{\rho}\|_2 \geq \eta$  (as otherwise  $\rho \in \mathcal{R}_0$ ), is separable (as otherwise  $\rho \in \mathcal{R}_1$ ), and is not stable (as otherwise  $\rho \in \mathcal{R}_2$ ). Moreover, by Lemma 5.3 there is a doubly-stochastic  $\rho'$  such that  $\|\rho - \rho'\|_2 < C/\sqrt{n}$ . However, this matrix  $\rho'$  may or may not be separable and/or stable. To rectify this, we form a convex combination between  $\rho'$  and a suitable doubly-stochastic matrix. More precisely, suppose that the matrix  $\rho$  has precisely  $l < k - 1$  entries that are greater than 0.51. Each row and each column contain at most one such entry (as  $\rho \in \mathcal{B}$ ). Thus, we may assume without loss of generality that  $\rho_{11}, \dots, \rho_{ll} > 0.51$ . Now, let  $\rho''$  be the doubly-stochastic matrix with  $\rho''_{11} = \dots = \rho''_{ll} = 1$  and  $\rho''_{ij} = (k - l)^{-1}$  for  $i, j > l$ . If  $\beta > 0$  is a small enough number, then  $\rho''' = (1 - \beta)\rho' + \beta\rho'' \in \mathcal{D}'$  and  $\|\rho - \rho'''\|_2 < \delta$ . Thus,  $\rho \in \mathcal{D}''$ .

As  $\mathcal{R}_3 \subset \mathcal{D}''$ , (5.13) yields

$$\max_{\rho \in \mathcal{R}_3} f(\rho) < f(\bar{\rho}) - \gamma/2. \quad (5.14)$$

Thus, (5.2) implies

$$\begin{aligned} \sum_{\rho \in \mathcal{R}_3} \mathbb{E}[Z_{\rho, \text{tame}}] &\leq |\mathcal{R}_3| \exp(n(f(\bar{\rho}) - \gamma/2)) \leq |\mathcal{R}| \exp(n(f(\bar{\rho}) - \gamma/2)) \\ &\leq n^{k^2} \exp(n(f(\bar{\rho}) - \gamma/2)) \leq \exp(n(f(\bar{\rho}) - \gamma/3)). \end{aligned} \quad (5.15)$$

Upon direct inspection, we find  $f(\bar{\rho}) = 2(\ln k + \frac{d}{2} \ln(1 - 1/k))$ . Recalling that  $m = \lceil dn/2 \rceil$ , we thus obtain from Proposition 2.4

$$\exp(n(f(\bar{\rho}) - \gamma/3)) \leq \mathbb{E}[Z_{k, \text{tame}}]^2 \cdot \exp(-\gamma n/4). \quad (5.16)$$

Combining (5.15) and (5.16), we obtain

$$\sum_{\rho \in \mathcal{R}_3} \mathbb{E}[Z_{\rho, \text{tame}}] = \mathbb{E}[Z_{k, \text{tame}}]^2 \cdot n^{k^2} \exp(-\gamma n/4) \leq \mathbb{E}[Z_{k, \text{tame}}]^2,$$

thereby completing the proof.  $\square$

Finally, Proposition 4.1 follows from (5.8) and Lemmas 5.1, 5.2 and 5.4.

## REFERENCES

- [1] D. Achlioptas, E. Friedgut: A sharp threshold for  $k$ -colorability. *Random Struct. Algorithms* **14** (1999) 63–70.
- [2] D. Achlioptas, A. Coja-Oghlan: Algorithmic barriers from phase transitions. *Proc. 49th FOCS* (2008) 793–802.
- [3] D. Achlioptas, M. Molloy: The analysis of a list-coloring algorithm on a random graph. *Proc. 38th FOCS* (1997) 204–212.
- [4] D. Achlioptas, C. Moore: The chromatic number of random regular graphs. *Proc. 8th RANDOM* (2004) 219–228.
- [5] D. Achlioptas, C. Moore: Random  $k$ -SAT: two moments suffice to cross a sharp threshold. *SIAM Journal on Computing* **36** (2006) 740–762.
- [6] D. Achlioptas, A. Naor: The two possible values of the chromatic number of a random graph. *Annals of Mathematics* **162** (2005), 1333–1349.
- [7] N. Alon, N. A. Kahale, A spectral technique for coloring random 3-colorable graphs. *SIAM J. Comput.* **26** (1997) 1733–1748.
- [8] N. Alon, M. Krivelevich: The concentration of the chromatic number of random graphs. *Combinatorica* **17** (1997) 303–313.
- [9] K. Appel, W. Haken: Every planar map is four colorable. *Illinois Journal of Mathematics* **21** (1977) 429–567.
- [10] V. Bapst, A. Coja-Oghlan, S. Hetterich, F. Raßmann, D. Vilenchik: The condensation transition in random graph coloring. *arXiv:1404.5513* (2014).

