Disproof of a packing conjecture of Alon and Spencer

Hüseyin Acan *† huseyin.acan@rutgers.edu

Jeff Kahn *‡ jkahn@math.rutgers.edu

Abstract

A 1992 conjecture of Alon and Spencer says, roughly, that the ordinary random graph $G_{n,1/2}$ typically admits a covering of a constant fraction of its edges by edge-disjoint, nearly maximum cliques. We show that this is not the case. The disproof is based on some (partial) understanding of a more basic question: for $k \ll \sqrt{n}$ and $A_1, \ldots, A_t$ chosen uniformly and independently from the k-subsets of $\{1, \ldots, n\}$, what can one say about

$$\mathbb{P}(|A_i \cap A_j| \leq 1 \ \forall i \neq j)?$$

Our main concern is trying to understand how closely the answers to this and a related question about matchings follow heuristics gotten by pretending that certain (dependent) choices are made independently.

1 Introduction

Write G for the the random graph $G_{n,1/2}$ and $f(k)$ $(= f_n(k))$ for the expected number of k-cliques in G; that is, $f(k) = \binom{n}{k} 2^{-\binom{k}{2}}$. Set

$$k_0 = k_0(n) = \min\{k : f(k) < 1\}$$

and temporarily (through Conjecture 1.1) set $k = k(n) = k_0 - 4$. It is easy to see that $k \sim 2\log_2 n$ and that $f(k)$ is at least about n^3 (precisely, $f(k) = \tilde{\Omega}(n^3)$, where, as usual, $\tilde{\Omega}$ ignores log factors).

AMS 2010 subject classification: 05D40, 05C80, 05C70, 60C05

Key words and phrases: Random graph, edge-disjoint cliques, hypergraph matchings

*Department of Mathematics, Rutgers University

†Supported by National Science Foundation Fellowship (Award No. 1502650).

‡Supported by NSF grant DMS1501962.

We will call a collection of edge-disjoint cliques a *packing* (and a *t-packing* if it has size t). Write $\nu_k(G)$ for the maximum size of a packing of k-cliques in G. This quantity (with independent sets in place of cliques) plays a central role in Bollobás' celebrated work [4] on the chromatic number of G, though all he needs from $\mathbb{E}\nu_k(G)$—the quantity that will interest us here—is the easy

$$\mathbb{E}\nu_k(G) = \Omega(n^2/k^4). \tag{1}$$

(His key point is that ν_k is Lipschitz, so martingale concentration implies it is (*very*) unlikely to be significantly smaller than its expectation.)

Of course one always has $\nu_k(G) \leq \binom{n}{2}/\binom{k}{2}$. A conjecture of Alon and Spencer, from the original 1992 edition of [3] (and subsequent editions), says that this trivial bound gives the true order of magnitude of $\mathbb{E}\nu_k(G)$, *viz.*

Conjecture 1.1. $\mathbb{E}\nu_k(G) = \Omega(n^2/k^2)$.

In other words, one can (in expectation) cover a constant fraction of the pairs from $[n]$ by edge-disjoint k-cliques of G. Here we show that this is not correct, even for somewhat smaller k:

Theorem 1.2. *For each C there is a D so that if $k = k_0 - C$, then*

$$\mathbb{P}(\nu_k(G) > Dn^2/k^3) < \exp[-n^2/k^2].$$

Again, it is easy to see that for k as in Theorem 1.2 we have

$$\tilde{\Omega}(n^{C-1}) < f(k) < n^C, \tag{2}$$

and that edges of G typically lie in many (at least about n^{C-3}) k-cliques, which might suggest plausibility of Conjecture 1.1. But as we will see below (following Theorem 1.5), falsity of the conjecture should not be surprising, though establishing this intuition so far seems less straightforward than one might expect.

We also observe a slight improvement in the lower bound of (1), an easy consequence of a seminal result of Ajtai, Komlós and Szemerédi [1, 2]:

Proposition 1.3. $\mathbb{E}\nu_k(G) = \Omega((n^2/k^4)\log k)$.

Though it may look like a detail at this point, determining the true order of magnitude of $\mathbb{E}\nu_k(G)$ still seems to us quite interesting, since it seems to require understanding more basic issues. For a guess, we slightly prefer the upper bound, but there are heuristics on both sides. It is not too hard to see that for a suitable c the *expected* number of (cn^2/k^3)-packings of k-cliques is large.

As above, a collection of sets is a *packing*—or is *nearly-disjoint*; we will find it convenient to have both terms—if no two of its members have more than one point in common, and a *t-packing* is a packing of size t. As usual a *matching* is a collection of pairwise *disjoint* sets and an m-matching is a matching of size m. Given n and k (for most of our discussion k need not be as above), we write $\mathcal{K}$ for $\binom{[n]}{k}$.

Our real interest in this paper is in the validity of heuristics based on the idea that certain events are close to independent. We view the next question in this way and will see a second instance in the discussion around Theorem 1.6.

Question 1.4. *For $A_1, \ldots, A_t$ drawn uniformly and independently from $\mathcal{K}$, what can be said about*

$$\zeta = \zeta(n,k,t) := \mathbb{P}(A_1, \ldots, A_t \textit{ form a packing})? \tag{3}$$

Of course what we expect here will depend on the parameters. We assume throughout that

$$1 \ll k \ll \sqrt{n}. \tag{4}$$

As noted below, the case of fixed k is handled in [11, 10] (with slight changes to our "natural" answers, e.g. since $\binom{k}{2} \not\sim k^2/2$ when k is fixed). The upper bound in (4) makes $\mathbb{P}(|A_i \cap A_j| \geq 2)$ small, without which the problem seems less natural. (We actually tend to think of $k = \Theta(\log n)$, the relevant range for Theorem 1.2.)

