On subgraphs with degrees of prescribed residues in the random graph

Asaf Ferber [*] Liam Hardiman [†] Michael Krivelevich[‡]

October 11, 2022

Abstract

We show that with high probability the random graph $G_{n,1/2}$ has an induced subgraph of linear size, all of whose degrees are congruent to $r \pmod q$ for any fixed r and $q \geq 2$. More generally, the same is true for any fixed distribution of degrees modulo q. Finally, we show that with high probability we can partition the vertices of $G_{n,1/2}$ into $q+1$ parts of nearly equal size, each of which induces a subgraph all of whose degrees are congruent to $r \pmod q$. Our results resolve affirmatively a conjecture of Scott, who addressed the case $q = 2$.

1 Introduction

In his comprehensive problem book [8] (see Ex. 5.17) Lovász states an unpublished but well known result of Gallai: every graph admits a vertex partition into two sets, each inducing a subgraph with all degrees even. This result guarantees the existence of two things: a large induced subgraph (at least one of the parts contains at least half of the vertices), and a vertex partition into subgraphs with all degrees congruent to zero modulo 2. We can ask if these guarantees still hold if we instead look for an induced subgraph with all degrees congruent to r mod q for fixed r and q. Towards discussing the existence of a large induced subgraph, define the following function. For a graph G and integers $q \geq 2$ and $0 \leq r < q$, we let $f(G, r, q)$ be the maximum order of an induced subgraph of G with all degrees congruent to $r \pmod q$ (we set $f(G, r, q) = 0$ if such a subgraph does not exist). In particular, it follows from Gallai's result that $f(G, 0, 2) \geq |V(G)|/2$ for every graph G. In other words, every graph admits an even induced subgraph (a graph, all of whose degrees are even) on at least half of its vertices.

The problem of finding a large odd subgraph, i.e. bounding $f(G, 1, 2)$ for arbitrary G, has a rich history. Since an odd graph cannot contain isolated vertices, we restrict our attention to graphs with minimum degree at least one. A conjecture, described as folklore by Caro [3], asserts that in this case there exists a constant $c > 0$ such that every such graph has an odd subgraph of order at least $c|V(G)|$. Following some partial results by Caro [3] and by Scott [9, 10], this conjecture was recently proved in [6] with $c = 1/10000$.

[*] Department of Mathematics, University of California, Irvine. Email: asaff@uci.edu. Research supported in part by NSF Awards DMS-1954395 and DMS-1953799.

[†] Department of Mathematics, University of California, Irvine. Email: lhardima@uci.edu.

[‡] School of Mathematical Sciences, Tel Aviv University, Tel Aviv, Israel. Email: krivelev@tauex.tau.ac.il. Research supported in part by USA–Israel BSF grant 2018267 and by ISF grant 1261/17.

Now we consider the problem of finding a lower bound for $f(G, r, q)$ for other values of r and q. In linear algebra terms, we want to find a large subgraph H of G, whose adjacency matrix $A = A(H)$ satisfies $A\mathbf{1} \equiv r\mathbf{1}$, where $\mathbf{1}$ is the all 1 vector of length $|V(H)|$ and the congruence is entrywise modulo q. In the case where G is a random graph, each entry of $A\mathbf{1}$ is a random sum of 0's and 1's with dependencies enforced by the condition that A is symmetric. Since the asymptotic behavior of random sums is tractable, this suggests studying the asymptotic behavior of $f(G, r, q)/|V(G)|$ when G is a random graph.

Recall that for $p \in [0, 1]$, $G_{n,p}$ is the random variable that outputs a graph on n vertices, where each potential (unordered) pair of vertices is included as an edge with probability p independently. In [9], Scott showed that with high probability (that is, with probability tending to 1 as n tends to infinity) $f(G_{n,1/2}, 1, 2) \approx cn$ where $c \approx 0.7729$ and n is sufficiently large, and asked for extensions to other values of r and q. We generalize Scott's result in the random setting as follows:

Theorem 1.1. *Let $q \geq 2$ and let $0 \leq r < q$ be an integer. If n is a sufficiently large integer and $k(n, q) > 0$ is the greatest integer such that $\binom{n}{k}q^{-k} \geq 1$, then with high probability, $|f(G_{n,1/2}, r, q) - k| = O(\log^{10} n)$.*

Remark 1. We can determine the value of k more precisely. If $H(p)$ is the binary entropy function,

$$H(p) = -p \log_2 p - (1 - p) \log_2(1 - p),$$

then we can estimate the binomial coefficient $\binom{n}{cn}$ for $0 < c < 1$ using Stirling's approximation to obtain

$$\binom{n}{cn} = 2^{nH(c)-o(n)}.$$

For a basic reference on entropy, see, e.g. [4], where the above appears as Lemma 2.2. If we set $k = cn$, then the value of c prescribed by Theorem 1.1 is the largest value of c such that $H(c)/c \geq \log_2(q) + o(1)$. When $q = 2$ we recover Scott's $c \approx 0.7729$. When $q = 3$ we get $c \approx 0.6091$ and when $q = 4$ we get the exact value $c = 1/2$.

With minor modifications to the proof of the above theorem, we obtain a stronger statement that allows us to prescribe the degree sequence modulo q of G in the following sense. Let $0 \leq \alpha_0, \ldots, \alpha_{q-1} \leq 1$, with $\alpha_0 + \cdots + \alpha_{q-1} = 1$, be the desired proportions of vertices having degree i (mod q) for each i. Set $\boldsymbol{\alpha} := (\alpha_0, \ldots, \alpha_{q-1})$ and define $f(G, \boldsymbol{\alpha}, q)$ to be the largest k for which G contains an induced subgraph on k vertices where, for each $0 \leq i \leq q - 1$, the number of vertices of degree i (mod q) is either $\lfloor \alpha_i k \rfloor$ or $\lceil \alpha_i k \rceil$. Notice that if $\alpha_r = 1$ and $\alpha_i = 0$ for all $i \neq r$, then $f(G, \boldsymbol{\alpha}, q)$ is just $f(G, r, q)$.

Theorem 1.2. *Let $q \geq 2$ and let $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_{q-1}) \in [0, 1]^q$ be such that $\alpha_0 + \cdots + \alpha_{q-1} = 1$. If n is a sufficiently large integer and $k(n, q, \alpha) > 0$ is the greatest integer such that*

$$\binom{n}{k}\binom{k}{k_0, \ldots, k_{q-1}}q^{-k} \geq 1$$

for all choices of $k_i \in \{\lceil \alpha_i k \rceil, \lfloor \alpha_i k \rfloor\}$ that satisfy $k_0 + \cdots + k_{q-1} = k$, then with high probability, $|f(G_{n,1/2}, \boldsymbol{\alpha}, q) - k| = o(n)$.

Remark 2. As in the remark following Theorem 1.1, we can get a more precise estimate for k. If $\boldsymbol{\alpha}$ is as in the statement of the theorem, then we define the entropy of $\boldsymbol{\alpha}$ by

$$H(\boldsymbol{\alpha}) = -\sum_{i=0}^{q-1} \alpha_i \log_2 \alpha_i.$$

Applying Stirling's approximation gives

$$\binom{k}{k_0, \dots, k_{q-1}} = 2^{kH(\boldsymbol{\alpha})-o(k)}.$$

For more details, see the Appendix. If we then set $k = cn$, then the value of c given by Theorem 1.2 is the largest c such that $H(c)/c \geq \log_2(q) - H(\boldsymbol{\alpha})$. The right-hand side of this inequality is always nonnegative since $H(\boldsymbol{\alpha}) \leq \log_2 q$, with equality achieved if and only if $\alpha_i = 1/q$ for all i.

Even though Theorem 1.2 implies Theorem 1.1, for the sake of readability, we will only prove the slightly simpler Theorem 1.1 in full. Theorem 1.2 is proved in a very similar way, so we simply outline its proof and mention the modifications that need to be made to the proof of Theorem 1.1 to obtain a proof for this theorem.

Now we address the second guarantee in Gallai's result — the existence of a partition into induced subgraphs under some degree constraints. Given a graph G, we say that a partition $V(G) = V_1 \cup \cdots \cup V_k$ is an (r, q)-**partition** if all degrees in $G[V_i]$ are congruent to $r \pmod q$ for every $1 \leq i \leq k$. Now define

$$p(G, r, q) = \min\{k : G \text{ has an } (r, q)\text{-partition with } k \text{ parts}\},$$

with the convention that $p(G, r, q) = \infty$ if no such partition exists for any k. In this notation, Gallai's aforementioned result on even subgraphs stated in [8] states that $p(G, 0, 2) \leq 2$, and in [10], Scott showed that $p(G, 1, 2)$ is finite if and only if every connected component of G has an even order. In the same paper, Scott also treated random graphs and showed that for n even and sufficiently large, with high probability $p(G_{n,1/2}, 1, n) \leq 3$. He conjectured that for every r, q there exists a constant $\tilde{c}_q$ so that with high probability $p(G_{n,1/2}, r, q) \leq \tilde{c}_q$. We resolve this conjecture in the affirmative with the following theorem.

Theorem 1.3. *Fix an integer $q \geq 2$ and let $0 \leq r < q$ be an integer. Then with high probability we have $p(G_{n,1/2}, r, q) \leq q + 1$.*

In light of the recent work of Balister, Powierski, Scott and Tan [2], this bound is the best possible. Specifically, they show that if X_n is the number of distinct partitions of $V(G_{n,1/2})$ into $V_1, \dots, V_q$, where all degrees in $G[V_i]$ are $r_i \pmod q$, then X_n is asymptotically Poisson in distribution for $q > 2$. For $q = 2$, they obtain a more complicated, but still explicit distribution. In both cases $\mathbb{P}[X_n = 0]$ is bounded away from zero.

We will use the second moment method to prove our theorems. The main difference between our approach and that of Scott is that when working with modulus $q > 2$, the arguments are more involved and more amenable to discrete Fourier analysis. Even though we do not believe that all of the Fourier-type lemmas appearing in this paper are new, we included full proofs as they may be of independent interest (for example, for an application of these lemmas to the singularity problem of random symmetric Bernoulli matrices, the reader is referred to [5]).

Notation Our graph theoretical notation is quite standard. In particular, for a graph $G = (V, E)$ and $U \subseteq V$, we use $G[U]$ to denote the subgraph induced by the set U.

As for linear algebraic notation, vectors will appear in boldface and their coordinates will not, and we opt for column vectors by default, e.g. $\boldsymbol{v} = (v_1, \dots, v_m)^T$. We write $\mathbb{Z}_q$ for the set of integers modulo $q \geq 2$, and for any $d \geq 1$, $\mathbf{1}_d$ denotes the vector $(1, \dots, 1)$ in $\mathbb{Z}_q^d$. If q is fixed, then we say that $\boldsymbol{u} \equiv \boldsymbol{v}$ if $u_i \equiv v_i \pmod q$ for all i. For any fixed integer q, we define the function $e_q : \mathbb{Z}_q \to \mathbb{C}$ by $e_q(x) = e^{2\pi i x/q}$. Finally, $\mathrm{Bern}(p)$ denotes a Bernoulli random variable with success probability p.

2 Auxiliary results

In this section we state and prove some auxiliary results, to be used in the proofs of our main theorems.

2.1 Chernoff's bounds

We will make use of the following tail estimates for binomial random variables.

Lemma 2.1 (Chernoff's inequality (see [1])). *Let $X \sim \mathrm{Bin}(n,p)$ and let $\mu = \mathbb{E}[X]$. Then*

- $\mathbb{P}[X < (1-a)\mu] < e^{-a^2\mu/2}$ *for every* $a > 0$*;*
- $\mathbb{P}[X > (1+a)\mu] < e^{-a^2\mu/3}$ *for every* $0 < a < 3/2$*.*

Remark 3. The conclusions of Chernoff's inequality remain the same when X has the hypergeometric distribution (see [7], Theorem 2.10).