- [11] B. Bollobás: The chromatic number of random graphs. *Combinatorica* **8** (1988) 49–55
- [12] B. Bollobás: Random graphs. 2nd edition. Cambridge University Press (2001)
- [13] B. Bollobás, C. Borgs, J. Chayes, J.-H. Kim, D. Wilson: The scaling window of the 2-SAT transition. *Random Struct. Algorithms* **18** (2001) 201–256.
- [14] A. Coja-Oghlan: Upper-bounding the  $k$ -colorability threshold by counting covers. *Electronic Journal of Combinatorics* **20** (2013) P32.
- [15] A. Coja-Oghlan, S. Hetterich, C. Efthymiou: On the chromatic number of random regular graphs. arXiv:1308.4287 (2013).
- [16] A. Coja-Oghlan, K. Panagiotou: Catching the  $k$ -NAESAT threshold. *Proc. 44th STOC* (2012) 899–908.
- [17] A. Coja-Oghlan, K. Panagiotou: Going after the  $k$ -SAT threshold. *Proc. 45th STOC* (2013), to appear.
- [18] A. Coja-Oghlan, L. Zdeborová: The condensation transition in random hypergraph 2-coloring. *Proc. 23rd SODA* (2012) 241–250.
- [19] V. Dani, C. Moore, A. Olson: Tight bounds on the threshold for permuted  $k$ -colorability. *Proc. 16th RANDOM* (2012) 505–516.
- [20] M. Dyer, A. Frieze, C. Greenhill: On the chromatic number of a random hypergraph. Preprint (2012).
- [21] P. Erdős, A. Rényi: On the evolution of random graphs. *Magyar Tud. Akad. Mat. Kutató Int. Kozl.* **5** (1960) 17–61.
- [22] A. Frieze, C. McDiarmid: Algorithmic theory of random graphs. *Random Struct. Algorithms* **10** (1997) 5–42
- [23] A. Frieze, N. Wormald: Random  $k$ -Sat: a tight threshold for moderately growing  $k$ . *Combinatorica* **25** (2005) 297–305.
- [24] E. Gilbert: Random graphs. *Annals Math. Statist.* **30** (1959) 1141–1144.
- [25] G. Grimmett, C. McDiarmid: On colouring random graphs. *Mathematical Proceedings of the Cambridge Philosophical Society* **77** (1975) 313–324
- [26] S. Janson, T. Łuczak, A. Ruciński: *Random Graphs*, Wiley 2000.
- [27] G. Kemkes, X. Pérez-Giménez, N. Wormald: On the chromatic number of random  $d$ -regular graphs. *Advances in Mathematics* **223** (2010) 300–328.
- [28] M. Krivelevich: Coloring random graphs – an algorithmic perspective. *Proc. 2nd Colloquium on Mathematics and Computer Science* (2002) 175–195.
- [29] M. Krivelevich, B. Sudakov: Coloring random graphs. *Information Processing Letters* **67** (1998) 71–74
- [30] F. Krzakala, A. Montanari, F. Ricci-Tersenghi, G. Semerjian, L. Zdeborová: Gibbs states and the set of solutions of random constraint satisfaction problems. *Proc. National Academy of Sciences* **104** (2007) 10318–10323.
- [31] F. Krzakala, A. Pagnani, M. Weigt: Threshold values, stability analysis and high- $q$  asymptotics for the coloring problem on random graphs. *Phys. Rev. E* **70** (2004) 046705.
- [32] T. Łuczak: The chromatic number of random graphs. *Combinatorica* **11** (1991) 45–54
- [33] T. Łuczak: A note on the sharp concentration of the chromatic number of random graphs. *Combinatorica* **11** (1991) 295–297
- [34] D. Matula: Expose-and-merge exploration and the chromatic number of a random graph. *Combinatorica* **7** (1987) 275–284.
- [35] M. Mézard, A. Montanari: *Information, physics and computation*. Oxford University Press 2009.
- [36] M. Mézard, G. Parisi, R. Zecchina: Analytic and algorithmic solution of random satisfiability problems. *Science* **297** (2002) 812–815.
- [37] M. Molloy: The freezing threshold for  $k$ -colourings of a random graph. *Proc. 43rd STOC* (2012) 921–930.
- [38] R. Mulet, A. Pagnani, M. Weigt, R. Zecchina: Coloring random graphs. *Phys. Rev. Lett.* **89** (2002) 268701
- [39] J. van Mourik, D. Saad: Random Graph Coloring - a Statistical Physics Approach. *Phys. Rev. E* **66** (2002) 056120.
- [40] N. Robertson, D. Sanders, P. Seymour, R. Thomas: The four-colour theorem. *J. Combin. Theory Ser. B* **70** (1997) 2–44.
- [41] E. Shamir, J. Spencer: Sharp concentration of the chromatic number of random graphs  $G(n, p)$ . *Combinatorica* **7** (1987) 121–129
- [42] L. Zdeborová, F. Krzakala: Phase transition in the coloring of random graphs. *Phys. Rev. E* **76** (2007) 031131.

## APPENDIX A. PROOF OF LEMMA 3.2

Throughout this section, we assume that  $2k \ln k - \ln k - 2 \leq d \leq 2k \ln k$ . In addition, we fix some  $\sigma \in \mathcal{B}$  and we let  $V_i = \sigma^{-1}(i)$  for  $i = 1, \dots, n$ .

To simplify the calculations we consider the following variant of the planted model. Given  $\sigma$ ,  $n$  and  $q \in (0, 1)$ , we let  $\mathcal{G}(n, q, \sigma)$  be the random graph in which any two vertices  $v, w$  with  $\sigma(v) \neq \sigma(w)$  are adjacent with probability  $p$  independently. The following observation relates this model to the planted model  $G(n, m, \sigma)$  from Lemma 3.2.