For k as in (4) and A, B drawn uniformly and independently from $\mathcal{K}$,

$$\mathbb{P}(|A \cap B| \geq 2) \approx k^4/(2n^2);$$

so thinking of the events $\{|A_i \cap A_j| \geq 2\}$ as close to independent suggests

$$\zeta \;\approx\; \left(1 - k^4/(2n^2)\right)^{\binom{t}{2}} \;\approx\; \exp\left[-\tfrac{t^2k^4}{4n^2}\right]. \tag{5}$$

Another, more robust way to arrive at the same guess: the probability that $m := t\binom{k}{2}$ pairs chosen *independently* (and uniformly) from $\binom{[n]}{2}$ are distinct is

$$\textstyle\prod_{i=1}^{m-1}(1 - i/\binom{n}{2}), \tag{6}$$

which agrees (approximately) with the r.h.s. of (5), provided

$$t \ll n^2/k^2. \tag{7}$$

It seems not impossible that these heuristics are close to the truth; precisely, that for t as in (7),

$$\log(1/\zeta) \sim t^2k^4/(4n^2) \tag{8}$$

(when the distinction matters, we use log for ln), while for larger t (where (5) and (6) are not so close) the asymptotics of $\log(1/\zeta)$ are given by (6).

Here we give upper bounds on ζ that (i) for t relevant to Theorem 1.2 support the theorem but fall somewhat short of (8), and (ii) agree with (8) for slightly smaller t. We will not have anything to say about lower bounds.

Theorem 1.5. (a) *There is a fixed $\beta > 0$ such that if $t = Dn^2/k^3$, then*

$$\zeta < \begin{cases} \exp[-\beta Dtk] & \text{if } e \geq D = \Omega(1), \\ \exp[-\beta(\log D)tk] & \text{if } D > e. \end{cases} \tag{9}$$

(b) *If $1 \ll t \ll n^2/k^3$ then* $\zeta < \exp[-(1-o(1))t^2k^4/(4n^2)]$.

(Note for perspective that for t as in (a) the bound in (b), which is essentially ideal if we have (7), becomes $\exp[-(1-o(1))Dtk/4]$. We won't bother with the silly case $t = O(1)$—which would require occasionally replacing t^2 by $t(t-1)$—and retain the uninteresting constant bounds for $t = O(n/k^2)$ only because they require no extra effort.)

Before continuing we observe that this gives Theorem 1.2. We may bound $\mathbb{P}(\nu_k(G) \geq t)$ by the expected number of t-packings in G ($= G_{n,1/2}$), which is less than

$$\zeta \binom{n}{k}^t 2^{-\binom{k}{2}t} = \zeta \left[\binom{n}{k} 2^{-\binom{k}{2}}\right]^t < \zeta \exp[Ct \log n], \tag{10}$$

where $\zeta\binom{n}{k}^t$ (crudely) bounds the number of t-packings in $\mathcal{K}$, each of which appears in G with probability $2^{-\binom{k}{2}t}$, and the inequality is given by (2). Now letting $t = Dn^2/k^3$ with D ($> e$) chosen so that $\beta \log D > C$ (where β is as in Theorem 1.5 and we recall $k \sim 2\log_2 n$) and combining (10) with the second bound in (9) gives

$$\mathbb{P}(\nu_k(G) > Dn^2/k^3) < \exp[-n^2/k^2]. \qquad \square$$

The argument for Theorem 1.5(a) (the part needed for Theorem 1.2) is mainly based on Theorem 1.6 below, which we next spend a little time motivating.

To begin, we remind the reader that there is a natural entropy-based approach to problems "like" that addressed by Theorem 1.5; this approach was introduced by J. Radhakrishnan [12] in his proof of Brégman's Theorem [5] and followed more recently in (e.g.) the Linial-Luria upper bound on the number of Steiner triple systems [11] and its extension to more general designs by Keevash [10]. In our situation the entropy argument works up to a point, but we don't see how to push it to a proof of Theorem 1.5 (or a disproof of Conjecture 1.1) and will take a different approach.

A first simple (but seemingly crucial) idea is that we should choose our packing in two rounds, the first round specifying just half, say B_i, of each A_i. A *necessary* condition for a packing is then:

$$\textit{for each } x \in [n],\ \{B_i : x \in A_i \setminus B_i\} \textit{ is a matching.}$$

Modulo a certain amount of fiddling, this gets us to the following situation, in which l will be $k/2$.

We assume $\mathcal{H}$ is a nearly-disjoint l-graph (l-uniform hypergraph) with n vertices and t edges, and $\mathcal{M} = \{e_1, \ldots, e_m\}$ is a random (uniform) m-subset of $\mathcal{H}$, and are interested in

$$\xi = \xi_{\mathcal{H}}(m) = \mathbb{P}(\mathcal{M} \text{ is a matching}).$$

(When we apply this to Theorem 1.5, t will be as in the theorem and m will be something like tl/n.) Setting $c = ml^2/n$, we again have a natural value for ξ, namely,

$$(1 - l^2/n)^{\binom{m}{2}} \;\approx\; \exp[-cm/2], \tag{11}$$

gotten by pretending independence of the events $\{e_i \cap e_j \neq \emptyset\}$, the natural value of whose probabilities is roughly $1 - l^2/n$. The next statement is perhaps our main point.

Theorem 1.6. *If $t \gg n/l$ and $c = \min\{ml^2/n, tl/n\}$, then*

$$\mathbb{P}(\mathcal{M} \textit{ is a matching}) < \begin{cases} \exp[-\Omega(cm)] & \textit{if } c \leq e, \\ \exp[-\Omega((\log c)m)] & \textit{if } c > e. \end{cases} \tag{12}$$

(We won't get into $t = O(n/l)$. Of course the theorem evaporates if $t \leq n/l$, since $\mathcal{H}$ itself can then be a matching.)

Note that here, unlike in Theorem 1.5, we may think of $\mathcal{H}$ as chosen adversarially, and should adjust expectations accordingly; in particular the probability in (12) can easily be zero, so at best we may hope that (11) offers some guidance on *upper* bounds. It's also true that, as shown by the following example, the probability of a matching can easily be about $(tl/n)^{-m}$, so even the second part of (12) (the one that differs more seriously from (11)) can't be much improved under the stated hypotheses. On the other hand—and more interestingly—it could be that (11) is about right (as an upper bound) if, say, $\log(tl/n) \gg c \ (= ml^2/n)$.