2.2 Key technical lemmas

In each of the following lemmas, q denotes a fixed positive integer at least 2, all equivalences are modulo q, and we write $\boldsymbol{u} \equiv \boldsymbol{v} \pmod q$ for vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ when $u_i \equiv v_i \pmod q$ for all i. We believe that not all (if any) of the following lemmas are new, but since we could not find a convenient reference in the literature, we include complete proofs for all of them. We state the lemmas first, deferring their proofs to the next subsection.

The first lemma states that the distribution of the sum of many Bern(1/2) random variables modulo q is asymptotically uniform.

Lemma 2.2. *Let n be a positive integer and let $\xi_1, \dots, \xi_n$ be iid Bern$(1/2)$ random variables. Then for a fixed $a \in \mathbb{Z}_q$,*

$$\mathbb{P}[\xi_1 + \cdots + \xi_n \equiv a] = \frac{1}{q}\left(1 + e^{-\Omega(n)}\right).$$

As an immediate corollary, we have the following result for random matrices with iid Bern(1/2) entries.

Corollary 2.3. *Let M be a random $s \times t$ matrix whose entries are iid Bern$(1/2)$ random variables. Then for any $\boldsymbol{v} \in \mathbb{Z}_q^s$,*

$$\mathbb{P}[M\mathbf{1}_t \equiv \boldsymbol{v}] = \frac{1}{q^s}\left(1 + e^{-\Omega(t)}\right)^s.$$

We will primarily use this corollary in the regime $s \le n$ and $\omega(\log n) = t \le n$, in which case this quantity is $\frac{1}{q^s}(1 + o(1))$.

The second lemma states that a similar result still holds for *symmetric* Bernoulli random matrices. If M is the adjacency matrix of $G \sim G(m, 1/2)$, a random symmetric $0/1$ $m \times m$ matrix (with zero diagonal), then the j-th entry of $M\mathbf{1}_m$ is the degree of the j-th vertex. Observe that if q is even, since the sum of the degrees in a graph is even, we have that $M\mathbf{1}_m$ is always some vector $\boldsymbol{v} \in \mathbb{Z}_q^m$ for which $\sum_i v_i$ is even modulo q. Since there are exactly $q^m/2$ such vectors, we obtain slightly different distributions for $M\mathbf{1}_m \pmod q$ for even and odd q.

Lemma 2.4. *Let M be a random $m \times m$ symmetric matrix whose diagonal is zero and whose entries above the diagonal are iid Bern$(1/2)$ random variables. Fix $\boldsymbol{v} \in \mathbb{Z}_q^m$. Then,*

$$\mathbb{P}[M\mathbf{1}_m \equiv \boldsymbol{v}] = \begin{cases} \frac{1}{q^m}(1 + e^{-\Omega(m)})\,, & \text{if } q \text{ is odd} \\ \frac{2}{q^m}(1 + e^{-\Omega(m)})\,, & \text{if } q \text{ is even and } \sum_i v_i \text{ is even} \\ 0\,, & \text{if } q \text{ is even and } \sum_i v_i \text{ is odd.} \end{cases}$$

The third lemma is a uniformity result about the joint distribution of $\mathbf{1}_s^T M$ and $M\mathbf{1}_t$ for a random $s \times t$ matrix M with iid Bern$(1/2)$ entries.

Lemma 2.5. *Let s, t be sufficiently large integers satisfying $\omega(\log t) = s \le t$. If M is a random $s \times t$ matrix with iid Bern$(1/2)$ entries and $\boldsymbol{u} \in \mathbb{Z}_q^s$ and $\boldsymbol{v} \in \mathbb{Z}_q^t$ are such that $\sum u_i \equiv \sum v_j \pmod q$, then*

$$\mathbb{P}[\mathbf{1}_s^T M \equiv \boldsymbol{v}^T \text{ and } M\mathbf{1}_t \equiv \boldsymbol{u}] = \frac{1 + o(1)}{q^{s+t-1}}.$$

Observe that if $\boldsymbol{u} \in \mathbb{Z}_q^s$ and $\boldsymbol{v} \in \mathbb{Z}_q^t$ are such that $\sum u_i \not\equiv \sum v_j \pmod q$, then we clearly cannot find a $0/1$ matrix M for which $\mathbf{1}_s^T M \equiv \boldsymbol{v}$ and $M\mathbf{1}_t \equiv \boldsymbol{u}$. Moreover, since there are exactly q^{s+t-1} pairs $(\boldsymbol{u}, \boldsymbol{v})$ with $\sum u_i \equiv \sum_j v_j$, we see that for M distributed as above, the pair $(\mathbf{1}_s^T M, M\mathbf{1}_t)$ is approximately uniformly distributed among all "feasible" values.

2.3 Proofs of key lemmas

We shall prove the above lemmas using some elementary discrete Fourier analysis (for a thorough introduction, the reader is referred to [11]). In what follows, $\delta^{(m)} : \mathbb{Z}_q^m \to \{0, 1\}$ is given by:

$$\delta^{(m)}(\boldsymbol{x}) = \begin{cases} 1\,, & \text{if } \boldsymbol{x} \equiv \mathbf{0} \\ 0\,, & \text{if } \boldsymbol{x} \not\equiv \mathbf{0}. \end{cases}$$

Proof of Lemma 2.2. First note that the claim is clearly true for $q = 2$ since a sum of iid Bern$(1/2)$ random variables is even or odd with equal probability. In general, we write

$$\mathbb{P}[\xi_1 + \cdots + \xi_n \equiv a] = \mathbb{E}[\delta^{(1)}(\xi_1 + \cdots + \xi_n - a)],$$

and then expand $\delta^{(1)}$ into its Fourier series.

$$\mathbb{E}[\delta^{(1)}(\xi_1 + \cdots + \xi_n - a)] = \frac{1}{q} \sum_{\ell \in \mathbb{Z}_q} \mathbb{E}\big[e_q\big(\ell \cdot (\xi_1 + \cdots + \xi_n - a)\big)\big],$$

which, by independence, becomes

$$\begin{aligned} \frac{1}{q} \sum_{\ell \in \mathbb{Z}_q} e_q(-\ell a) \prod_{j=1}^{n} \mathbb{E}[e_q(\ell \xi_j)] &= \frac{1}{q} \sum_{\ell \in \mathbb{Z}_q} \left[e_q(-\ell a) \left(\frac{1 + e_q(\ell)}{2} \right)^n \right] \\ &= \frac{1}{q} + \frac{1}{q} \sum_{\ell \in \mathbb{Z}_q \setminus \{0\}} \left[e_q(-\ell a) \left(\frac{1 + e_q(\ell)}{2} \right)^n \right]. \end{aligned}$$

If we move the $1/q$ term to the left-hand side and apply the triangle inequality, we obtain

$$\left|\mathbb{P}[\xi_1 + \cdots + \xi_n \equiv a] - \frac{1}{q}\right| \leq \frac{1}{q}\sum_{\ell=1}^{q-1} |\cos(\pi\ell/q)|^n.$$

Note that when $q = 2$, the right-hand side above is simply zero. It is easy to verify with elementary calculus that for $1 \leq \ell \leq q-1$, we have

$$|\cos(\pi\ell/q)| \leq e^{-2/q^2}. \tag{1}$$

Using this, we obtain

$$\left|\mathbb{P}[\xi_1 + \cdots + \xi_n \equiv a] - \frac{1}{q}\right| \leq \frac{1}{q}\sum_{\ell=1}^{q-1} e^{-2n/q^2} = \frac{q-1}{q}e^{-2n/q^2}.$$

This completes the proof. □

Proof of Lemma 2.4. Like in the proof of Lemma 2.3, we write the probability of interest as the expectation of a delta function, and then expand it into its Fourier series.

$$\mathbb{P}[M\mathbf{1}_m \equiv \boldsymbol{v}] = \frac{1}{q^m}\sum_{\boldsymbol{\ell}\in\mathbb{Z}_q^m}\Bigg[\mathbb{E}\left[e_q\left(\boldsymbol{\ell}^T M\mathbf{1}_m\right)\right] e_q\left(-\boldsymbol{\ell}^T\boldsymbol{v}\right)\Bigg]. \tag{2}$$

Now, letting M_{jk} be the entries of the matrix M, by the fact that $M_{jk} = M_{kj}$ for all j and k, the right-hand side of (2) equals

$$\frac{1}{q^m}\sum_{\boldsymbol{\ell}\in\mathbb{Z}_q^m}\mathbb{E}\left[e_q\left(\sum_{j<k}(\ell_j+\ell_k)M_{jk}\right)\right] e_q\left(-\boldsymbol{\ell}^T\boldsymbol{v}\right),$$

which by independence becomes

$$\frac{1}{q^m}\sum_{\boldsymbol{\ell}\in\mathbb{Z}_q^m} e_q\left(-\boldsymbol{\ell}^T\boldsymbol{v}\right)\prod_{1\leq j<k\leq m}\left(\frac{1+e_q(\ell_j+\ell_k)}{2}\right). \tag{3}$$

Let us first consider the case where q is odd. The product in the above expression is 1 if and only if $\boldsymbol{\ell} \equiv \mathbf{0}$, in which case we isolate this term and estimate

$$\left|\mathbb{P}[M\mathbf{1}_m \equiv v] - \frac{1}{q^m}\right| \leq \frac{1}{q^m}\sum_{\boldsymbol{\ell}\in\mathbb{Z}_q^m\setminus\{\mathbf{0}\}}\prod_{1\leq j<k\leq m}\left|\cos\left(\frac{\pi}{q}(\ell_j+\ell_k)\right)\right|.$$

For each vector $\boldsymbol{\ell} \in \mathbb{Z}_q^m$, we let $a(\boldsymbol{\ell})$ be the number of pairs $1 \leq j < k \leq m$ for which $\ell_j + \ell_k \not\equiv 0 \pmod{q}$. Next, we again apply the bound $|\cos(\pi r/q)| \leq e^{-2/q^2}$ for $r \not\equiv 0 \pmod{q}$ to obtain

$$\left|\mathbb{P}[M\mathbf{1}_m \equiv v] - \frac{1}{q^m}\right| \leq \frac{1}{q^m}\sum_{\boldsymbol{\ell}\in\mathbb{Z}_q^m\setminus\{\mathbf{0}\}} e^{-2\cdot a(\boldsymbol{\ell})/q^2}.$$

Now let L_s be the set of all vectors $\boldsymbol{\ell} \in \mathbb{Z}_q^m$ with support of size exactly s, and let $L_{\geq s}$ be those with support of size at least s. We collect the terms in the above sum based on whether their support is small (less than $m/2$) or large (exceeding $m/2$) to get

$$\left|\mathbb{P}[M\mathbf{1}_m \equiv v] - \frac{1}{q^m}\right| \leq \frac{1}{q^m}\left(\sum_{1\leq s<m/2} |L_s|e^{-2s(m-s)/q^2} + \sum_{m/2\leq s\leq m} |L_s|e^{-s(s-2)/2q^2}\right).$$