**Fact A.1.** *Given  $\sigma \in \mathcal{B}$ , let  $p$  be such that the expected number of edges in  $\mathcal{G}(n, p, \sigma)$  is equal to  $m = \lceil dn/2 \rceil$ . There is a number  $C = C(k) > 0$  such that*

$$\mathbb{P}[G(n, m, \sigma) \in \mathcal{A}] \leq C\sqrt{n} \cdot \mathbb{P}[\mathcal{G}(n, p, \sigma) \in \mathcal{A}] \quad \text{for any event } \mathcal{A}.$$

*Proof.* By the choice of  $p$ , the number  $e(\mathcal{G}(n, p, \sigma))$  of edges of the random graph  $\mathcal{G}(n, p, \sigma)$  has a binomial distribution with mean

$$p \left[ \binom{n}{2} - \sum_{i=1}^k \binom{|V_i|}{2} \right] = m. \tag{A.1}$$

Hence, Stirling’s formula shows that for some number  $C = C(k) > 0$  we have  $\mathbb{P}[e(\mathcal{G}(n, p, \sigma)) = m] \geq (C\sqrt{n})^{-1}$ . Further, given that  $e(\mathcal{G}(n, p, \sigma)) = m$ , the distribution of the random graph  $\mathcal{G}(n, p, \sigma)$  is identical to that of  $G(n, m, \sigma)$ .



Thus, for any event  $\mathcal{A}$

$$\mathbb{P}[G(n, m, \sigma) \in \mathcal{A}] \leq \frac{\mathbb{P}[\mathcal{G}(n, p, \sigma) \in \mathcal{A}]}{\mathbb{P}[e(\mathcal{G}(n, p, \sigma)) = m]} \leq C\sqrt{n} \cdot \mathbb{P}[\mathcal{G}(n, p, \sigma) \in \mathcal{A}],$$

as claimed.  $\square$

From here on out, we fix  $\sigma \in \mathcal{B}$  and choose  $p \in (0, 1)$  such that the expected number of edges in  $\mathcal{G}(n, p, \sigma)$  is equal to  $m$ ; because  $\sigma$  is balanced, (A.1) implies that

$$p \sim \frac{k}{k-1} \cdot \frac{d}{n}. \quad (\text{A.2})$$

In the following, we are going to show that the properties **P1–P4** are satisfied in  $\mathcal{G}(n, p, \sigma)$  with probability  $1 - O(1/n)$ . Then Fact A.1 readily implies that they hold in  $G(n, m, \sigma)$  w.h.p.

The following instalment of the Chernoff bound will prove useful.

**Lemma A.2** ([26]). *Let  $\varphi(x) = (1+x)\ln(1+x) - x$ . Let  $X$  be a binomial random variable with mean  $\mu > 0$ . Then for any  $t > 0$ ,*

$$\mathbb{P}[X > \mathbb{E}[X] + t] \leq \exp(-\mu \cdot \varphi(t/\mu)), \quad \mathbb{P}[X < \mathbb{E}[X] - t] \leq \exp(-\mu \cdot \varphi(-t/\mu)).$$

In particular, for any  $t > 1$  we have  $\mathbb{P}[X > t\mu] \leq \exp[-t\mu \ln(t/e)]$ .

**A.1. Proof of P1.** We may assume  $i = 1$  without loss of generality. Let  $0.509 \leq \alpha \leq 1 - k^{-0.499}$  and let  $S \subset V_1$  be a set of size  $|S| = \alpha n/k$ . Because in  $\mathcal{G}(n, p, \sigma)$  edges occur independently, for any  $v \in V \setminus V_1$  the number of neighbors of  $v$  in  $S$  has distribution  $\text{Bin}(\alpha n/k, p)$ . Hence, as  $\sigma$  is balanced the number  $X_S$  of  $v \in V \setminus V_1$  with no neighbor in  $S$  has a binomial distribution with mean  $n(1 - 1/k + o(1))(1 - p)^{\alpha n/k}$ . Our assumption on  $d$  and (A.2) imply that  $(1 - p)^{\alpha n/k} \leq \exp[-\alpha np/k] \leq 2k^{-2\alpha}$ . Thus,

$$\mathbb{E}[X_S] \leq (1 + o(1))n(1 - 1/k) \cdot 2k^{-2\alpha}. \quad (\text{A.3})$$

Consequently, by Lemma A.2

$$\mathbb{P}\left[X_S \geq (1 - \alpha)n/k - n^{2/3}\right] \leq \exp\left[-(1 - \alpha + o(1))\frac{n}{k} \cdot \ln\left(\frac{1 - \alpha}{2e} \cdot k^{2\alpha-1}\right)\right]. \quad (\text{A.4})$$

By comparison, because  $\sigma$  is balanced, for a given  $\alpha$  the number of ways to choose  $S$  is

$$\binom{(1 + o(1))n/k}{(1 - \alpha + o(1))n/k} \leq \left(\frac{e}{1 - \alpha}\right)^{(1 - \alpha + o(1))\frac{n}{k}} = \exp\left[\frac{n}{k}(1 - \alpha + o(1))(1 - \ln(1 - \alpha))\right]. \quad (\text{A.5})$$

Let us call  $S$   $\alpha$ -bad if  $X_S \geq (1 - \alpha)\frac{n}{k} - n^{2/3}$ . Combining (A.3), (A.4) and (A.5) and taking the union bound over  $S \subset V_1$  with  $|S| = \alpha n/k$ , we obtain

$$\mathbb{P}[\text{there is an } \alpha\text{-bad } S] \leq \exp\left[\frac{(1 - \alpha)n}{k} \cdot \left(1 - \ln(1 - \alpha) - \ln\left(\frac{1 - \alpha}{2e} \cdot k^{2\alpha-1}\right)\right) + o(n)\right].$$

To complete the proof of **P1**, we are going to show that the right hand side is  $\exp(-\Omega(n))$ .