Example. For $t = sn/l$ with l a prime power, let $\mathcal{G}$ consist of s parallel classes of an affine plane of order l, and let $\mathcal{H}$ be the disjoint union of n/l^2 copies of $\mathcal{G}$. Then for $m \ll n/l$ and $e_1, \ldots, e_m$ drawn uniformly and independently from $\mathcal{H}$,

$$\mathbb{P}(\{e_1, \ldots, e_m\} \text{ is a matching}) > s^{-(1-o(1))m},$$

as follows from the observation that if $\{e_1, \ldots, e_i\}$ is a matching then the number of edges disjoint from $e_1, \ldots, e_i$ is at least $n/l - i$ (and exactly this if $\{e_1, \ldots, e_i\}$ meets all copies of $\mathcal{G}$). □

Outline Theorems 1.5 and 1.6 are proved in Sections 3 and 4, following a quick large deviation review (mainly for Theorem 1.5(b)) in Section 2. The proof of Proposition 1.3 is sketched in Section 5.

Usage. For asymptotics we use $a \ll b$ and $a = o(b)$ interchangeably. As is common we pretend all large numbers are integers and always assume n is large enough to support our arguments. As mentioned earlier, log is ln.

2 Preliminaries

We will need the following "Chernoff bounds" (see e.g. [8, Thm. 2.1 and Cor. 2.4]; we won't need to deal with lower tails).

Theorem 2.1. *If $X \sim \text{Bin}(n, p)$ and $\mu = \mathbb{E}[X] = np$, then*

$$\Pr(X > \mu + t) < \exp\left[-t^2/(2(\mu + t/3))\right] \quad \forall t > 0,$$
$$\Pr(X > K\mu) < \exp[-K\mu \log(K/e)] \quad \forall K.$$

(Of course the second bound is only of interest for slightly large K. We won't need to deal with lower tails.)

Though it could be avoided, the following less usual bit of machinery is nice and will be convenient for us at one point. Recall that r.v.'s $\xi_1, \ldots, \xi_n$ are *negatively associated* if $\mathbb{E}fg \leq \mathbb{E}f\mathbb{E}g$ whenever there are disjoint $I, J \subseteq [n]$ for which f and g are increasing functions of $\{\xi_i : i \in I\}$ and $\{\xi_i : i \in J\}$ (respectively). As observed in [6, Lemma 8.2], Chernoff-type bounds usually apply at the level of negatively associated r.v.'s; we state only what we need in this direction:

Proposition 2.2. (a) *If $A_1, \ldots, A_t$ are drawn uniformly and independently from $\binom{[n]}{k}$, then the degrees $d(j) = |\{i : j \in A_i\}|$ ($j \in [n]$) are negatively associated, as are any r.v.'s $\xi_1, \ldots, \xi_n$ with ξ_j an increasing function of $d(j)$.*

(b) *If $\xi = \sum \xi_i$ with the ξ_i's negatively associated, then for any α and $\lambda > 0$,*

$$\mathbb{P}(\xi > \alpha) \ < \ e^{-\lambda\alpha}\mathbb{E}e^{\lambda\xi} \ \leq \ e^{-\lambda\alpha}\prod \mathbb{E}e^{\lambda\xi_i}. \tag{13}$$

For (a) see [7, Propositions 3.1 and 3.2] (as remarked there, the statement is probably not news to anyone interested in such things). The content of (13) is the second inequality; the first, included here just for orientation, is the usual use of Markov's Inequality in proving Chernoff bounds.

3 Proof of Theorem 1.5

Proof of Theorem 1.5(a) (given Theorem 1.6). As mentioned in Section 1, a crucial first idea is that we should choose the A_i's in two stages. For simplicity suppose k is even, say $k = 2l$. For $i \in [t]$, let $A_i = B_i \cup C_i$, with B_i uniform from $\binom{[n]}{l}$ and C_i uniform from $\binom{[n]\setminus B_i}{l}$ (with the choices for different i's independent), and let $\mathcal{H} = \{B_1, \ldots, B_t\}$. Let $\mathcal{P} = \{A_1, \ldots, A_t \text{ form a packing}\}$ (the event in (3)) and $\mathcal{Q} = \{B_1, \ldots, B_t \text{ form a packing}\}$. Of course $\mathcal{Q}$ is a prerequisite for $\mathcal{P}$, so we need only show

$$\mathbb{P}(\mathcal{P}|\mathcal{Q}) < \begin{cases} \exp[-\Omega(D)tk] & \text{if } D \leq e \text{ (say)}, \\ \exp[-\Omega(\log D)tk] & \text{if } D > e. \end{cases} \tag{14}$$

From this point we fix a packing $\{B_1, \ldots, B_t\}$ and consider the probability of $\mathcal{P}$ given $\{\mathcal{H} = \{B_1, \ldots, B_t\}\}$. The problem is now more about counting than probability: we want to bound the number of ways of choosing $\mathcal{G} := \{C_1, \ldots, C_t\}$ so that the resulting A_i's form a packing.

We may think of choosing the C_i's by first choosing degrees $d_j := d_{\mathcal{G}}(j)$ ($j \in [n]$) satisfying

$$\sum d_j = tl \tag{15}$$

and then sets

$$S_j := \{i : j \in C_i\}$$

satisfying, for each $j \in [n]$,

$$\{B_i : i \in S_j\} \text{ is a matching}$$

(another prerequisite for $\mathcal{P}$). Here, for each j, S_j is the set of edges containing j and hence $|S_j| = d_j$. Of course only a small fraction of such choices correspond to legitimate C_i's, but this overcount turns out to be affordable.

Given d_j's the number of choices of S_j's as above is $\prod_{j\in[n]} N(d_j)$, where $N(d) = N_{\mathcal{H}}(d)$ is the number of d-matchings in $\mathcal{H}$.

