Hardness of FO Model-Checking on Random Graphs

Jan Dreier
Department of Computer Science, RWTH Aachen University, Germany
https://tcs.rwth-aachen.de/~dreier
dreier@cs.rwth-aachen.de

Peter Rossmanith
Department of Computer Science, RWTH Aachen University, Germany
https://tcs.rwth-aachen.de
rossmani@cs.rwth-aachen.de

Abstract

It is known that FO model-checking is fixed-parameter tractable on Erdős–Rényi graphs $G(n, p(n))$ if the edge-probability $p(n)$ is sufficiently small [23] ($p(n) = O(n^\epsilon/n)$ for every $\epsilon > 0$). A natural question to ask is whether this result can be extended to bigger probabilities. We show that for Erdős–Rényi graphs *with vertex colors* the above stated upper bound by Grohe is the best possible.

More specifically, we show that there is no FO model-checking algorithm with average FPT run time on vertex-colored Erdős–Rényi graphs $G(n, n^\delta/n)$ $(0 < \delta < 1)$ unless $\mathrm{AW}[*] \subseteq \mathrm{FPT/poly}$. This might be the first result where parameterized average-case intractability of a natural problem with a natural probability distribution is linked to worst-case complexity assumptions.

We further provide hardness results for FO model-checking on other random graph models, including $G(n, 1/2)$ and Chung-Lu graphs, where our intractability results tightly match known tractability results [13]. We also provide lower bounds on the size of shallow clique minors in certain Erdős–Rényi and Chung–Lu graphs.

2012 ACM Subject Classification Theory of computation → Parameterized complexity and exact algorithms

Keywords and phrases random graphs, FO model-checking

Digital Object Identifier 10.4230/LIPIcs.IPEC.2019.11

1 Introduction

Model-checking is an important and well-investigated problem with various applications in database theory, verification, artificial intelligence and many other areas. The input to the model-checking problem is a structure and a logical sentence and the question is whether the structure is a model for the sentence, i.e., if the sentence is true in the model. We consider the FO model-checking problem on colored graphs. This means that sentences can express (besides the common rules of first-order logic) adjacency between vertices and whether a vertex has a given color. This problem is known to be PSPACE-complete [39]. Let $\mathcal{G}$ be a graph class and L be a logic. We are interested in model-checking as a parameterized problem, which is defined as follows:

p-MC$(L, \mathcal{G})$	
Input:	A graph $G \in \mathcal{G}$ and a logical sentence $\varphi \in L$
Parameter:	$\lvert\varphi\rvert$
Problem:	$G \models \varphi$?

We denote the class of all graphs by $\mathfrak{G}$. Downey, Fellows, and Taylor showed that p-MC(FO, $\mathfrak{G}$) is AW[$*$]-complete and thus very hard on general graphs [15]. However, model-checking becomes tractable when restricted to special graph classes. Courcelle's theorem states that if $\mathcal{G}$ is a graph class with bounded treewidth then p-MC(MSO, $\mathcal{G}$) is in FPT [11]. The FO model-checking problem p-MC(FO, $\mathcal{G}$) can be solved in FPT time if $\mathcal{G}$ has bounded expansion [17, 38] or is nowhere-dense [25].

For a graph class $\mathcal{G}$, we define $\mathcal{G}_{col}$ to be the class of all vertex colorings of $\mathcal{G}$. For most graph classes $\mathcal{G}$ it makes no difference if we consider the model-checking problem on $\mathcal{G}$ or $\mathcal{G}_{col}$ because colors can be encoded by small gadgets. Given an instance (G, φ) with $G \in \mathcal{G}_{col}$, for most graph classes $\mathcal{G}$ it is easy to construct a new instance (G', φ') of similar size with $G' \in \mathcal{G}$, and $G \models \varphi$ iff $G' \models \varphi'$. In particular, if G comes from a nowhere-dense class, then so does G'.

Average-Case Model-Checking

Average-case complexity analyzes the typical run time of algorithms on random instances (such as random graphs) and is a well-established field of complexity theory [3]. While the worst-case complexity of the parameterized model-checking problem is well analyzed, much less is known about its average-case complexity, or parameterized average-case complexity in general.

We fix a sequence of vertices $(u_i)_{i\in\mathbf{N}}$ and say a *random graph model* is a sequence $\mathcal{G} = (\mathcal{G}_n)_{n\in\mathbf{N}}$, where $\mathcal{G}_n$ is a probability distribution over all graphs G with $V(G) = \{u_1, \dots, u_n\}$. The most well-known random graph model are so called Erdős–Rényi graphs [6]. The Erdős–Rényi graph $G(n, p(n))$ consists of n vertices where each edge is added independently with probability $p(n)$. This very natural model is of great theoretical interest and has been investigated in many ways. Other models such as the preferential attachment model [2, 5], the Chung–Lu model [10, 9, 7], or the configuration model [32, 33] were defined to mimic complex networks that are observed in the real world.

There exist some tractability results for the model-checking problem on random graph models, including sparse Erdős–Rényi graphs, Chung–Lu graphs and the configuration model, as we will see later on. We distinguish between the average-case complexity of model-checking on uncolored graphs (p-MC(FO, $\mathfrak{G}$)) and colored graphs (p-MC(FO, $\mathfrak{G}_{col}$)):

▶ **Definition 1.** We say p-MC(FO, $\mathfrak{G}$) can be decided on a random graph model $\mathcal{G}$ in *expected time* $f(|\varphi|, n)$ if there exists a deterministic algorithm $\mathcal{A}$ which decides p-MC(FO, $\mathfrak{G}$) on input G, φ in time $t_{\mathcal{A}}(G, \varphi)$ and for all $n \in \mathbf{N}$, all FO-sentences φ, $\mathrm{E}_{G\sim\mathcal{G}_n}\left[t_{\mathcal{A}}(G, \varphi)\right] \leq f(|\varphi|, n)$.

A function $C : \mathfrak{G} \to \mathfrak{G}_{col}$ is called a *c-coloring function* for $c \in \mathbf{N}$ if for every $G \in \mathfrak{G}$, $C(G)$ is a coloring of G with up to c colors. The colorings do not need to be proper.

▶ **Definition 2.** We say p-MC(FO, $\mathfrak{G}_{col}$) can be decided on a random graph model $\mathcal{G}$ in *expected time* $f(|\varphi|, n)$ if there exists a deterministic algorithm $\mathcal{A}$ which decides p-MC(FO, $\mathfrak{G}_{col}$) on input G, φ in time $t_{\mathcal{A}}(G, \varphi)$ and if for all $n \in \mathbf{N}$, all FO-sentences φ and all $|\varphi|$-coloring functions C, $\mathrm{E}_{G\sim\mathcal{G}_n}\left[t_{\mathcal{A}}(C(G), \varphi)\right] \leq f(|\varphi|, n)$.

We say p-MC(FO, $\mathfrak{G}_{col}$) or p-MC(FO, $\mathfrak{G}$) can be decided in *expected FPT time* on a random graph model if it can be decided in expected time $f(|\varphi|)n^{O(1)}$ for some function f. Clearly, p-MC(FO, $\mathfrak{G}_{col}$) is harder than p-MC(FO, $\mathfrak{G}$) on random graph models because the model-checking algorithm has to be efficient for every possible coloring. However, all efficient average-case model-checking algorithms so far work by placing the random graph model

with high probability in a tractable graph class (for example low degree [23], or bounded expansion [13]) and then using well-known model-checking algorithms for such graph classes. Thus, the algorithms work no matter how the vertices of the random graphs are colored.

The following tractability results are known: Let $p(n)$ be a function with $p(n) = O(n^\varepsilon/n)$ for all $\varepsilon > 0$. Grohe showed that one can solve p-MC(FO, $\mathfrak{G}_{col}$) on $G(n, p(n))$ in expected time $f(|\varphi|, \delta)n^{1+\delta}$ for every $\delta > 0$ [23]. Later Demaine et al. proved that p-MC(FO, $\mathfrak{G}_{col}$) can be solved in expected FPT linear time on Chung–Lu and configuration graphs whose degrees follow a power law distribution with exponent $\alpha > 3$ and maximal degree at most $n^{1/\alpha}$ [13].

