k-Wise Independent Random Graphs

Noga Alon[*]
Schools of Mathematics and Computer Science,
Sackler Faculty of Exact Sciences,
Tel Aviv University, Tel Aviv 69978, Israel, and
IAS, Princeton, NJ 08540, USA.
nogaa@post.tau.ac.il.

Asaf Nussboim[†]
Department of Computer Science and Applied Mathematics,
Weizmann Institute of Science, Rehovot, Israel.
asaf.nussbaum@weizmann.ac.il.

Abstract

We study the k-wise independent relaxation of the usual model $\mathcal{G}(N,p)$ of random graphs where, as in this model, N labeled vertices are fixed and each edge is drawn with probability p, however, it is only required that the distribution of any subset of k edges is independent. This relaxation can be relevant in modeling phenomena where only k-wise independence is assumed to hold, and is also useful when the relevant graphs are so huge that handling $\mathcal{G}(N,p)$ graphs becomes infeasible, and cheaper random-looking distributions (such as k-wise independent ones) must be used instead. Unfortunately, many well-known properties of random graphs in $\mathcal{G}(N,p)$ are global, and it is thus not clear if they are guaranteed to hold in the k-wise independent case. We explore the properties of k-wise independent graphs by providing upper-bounds and lower-bounds on the amount of independence, k, required for maintaining the main properties of $\mathcal{G}(N,p)$ graphs: connectivity, Hamiltonicity, the connectivity-number, clique-number and chromatic-number and the appearance of fixed subgraphs. Most of these properties are shown to be captured by either constant k or by some $k = poly(\log(N))$ for a wide range of values of p, implying that random looking graphs on N vertices can be generated by a seed of size $poly(\log(N))$. The proofs combine combinatorial, probabilistic and spectral techniques.

1. Introduction

We study the k-wise independent relaxation of the usual model $\mathcal{G}(N,p)$ of random graphs where, as in this model, N labeled vertices are fixed and each edge is drawn with probability (w.p., for short) $p = p(N)$, however, it is only required that the distribution of any subset of k edges is independent (in $\mathcal{G}(N,p)$ all edges are mutually independent). These k-wise independent graphs are natural combinatorial objects that may prove to be useful in modeling scientific phenomena where only k-wise independence is assumed to hold. Moreover, they can be used when the relevant graphs are so huge that handling $\mathcal{G}(N,p)$ graphs is infeasible, and cheaper random-looking distributions must be used instead. However, what happens when the application that uses these graphs (or the analysis conducted on them) critically relies on the fact that random graphs are, say, almost surely connected? After all, k-wise independence is defined via 'local' conditions, so isn't it possible that k-wise independent graphs will fail to meet 'global' qualities like connectivity? This motivates studying which global attributes of random graphs are captured by their k-wise independent counterparts.

Before elaborating on properties of k-wise independent graphs we provide some background on k-wise independence, on properties of random graphs, and on the emulation of huge random graphs.

1.1. Emulation of Huge Random Graphs

Suppose that one wishes to test the execution of some graph algorithm on random input graphs. Utilizing $\mathcal{G}(N,p)$ graphs requires resources polynomial in N, which

[*] Research supported in part by the Israel Science Foundation and by a USA-Israeli BSF grant.

[†] Partly supported by a grant from the Israel Science Foundation.

is infeasible when N is huge (for example, exponential in the input length, n, of the relevant algorithms). A plausible solution is to replace $\mathcal{G}(N,p)$ by a cheaper 'random looking' distribution $\mathcal{G}_N$. To this end, each graph G in the support of $\mathcal{G}_N$ is represented by a very short binary string (called seed) $s(G)$, s.t. evaluating edge queries on G can be done efficiently when $s(G)$ is known; then, sampling a graph from $\mathcal{G}_N$ is done by picking the seed uniformly at random.

Goldreich, Goldwasser and the second author were the first to address this scenario in [24, 37]. They studied emulation by computationally pseudorandom graphs that are indistinguishable from $\mathcal{G}(N,p)$ from the view of any $poly(\log(N))$-time algorithm that inspects graphs via edge-queries of its choice. They considered several prominent properties of $\mathcal{G}(N,p)$ graphs, and constructed computationally pseudorandom graphs that preserve many, tough not all, of those properties (see the final paragraph of Section 2).

We consider replacing random graphs by k-wise independent ones. The latter can be sampled and accessed using only $poly(k\log(N))$-bounded resources. This is achieved thanks to efficient constructions of discrete k-wise independent variables by Joffe [27], see also Alon, Babai and Itai [1]: the appearance of any potential edge in the graph is simply decided by a single random bit (that has probability p to attain the value 1). Such k-wise independent graphs were used by Naor, Tromer and the second author [36] to efficiently capture arbitrary first-order properties of huge $\mathcal{G}(N,p)$ graphs (see Section 3.6), and by [24, 37] as a building block for their main construction.

1.2. k-Wise Independent Random Variables

Distributions of discrete k-wise independent variables play an important role in computer science. Such distributions are mainly used for de-randomizing algorithms (and for some cryptographic applications). In addition, the randomness complexity of constructing k-wise independent variables was studied in depth, and in particular, the aforementioned constructions [27, 1] (based on degree k polynomials over finite fields) are known to provide essentially the smallest possible sample spaces. Our work is, however, the first systematic study of *combinatorial properties* of k-wise independent objects. Properties of various other k-wise independent objects (mainly percolation on $\mathbb{Z}^d$ and on Galton-Watson trees) were subsequently explored by Benjamini, Gurel-Gurevich and Peled [7].

1.3. The Combinatorial Structure of Random Graphs

What are the principal attributes of random graphs that k-wise independent ones should maintain? Most theorems that manifest the remarkable structure of random graphs state that certain properties occur either almost surely (a.s. for short), or alternatively hardly ever, (namely, with probability tending either to 1 or to 0 as N grows to ∞). These results typically fall into one of the following categories.

Tight concentration of measure. A variety of prominent random variables (regarding random graphs) a.s. attain only values that are *extremely close* to their expectation. For instance, random graphs (with, say, constant p) a.s. have connectivity number $\kappa = (1 \pm o(1))pN$, clique number $c = (1 \pm o(1))\frac{2\log(pN)}{\log(1/p)}$ (Bollobás and Erdös [11], Matula [35], Frieze [23]) and chromatic number $\chi = (1 \pm o(1))\frac{N\log(1/(1-p))}{2\log(pN)}$ (Bollobás [10], Łuczak [34]).