Set $u = tl/n$ (the average of the d_j's). Since $\sum\{d_j : d_j \leq u/2\} \leq un/2$, (15) implies

$$\sum\{d_j : d_j > u/2\} \geq un/2 = tl/2. \tag{16}$$

For bounding $N(d)$ when $d \leq u/2$, we use the trivial $N(d) \leq \binom{t}{d}$. For larger d, noting that $u/2 = Dn/(16l^2)$, we may apply Theorem 1.6 with $m = d$ and $c \geq D/(16)$ (and $t = t$, so $tl/n = Dn/(8l^2) \gg D$) to obtain

$$N(d) < e^{-Bd}\tbinom{t}{d}, \tag{17}$$

where

$$B = \begin{cases} \Omega(D) & \text{if } D \leq 16e, \\ \Omega(\log D) & \text{otherwise.} \end{cases}$$

Thus for a particular set of d_j's the number of ways to choose the S_j's is less than

$$\exp[-B\textstyle\sum^* d_j] \cdot \prod \binom{t}{d_j} < e^{-Btl/2} \prod \binom{t}{d_j}, \tag{18}$$

where $\sum^*$ runs over j with $d_j > u/2$ (and we use $u = tl/n$ and (16)). For the product we have, again using (15),

$$\prod \tbinom{t}{d_j} < (et)^{\sum d_j} \prod d_j^{-d_j} \leq (et)^{tl}(tl/n)^{-tl} = (en/l)^{tl} \tag{19}$$

(since convexity of $x \log x$ implies that, given (15), $\prod d_j^{d_j}$ is minimum when $d_j = u$ for all j). The (negligible) number of ways to choose the d_j's is

$$\tbinom{tl+n-1}{n-1} < n^n. \tag{20}$$

On the other hand, the (*total*) number of ways of choosing $C_1, \ldots, C_t$ (again, for given B_i's) is

$$\tbinom{n-l}{l}^t > l^{-t}(en/l)^{tl}$$

(since $l \ll \sqrt{n}$, Stirling's formula gives $\binom{n-l}{l} \sim (2\pi l)^{-1/2}(en/l)^l$), and combining this with (18)-(20) we find that the probability of $\mathcal{P}$ (given the specified B_i's) is less than

$$n^n l^t e^{-Btl/2}(en/l)^{tl}(en/l)^{-tl} = e^{-(1-o(1))Btl/2}. \qquad \square$$

Proof of Theorem 1.5(b). Set $t = \varepsilon n^2/k^3$ (so $\varepsilon = o(1)$). Let δ be some sufficiently slow $o(1)$ and set $t_0 = \delta t$. (We need $\delta^2 \gg \varepsilon$ and, at (4), $\exp[-\Omega(\delta^2 k)] \ll \delta$.) Set $\mathcal{H}_i = \{A_1, \ldots, A_i\}$ and $\mathcal{H} = \mathcal{H}_t$, and write d_i and d for degrees in $\mathcal{H}_i$ and $\mathcal{H}$.

We first need to dispose of some pathological situations in which vertices with very large degrees meet too many edges of $\mathcal{H}$, to which end we set $a_0 = \delta n/k^2$ and $W = \{j \in [n] : d(j) \geq a_0\}$, and consider the event

$$\mathcal{Q} = \{\textstyle\sum_{j \in W} d(j) < \delta t_0 k\}.$$

Claim 1. $\mathbb{P}(\overline{\mathcal{Q}}) < \exp[-t^2k^4/n^2]$

Proof. The second bound in Theorem 2.1 applied to $d(j) \sim \mathrm{Bin}(t, k/n)$ is easily seen to imply that for any $a \geq a_0$ (using $\delta \gg \varepsilon$ to say $a_0 \gg tk/n$),

$$\mathbb{P}(d(j) \geq a) < (e\varepsilon/\delta)^a$$

which for $\xi_j := d(j)\mathbf{1}_{\{d(j) \geq a_0\}}$ implies

$$\mathbb{E}e^{\xi_j} \ < \ 1 + \textstyle\sum_{a \geq a_0} a(e\varepsilon/\delta)^a \ < \ \exp[\varepsilon^{\omega(1)}]. \tag{21}$$

Maybe we can replace the above equation by the following:

$$\begin{aligned}\mathbb{E}e^{\xi_j} &< 1 + \sum_{a \geq a_0} e^a (e\varepsilon/\delta)^a \\ &< 1 + \sum_{a \geq a_0} \varepsilon^{a/2} = \exp[\varepsilon^{\omega(1)}]\end{aligned}$$

Here we are thinking $a_0 \to \infty$. Should we say above that $\delta \to 0$ slowly enough such that $a_0 = \delta n/k^2 \to \infty$? Moreover, by Proposition 2.2(a), the ξ_j's are negatively associated, so part (b) of the proposition with $\lambda = 1$ gives, for $\xi = \sum \xi_j$,

$$\mathbb{P}(\overline{\mathcal{Q}}) = \mathbb{P}(\xi > \delta t_0 k) < \exp[-\delta t_0 k + n\varepsilon^{\omega(1)}] = \exp[-(1 - o(1))\delta t_0 k],$$

which, since $\delta^2 \gg \varepsilon$, is less than the bound in Claim 1. (Note also that $\delta t_0 k \gg n\varepsilon^{\omega(1)}$ is the same as $\delta^2 \varepsilon n/k^2 \gg \varepsilon^{\omega(1)}$.)

□

Now let $\mathcal{P}_i = \{\mathcal{H}_i \text{ is a packing}\}$, $\mathcal{P} = \mathcal{P}_t$, $W_i = \{j \in [n] : d_i(j) \geq a_0\}$ and $\mathcal{Q}_i = \{\sum_{j \in W_i} d_i(j) < \delta t_0 k\}$.