Average-Case Intractability

A natural question to ask next is: For which graphs does model-checking become intractable? For the worst-case complexity of monotone graph classes (classes which are closed under subgraphs) this question is settled: FO model-checking is in FPT if and only if the graph class is nowhere-dense [25]. For non-monotone classes and especially random graph models the question is more difficult.

Ideally, positive algorithmic results should be accompanied by lower bounds that show that the result is the best possible. Very often such matching lower bounds are the triumphant last step in completely answering a question that has had a long history of incremental partial results. The best example is the theory of NP-completeness, but there are many other nice examples from parameterized complexity: ETH-based lower bounds, non-existence of polynomial kernels, and in the area of FO model-checking the fact that p-MC(FO, $\mathcal{G}$) $\in$ FPT for some monotone somewhere-dense graph class $\mathcal{G}$ implies AW[$*$] = FPT.

On the other hand, the situation does not look as good in the area of average-case complexity. While we know that FO model-checking on $G(n, d/n)$ can be decided in expected FPT time if d is constant or grows slower than n^ϵ for every $\epsilon > 0$, we do not have any lower bounds for a larger d.

The lack of lower bounds of average-case runtimes is not restricted to random graphs and the model-checking problem. At this point of time we still do not know techniques to prove good lower bounds in that area. While it is certainly possible to reduce between problems preserving bounds on the expected running time, there are virtually no results linking average- to worst-case complexity. What we are missing in particular are results of this kind: If we can solve parameterized problem X fast on average then some unexpected consequence holds in the world of worst-case complexity (such as P = NP).

There has been some work on average-case complexity of parameterized problems. Fountoulakis, Friedrich, and Hermelin showed that parameterized clique can be decided efficiently on Erdős–Rényi graphs with arbitrary density [18] and Friedrich and Krohmer proved the same result for certain scale free random graphs where the degree sequence follows a power law with exponent $\alpha > 2$ [19]. However, there exist some artificial, computable distributions for which the problem is distW[1]-complete [18], where distW[1] is an average-complexity class, which is assumed to be hard. This means that parameterized clique cannot be decided efficiently on average on that distribution unless every problem in distW[1] can be decided efficiently on average. This promising result identifies distW[1] as a possible corner stone for an average-case parameterized complexity theory. There is, however, no link between average-case and worst-case complexity and no lower bounds for more natural probability distributions.

Hardness results on less artificial distributions are known if one considers counting problems instead of decision problems. Müller presented a counting problem on matrices that is hard on average on certain uniform distributions unless W[1] $\subseteq$ paraNP-BPFPT [35], thereby linking parameterized average-case complexity and classical parameterized complexity.

Our main result is a lower bound for FO model-checking on certain vertex-colored random graph models, in particular certain Erdős–Rényi and Chung–Lu graphs. If for every coloring function we can solve FO model-checking on such a random graph in expected FPT time, then AW[$*$] $\subseteq$ FPT/poly, which is quite unexpected because i.a. every level of the W-hierarchy is contained in AW[$*$]. While the hardness results hold for many random graph models (see Theorem 14) the following theorem shows three examples:

▶ **Theorem 3.** *If* p-MC(FO, $\mathfrak{G}_{col}$) *can be decided in expected* FPT *time on any of the following random graph models, then* AW[$*$] $\subseteq$ FPT/poly*:*

- $G(n, 1/2)$*,*
- $G(n, p(n))$ *with* $p(n) = n^\delta/n$ *for some* $0 < \delta < 1$*,* $\delta \in \mathbf{Q}$*,*
- *Chung–Lu graphs with exponent* $2.5 \leq \alpha < 3$*,* $\alpha \in \mathbf{Q}$*.*

This might be the first result where parameterized average-case hardness of a natural problem with a natural probability distribution is linked to classical complexity assumptions. For a more complete list of hard random graph models see Section 3.3. Our intractability results tightly match known tractability results:

▶ **Corollary 4.** *Assume that* AW[$*$] $\not\subseteq$ FPT/poly *and let* $p\colon \mathbf{N} \to [0, \frac{1}{2}]$ *be monotone and computable in polynomial time. Then* p-MC(FO, $\mathfrak{G}_{col}$) *can be decided on Erdős–Rényi graphs* $G(n, p(n))$ *in expected* FPT *time if and only if* $p(n) = O(n^\varepsilon/n)$ *for every* $\varepsilon > 0$*.*

In Theorem 3 and Corollary 4 we mention expected FPT time which is not closed under invoking polynomial subroutines. Our hardness results also hold for more permissive measures of parameterized tractability, similar to *average polynomial run time* [31], as introduced by Levin (see Theorem 8 and 9).

The drawback of this result is the usage of colored graphs, which turns out to be instrumental in the proof and it seems that colorings introduce a bit of worst-case behavior into the otherwise random sampling of a graph. In the past every positive result about model-checking on graphs worked for colored and uncolored graphs alike, but it is not clear whether something similar is true in the world of average-case complexity. The big open question that remains is whether we can prove a similar lower bound on uncolored random graphs and this paper is merely trying to contribute in the building of tools to reach this goal. A next step could be to show lower bounds under more restricted colorings.

There are examples for other lower bounds, which were shown first on colored graphs. One example is Kreutzer's proof that a graph class whose tree-width is not bounded, but grows at least moderately, has no efficient MSO model-checking algorithm. One of the conditions on the graph class was closure under colorings [29]. This lower bound complements Courcelle's theorem [11], which states that MSO model-checking can be done in linear time on graph classes with bounded tree-width (with or without colors). Later Kreutzer and Tazari could replace closure under colorings by closure under subgraphs, which is less restrictive [30]. Ganian et al. reintroduced closure under (vertex-)colorings to prove a similar result for MSO_1 model-checking [22]. These examples show that lower bounds are sometimes easier to prove in the presence of colorings.

Structural Sparsity and Average-Case Model-Checking

For monotone graph classes, model-checking is tractable if the graph class is nowhere-dense and intractable if it is somewhere-dense [25]. For random graph models, even for sparse random graph models, the situation is more complicated. We say a random graph model $\mathcal{G}$ is *asymptotically almost surely (a.a.s.) somewhere-dense* if there exists a somewhere-dense

graph class $\mathcal{H}$ such that for $n \to \infty$, a graph sampled from $\mathcal{G}_n$ belongs with probability one to $\mathcal{H}$. We similarly define *a.a.s. nowhere-dense*. Erdős–Rényi graphs, Chung–Lu graphs, the configuration model, and preferential attachment graphs have been classified with respect to a.a.s. somewhere- and nowhere-density [36, 13]. However, it is important to note that *a.a.s. somewhere-density is neither necessary nor sufficient for intractability*:

- There exist a.a.s. somewhere-dense random graph models for which p-MC(FO, $\mathfrak{G}_{col}$) is fixed parameter tractable.
- There exist a.a.s. nowhere-dense random graph models for which p-MC(FO, $\mathfrak{G}$) is not fixed parameter tractable (under some assumptions).

We state why: On the one hand, there exist trivial dense random graph models for which p-MC(FO, $\mathfrak{G}_{col}$) is tractable, such as the complete graph. In an upcoming work, we want to show that p-MC(FO, $\mathfrak{G}_{col}$) even is decidable on the a.a.s. somewhere-dense preferential attachment model in expected FPT time. On the other hand, Fountoulakis, Friedrich, and Hermelin showed that under the hypothesis distW[1] $\not\subseteq$ avgFPT $\cup$ typFPT there exists a random graph model $\mathcal{H}$ for which the parameterized clique problem is not tractable [18]. We construct a random graph model $\mathcal{G}$ as follows: With probability $1/\log(n)$, $\mathcal{G}_n$ is distributed according to $\mathcal{H}_n$ and with probability $1 - 1/\log(n)$, $\mathcal{G}_n$ is an independent set of size n. Now $\mathcal{G}$ is a.a.s. sparse. If p-MC(FO, $\mathfrak{G}$) could be solved on $\mathcal{G}$ in expected FPT time then it could also be solved on $\mathcal{H}$ in expected FPT time, which contradicts our hypothesis.

