2018 IEEE 59th Annual Symposium on Foundations of Computer Science

# Revealing Network Structure, Confidentially: Improved Rates for Node-Private Graphon Estimation

Christian Borgs and Jennifer Chayes
*Microsoft Research.*
*Cambridge, MA*
{*borgs, jchayes*}*@microsoft.com*

Adam Smith
*Boston University*
*Boston, MA*
*ads22@bu.edu*

Ilias Zadik
*MIT*
*Cambridge, MA*
*izadik@mit.edu*

***Abstract*—Motivated by growing concerns over ensuring privacy on social networks, we develop new algorithms and impossibility results for fitting complex statistical models to network data subject to rigorous privacy guarantees. We consider the so-called *node-differentially private* algorithms, which compute information about a graph or network while provably revealing almost no information about the presence or absence of a particular node in the graph.**

**We provide new algorithms for node-differentially private estimation for a popular and expressive family of network models: *stochastic block models* and their generalization, *graphons*. Our algorithms improve on prior work [15], reducing their error quadratically and matching, in many regimes, the optimal nonprivate algorithm [37]. We also show that for the simplest random graph models ($G(n,p)$ and $G(n,m)$), node-private algorithms can be qualitatively more accurate than for more complex models—converging at a rate of $\frac{1}{\varepsilon^2 n^3}$ instead of $\frac{1}{\varepsilon^2 n^2}$. This result uses a new extension lemma for differentially private algorithms that we hope will be broadly useful.**

***Keywords*-Differential privacy, stochastic block models, graphons, private data analysis.**

## I. Introduction

Network data play an increasingly important role in many scientific fields. Data from social networks, in which the nodes represent individuals and edges represent relationships among them, are transforming sociology, marketing, and political science, among others. However, what makes these data so valuable also makes them highly sensitive—consider, for example, the public sentiment surrounding the recent Cambridge Analytica scandal.

What kinds of information can we release about social networks while preserving the privacy of their users? Straightforward approaches, such as removing obvious identifiers or releasing summaries that concern at least a certain number of nodes, can be easily broken [46, 38].

In this paper, we develop new algorithms and impossibility results for fitting complex statistical models to network data subject to rigorous privacy guarantees. We consider *differentially private* algorithms [23]. There are two main variants of differential privacy for graphs: *edge* and *node* differential privacy [50]. Intuitively, edge differential privacy ensures that an algorithm's output does not reveal the inclusion or removal of a particular edge in the graph, while node differential privacy hides the inclusion or removal of a node together with all its adjacent edges. Edge privacy is weaker (hence easier to achieve) and has been studied more extensively [47, 50, 34, 45, 43, 35, 28, 29, 33, 40, 32, 27, 7, 45, 35, 43, 32, 54].

We study node-differentially private algorithms. These ensure that, no matter what an analyst observing the output knows ahead of time, she learns the same things about an individual Alice regardless of whether Alice's data are used or not. Node privacy's stringency makes the design of accurate, private algorithms challenging; only a small number of techniques for designing such algorithms are known [36, 8, 18, 49, 21].

We provide new algorithms for node-differentially private estimation for a popular and expressive family of network models: *stochastic block models* and their generalization, *graphons*. Our algorithms improve on prior work (by a subset of us [15]), roughly reducing their error quadratically and matching, in many regimes, the optimal nonprivate algorithm [37, 44]. We also show that for the simplest random graph models ($G(n,p)$ and $G(n,m)$), node-private algorithms can be qualitatively more accurate than for more complex models—converging at a rate of $\frac{1}{\varepsilon^2 n^3}$ instead of $\frac{1}{\varepsilon^2 n^2}$. This result uses a new extension lemma for differentially private algorithms that we hope will be broadly useful.

*Modeling Large Graphs via Graphons:* Traditionally, large graphs have been modeled using various parametric models, one of the most popular being the *stochastic block model* [30]. Here one postulates that an observed graph was generated by first assigning vertices at random to one of $k$ groups, and then connecting two

2575-8454/18/$31.00 ©2018 IEEE
DOI 10.1109/FOCS.2018.00057

vertices with a probability that depends on the groups the two vertices are members of.

As the number of vertices of the graph in question grows, we do not expect the graph to be well described by a stochastic block model with a fixed number of blocks. We therefore consider nonparametric models described by a *graphon*. A graphon is a measurable, bounded function $W : [0,1]^2 \to [0,\infty)$ such that $W(x,y) = W(y,x)$, which for convenience we take to be normalized: $\int W = 1$. Given a graphon, we generate a graph on $n$ vertices by first assigning i.i.d. uniform labels $x_i \in [0,1], i = 1,2,\ldots,n$ to the vertices, and then connecting vertices $i,j$ with labels $x_i, x_j$ with probability $H_n(i,j) = \rho_n W(x_i,x_j)$, where $\rho_n$ is a parameter determining the density of the generated graph $G_n$ with $\rho_n \|W\|_\infty \leq 1$. We call $G_n = G_n(\rho W)$ a $W$-random graph with target density $\rho_n$ (or simply a $\rho_n W$-random graph).

This model captures stochastic block models as well as more complex models, e.g. random geometric graphs, where each vertex corresponds to a point in a metric space (selected randomly according to a particular distribution) and vertices share an edge if their points are sufficiently close [26, 20, 48, 24].

For both the "dense" setting (where the target density $\rho_n$ does not depend on the number of vertices) and the "sparse" setting (where $\rho_n \to 0$ as $n \to \infty$), graphons play a key role in the convergence theory for graph sequences [31, 4, 42, 9, 10, 12, 13, 14], providing limit objects in several natural topologies.

*Metrics for Estimation:* Given a single graph $G_n$ generated as $\rho W$-random for unknown $\rho$ and $W$, how well can we estimate $\rho$ and $W$? This task has now been studied extensively [5, 51, 19, 6, 41, 52, 39, 53, 16, 3, 55, 25, 2, 17, 1, 37, 44]. One issue faced by all these works is *identifiability*: multiple graphons can lead to the same distribution on $G_n$. Specifically, two graphons $W$ and $\tilde{W}$ lead to the same distribution on $W$-random graphs if and only if there are measure preserving maps $\varphi, \tilde{\varphi} : [0,1] \to [0,1]$ such that $W^\varphi = \widetilde{W}^{\tilde{\varphi}}$, where $W^\varphi$ is defined by $W(x,y) = W(\varphi(x),\varphi(y))$ [22, 11]. Hence, there is no "canonical graphon" that an estimation procedure can output. Some of the literature circumvents identifiability by making strong additional assumptions that imply the existence of canonical equivalence class representatives. We make no such assumptions, but instead define consistency in terms of a metric on equivalence classes. We use a variant of the $L_2$ metric,

$$\delta_2(W,W') = \inf_{\varphi:[0,1]\to[0,1]} \|W^\varphi - W'\|_2 \,, \qquad \text{(I.1)}$$

where $\varphi$ ranges over measure-preserving bijections.

In this work, we set aside questions of computational efficiency and focus on establishing what rates are possible in principle (our algorithms, like the nonprivate state of the art, run in time roughly exponential in $n$).

For our purposes, the most relevant work is that of Klopp, Tzybakov and Verzalen [37], who establish tight upper and (in parallel to [44]) lower bounds on the error rate of nonprivate algorithms, given a single $n$-vertex $\rho W$-random graph and a target number of blocks, $k$. Our algorithms match their rate for large enough values of the privacy parameter.