Thus, we need to estimate

$$1 - \ln(1 - \alpha) - \ln\left(\frac{1 - \alpha}{2e} \cdot k^{2\alpha-1}\right) = \ln\left(\frac{2e^2}{(1 - \alpha)^2} k^{1-2\alpha}\right).$$

This is negative iff

$$\exp\left[\left(\frac{1}{2} - \alpha\right) \ln k\right] < \frac{1 - \alpha}{\sqrt{2e}}. \quad (\text{A.6})$$

By convexity, the exponential function on the l.h.s. and the linear function on the r.h.s. intersect at most twice, and between these two intersections the linear function is greater. Further, an explicit calculation verifies that the r.h.s. of (A.6) is larger than the l.h.s. at both  $\alpha = 0.509$  and  $\alpha = 1 - k^{-0.499}$ . Thus, (A.6) is true in the entire range  $0.509 < \alpha < 1 - k^{-0.499}$ .  $\square$

**A.2. Proof of P2.** In  $\mathcal{G}(n, p, \sigma)$ , for each vertex  $v \in V \setminus V_i$  the number of neighbors of  $v$  in  $V_i$  has distribution  $\text{Bin}(|V_i|, p)$ . Due to (A.2) and because  $\sigma$  is balanced, the mean is  $\lambda = |V_i|p \sim \frac{n}{k}p > 2 \ln k$ . Hence, by Stirling's formula the probability that  $v$  has fewer than 15 neighbors in  $V_i$  is  $q \leq 2\lambda^{14} \exp(-\lambda) \leq 2k^{-2} \ln^{14} k$ . Further, because the event of having fewer than 15 neighbors in  $V_i$  occurs independently for all  $v \in V \setminus V_i$ , the total number  $Y_i$  of such vertices has a binomial distribution  $\text{Bin}(|V \setminus V_i|, q)$ . As  $\sigma$  is balanced, the mean is  $|V \setminus V_i|q \leq (1 - 1/k + o(1))n \cdot q \leq 3k^{-2} \ln^{14} k$ . Since we chose  $\kappa = k^{-1} \ln^{20} k$ , a straightforward application of Lemma A.2 (the Chernoff bound) implies that  $\mathbb{P}[Y_i > \frac{\kappa n}{3k}] \leq \exp(-\Omega(n))$ , as desired.  $\square$

**A.3. Proof of P3.** Let  $0 < \alpha < k^{-4/3}$  and let  $S \subset V$  of size  $|S| = \alpha n$ . The number  $e(S)$  of edges spanned by  $S$  in  $\mathcal{G}(n, p, \sigma)$  is stochastically dominated by a random variable with distribution  $\text{Bin}(\binom{\alpha n}{2}, p)$ . For any two vertices  $v, w \in S$  are connected with probability at most  $p$  in  $\mathcal{G}(n, p, \sigma)$  (as the probability is exactly  $p$  if  $\sigma(v) \neq \sigma(w)$  and 0 otherwise). Thus,

$$\mathbb{P}[e(S) \geq 5|S|] \leq \mathbb{P}\left[\text{Bin}\left(\binom{\alpha n}{2}, p\right) \geq 5\alpha n\right] \leq \left(\frac{\binom{\alpha n}{2}}{5\alpha n}\right)^{5\alpha n}.$$

Now, let  $X_\alpha$  be the number of sets  $S$  of size  $|S| = \alpha n$  such that  $e(S) \geq 5|S|$ . Let  $d' = pn \sim \frac{dk}{k-1}$ . By the union bound,

$$\mathbb{P}[X_\alpha > 0] \leq \binom{n}{\alpha n} \left(\frac{\binom{\alpha n}{2}}{5\alpha n}\right)^{5\alpha n} \leq \left(\frac{e}{\alpha}\right)^{\alpha n} \left(\frac{e\alpha d'}{10}\right)^{5\alpha n} \leq \left[e \left(\frac{ed'}{10}\right)^5 \alpha^4\right]^{\alpha n}. \quad (\text{A.7})$$

Further, let  $X = \sum_\alpha X_\alpha$ , where the sum ranges over  $0 < \alpha < k^{-4/3}$  such that  $\alpha n$  is an integer. Then (A.7) implies together with the assumption that  $\alpha < k^{-4/3}$  that

$$\mathbb{P}[X > 0] \leq \sum_\alpha \left[e \left(\frac{ed'}{10}\right)^5 \alpha^4\right]^{\alpha n} = O(1/n).$$

Thus, the probability that there is a set violating **P3** is  $O(1/n)$ .  $\square$

**A.4. Proof of P4.** We start by estimating the size of the core; the proof of the following proposition draws on arguments developed in [2, 7].