Thresholds for monotone properties. For a given monotone increasing[1] graph property T, how large should $p(N)$ be for the property to hold a.s.? This question has been settled for many prominent properties such as connectivity (Erdös and Rényi [15]), containing a perfect matching (Erdös and Rényi [17, 18, 19]), Hamiltonicity (Pósa [38], Koršunov [30], Komlós and Szemerédi [31]), and the property of containing copies of some fixed graph H (Erdös and Rényi [16], Bollobás [9]). For these (and other) graph properties the sufficient density (for obtaining the property) is surprisingly small, and moreover, a threshold phenomenon occurs when by 'slightly' increasing the density from $\underline{p}(N)$ to $\overline{p}(N)$, the probability that T holds dramatically changes from $o(1)$ to $1 - o(1)$.[2] Thus, good emulation requires the property T to be guaranteed at densities as close as possible to the true $\mathcal{G}(N,p)$ threshold.

Zero-one laws. These well known theorems reveal that *any* first-order property holds either a.s. or hardly ever for $\mathcal{G}(N,p)$. A first-order property is any graph property that can be expressed by a single formula in the canonical language where variables stand for vertices and the only relations are equality and adjacency (e.g. "having an isolated vertex" is specified by $\exists x \forall y \neg \text{EDGE}(x,y)$). These Zero-one laws hold for any fixed p (Fagin [20], Glebskii, Kogan, Liagonkii and Talanov [25]), and whenever $p(N) = N^{-\alpha}$ for a fixed irrational α (Shelah and Spencer [40]).

[1] Namely, any property closed under graph isomorphism and under addition of edges.

[2] Thresholds for prominent properties are often so sharp that $\overline{p} = (1 + o(1))\underline{p}$. Somewhat coarser thresholds were (later) established for *arbitrary* monotone properties by Bollobás and Thomason [12], and by Friedgut and Kalai [22].

2. Our Contribution

We investigate the properties of k-wise independent graphs by providing upper bounds and lower bounds on the 'minimal' amount of independence, k_T, required for maintaining the main properties T of random graphs. The properties considered are: connectivity, perfect matchings, Hamiltonicity, the connectivity-number, clique-number and chromatic-number and the appearance of copies of a fixed subgraph H. We mainly establish upper bounds on k_T (where arbitrary k-wise independent graphs are shown to exhibit the property T) but also lower bounds (that provide specific constructions of k-wise independent graphs that fail to preserve T). Our precise results per each of these properties are discussed in Section 3, and proved in Section 5 (and the appendices of the complete version of this paper [5]). Interestingly, our results reveal a deep difference between k-wise independence and almost k-wise independence (a.k.a. (k, ϵ)–wise independence[3]). All aforementioned graph properties are guaranteed by k-wise independence (even for small $k = poly(\log(N))$), but are strongly violated by some almost k-wise independent graphs - even when $k = N^{\Omega(1)}$ is huge and $\epsilon = N^{-\Omega(1)}$ is tiny. For some properties of random graphs, T, our results demonstrate for the first time how to efficiently construct random-looking distributions on huge graphs that satisfy T.

Our Techniques & Relations to Combinatorial Pseudorandomness. For positive results (upper bounding k_T), we note that the original proofs that establish properties of $\mathcal{G}(N,p)$ graphs often fail for k-wise independent graphs. These proofs use a union bound over $M = 2^{\Theta(N)}$ undesired events, by giving a $2^{-\Omega(N)}$ upper-bound on the probability of each of these events.[4] Unfortunately, there exist $poly(\log(N))$–wise independent graphs where any event that occurs with positive probability, has probability $\geq 2^{-o(N)}$. Therefore, directly 'de-randomizing' the original proof fails, and alternative arguments (suitable for the k-wise independent case) are provided.

In particular, many properties are inferred via a variant of Thomason's notion of 'jumbledness' [42] (mostly known in its weaker form as quasirandomness or pseudorandomness, as defined by Chung, Graham and Wilson [14], and related to the so called Expander Mixing Lemma and the pseudorandom properties of graphs that follow from their spectral properties, see [2]). For our purposes, α-jumbledness means that (as expected in $\mathcal{G}(N,p)$ graphs) for all vertex-sets U, V, the number of edges that pass from U to V should be $p|U||V| \pm \alpha\sqrt{|U||V|}$. Jumbledness and quasirandomness have been studied extensively (see [32] and its many references), and serve in Graph Theory as *the* common notion of resemblance to random graphs. In particular, $\mathcal{G}(N,p)$ graphs are known to exhibit (the best possible) jumbledness parameter, $\alpha = \Theta(\sqrt{pN})$. One of our main results (Theorem 1) demonstrates that k-wise independence for $k = \Theta(\log(N))$ is stronger than jumbledness, in the sense that it guarantees the optimal $\alpha = \Theta(\sqrt{pN})$ even for tiny densities $p = \Theta(\frac{\ln(N)}{N})$. Therefore, prominent properties of k-wise independent graphs can be directly deduced from properties of jumbled graphs.

Proving Theorem 1 exploits a known connection between jumbledness and the eigenvalues of (a shifted variant of) the adjacency matrix of graphs, following the approach of Alon and Chung [2]. In particular, the analysis of Vu ([43], extending [21]) regarding the eigenvalues of random graphs is strengthened, in order to achieve optimal eigenvalues even for smaller densities p than those captured by [43]. This improvement implies, among other results, the remarkable fact that k-wise independent graphs for $k = \Theta(\log(N))$ preserve (up to constant factors) the $\mathcal{G}(N,p)$ sufficient density for connectivity.

More on Techniques & Relations to Almost k-Wise Independence. For negative results (producing random-looking graphs that defy a given property T of random graphs), the [24, 37] approach is to first construct some random-looking graph G, and later to 'mildly' modify G s.t. T is defied. This is done w.r.t. all graph properties considered here. For instance, the modification of choosing a random vertex and then deleting all its edges violates connectivity while preserving computational pseudorandomness. Unfortunately, such modifications fail to preserve k-wise independence (the resulting graphs are only almost k-wise independent). In contrast, most of our negative results exploit the fact that some constructions of k-wise independent bits produce strings with significantly larger probability than in the completely independent case. This is translated (by the construction in Lemma 5) to the unexpected appearance of some subgraphs (in k-wise independent graphs): either huge independent sets inside dense graphs or fixed subgraphs inside sparse graphs.

Comparison with Computational Pseudorandomness. Finally, k-wise independence guarantees all random graphs' properties that were met by the (specific) computationally pseudorandom graphs of [24, 37]. In addition, only k-wise independence is known to capture (i) arbitrary first-order properties of $\mathcal{G}(N,p)$ graphs, (ii) high connectivity, (iii) strongest possible parameters of jumbledness, and (iv) almost regular $(1 \pm o(1))pN$ degree for all vertices, and $(1 \pm o(1))p^2N$ co-degrees for all vertex pairs. A single ex-

[3] (k, ϵ)–wise independence means that the joint distribution of any k potential edges is only required to be within small statistical distance ϵ from the corresponding distribution in the $\mathcal{G}(N,p)$ case.