*Private Algorithms for Graph Data and the Rewiring Metric:* Let $\mathcal{A}$ be a randomized algorithm that takes values from some input metric space $(\mathcal{M}, d)$ (called the space of *data sets*) and ouputs probability distributions on some measurable space $(\Omega, \mathcal{F})$.

**Definition I.1.** *The algorithm $\mathcal{A}$ is $\varepsilon$-differential private ($\varepsilon$-DP) with respect to the metric $d$ if, for all subsets $S \in \mathcal{F}$ and $D_1, D_2 \in \mathcal{M}$,*

$$\mathbb{P}\left(\mathcal{A}(D_1) \in S\right) \leq \exp\left[\varepsilon d(D_1,D_2)\right] \mathbb{P}\left(\mathcal{A}(D_2) \in S\right).$$

The metric $d$ is typically defined by specifying pairs of data sets that are adjacent (i.e., at distance 1 from each other), and then letting $d$ be the induced path metric.

There are two natural variants of differential privacy suited for graph datasets, edge differential privacy and node differential privacy. Intuitively, edge differentially private algorithms hide the presence or absence of a particular relationship between individuals in a social network, while node differentially private algorithms protect each individual together with all his/her relationsips. In both cases, the data set is an undirected graph with no self-loops; we let $\mathcal{G}_n$ denote the set of such graphs on $n$ vertices. Formally, edge differential privacy is obtained by taking $d$ to count the number of edges that differ between two graphs (the Hamming metric on adjacency matrices). In contrast, node differential privacy is defined with respect to the *rewiring* metric, or *node distance*, between graphs: we say that two distinct graphs $G, G'$ are at node-distance 1 (or *adjacent*) if one can be obtained from the other by inserting or removing arbitrary sets of edges adjacent to a singe vertex, a process we call *rewiring* the vertex. For arbitrary $G_1, G_2 \in \mathcal{G}_n$, define the **node-distance** between them, $d_v(G_1,G_2)$, to be the minimum number of vertices of $G_1$ that need to be rewired to obtain $G_2$. A randomized algorithm $\mathcal{A}$ defined on $\mathcal{G}_n$ is $\varepsilon$-node differentially private ($\varepsilon$-node DP) if it is $\varepsilon$-differentially private with respect to the node-distance $d_v$.

Edge differential privacy is a weaker notion and has been extensively studied over the past decade. Algorithms have been developed for various tasks such as the release of subgraph counts, the degree distribution and the parameters of generative graph models [28], [35], [45], [33], [34], [47]. On the other hand, the node-differential privacy is a much stronger privacy guarantee. The first nontrivial node-differentially algorithms were designed (concurrently) in [8, 18, 36], with a focus on algorithms that release one-dimensional summaries of a network such as subgraph counts. Later work [49, 15, 21] introduced higher-dimensional techniques. Most relevant here, a subset of us gave the first algorithms for node-private graphon estimation [15]. A common thread to all these works is the use of *Lipschitz extensions* in the rewiring metric to control the sensitivity of summary statistics for sparse graphs. A key piece of this paper is a novel use of such extensions.

The previous results for graphon estimation achieved estimation error going to 0 for a large parameter range, but fell short in several respects: first, even when $\varepsilon$ is arbitrarily large, the algorithm does not match the best nonprivate bounds. Secondly, there was no evidence that the extra terms due to privacy (involving $\varepsilon$) in the accuracy guarantee were necessary.

### A. Contributions

*New Upper Bounds for Estimating $k$-Block Graphons:* Our main focus is the problem of estimating a bounded normalized graphon $W$ via a node-differentially private algorithm. The estimation algorithm observes one sample of a $\rho W$-random graph, and outputs the description of a graphon $\hat{W}$ that it hopes is close to $W$. We consider algorithms that output a graphon with a succinct description—namely, we assume the estimate $\hat{W}$ is a $k$-block graphon with equal-weight blocks (such a graphon can be described by a $k \times k$ symmetric matrix). The parameter $k$ offers a regularization of sorts, trading off the model's expressivity for complexity. We measure the algorithm's error by the expected squared $\delta_2$ distance (see (I.1)) between $\hat{W}$ and $W$. Borgs et al. [15] studied this problem, developing an inefficient estimation procedure (henceforth the "BCS" algorithm [15, Algorithm 1]) and establishing an upper bound on its error.

Our first contribution is a new analysis of the BCS algorithm that significantly improves the error bound, matching the (tight) nonprivate bounds for a large range of parameters. The new and old results can be summarized as the following upper bound on the mean squared error $\mathbb{E}\left[\delta_2(\hat{W}, W)^2\right]$ of the following form.

**Theorem 1** (Informal)**.** *Fix some $k \geq 1$ and let $\mathcal{A}$ be the BCS algorithm. Then for all bounded graphons $W$,*

$$\mathop{\mathbb{E}}_{G\sim G_n(\rho W)}[\delta_2(\mathcal{A}(G), W)^2] = \underbrace{O\left(\begin{array}{c}\textit{“agnostic and}\\ \textit{sampling errors”}\end{array} + \frac{k^2\log n}{n\varepsilon} + \frac{1}{n^2\rho^2\varepsilon^2}\right)}_{\textit{as in Borgs et al. [15]}} + \underbrace{O\left(\sqrt{\frac{k-1}{n}} + \left(\frac{\log k}{\rho n} + \frac{k^2}{\rho n^2}\right)\right)}_{\textit{improving quadratically Borgs et al. [15]}}$$

Here, the phrase "agnostic and sampling errors" covers two terms that are present in both bounds. The "agnostic error" corresponds to the distance from the true graphon $W$ to the nearest $k$-block graphon—a model misspecification error. It is unavoidable for algorithms that output $k$-block graphons. The "sampling" term corresponds to the expected distance between the true graphon $W$ and the probability matrix $(W(x_i, x_j))_{i,j=1}^n$ defining the $\rho W$-random graph. This distance is a random variable that can be bounded in different ways depending on what is known about $W$. If $W$ is itself a $k$-block graphon, then the the agnostic error is 0, and the sampling error (about $\sqrt{k/n}$ with high probability) is subsumed by the other error terms.

Notice that our improvement to the accuracy bound lies in the "non-private" (that is, independent of $\varepsilon$) part of the error.