Claim 2. For $i > t_0$, if $A_1, \ldots, A_{i-1}$ satisfy $\mathcal{P}_{i-1}\mathcal{Q}_{i-1}$, then

$$\mathbb{P}(|A_i \cap A_j| \le 1 \ \forall j < i) < \exp[-(1-o(1))ik^4/(2n^2)].$$

Once this is established, we have (noting that $\mathcal{P}\mathcal{Q} = \cap(\mathcal{P}_i\mathcal{Q}_i)$, since in fact $\mathcal{P}_1 \supseteq \cdots \supseteq \mathcal{P}_t = \mathcal{P}$ and $\mathcal{Q}_1 \supseteq \cdots \supseteq \mathcal{Q}_t = \mathcal{Q}$),

$$\begin{aligned} \mathbb{P}(\mathcal{P}) \le \mathbb{P}(\overline{\mathcal{Q}}) + \mathbb{P}(\mathcal{P}\mathcal{Q}) &\le \mathbb{P}(\overline{\mathcal{Q}}) + \textstyle\prod_i \mathbb{P}(\mathcal{P}_i\mathcal{Q}_i|\mathcal{P}_{i-1}\mathcal{Q}_{i-1}), \\ &\le \mathbb{P}(\overline{\mathcal{Q}}) + \textstyle\prod_{i=t_0+1}^t \mathbb{P}(\mathcal{P}_i|\mathcal{P}_{i-1}\mathcal{Q}_{i-1}), \end{aligned}$$

which, according to Claims 1 and 2, is less than

$$\exp[-\tfrac{t^2k^4}{n^2}] + \exp[-(1-o(1))\textstyle\sum_{i=t_0+1}^t \tfrac{ik^4}{2n^2}] = \exp[-(1-o(1))\binom{t}{2}\tfrac{k^4}{2n^2}],$$

completing the proof of Theorem 1.5(b). □

Proof of Claim 2. Let $\mathcal{S} = \{P_1, \ldots, P_m\}$ be the set of pairs contained in (at least one of) $A_1, \ldots, A_{i-1}$ and not meeting W_{i-1}, and

$$\mathcal{T} = \{X \subseteq [n] : \tbinom{X}{2} \cap \mathcal{S} = \emptyset\} \supseteq \{X \subseteq [n] : |X \cap A_j| \le 1 \ \forall j < i\}.$$

It is enough to bound $\mathbb{P}(A_i \in \mathcal{T})$. In view of $\mathcal{P}_{i-1}$, the number of pairs covered by $A_1, \ldots, A_{i-1}$ is $(i-1)\binom{k}{2}$, while $\mathcal{Q}_{i-1}$ says that the number of these that meet W_{i-1} is at most $\delta t_0 k(k-1)$; thus, since $i > t_0$, m $(= |\mathcal{S}|)$ $\sim ik^2/2$. Note also that the number of non-disjoint (unordered) pairs from $\mathcal{S}$ is less than

$$\sum d_{\mathcal{S}}^2(j)/2 \ < \ a_0 k \sum d_{\mathcal{S}}(j)/2 \sim \delta nik/2.$$

For a silly technical reason (see (23)) we now treat $t \ll n^2/k^4$ separately. Let $R_l = \{A_i \supseteq P_l\}$ $(l \in [m])$. Then using $\mathbb{P}(A_i \supseteq I) \sim (k/n)^{|I|}$ for fixed $|I|$ together with the above asymptotics yields

$$\mathbb{P}(A_i \notin \mathcal{T}) \ge \sum \mathbb{P}(R_l) - \sum\sum \mathbb{P}(R_l R_{l'}) \sim ik^4/(2n^2).$$

(The first sum is asymptotic to the r.h.s. and the double sum is asymptotically at most $(\delta nik/2)(k/n)^3 + (ik^2/2)^2(k/n)^4 = \delta ik^4/(2n^2) + i^2k^8/(4n^4)$, which is $o(ik^4/n^2)$ since we assume $t \ll n^2/k^4$.)

Now assume $t = \Omega(n^2/k^4)$ (so $\varepsilon = \Omega(1/k)$). Set $p = (1-\delta)k/n$ and let B be the random subset of $[n]$ gotten by including each element with probability p, independent of other choices. According to the "Basic Janson Inequality" ([9] or e.g. [3, Ch. 8])),

$$\mathbb{P}(B \in \mathcal{T}) \le e^{-\mu+\Delta}, \tag{22}$$

where (*cf.* the above discussion for $t \ll n^2/k^4$) $\mu = mp^2 \sim ik^4/(2n^2)$ and

$$\Delta \;=\; \tfrac{1}{2}\sum_j d_{\mathcal{S}}(j)(d_{\mathcal{S}}(j)-1)p^3 \;<\; (1-o(1))\delta ik^4/(2n^2) \;\ll\; \mu.$$

Thus (22) gives the desired bound with B in place of A_i; that is,

$$\mathbb{P}(B \in \mathcal{T}) < \exp[-(1-o(1))ik^4/(2n^2)].$$

Finally, we combine this with $\mathbb{P}(|B| > k) < \exp[-\Omega(\delta^2 k)]$ (see Theorem 2.1) to obtain

$$\begin{aligned}\mathbb{P}(A_i \in \mathcal{T}) &\leq \mathbb{P}(B \in \mathcal{T} \| B| \leq k) < \mathbb{P}(B \in \mathcal{T})/\mathbb{P}(|B| \leq k)\\ &= \mathbb{P}(B \in \mathcal{T})(1+e^{-\Omega(\delta^2 k)}) < \exp[-(1-o(1))ik^4/(2n^2)] \quad (23)\end{aligned}$$

(note $\varepsilon = \Omega(1/k)$ and the assumed $\exp[-\Omega(\delta^2 k)] \ll \delta$ give $\exp[-\Omega(\delta^2 k)] \ll \varepsilon\delta k = t_0 k^4/n^2$). □

4 Proof of Theorem 1.6

We will give two proofs; the second is easier and proves more (*as far as we can see,* the first handles only the more interesting case of larger c), but we include the first, which was our original argument, as it seems to us the more interesting. We will not try to optimize the implied constants in (12).