[4] For instance w.r.t. connectivity, M is the number of choices for partitioning the vertices into 2 disconnected components.

ception is that in [24, 37] the chromatic number of random graphs is achieved precisely, while here it is met only up to a constant factor. Importantly, our results hold for any k-wise independent graphs, (and in particular for the very simple and efficiently constructable ones derived from [27, 1]), whereas the approach of [24, 37] requires non-trivial modifications of the construction per each new property.

3. Combinatorial Properties of k-Wise Independent Graphs

We now survey our main results per each of the aforementioned graph properties T. Typically our arguments establish the following tradeoff: the smaller p is, the larger k should be to maintain T. Given this tradeoff we highlight minimizing k or, alternatively, minimizing p. The latter is motivated by the fact that the $\mathcal{G}(N,p)$ threshold for many central properties occurs at some $p^* \ll 1$. Minimizing p is subject to some reasonable choice of k, which is $k \leq poly(\log(N))$. Indeed, as the complexity of implementing k-wise independent graphs is $poly(k\log(N))$, we get efficient implementations whenever $k \leq poly(\log(N))$ even when the graphs are huge and $N = 2^{poly(n)}$. [5]

3.1. Connectivity, Hamiltonicity and Perfect Matchings (see Section 5.2)

The well known sufficient $\mathcal{G}(N,p)$ density for all these properties is $\sim \frac{\ln(N)}{N}$. For connectivity, this sufficient density is captured (up to constant factors) by all $\log(N)$–wise independent graphs. Even $k = 4$ suffices for larger densities $p \gg N^{-\frac{1}{2}}$. Based on Hefetz, Krivelevich and Szabo's [26], Hamiltonicity (and hence perfect matchings) are guaranteed at $p \geq \frac{\log^2(N)}{N}$ with $k \geq 4\log(N)$, and at $p \geq N^{-\frac{1}{2}+o(1)}$ with $k \geq 4$. On the other hand, some pair-wise independent graphs are provided that despite having constant density, are still a.s. disconnected and fail to contain any perfect matching.

3.2. High Connectivity (see Section 5.3)

The connectivity number, $\kappa(G)$, is the largest integer, ℓ, s.t. any pair of vertices is connected in G by at least ℓ internally vertex-disjoint paths. Since a typical degree in a random graph is $(1 \pm o(1))pN$, it is remarkable that $\mathcal{G}(N,p)$ graphs a.s. achieve $\kappa = (1 \pm o(1))pN$. Surprisingly, such optimal connectivity is guaranteed by $\Theta(\log(N))$-wise independence whenever $p \geq \Theta(\frac{\log(N)}{N})$, and alternatively, by $k \geq 4$ whenever $p \gg N^{-\frac{1}{3}}$.

3.3. Cliques and independent sets (see Appendix 7 in [5])

For $N^{-o(1)} \leq p \leq 1 - N^{o(1)}$ the independence number, I, of random graphs has a.s. only two possible values: either S^* or S^*+1 for some $S^* = (1-o(1))\frac{2\log(pN)}{\log(1/(1-p))}$. This remarkable phenomenon is observed to hold by virtue of $c\log^2(N)$–wise independence whenever p is bounded away from 0 and c is sufficiently large. On the other hand, k-wise independent graphs are provided with $k = \Theta(\frac{\log(N)}{\log\log(N)})$ where $I \geq (S^*)^{1+\Omega(1)}$ a.s. (for $k = \Theta(1)$, even huge $N^{\Omega(1)}$ independent sets may appear). For smaller densities, random graphs a.s. have $I \leq O(p^{-1}\log(N))$, while $c'\log(N)$-wise independence (for sufficiently large c') gives a weaker, yet useful, $I \leq O(\sqrt{N/p})$ bound whenever $p \geq \Omega(\frac{\log(N)}{N})$. By symmetry (replacing p with $1-p$), analogous results to all the above hold for the clique number as well. Discussing the clique- and independence-number is deferred to the appendices in [5], since the main relevant techniques are demonstrated elsewhere in the paper.

3.4. Coloring (see Section 5.5)

For $1/N \ll p \leq 1 - \Omega(1)$, the chromatic number χ of random graphs is a.s. $(1+o(1))\frac{N\log(1/(1-p))}{2\log(pN)}$. Given any $p \geq (\log(N))^{-d}$, this $\mathcal{G}(N,p)$ lower-bound on χ is observed to hold for any $(\log(N))^c$-wise independent graphs for some sufficiently large c. More surprisingly, some $k = c'\log(N)$ suffices to capture a similar upper-bound even for tiny densities $p = c''\log(N)/N$. Such upper-bounds are also implied by $k = 12$ for some larger densities $p = N^{-\Omega(1)}$, whereas for $k = 2$ a huge $\chi = \Theta(N)$ might a.s. occur for constant ps (Theorem 4). The k-wise independent upper-bounds on χ are based on results of Alon, Krivelevich and Sudakov [3], [4] and of Johansson [28].

3.5. Thresholds for the Appearance of Subgraphs (see Section 5.4)

For a fixed (non-empty) graph H, consider the appearance of H-copies (*not necessarily* as an induced subgraph) in either a random or a k-wise independent graph. The $\mathcal{G}(N,p)$ threshold for the occurrence of H sub-graphs lies at $p^*_H \overset{\text{def}}{=} N^{-\rho}$, where the constant $\rho = \rho(H)$ is the minimum, taken over all subgraphs H' of H (including H itself), of the ratio $\frac{v(H')}{e(H')}$ (here, $v(H')$ and $e(H')$ respectively denote the number of vertices and edges in H'). Thus, no H-copies are found when $p \ll p^*$, while for any $p \gg p^*$, copies of H abound (Erdös and Rényi [16], Bollobás [9]). For any graph H, this $\mathcal{G}(N,p)$ threshold holds whenever

[5] Accessing the graphs via edge-queries is adequate only when $p \geq n^{-\Theta(1)}$ - otherwise a.s. no edges are detected by the $poly(n)$ inspecting algorithm. For smaller densities our study has thus mostly a combinatorial flavor.

$k \geq cv^4(H)$ (for some constant c), but as k is decreased to $\lfloor \frac{2}{\rho} \rfloor$, the $\mathcal{G}(N,p)$ threshold is defied: much sparser graphs exist where $p \ll p^*_H$ and yet copies of H are a.s. found. In particular, when $e(H) \geq \Omega(v^2(H))$, the threshold violation occurs at $k = \Omega(v(H))$.