This nonprivate part of our new bound is in fact optimal, as it matches the lower bounds for *nonprivate* algorithms. Specifically, consider the case that the true graphon $W$ is in fact a $k$-block graphon and define the rate

$$R_k(\rho, \varepsilon, n) = \min_{\substack{\mathcal{A}\\ \varepsilon-\text{node-DP}}} \max_{W\, k-\text{block}} \mathop{\mathbb{E}}_{G\sim G_n(\rho W)}[\delta_2(\mathcal{A}(G), W)^2].$$

Klopp et al. [37, Prop. 3.4] (and McMillan and Smith [44, Theorem 3]) establish the best rate if we allow any estimation algorithm $\mathcal{A}$—private or not—to be

$$\Theta\left(\min\{\sqrt{\frac{k}{n}} + \left(\frac{\log k}{\rho n} + \frac{k^2}{\rho n^2}\right), 1\}\right) \text{ for } k \geq 2.$$

In particular, focusing on $\varepsilon$-node-DP algorithms we conclude that for any $k \geq 2$,

$$R_k(\rho, \varepsilon, n) = \Omega\left(\min\{\sqrt{\frac{k}{n}} + \left(\frac{\log k}{\rho n} + \frac{k^2}{\rho n^2}\right), 1\}\right) \tag{I.2}$$

Notice that our upper bound as established in Theorem 1 matches exactly this lower bound when the true graphon has exactly $k$ blocks and $\varepsilon$ is sufficiently large (since then the agnostic error is 0, the sampling error is know to be $O(\sqrt{k/n})$, and the $\varepsilon$-dependent terms go to 0). In particular, using Theorem 1 we conclude a tight characterization of the $\varepsilon$-independent part of the rate $R_k(\rho, \varepsilon, n)$,

**Collorary 1** (Informal)**.** *Fix some $k \geq 2$. Then there exists an algorithm such that for all bounded graphons $W$,*

$$R_k(\rho,\varepsilon,n) = O\left(\frac{k^2\log n}{n\varepsilon} + \frac{1}{n^2\rho^2\varepsilon^2}\right) + \underbrace{O\left(\sqrt{\frac{k-1}{n}} + \left(\frac{\log k}{\rho n} + \frac{k^2}{\rho n^2}\right)\right)}_{\textit{tight nonprivate part based on (I.2)}}$$

*Additional Error Due to Privacy ($k \geq 2$):* To understand whether we have found the true minimax rate, it remains to understand whether the terms based on $\varepsilon$ are optimal. We show that the second of these cannot be improved, on the slightly less restrictive case where the blocks of the $k$-block graphon can have different sizes, a set we denote by $\tilde{W}[k]$.

**Theorem 2** (Informal)**.** *For $k \geq 2$,*

$$\tilde{R}_k(\rho,\varepsilon,n) = \Omega\left(\frac{1}{n^2\varepsilon^2}\right),$$

*where $\tilde{R}_k(\rho,\varepsilon,n)$ is defined to be*

$$\min_{\mathcal{A}\ \varepsilon-\textit{node-DP}} \max_{W\in\tilde{W}[k]} \mathbb{E}_{G\sim G_n(\rho W)}[\delta_2(\mathcal{A}(G), W)^2]. \quad \text{(I.3)}$$

This lower bound applies even to algorithms that simply estimate the unknown density parameter $\rho$. The proof of this lower bound is fairly simple, relying on the fact that even if the connection probabilities of a 2-block graphon are known, estimating the graphon requires one to accurately estimate the probability mass of the two blocks. We reduce to this latter problem from the well-studied problem of estimating the bias of a sequence of $n$ coin flips differentially privately.

We leave open the question of whether the term $\frac{k^2\log n}{n\varepsilon}$ is necessary.

*The Case of Erdős-Renyi Graphs (1-Block Graphons):* The upper bounds above all apply for $k = 1$, in particular, but the lower bounds generally do not yield anything interesting in that case. The case of $k = 1$ corresponds to graphs generated according to the well-studied Erdős-Renyi model, where each possible edge appears independently with an unknown probability $p$. To phrase this as an estimation problem, consider the scale parameter $\rho$ to be known, and the algorithm's goal is to estimate a constant graphon $W(x, y) = p$ subject to $p \leq \rho$. (Unlike in the case of larger $k$, estimating the normalized graphon $W$ is trivial since, after normalization, $W(x, y) = 1$.)

Nonprivately, the optimal estimator is the edge density of the observed graph, $(\#\text{edges})/\binom{n}{2}$.

What about private algorithms? First, observe that the algorithm $\mathcal{A}_0$ that adds Laplace noise of order $\frac{1}{n\varepsilon}$ to the edge density is $\varepsilon$-node differentially private. Furthermore, for $p \in [0, \rho]$,

$$\mathbb{E}_{G\sim G_{n,p}}\left[|\mathcal{A}_0(G) - p|^2\right] = O\left(\frac{\rho}{n^2} + \frac{1}{n^2\varepsilon^2}\right).$$

Potentially surprisingly, we establish that the rate obtained this way is not optimal. As we explain in section 3, the main reason for the suboptimality of this method is that it is based on calculating the worst-case sensitivity of the edge density over the space of all undirected graphs. In particular, this estimator ignores the rich structure of the Erdos-Renyi graphs. Using this structure, we establish a series of results relating the node-distance and the Erdos-Renyi graphs along-side with a general extension result (Proposition V.1) which combined allows to prove the following improved upper bound

**Theorem 3** (Informal)**.** *There exists an $\varepsilon$-node-DP algorithm $\mathcal{A}$ such that for any $\rho \in (0, 1]$,*

$$\max_{p\in[0,\rho]} \mathbb{E}_{G\sim G_{n,p}}[(A(G) - p)^2] = O\left(\frac{\rho}{n^2} + \frac{\log n}{n^3\varepsilon^2}\right). \quad \text{(I.4)}$$

Using the same techniques we are able to establish the corresponding result for the uniform $G(n, m)$ model which obtains an error

$$O\left(\frac{\log n}{n^3\varepsilon^2}\right),$$

avoiding the edge-density variance term which appears in the Erdos-Renyi case, $\frac{\rho}{n^2}$. We end this section with a novel lower bound for $G(n, m)$ model.

**Theorem 4** (Informal)**.** *Suppose $\varepsilon$ is a constant. Then,*

$$\min_{\mathcal{A}\varepsilon-\textit{node-DP}} \max_{m\in[\frac{1}{3}\binom{n}{2},\frac{2}{3}\binom{n}{2}]} \mathbb{E}_{G\sim G(n,m)}[(A(G) - \frac{m}{\binom{n}{2}})^2] = \Omega\left(\frac{1}{n^3\varepsilon^2}\right).$$

This Theorem establishes that the upper bound for the $G(n, m)$ model is optimal up-to-logarithmic terms in the $\varepsilon$-constant regime and suggests the same for the Erdos-Renyi case.

*A General Extension Result:* In Section 4, we present in detail the general extension result we used in Section 3 as it could be of independent interest. The extension result works for an arbitrary $\varepsilon$-differentially private algorithm which receives input from a metric space $(M, d)$ and outputs distributions of an arbitrary output measurable space $(\Omega, \mathcal{F})$. We establish that if there exists such an $\varepsilon$-differentially private algorithm $\hat{\mathcal{A}}$ defined only on a subset of the input space $\mathcal{H}$, the algorithm can be extended to an $2\varepsilon$-differentially private algorithm $\mathcal{A}$ defined on the whole input space $M$ such that if the input $G \in \mathcal{H}$, the distributions of the output of $\hat{\mathcal{A}}(G)$ coincides with the distribution of $\mathcal{A}(G)$.

## II. Notation and Preliminaries

*$k$-block Graphons:* For every $k \in \mathbb{N}$, we embed the set of $k \times k$ symmetric matrices into the space of graphons as following: let $\mathcal{P}_k = (I_1, \ldots, I_k)$ be the partition of $[0,1]$ into adjacent intervals of lengths $\frac{1}{k}$. For $A \in \mathbb{R}^{k\times k}_{\geq 0}$ define $W[A]$ to be the step function which equals $A_{ij}$ on $I_i \times I_j$, for every $i, j \in [k]$. We say a graphon $W$ is a $k$-block graphon if $W = W[A]$ for some $A \in \mathbb{R}^{k\times k}_{\geq 0}$ and denote by $\mathcal{W}[k]$ the space of $k$-block graphon.