In each proof the following observation, which is where we use near-disjointness, will play a key role. For an l-graph $\mathcal{G}$ and set e (in practice a member of $\mathcal{G}$), let

$$I(e, \mathcal{G}) = |\{g \in \mathcal{G} : e \cap g \neq \emptyset\}|.$$

Proposition 4.1. *For any nearly-disjoint l-graph $\mathcal{G}$ on n vertices and $\delta > 0$,*

$$|\{e \in \mathcal{G} : I(e, \mathcal{G}) < \delta|\mathcal{G}|l^2/n\}| < \delta|\mathcal{G}| + n/l. \quad (24)$$

Proof. Writing $\mathcal{S}$ for the set in (24), we have $\sum_x d_{\mathcal{S}}(x) = l|\mathcal{S}|$. On the other hand, near-disjointness implies that for any $e \in \mathcal{S}$,

$$\textstyle\sum_{x\in e} d_{\mathcal{G}}(x) < \delta|\mathcal{G}|l^2/n + l - 1,$$

yielding

$$\textstyle\sum_x d_{\mathcal{S}}(x) d_{\mathcal{G}}(x) = \sum_{e\in\mathcal{S}}\sum_{x\in e} d_{\mathcal{G}}(x) < |\mathcal{S}|(\delta|\mathcal{G}|l^2/n + l - 1)$$

and

$$n\textstyle\sum_x d_{\mathcal{S}}^2(x) \;\leq\; n\sum_x d_{\mathcal{S}}(x)d_{\mathcal{G}}(x) \;<\; |\mathcal{S}|(\delta|\mathcal{G}|l^2 + n(l-1)).$$

Combining and using Cauchy-Schwarz we have

$$l^2|\mathcal{S}|^2 = (\sum_x d_{\mathcal{S}}(x))^2 < |\mathcal{S}|(\delta|\mathcal{G}|l^2 + n(l-1)),$$

which implies (24). □

First proof of Theorem 1.6. Here $\mathcal{M}$ and $\mathcal{S}$ will always be matchings (of $\mathcal{H}$) of sizes m and γm respectively. As indicated above, we are now considering only the second regime in (12), so may assume c is a bit large. To bound the number of $\mathcal{M}$'s we first want an $\mathcal{S} \subseteq \mathcal{M}$ for which the number of possible continuations $\mathcal{M} \setminus \mathcal{S}$ is "small." (The parameters $\gamma, \delta, \vartheta$ will be set below.)

Given $\mathcal{S}$, set

$$\mathcal{R} = \mathcal{R}_{\mathcal{S}} = \{e \in \mathcal{H} : I(e, \mathcal{S}) = 0\},$$

$$\mathcal{B} = \mathcal{B}_{\mathcal{S}} = \{e \in \mathcal{R} : I(e, \mathcal{R}) \geq \delta|\mathcal{R}|l^2/n\}$$

and $r = |\mathcal{R}|$. If $\mathcal{M} \supseteq \mathcal{S}$ then, trivially,

$$\mathcal{M} \setminus \mathcal{S} \subseteq \mathcal{R}; \tag{25}$$

so the number of $\mathcal{M}$'s containing $\mathcal{S}$ is at most

$$\tbinom{r}{m-\gamma m}. \tag{26}$$

Note also that Proposition 4.1 gives

$$|\mathcal{R} \setminus \mathcal{B}| < \delta r + n/l \ =: r^*. \tag{27}$$

Since we will choose δ fairly small, (27) (with (25)) will limit possibilities for $(\mathcal{M} \setminus \mathcal{S}) \setminus \mathcal{B}$. We next show that for any $\mathcal{M}$ there is some $\mathcal{S}$ for which $(\mathcal{M} \setminus \mathcal{S}) \cap \mathcal{B}$ is small.

Given $\mathcal{M}$ and $\mathcal{S} \subseteq \mathcal{M}$, with $\mathcal{R}, \mathcal{B}, r$ as above, let

$$\mathcal{R}_1 = \{e \in \mathcal{R} : I(e, \mathcal{M}) < \vartheta m l^2/n\}, \quad \mathcal{R}_2 = \mathcal{R} \setminus \mathcal{R}_1,$$

$$\mathcal{A}_1 = \{e \in \mathcal{M} \cap \mathcal{B} : I(e, \mathcal{R}_1) \geq \delta r l^2/(2n)\}$$

and $\mathcal{A}_2 = (\mathcal{M} \cap \mathcal{B}) \setminus \mathcal{A}_1$; thus $e \in \mathcal{A}_2$ implies $I(e, \mathcal{R}_2) > \delta r l^2/(2n)$.

We then want to bound $|\mathcal{A}_1|$ and $|\mathcal{A}_2|$, the first in general, the second for a suitable $\mathcal{S}$. In each case we consider

$$N_i = |\{(e, f) \in \mathcal{A}_i \times \mathcal{R}_i : e \cap f \neq \emptyset\}|.$$

For $i = 1$, we have $|\mathcal{A}_1|\delta r l^2/(2n) \leq N_1 < |\mathcal{R}_1|\vartheta m l^2/n$, implying

$$|\mathcal{A}_1| \leq 2m\vartheta/\delta. \tag{28}$$

For $i = 2$ we again have $N_2 \geq |\mathcal{A}_2|\delta r l^2/(2n)$, but our upper bound now depends on $\mathcal{S}$. Suppose $\mathcal{S}$ is chosen uniformly from $\binom{\mathcal{M}}{\gamma m}$ (so $\mathcal{R}$, $\mathcal{B}$, $\mathcal{R}_1$, and $\mathcal{R}_2$ are also random). Set $\mathcal{C} = \{f \in \mathcal{H} : I(f, \mathcal{M}) \geq \vartheta m l^2/n\}$ (the edges that will be in $\mathcal{R}_2$ if they are in $\mathcal{R}$). Then

$$\mathbb{E}N_2 \;<\; \textstyle\sum_{f\in\mathcal{C}} I(f,\mathcal{M})(1-\gamma)^{I(f,\mathcal{M})} \;<\; \sum_{f\in\mathcal{C}} I(f,\mathcal{M})e^{-\gamma I(f,\mathcal{M})}. \tag{29}$$