3.6. First Order Zero-One Laws (Previous Results)

A recent study (of Naor, Tromer and the second author [36]) considered capturing arbitrary depth-$D(N)$ properties of random graphs. These are graph properties expressible by a sequence of first-order formulas $\Phi = \{\phi_N\}_{N \in \mathbb{N}}$, with quantifier depth $depth(\phi_N) \leq D(N)$ (e.g. "having a clique of size $t(N)$" can be specified by $\phi_N = \exists x_1 ... \exists x_{t(N)} \bigwedge_{i \neq j}(\text{EDGE}(x_i, x_j))$. A 'threshold' depth function $D^* = \frac{\log(N)}{\log(1/p)}$ was identified s.t. a graph sampled from any k-wise independent distribution simultaneously agrees with a random $\mathcal{G}(N,p)$ graph on all depth $(1-o(1))D^*$ properties whenever $k \gg (D^*)^2$. In contrast, any efficiently computable graphs are strongly separated from $\mathcal{G}(N,p)$ by properties of only slightly higher depth $(1+o(1))D^*$. These results are incomparable to the ones in the current paper, since most of the graph properties studied here require larger depth than D^*.

4. Preliminaries

Asymptotics. Invariably, $k : \mathbb{N} \rightarrow \mathbb{N}$, while $p, \epsilon, \delta, \gamma, \Delta : \mathbb{N} \rightarrow (0,1)$. We often use $k, p, \epsilon, \delta, \gamma, \Delta$ instead of $k(N), p(N), \epsilon(N), \delta(N), \gamma(N), \Delta(N)$. Asymptotics are taken as $N \rightarrow \infty$, and some inequalities hold only for sufficiently large N. The $\lfloor \cdot \rfloor$ and $\lceil \cdot \rceil$ operators are ignored whenever insignificant for the asymptotic results. Constants $c, \bar{c}$ are not optimized in expressions of the form $k = c\log(N)$ or $p = (\log(N))^{\bar{c}}/N^{\Delta}$, whereas the constant Δ is typically optimized.

Subgraphs. For a graph H, let $v(H)$ and $e(H)$ denote the number of vertices and edges in H. For vertex sets U, V let $e(U,V)$ denote the number of edges that pass from U to V (if $S = U \bigcap V \neq \emptyset$, then any internal edge of S is counted twice). Similarly, we let $e(U) = e(U,U)$.

Random and k-Wise Independent Graphs. Throughout, graphs are simple, labeled and undirected. Given N, k, p as above then $\mathcal{G}^{k(N)}(N, p(N))$ (or $\mathcal{G}^k(N,p)$ for short) denotes some distribution over the set of graphs with vertex set $\{1, ..., N\}$, where each edge appears w.p. $p(N)$, and the random variables that indicate the appearance of any $k(N)$ potential edges are mutually independent. We use the term 'k-wise independent graphs' for a sequence of distributions $\{\mathcal{G}^k(N,p)\}_{N \in \mathbb{N}}$ indexed by N.

Almost Sure Graph Properties. A graph property T, is any property closed under graph isomorphism. We say that 'T holds a.s. (almost surely) for $\mathcal{G}^k(N,p)$' or that (abused notation) 'T holds for $\mathcal{G}^k(N,p)$' whenever $\Pr_{\mathcal{G}^k(N,p)}[T] \overset{N \rightarrow \infty}{\longrightarrow} 1$. Similar terminology is used for $\mathcal{G}(N,p)$ graphs.

Monotonicity in $(\mathbf{k}, \mathbf{p})$. Since $\bar{k}$–wise independence implies k–wise independence for all $\bar{k} > k$ we may state claims for arbitrary $k \geq k'$ but prove them only for $k = k'$. When establishing monotone increasing properties we often state claims for arbitrary $p \geq p'$ but prove them only for $p = p'$. The latter is valid since for any $N, k, p > p'$, the process of sampling from any (independent) $\mathcal{G}^k(N,p)$, $\mathcal{G}^k(N, p'/p)$ distributions and defining the final graph with edge-set being the intersection of the edge-sets of the two sampled graphs, clearly results in a $\mathcal{G}^k(N,p')$ distribution.

k-Wise Independent Random Variables. The term '(M,k,p)-variables' stands for any M binary variables that are k-wise independent with each variable having probability p of attaining value 1. Lemma 1 (proved in Section 6.2 in [5]) adjusts the known construction of discrete k-wise independent variables of [27],[13], [1] to provide (M,k,p)-variables that induce some predetermined values with relatively high probability. Throughout, e_1 and e_0 resp. denote the number of edges and non-edges in a graph H.

Lemma 1 *Given $0 < p < 1$ with binary representation $p = 0.b_1...b_\ell$, and natural numbers e_0, e_1, M satisfying $e_0 + e_1 \leq M$, let $F = \max\{2^{\lceil \log_2 M \rceil}, 2^\ell\}$. Then there exists (M,k,p)-variables s.t. $\Pr[A] = F^{-k}$, where A denotes the event that the first e_0 variables receive value 0 while the next e_1 variables receive value 1.*

Tail Bounds for k-Wise Independent Random Variables. The following strengthened version of standard tail bounds (proved in Section 6.2 in [5]) translates into smaller densities p for which monotone graph properties are established for k-wise independent graphs. After submission of this paper it came to our knowledge that similar bounds were already obtained by Schmidt, Siegel and Srinivasan [41].

Lemma 2 *Let $X = \sum_{j=1}^M X_j$ be the sum of k-wise independent binary variables where $\Pr[X_j = 1] = \mu$ holds for all j. Let $\delta > 0$, and let k be even s.t. $\frac{M-k}{k}\mu(1-\mu) \geq 1$. Then*

$$\Pr[|X - \mathbb{E}(X)| \geq \delta\mathbb{E}(X)] \leq \left[\frac{2k(1-\mu)}{\delta^2 \mu M}\right]^{\frac{k}{2}}.$$

5. The properties of k-wise independent graphs

5.1. Degrees, Co-Degrees and Jumbledness

Lemma 3 (Achieving almost regular degrees) *In all k-wise independent graphs $\{\mathcal{G}^k(N,p)\}_{N\in\mathbb{N}}$ it a.s. holds that all vertices have degree $p(N-1)(1\pm\epsilon)$ whenever $N\big[\frac{3k}{\epsilon^2 pN}\big]^{\lfloor k/2\rfloor} \longrightarrow 0$, and in particular when either*

1. *$k \geq 4$, $N^{-1/2} \ll p \leq 1-\frac{5}{N}$, and $1 \geq \epsilon \gg p^{-1/2}N^{-1/4}$; or*
2. *$k \geq 4\log(N)$, $\frac{25\log(N)}{N} \leq p \leq 1-\frac{5\log(N)}{N}$, and $1 \geq \epsilon \geq \sqrt{\frac{25\log(N)}{pN}}$.*