*Distances between Graphons:* For $A, B$ symmetric $n \times n$ matrices and a graphon $W$ we set for convenience $\delta_2(A, W) = \delta_2(W[A], W)$ and $\delta_2(A, B) = \delta_2(W[A], W[B])$, where $\delta_2$ is defined for two graphons in I.1. Furthermore we focus also on the, in general larger than $\delta_2$, distance

$$\hat{\delta}_2(A, W) = \inf_{\pi \in \mathcal{S}_n} \|W[A^\pi] - W\|_2,$$

where $\pi$ ranges over all permurations of $\{1, 2, \ldots, n\}$ and for all $i, j \in [n]$, $A^\pi_{ij} = A_{\pi(i),\pi(j)}$. $\delta_2$ is in principle smaller than $\hat{\delta}_2$ as it minimizes the $\ell_2$ distance over all measure-preserving transformations, while the latter distance minimizes only on such transformation that can be expressed as permutations of the rows and columns of the underlying matrix $A$.

We consider two fundamental types of errors of approximation of $W$.

The **agnostic error**, or *oracle error*, of approximating $W$ by a $k$-block graphon with respect to $\delta_2$ and $\hat{\delta}_2$,

$$\varepsilon^{(O)}_k(W) = \min_B \delta_2(B, W)$$

and

$$\hat{\varepsilon}^{(O)}_k(W) = \min_B \hat{\delta}_2(B, W),$$

where $B$ ranges over all matrices in $\mathbb{R}^{k\times k}$. The agnostic errors corresponds to the model mispecification errors of the statistical problem of estimating $W$ using a $k$-block graphon. We consider them as benchmarks for our approach, and the errors an "oracle" could obtain (hence the superscript $O$).

*Scale of agnostic error:* For any bounded $W$, both $\varepsilon^{(O)}_k(W)$ and $\hat{\varepsilon}^{(O)}_k(W)$ tend to zero as $k \to +\infty$ (see [15, Sec. 2] for details).

The **sampling error** of approximating $W$ from $G = G_n(\rho W)$ with respect to $\hat{\delta}_2$,

$$\varepsilon_n(W) = \hat{\delta}_2(H_n(W), W).$$

Recall that the only information for $W$ in the observed graph $G$ comes from the edge probabilities $H_n(i, j) = \rho W(x_i, x_j)$ where $x_i$ are the iid uniform in $[0, 1]$ labels of the vertices. Intuitively, a large discrepancy between the edge probability matrix $H_n(W)$ and $W$ results in bad estimation of $W$ given $G$. Unlike the agnostic error, the sampling error is a random variable (depending on the assignment of nodes to "types" in $[0, 1]$.)

*Scale of sampling error:* For any bounded $W$, $\varepsilon_n(W) \xrightarrow{P} 0$ as $n \to +\infty$ [15, Lemma 1]. Furthermore, if additionally $W$ is a $k$-block graphon it can be established that $\varepsilon_n(W) = O(\sqrt[4]{\frac{k}{n}})$ with probability tending to one as $n \to +\infty$ [15, Appendix D].

## III. Private Graphon Estimation

*Model:* Let $k, n \in \mathbb{N}$ with $k \leq n$, $\Lambda \geq 1$ and $\varepsilon > 0$. Suppose $W$ is an unknown normalised graphon with $\|W\|_\infty \leq \Lambda$. For some unknown "sparsity level" $\rho = \rho_n \in (0, 1)$ with $\rho\Lambda \leq 1$, the analyst observes a graph $G$ sampled from the $\rho W$-random graph, $G_n(\rho W)$. The analyst's goal is to use an $\varepsilon$-node-DP algorithm $\mathcal{A}$ on $G$ to output a $k$-block model approximation of $W$, say $W[\hat{B}]$ for $\hat{B} \in \mathbb{R}^{k\times k}$, which minimizes the mean squared error,

$$\mathbb{E}_{G\sim G_n(\rho W), \hat{B}\sim\mathcal{A}(G)}[\delta_2(\hat{B}, W)^2].$$

### A. Main Algorithm

We use the same algorithm as Borgs et al. [15], described in Algorithm 1.

*Notation for Algorithm 1:* For $k, n \in \mathbb{N}$ with $k \leq n$, we say that $\pi : [n] \to [k]$ is a $k$-equipartition of $[n]$, if it partitions $[n]$ into $k$ classes such that is for every $i \in [n]$, $||\pi^{-1}(i)| - \frac{n}{k}| < 1$. For a matrix $Q \in \mathbb{R}^{k\times k}$ and a matrix $A \in \mathbb{R}^{n\times n}$, we set $\mathrm{Score}(Q, \pi, A) = \|A\|_2^2 - \|A - Q_\pi\|_2^2$, where $\pi$ ranges over all $k$-equipartitions of $[n]$,$(Q_\pi)_{i,j} = Q_{\pi(i),\pi(j)}$ for all $i, j \in [n]$ and $\|A\|_2 = \left(\frac{1}{n^2}\sum_{i,j=1}^n A_{ij}^2\right)^{\frac{1}{2}}$. Finally, we denote by $\mathcal{G}_n$ the space of undirected graphs on $n$ vertices and $\mathcal{G}_{n,d}$ the subset

of graphs in $\mathcal{G}_n$ where the maximum degree is bounded by $d$.

We now describe the steps of the algorithm. The algorithm takes as input the privacy parameter $\varepsilon$, the graph $G$, a number $k$ of blocks, and a constant $\lambda \geq 1$ that will have to be chosen large enough to guarantee consistency of the algorithm.

**Algorithm 1:** Private Estimation Algorithm

**Input:** $\varepsilon > 0$, $\lambda \geq 1$, an integer $k$ and graph $G$ on $n$ vertices.

**Output:** $k$-block graphon (represented as a $k \times k$ matrix $\hat{B}$) estimating $\rho W$

Compute an $(\varepsilon/2)$-node-private density approximation $\hat{\rho} = \rho(G) + \mathrm{Lap}(4/n\varepsilon)$ ;

$d = \lambda \hat{\rho} n$ (the target maximum degree) ;

$\mu = \lambda \hat{\rho}$ (the target $L_\infty$ norm for $\hat{B}$) ;

For each $B$ and $\pi$, let $\widehat{\mathrm{Score}}(B, \pi; \cdot)$ denote a nondecreasing Lipschitz extension (from [36]) of $\mathrm{Score}(B, \pi; \cdot)$ from $\mathcal{G}_{n,d}$ to $\mathcal{G}_n$ such that for all matrices $A$, $\widehat{\mathrm{Score}}(B, \pi; A) \leq \mathrm{score}(B, \pi; A)$, and define

$$\widehat{\mathrm{Score}}(B; A) = \max_{\pi} \widehat{\mathrm{Score}}(B, \pi; A)$$

**return** $\hat{B}$, sampled from the distribution

$$\Pr(\hat{B} = B) \propto \exp\left(\frac{\varepsilon}{4\Delta} \widehat{\mathrm{Score}}(B; A)\right),$$

where $\Delta = \dfrac{4d\mu}{n^2} = \dfrac{4\lambda^2\hat{\rho}^2}{n}$ and $B$ ranges over matrices in

$$\mathcal{B}_\mu = \{B \in [0, \mu]^{k \times k} : \text{all } B_{i,j} \text{ are multiples of } \tfrac{1}{n}\};$$