**Proposition A.3.** *With probability  $1 - \exp(-\Omega(n))$ , the core of  $\mathcal{G}(n, p, \sigma)$  contains  $(1 - \tilde{O}_k(k^{-1}))n$  vertices.*

The proof of Proposition A.3 is constructive: basically, we iteratively remove vertices of that have too few neighbors of some color other than their own among the remaining vertices. More precisely, we consider the following process. For a vertex  $v$  and a set  $S$  of vertices let  $e(v, S)$  denote the number of neighbors of  $v$  in  $S$  in  $\mathcal{G}(n, p, \sigma)$ .

**CR1:** For  $i, j \in [k]$ ,  $i \neq j$ , let  $W_{ij} = \{v \in V_i : e(v, V_j) < 300\}$ ,  $W_{ii} = \emptyset$ ,  $W_i = \bigcup_{j=1}^k W_{ij}$ , and  $W = \bigcup_{i=1}^k W_i$ .

**CR2:** For  $i \neq j$ , let  $U_{ij} = \{v \in V_i : e(v, W_j) > 100\}$  and  $U = \bigcup_{i \neq j} U_{ij}$ .

**CR3:** Set  $Z^{(0)} = U$  and repeat the following for  $i \geq 0$ :

- if there is  $v \in V \setminus Z^{(i)}$  such that  $e(v, Z^{(i)}) \geq 100$ , pick one such  $v$  and let  $Z^{(i+1)} = Z^{(i)} \cup \{v\}$ ;
- otherwise, let  $Z^{(i+1)} = Z^{(i)} \cup \{v\}$ .

Let  $Z = \bigcup_{i \geq 0} Z^{(i)}$  be the final set resulting from **CR3**. By construction, the set  $V \setminus (W \cup Z)$  is contained in the core. To complete the proof of Proposition A.3, we bound the sizes of  $W$ ,  $U$  and  $Z$  (Lemmas A.4, A.5 and A.6).

**Lemma A.4.** *With probability at least  $1 - \exp(-\Omega(n))$  we have  $|W_{ij}| \leq \tilde{O}_k(k^{-3})$  for any  $i, j$ .*

*Proof.* Fix  $i, j$ ,  $i \neq j$ . Due to the independence of the edges in  $\mathcal{G}(n, p, \sigma)$ , for any  $v \in V_i$  the number  $e(v, V_j)$  of neighbors in  $V_j$  has distribution  $\text{Bin}(|V_j|, p)$ . As  $\sigma$  is balanced, (A.2) shows that the mean is  $\mu = |V_j|p \geq 2 \ln k$ . Using the Chernoff bound (Lemma A.2), we obtain  $\mathbb{P}[|e(v, V_j)| \leq 300] \leq \exp(-2 \ln k + O_k(\ln \ln k)) = \tilde{O}_k(k^{-2})$ . Hence, by the linearity of expectation and because  $\sigma$  is balanced,  $\mathbb{E}[|W_{ij}|] \leq \tilde{O}_k(k^{-2}) \cdot |V_i| = n \cdot \tilde{O}_k(k^{-3})$ . Further, once more due to the independence of the edges in  $\mathcal{G}(n, p, \sigma)$ ,  $|W_{ij}|$  is a binomial random variable. Thus, using the Chernoff bound once more (with, say,  $t = k^{-4}n$ ), we see that  $\mathbb{P}[|W_{ij}| \leq \tilde{O}_k(k^{-3})n] \geq 1 - \exp(-\Omega(n))$ , as required.  $\square$

**Lemma A.5.** *With probability at least  $1 - \exp(-\Omega(n))$  we have  $|U| \leq n/k^{30}$ .*

*Proof.* We define two sets whose union contains  $U_{ij}$ :

$$U'_{ij} = \{v \in V_i : e(v, W_j \setminus W_{ji}) \geq 50\}, \quad U''_{ij} = \{v \in V_i : e(v, W_{ji}) \geq 50\}.$$

Thus, it suffices to bound the sizes of  $U'_{ij}, U''_{ij}$  separately.

Let's start with  $U'_{ij}$ . By construction, which vertices belong to  $W_j \setminus W_{ji}$  is independent of the edges between color classes  $V_i, V_j$ . Hence, for any  $v \in V_i$  the number  $e(v, W_j \setminus W_{ji})$  has distribution  $\text{Bin}(|W_j \setminus W_{ji}|, p)$ . Thus,

$$\mathbb{E} \left[ e(v, W_j \setminus W_{ji}) \mid |W_j \setminus W_{ji}| \leq n \cdot \tilde{O}_k(k^{-2}) \right] \leq pn \cdot \tilde{O}_k(k^{-2}) \leq \tilde{O}_k(k^{-1}).$$

Therefore, the Chernoff bound (Lemma A.2) applied with, say,  $t = 45$  yields

$$\mathbb{P} \left[ v \in U'_{ij} \mid |W_j \setminus W_{ji}| \leq n \cdot \tilde{O}_k(k^{-2}) \right] \leq \tilde{O}_k(k^{-45}). \quad (\text{A.8})$$