The first sum comes from pairing the nonzero entries of $\boldsymbol{\ell} \neq \mathbf{0}$ with its zero entries, giving a bound of $a(\boldsymbol{\ell}) \geq s(m-s)$. For the second sum, start by considering the auxiliary graph on the nonzero entries of $\boldsymbol{\ell} \neq \mathbf{0}$ where we connect two vertices if they sum to zero modulo q. Since q is odd, this graph has no loops and is a vertex-disjoint union of complete bipartite graphs, with parts corresponding to residue classes of the entries of $\boldsymbol{\ell}$. The maximum number of edges in such a graph is $s^2/4$, which is achieved when half of the support is equal to r and the rest is equal to $-r$ for some residue r. The number of pairs of entries in the support of $\boldsymbol{\ell}$ that sum to a nonzero residue modulo q is then at least $\binom{s}{2} - s^2/4 = s(s-2)/4$. We then estimate $|L_s|$ and crudely bound $|L_{\geq m/2}|$ by q^m to obtain

$$\begin{aligned}\left|\mathbb{P}[M\mathbf{1}_m \equiv v] - \frac{1}{q^m}\right| &\leq \frac{1}{q^m}\left(\sum_{1\leq s<m/2} \binom{m}{s} q^s e^{-sm/q^2} + |L_{\geq m/2}|e^{-m^2/16q^2}\right)\\ &= \frac{1}{q^m}\cdot e^{-\Omega(m)}.\end{aligned}$$

When q is even, the entries of $M\mathbf{1}_m$ sum to an even residue modulo q, so $\mathbb{P}[M\mathbf{1}_m \equiv \boldsymbol{v}] = 0$ when $\boldsymbol{v}$ does not satisfy this condition. Assume then that $\sum_j v_j$ is an even residue modulo q. The product in (3) is 1 if and only if $\boldsymbol{\ell}$ is $\mathbf{0}$ or $\frac{q}{2}\cdot\mathbf{1}$, and since $e^{-2\pi i \boldsymbol{\ell}^T \boldsymbol{v}/q} = 1$ for these values of $\boldsymbol{\ell}$, these terms combine to give us a leading term of $\frac{2}{q^m}$. We isolate these terms and bound the difference

$$\begin{aligned}\left|\mathbb{P}[M\mathbf{1}_m \equiv v] - \frac{1}{q^m}\right| &= \left|\mathbb{P}[M\mathbf{1}_m = v] - \frac{2}{q^m}\right|\\ &\leq \frac{1}{q^m}\sum_{\boldsymbol{\ell}\in\mathbb{Z}_q^m\setminus\{\mathbf{0},\frac{q}{2}\cdot\mathbf{1}\}} \prod_{1\leq j<k\leq m}\left|\cos\left(\frac{\pi}{q}(\ell_j+\ell_k)\right)\right|\\ &\leq \frac{1}{q^m}\sum_{\boldsymbol{\ell}\in\mathbb{Z}_q^m\setminus\{\mathbf{0},\frac{q}{2}\cdot\mathbf{1}\}} e^{-2\cdot a(\boldsymbol{\ell})/q^2}.\end{aligned}$$

Like before, we let L_s denote the set of vectors in $\mathbb{Z}_q^m$ with support of size exactly s, and now we let $L_{s,t}$ denote the set of vectors in $\mathbb{Z}_q^m$ with support s and exactly t entries equal to $q/2$. We again split the above sum according to the size of the support of $\boldsymbol{\ell}$ and then further by the number of entries equal to $q/2$.

$$\begin{aligned}\left|\mathbb{P}[M\mathbf{1}_m \equiv v] - \frac{1}{q^m}\right| \leq \frac{1}{q^m}\Bigg(&\sum_{s=1}^{3m/4} |L_s|e^{-2s(m-s)/q^2} + \sum_{s=3m/4}^{m}\sum_{t=0}^{m/4} |L_{s,t}|e^{-(s-t)(s-t-2)/2q^2}\\ &+ \sum_{s=3m/4}^{m}\sum_{t=m/4}^{\min(s,m-1)} |L_{s,t}|e^{-2t(m-t)}\Bigg).\end{aligned}$$

The first sum comes from pairing up the zero and nonzero entries of $\boldsymbol{\ell} \in \mathbb{Z}_q^m \setminus \{\mathbf{0}, \frac{q}{2} \cdot \mathbf{1}\}$. For the second sum, we consider the graph whose vertex set consists of the nonzero, non-$q/2$ entries of $\boldsymbol{\ell}$ and apply the same argument from the odd q case. In the third sum, we pair the entries equal to $q/2$ with those that are not.

The first and second sums are $e^{-\Omega(m)}$ by the same argument used for odd q. To bound the third sum, note that $\ell_i + \ell_j \equiv 0 \pmod q$ if and only if $(\ell_i + q/2) + (\ell_j + q/2) \equiv 0 \pmod q$. Therefore, by adding $(q/2) \cdot \mathbf{1}$ to every vector considered in the third sum, we obtain a set of vectors with support at most $3m/4$. The third sum is then bounded by the first, so this upper bound for $\left|\mathbb{P}[M\mathbf{1}_m \equiv v] - \frac{1}{q^m}\right|$ is at most $e^{-\Omega(m)}/q^m$. □

Proof of Lemma 2.5. We use the same Fourier-based approach that we employed to prove Lemmas 2.3 and 2.4. We have

$$\begin{aligned}\mathbb{P}[\mathbf{1}_s^T M \equiv \boldsymbol{v},\ M\mathbf{1}_t \equiv \boldsymbol{u}] &= \mathbb{E}[\delta_0^{(t)}(\mathbf{1}_s^T M - \boldsymbol{v}^T) \cdot \delta_0^{(s)}(M\mathbf{1}_t - \boldsymbol{u})] \\ &= \frac{1}{q^{s+t}} \sum_{(\boldsymbol{\ell},\boldsymbol{m}) \in \mathbb{Z}_q^s \times \mathbb{Z}_q^t} \prod_{\substack{1 \le j \le s \\ 1 \le k \le t}} \mathbb{E}\big[e_q\big(M_{jk}\,(\ell_j + m_k)\big)\big] \cdot e_q\left(-\left(\boldsymbol{v^T m} + \boldsymbol{\ell}^T \boldsymbol{u}\right)\right).\end{aligned}$$

Note that for all pairs $(\boldsymbol{\ell}, \boldsymbol{m})$ for which $\ell_j + m_k \equiv 0 \pmod q$ for all j, k, we have that the product in the above expression equals 1. Moreover, it is easy to see that $\ell_j + m_k \equiv 0 \pmod q$ for all j, k if and only if there exists some $r \in \mathbb{Z}_q$ for which $\boldsymbol{m} \equiv r \cdot \mathbf{1}_t$ and $\boldsymbol{\ell} \equiv -r \cdot \mathbf{1}_s$. Since there are exactly q such pairs $(\boldsymbol{\ell}, \boldsymbol{m})$, by letting $\mathcal{Z}$ be the set of all pairs $(\boldsymbol{\ell}, \boldsymbol{m}) \in \mathbb{Z}_q^s \times \mathbb{Z}_q^t$ which are not of this form, we have

$$\mathbb{P}[\mathbf{1}_s^T M \equiv \boldsymbol{v},\ M\mathbf{1}_t \equiv \boldsymbol{u}] = \frac{1}{q^{s+t-1}} + \frac{1}{q^{s+t}} \sum_{(\boldsymbol{\ell},\boldsymbol{m}) \in \mathcal{Z}} \prod_{\substack{1 \le j \le s \\ 1 \le k \le t}} \mathbb{E}\big[e_q\big(M_{jk}\,(\ell_j + m_k)\big)\big] \cdot e_q\left(-\left(\boldsymbol{v^T m} + \boldsymbol{\ell}^T \boldsymbol{u}\right)\right).$$

If we let $N(z)$ be the set of all pairs $(\boldsymbol{\ell}, \boldsymbol{m}) \in \mathcal{Z}$ for which the number of non-zero residues among $\ell_i + m_j$, where $1 \le i \le s$ and $1 \le j \le t$, is exactly z, then the exponential bound for the cosine (1) gives

$$\left|\mathbb{P}[\mathbf{1}_s^T M \equiv \boldsymbol{v},\ M\mathbf{1}_t \equiv \boldsymbol{u}] - \frac{1}{q^{s+t-1}}\right| \le \frac{1}{q^{t+s}} \sum_z |N(z)| e^{-2z/q^2},$$

Note that if $z \ge z_0 := \frac{3}{2} q^2 (s+t) \log q$, then $e^{-2z/q^2} \le 1/q^{3(s+t)}$ and therefore, even if we use the crude bound $\sum_{z \ge z_0} |N(z)| \le q^{s+t}$, we obtain

$$\sum_{z \ge z_0} |N(z)| e^{-2z/q^2} \le \frac{1}{q^{2(s+t)}} = e^{-\Omega(s+t)}. \tag{4}$$

It is thus enough to prove that

$$\sum_{0 < z < z_0} |N(z)| e^{-2z/q^2} = o(1). \tag{5}$$

To this end, we fix $0 < z < z_0$ and investigate when $(\boldsymbol{\ell}, \boldsymbol{m}) \in N(z)$. Given a positive integer d and a vector $\boldsymbol{w} \in \mathbb{Z}_q^d$, we define the r-th *level set* of $\boldsymbol{w}$, $L_r(\boldsymbol{w}) \subseteq [d]$ for some $r \in \mathbb{Z}_q$, by

$$L_r(\boldsymbol{w}) = \{i : w_i \equiv r \pmod q\},$$

and we write $L_{\neq r}$ for the set of all other indices. Let us first observe that for $(\boldsymbol{\ell}, \boldsymbol{m}) \in \mathscr{Z}$, if there exists some residue r for which $|L_r(\boldsymbol{\ell})| \cdot |L_{\neq -r}(\boldsymbol{m})| > z$, then we have that $(\boldsymbol{\ell}, \boldsymbol{m}) \notin N(z)$.

Suppose that each level set of $\boldsymbol{m} \in \mathbb{Z}_q^t$ has size at most $t/2$. For any $\boldsymbol{\ell} \in \mathbb{Z}_q^s$, choose $r \in \mathbb{Z}_q$ such that $|L_r(\boldsymbol{\ell})| \geq s/q$. We have $|L_{\neq -r}(\boldsymbol{m})| \geq t/2$, which, for large s and t, implies that

$$|L_r(\boldsymbol{\ell})| \cdot |L_{\neq -r}(\boldsymbol{m})| \geq st/2q > z_0 > z$$

and therefore $(\boldsymbol{\ell}, \boldsymbol{m}) \notin N(z)$.

In order for $(\boldsymbol{\ell}, \boldsymbol{m})$ to lie in $N(z)$ it must then be the case that $\boldsymbol{m}$ has a (unique) level set of size exceeding $t/2$, say $a = L_r(\boldsymbol{m}) > t/2$. Observe that we cannot have $|L_{\neq -r}(\boldsymbol{\ell})| > z/a$, or else

$$|L_{\neq -r}(\boldsymbol{\ell})| \cdot |L_r(\boldsymbol{m})| > z.$$

Therefore, from now on we assume that $|L_{\neq -r}(\boldsymbol{\ell})| \leq z/a$ which is equivalent to $|L_{-r}(\boldsymbol{\ell})| \geq s - z/a$. Next, if $|L_{\neq r}(\boldsymbol{m})| \geq 2z/s$ then

$$|L_{-r}(\boldsymbol{\ell})| \cdot |L_{\neq r}(\boldsymbol{m})| \geq (s - z/a) \cdot 2z/s = 2z(1 - z/as) \geq 2z(1 - z/(st/2)),$$

which is larger than z for large s and t and we once again have that $(\boldsymbol{\ell}, \boldsymbol{m}) \notin N(z)$. We then assume that $|L_r(\boldsymbol{m})| > t - 2z/s$. Since $(\boldsymbol{\ell}, \boldsymbol{m}) \in \mathscr{Z}$, then $|L_{\neq -r}(\boldsymbol{\ell})| > 0$ or $|L_{\neq r}(\boldsymbol{m})| > 0$, and therefore the number of non-zero residues among $\ell_i + k_j$ is at least

$$|L_{-r}(\boldsymbol{\ell})| \cdot |L_{\neq r}(\boldsymbol{m})| + |L_{\neq -r}(\boldsymbol{\ell})| \cdot |L_r(\boldsymbol{m})| \geq \min\{s - z/a, t - 2z/s\}.$$

Since $z \leq z_0 = O(s+t)$, $a > t/2$, and $\omega(t) = s \leq t$, this is at least $s/2$ for large s and t. In particular, we see that $N(z)$ is empty for all $0 < z \leq s/2$. Therefore, we may assume that $s/2 < z < z_0$.