*Main Result:* Algorithm 1 is $\varepsilon$-node-DP [15, Lemma 3]. Borgs et al gave upper bound on its worst-case mean squared error, $\mathbb{E}_{G \sim G_n(\rho W), \hat{B} \sim \mathcal{A}_G}[\delta_2(\hat{B}, W)^2]$. We state the improved bound here:

**Theorem III.1.** *Suppose*

- $\frac{6 \log n}{n} < \rho \leq \frac{1}{\Lambda}$, $8\Lambda \leq \lambda \leq \sqrt{n}$, *and*
- $\rho n \varepsilon / \log n \to +\infty$, $\varepsilon = O(k^2 \log n / \lambda)$

*Then the $\varepsilon$-node-DP Algorithm 1 from [15], $\mathcal{A}$, with input $\varepsilon, \lambda, k$ and $G$ outputs a pair $(\hat{\rho}, \hat{B}) \in [0,1] \times [0,1]^{k \times k}$ with $\mathbb{E}_{G \sim G_n(\rho W), \hat{B} \sim \mathcal{A}_G}[\delta_2(\frac{1}{\hat{\rho}}\hat{B}, W)^2]$ of the order*

$$O\left(\mathbb{E}\left[\varepsilon_k^{(O)}(W)^2\right] + \mathbb{E}\left[\varepsilon_n(W)^2\right] + \lambda^2\sqrt{\frac{k-1}{n}}\right) + O\left(\lambda\left(\frac{\log k}{\rho n} + \frac{k^2}{\rho n^2}\right) + \lambda^2 \frac{k^2 \log n}{n\varepsilon} + \frac{\lambda^2}{n^2\rho^2\varepsilon^2}\right).$$

The bound from Theorem 1 in [15] states that, under slightly different parameter assumptions, the mean squared error $\mathbb{E}_{G \sim G_n(\rho W), \hat{B} \sim \mathcal{A}_G}[\delta_2(\frac{1}{\hat{\rho}}\hat{B}, W)^2]$ is at most

$$O\left(\mathbb{E}\left[\varepsilon_k^{(O)}(W)^2\right] + \mathbb{E}\left[\varepsilon_n(W)^2\right]\right) + O\left(\sqrt{\lambda^2\left(\frac{\log k}{\rho n} + \frac{k^2}{\rho n^2}\right)}\right) + O\left(\lambda^2 \frac{k^2 \log n}{n\varepsilon} + \frac{\lambda^2}{n^2\rho^2\varepsilon^2}\right).$$

The improvement therefore of our result lies on the $\varepsilon$-independent part of the bound. For convenience, we call this part of the bound the non-private part of the bound and the $\varepsilon$-dependent part, the private part of the bound. As we establish in the following subsection, the improvement of Theorem III.1 on the non-private part is the optimal possible.

*The $k$-block Estimation Rate:* In this subsection we focus on the case $W$ is a $k$-block graphon and establish that the improvement of Theorem 1 on the non-private part of the bound is optimal in the following sense. For some $k \geq 1$, assume that $W \in \mathcal{W}[k]$ with $\|W\|_\infty \leq \Lambda$, that is $W = W[B]$ for some $B \in [0, \Lambda]^{k \times k}$. Restricting ourselves to the specified subset of graphons we consider the minimax rate,

$$\min_{\mathcal{A}\ \varepsilon-\text{node-DP}} \max_{W \in \mathcal{W}[k], \|W\|_\infty \leq \Lambda} \mathbb{E}_{G \sim G_n(\rho W)}[\delta_2(\mathcal{A}_G, W)^2].$$

which we denote by $R_k(\rho, \varepsilon, \Lambda, n)$.

If $k \geq 2$, Theorem 3 from [44] and (up-to-$\log k$ factors) Proposition 3.4 of [37], establishes that this rate, under no differential-privacy constraint (a case corresponding to $\varepsilon$ "equal to" $+\infty$ for our purposes), behaves like

$$\Theta\left(\min\{\Lambda^2\sqrt{\frac{k}{n}} + \Lambda\left(\frac{\log k}{\rho n} + \frac{k^2}{\rho n^2}\right), \Lambda^2\}\right).$$

This result does not directly apply to our setting as we consider only finite $\varepsilon > 0$. Note, though, that $\varepsilon$-node-DP is an increasing property, as if an algorithm is $\varepsilon$-node-DP, it is also $\varepsilon'$-node-DP for any $\varepsilon' > \varepsilon$. Therefore $R_k(\rho, \varepsilon, \Lambda, n)$ is a non-increasing function of $\varepsilon$, as increasing $\varepsilon$ only can shrink the feasible sets of estimators. Hence, the result from provides a

lower bound for the rate $R_k(\rho,\varepsilon,\Lambda,n)$. Combined with Theorem III.1 we obtain a tight characterization of the non-private part of the rate $R_k(\rho,\varepsilon,\Lambda,n)$, and establish that Algorithm 1 from [15] obtains the optimal non-private part of the rate.

**Corollary III.2.** *Suppose $k \geq 2$. Under the assumptions of Theorem III.1 and the additional assumption $\rho n \geq k-2$,*

$$R_k(\rho,\varepsilon,\Lambda,n) = \Omega\left(\min\{\Lambda^2\sqrt{\frac{k}{n}} + \Lambda\left(\frac{\log k}{\rho n} + \frac{k^2}{\rho n^2}\right), \Lambda^2\}\right)$$

*and*

$$R_k(\rho,\varepsilon,\Lambda,n) = O\left(\Lambda^2\sqrt{\frac{k}{n}} + \Lambda\left(\frac{\log k}{\rho n} + \frac{k^2}{\rho n^2}\right)\right) + O\left(\Lambda^2\frac{k^2\log n}{n\varepsilon} + \frac{\Lambda^2}{n^2\rho^2\varepsilon^2}\right),$$

*where the upper bound is achieved by Algorithm 1 from [15].*

*A Lower Bound on the Private Part:* In this subsection we establish for $k \geq 2$ a lower bound on the private part of the rate. We establish that the term of order $\frac{\Lambda^2}{n^2\rho^2\varepsilon^2}$ appearing in the upper bound of Theorem 1 is necessary, up to the dependence on $\rho, \Lambda$. For the lower bound we focus on $k$-block graphons $W = W[B]$ with potentially slightly-unequal sizes, we do not require them to be normalized, and we set $\rho = \Lambda = 1$. Specifically, let $\tilde{\mathcal{W}}[k]$ be the set of all graphons $W$ for which $\|W\|_\infty \leq 1$ and for some $A \in \mathbb{R}_{\geq 0}^{k\times k}$ and some $\mathcal{P}_k = (I_1,\ldots,I_k)$ partition of $[0,1]$ into adjacent intervals of (potentially different) lengths in $[\frac{1}{4k}, \frac{4}{k}]$, $W$ is the step function which equals $A_{ij}$ on $I_i \times I_j$, for every $i,j \in [k]$. Let also

$$\tilde{R}_k(\varepsilon,n) = \min_{\mathcal{A}\ \varepsilon-\text{node-DP}} \max_{W\in\tilde{\mathcal{W}}[k]} \mathbb{E}_{G\sim G_n(W),\hat{B}\sim\mathcal{A}_G}[\delta_2(\hat{B},W)^2].$$

**Theorem III.3.** *Suppose $k \geq 2$. Then*

$$\tilde{R}_k(\varepsilon,n) = \Omega\left(\frac{1}{n^2\varepsilon^2}\right).$$

## IV. Private Estimation of Erdos Renyi Graphs (1-Block Graphons)

This section is devoted to the study of the privately estimating $k$-block graphons in the special case $k=1$. Since for $k=1$ the graphon corresponds to a constant function, we deal with the fundamental question of estimating privately the parameter of an Erdos-Renyi random graph model. Note that since the graphon is constant, to make the estimation task non-trivial we do not adopt the assumption that the graphon is normalized. Furthermore, using the notation of the previous section for reasons of simplicity we focus on the case $\rho$ is known to the analyst and $\Lambda = 1$.