Connections to Shallow Topological Clique Minors

A byproduct of our work is a polynomial lower bound on the size of subdivided cliques in sufficiently dense random graphs, and polynomial time algorithms to find them. Let $\varepsilon > 0$. Dvořák [16] and Jiang [26] showed independently (using a slightly different formulation) that there exists a sequence $(\ell_{n,\varepsilon})_{n\in\mathbf{N}}$ with $\lim_{n\to\infty} \ell_{n,\varepsilon} = \infty$ and an integer c_ε such that every graph G with n vertices and at least $n^{1+\varepsilon}$ edges contains a c_ε-subdivision of a clique of size $\ell_{n,\varepsilon}$. Jiang further showed that one can choose $c_\varepsilon = 10/\varepsilon$. Both authors did not give a lower bound on $\ell_{n,\varepsilon}$.

A simple application of Chernoff bounds together with this result yields that $G(n, n^\varepsilon/n)$ contains a.a.s. a $c_{\varepsilon/2}$-subdivided clique of size $\ell_{n,\varepsilon/2}$ with $\lim_{n\to\infty} \ell_{n,\varepsilon} = \infty$. To obtain good lower bounds for the model-checking problem we need the clique size $\ell_{n,\varepsilon}$ to be polynomial in n. Therefore we show that $G(n, n^\varepsilon/n)$ contains a.a.s. a $6/\varepsilon$-subdivided clique of size $n^{\varepsilon/5}$ (Lemma 15). We also show that the Chung–Lu random graph model with exponent $2.5 \le \alpha < 3$ contains a.a.s. a one-subdivided clique of polynomial size (Lemma 18). We further show that these shallow clique minors can be found in polynomial time.

It is left as an open question whether $l_{n,\varepsilon}$ grows polynomially in n for general graphs. If affirmative then the result is probably not easy to prove: Kostochka and Pyber showed that a graph with n vertices and at least $4^{t^2} n^{1+\varepsilon}$ edges contains a subdivision of K_t with at most $7t^2 \ln(t)/\varepsilon$ (principal and non-principal) vertices [28]. Even with such weaker requirements the bound on t is smaller than $\log n$ and leaves an exponential gap to be filled.

Our Techniques

We use colorings and so called *FO-interpretations* on random graphs. An FO-interpretation a translates a graph G into another graph G' with the help of an FO-formula $\psi(x, y)$: The graph G' contains an edge (x, y) iff $G \models \psi(x, y)$. FO-interpretations are a standard tool in logic and have lately been used in the context of model-checking (for example [20, 21]).

We use FO-interpretations to establish a reduction framework. Let X and Y be two random graph models. We say Y *polynomially FO-interprets to* X ($X \preccurlyeq Y$) if an interpretation of a coloring of a graph G is nearly distributed like X assuming that G is distributed like Y (Definition 11). We further say that X *polynomially FO-interprets to* $\mathfrak{G}$ ($\mathfrak{G} \preccurlyeq X$) if an arbitrary graph $H \in \mathfrak{G}$ can be encoded into X using colorings and interpretations (Definition 7). In both cases, we require the interpretations to change the size of the graph at most polynomially. We show that p-MC(FO, $\mathfrak{G}_{col}$) is not tractable on any random graph model X with $\mathfrak{G} \preccurlyeq X$ (Theorem 9) and that $\preccurlyeq$ propagates hardness (Lemma 12, 13), yielding a way to prove intractability of p-MC(FO, $\mathfrak{G}_{col}$) on random graphs by means of reductions.

Let $\mathcal{G}$ be a random graph model with $\mathfrak{G} \preccurlyeq \mathcal{G}$. Let H be a graph and φ an FO-sentence. We sample a graph G from $\mathcal{G}_n$ for some $n = |H|^{O(1)}$ and use colorings and FO-interpretations to encode H with sufficiently high probability into G. Then one can solve the model-checking problem on H by solving it on the coloring of G instead. If p-MC(FO, $\mathfrak{G}_{col}$) can be decided on $\mathcal{G}$ in expected FPT time then one can also solve the model-checking problem on *every graph* H in expected FPT time. The result is a link between worst-case and average-case complexity.

2 Preliminaries

2.1 Graph Notation

We use common graph theory notation [14]. In this work we obtain results for undirected *colored graphs* [24]. A colored graph is a tuple $G = (V(G), E(G), C_1(G), \dots, C_l(G))$ with $C_i \subseteq V(G)$. We call $C_1(G), \dots, C_l(G)$ the *colors* of G. Vertices may have multiple colors. We say a vertex v is colored with color C_i if $v \in C_i$. All notion for graphs extends to colored graphs as expected. We define $\mathfrak{G}$ to be the class of all graphs and $\mathfrak{G}_{col}$ to be the class of all colored graphs. A *coloring* of an uncolored graph G is a colored graph G' with $(V(G'), E(G')) = G$. We define the *order* of a graph G to be $|G| = |V(G)|$.

A *r-subdivision*[1] of a graph H is a graph H' obtained by replacing edges with disjoint paths of length at least 2 and at most $r+1$. The *principal vertices* of H' are those vertices which are in H. We say a graph G contains an *r-subdivided induced clique* of size k if an r-subdivision of K_k is an induced subgraph of G. We say a graph G contains an *one-subdivided half-induced clique* of size k if there exist k vertices $v_1, \dots, v_k \subseteq V(G)$ such that for every $1 \leq i < j \leq k$ there exists a vertex $w_{i,j} \in V(G)$ with $N(w_{i,j}) \cap \{v_1, \dots, v_k\} = \{v_i, v_j\}$. We call $v_1, \dots, v_k$ the *principal vertices* and $w_{i,j}$ the *bridge* between v_i and v_j.

2.2 Probabilities and Random Graph Models

We denote probabilities by $\Pr[*]$ and expectation by $\mathrm{E}[*]$. We consider a random graph model to be a sequence of probability distributions. A random graph model describes for every $n \in \mathbf{N}$ a probability distribution on graphs with n vertices. In order to speak of probability distributions over graphs we fix a sequence of vertices $(u_i)_{i \geq 1}$ and require that a graph with n vertices has the vertex set $\{u_1, \dots, u_n\}$. A random graph model is a sequence $\mathcal{G} = (\mathcal{G}_n)_{n \in \mathbf{N}}$, where $\mathcal{G}_n$ is a probability distribution over all graphs G with $V(G) = \{u_1, \dots, u_n\}$. We write $G \sim \mathcal{G}_n$ if a graph G is is distributed as $\mathcal{G}_n$. In slight abuse of notation, we sometimes treat a probability distribution $\mathcal{G}_n$ as a random variable itself. For example the random variable $E(\mathcal{G}_n)$ stands for $E(G)$ with $G \sim \mathcal{G}_n$. We say a property of a random graph model holds *a.a.s.* if the probability that the property holds in $\mathcal{G}_n$ converges to one for $n \to \infty$.

[1] Usually, in an r-subdivision paths have length exactly $r+1$ but this definition is more convenient for us.

Erdős–Rényi graphs [6] with edge probability $p(n)$ are denoted by $G(n, p(n))$. The Chung–Lu model [10, 9, 7] has been proposed to generate random graphs that fit a certain degree sequence. For a given $n \in \mathbf{N}$ let $W_n = (w_1, \dots, w_n)$ be a sequence of weights. The Chung–Lu random graph to W_n is a random graph $\mathcal{G}_n$ with $V(\mathcal{G}_n) = \{u_1, \dots, u_n\}$ such that each edge $u_i u_j$ with $1 \leq i, j \leq n$ occurs in $\mathcal{G}_n$ independently with probability $w_i w_j / \sum_{k=1}^{n} w_k$. Let $\alpha > 2$. We say $\mathcal{G}$ is the *Chung–Lu random graph model with exponent* α if for every $n \in \mathbf{N}$, $\mathcal{G}_n$ is the Chung–Lu random graph to $W_n = \{w_1, \dots, w_n\}$ with $w_i = c \cdot (n/i)^{1/(\alpha-1)}$ where c is a constant depending on α.