All in all, we have

$$\begin{aligned} |N(z)| &\leq \binom{s}{z/a} q^{z/a+1} \binom{t}{2z/s} q^{2z/s} \\ &\leq q \cdot (qt)^{z/a + 2z/s} \\ &\leq q \cdot e^{\frac{4z}{s} \cdot \log(q \cdot t)}. \end{aligned}$$

Indeed, we choose a residue r, at most z/a elements of $\boldsymbol{\ell}$ to fill out $L_{\neq -r}(\boldsymbol{\ell})$ and at most $2z/s$ elements of $\boldsymbol{m}$ for $L_{\neq r}(\boldsymbol{m})$. The last inequality follows from the fact that $a \geq t/2$ and $t \geq s$. Finally, we have

$$\begin{aligned} \sum_{0<z<z_0} |N(z)| e^{-2z/q^2} &= \sum_{z=s/2}^{z_0} |N(z)| e^{-2z/q^2} \\ &\leq \sum_{z=s/2}^{z_0} \exp\left[z \left(\frac{4\log(qt)}{s} - \frac{2}{q^2} \right) \right]. \end{aligned}$$

Now, since $s = \omega(\log t)$, the argument of the exponential is negative for all z when s, t are sufficiently large, in which case we have

$$\sum_{z \leq z_0} |N(z)| e^{-2z/q^2} \leq z_0 \cdot \exp\left[\frac{s}{2} \left(\frac{4\log(qt)}{s} - \frac{2}{q^2} \right) \right].$$

Since $z_0 = \frac{3}{2} q^2 (s+t) \log q \leq 3q^2 t \log q$ and $s = \omega(\log t)$, the above quantity is $o(1)$. We have then established (5), which combined with (4) gives the desired conclusion. □

3 Large induced subgraphs

Here we prove Theorem 1.1 with the second moment method and then make slight modifications to this proof to arrive at Theorem 1.2.

3.1 Proof of Theorem 1.1

The strategy is to first show that we expect $G := G_{n,1/2}$ to have many induced subgraphs of the type specified by Theorem 1.1 (in particular, such subgraphs are of order linear in n for n sufficiently large). Next we will show that this number of good subgraphs is asymptotically concentrated around its mean and then apply Chebyshev's inequality to conclude that G has a good subgraph with high probability.

Proof of Theorem 1.1. For simplicity, we will assume throughout the proof that q is odd and point out where special considerations need to be made for even q. We may further assume that $q \geq 3$ since the (slightly simpler) case of $q = 2$ was handled by Scott in [9].

Fix a positive integer k to be determined later, and let X_k be the number of k-vertex induced subgraphs of $G := G_{n,1/2}$, all of whose degrees are $r \pmod q$, henceforth known as "good" subgraphs. Such subgraphs correspond to $k \times k$ principal submatrices[1] B of $A(G)$, the adjacency matrix of G, satisfying $B\mathbf{1}_k \equiv r\mathbf{1}_k \pmod q$. Our goal then is to show that we can choose k to be linear in n and have X_k positive with high probability for large n. By Lemma 2.4, the expected number of good subgraphs is

$$\mathbb{E}[X_k] = \binom{n}{k}\left(\frac{1}{q^k} + \frac{o(1)}{q^k}\right) \tag{6}$$

when q is odd (and twice this when q is even) and kr is even, and zero otherwise (the sum of the degrees must be even; we can escape this by taking k to be even). Now define the function g by

$$g(k) = \binom{n}{k}\frac{1}{q^k}$$

and choose k' to be the greatest integer such that $g(k')$ is at least 1. For any positive integer t, we have that

$$g(k'+t) \leq \left(\frac{n-k'}{(k'+1)q}\right)^t g(k').$$

Since $g(k) \geq (\frac{n}{qk})^k$, we see that $g(k) \geq 1$ when $k \leq n/q$, so $k' \geq n/q$ and $(k'+1)q \geq n$ (for a sharper bound, see Remark 1). Then the first factor on the right-hand side can be bounded from above by c^t for some constant $c < 1$ depending only on q. Since $\frac{g(k)}{g(k+1)} = q \cdot \frac{k+1}{n-k}$ for any k, our choice of k' ensures that we may bound $g(k')$ above by a constant. If we set $t = \lceil \log^{10} n \rceil$, then we may conclude that $g(k'+t) = o(1)$, so $X_{k'+t} = 0$ with high probability by Markov's inequality. In the other direction, observe that

$$g(k'-t) \geq \left(\frac{k'-t+1}{n-k'+t}q\right)^t g(k').$$

As $k' \geq n/q$, this quantity is exponentially large in t, and it follows that $\mathbb{E}[X_{k'-t}] = e^{\Omega(\log^{10} n)}$.

[1] B is a principal submatrix of the $n \times n$ matrix A if there is some subset $I \subseteq [n]$ such that B is obtained after deleting all rows and columns from A whose indices are not in I.

Now we set $k = k' - \log^{10} n$ and show that X_k is asymptotically concentrated around its mean. To this end, it suffices to show that $\operatorname{Var}[X_k] = o(\mathbb{E}[X_k]^2)$ and to apply Chebyshev's inequality. For every $I \in \binom{V}{k}$, where $\binom{V}{k}$ consists of all size-k subsets of V, we let X_I be the random variable indicating whether or not $G[I]$ is a good subgraph. We write the variance of X_k in terms of these indicator variables.

$$\operatorname{Var}[X_k] = \sum_{I \in \binom{V}{k}} \operatorname{Var}[X_I] + \sum_{I,J \in \binom{V}{k} : I \neq J} \operatorname{Cov}(X_I, X_J) \leq \mathbb{E}[X_k] + \sum_{I,J \in \binom{V}{k} : I \neq J} \operatorname{Cov}(X_I, X_J). \tag{7}$$

As $\mathbb{E}[X_k]$ is clearly $o(\mathbb{E}[X_k]^2)$, it suffices to show that the same is true for the covariance sum.

If the sets I and J are disjoint, then their corresponding submatrices do not overlap, so the variables X_I and X_J are independent and $\operatorname{Cov}(X_I, X_J) = 0$. On the other hand, if $|I \cap J|$ is large, say greater than $k - \log^2 n$, then the submatrices corresponding to I and J share many entries and $\operatorname{Cov}(X_I, X_J)$ may be large. Let $\mathcal{B}$ be the collection of all pairs of such sets with large overlap,

$$\mathcal{B} = \left\{ (I, J) : I, J \in \binom{V}{k},\ I \neq J,\ |I \cap J| \geq k - \log^2 n \right\} \tag{8}$$

We can estimate the size of $\mathcal{B}$ as follows. Suppose $|I \cap J| \geq k - t$ for some $0 \leq t \leq \log^2 n$. First choose the set I. Then choose $k - t$ vertices of I to also belong to J and then choose the remaining $k - t$ vertices of J.

$$|\mathcal{B}| = \sum_{t=1}^{\log^2 n} \binom{n}{k} \binom{k}{k-t} \binom{n-k}{t} \leq \binom{n}{k} \binom{k}{\log^2 n} \binom{n-k}{\log^2 n} \log^2 n.$$

Let us bound the contribution of $\mathcal{B}$ to the variance of X_k. For any $I' \in \binom{V}{k}$ we have

$$\begin{aligned} \sum_{(I,J) \in \mathcal{B}} \operatorname{Cov}(I, J) &\leq \binom{n}{k} \binom{k}{\log^2 n} \binom{n-k}{\log^2 n} \log^2 n \cdot \max_{(I,J) \in \mathcal{B}} \mathbb{E}[X_I X_J] \\ &\leq \binom{n}{k} \binom{k}{\log^2 n} \binom{n}{\log^2 n} \log^2 n \cdot \mathbb{E}[X_{I'}] \\ &= \binom{k}{\log^2 n} \binom{n-k}{\log^2 n} \log^2 n \cdot \mathbb{E}[X_k] \\ &= o(\mathbb{E}[X_k]^2), \end{aligned} \tag{9}$$

where the last line follows from using Stirling to bound both of the binomial coefficients by $e^{O(\log^3 n)}$ and the fact that $\mathbb{E}[X_k] = e^{\Omega(\log^{10} n)}$.

Now consider the collection of pairs with small overlap, $\mathcal{B}'$, given by

$$\mathcal{B}' = \left\{ (I, J) : I, J \in \binom{V}{k},\ I \neq J,\ |I \cap J| < k - \log^2 n \right\}$$

We stratify $\mathcal{B}'$ according to the size of the overlap. Suppose that $(I, J) \in \mathcal{B}'$ and $|I \cap J| = d$. The corresponding covariance term is

$$\operatorname{Cov}(X_I, X_J) = \mathbb{P}[A_I \mathbf{1}_k \equiv r\mathbf{1}_k,\ A_J \mathbf{1}_k \equiv r\mathbf{1}_k] - \mathbb{P}[A_I \mathbf{1}_k \equiv r\mathbf{1}_k] \cdot \mathbb{P}[A_J \mathbf{1}_k \equiv r\mathbf{1}_k],$$

where A_I is the principal submatrix of $A(G)$ obtained by removing row and column i for all $i \notin I$. Suppose that A_I and A_J are both adjacency matrices of good subgraphs. By Lemma 2.4, $\mathbb{P}[A_I\mathbf{1}_k \equiv r\mathbf{1}_k] = \frac{1}{q^k}(1+e^{-\Omega(k)})$ when q is odd and twice this when q and k are both even.

Without loss of generality, A_I and A_J overlap on the upper left $d \times d$ corner of A_J, which we call U. In order for $A_J\mathbf{1}_k \equiv r\mathbf{1}_k$ to hold, the upper right $d \times (k-d)$ submatrix of A_J, call it M, must complete the first d rows of A_J so that they each sum to $r \pmod q$. This event, which we call E_{asym}, occurs precisely when

$$M\mathbf{1}_{k-d} = r\mathbf{1}_d - U\mathbf{1}_d$$

By the symmetry of A_J, the submatrix M determines the lower left $(k-d) \times d$ submatrix of A_J. The lower-right $(k-d) \times (k-d)$ submatrix, call it L, must then complete the bottom $k-d$ rows so that they each sum to $r \pmod q$. This event, which we call E_{sym}, occurs when

$$L\mathbf{1}_{k-d} = r\mathbf{1}_d - M^T\mathbf{1}_d$$

This is illustrated in Figure 1.