Once more due to the independence of the edges in  $\mathcal{G}(n, p, \sigma)$ , the events  $v \in U'_{ij}$  are mutually independent for  $v \in V_i$ . by Lemma A.4, this event occurs with probability  $1 - \exp(-\Omega(n))$ . In effect, given  $|W_j \setminus W_{ji}| \leq n \cdot \tilde{O}_k(k^{-2})$ ,  $|U'_{ij}|$  has a binomial distribution. Thus, (A.8) implies together with the Chernoff bound (applied with, say,  $t = k^{-100}n$ ) that

$$\mathbb{P} \left[ |U'_{ij}| > nk^{-40} \mid |W_j \setminus W_{ji}| \leq n \cdot \tilde{O}_k(k^{-2}) \right] \leq \exp(-\Omega(n)). \quad (\text{A.9})$$

Further, Lemma A.4 implies that  $\mathbb{P}[|W_j \setminus W_{ji}| \leq n \cdot \tilde{O}_k(k^{-2})] \geq 1 - \exp(-\Omega(n))$ . Combining this bound with (A.10), we obtain

$$\mathbb{P} \left[ |U'_{ij}| > nk^{-40} \right] \leq \exp(-\Omega(n)). \quad (\text{A.10})$$

With respect to  $U''_{ij}$ , we observe the following. Given that  $w \in W_{ji}$ , we know that  $w$  has fewer than 300 neighbors in  $V_i$ . But the fact that  $w \in W_{ji}$  has no implications as to which  $v \in V_i$  vertex  $w$  is adjacent to. Thus, given that  $w \in W_{ji}$  and given  $e(w, V_i)$ , the actual set of neighbors of  $w$  in  $V_i$  is a random subset of  $V_i$  of size  $e(w, V_i) \leq 300$ . In fact, these sets are mutually independent for all  $w \in W_{ji}$ . Thus, we can bound  $|U''_{ij}|$  by means of the following balls and bins experiment: let us think of the vertices in  $V_i$  as bins. Then each vertex  $w \in W_{ji}$  tosses 300 balls randomly into the bins  $V_i$ , independently of all other vertices in  $W_{ji}$ . In this experiment, let  $\mathcal{X}$  be the set of  $v \in V_i$  that receive at least 50 balls. Then  $|U''_{ij}|$  is dominated by  $|\mathcal{X}|$  stochastically.

Now, consider one  $v \in V_i$ . Given  $|W_{ji}|$ , the number of balls that land in  $v$  has distribution  $\text{Bin}(300|W_{ji}|, |V_i|^{-1})$ . Therefore, the Chernoff bound yields

$$\mathbb{P} \left[ v \in \mathcal{X} \mid |W_{ji}| \leq n \cdot \tilde{O}_k(k^{-3}) \right] \leq \mathbb{P} \left[ \text{Bin}(\tilde{O}_k(k^{-3})n, (1 + o(1))k/n) \geq 50 \right] \leq k^{-45}.$$

Hence, by the linearity of expectation  $\mathbb{E}|\mathcal{X}| \leq nk^{-45}$ . Hence, Azuma's inequality yields

$$\mathbb{P} \left[ |U''_{ij}| > nk^{-40} \mid |W_{ji}| \leq n \cdot \tilde{O}_k(k^{-3}) \right] \leq \mathbb{P} \left[ |\mathcal{X}| > nk^{-40} \mid |W_{ji}| \leq n \cdot \tilde{O}_k(k^{-3}) \right] \leq \exp(-\Omega(n)).$$

Thus, Lemma A.4 implies

$$\mathbb{P} \left[ |U''_{ij}| > nk^{-40} \right] \leq \exp(-\Omega(n)). \quad (\text{A.11})$$

Finally, the assertion follows from (A.10) and (A.11), with room to spare.  $\square$

**Lemma A.6.** *With probability at least  $1 - \exp(-\Omega(n))$  we have  $|Z| \leq n/k^{29}$ .*

*Proof.* Lemma A.5 entails that with probability at least  $1 - \exp(-\Omega(n))$ ,  $|U| \leq n/k^{30}$ . Assume that this is indeed the case. Further, suppose that  $|Z \setminus U| \geq i^* = n/k^{30}$ . Let us stop the process **CR3** at this point, and let  $Z^* = Z^{(i^*)}$ . By construction, the graph induced on  $S = U \cup Z^*$  spans at least  $100i^* \geq 50|S|$  edges, while  $|S| \leq 2k^{-30}n$ . Thus, the set  $S$  violates condition **P3**. But since we saw in Section A.3 that **P3** is satisfied with probability  $1 - \exp(-\Omega(n))$ , the assertion follows.  $\square$

Now, Proposition A.3 is immediate from Lemmas A.4–A.6. For a set  $Y \subset V$  let us denote by  $N(Y)$  the set of all vertices  $v \in V$  that have a neighbor in  $Y$  in  $\mathcal{G}(n, p, \sigma)$ . As a further step towards the proof of **P4**, we establish

**Lemma A.7.** *With probability  $1 - \exp(-\Omega(n))$  the random graph  $\mathcal{G}(n, p, \sigma)$  has the following property.*

$$\text{Let } Y \subset V \text{ be a set of } |Y| \leq nk^{-29} \text{ vertices. Then } |N(Y)| \leq nk^{-20}. \quad (\text{A.12})$$