We say a random graph model $\mathcal{G}$ is *expected polynomial time samplable* if there exists a randomized algorithm which runs on input $n \in \mathbf{N}$ in expected time polynomial in n and creates an output which is distributed like $\mathcal{G}_n$. This excludes for example Erdős–Rényi graphs where $p(n)$ is not computable.

2.3 First-Order Logic

We consider only first-order logic over colored graphs. We interpret a colored graph $G = (V, E, C_1, \dots, C_l)$, as a structure over the universe V with signate $(E, C_1, \dots, C_l)$. The binary relation E expresses adjacency between vertices and the unary relations $C_1, \dots, C_l$ indicate the colors of the vertices. Other structures can be easily converted into colored graphs. We write $\varphi(x_1, \dots, x_k)$ to indicate that a formula φ has *free variables* $x_1, \dots, x_k$. Furthermore, $|\varphi|$ is the number of symbols in φ.

An FO interpretation is a pair $I = (\nu(x), \psi(x, y))$ of FO formulas (with one and two free variables, respectively). For a colored graph G, this defines an uncolored graph $I(G)$ with $V(I(G)) = \{v \mid G \models \nu(v)\}$, $E(I(G)) = \{uv \mid G \models \psi(u, v)\}$. For an FO sentence φ, the interpretation I defines an FO sentence φ^I as follows: Every occurrence of $E(x, y)$ is replaced with $\psi(x, y) \vee \psi(y, x)$. Every occurrence of $\exists x \psi$ is replaced with $\exists x \nu(x) \wedge \psi$ and every occurrence of $\forall x \psi$ is replaced with $\forall x \nu(x) \to \psi$. Then $G \models \varphi^I \iff I(G) \models \varphi$.

2.4 Parameterized Complexity

The classes paraNP-BPFPT and FPT/poly are parameterized analogues of BPP and P/poly.

▶ **Definition 5.** [34] paraNP-BPFPT is the class of parameterized problems that can be decided by a randomized Turing machine with two-sided error $1/n$ (where n is the size of the input). The run time of the Turing machine on every input of size n and parameter k needs to be at most $f(k)n^{O(1)}$ for some computable function f.

▶ **Definition 6.** [12] FPT/poly is the class of all parameterized problems Q for which there exists a parameterized problem $Q' \in \text{FPT}$ and a constant c such that for each $(n, k) \in \mathbf{N} \times \mathbf{N}$ there exists some $\alpha(n, k) \in \Sigma^*$ of size n^c, with the property that for all instances $\langle x, k \rangle$ with $|x| = n$, it holds that $\langle x, k \rangle \in Q$ if and only if $\langle (x, \alpha(|x|, k)), k \rangle \in Q'$.

The complexity class AW[$*$] can be defined as the class of all parameterized problems that can be reduced to p-MC(FO, $\mathfrak{G}$) by fpt-reductions and contains the whole W-hierarchy. In summary

$$\text{FPT} \subseteq \text{W[1]} \subseteq \text{W[2]} \subseteq \text{W[3]} \subseteq \cdots \subseteq \text{AW[}*\text{]} \subseteq \text{XP},$$

$$\text{paraNP-BPFPT} = \text{FPT} \iff \text{BPP} = \text{P} \text{ (see [35])}.$$

It is widely believed that BPP = P.

3 Results

3.1 Hardness

In this section we define a property of random graph models (denoted by $\mathfrak{G} \preccurlyeq \mathcal{G}$, see Definition 7) and then show that p-MC(FO, $\mathfrak{G}_{col}$) is not tractable on average on random graph models with this property. We base our results either on the assumption AW[$*$] $\not\subseteq$ FPT/poly or on AW[$*$] $\not\subseteq$ paraNP-BPFPT. As discussed in Section 2.4, these are well-funded assumptions of parameterized worst-case complexity. In the following definition we characterize those random graph models which have enough structure such that an arbitrary graph can with high probability be embedded using FO-interpretations and colorings.

▶ **Definition 7.** Let $\mathcal{G}$ be a random graph model. We say $\mathcal{G}$ *polynomially FO-interprets to* $\mathfrak{G}$ *(short:* $\mathfrak{G} \preccurlyeq \mathcal{G}$*)* if $\mathcal{G}$ is expected polynomial time samplable and there exists an FO interpretation I, a polynomial p, a constant c and a randomized algorithm B which gets as input $G, H \in \mathfrak{G}$ with $|G| = p(|H|)$ and runs in polynomial time in $|H|$. Either the algorithm fails and $B(G,H)$ is a special failure symbol $\perp$ or $B(G,H)$ is a coloring of G with $I(B(G,H)) = H$. Furthermore for every H, $\Pr(B(\mathcal{G}_{p(|H|)}, H) \neq \perp) \geq 1/|H|^c$.

Our notion of tractability (as used in the following two theorems) is similar to the well-known notion of *average polynomial time* (for example [3, Definition 3]): Let $\mathcal{D} = \{\mathcal{D}_n\}_{n\in\mathbf{N}}$ be a sequence of distributions. A deterministic algorithm with run time $t(x)$ on input x runs in average polynomial time on $\mathcal{D}$ if there exists an $\varepsilon > 0$ and a polynomial p such that for every n and t, $\Pr_{x\sim\mathcal{D}_n}[t(x) \geq t] \leq p(n)/t^\varepsilon$. Average polynomial time is closed under polynomial subroutines and implies polynomial expected time. We show that if one can solve the model-checking problem *with adversary colorings* efficiently then AW[$*$] $\subseteq$ paraNP-BPFPT.

▶ **Theorem 8.** *Let $\mathcal{G}$ be a random graph model with $\mathfrak{G} \preccurlyeq \mathcal{G}$. If there exists a function f, a polynomial p, an $\varepsilon > 0$ and a deterministic algorithm $\mathcal{A}$ which decides p-MC(FO, $\mathfrak{G}_{col}$) on input G, φ in time $t_{\mathcal{A}}(G,\varphi)$ such that for all $n, t \in \mathbf{N}$, all FO-sentences φ and all $|\varphi|$-coloring functions C it holds that*

$$\Pr\big[t_{\mathcal{A}}\big(C(\mathcal{G}_n), \varphi\big) \geq t\big] \leq f(|\varphi|)p(n)/t^\varepsilon,$$

then AW[$*$] $\subseteq$ paraNP-BPFPT. *Moreover, then there exists a randomized algorithm which gets as input a graph $H \in \mathfrak{G}$ and a FO-sentence φ and returns whether $G \models \varphi$ or $\perp$, whereas $\perp$ is returned with probability at most $1/2$. The algorithm always runs in time $g(|\varphi|)|H|^{O(1)}$ for some function g and uses only $|H|^{O(1)}$ random bits.*

Proof. It is known that p-MC(FO, $\mathfrak{G}$) is AW[$*$]-complete [15]. We assume $\mathfrak{G} \preccurlyeq \mathcal{G}$ with interpretation I, polynomial q and algorithm B. Let H be a graph with $|H| = n$ and φ be a FO-sentence. Consider the following procedure: We sample a graph G with $G \sim \mathcal{G}_{q(n)}$. We then compute $B(G,H)$, which is either a coloring of G or $\perp$. If $B(G,H) = \perp$, we return $\perp$. If not then $I(B(G,H)) = H$. This means $H \models \varphi \iff B(G,H) \models \varphi^I$. In this case, we use $\mathcal{A}$ to compute whether $B(G,H) \models \varphi^I$.