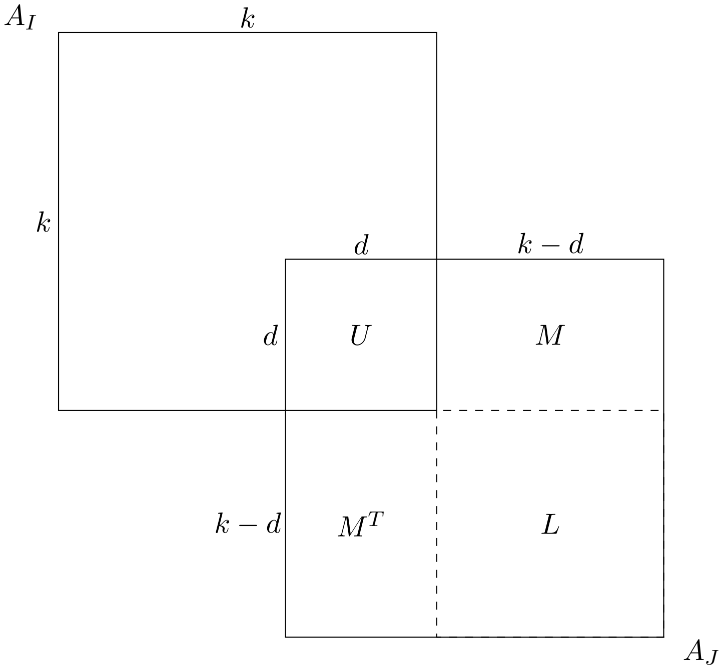


Figure 1: Overlapping submatrices, A_I and A_J, of $A(G)$.

The first term in $\mathrm{Cov}(X_I, X_J)$ is then

$$\begin{aligned}\mathbb{P}[A_I\mathbf{1}_k \equiv r\mathbf{1}_k,\ A_J\mathbf{1}_k \equiv r\mathbf{1}_k] &= \mathbb{P}[A_I\mathbf{1}_k \equiv r\mathbf{1}_k] \cdot \mathbb{P}[A_J\mathbf{1}_k \equiv r\mathbf{1}_k \mid A_I\mathbf{1}_k \equiv r\mathbf{1}_k] \\ &= \mathbb{P}[A_I\mathbf{1}_k \equiv r\mathbf{1}_k] \cdot \mathbb{P}[E_{asym} \mid A_I\mathbf{1}_k \equiv r\mathbf{1}_k] \cdot \mathbb{P}[E_{sym} \mid E_{asym},\ A_I\mathbf{1}_k \equiv r\mathbf{1}_k].\end{aligned}$$

Now for any value $r\mathbf{1}_d - U\mathbf{1}_d$ takes, $M\mathbf{1}_{k-d}$ takes this same value with probability $1/q^d$ plus some uniformly small error by Corollary 2.3, so

$$\mathbb{P}[E_{asym} \mid A_I\mathbf{1}_k \equiv r\mathbf{1}_k] = \frac{1}{q^d}\left(1+e^{-\Omega(k-d)}\right)^d = \frac{1}{q^d}\left(1+e^{-\Omega(\log^2 n)}\right)^d.$$

Similarly, $L\mathbf{1}_{k-d}$ takes all values in $\mathbb{Z}_q^{k-d}$ with probability $1/q^{k-d}$ plus some uniformly bounded error by Lemma 2.4, so

$$\mathbb{P}[E_{sym} \mid E_{asym},\ A_I\mathbf{1}_k \equiv r\mathbf{1}_k] = \frac{1}{q^{k-d}}\left(1+e^{-\Omega(k-d)}\right) = \frac{1}{q^{k-d}}\left(1+e^{-\Omega(\log^2 n)}\right).$$

For even q, we double this probability since $L\mathbf{1}_{k-d}$ takes only the values in $\mathbb{Z}_q^{k-d}$ whose entrywise sums are even. We then have

$$\mathbb{P}[A_I\mathbf{1}_k \equiv r\mathbf{1}_k,\ A_J\mathbf{1}_k \equiv r\mathbf{1}_k] = \frac{1}{q^k}\left(1+e^{-\Omega(n)}\right)\cdot\frac{1}{q^d}\left(1+e^{-\Omega(\log^2 n)}\right)^d\cdot\frac{1}{q^{k-d}}\left(1+e^{-\Omega(\log^2 n)}\right), \tag{10}$$

with the first and third factors doubled when q is even. Thus, the covariance becomes

$$\mathrm{Cov}(X_I,X_J) = \frac{1}{q^k}\left(1+e^{-\Omega(n)}\right)\cdot\frac{1}{q^d}\left(1+e^{-\Omega(\log^2 n)}\right)^d\cdot\frac{1}{q^{k-d}}\left(1+e^{-\Omega(\log^2 n)}\right) - \frac{1}{q^{2k}}\left(1+e^{-\Omega(n)}\right)^2, \tag{11}$$

and four times this when q is even. Since $k=\Theta(n)$ and $d \le k-\log^2 n$, the above quantity is $\frac{1}{q^{2k}}\cdot o(1)$, from which we conclude

$$\sum_{(I,J)\in\mathcal{B}'}\mathrm{Cov}(X_I,X_J) \le \binom{n}{k}^2\cdot\frac{1}{q^{2k}}\cdot o(1) = o(\mathbb{E}[X_k]^2). \tag{12}$$

Combining (7), (9) and (12), we see that $\mathrm{Var}[X_k] = o(\mathbb{E}[X_k])^2$, so with high probability G contains a good subgraph of order k. □

3.2 Proof of Theorem 1.2

In order to prove Theorem 1.2, we only need to make a few changes to the proof of Theorem 1.1. Consequently, we present an overview of the proof, again assuming that q is odd for convenience and mentioning the modifications needed to make it work for even q.

Proof of Theorem 1.2. Recall that $\boldsymbol{\alpha} = (\alpha_0,\ldots,\alpha_{q-1})$ encodes the proportions of the degrees modulo q in the desired subgraph, i.e. our subgraph should have an α_i proportion of its degrees congruent to i modulo q. Given an integer k and any $k_0,\ldots,k_{q-1}$ with $k_i \in \{\lceil\alpha_i k\rceil, \lfloor\alpha_i k\rfloor\}$ and $k_0+\cdots+k_{q-1}=k$, let $S_{k_0,\ldots,k_{q-1}}$ be the set of vectors $v\in\mathbb{Z}_q^k$ having k_i many entries congruent to $i \pmod q$ for all i. The size of $S_{k_0,\ldots,k_{q-1}}$ is given by the multinomial coefficient

$$|S_{k_0,\ldots,k_{q-1}}| = \binom{k}{k_0,\ldots,k_{q-1}}.$$

We use Lemma 2.4 to estimate the probability that $M\mathbf{1}_k$ lies in $S_{k_0,\ldots,k_{q-1}}$, where M is any $k\times k$ principal submatrix of $A(G)$:

$$\mathbb{P}[M\mathbf{1}_k \in S_{k_0,\ldots,k_{q-1}}] = |S_{k_0,\ldots,k_{q-1}}|\left(\frac{1}{q^k}+\frac{o(1)}{q^k}\right),$$

for odd q (and twice this when q is even) and when k and $\boldsymbol{\alpha}$ give rise to a valid degree sequence modulo q. The remainder of the proof is nearly identical to that of Theorem 1.1. If X_k is the number of subgraphs of G of order k with degree distribution given by $\boldsymbol{\alpha}$ ("good" subgraphs for short), then

$$\mathbb{E}[X_k] = \binom{k}{k_0, \ldots, k_{q-1}} \binom{n}{k} \left(\frac{1}{q^k} + \frac{o(1)}{q^k} \right).$$

Let k' be the largest integer such that $|S_{k_0,\ldots,k_{q-1}}|\binom{n}{k}\frac{1}{q^k} \geq 1$ for all choices of the k_i as described above, and let $\epsilon > 0$ be arbitrarily small. A routine calculation (see Appendix) shows that

$$\mathbb{E}[X_{k'+\epsilon n}] = o(1) \text{ and } \mathbb{E}[X_{k'-\epsilon n}] = 2^{f(\epsilon)n} \text{ for some function } f. \tag{13}$$

In particular, by Markov's inequality we obtain that, with high probability, $X_{k'+\epsilon n} = 0$. Now, let $k := k' - \epsilon n$, and as in the proof of the previous theorem, we will show that $\mathrm{Var}[X_k] = o(\mathbb{E}[X_k]^2)$. As per (7), it suffices to show that

$$\sum_{I,J \in \binom{V}{k} : I \neq J} \mathrm{Cov}(X_I, X_J) = o(\mathbb{E}[X_k]^2),$$

where X_I and X_J indicate whether I and J span good subgraphs (now a good subgraph is one whose distribution of degrees is given by $\boldsymbol{\alpha}$). Letting $\mathcal{B}$ be as in (8), calculation (9) carries over exactly, so we have

$$\sum_{(I,J)\in\mathcal{B}} \mathrm{Cov}(I, J) = o(E[X_k]^2).$$

The calculation for the contribution of $\mathcal{B}'$ to the variance is nearly identical to the corresponding calculation in the proof of Theorem 1.1. For any k, I, and J we have

$$\mathrm{Cov}(X_I, X_J) = \mathbb{P}[A_I\mathbf{1}_k, A_J\mathbf{1}_k \in S_{k_0,\ldots,k_{q-1}}] - \mathbb{P}[A_I\mathbf{1}_k \in S_{k_0,\ldots,k_{q-1}}]\mathbb{P}[A_J\mathbf{1}_k \in S_{k_0,\ldots,k_{q-1}}].$$

By Lemma 2.4, $\mathbb{P}[A_I\mathbf{1}_k \in S_{k_0,\ldots,k_{q-1}}] = \mathbb{P}[A_J\mathbf{1}_k \in S_{k_0,\ldots,k_{q-1}}] = |S_{k_0,\ldots,k_{q-1}}|\frac{1}{q^k}(1 + e^{-\Omega(n)})$ when q is odd and twice this when q and k are both even. We also have

$$\begin{aligned}\mathbb{P}[A_I\mathbf{1}_k \in S_{k_0,\ldots,k_{q-1}},\ A_J\mathbf{1}_k \in S_{k_0,\ldots,k_{q-1}}] &= \sum_{\boldsymbol{u},\boldsymbol{v}\in S_{k_0,\ldots,k_{q-1}}} \mathbb{P}[A_I\mathbf{1}_k = \boldsymbol{u},\ A_J\mathbf{1}_k = \boldsymbol{v}] \\ &\leq |S_{k_0,\ldots,k_{q-1}}|^2 \cdot \max_{\boldsymbol{u},\boldsymbol{v}\in S_{k_0,\ldots,k_{q-1}}} \mathbb{P}[A_I\mathbf{1}_k = \boldsymbol{u},\ A_J\mathbf{1}_k = \boldsymbol{v}].\end{aligned}$$

We can estimate $\mathbb{P}[A_I\mathbf{1}_k = \boldsymbol{u},\ A_J\mathbf{1}_k = \boldsymbol{v}]$ just as we estimated $\mathbb{P}[A_I\mathbf{1}_k = r\mathbf{1}_k,\ A_J\mathbf{1}_k = r\mathbf{1}_k]$ for some fixed r in the proof of Theorem 1.1. To elaborate, if $|I \cap J| = d \leq k - \log^2 n$, then by (10) we have

$$\max_{\boldsymbol{u},\boldsymbol{v}\in S_{k_0,\ldots,k_{q-1}}} \mathbb{P}[A_I\mathbf{1}_k = \boldsymbol{u},\ A_J\mathbf{1}_k = \boldsymbol{v}] = \frac{1}{q^k}\left(1 + e^{-\Omega(n)}\right) \cdot \frac{1}{q^d}\left(1 + e^{-\Omega(\log^2 n)}\right)^d \cdot \frac{1}{q^{k-d}}\left(1 + e^{-\Omega(\log^2 n)}\right)$$

when q is odd (see the discussion immediately before (10) for slight changes needed when q is even). Since $d \leq k - \log^2 n$ and $k = \Theta(n)$, this is $\frac{1}{q^{2k}}(1 + o(1))$. In particular, $\sum_{(I,J)\in\mathcal{B}'} \mathrm{Cov}(X_I, X_J) = |S_{k_0,\ldots,k_{q-1}}|^2 \cdot \frac{1}{q^{2k}} \cdot o(1)$ and so $\mathrm{Var}[X_k] = o(E[X_k]^2)$. □

4 Packing

We employ another second moment argument to prove Theorem 1.3. Before getting into the proof we introduce some terminology. Suppose $V(G) = V_1 \cup \ldots \cup V_t$ is a partition of the vertex set of a graph G, and $n_i := |V_i|$ for all i. Such a partition is *balanced* if $n_i \in \{\lfloor n/t \rfloor, \lceil n/t \rceil\}$ for all i. For any fixed integers $q \geq 2$ and $0 \leq r < q$, we call a partition $V(G) = V_1 \cup \ldots \cup V_t$ an (r, q)*-partition* if each vertex in $G[V_i]$ has degree congruent to $r \pmod q$ for all $i \leq t$.