Proof. Fix a vertex v, and let X_w be the random variable that indicates the appearance of the edge $\{v,w\}$ in the graph. Thus, the degree of v is $X = \sum_{w\neq v} X_w$. Since X is the sum of $(N-1,k,p)$-variables, Lemma 2 implies that the probability that v has an unexpected degree $X \neq p(N-1)(1\pm\epsilon)$ is bounded by $\big[\frac{3k}{\epsilon^2 pN}\big]^{\lfloor k/2\rfloor}$. Applying a union-bound over the N possible vertices v, gives that the probability of having *some* vertex with unexpected degree is bounded by $N\big[\frac{3k}{\epsilon^2 pN}\big]^{\lfloor k/2\rfloor}$, which vanishes for the parameters in items 1 and 2. ■

Lemma 4 (Achieving almost regular co-degrees) *In all k-wise independent graphs $\{\mathcal{G}^k(N,p)\}_{N\in\mathbb{N}}$ it a.s. holds that all vertex pairs have co-degree $p^2(N-2)(1\pm\gamma)$ whenever either*

1. *$k \geq 12$, $N^{-\frac{1}{6}} \ll p \leq 1-\frac{13}{N}$, and $1 \geq \gamma \gg p^{-1}N^{-\frac{1}{6}}$; or*
2. *$k \geq 12\log(N)$, $\sqrt{\frac{73\log(N)}{N}} \leq p \leq 1-\frac{13\log(N)}{N}$ and $1 \geq \gamma \geq \sqrt{\frac{73\log(N)}{p^2N}}$.*

Proof. The proof is completely analogous to that of Lemma 3. Here the union-bound is over all $\binom{N}{2}$ vertex pairs $\{u,v\}$, and the co-degree of each $\{u,v\}$ is the sum of $(N-2,\lfloor\frac{k}{2}\rfloor,p^2)$-variables. ■

The following definition is a modified version of the one in [42, 14], see also [2] and [6], Chapter 9.

Definition 1 (Jumbledness) *For vertex sets U,V, let $e(U,V)$ denote the number of edges that pass from U to V (internal edges of $U\bigcap V$ are counted twice). A graph is (p,α)-jumbled if $e(U,V) = p|U||V| \pm \alpha\sqrt{|U||V|}$ holds for all U,V.*

Theorem 1 (Achieving optimal jumbledness) *There exist absolute constants c_1,c_2,c_3 s.t. all k-wise independent graphs $\{\mathcal{G}^k(N,p)\}_{N\in\mathbb{N}}$ are a.s. (p,α)-jumbled whenever either:*

1. *$k \geq 4$, $p \geq \Omega(\frac{1}{N})$ and $\alpha \gg \sqrt{p}N^{3/4}$; or*
2. *$k \geq \log(N)$, $\frac{c_1\log(N)}{N} \leq p \leq 1-\frac{c_2\log^4(N)}{N}$ and $\alpha \geq c_3\sqrt{pN}$.*

Proof. The proof is based on spectral techniques and combines some refined versions of ideas from [2], [21] and [43], using the fact that traces of the k-th power of the adjacency matrix of a graph are identical in the k-wise independent case and in the totally random one. The details are lengthy and are thus deferred to Appendix 8 in [5].

5.2. Connectivity, Hamiltonicity and Perfect Matchings

Theorem 2 (Achieving connectivity) *There exists a constant c s.t. the following holds. All k-wise independent graphs $\{\mathcal{G}^k(N,p)\}_{N\in\mathbb{N}}$ are a.s. connected whenever either:*

- *$k \geq 4$ and $p \gg \frac{1}{\sqrt{N}}$; or*
- *$k \geq 4\log(N)$ and $p \geq \frac{c\ln(N)}{N}$.*

Proof. Let U be a vertex-set that induces a connected component. Connectivity follows from having $|U| > 0.5N$ for all such U. The following holds a.s. for $\mathcal{G}^k(N,p)$. By Lemma 3, all vertices have degree $\geq 0.9pN$, so $e(U) \geq 0.9pN|U|$. By Theorem 1, all sets U satisfy $e(U) \leq p|U|^2 + \alpha|U|$ with $\alpha = O(\sqrt{pN}) = o(pN)$. Re-arranging gives $(0.9-o(1))N \leq |U|$. ■

Theorem 3 (Achieving Hamiltonicity) *All k-wise independent graphs $\{\mathcal{G}^k(N,p)\}_{N\in\mathbb{N}}$ are a.s. Hamiltonian (and for even N contain a perfect matching) whenever either:*

- *$k \geq 4$ and $p \geq \frac{\log^2(N)}{\sqrt{N}}$; or*
- *$k \geq 4\log(N)$ and $p \geq \frac{\log^2(N)}{N}$.*

Proof. Let $\bar{\Gamma}(V)$ denote the set of vertices $v \notin V$ that are adjacent to some vertex in the vertex-set V. By Theorem 1.1 in Hefetz, Krivelevich and Szabo's [26], Hamiltonicity follows from the existence of constants b,c such that a.s. (i) $|\bar{\Gamma}(V)| \geq 12|V|$ holds for all sets V of size $\leq bN$, and (ii) $e(U,V) \geq 1$ holds for all disjoint sets U,V of size $\frac{cN}{\log(N)}$. We remark that (unlike other asymptotic arguments in this paper), the sufficiency of (i) and (ii) might hold only for very large N. For (i), let $b = \frac{1}{170}$ and consider an arbitrary set V. By Theorem 1, a.s. all vertex-sets T have $e(T) \leq p|T|^2 + o(pN)|T|$. By Lemma 3 a.s. all the degrees are $(1\pm o(1))pN$, so exactly $(1\pm o(1))pN|V|$ edges touch V (where internal edges are counted twice). Let $T = V\bigcup\bar{\Gamma}(V)$, and assume that $|\bar{\Gamma}(V)| < 12|V|$. We get

$(1 - o(1))pN|V| \leq e(T) \leq p(13|V|)^2 + o(pN)|V|$. Re-arranging gives $|V| > \frac{N}{170}$. Condition (i) follows. For (ii), by Theorem 1, a.s. all (equal-sized and disjoint) vertex-sets U, V have $e(U, V) \geq p|U||V| - O(\sqrt{pN})|U|$. If there is no edge between U and V, then $e(U, V) = 0$. Re-arranging gives $|U| \leq O(\sqrt{N/p}) \leq O(\frac{N}{\log(N)})$. Condition (ii) follows. ■