Let us analyze this procedure: Since $\Pr(B(\mathcal{G}_{q(n)}, H) \neq \perp) \geq 1/n^c$ for some constant c, the probability that the procedure returns $\perp$ is at most $1 - 1/n^c$. Let C be a $|\varphi^I|$-coloring function such that for every graph $G' \in \mathfrak{G}$, $C(G')$ is a coloring of G' with $|\varphi^I|$ colors maximizing $t_{\mathcal{A}}(C(G'), \varphi^I)$. We can assume that $\mathcal{A}$ immediately returns $\perp$ on a malformed input $\perp$, thus $t_{\mathcal{A}}(B(G,H), \varphi^I) \leq t_{\mathcal{A}}(C(G), \varphi^I)$. Therefore for every $t \in \mathbf{N}$, $\Pr\big[t_{\mathcal{A}}(B(H, \mathcal{G}_{q(n)}), \varphi^I) \geq t\big] \leq \Pr\big[t_{\mathcal{A}}(C(\mathcal{G}_{q(n)}), \varphi^I) \geq t\big]$. Let $g(|\varphi|) = f(|\varphi^I|)^{1/\varepsilon}$. By our

assumption, we have $\Pr\big[t_{\mathcal{A}}(C(\mathcal{G}_{q(n)}), \varphi^I) \geq g(|\varphi|)t\big] \leq p(q(n))/t^\varepsilon$. Thus, for every $t \in \mathbf{N}$, $\mathcal{A}$ does not terminate on $(B(G,H), \varphi^I)$ after $g(|\varphi|)t$ steps with probability at most $p(q(n))/t^\varepsilon$. We choose $t = n^{O(1)}$ such that $p(q(n))/t^\varepsilon \leq 1/4n^c$, run $\mathcal{A}$ for $g(|\varphi^I|)t$ steps, and then abort it. The probability that it was aborted is at most $1/4n^c$. The graph $G \sim \mathcal{G}_{q(n)}$ is sampled in expected polynomial time. We also abort the sampling procedure after $n^{O(1)}$ steps such that the probability that it was aborted is at most $1/4n^c$. In total, the procedure was aborted with probability at most $1/2n^c$ and returns $\perp$ with probability at most $1 - 1/n^c$, leaving a probability of at least $1/2n^c$ to not be aborted and to not return $\perp$. Therefore, we compute whether $H \models \varphi$ with probability at least $1/2n^c$ and always run in FPT time. We repeat this $n^{O(1)}$ times to amplify the probability. Altogether we needed randomness to sample from $\mathcal{G}_n$ and to run B for a polynomial number of steps, which results in the usage of polynomially many random bits. ◀

Adleman's theorem states that BPP $\subseteq$ P/poly [1, Theorem 7.17]. The following proof is very similar to its proof, thus we are brief.

▶ **Theorem 9.** *Let $\mathcal{G}$ be a random graph model with $\mathfrak{G} \preccurlyeq \mathcal{G}$. If there exists a function f, a polynomial p, an $\varepsilon > 0$ and a deterministic algorithm $\mathcal{A}$ which decides p-MC(FO, $\mathfrak{G}_{col}$) on input G, φ in time $t_{\mathcal{A}}(G, \varphi)$ such that for all $n, t \in \mathbf{N}$, all FO-sentences φ and all $|\varphi|$-coloring functions C*

$$\Pr\big[t_{\mathcal{A}}\big(C(\mathcal{G}_n), \varphi\big) \geq t\big] \leq f(|\varphi|)p(n)/t^\varepsilon,$$

then AW[$*$] $\subseteq$ FPT/poly.

Proof. It is known that p-MC(FO, $\mathfrak{G}$) is AW[$*$]-complete [15]. If we assume that the preconditions of this theorem are fulfilled then by Theorem 8 there is a randomized algorithm that can decide for a graph $G \in \mathfrak{G}$ with $|G| = n$ and FO-sentence φ whether $G \models \varphi$ in FPT time with probability at least $1/2$ and that returns $\perp$ otherwise. Moreover, that algorithm uses only $n^{O(1)}$ random bits.

We can run that algorithm n^3 times and the probability that we get at least once the answer to $G \models \varphi$ is then at least $1 - 2^{-n^3}$. There are at most 2^{n^2} graphs with a fixed vertex set of size n. For each of these at most 2^{n^2} possible input graphs G there is a fraction of at most 2^{-n^3} of possible random bit strings that cause the amplified algorithm to fail on G. The total fraction of random bit strings that cause the algorithm to fail on at least one G is then at most $2^{-n^3} \cdot 2^{n^2} < 1$ and there must be at least one choice of random bits that causes the algorithm to give the right answer on every colored graph G of order n. Feeding the randomized algorithm this fixed string of bits instead of using true random bits yields a deterministic FPT algorithm that needs for each n an advice string of polynomial length, which places the problem in FPT/poly. ◀

A simple application of the Markov bound yields the following more compact statement.

▶ **Corollary 10.** *Let $\mathcal{G}$ be a random graph model with $\mathfrak{G} \preccurlyeq \mathcal{G}$. If p-MC(FO, $\mathfrak{G}_{col}$) can be solved on $\mathcal{G}$ in expected* FPT *time then* AW[$*$] $\subseteq$ FPT/poly.

3.2 Reductions

In this section we use colorings and FO-interpretations to define reductions between random graph models (Definition 11) and show that these reductions are transitive and propagate hardness (Lemma 12 and 13). For two random graph models X and Y we say Y *polynomially FO-interprets to* X ($X \preccurlyeq Y$) if an interpretation of a coloring of a graph G is nearly distributed like X, assuming G is distributed like Y. This section is a technical necessity, but contains no surprising results.

▶ **Definition 11.** Let X and Y be random graph models. We say Y *polynomially FO-interprets to* X ($X \preccurlyeq Y$) if Y is expected polynomial time samplable and there exists an interpretation I, a polynomial p, a constant c and a randomized algorithm C which gets as input an uncolored graph G, runs in polynomial time in $|G|$ and returns $C(G)$. Either the algorithm fails and $C(G)$ equals a special failure symbol $\perp$ or $C(G)$ is a coloring of G. Furthermore for every x in the support of X_n, $\Pr_{G\sim Y_{p(n)}}[I(C(G)) = x] \geq \Pr_{G\sim X_n}[G = x]/n^c$.

▶ **Lemma 12.** *Let X and Y be random graph models. If $\mathfrak{G} \preccurlyeq X$ and $X \preccurlyeq Y$ then $\mathfrak{G} \preccurlyeq Y$.*

Proof. Assume $X \preccurlyeq Y$ with algorithm C_1, interpretation I_1, polynomial p_1 and constant c_1. and $\mathfrak{G} \preccurlyeq X$ with algorithm B_2, interpretation I_2, polynomial p_2 and constant c_2. Let I be the interpretation obtained by applying I_1 and then I_2. By Definition 11, Y is expected polynomial time samplable. It is sufficient to construct a randomized algorithm B which gets as input $G, H \in \mathfrak{G}$ with $|G| = p_2(p_1(|H|))$ and $B(G, H)$ is either $\perp$ or a coloring of G with $I(B(G, H)) = H$, and for every $H \in \mathfrak{G}$, $\Pr_{G\sim Y_{p_1(p_2(|H|))}}(B(G, H) \neq \perp) \geq 1/|H|^c$ for some c.