Since $xe^{-\gamma x}$ is decreasing for $x \geq 1/\gamma$ and—a very small point—we will choose parameters so

$$\vartheta m l^2/n \geq 1/\gamma, \tag{30}$$

the r.h.s. of (29) is at most $t(\vartheta m l^2/n)e^{-\gamma\vartheta m l^2/n}$. Thus each $\mathcal{M}$ admits some $\mathcal{S}$ for which N_2 is at most this value, implying

$$|\mathcal{A}_2| \leq \tfrac{2\vartheta}{\delta}\,\tfrac{t}{r}e^{-\gamma\vartheta m l^2/n}m$$

and (recall (28))

$$|\mathcal{M}\cap\mathcal{B}| \;\leq\; \tfrac{2\vartheta}{\delta}(1+\tfrac{t}{r}e^{-\gamma\vartheta m l^2/n})m \;=:\; s_r. \tag{31}$$

Thus the number of choices for $\mathcal{M}$ is at most the number of ways to choose $\mathcal{S}$ and then an $\mathcal{M} \supseteq \mathcal{S}$ satisfying (31).

Remark. Note we are not *choosing* the $\mathcal{R}_i$'s and $\mathcal{A}_i$'s (which do depend on $\mathcal{M}$); these are just used in establishing existence of the desired $\mathcal{S}$.

For a given $\mathcal{S}$ the number of choices for $\mathcal{M} \supseteq \mathcal{S}$ satisfying (31) is at most

$$\psi = \max_r \min\left\{\tbinom{r}{m-\gamma m},\ \textstyle\sum_{a\leq s_r}\tbinom{t-\gamma m}{a}\tbinom{r^*}{m-\gamma m-a}\right\}, \tag{32}$$

where $r = |\mathcal{R}_{\mathcal{S}}|$ (see (27) for r^*) and the first bound is from (26). We may thus bound the number of $\mathcal{M}$'s by $\binom{t}{\gamma m}\psi$, and the probability in (12) by

$$\tbinom{t}{m}^{-1}\tbinom{t}{\gamma m}\psi. \tag{33}$$

Finally, we need to set parameters and discuss bounds. Set $\gamma = 0.1$, $\delta = 100c^{-1}\log c$ and $\vartheta = 0.1\delta$. (Note these support (30).) For $r < \delta t$ we use the first bound in (32) to say the expression in (33) is at most

$$\tbinom{t}{m}^{-1}\tbinom{t}{\gamma m}\tbinom{\delta t}{m-\gamma m} < \tbinom{m}{\gamma m}\delta^{(1-\gamma)m} \;<\; \exp[-((1-\gamma)\log(1/\delta)-1)m].$$

For the above inequality:

$$\binom{t}{m}^{-1}\binom{t}{\gamma m}\binom{\delta t}{m-\gamma m} = \binom{m}{\gamma m}\prod_{i=0}^{m-\gamma m-1}\frac{\delta t - i}{t-\gamma m - i}.$$

Since

$$\frac{\delta t - i}{t - \gamma m - i} \le \frac{\delta t}{t - \gamma m} \le \frac{2\delta t}{t} = 2\delta,$$

the right hand side above is at most

$$2^m (2\delta)^{m-\gamma m} < \exp[m + (1-\gamma)\log(2\delta)m] = \exp[-\Omega(\log c)m].$$

For $r \ge \delta t$, referring to (31), we have $s := s_r < 0.2[1 + 1/(\delta c)]m < 0.3m$. Note that,

$$r^* = \delta r + \frac{n}{\ell} \le \delta t + \frac{t}{c} = \delta t\left(1 + \frac{1}{100\log c}\right) \le (1.1)\delta t \le 2\delta(t - \gamma m - s).$$

So $t - \gamma m \ge r^*$ and $a \le m - \gamma m - a$ for any $a \le s$. Hence the terms in the sum (32) are increasing for $a \le s$. So, using the second part of (32), we may bound the expression in (33) by

$$s\tbinom{t}{m}^{-1}\tbinom{t}{\gamma m}\tbinom{t-\gamma m}{s}\tbinom{r^*}{m-\gamma m-s} < \exp[-0.5\log(1/\delta)m],$$

where we used

$$\tbinom{t}{m}^{-1}\tbinom{t}{\gamma m}\tbinom{t-\gamma m}{s} = \tbinom{m}{\gamma m, s, m-\gamma m-s}\tbinom{t-\gamma m-s}{m-\gamma m-s}^{-1}$$

and, say, $r^* < 2\delta(t - \gamma m - s)$. □

Second proof of Theorem 1.6. Here it will be easier to consider $e_1, \ldots, e_m$ drawn uniformly and *independently* from $\mathcal{H}$ and prove bounds as in (12) for the probability that these e_i's form a matching. This is equivalent since

$$\zeta = \mathbb{P}(\text{the } e_i\text{'s form a matching})/\mathbb{P}(\text{the } e_i\text{'s are distinct})$$

(recall $\zeta = \mathbb{P}(\mathcal{M} \text{ is a matching})$), and the denominator (roughly $\exp[-\frac{m^2}{2t}]$) doesn't significantly affect the bounds in (12).