Now let us assume for simplicity that q is odd (the case of $q = 2$ was settled by Scott in [10]; for other even q, whenever we use Lemma 2.4 one needs to multiply the estimate by 2) and let $t = q + 1$ for the remainder of this proof. Let X be the number of balanced (r, q)-partitions of the vertex set of $G := G_{n,1/2}$ into t parts $V_1, \ldots, V_t$. By Lemma 2.4, for every $1 \leq i \leq t$, the probability that all the vertices in the induced subgraph $G[V_i]$ have degree $r \pmod q$ is $\frac{1}{q^{n_i}}(1 + o(1))$. We then have

$$\begin{aligned}
\mathbb{E}[X] &= \binom{n}{n_1, \ldots, n_t} \cdot \frac{(1 + o(1))^t}{q^n} \\
&= \frac{n!}{\prod_{i=1}^t n_i!} \cdot \frac{1 + o(1)}{q^n} \\
&\geq n^{-O(1)} \frac{n^n}{(n/t)^n} \cdot \frac{1}{q^n} \\
&= n^{-O(1)} \left(\frac{q+1}{q}\right)^n = e^{\Theta(n/q)},
\end{aligned}$$

where the second to last equality holds by Stirling's approximation.

In particular we have that the expected number of balanced (r, q)-partitions with t parts is exponentially large in n (assuming that q is fixed). Note that taking $t = q + 1 > q$ is critical in achieving this exponential bound, and for smaller values of t the expectation has a smaller order of magnitude. Indeed, as Balister, Powierski, Scott and Tan show in [2], the number of balanced (r, q)-partitions of $G_{n,1/2}$ with q parts is distributed like a Poisson random variable (for $q > 2$ at least; the $q = 2$ case is more nuanced, but there is still no "with high probability" statement).

Now we need to show that $\mathrm{Var}[X] = o(\mathbb{E}[X]^2)$ and then apply Chebyshev's inequality. To this end, let $\mathcal{P}_t$ be the set of all balanced partitions of $V(G)$ into t parts. Specifically, an element $\mathcal{U}$ of $\mathcal{P}_t$ is a collection of t subsets of $V(G)$, $U_1, \ldots, U_t$, that form a balanced partition. We also let $X_\mathcal{U}$ denote the random variable indicating whether or not the partition $\mathcal{U} \in \mathcal{P}_t$ is an (r, q)-partition. Using this notation, we write $X = \sum_{\mathcal{U} \in \mathcal{P}_t} X_\mathcal{U}$ and our goal becomes estimating $\sum_{\mathcal{U},\mathcal{V} \in \mathcal{P}_t} \mathrm{Cov}(X_\mathcal{U}, X_\mathcal{V})$.

We will achieve this goal by defining a collection $\mathcal{T}_t$ of pairs of partitions $(\mathcal{U}, \mathcal{V})$ that behave more or less independently of one another, i.e. the probability that both are simultaneously (r, q)-partitions is around q^{-2n}, and hence their covariance is small. We will show that this independent behavior is typical, in the sense that most pairs behave this way (precise definitions of "typical" and "small" will follow). Then we split the sum to be estimated into one over the collection of typical pairs and one over the remaining pairs:

$$\sum_{\mathcal{U},\mathcal{V} \in \mathcal{P}_t} \mathrm{Cov}(X_\mathcal{U}, X_\mathcal{V}) = \sum_{(\mathcal{U},\mathcal{V}) \in \mathcal{T}_t} \mathrm{Cov}(X_\mathcal{U}, X_\mathcal{V}) + \sum_{(\mathcal{U},\mathcal{V}) \in \mathcal{T}_t^C} \mathrm{Cov}(X_\mathcal{U}, X_\mathcal{V}).$$

The first sum is small compared to $\mathbb{E}[X]^2$ because $\mathrm{Cov}(X_\mathcal{U}, X_\mathcal{V})$ is small for typical pairs $(\mathcal{U}, \mathcal{V})$, which make up the majority of all pairs. While $\mathrm{Cov}(X_\mathcal{U}, X_\mathcal{V})$ might be larger for atypical pairs, a negligible proportion of all pairs behave this way.

We expect two partitions $\mathcal{U}, \mathcal{V}$ to behave (nearly) independently if their parts are all "significantly different" from each other. This intuition motivates the following definition.

Definition 4.1. *A pair $(\mathcal{U}, \mathcal{V}) \in \mathcal{P}_t^2$ is called* typical *if for all i and j we have $|U_i \cap V_j| \le n/3t$. We call all other pairs* atypical. *The set $\mathcal{T}_t$ consists exactly of all typical pairs in $\mathcal{P}_t^2$.*

Note that in any typical pair of partitions $(\mathcal{U}, \mathcal{V})$, we have that each U_i intersects at least three parts of $\mathcal{V}$ in at least, say, $\log^2 n$ vertices (and the same is true if we reverse the roles of $\mathcal{U}$ and $\mathcal{V}$). Now we show that this definition ensures the desired behavior.

Claim 4.2. *If $(\mathcal{U}, \mathcal{V}) \in \mathcal{T}_t$, then $Cov(X_{\mathcal{U}}, X_{\mathcal{V}}) = o(1)/q^{2n}$.*

Proof. Let $(\mathcal{U}, \mathcal{V}) \in \mathcal{T}_t$ and write $\mathcal{U} = \{U_1, \dots, U_t\}$ and $\mathcal{V} = \{V_1, \dots V_t\}$. We reveal portions of the subgraphs $G[U_i]$ in stages. In the first stage, depicted in Figure 2 (a), reveal the edges in $G[U_i \cap V_j]$ for all $1 \le i, j \le t$. If we look at the adjacency matrix $A(G[U_i])$ for some i, then we have revealed a sequence of block submatrices along its diagonal. By the pigeonhole principle, we may choose, for each i, an index j_i such that $|U_i \cap V_{j_i}| \ge n/t$ (note that the j_i's are not necessarily distinct indices). We arrange the vertices in G so that, for each i, the induced subgraph $G[U_i \cap V_{j_i}]$ corresponds to the bottom-right corner of the matrix $A(G[U_i])$.

In the second stage, for each i, reveal the remaining edges in $G[U_i \setminus V_{j_i}]$, i.e. those edges in $G[U_i]$ not incident to any vertex in V_{j_i}. This reveals the upper-left corner of $A(G[U_i])$, as shown in Figure 2 (b). The still unrevealed edges in $G[U_i]$ correspond to those that cross between V_{j_i} and $U_i \setminus V_{j_i}$. Let M_i be the portion of $A(G[U_i])$ corresponding to these vertices, the upper-right corner, and let its size be $s_i \times t_i$. In order for $G[U_i]$ to have all degrees congruent to $r \pmod q$, we must have

$$M_i \mathbf{1}_{t_i} \equiv r \cdot \mathbf{1}_{s_i} - A(G[U_i \setminus V_{j_i}])\mathbf{1}_{s_i}, \qquad \text{and} \qquad \mathbf{1}_{s_i}^T M_i \equiv (r\mathbf{1}_{t_i} - A(G[U_i \cap V_{j_i}])\mathbf{1}_{t_i})^T, \tag{14}$$

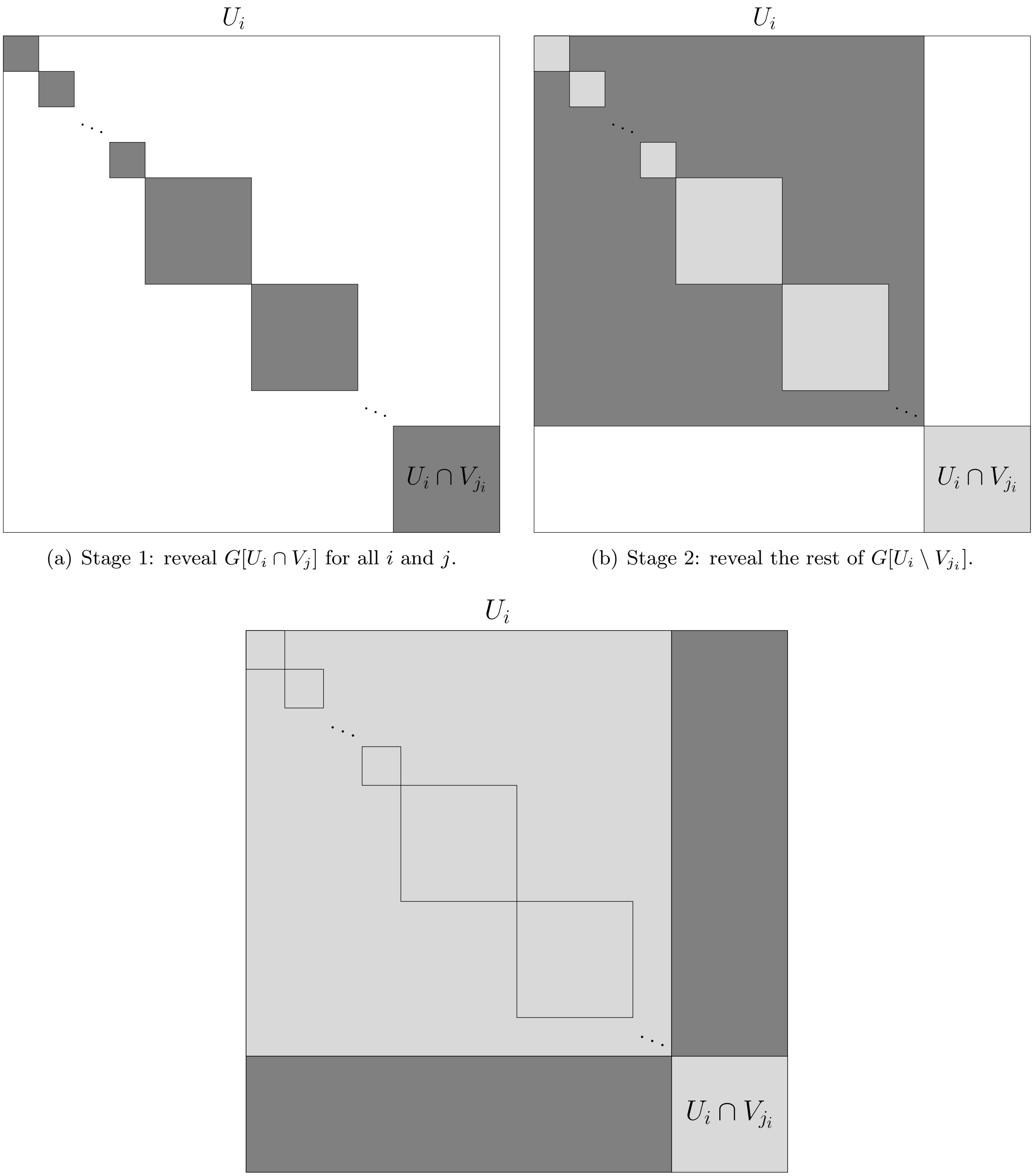
which gives us the following necessary condition on $A(G[U_i \cap V_{j_i}])$ and $A(G[U_i \setminus V_{j_i}])$ after the second stage of revealing entries:

$$r \cdot |U_i \setminus V_{j_i}| - \mathbf{1}_{s_i}^T A(G[U_i \setminus V_{j_i}])\mathbf{1}_{s_i} \equiv r \cdot |U_i \cap V_{j_i}| - \mathbf{1}_{t_i}^T A(G[U_i \cap V_{j_i}])\mathbf{1}_{t_i}. \tag{15}$$

We say that the subgraphs $G[U_i \cap V_{j_i}]$ and $G[U_i \setminus V_{j_i}]$ are *compatible* in $G[U_i]$ when congruence (15) holds, and Lemma 2.5, applied to M_i and (14), gives the probability that $G[U_i]$ has all degrees congruent to $r \pmod q$ given this compatibility.