Theorem 4 (Failing to preserve connectivity) *There exist pair-wise independent graphs $\{\mathcal{G}^k(N, p)\}_{N\in\mathbb{N}}$ where $p = 1/2$ that (i) are a.s. disconnected (and contain no Hamiltonian cycles), (ii) contain no perfect matchings with probability* 1, *and (iii) a.s. have clique number and chromatic number $(1/2 \pm o(1))N$ and independence number 2.*

Proof. Consider the graphs defined by partitioning all vertices into 2 disjoint sets V_0, V_1 where each V_j induces a clique, no edges connect V_0 to V_1, and V_1 is chosen randomly and uniformly among all subsets of odd cardinality of the vertex set. Note that for every set of 4 vertices, there are 16 ways to split its vertices among V_0 and V_1, and it is not difficult to check that if $N \geq 5$, then each of these 16 possibilities is equally likely. Therefore, any edge appears w.p. $\frac{1}{2}$, and any pair of edges (whether they share a common vertex or not) appears w.p. $\frac{1}{4}$. Still the graph is connected iff all the vertices belong to the same V_j which happens only w.p. 2^{-N+1} (and only if N is odd). Since $|V_1|$ is odd, the graph contains no perfect matching. It is easy to verify that a.s. $|V_0|, |V_1| = (1/2 \pm o(1))N$ implying the last item. ■

5.3. High-connectivity

Theorem 5 (Achieving optimal connectivity) *There exists an absolute constant c, s.t. for all k-wise independent graphs $\{\mathcal{G}^k(N, p)\}_{N\in\mathbb{N}}$ the connectivity number is a.s. $(1 \pm o(1))pN$ when either*

- $k \geq 4$ *and* $p \gg N^{-\frac{1}{3}}$; *or*
- $k \geq \log(N)$ *and* $p \geq c\frac{\log(N)}{N}$.

Proof. The connectivity is certainly not larger than $(1 + o(1))pN$, as it is upper-bounded by the minimum degree. By Theorem 2.5 in Thomason's [42] $\kappa \geq d - \alpha/p$ holds for any (p, α)-jumbled graph with minimal degree $\geq d$. Thus, achieving $\kappa \gtrsim pN$, reduces to obtaining (i) $d = (1 \pm o(1))pN$, and (ii) $\alpha \ll pd$. Condition (i) a.s. holds by Lemma 3. By Theorem 1, we a.s. achieve $(c_3\sqrt{pN})$-jumbledness for some constant c_3, so condition (ii) becomes $p^2N \gg \sqrt{pN}$. This proves the first part of the theorem. To prove the second we note, first, that we may assume that $p \ll 1$ (since otherwise 4-wise independence suffices). Let S be a smallest separating set of vertices, assume that $|S|$ is smaller than $(1 - o(1))pN$, let U be the smallest connected component of $G - S$ and let W be the set of all vertices but those in $U \cup S$. Clearly $|W| \geq (\frac{1}{2} - o(1))N$. Note that $e(U, W) = 0$, but by jumbledness $e(U, W) \geq p|U||W| - c_3\sqrt{pN|U||W|}$. This implies, using the fact that $|W| > N/3$, that $|U| \leq \frac{3c_3^2}{p}$. Using jumbledness again, $e(U, S) \leq p|U||S| + c_3\sqrt{pN|U||S|}$ but as all degrees are at least $(1 - o(1))pN$, $e(U, S) \geq (1 - o(1))pN|S| - e(U) \geq (1 - o(1))pN|U| - p|U|^2 - c_3\sqrt{pN}|U| \geq |U|(1 - o(1))pN$, where here we used the fact that $|U| \leq O(1/p)$ and that $\sqrt{pN} = o(pN)$. This implies that either $p|U||S| \geq \frac{1}{2}|U|pN$, implying that $|S| \geq N/2 \gg pN$, as needed, or $c_3\sqrt{pN|U||S|} \geq \frac{1}{3}|U|pN$, implying that $|S| \geq \frac{1}{9c_3^2}|U|pN$ which is bigger than pN provided $|U| \geq 9c_3^2$. However, if $|U|$ is smaller, then surely $|S| \geq (1 - o(1))pN$, since all degrees are at least $(1 - o(1))pN$ and every vertex in U has all its neighbors in $U \cup S$. ■

5.4. Thresholds for the Appearance of Sub-graphs

For a fixed non-empty graph H, let $\rho(H)$ and p^*_H be as in Section 3.5.

Observation 1 (Preserving the threshold for appearance of sub-graphs) *There exists a function $D(v) = (1 \pm o(1))\frac{v^4}{16}$ s.t. for any graph H with at most v vertices, and for all k-wise independent graphs $\{\mathcal{G}^k(N, p)\}_{N\in\mathbb{N}}$ with $k \geq D(v)$ the following holds. Let A denote the event that H appears in $\mathcal{G}^k(N, p)$ (not necessarily as an induced sub-graph). Then*

- *If $p(N) \ll p^*_H(N)$ then $(\neg A)$ a.s. holds.*
- *If $p(N) \gg p^*_H(N)$ then A a.s. holds.*

Proof. The proof (given in Appendix 6.3 in [5]) applies Rucinski and Vince's [39] to specify a sufficiently large k for the original $\mathcal{G}(N, p)$ argument to hold. ■

Theorem 6 (Defying the threshold for appearance of sub-graphs) *For any (fixed) graph H that satisfies*[6] *$\rho(H) < 2$, there exists k-wise independent graphs $\{\mathcal{G}^k(N, p)\}_{N\in\mathbb{N}}$ where $k = \lceil\frac{2}{\rho(H)} - 1\rceil$ and $p(N) \ll p^*_H(N)$ s.t. H a.s. appears in $\mathcal{G}^k(N, p)$ as an induced sub-graph.*

Proof. Theorem 6 relies on Lemma 5. This lemma considers the appearance of the sub-graph H_N in $\mathcal{G}^k(N, p)$ where $\{H_N\}_{N\in\mathbb{N}}$ is any sequence of graphs (possibly) with unbounded order.

[6] This condition rules out only graphs H that are a collection of disjoint edges. For such graphs $\rho(H) = 2$, so clearly no H-copies can be produced (even if $k = 1$) when $p(N) \ll p^*_H(N) = N^{-2}$.