This algorithm proceeds as follows: At first, we compute $C_1(G)$. If $G' = I_1(C_1(G))$ is $\perp$ or no graph of order $p_2(n)$ we return $\perp$. Then we compute $B_2(G', H)$. Again, if $B_2(G', H) = \perp$ we return $\perp$. With at least polynomial probability no $\perp$ was returned, since

$$\begin{aligned}\Pr_{G\sim Y_{p_1(p_2(|H|))}}[B_2(G', H) \neq \perp] &= \sum_{G'} \Pr_{G\sim Y_{p_1(p_2(|H|))}}[I_1(C_1(G)) = G', B_2(G', H) \neq \perp] \\ &\geq \Pr_{G'\sim X_{p_2(|H|)}}[B_2(G', H) \neq \perp]/p_2(|H|)^{c_1} \geq 1/(p_2(|H|)^{c_1}|H|^{c_2}) \geq 1/|H|^c,\end{aligned}$$

for some constant c. If no $\perp$ was returned, we know that $I_2(B_2(I_1(C_1(G)), H)) = H$. This means H can be obtained from G by first putting colors on it via C_1, then interpreting it via I_1, then again putting colors on it via B_2 and again interpreting it via I_2. The same result can be obtained by putting all colors directly on G and then applying I_1 and I_2. Let G^* be the coloring of G which contains the colors of $C(G)$ and the lifted colors of $B_2(G', H)$. The algorithm returns $B(G, H) = G^*$. Then $I(G^*) = I_2(I_1(G^*)) = H$. ◀

With the same techniques as in the lemma before one can show that $\preccurlyeq$ is transitive. Since the proof is straightforward, we leave it out.

▶ **Lemma 13.** *Let X, Y, and Z be random graph models. If $X \preccurlyeq Y$ and $Y \preccurlyeq Z$ then $X \preccurlyeq Z$.*

3.3 Hard Random Graph Models

In this section we prove intractability of p-MC(FO, $\mathfrak{G}_{col}$) for certain random graph models. As a side result, we obtain polynomial lower bounds on the size of shallow clique minors in Erdős–Rényi graphs (Lemma 15) and Chung–Lu graphs (Lemma 18). The main results are summarized in the following theorem.

▶ **Theorem 14.** *The following list of random graph models polynomially FO-interpret to $\mathfrak{G}$ (for $0 < \varepsilon < 1$):*

- **(i)** *every Erdős–Rényi random graph model $G(n, p(n))$ with $n^\varepsilon/n \leq p(n) \leq 1 - n^\varepsilon/n$ that is expected polynomial time samplable,*
- **(ii)** *every Chung–Lu random graph model with exponent $\alpha \in \mathbf{Q}$ with $2.5 \leq \alpha < 3$,*
- **(iii)** *every expected polynomial time samplable random graph model $\mathcal{G}$ such that in $\mathcal{G}_n$ every edge is independent and has an individual probability p with $n^\varepsilon/n \leq p \leq 1/n^\varepsilon$.*

Proof. The second and third case correspond to Lemma 19 and16 respectively. For the first case, the interval $[n^\varepsilon/n, 1 - n^\varepsilon/n]$ can be broken into three parts: $[n^\varepsilon/n, n^{-1/2}]$, $[n^{-1/2}, 1 - n^{-1/2}]$, $[1 - n^{-1/2}, 1 - n^\varepsilon/n]$. The first interval corresponds to Lemma 16. The third interval can be reduced to the first interval using the complement graph. The missing region is filled by Lemma 17. ◀

▶ **Lemma 15.** *Let $\varepsilon > 0$. Let $\mathcal{G}$ be a random graph model such that in $\mathcal{G}_n$ every edge is independent and has an individual probability p with $n^\varepsilon/n \leq p \leq 1/n^\varepsilon$. There exists a deterministic polynomial time algorithm which gets a graph with n vertices and either returns $\perp$ or an induced $6/\varepsilon$-subdivided clique of size $\lfloor n^{\varepsilon/5} \rfloor$. If the input is distributed according to $\mathcal{G}$ then a.a.s. the algorithm does not return $\perp$.*

Proof. Let $n \in \mathbf{N}$ and $k = \lfloor n^{\varepsilon/5} \rfloor$. We fix k principal vertices $v_1, \ldots, v_k$. Each edge in $\mathcal{G}_n$ occurs with probability at least n^ε/n. Thus, the expected degree of each principal vertex is at least $n^\varepsilon = \Theta(k^5)$. The degree of a vertex is a sum of independent Bernoulli variables. According to the Chernoff Bound, a.a.s., each principal vertex has degree at least k^2. We assume that this is the case. This means, there are k^2 distinct nodes w_j^i $(1 \leq i, j \leq k)$ such that w_j^i is adjacent to v_i.

We choose k^2 disjoint subsets $S_{i,j}$ $(1 \leq i, j \leq k)$ of size $N = \lceil n/k^3 \rceil$ such that $S_{i,j}$ contains w_i^j and w_j^i but none of the vertices $v_1, \ldots, v_k$. Each subgraph $\mathcal{G}_n[S_{i,j}]$ can be interpreted as a random graph of order N where edges have independent probability at least $n/n^\varepsilon = \Theta(N/N^{\varepsilon/3})$. It is known that the diameter of a graph $G(n, p(n))$ is a.a.s. at most $\lceil \log(n)/\log(np(n)) \rceil$ [8, Theorem 2] (also [27, 4, 37]). By the argument above, $\mathcal{G}_n[S_{i,j}]$ a.a.s. has diameter at most $\lceil \log(N)/\log(N^{\varepsilon/3}) \rceil = \lceil 3/\varepsilon \rceil \leq 4/\varepsilon$. While not explicitly mentioned in the references, this holds with sufficiently high probability to guarantee that that a.a.s. *each* subgraph $\mathcal{G}_n[S_{i,j}]$ $(1 \leq i, j \leq k)$ has diameter at most $4/\varepsilon$. We again assume that this is the case. Then for each pair of vertices w_i^j, w_j^i we compute a path $p_{i,j}$ in $S_{i,j}$ of length at most $4/\varepsilon$ connecting them. All paths $p_{i,j}$ are disjoint. Therefore, the principal vertices $v_1, \ldots, v_j$ together with the paths $p_{i,j}$ span a $4/\varepsilon + 2$-subdivided clique.

At last, we need to show that this subdivided clique is a.a.s. an induced subdivided clique. The subdivided clique consists of at most $O(k^2)$ vertices. Thus, there is a set F of at most $O(k^4) = O(n^{\varepsilon 4/5})$ possible edges whose presence would mean that the subdivided clique is no induced subdivided clique. Let A be the event that the degree of all principal vertices is at least k^2 and that each subgraph $\mathcal{G}_n[S_{i,j}]$ $(1 \leq i, j \leq k)$ has diameter at most $4/\varepsilon$. Now we need to show that with high probability no edge from F is present, assuming that A holds. Earlier, we showed that A holds a.a.s. Thus, there exists n_0 such that for $n \geq n_0$, $P[A] \geq 1/2$. For every event B and $n \geq n_0$ holds $\Pr[\bar{B} \mid A] \leq \Pr[\bar{B}]/\Pr[A] \leq 2\Pr[\bar{B}]$. Thus if a.a.s. no edge from F is present, then also a.a.s. no edge from F is present under the assumption that A holds. Each edge occurs with probability at most $n^{-\varepsilon}$. Thus, the probability that none of these edges in F is present is at least $\left(1 - n^{-\varepsilon}\right)^{O(n^{\varepsilon 4/5})}$ which converges to one. ◀

▶ **Lemma 16.** *Let $\varepsilon > 0$. Let $\mathcal{G}$ be an expected polynomial time samplable random graph model such that in $\mathcal{G}_n$ every edge is independent and has an individual probability p with $n^\varepsilon/n \leq p \leq 1/n^\varepsilon$. Then $\mathfrak{G} \preccurlyeq \mathcal{G}$.*

Proof. Let H be a graph with $|H| = n$ and $G \sim \mathcal{G}_{\lceil n^{5/\varepsilon} \rceil}$. We use the algorithm from Lemma 15 on G to a.a.s. compute an induced $6/\varepsilon$-subdivided clique of size n. If the algorithm from Lemma 15 returns $\perp$, we set $B(G, H) = \perp$, which a.a.s. never happens. Otherwise, we proceed as follows: Let $v_1, \ldots, v_n$ be the principal vertices of the induced clique and let $p_{i,j}$ $(1 \leq i < j \leq k)$ be the disjoint paths of length at most $6/\varepsilon$ connecting v_i and v_j. Each

path $p_{i,j}$ is adjacent to exactly two principal vertices and no other path. The final output $B(G,H)$ is constructed by adding colors C_1 and C_2 to G: We define $C_1 = \{v_1, \dots, v_n\}$ and $C_2 = \bigcup_{ij \in E(H)} V(p_{\min(i,j),\max(i,j)})$. Now i and j are adjacent in H if and only if v_i and v_j have a connecting path of length at most $6/\varepsilon$ in G which is colored completely with C_2.