Note that the compatibility condition (15) depends only on the numbers of edges in $G[U_i \cap V_{j_i}]$ and $G[U_i \setminus V_{j_i}]$ modulo q. Here is where the typicality of $(\mathcal{U}, \mathcal{V})$ comes into play. Since $(\mathcal{U}, \mathcal{V})$ is typical, U_i intersects at least two other parts of $\mathcal{V}$ other than V_{j_i} in at least $\log^2 n$ vertices, so the number of entries revealed in the second stage is $\Omega(\log^4 n)$. By Lemma 2.2, the probability that $G[U_i \cap V_{j_i}]$ and $G[U_i \setminus V_{j_i}]$ are compatible in $G[U_i]$ is $\frac{1+o(1)}{q}$. In other words, there is indeed enough dark gray area in Figure 2 (b) to ensure that the probability that $G[U_i \cap V_{j_i}]$ and $G[U_i \setminus V_{j_i}]$ are compatible in $G[U_i]$ is reasonably close to $1/q$.

In the third and final stage, shown in Figure 2 (c), we reveal the remaining edges in $G[U_i]$, which are those that cross between $U_i \cap V_{j_i}$ and $U_i \setminus V_{j_i}$ and correspond to the matrix M_i. We condition on $G[U_i \cap V_{j_i}]$ and $G[U_i \setminus V_{j_i}]$ being compatible in $G[U_i]$, and since the corresponding part of the adjacency matrix has dimensions $\Omega(\log^2 n) \times \Omega(n)$, we may apply Lemma 2.5 to conclude that this revealing step produces a good subgraph with probability $\frac{1+o(1)}{q^{|U_i|-1}}$. Each revealing step in U_i is independent



(a) Stage 1: reveal $G[U_i \cap V_j]$ for all i and j.

(b) Stage 2: reveal the rest of $G[U_i \setminus V_{j_i}]$.

(c) Stage 3: reveal the rest of $G[U_i]$.

Figure 2: The adjacency matrix of $G[U_i]$ when performing the three revealing stages.

of the revealing steps in $U_{i'}$ for distinct i, i', so each $G[U_i]$ is good independently with probability $\frac{1+o(1)}{q^{|U_i|}}$.

We repeat the three revealing stages for partition $\mathcal{V}$. Since $\mathcal{V}$ is typical, each V_i intersects at least three parts of $\mathcal{U}$ in at least $\log^2 n$ vertices and for each i, we choose an index j_i such that $|V_i \cap U_{j_i}| \geq \log^2 n$. The first stage would have us reveal $G[V_i \cap U_j]$ for all i and j, but we have already revealed these subgraphs. In the second stage we reveal, for each i, the edges in $G[V_i]$ not incident to any vertex in U_{j_i}. Each such edge crosses between $G[V_i \cap U_j]$ and $G[V_i \cap U_{j'}]$ for some $j \neq j'$ with neither j nor j' equal to j_i. Prior to this step we had only revealed the edges in the induced subgraphs $G[U_i]$ for all i, so no such crossing was revealed. Whether $G[V_i \cap U_{j_i}]$ and $G[V_i \setminus U_{j_i}]$ are compatible in V_i depends only on the number of edges we reveal here. Since the pair $(\mathcal{U}, \mathcal{V})$ is typical, we reveal $\Omega(\log^4 n)$ edges here, so we can then apply Lemma 2.2 to estimate the probability that these subgraphs satisfy the compatibility condition (15). Likewise, in stage three we reveal the edges that cross between $G[V_i \cap U_{j_i}]$ and $G[V_i \setminus U_{j_i}]$, all of which were previously unrevealed by the same argument. We conclude that $\mathcal{U}$ and $\mathcal{V}$ are both (r, q)-partitions with probability $\frac{1+o(1)}{q^{2n}}$. □

The typicality of the pair $(\mathcal{U}, \mathcal{V})$ was important for the second part of the revealing process outlined above. It guaranteed that for each i, there is some j_i such that the induced subgraphs $G[U_i \cap V_{j_i}]$ and $G[U_i \setminus V_{j_i}]$ were compatible in $G[U_i]$ (in the sense of 15) with probability reasonably close to $1/q$. Loosely speaking, this works because each part of $\mathcal{U}$ significantly overlaps with enough parts of $\mathcal{V}$ so that when we reveal the edges that cross between the $G[U_i \cap V_j]$'s (for fixed i and different j), we reveal enough edges to apply Lemma 2.2 to estimate the probability of compatibility. When we treat the atypical pairs, we'll show that although we can't estimate their contribution to the covariance in the same way, they contribute a negligible amount.

First, we show that the atypical pairs make up an exponentially small fraction of $\mathcal{P}_t^2$. For ease of notation, we let $M(n, t)$ denote the number of balanced partitions of $V(G)$ into t sets, i.e. $M(n, t) := \binom{n}{n_1, \ldots, n_t}$, where $n_i \in \{\lfloor n/t \rfloor, \lceil n/t \rceil\}$. Note that this quantity is indeed well-defined since the n_i are unique up to relabelling.

Claim 4.3. *The number of atypical pairs of partitions, $|\mathcal{T}_t^C|$, is at most $M(n, t)^2 \cdot e^{-\epsilon n}$ for some constant ϵ that depends only on q.*

Proof. Fix a partition $\mathcal{U}$ and sample $\mathcal{V}$ uniformly at random from $\mathcal{P}_t$. For any i and j, the quantity $|U_i \cap V_j|$ is hypergeometrically distributed with mean n/t^2. Since $q \geq 3$, a simple application of Chernoff's bound for the hypergeometric distribution (see Remark 3) shows that the probability that there exist U_i and V_j such that $|U_i \cap V_j| \geq \frac{|U_i|}{3}$ is at most $t^2 e^{-\Theta(n)}$, where the implicit constant depends only on q. Since there are at most $M(n, t)^2$ pairs of balanced partitions, the claim follows. □

Now split the atypical partitions into $\mathcal{T}_t^C = \mathcal{B}_1 \cup \mathcal{B}_2$, where $\mathcal{B}_1$ is the set of atypical pairs where for all i and j we have $|U_i \setminus V_j|, |V_j \setminus U_i| \geq \log^2 n$ and $\mathcal{B}_2$ consists of the remaining pairs. In other words, $\mathcal{B}_1$ represents the pairs of atypical partitions where no symmetric difference $U_i \triangle V_j$ is too small. We'll show that although the pairs in these parts have (potentially) larger covariance, there are so few of them that their overall contribution is negligible. The pairs in $\mathcal{B}_1$ are "different" enough so that they still behave somewhat independently and have small covariance. The pairs in $\mathcal{B}_2$, however, overlap significantly, so they have larger covariance and we have to estimate how many of these pairs there are more carefully.

Claim 4.4. *If $(\mathcal{U}, \mathcal{V}) \in \mathcal{B}_1$, then*

$$\mathbb{P}[\mathcal{U} \text{ and } \mathcal{V} \text{ are both } (r,q)\text{-partitions}] \leq (1+o(1)) \cdot \frac{1}{q^{2n}} \cdot q^{2t}.$$

Proof. For every i there exists some j_i so that $|U_i \cap V_{j_i}| \geq |U_i|/t = n/t^2$ (here we are ignoring any rounding since it is inconsequential to the argument). Like in the proof of Claim 4.2, we reveal the subgraphs $G[U_i]$ in stages. In the first stage, we reveal $G[U_i \cap V_j]$ for all i and j.

In stage two, we reveal the remaining entries in $G[U_i \setminus V_{j_i}]$ for each i. Unlike in the proof of Claim 4.2, we might have too few unrevealed edges at the end of the first stage to use Lemma 2.2 to estimate the probability that $G[U_i \cap V_{j_i}]$ and $G[U_i \setminus V_{j_i}]$ are compatible in $G[U_i]$ (e.g., if $G[U_i]$ intersects only two parts of $\mathcal{V}$). Instead, we simply reveal the remaining edges in $G[U_i \setminus V_{j_i}]$ and bound the probability of compatibility from above by 1.

In the third step, as in the proof of Claim 4.2, we reveal the rest of the edges in $G[U_i]$, namely those that cross between $G[U_i \cap V_{j_i}]$ and $G[U_i \setminus V_{j_i}]$. The probability that this produces a good subgraph is at most what it would be given that $G[U_i \cap V_{j_i}]$ and $G[U_i \setminus V_{j_i}]$ are compatible, $\frac{1+o(1)}{q^{|U_i|-1}}$ by Lemma 2.5 and the assumption that $|U_i \setminus V_{j_i}| \geq \log^2 n$. By the same argument used in the proof of Claim 4.2, the revealing steps within each $G[U_i]$ are independent of one another and we may repeat this argument on $G[V_i]$'s as well. □

Now we estimate the contribution to the covariance of $\mathcal{B}_2$, which consists of all the remaining atypical pairs. Split $\mathcal{B}_2$ into $\mathcal{B}_2 = \cup_{s=1}^{t} \mathcal{B}_{2,s}$, where $\mathcal{B}_{2,s}$ is the set of atypical pairs $(\mathcal{U}, \mathcal{V})$ where $|U_i \setminus V_j| \leq \log^2 n$ or $|V_j \setminus U_i| \leq \log^2 n$ for exactly s pairs (i,j). In other words, $\mathcal{B}_{2,s}$ is the set of atypical pairs that have s parts (nearly) in common. Let us estimate the probability that a pair of partitions in $\mathcal{B}_{2,s}$ are both simultaneously (r,q)-partitions.

Claim 4.5. *For any pair $(\mathcal{U}, \mathcal{V}) \in \mathcal{B}_{2,s}$, we have*

$$\mathbb{P}[\mathcal{U} \text{ and } \mathcal{V} \text{ are } (r,q)\text{-partitions}] \leq \frac{1+o(1)}{q^{2n}} \cdot q^{s\lceil n/t \rceil + 2(t-s)}.$$

Proof. Since for every i, $|U_i \setminus V_j| \leq \log^2 n$ can hold for at most one value of j, we may, without loss of generality, assume that $|U_i \setminus V_i| \leq \log^2 n$ for $i \leq s$, i.e., that the first s parts of both $\mathcal{U}$ and $\mathcal{V}$ are nearly identical. Recalling that a subgraph of G is "good" if all of its degrees are r modulo q, we have by Lemma 2.4 that

$$\begin{aligned}\mathbb{P}[G[U_i] \text{ and } G[V_i] \text{ are good subgraphs}, i \leq s] &\leq \mathbb{P}[G[U_i] \text{ is a good subgraph, } i \leq s] \\ &\leq (1+o(1))q^{-\sum_{i \leq s}|U_i|}.\end{aligned}$$

Then we apply the argument from the proof of Claim 4.4 to the remaining $t-s$ parts of both $\mathcal{U}$ and $\mathcal{V}$. Specifically, for $i > s$, parts U_i and V_i have probability around $1/q^{|U_i|-1}$ and $1/q^{|V_i|-1}$ of being good, respectively. In total, the desired probability is then

$$(1+o(1))q^{-\sum_{i \leq s}|U_i|} \cdot q^{-\sum_{i>s}|U_i|} \cdot q^{-\sum_{i>s}|V_i|} \cdot q^{2(t-s)} \leq (1+o(1))q^{-2n} \cdot q^{s\lceil n/t \rceil} \cdot q^{2(t-s)}.$$

This completes the proof. □

Next we estimate the size of each $\mathcal{B}_{2,s}$.