*Proof.* Let  $\alpha < k^{-29}$  be the largest number such that  $\alpha n$  is an integer and let  $q = 1 - (1 - p)^{\alpha n}$ . For a set  $Y \subset V$  with  $|Y| = \alpha n$  the number of vertices  $v \in V \setminus Y$  that have a neighbor in  $Y$  in  $\mathcal{G}(n, p, \sigma)$  is stochastically dominated by  $\text{Bin}(n, q)$ . This is because for any vertex  $y \in Y$  the probability that  $v, y$  are adjacent is either  $p$  (if  $\sigma(v) \neq \sigma(y)$ ) or 0 (if  $\sigma(v) = \sigma(y)$ ). Hence, observing that  $p \leq \alpha np$  and using the Chernoff bound, we get

$$\mathbb{P}[|N(Y) \setminus Y| \geq nk^{-21}] \leq \mathbb{P}[\text{Bin}(n, q) \geq nk^{-21}] \leq \exp(-nk^{-21}). \quad (\text{A.13})$$

Now, let  $X$  be the number of sets  $Y$  with  $|Y| = \alpha n$  such that  $|N(Y) \setminus Y| \geq nk^{-21}$ . Together with the union bound, (A.13) shows

$$\mathbb{P}[X > 0] \leq \binom{n}{\alpha n} \exp(-nk^{-21}) \leq \exp[n(\alpha(1 - \ln \alpha) - k^{-21})] \leq \exp(-\Omega(n)); \quad (\text{A.14})$$

the last inequality follows because  $\alpha(1 - \ln \alpha) \leq 32k^{-29} \ln k$  for  $0 < \alpha < k^{-29}$ . Thus, we obtain from (A.14) that  $X_\alpha = 0$  for all such  $\alpha$  with probability  $1 - \exp(-\Omega(n))$ . If so, we see that any set  $Y$  of size  $|Y| \leq nk^{-29}$  satisfies  $|N(Y)| \leq |Y| + |N(Y) \setminus Y| \leq n(k^{-29} + k^{-21}) \leq nk^{-20}$ , as claimed.  $\square$

**Corollary A.8.** *With probability  $1 - \exp(-\Omega(n))$  we have  $|N(Z)| \leq nk^{-20}$ .*

*Proof.* This is immediate from Lemmas A.6 and A.7.  $\square$

We define two sets of vertices, which capture the 1-free and 2-free vertices. In what follows, when always let  $i, j \in [k]$ ,  $i \neq j$ . Let  $S_0$  be the set of vertices that have zero neighbors in some color class other than their own. Moreover,  $S_1 = \{v \in V \setminus S_0 : \exists i, j \text{ s.t. } v \in V_i \text{ and } N(v) \cap V_j \subseteq W_j\}$ . By the construction of the core, we have

**Fact A.9.** *If  $v$  is 1-free, then  $v \in S_0 \cup S_1 \cup Z \cup N(Z)$ .*

We proceed by estimating the sizes of  $S_0, S_1$ .

**Lemma A.10.** *With probability  $1 - \exp(-\Omega(n))$  we have  $|S_0| \leq \frac{n}{k}$ .*

*Proof.* Consider a vertex  $v \in V_i$ . The number  $e(v, V_j)$  of neighbors of  $V_i$  in  $V_j$  has distribution  $\text{Bin}(|V_j|, p)$ . Since  $\sigma$  is balanced, (A.2) yields  $\mathbb{P}[e(v, V_j) = 0] \leq (1 - p)^{|V_j|} \leq k^{-2}$ . Thus, by the union bound,

$$\mathbb{P}[v \in S_0] \leq \sum_j \mathbb{P}[e(v, V_j) = 0] \leq (k - 1)k^{-2}. \quad (\text{A.15})$$

Because the events  $\{v \in S_0\}$  are mutually independent for all  $v \in V_i$ , the Chernoff bound and (A.15) yield  $\mathbb{P}[|S_0 \cap V_i| > n/k^2] \leq \exp(-\Omega(n))$ . Taking the union bound over  $i$  completes the proof.  $\square$

**Lemma A.11.** *With probability  $1 - \exp(-\Omega(n))$  we have  $|S_1| \leq \tilde{O}_k(k^{-2})n$ .*

*Proof.* Fix  $i \neq j$ . The total number  $e(V_i, V_j)$  of edges joining  $V_i$  and  $V_j$  in  $\mathcal{G}(n, p, \sigma)$  has distribution  $\text{Bin}(|V_i| \times |V_j|, p)$ . Because  $\sigma$  is balanced, the Chernoff bound yields

$$\mathbb{P}\left[e(V_i, V_j) \geq \frac{1}{2}k^{-2}n^2p\right] \geq 1 - \exp(-\Omega(n)). \quad (\text{A.16})$$

In addition, we claim that the number  $e(V_i, W_j)$  of  $V_i$ - $W_j$ -edges satisfies

$$\mathbb{P}\left[e(V_i, W_j) \leq \tilde{O}_k(k^{-3})n^2p\right] \geq 1 - \exp(-\Omega(n)). \quad (\text{A.17})$$