Let further $I = (\nu(x), \psi(x,y))$ be the interpretation such that $\nu(x) = C_1(x)$ and $\psi(x,y)$ is the formula which checks if x and y have a connecting path of length at most $6/\varepsilon$ which is colored completely with C_2. The length of $\psi(x,y)$ depends on ε, which is a constant. Now if $B(G,H) \neq \bot$ then $B(G,H)$ is a coloring of G with $I(B(G,H)) = H$ and the probability of $B(G,H) = \bot$ is sufficiently low. Therefore $\mathfrak{G} \preccurlyeq \mathcal{G}$. ◀

▶ **Lemma 17.** *Let $G(n,p(n))$ be an expected polynomial time samplable Erdős–Rényi random graph model with $n^{-1/2} \leq p(n) \leq 1 - n^{-1/2}$. Then $\mathfrak{G} \preccurlyeq G(n,p(n))$.*

Proof. By Lemma 16 and Lemma 12, it is sufficient to prove $G(n, \lfloor\sqrt{n}\rfloor/n) \preccurlyeq G(n,p(n))$. We assume $n > 10$. Let $m = n^{14}$. Let G be the input graph with $G \sim G(m,p(m))$. We shall construct a randomized polynomial time algorithm C and an interpretation I such that $I(C(G))$ behaves similar to $G(n, \lfloor\sqrt{n}\rfloor/n)$. For sets $N \subseteq V(G)$ and vertices $u, v \in V(G) \setminus N$ with $u \neq v$ we say u and v have the same N-neighborhood if $N^G(u) \cap N = N^G(v) \cap N$. Since $G \sim G(m,p(m))$, the probability that u and v have the same N-neighborhood equals $c_N(m) := \big(p(m)^2 + (1-p(m))^2\big)^{|N|}$. We compute the minimal value $k \in \mathbf{N}$ such that $1/n^4 \leq \big(p(m)^2 + (1-p(m))^2\big)^k \leq 1/n^3$. Clearly, k exists and is computable in polynomial time. Furthermore, one can easily show that $k \leq m^{2/3}$.

We fix three sets $X, Y, Z \subseteq V(G)$ with $X = \{v_1, \dots, v_n\}$, $|Y| = |Z| = k$. This yields $1/n^4 \leq c_Y(m), c_Z(m) \leq 1/n^3$. We further fix $\binom{n}{2}$ subsets $S_{i,j} \subseteq V(G)$ for $1 \leq i < j \leq n$ with $|S_{i,j}| = n^{11}$. Since $n + k + \binom{n}{2} n^{11} \leq m$, we can assume all these subsets to be disjoint.

If there exist two vertices v_i and v_j with $1 \leq i \neq j \leq n$ which have the same Y-neighborhood or the same Z-neighborhood we return $\bot$. The probability that this happens is, by the union bound, at most $\binom{n}{2}(c_Y(m) + c_Z(m)) \leq 1/n$. Furthermore, if there exists $1 \leq i < j \leq n$ such that there is no vertex in $S_{i,j}$ which has the same Y-neighborhood as v_i and the same Z-neighborhood as v_j, we return $\bot$. For fixed i, j, the probability that there is no vertex in $S_{i,j}$ which has the same Y-neighborhood as v_i and the same Z-neighborhood as v_j is at most $(1 - c_Y(m)c_Z(m))^{|S_{i,j}|} \leq (1 - 1/n^8)^{n^{11}} \leq 1/n^3$. Thus, by the union bound, $\bot$ is returned with probability at most $\binom{n}{2}/n^3 \leq 1/n$. In total, $\bot$ is a.a.s. never returned.

If the algorithm did not return $\bot$, we know that the Y- and Z-neighborhoods of $v_1, \dots, v_n$ are distinct and for all $1 \leq i < j \leq n$ there exists a vertex $s_{i,j}$ which has the same Y-neighborhood as v_i and the same Z-neighborhood as v_j. We construct a set W which represents the edge set of a random graph $G(n, \lfloor\sqrt{n}\rfloor/n)$ by adding each vertex $s_{i,j}$ for $1 \leq i < j \leq k$ independently with probability $\lfloor\sqrt{n}\rfloor/n$ to W. Let the final output $C(G)$ be the graph G augmented with colors X, Y, Z, W. Let further $I = (\nu(x), \psi(x,y))$ be the interpretation where $\nu(x) = X(x)$ and $\psi(a,b)$ is the FO formula which checks if there exists a vertex $w \in W$ which has the same Y-neighborhood as a and the same Z-neighborhood as b. Now v_i and v_j with $i < j$ are adjacent in $I(C(G))$ if and only if $s_{i,j} \in W$, which occurs with probability $\lfloor\sqrt{n}\rfloor/n$. Therefore under the condition that $C(G) \neq \bot$ we have $I(C(G)) \sim G(n, \lfloor\sqrt{n}\rfloor/n)$. Since a.a.s. $I(C(G)) \neq \bot$, we have for every x in the support of $G(n, \lfloor\sqrt{n}\rfloor/n)$ and n sufficiently large, $\Pr_{G \sim G(m,p(m))}[I(C(G)) = x] \geq \Pr_{G \sim G(n, \lfloor\sqrt{n}\rfloor/n)}[G = x]/2$. This means $G(n, \lfloor\sqrt{n}\rfloor/n) \preccurlyeq G(n,p(n))$. ◀

The threshold $2.5 < \alpha$ in the following lemma has been chosen to ease the calculations and can be considerably improved.

▶ **Lemma 18.** *Let $\mathcal{G}$ be a Chung–Lu random graph model with exponent $2.5 \leq \alpha < 3$. There exists an $\varepsilon > 0$ such $\mathcal{G}_n$ contains a.a.s. a one-subdivided half-induced clique with principal vertices $u_1, \dots, u_{\lceil n^\varepsilon \rceil}$.*

Proof. Let $n \in \mathbf{N}$ and $V(\mathcal{G}_n) = \{u_1, \dots, u_n\}$. By definition [10], the probability of an edge $u_i u_j$ in $\mathcal{G}_n$ is $w_i w_j / \sum_{k=1}^n w_k$, where $w_k = \Theta(n/k)^{1/(\alpha-1)}$. One can easily verify that for $\alpha > 2$, $\sum_{k=1}^n w_k = \Theta(n)$. We choose $\varepsilon = 1/(\alpha-1) - 1/2$ and get

$$\Pr[u_i u_j \in E(\mathcal{G}_n)] = \frac{w_i w_j}{\sum_{k=1}^n w_k} = \frac{(n/i)^{1/(\alpha-1)}(n/j)^{1/(\alpha-1)}}{\Theta(n)} = \Theta(n^{2\varepsilon}(ij)^{-\varepsilon-1/2}).$$

Since $2.5 \leq \alpha < 3$, we have $0 < \varepsilon \leq 1/6$. Let $k = \lceil n^{\varepsilon/2} \rceil$. We fix $a, b \leq k$. For $n/2 \leq x \leq n$ let $p(x)$ be the probability that u_x is a bridge between u_a and u_b. Then

$$p(x) = \Omega\big(n^{2\varepsilon}(xa)^{-\varepsilon-1/2} n^{2\varepsilon}(xb)^{-\varepsilon-1/2}\big) \prod_{c=1}^{k} \Big(1 - O(n^{2\varepsilon}(xc)^{-\varepsilon-1/2})\Big) =$$
$$\Omega(k^{-2\varepsilon-1} n^{2\varepsilon-1}) \Big(1 - O(n^{\varepsilon-1/2})\Big)^k = \Omega(k^{-2} n^{2\varepsilon-1}) = \Omega(n^{\varepsilon-1}).$$