Claim 4.6. *For any* $1 \le s \le t$,

$$|\mathcal{B}_{2,s}| \le M(n,t)^2 \cdot q^{-s\lfloor n/t \rfloor} \cdot o(1).$$

Proof. If $\mathcal{U}$ and $\mathcal{V}$ are partitions, we say that the parts U_i and V_j *overlap significantly* if $|U_i \cap V_j| \ge (n/t) - \log^2 n$. There are $M(n,t)$ ways to choose the first partition $\mathcal{U}$ and at most t^{2s} ways to choose disjoint pairs (U_{i_ℓ}, V_{j_ℓ}) for which U_{i_ℓ} and V_{j_ℓ} will overlap significantly. There are $M(n,t)$ ways to choose the first partition $\mathcal{U}$ and at most t^{2s} ways to choose disjoint pairs (U_{i_ℓ}, V_{j_ℓ}) for which U_{i_ℓ} and V_{j_ℓ} will overlap significantly (i.e., in more than $n/t - \log^2 n$ vertices). Observe that if U_i and V_j overlap significantly, the V_j cannot overlap significantly with any other U_ℓ.

Consider such a pair (U_i, V_j). At most $\log^2 n$ of the vertices in V_j miss the vertices in U_i and land in the remaining $n - |U_i|$ vertices of G. There are then at most

$$\binom{\lceil n/t \rceil}{\log^2 n}^s \cdot \binom{n}{\log^2 n}^s \le \binom{n}{\log^2 n}^{2s}$$

ways to choose the elements of the s parts of $\mathcal{V}$ that overlap significantly with $\mathcal{U}$. There are at most $n - s\lfloor n/t \rfloor$ vertices and $t - s$ parts of $\mathcal{V}$ left to fill and there are at most $M(n - s\lfloor n/t \rfloor, t - s)$ ways to do this. So far, we have that

$$\begin{aligned} |\mathcal{B}_{2,s}| &\le M(n,t) \cdot t^{2s} \cdot \binom{n}{\log^2 n}^{2s} \cdot M\left(n - s\lfloor n/t \rfloor, t - s\right) \\ &\le M(n,t) \cdot M\left(n - s\lfloor n/t \rfloor, t - s\right) \cdot (tn^{\log^2 n})^{2s}, \end{aligned}$$

for n sufficiently large. For any fixed s, it suffices to show that

$$M\left(n - s\lfloor n/t \rfloor, t - s\right) \le M(n,t) \cdot q^{-sn/t} \cdot o\left(n^{-2s\log^2 n}\right).$$

By Stirling's approximation we have

$$M(n,t) \sim \frac{t^n}{n^{(t-1)/2}} \cdot C(q),$$

where $C(q)$ is some constant depending only on q. We bound $M(n - s\lfloor n/t \rfloor, t - s)$ as follows:

$$\begin{aligned} M(n - s\lfloor n/t \rfloor, t - s) &\le (t - s)^{n - s\lfloor n/t \rfloor} \\ &\le t^n t^{-s\lfloor n/t \rfloor} \\ &\sim \frac{1}{C(q)} \cdot M(n,t) \cdot (q+1)^{-s\lfloor n/t \rfloor} \cdot n^{t/2-1} \\ &\le \frac{1}{C(q)} \cdot M(n,t) q^{-s\lfloor n/t \rfloor} e^{-s\lfloor n/t \rfloor/q} \cdot n^{t/2-1} \\ &= M(n,t) q^{-s\lfloor n/t \rfloor} o(n^{-2s\log^2 n}). \end{aligned}$$

This completes the proof. □

By Claim 4.2, in the typical case we have

$$\sum_{(\mathcal{U},\mathcal{V}) \in \mathcal{T}_t} \mathrm{Cov}(X_{\mathcal{U}}, X_{\mathcal{V}}) \le M(n,t)^2 \cdot q^{-2n} \cdot o(1) = o(\mathbb{E}[X]^2).$$

In the atypical case, we use Claim 4.3 to bound the size of $\mathcal{B}_1$ and Claim 4.4 to estimate the covariance for each term here. We similarly use Claims 4.6 and 4.5 to estimate the size of $\mathcal{B}_{2,s}$ and the covariance of each term here, respectively.

$$\begin{aligned}\sum_{(\mathcal{U},\mathcal{V})\in\mathcal{T}_t^C}\operatorname{Cov}(X_{\mathcal{U}},X_{\mathcal{V}}) &= \sum_{(\mathcal{U},\mathcal{V})\in\mathcal{B}_1}\operatorname{Cov}(X_{\mathcal{U}},X_{\mathcal{V}}) + \sum_{s=1}^{t}\sum_{(\mathcal{U},\mathcal{V})\in\mathcal{B}_{2,s}}\operatorname{Cov}(X_{\mathcal{U}},X_{\mathcal{V}})\\ &\le |\mathcal{B}_1|\cdot\frac{1+o(1)}{q^{2n}}(q^{2t}-1) + \sum_{s=1}^{t}|\mathcal{B}_{2,s}|\cdot\frac{1+o(1)}{q^{2n}}(q^{s\lceil n/t\rceil+2(t-s)}-1)\\ &\le M(n,t)^2\cdot e^{-\epsilon n}\cdot\frac{1+o(1)}{q^{2n}}\cdot(q^{2t}-1) + M(n,t)^2\cdot o(1)\cdot\frac{1+o(1)}{q^{2n}}\cdot\sum_{s=1}^{t}q^{2(t-s)}\\ &= o(\mathbb{E}[X]^2).\end{aligned}$$

Hence, $\operatorname{Var}[X] = o(\mathbb{E}[X]^2)$, so there exists an (r,q)-partition with high probability.

Acknowledgement We would like to thank the anonymous referees for their many thorough and helpful comments.

References

[1] N. Alon and J. H. Spencer. *The Probabilistic Method.* Wiley, fourth edition, 2015.

[2] P. Balister, E. Powierski, A. Scott, and J. Tan. Counting partitions of $G_{n,1/2}$ with degree congruence conditions. *arXiv:2105.12612 [math.CO]*, 2021.

[3] Y. Caro. On induced subgraphs with odd degrees. *Discrete Mathematics*, 132(1-3):23–28, 1994.

[4] I. Csizár and P. C. Shields. *Information Theory and Statistics: A Tutorial.* Foundations and Trends in Communications and Information Theory. Now Publishers Inc, 2004.

[5] A. Ferber. Singularity of random symmetric matrices — simple proof. *Comptes Rendus. Mathématique*, 359(6):743–747, 2021.

[6] A. Ferber and M. Krivelevich. Every graph contains a linearly sized induced subgraph with all degrees odd. *Advances in Mathematics*, 406:108534, 2022.

[7] S. Janson, T. Łuczak, and A. Ruciński. *Random Graphs.* John Wiley & Sons, Inc., 2000.

[8] L. Lovász. *Combinatorial Problems and Exercises.* AMS Chelsea Publishing, second edition, 1993.

[9] A. Scott. Large induced subgraphs with all degrees odd. *Combinatorics, Probability and Computing*, 1(4):335–349, 1992.

[10] A. Scott. On induced subgraphs with all degrees odd. *Graphs and Combinatorics*, 17:539–553, 2001.

[11] E. M. Stein and R. Shakarchi. *Fourier Analysis: an Introduction.* Princeton University Press, 2003.

A Proof of Equation (13)

The proof is based on bounding the multinomial coefficient in terms of the entropy function. For any $\boldsymbol{\alpha} \in [0,1]^q$ with $\alpha_0 + \cdots + \alpha_{q-1} = 1$, its entropy (or really, the entropy of the corresponding random variable) is given by

$$H(\boldsymbol{\alpha}) = -\sum_{i=0}^{q-1} \alpha_i \log_2 \alpha_i,$$

where we extend $x \mapsto x \log_2 x$ by continuity to the origin with $0 \cdot \log_2 0 \coloneqq 0$. If $p \in [0,1]$, then we define the binary entropy, $H(p) \coloneqq H((p, 1-p))$. Now for $x \in [0,1]$ and $\boldsymbol{\alpha}$ as above, define

$$h(x) = H(\boldsymbol{\alpha})x + H(x) - \log_2 q \cdot x.$$

Some basic calculus reveals the following properties of $h(x)$:

1. $h'(x) = H(\boldsymbol{\alpha}) + \log_2 \frac{1-x}{x} - \log q$ for $x \in (0,1)$;
2. $h''(x) = -\frac{1}{\ln 2 \cdot x(1-x)} < 0$ for $x \in (0,1)$;
3. $h(0) = 0$, $h(1) = H(\boldsymbol{\alpha}) - \log_2 q \le 0$, with $h(1) = 0$ if and only if $\alpha_i = 1/q$ for all i (we call this the "uniform case");
4. for $0 < x \le \frac{1}{q+1}$, $h'(x) \ge \log_2 \frac{1-x}{x} - \log_2 q \ge 0$, implying $h(x) \ge 0$ in this range;
5. $h'(x) = 0$ in a unique point in $(0,1)$, this is a maximum point of $h(x)$ since $h''(x) < 0$ in the interval. Hence $h(x) > 0$ in this point.

Define $x_0 = \max\{x \in (0,1] : h(x) = 0\}$. This is well defined due to property (3) above. In the non-uniform case we can see that $x_0 < 1$ and, due to the maximality of x_0, we have $h'(x_0) \le 0$ (in fact, $h'(x_0) < 0$). In this case, suppose $h'(x_0) = -a$ for $a > 0$. Then $h'(x) < -a$ for $x > x_0$ by (2). This implies that for $x = x_0 + t$ (assuming $x_0 + t < 1$), $h(x) \le -at$ by the intermediate value theorem. Also, for $x = x_0 - t$ and $t > 0$ small enough, we have $h(x) = \Omega(at)$, due to the continuity of $h''(x)$.

Now, for an integer $0 \le k \le n$, define

$$g(k) = \log_2 \left(\binom{k}{k_0, \ldots, k_{q-1}} \binom{n}{k} q^{-k} \right).$$

By the mean value theorem and the following estimate (see, e.g. [4], Lemma 2.2)

$$\log_2 \binom{k}{k_0, \ldots, k_{q-1}} = H\big((k_0/k, \ldots, k_{q-1}/k)\big)k - o(k),$$

we have

$$g(k) = H(\boldsymbol{\alpha})k + H(k/n)n - \log_2 q \cdot k + o(n),$$

implying:

$$\begin{aligned} \frac{g(k)}{n} &= H(\alpha_0, \ldots, \alpha_{q-1})\frac{k}{n} + H(k/n) - \log_2 q \cdot \frac{k}{n} + o(1) \\ &= h(k/n) + o(1). \end{aligned}$$

Assuming that $x_0 < 1$, choose a positive integer $k \leq n$ satisfying $k \geq x_0 n + \epsilon n$. In this case, $g(k)/n = -\Theta(\epsilon) + o(1)$, implying that $2^{g(k)} = 2^{-\Theta(n)}$. In the opposite direction (and in every case, including the uniform one) choose a positive integer $k \leq n$ satisfying $k \leq x_0 n - \epsilon n$, for small enough $\epsilon > 0$; we can conclude that $2^{g(k)} = 2^{\Theta(n)}$.