Indeed, by Lemma A.4 we may assume that  $|W_j \setminus W_{ji}| \leq \tilde{O}_k(k^{-2})n$ . By construction, the set  $W_j \setminus W_{ji}$  is independent of the random bipartite subgraph of  $\mathcal{G}(n, p, \sigma)$  consisting of the  $V_i$ - $V_j$ -edges. Hence, the number  $e(V_i, W_j \setminus W_{ji})$  of edges between  $V_i$  and  $W_j \setminus W_{ji}$  has distribution  $\text{Bin}(|V_i| \times (|W_j| - |W_{ji}|), p)$ . Given the upper bound on  $|W_j \setminus W_{ji}|$ , the Chernoff bound thus implies that

$$\mathbb{P}\left[e(V_i, W_j \setminus W_{ji}) \leq \tilde{O}_k(k^{-3})n^2p\right] \geq 1 - \exp(-\Omega(n)). \quad (\text{A.18})$$

Further, by construction the number of  $V_i$ - $W_{ji}$ -edges is bounded by  $300|W_{ji}|$ . Since by Lemma A.4 we may assume that  $|W_{ji}| \leq n\tilde{O}_k(k^{-3})$ , (A.18) implies (A.17).

Let us condition on the event  $\mathcal{A}$  that  $b = e(V_i, V_j \setminus W_j) \geq \frac{1}{3}k^{-2}n^2p$  and  $r = e(V_i, W_j) \leq O_k(k^{-3}) \leq n^2p$ . Let us think of the vertices in  $V_i$  as bins, and of the  $V_i - V_j \setminus W_j$  edges as balls that are tossed independently and uniformly into the bins. More precisely, we think of the  $V_i - V_j \setminus W_j$  edges as blue balls, and of the  $V_i - W_j$ -edges as red balls. Let  $\mathcal{X}_{ij}$  be the number of bins  $v \in V_i$  that receive at least one ball but that do not receive a blue ball. Now, given that  $v$  receives  $l$  balls in total, the probability that all the balls it receives are red is equal to the probability that a hypergeometric random variable with parameters  $l, b, r$  takes the value  $l$ . Therefore, summing over all  $l \geq 1$  and using our conditions on  $b, r$ , we see that  $P[v \in \mathcal{X}_{ij}] \leq \tilde{O}_k(k^{-3})$ . Because  $\sigma$  is balanced, we thus obtain

$$E[|\mathcal{X}_{ij}| \mid \mathcal{A}] \leq \frac{n}{k} \cdot O_k(k^{-3}). \quad (\text{A.19})$$

In fact, because the balls are tossed into the bins independently of each other, Azuma's inequality implies together with (A.19) that

$$P[|\mathcal{X}_{ij}| \leq \tilde{O}_k(k^{-4})n \mid \mathcal{A}] \geq 1 - \exp(-\Omega(n)). \quad (\text{A.20})$$

Since  $P[\mathcal{A}] \geq 1 - \exp(-\Omega(n))$  by (A.16) and (A.17), (A.20) yields that  $P[|\mathcal{X}_{ij}| \leq \tilde{O}_k(k^{-4})n] \geq 1 - \exp(-\Omega(n))$ . Taking the union bound over  $i, j$  completes the proof because  $S_1 \subset \cup_{i,j} \mathcal{X}_{ij}$ .  $\square$

Fact A.9 implies together with Lemma A.6, Corollary A.8, Lemma A.10 and Lemma A.11 the desired bound on the number of 1-free vertices. To bound the number of 2-free variables, we need

**Lemma A.12.** *Let  $i, j, l \in [k]$  be distinct. With probability at least  $1 - \exp(-\Omega(n))$  there are no more than  $n\tilde{O}_k(k^{-5})$  vertices  $v \in V_i$  such that  $e(v, V_j) \leq 100$  and  $e(v, V_l) \leq 100$ .*

*Proof.* For any  $v$ ,  $e(v, V_j)$ ,  $e(v, V_l)$  are independent binomial variables. Because  $\sigma$  is balanced, their means are  $(1+o(1))\frac{n}{k}p$ . Hence, (A.2) shows that  $P[e(v, V_j), e(v, V_l) \leq 100] \leq \tilde{O}_k(k^{-4})$ . Consequently, the expected number of  $v \in V_i$  with  $e(v, V_j), e(v, V_l) \leq 100$  is  $nO_k(k^{-5})$ . In fact, this is a binomial random variable due to the independence of the edges in  $\mathcal{G}(n, p, \sigma)$ . Thus, the assertion follows from the Chernoff bound.  $\square$

Now, let  $S_2$  be the set of all  $v \in V_i$  such that there exist distinct  $j, l \in [k] \setminus \{i\}$  such that  $e(v, V_j) \leq 100$  and  $e(v, V_l) \leq 100$ . By construction, if  $v$  is 2-free, then  $v \in S_2 \cup Z \cup N(Z)$  (note that  $U \subset Z$ ). Thus, the desired bound on the number of 2-free vertices follows from Lemma A.6, Corollary A.8 and Lemma A.12.  $\square$

AMIN COJA-OGHLAN, [acoghlan@math.uni-frankfurt.de](mailto:acoghlan@math.uni-frankfurt.de), GOETHE UNIVERSITY, MATHEMATICS INSTITUTE, 10 ROBERT MAYER ST, FRANKFURT 60325, GERMANY.

DAN VILENCHIK, [dan.vilenchik@weizmann.ac.il](mailto:dan.vilenchik@weizmann.ac.il), FACUTLY OF MATHEMATICS & COMPUTER SCIENCE, THE WEIZAMNN INSTITUTE, REHOVOT, ISRAEL.