Let $\mathcal{H}_0 = \mathcal{H}$ and, for $j \ge 1$,

$$\mathcal{H}_j = \{e \in \mathcal{H} : e \cap e_i = \emptyset \ \forall i \le j\}.$$

(Thus $\mathcal{H}_0 \supseteq \mathcal{H}_1 \supseteq \cdots$ and the e_i's form a matching iff $e_i \in \mathcal{H}_{i-1}$ for all $\forall i \in [m]$.) Set

$$\delta = \begin{cases} e^{-1} & \text{if } c \le e, \\ c^{-1}\log c & \text{otherwise} \end{cases}$$

(the precise values are not very important) and

$$\mathcal{C}_j = \{e \in \mathcal{H}_j : I(e, \mathcal{H}_j) < \delta|\mathcal{H}_j|l^2/n\},$$

and let $\mathcal{Q}$ be the event

$$\{|\{j \in [m/2] : e_j \in \mathcal{C}_{j-1}\}| > m/3\}.$$

Proposition 4.1 gives

$$|\mathcal{C}_j| < \delta|\mathcal{H}_j| + n/l, \tag{34}$$

so that we always (regardless of history) have

$$\mathbb{P}(e_j \in \mathcal{C}_{j-1}) < \delta + n/(lt) =: \delta' < \begin{cases} e^{-1} + o(1) & \text{if } c \le e, \\ c^{-1}\log c + \min\{c^{-1}, o(1)\} & \text{otherwise,} \end{cases}$$

and in either case $\delta' < 1/2$. Thus $|\{j \in [m/2] : e_j \in \mathcal{C}_{j-1}\}|$ is stochastically dominated by a r.v. with the distribution $\text{Bin}(m/2, \delta')$, and Theorem 2.1 gives

$$\mathbb{P}(\mathcal{Q}) < \exp[-\Omega(\log(1/\delta'))m]. \tag{35}$$

(Of course $\Omega(\log(1/\delta'))$ is just $\Omega(1)$ until c is a bit large.) On the other hand, if $\mathcal{Q}$ does not occur then

$$|\mathcal{H}_{m/2}| < (1 - \delta l^2/n)^{m/6} t,$$

so the probability that we continue to a matching is less than

$$(1 - \delta l^2/n)^{(m/6)\cdot(m/2)} < \exp[-\delta cm/(12)]. \tag{36}$$

The theorem follows. $\square$

5 Lower bound

As noted earlier, Proposition 1.3 is an application of the following celebrated result of Ajtai, Komlós and Szemerédi [1, 2].

Theorem 5.1. *There is a fixed $c > 0$ such that $\alpha(\Gamma) > c(N \log D)/D$ for any triangle-free graph Γ with N vertices and average degree at most D.*

(As usual α is independence number). The reduction to Theorem 5.1 is quite routine and we will not give the full blow-by-blow.

In what follows we set $M = f(k)$ $(= \binom{n}{k} 2^{-\binom{k}{2}})$. We want existence of a large independent set in the graph Γ whose vertices are the k-cliques of G $(= G_{n,1/2})$ and edges the pairs that share edges (of G). A standard application of the second moment method (e.g. [3, Sec. 4.5 and Cor. 4.3.5] gives $|V(\Gamma)| > (1-o(1))M$ w.h.p. (meaning, as usual, with probability tending to 1 as $n \to \infty$), and routine analysis shows that the expected numbers of edges and triangles in Γ are respectively at most $k^4M^2/(2n^2)$ and $2k^6M^3/(3n^4)$. (The main contributions are from edges consisting of pairs of cliques with just one common edge and triangles composed of three cliques sharing the same edge.) So Markov's Inequality says that with probability at least $1/6 - o(1)$, we have

$$|V(\Gamma)| \sim M, \quad |E(\Gamma)| < k^4M^2/n^2 \text{ and } |T(\Gamma)| < 2k^6M^3/n^4, \tag{37}$$

where T denotes number of triangles. Thus Proposition 1.3 will follow from the next assertion.

Claim. If (37) holds then $\alpha(\Gamma) > \Omega(k^{-4}n^2 \log k)$.

To see this let $\delta = n^2/(2k^3M)$ and consider the subgraph H of Γ induced by W chosen uniformly from the subsets of $V(\Gamma)$ of size $\delta M \sim n^2/(2k^3)$. Then $\mathbb{E}|E(H)| < \delta^2|E(\Gamma)|$ and $\mathbb{E}|T(H)| < \delta^3|T(\Gamma)|$, so (again using Markov) there is a choice of W for which $|E(H)| \leq n^2/k^2$ and $|T(H)| \leq n^2/(3k^3)$. We may then find some triangle-free $K \subseteq H$ on $(1/3 - o(1))n^2/k^3$ vertices with average degree at most $\frac{2n^2/k^2}{|V(K)|} = O(k)$, and applying Theorem 5.1 gives the claim. □

References

[1] M. Ajtai, J. Komlós and E. Szemerédi, A note on Ramsey numbers, *J. Combinatorial Th.* (A) **299** (1980), 354-360.

[2] M. Ajtai, J. Komlós and E. Szemerédi, A dense infinite Sidon sequence, *Europ. J. Combinatorics* **2** (1981), 1-11.

[3] N. Alon and J.H. Spencer, *The Probablistic Method*, Wiley, New York, 2008.

[4] B. Bollobás, The chromatic number of random graphs, *Combinatorica* **8** (1988), 49-55.

[5] L. Brégman, Some properties of nonnegative matrices and their permanents, *Soviet Math. Dokl.* **15** (1973), 945-949.

[6] D. Dubhashi and D. Ranjan, Balls and bins: a study in negative dependence, *Random Structures & Algorithms* **13** (1998), 99-124.

[7] A. Hamm and J. Kahn, On Erdős-Ko-Rado for random hypergraphs I, submitted. arXiv:1412.5085 [math.CO]

[8] S. Janson, T. Łuczak and A. Ruciński, *Random Graphs*, Wiley, New York, 2000.

[9] S. Janson, T. Łuczak and A. Ruciński, An exponential bound for the probability of nonexistence of a specified subgraph in a random graph, pp. 73-87 in *Random graphs '87 (Poznań, 1987)*, Wiley, Chichester, 1990.

[10] P. Keevash, Counting designs, *J. Eur. Math. Soc.*, to appear. arXiv:1504.02909 [math.CO]

[11] N. Linial and Z. Luria, Upper bounds on the number of Steiner triple systems and 1-factorizations, *Random Structures & Algorithms* **43** (2013), 399-406.

[12] J. Radhakrishnan, An Entropy Proof of Bregman's Theorem, *J. Combin. Theory Ser. A* **77** (1997), 161-164.