Lemma 5 (k-wise independent graphs with unexpected appearance of sub-graphs) *Let $\{H_N\}_{N\in\mathbb{N}}$ be a sequence of graphs where H_N has exactly $S(N) < \sqrt{N}$ vertices, $e_1(N)$ edges and $e_0(N)$ none-edges. Assume that for each N there exists $(\binom{S(N)}{2}, k(N), p(N))$-variables s.t. with probability $\Delta(N) \gg (S(N)/N)^2$ it holds that the first $e_0(N)$ variables attain value 0 and the next $e_1(N)$ variables attain value 1. Then there exist k-wise independent graphs $\{\mathcal{G}^k(N,p)\}_{N\in\mathbb{N}}$ that a.s. contain H_N-copies as induced sub-graphs.*

Proof (Lemma 5). Fix N, so $H = H_N, S = S(N), e_i = e_i(N), k = k(N), p = p(N), \Delta = \Delta(N)$. We construct graphs $\mathcal{G}^k(N,p)$ that a.s. contain H copies. Given the N vertices, let $\{V_j\}_{j=1}^{M}$ be any maximal collection of *edge-disjoint* vertex-sets, each of size $|V_j| = S$. For each j, decide the internal edges of V_j by some $(\binom{S}{2}, k, p)$-variables s.t. H is induced by V_j with probability Δ. This can be done by appropriately defining which specific edge in V_j is decided by which specific variable. Critically, the constructions for distinct sets V_j are totally independent. The $R = \binom{N}{2} - M\binom{S}{2}$ remaining edges can be decided by any (R, k, p)-variables. The resulting graph is clearly k-wise independent.

The main point is that (i) the events of avoiding H-copies on the various sets V_j are totally independent (by the edge-disjointness of the V_j-s), and that (ii) in our k-wise independent case Δ is rather large (compared with the totally independent case). Thus, avoiding H-copies on *any* of the V_j-s is unlikely. Indeed, let B denote the event that no H-copies appear in the resulting graph, while B' only denotes the event that none of the V_j-s induces H. By Wilson's [45] and Kuzjurin's [33] we have $M = \Theta(N^2/S^2)$, so

$$\Pr[B] \le \Pr[B'] = (1-\Delta)^M \le e^{-\Theta\left(\frac{\Delta N^2}{S^2}\right)},$$

which vanishes by our requirement that $\Delta \gg (S/N)^2$. ■ (Lemma 5)

Completing the proof of Theorem 6. For $v = v(H), \rho = \rho(H), p^* = p^*_H$, and some $1 \ll f(N) \le N^{o(1)}$, define p s.t. p^{-1} is the minimal power of 2 that is larger than $\frac{f(N)}{p^*}$. As desired $p \ll p^*$. Let e_1 and e_0 respectively denote the number of edges and non-edges in H. With $M = \binom{v}{2}$ and $F = 1/p$, we apply Lemma 1 to produce (M,k,p)-variables s.t. with probability $\ge F^{-k}$ the first e_0 variables have value 0, and the remaining e_1 variables have value 1. By Lemma 5, the latter immediately implies the existence of k-wise independent graphs that a.s. contain H-copies as long as $F^k \ll (N/v)^2$. As $F = 1/p = N^{\rho+o(1)}$, this $\ll$ requirement translates to $k\rho \lneqq 2$. ■ (Theorem 6)

5.5. The Chromatic Number

Observation 2 (Preserving the chromatic number lower bound) *For any $c > 0$ there exists some $d > 0$, s.t. all k-wise independent graphs $\{\mathcal{G}^k(N,p)\}_{N\in\mathbb{N}}$ with $(\log(N))^{-c} \le p \le 1 - N^{-o(1)}$ and $k \ge d(\log(N))^{c+1}$ a.s. have chromatic number $\chi \ge \frac{N\log(1/(1-p))}{2\log(pN)}$.*

Proof. Let $I(G)$ denote the independence number of (a single) N-vertex graph G. Clearly, $\chi(G) \ge \frac{N}{I(G)}$, so observation 2 follows from the fact that a.s. $I \le \frac{2\log(pN)}{\log(1/(1-p))}$ which is precisely observation 3 in [5]. ■

Theorem 7 (Preserving the chromatic number upper bound) *There exists an absolute constant c s.t. the following holds. All k-wise independent graphs $\{\mathcal{G}^k(N,p)\}_{N\in\mathbb{N}}$ with $p \le 1/2$ a.s. have chromatic number $\chi \le \frac{cN\log(1/(1-p))}{\log(pN)}$, whenever either:*

1. *$k \ge 12$ and $p \ge N^{-\frac{1}{75}}$; or*

2. *$k \ge \log(N)$ and $p \ge c\frac{\log(N)}{N}$.*

Remark. No special effort was made to optimize the constants $\frac{1}{2}$ and $\frac{1}{75}$.

Proof (sketch). Since p is bounded from above and $\log(1/(1-p)) \xrightarrow{p\to 0} p/\ln(2)$, it suffices to show that a.s. $\chi \le O(\frac{pN}{\log(pN)})$. Item 1 is based on Alon, Krivelevich and Sudakov's [3]. Specifically, choose $\delta = 1/25$, s.t. by item 1 in Lemma 3 (with $\epsilon = (\log(N))p^{-1/2}N^{-3/8}$) and by item 1 in Lemma 4 (with $\gamma = (\log(N))p^{-1}N^{-1/6}$), a.s. all the degrees are lower bounded by $pN(1 - p^{-1/2}N^{-3/8+o(1)}) \ge pN - N^{1-4\delta}$, and all co-degrees are upper bounded by $p^2N(1 + p^{-1}N^{-1/6+o(1)}) \le p^2N - N^{1-4\delta}$. By Theorem 1.2 in [3], these conditions (with $\delta < 1/4$ and $p \ge N^{-\frac{\delta}{3}}$) imply that $\chi \le \frac{4pN}{\delta\ln N} \le O(\frac{pN}{\log(pN)})$.

Item 2 follows from jumbledness and the main result of Alon, Krivelevich and Sudakov in [4] (which is based on Johansson's [28]), by which any graph with maximum degree d in which every neighborhood of a vertex contains at most $d^{2-\beta}$ edges (for some constant β) has chromatic number $\chi \le O(\frac{d}{\log d})$. ■

Acknowledgements. The second author wishes to thank Oded Goldreich for his encouragement, and Ori Gurel-Gurevich, Chandan Kumar Dubey, Ronen Gradwohl, Moni Naor, Eran Ofek, Ron Peled, and Ariel Yadin for useful discussions. We thank the anonymous referees for their useful comments and for referring us to [41].

References

[1] N. Alon, L. Babai, A. Itai. *A Fast and Simple Randomized Parallel Algorithm for the Maximal Independent Set Problem.* Journal of Algorithms 7, 567-583, 1986.

[2] N. Alon , F. R. K. Chung. *Explicit construction of linear sized tolerant networks.* Discrete Math. 72, 15-19, 1988; (Proc. of the First Japan Conference on Graph Theory and Applications, Hakone, Japan, 1986.)

[3] N. Alon, M. Krivelevich, B. Sudakov. *List Coloring of Random and Pseudo-Random Graphs.* Combinatorica 19 (1999), 453-472.