Using such a graphon $W$, we conclude that for some $p_0 \in [0,1]$ $W(x,y) = p_0$ for every $x,y \in [0,1]$ and the analyst's observes simply a sample from an Erdos Renyi random graph with $n$ vertices and parameter $p := \rho\cdot p_0 \leq \rho$. Multiplying the rate by the known $\rho$, the goal becomes to estimate $p$ using an $\varepsilon$-differentially private algorithm. In agreement with the non-private behavior where the estimation rate is provably much smaller when $k=1$ compared to $k>1$ (see Sec. 3.2 in [37] for details), we reveal a similar behavior in the case of private estimation. In particular, based on Theorem III.3 for $k>1$ and $\Lambda = 1$ the rate of interest is

$$\Omega\left(\frac{1}{n^2\varepsilon^2}\right).$$

Here we establish that the $\varepsilon$-dependent part of the rate for $k=1$ drops to

$$O\left(\frac{\log n}{n^3\varepsilon^2}\right).$$

### A. A New Algorithm for Density Estimation in Erdos Renyi Random Graphs

The rate we want to find is for $\rho \in [0,1]$,

$$R(\rho,\varepsilon,n) = \min_{\mathcal{A}\ \varepsilon-\text{node-DP}} \max_{p\in[0,\rho]} \mathbb{E}_{G\sim G_{n,p}}[(A(G)-p)^2].$$

A standard $\varepsilon$-node-DP algorithm for this task is the addition of appropriate Laplace noise to the edge density of the graph $G$ (Lemma 10 of [15]). The global sensitivity (Definition 2 in [15]) of the edge density with respect to the node-distance can be easily proven to be of the order $\Theta(\frac{1}{n})$. In particular it is upper bounded by $\frac{4}{n}$, as if $G, G' \in \mathbb{G}_n$,

$$|e(G) - e(G')| \leq \frac{4}{n} d_v(G,G').$$

Therefore, using Lemma 10 of [15], the addition of $\mathrm{Lap}(\frac{4}{n\varepsilon})$ noise to the edge density provides an $\varepsilon$-node-DP estimator. This estimator allows us to conclude the following Lemma.

**Lemma IV.1.** *For any $\rho, \varepsilon > 0$,*

$$R(\rho,\varepsilon,n) = O\left(\frac{\rho}{n^2} + \frac{1}{n^2\varepsilon^2}\right).$$

As we establish in Theorem IV.3 the upper bound of Lemma IV.1 is, potentially surprisingly, not tight. A

weakness of the proposed algorithm is that it computes an estimator based on the global sensitivity of the edge density over all pairs of undirected graphs of $n$ vertices and on the other hand applies it only to graphs coming from Erdos-Renyi models. To reveal more the potential weakness of the estimator, let us consider a pair of node-neighbors $G, G'$, that is $d_v(G, G') = 1$, where the difference $e(G) - e(G')$ is of the order $\frac{1}{n}$. It is easy to check that the difference can become of this order only if the degree of the rewired vertex had $o(n)$ degree in $G$ and $\Theta(n)$ degree in $G'$ or vice versa. Since the degree of every other vertex changes by at most 1, the rewired vertex in $G$ or $G'$ has either very high degree or very low degree compared to the average degree in $G$ or $G'$. Such a non-homogenuous property of the degree distribution appears, though, only with a negligible probability under any Erdos-Renyi model. This line of thought suggests that there could possibly be some "homogeneity" set, $\mathcal{H}$, for which any graph sampled from Erdos Renyi model belongs to with probability $1 - o(1)$ and the sensitivity of the edge density on pairs of graphs from $\mathcal{H}$ is much lower than $\frac{1}{n}$.

Unfortunately the existence of such a set can be proven to be non-true for the following reason. The empty graph $G_0$ (which appears almost surely for the Erdos Renyi graph with $p = 0$) and the complete graph $G_1$ (which appears almost surely for the Erdos Renyi random graph with $p = 1$) should be included in such "homogeneity" set and furthermore

$$\frac{e(G_1) - e(G_0)}{d_v(G_0, G_1)} = \frac{1}{n-1} = \Theta(\frac{1}{n}).$$

We establish, though, that this is essentially the only "extreme" case and such an "homogeneity" set $\mathcal{H}$ exists, in the following sense. There exist a set $\mathcal{H}$ which contains any Erdos Renyi graph with probability $1 - o(1)$, that is

$$\min_{p\in[0,1]} \mathbb{P}_{G\sim G_{n,p}} (G \in \mathcal{H}) = 1 - o(1),$$

and furthermore from any $G, G' \in \mathcal{H}$ either

$$d_v(G, G') > n/4$$

or

$$\frac{|e(G) - e(G')|}{d_v(G, G')} = O(\frac{\sqrt{\log n}}{n^{3/2}}).$$

This $\sqrt{n}$-improvement on the edge density sensitivity on $\mathcal{H}$ allows us to establish the existence of an $\varepsilon/2$-node-DP algorithm which is defined on graphs in $\mathcal{H}$ and has mean squared error of the order $O(\frac{\log n}{n^3\varepsilon^2})$.Notice that the order is much lower than the performance of the addition of Laplace noise (Lemma IV.1). Next we establish a general extension result (Theorem V.1) which allows us to extend the $\varepsilon/2$-node-DP algorithm defined on $\mathcal{H}$ to an $\varepsilon$-node-DP on the whole space of undirected graphs with $n$ nodes. The extension has the crucial property that it outputs the same probability distributions with the original algorithm when the input belongs in $\mathcal{H}$. The extension result applies generally to any $\varepsilon$-differentially private algorithm which takes values in an arbitrary metric space and outputs probability distributions of any measurable space. Since such a result could be of independent interest we devote Section V solely for its presentation.

Using the extented algorithm we establish the following results for graphs sampled from the Erdos Renyi random graph $G_{n,p}$ and the uniform graph $G(n, m)$. Notice that for the $G_{n,p}$ model there exists an additional non-private term $\frac{\rho}{n^2}$. This appears only in the Erdos-Renyi case and not in the uniform model as it comes from the vanishing but non-zero variance term of the edge density in the Erdos Renyi model.