[4] N. Alon, M. Krivelevich, B. Sudakov. *Coloring graphs with sparse neighborhoods.* J. Combinatorial Theory, Ser. B 77 (1999), 73-82.

[5] N. Alon, A. Nussboim. *k-Wise Independent Random Graphs.* Complete version is available at `http://www.wisdom.weizmann.ac.il/~asafn/PAPERS/K_WISE_GNP.pdf`.

[6] N. Alon, J. Spencer. *The Probabilistic Method.* John Wiley, New York, 1992.

[7] I. Benjamini, O. Gurel-Gurevich, R. Peled. *On k-wise independent distributions and boolean functions.* To appear.

[8] B. Bollobás. *Random Graphs.* Academic Press, 1985.

[9] B. Bollobás. *Random Graphs.* In Combinatorics (Swansea, 1981), Volume 52 of London. Math. Soc. Lecture Note Ser., 80102. Cambridge Univ. Press, 1981.

[10] B. Bollobás. *The Chromatic Number of Random Graphs.* In Combinatorica 8 49-55, 1988.

[11] B. Bollobás, P. Erdös. *Cliques in Random Graphs.* Math Proc Camb Phil Soc 80 (1976), 419-427.

[12] B. Bollobás, A. Thomason. *Threshold Functions.* Combinatorica 7 (1986), 35-38.

[13] B. Chor, O. Goldreich. *On the Power of Two-Point Based Sampling.* J. Complexity 5(1): 96-106 (1989).

[14] F. R. K. Chung, R. L. Graham , R. M. Wilson. *Quasi-Random Graphs.* Combinatorica 9, 345-362, 1989.

[15] P. Erdös, A. Rényi. *On Random Graphs I.* Publicationes Mathematicae 6 (1959), 290-297.

[16] P. Erdös, A. Rényi. *On the Evolution of Random Graphs.* Publications of the Mathematical Institute of the Hungarian Academy of Sciences, 5:17-61, 1960.

[17] P. Erdös, A. Rényi. *On Random Matrices.* Publicationes Mathematicae 8 (1964), 455-461.

[18] P. Erdös, A. Rényi. *On the Existence of a Factor of Degree One of a Connected Random Graph.* Acta Mathematica 17 (1966),359-368.

[19] P. Erdös, A. Rényi. *On Random Matrices ii.* Studia Sci. Math. Hungar. 3, 459-464, 1968.

[20] R. Fagin. *Probabilities in Finite Models*, Journal of Symbolic Logic, Vol. 41, 50-58, 1969.

[21] Z. Füredi , J. Komlos. *The eigenvalues of random symmetric matrices.* Combinatorica 1 (1981), 233-241.

[22] E. Friedgut, G. Kalai. *Every Monotone Graph Property Has a Sharp Threshold.* Proc. Amer. Math. Soc. 124 (1996), 2993-3002.

[23] A. Frieze. *On the Independence Number of Random Graphs.* Discrete Math.81 171-175, 1990

[24] O. Goldreich, S. Goldwasser, A. Nussboim. *On the Implementation of Huge Random Objects.* In Proc. 44th IEEE Symposium on Foundations of Computer Science, 68-79, 2003.

[25] Y. V. Glebskii, D. I. Kogan, M. I. Liagonkii, V. A. Talanov. *Range and Degree of Realizability of Formulas in the Restricted Predicate Calculus*. Cybernetics, Vol. 5, 142-154, 1976.

[26] D. Hefetz, M. Krivelevich, T. Szabo. *Hamilton Cycles in Highly Connected and Expanding Graphs.* Preprint.

[27] A. Joffe. *On a Set of Almost Deterministic k-Wise Independent Random Variables.* Annals of Probability 2, 1961-1962, 1974.

[28] A.R. Johansson. *Asymptotic Choice Number for Triangle Free Graphs.* DIMACS Technical Report 91-5.

[29] S. Janson, T. Łuczak, A. Rucinski. *Random Graphs.* New York: Wiley, 2000.

[30] A.D. Koršunov. *Solution of a Problem of Erdös and Rényi on Hamiltonian Cycles in Nonoriented Graphs.* Dokl. Akad. Nauk SSSR Tom 228(1976) 760-764.

[31] J. Komlós, E. Szemerédi. *Limit Distributions for the Existence of Hamilton Circuits in a Random Graph.* Discrete Math. 43 (1983) 55-63.

[32] M. Krivelevich , B. Sudakov. *Pseudo-random Graphs.* In More Sets, Graphs and Numbers, Bolyai Society Mathematical Studies 15, Springer, 2006, 199-262.

[33] Nikolai N. Kuzjurin. *On the difference between asymptotically good packings and coverings.* European J. Combin. 16 (1995), no. 1, 35-40.

[34] T. Łuczak. *The Chromatic Number of Random Graphs.* Combinatorica(11),45-54,1991.

[35] D.W. Matula. *The Largest Clique Size in a Random Graph.* Tech. Rep. Dept. Comp. Sci. Southern Methodist Univ., Dallas, 1976.

[36] M. Naor, A. Nussboim, E. Tromer. *Efficiently Constructible Huge Graphs that Preserve First Order Properties of Random Graphs*. Proceedings of the 2'nd Theory of Cryptography Conference, 66-85, 2005.

[37] A. Nussboim. *Huge Pseudo-Random Graphs that Preserve Global Properties of Random Graphs.* M.Sc. Thesis, Advisor: S. Goldwasser, Weizmann Institute of Science, 2003, `http://www.wisdom.weizmann.ac.il/~asafn/psdgraphs.ps`.

[38] L. Pósa. *Hamiltonian Circuits in Random Graphs.* Discrete Math 14 (1976), 359-364.

[39] A. Rucinski, A. Vince. *Strongly Balanced Graphs and Random Graphs.* J. Graph Theory 10 (1986) 251-264.

[40] S. Shelah, J. H. Spencer. *Zero-One Laws for Sparse Random Graphs*, Journal of the American Mathematical Society, Vol. 1, 97-115, 1988.

[41] J. P. Schmidt, A. Siegel, A. Srinivasan. *Chernoff-Hoeffding Bounds for Applications with Limited Independence.* SIAM J. Discrete Math. 8(2): 223-250 (1995).

[42] A. Thomason. *Pseudo-Random Graphs.* Proceedings of Random Graphs, Annals of Discrete Mathematics 33, 307-331, 1987.

[43] V. H. Vu. *Spectral norm of random matrices.* STOC 2005, 423-430.

[44] E. Wigner. *On the Distribution of the Roots of Certain Symmetric Matrices.* Ann. of Math. 67, 325-328, 1958.

[45] R. M. Wilson. *Decomposition of complete graphs into subgraphs isomorphic to a given graph.* Congressus Numerantium XV (1975), 647-659.