**Proposition IV.2** (The $G(n, m)$ case)**.** *Let $\varepsilon, \rho \in (0, 1)$ be functions of $n$ such that $\varepsilon n/\log n \to +\infty$. There is an $\varepsilon$-node-DP algorithm $A$ such that, for all $m < \rho\binom{n}{2}$,*

$$\mathop{\mathbb{E}}_{G\sim G(n,m)} \left|A(G) - \frac{m}{\binom{n}{2}}\right|^2 = O\left(\max\left\{\rho, \tfrac{\log n}{n}\right\} \cdot \frac{\log n}{n^3\varepsilon^2}\right).$$

**Theorem IV.3** (The Erdos-Renyi case)**.** *If $\varepsilon \in (0, 1)$ with $\varepsilon n/\log n \to +\infty$, then*

$$R(\rho, \varepsilon, n) = O\left(\frac{\rho}{n^2} + \max\{\rho, \frac{\log n}{n}\}\frac{\log n}{n^3\varepsilon^2}\right).$$

### *B. Lower bounds for $G(n, m)$*

In this subsection we dicuss the complementary question of lower bounds for the edge density estimation question in random graphs. We establish that when $\varepsilon$ in constant and the graph is generated by the uniform model $G(n, m)$, the bound implied by Proposition IV.2 is tight.

We establish this by first proving the following proposition on coupling of $G(n, m)$ models with varying $m$ which could be of independent interest.

**Proposition IV.4.** *Let $n$ be sufficiently large, and $k$ an arbitrary function of $n$ which is $o(\sqrt{n})$. Let $m = \frac{1}{2}\binom{n}{2} - \frac{k}{2}$ Let $P = G(n, m)$ and $Q = G(n, m + k)$. There exists a coupling of $(G, H)$ of $P$ and $Q$ such that, with probability tending to one, one can obtain $G$ from $H$ by rewiring one vertex.*

Using the proposition we establish the following lower bound.

**Theorem IV.5.** *Let $\varepsilon > 0$ be a constant positive number, $n \in \mathbb{N}$, $m = \frac{1}{2}\binom{n}{2} - \frac{k}{2}$ and $k$ an arbitrary function of $n$ which is $o(\sqrt{n})$ . Then there exists a $\beta = \beta(\varepsilon) \in (0,1)$ such that no $\varepsilon$-node DP private algorithm can distinguish $G(n,m)$ from $G(n,m+k)$ with probability bigger than $\beta(\varepsilon) > 0$. In particular, the upper bound of Proposition IV.2 is tight up-to-logarithmic terms for constant $\varepsilon$ and $\rho$.*

## V. A General Extension Technique

In this section we describe the general extension technique which allowed us to conclude the upper bound in Theorem IV.3. Since the technique applies generally to the extension of any $\varepsilon$-differentially private algorithm from any input metric space to any output measurable space, we present it here for the following general model.

*The Model:* Let $n \in \mathbb{N}$ and $\varepsilon > 0$. We assume that the analyst's objective is to estimate a certain quantity which takes values in some measurable space $(\Omega, \mathcal{F})$ from input data which take values in a metric space $(\mathcal{M}, d)$. The analyst is assumed to use for this task a randomized algorithm $\mathcal{A}$ which should be

(1) as highly **accurate** as possible for input data belonging in some *hypothesis set* $\mathcal{H} \subseteq \mathcal{M}$;
(2) $\varepsilon$-**differentially private** on the whole metric space of input data $(M, d)$.

In this section we state the following result. Consider an arbitrary $\varepsilon$-differentially private algorithm defined on input belonging in some set $\mathcal{H} \subset \mathcal{M}$. We show that it **can be always extended** to a $2\varepsilon$-differentially private algorithm defined for arbitrary input data from $\mathcal{M}$ with the property that if the input data belongs in $\mathcal{H}$, the distribution of output values is the same with the original algorithm. We state formally the result.

**Proposition V.1** ("Extending Private Algorithms at $\varepsilon$-cost")**.** *Let $\hat{\mathcal{A}}$ be an $\varepsilon$-differentially private algorithm designed for input from $\mathcal{H} \subseteq \mathcal{M}$. Then there exists a randomized algorithm $\mathcal{A}$ defined on the whole input space $\mathcal{M}$ which is $2\varepsilon$-differentially private and satisfies that for every $D \in \mathcal{H}$, $\mathcal{A}(D) \stackrel{d}{=} \hat{\mathcal{A}}(D)$.*


## Acknowledgments

A.S. was supported by NSF awards IIS-1447700 and AF-1763665, and a Sloan Foundation Research Award. I.Z. would like to thank Microsoft Research New England for providing exciting and hospitable enviroment during his summer internship in 2017 where part of this work was conducted.


## References


[1] E. Abbe and C. Sandon. Recovering communities in the general stochastic block model without knowing the parameters. arXiv:1503.00609, 2015.

[2] E. Abbe, A. S. Bandeira, and G. Hall. Exact recovery in the stochastic block model. arXiv:1405.3267, 2014.

[3] E. M. Airoldi, T. Costa, and S. Chan. A nonparametric perspective on network analysis: Theory and consistent estimation. In *Advances in Neural Information Processing Systems (NIPS)*, volume 26, pages 692–700, 2013.

[4] D. Aldous. Representations for partially exchangeable arrays of random variables. *J. Multivar. Anal.*, 11:581–598, 1981.

[5] P. J. Bickel and A. Chen. A nonparametric view of network models and newman-girvan and other modularities. *Proceedings of the National Academy of Sciences*, 106:21068–21073, 2009.

[6] P. J. Bickel, A. Chen, and E. Levina. The method of moments and degree distributions for network models. *Annals of Statistics*, 39(5):2280–2301, 2011.

[7] J. Blocki, A. Blum, A. Datta, and O. Sheffet. The Johnson-Lindenstrauss transform itself preserves differential privacy. In *Symposium on Foundations of Computer Science (FOCS)*, pages 410–419, 2012. doi: 10.1109/FOCS.2012.67. URL http://dx.doi.org/10.1109/FOCS.2012.67.

[8] J. Blocki, A. Blum, A. Datta, and O. Sheffet. Differentially private data analysis of social networks via restricted sensitivity. In *Innovations in Theoretical Computer Science (ITCS)*, pages 87–96, 2013.

[9] C. Borgs, J. T. Chayes, L. Lovász, V. Sós, and K. Vesztergombi. Counting graph homomorphisms. In *Topics in Discrete Mathematics*, pages 315–371. Springer, 2006.

[10] C. Borgs, J. T. Chayes, L. Lovász, V. Sós, and K. Vesztergombi. Convergent graph sequences I: Subgraph frequencies, metric properties, and testing. *Advances in Math.*, 219:1801–1851, 2008.

[11] C. Borgs, J. T. Chayes, and L. Lovász. Moments of two-variable functions and the uniqueness of graph limits. *Geometric And Functional Analysis*, 19(6):1597–1619, 2010.

[12] C. Borgs, J. T. Chayes, L. Lovász, V. Sós, and K. Vesztergombi. Convergent graph sequences II: Multiway cuts and statistical physics. *Ann. of Math.*, 176:151–219, 2012.

[13] C. Borgs, J. T. Chayes, H. Cohn, and Y. Zhao.

An $L^p$ theory of sparse graph convergence I: limits, sparse random graph models, and power law distributions. *arXiv:1401.2906*, 2014.

[14] C. Borgs, J. T. Chayes, H. Cohn, and Y. Zhao. An $L^p$ theory of sparse graph convergence II: LD convergence, quotients, and right convergence. *arXiv:1408.0744*, 2014.

[15] C. Borgs, J. T. Chayes, and A. D. Smith. Private graphon estimation for sparse graphs. In *Advances in Neural Information Processing Systems (NIPS)*, pages 1369–1377, 2015.

[16] S. H. Chan and E. M. Airoldi. A consistent histogram estimator for exchangeable graph models. *Journal of Machine Learning Research Workshop and Conference Proceedings*, 32:208–216, 2014.

[17] S. Chatterjee. Matrix estimation by universal singular value thresholding. *Annals of Statistics*, 43(1):177–214, 2015.

[18] S. Chen and S. Zhou. Recursive mechanism: towards node differential privacy and unrestricted joins. In *ACM SIGMOD International Conference on Management of Data*, pages 653–664, 2013.

[19] D. S. Choi, P. J. Wolfe, and E. M. Airoldi. Stochastic blockmodels with a growing number of classes. *Biometrika*, 99:273–284, 2012.

[20] J. Dall and M. Christensen. Random geometric graphs. *Physical Review E*, 2002.

[21] W. Day, N. Li, and M. Lyu. Publishing graph degree distribution with node differential privacy. In *International Conference on Management of Data SIGMOD*, pages 123–138, 2016. doi: 10.1145/2882903.2926745. URL http://doi.acm.org/10.1145/2882903.2926745.

[22] P. Diaconis and S. Janson. Graph limits and exchangeable random graphs. *Rendiconti di Matematica*, 28:33—61, 2008.

[23] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography Conference (TCC)*, pages 265–284, 2006.

[24] S. Galhotra, A. Mazumdar, S. Pal, and B. Saha. The geometric block model. In *AAAI*, 2018.

[25] C. Gao, Y. Lu, and H. H. Zhou. Rate-optimal graphon estimation. *arXiv:1410.5837*, 2014.

[26] E. N. Gilbert. Random plane networks. *J. Soc. Indust. Appl. Math.*, (9):533–543, 1961.

[27] A. Gupta, A. Roth, and J. Ullman. Iterative constructions and private data release. In *TCC*, 2012.

[28] M. Hay, C. Li, G. Miklau, and D. Jensen. Accurate estimation of the degree distribution of private networks. In *Int. Conf. Data Mining (ICDM)*, pages 169–178, 2009.

[29] M. Hay, V. Rastogi, G. Miklau, and D. Suciu. Boosting the Accuracy of Differentially Private Histograms Through Consistency. *PVLDB*, 3(1): 1021–1032, 2010.

[30] P. Holland, K. Laskey, and S. Leinhardt. Stochastic blockmodels: First steps. *Soc Netw*, 5:109–137, 1983.

[31] D. Hoover. Relations on probability spaces and arrays of random variables. *Preprint, Institute for Advanced Study, Princeton, NJ*, 1979.

[32] V. Karwa and A. Slavkovic. Inference using noisy degrees: Differentially private $\beta$-model and synthetic graphs. *Ann. Statist.*, 44(1):87–112, 2016.

[33] V. Karwa and A. B. Slavkovic. Differentially private graphical degree sequences and synthetic graphs. In *Privacy in Statistical Databases*, pages 273–285, 2012.

[34] V. Karwa, S. Raskhodnikova, A. D. Smith, and G. Yaroslavtsev. Private analysis of graph structure. *ACM Trans. Database Syst.*, 39(3):22:1–22:33, 2014.

[35] V. Karwa, A. B. Slavkovic, and P. N. Krivitsky. Differentially private exponential random graphs. In *Privacy in Statistical Databases (PSD)*, pages 143–155, 2014. doi: 10.1007/978-3-319-11257-2_12.

[36] S. P. Kasiviswanathan, K. Nissim, S. Raskhodnikova, and A. Smith. Analyzing graphs with node-differential privacy. In *Theory of Cryptography Conference (TCC)*, pages 457–476, 2013.

[37] O. Klopp, A. B. Tsybakov, and N. Verzelen. Oracle inequalities for network models and sparse graphon estimation. *Annals of Statistics Statistics*, 45(1):316–354, 2017. doi: 10.1214/16-AOS1454.

[38] A. Korolova. Privacy violations using microtargeted ads: A case study. In *IEEE International Conference on Data Mining Workshops*, pages 474–482, 2010. doi: 10.1109/ICDMW.2010.137.

[39] P. Latouche and S. Robin. Bayesian model averaging of stochastic block models to estimate the graphon function and motif frequencies in a w-graph model. *ArXiv:1310.6150*, 2013.

[40] B.-R. Lin and D. Kifer. Information preservation in statistical privacy and Bayesian estimation of unattributed histograms. In *ACM SIGMOD International Conference on Management of Data*, pages 677–688, 2013.

[41] J. R. Lloyd, P. Orbanz, Z. Ghahramani, and D. M. Roy. Random function priors for exchangeable

arrays with applications to graphs and relational data. In *Advances in Neural Information Processing Systems (NIPS)*, volume 25, pages 1007–1015, 2012.

[42] L. Lovász and B. Szegedy. Limits of dense graph sequences. *Journal of Combinatorial Theory, Series B*, 96:933–957, 2006.

[43] W. Lu and G. Miklau. Exponential random graph estimation under differential privacy. In *20th ACM SIGKDD International Conference on Knowledge discovery and data mining*, pages 921–930, 2014.

[44] A. McMillan and A. Smith. When is nontrivial estimation possible for graphons and stochastic block models? *Information and Inference: A Journal of the IMA*, 2017.

[45] D. J. Mir and R. N. Wright. A differentially private estimator for the stochastic kronecker graph model. In *EDBT/ICDT Workshops*, pages 167–176, 2012.

[46] A. Narayanan and V. Shmatikov. De-anonymizing social networks. In *IEEE Symp. Security and Privacy*, pages 173–187, 2009.

[47] K. Nissim, S. Raskhodnikova, and A. Smith. Smooth sensitivity and sampling in private data analysis. In *Symp. Theory of Computing (STOC)*, pages 75–84, 2007.

[48] M. D. Penrose. *Random geometric graphs*. Oxford University Press, 2003.

[49] S. Raskhodnikova and A. D. Smith. Lipschitz extensions for node-private graph statistics and the generalized exponential mechanism. In *Symposium on Foundations of Computer Science (FOCS)*, pages 495–504, 2016. doi: 10.1109/FOCS.2016.60.

[50] V. Rastogi, M. Hay, G. Miklau, and D. Suciu. Relationship privacy: output perturbation for queries with joins. In *Symp. Principles of Database Systems (PODS)*, pages 107–116, 2009.

[51] K. Rohe, S. Chatterjee, and B. Yu. Spectral clustering and the high-dimensional stochastic blockmodel. *Ann. Statist.*, 39(4):1878–1915, 08 2011.

[52] M. Tang, D. L. Sussman, and C. E. Priebe. Universally consistent vertex classification for latent positions graphs. *Annals of Statistics*, 41(3):1406–1430, 06 2013. doi: 10.1214/13-AOS1112.

[53] P. Wolfe and S. C. Olhede. Nonparametric graphon estimation. *arXiv:1309.5936*, 2013.

[54] Q. Xiao, R. Chen, and K. Tan. Differentially private network data release via structural inference. In *The 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), New York, NY, USA*, pages 911–920, 2014.

[55] J. J. Yang, Q. Han, and E. M. Airoldi. Nonparametric estimation and testing of exchangeable graph models. In *Proceedings of 17th AISTATS (JMLR: W&CP volume 33)*, 2014.