The probability that none of the vertices $u_{\lceil n/2 \rceil}, \dots, u_n$ are a bridge between u_a and u_b is at most

$$\prod_{x=\lceil n/2 \rceil}^{n} \Big(1 - p(x)\Big) = \Big(1 - \Theta(n^{\varepsilon-1})\Big)^{\Theta(n)} = e^{-\Theta(n^\varepsilon)}.$$

By the union bound, $\mathcal{G}_n$ contains no one-subdivided half-induced clique with principal vertices $u_1, \dots, v_k$ with probability at most $k e^{-\Theta(n^\varepsilon)}$. Since $k = \lceil n^{\varepsilon/2} \rceil$, this converges to zero. ◀

▶ **Lemma 19.** *Let $\mathcal{G}$ be a Chung–Lu random graph model with exponent $2.5 \leq \alpha < 3$, $\alpha \in \mathbf{Q}$. Then $\mathfrak{G} \preccurlyeq \mathcal{G}$.*

Proof. The proof is very similar to that of Lemma 16, therefore we merely sketch it. Since $\alpha \in Q$, we know that $\mathcal{G}$ is expected polynomial time samplable (see [1, Lemma 7.14]). Given a graph $G \sim \mathcal{G}_n$, by Lemma 18, the first $\lceil n^\varepsilon \rceil$ vertices of G a.a.s. are the principal vertices of a one-subdivided half-induced clique. If it exists, one can easily find the bridges of said clique in polynomial time. We color the principal vertices with color C_1 and a subset of the bridges with color C_2. We define an FO-interpretation which selects the principal vertices as nodes and connects them if they are joined by a bridge with color C_2. By choosing C_2 accordingly, we can construct an arbitrary graph of order $\lceil n^\varepsilon \rceil$. ◀

References

1. Sanjeev Arora and Boaz Barak. *Computational complexity: A modern approach*. Cambridge University Press, 2009.
2. Albert-László Barabási and Réka Albert. Emergence of scaling in random networks. *Science*, 286(5439):509–512, 1999.
3. Andrej Bogdanov and Luca Trevisan. Average-Case Complexity. *Foundations and Trends in Theoretical Computer Science*, 2(1):1–106, 2006.
4. Béla Bollobás. The diameter of random graphs. *Transactions of the American Mathematical Society*, 267(1):41–52, 1981.
5. Béla Bollobás, Oliver Riordan, Joel Spencer, and Gábor Tusnády. The Degree Sequence of a Scale-free Random Graph Process. *Random Structures & Algorithms*, 18(3):279–290, May 2001.

6 B. Bollobás. *Random Graphs*. Cambridge University Press, 2nd edition, 2001.

7 Fan Chung, Fan RK Chung, Fan Chung Graham, Linyuan Lu, Kian Fan Chung, et al. *Complex graphs and networks*, volume 107. American Math. Soc., 2006.

8 Fan Chung and Linyuan Lu. The diameter of sparse random graphs. *Advances in Applied Mathematics*, 26(4):257–279, 2001.

9 Fan Chung and Linyuan Lu. Connected Components in Random Graphs with Given Expected Degree Sequences. *Annals of Combinatorics*, 6(2):125–145, 2002.

10 Fan Chung and Linyuan Lu. The average distances in random graphs with given expected degrees. *Proc. of the National Academy of Sciences*, 99(25):15879–15882, 2002.

11 Bruno Courcelle. The Monadic Second-Order Logic of Graphs I. Recognizable Sets of Finite Graphs. *Information and Computation*, 85(1):12–75, 1990.

12 Ronald de Haan. An Overview of Non-Uniform Parameterized Complexity. *Electronic Colloquium on Computational Complexity (ECCC)*, 22:130, 2015.

13 E. D. Demaine, F. Reidl, P. Rossmanith, F. Sánchez Villaamil, S. Sikdar, and B. D. Sullivan. Structural Sparsity of Complex Networks: Random Graph Models and Linear Algorithms. *CoRR*, abs/1406.2587, 2014. To appear in JCSS. URL: `http://arxiv.org/abs/1406.2587`, `arXiv:1406.2587`.

14 R. Diestel. *Graph Theory*. Springer, Heidelberg, 2010.

15 Rodney G. Downey, Michael R. Fellows, and Udayan Taylor. The Parameterized Complexity of Relational Database Queries and an Improved Characterization of W[1]. In *First Conference of the Centre for Discrete Mathematics and Theoretical Computer Science, DMTCS 1996, Auckland, New Zealand, December, 9-13, 1996*, pages 194–213, 1996.

16 Z. Dvořák. *Asymptotical Structure of Combinatorial Objects*. PhD thesis, Charles University, Faculty of Mathematics and Physics, 2007.

17 Zdenek Dvořak, Daniel Král, and Robin Thomas. Deciding First-Order Properties for Sparse Graphs. In *Proceedings of the 51st Conference on Foundations of Computer Science*, pages 133–142, 2010.

18 Nikolaos Fountoulakis, Tobias Friedrich, and Danny Hermelin. On the Average-Case Complexity of Parameterized Clique. *Theoretical Computer Science*, 576:18–29, 2015.

19 Tobias Friedrich and Anton Krohmer. Parameterized Clique on Inhomogeneous Random Graphs. *Discrete Applied Mathematics*, 184:130–138, 2015.

20 Jakub Gajarský, Petr Hlinený, Daniel Lokshtanov, Jan Obdrzálek, and M. S. Ramanujan. A New Perspective on FO Model Checking of Dense Graph Classes. *CoRR*, abs/1805.01823, 2018. `arXiv:1805.01823`.

21 Jakub Gajarskỳ, Stephan Kreutzer, Jaroslav Nešetřil, Patrice Ossona de Mendez, Michał Pilipczuk, Sebastian Siebertz, and Szymon Toruńczyk. First-order interpretations of bounded expansion classes. *arXiv preprint arXiv:1810.02389*, 2018.

22 Robert Ganian, Petr Hlinený, Alexander Langer, Jan Obdrzálek, Peter Rossmanith, and Somnath Sikdar. Lower bounds on the complexity of MSO_1-model checking. *J. Comput. Syst. Sci.*, 80(1):180–194, 2014.

23 Martin Grohe. Generalized model-checking problems for first-order logic. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 12–26. Springer, 2001.

24 Martin Grohe. Logic, graphs, and algorithms. *Logic and Automata*, 2:357–422, 2008.

25 Martin Grohe, Stephan Kreutzer, and Sebastian Siebertz. Deciding First-Order Properties of Nowhere Dense Graphs. *JACM*, 64(3):17, 2017.

26 Tao Jiang. Compact topological minors in graphs. *Journal of Graph Theory*, 67(2):139–152, 2011.

27 Victor Klee and David Larman. Diameters of random graphs. *Canadian Journal of Mathematics*, 33(3):618–640, 1981.

28 A. Kostochka and L. Pyber. Small topological complete subgraphs of "dense" graphs. *Combinatorica*, 8:83–86, 1988.

29 Stephan Kreutzer. On the Parameterized Intractability of Monadic Second-Order Logic. *Logical Methods in Computer Science*, 8(1), 2012.

30 Stephan Kreutzer and Siamak Tazari. Lower Bounds for the Complexity of Monadic Second-Order Logic. In *Proceedings of the 22nd Symposium on Logic in Computer Science*, pages 189–198. IEEE Computer Society, 2010.

31 Leonid A Levin. Average case complete problems. *SIAM Journal on Computing*, 15(1):285–286, 1986.

32 M. Molloy and B. A. Reed. A Critical Point for Random Graphs with a Given Degree Sequence. *Random Structures & Algorithms*, 6(2/3):161–180, 1995.

33 M. Molloy and B. A. Reed. The Size of the Giant Component of a Random Graph with a Given Degree Sequence. *Combin., Probab. Comput.*, 7(3):295–305, 1998.

34 Juan Andrés Montoya and Moritz Müller. Parameterized random complexity. *Theory of Computing Systems*, 52(2):221–270, 2013.

35 Moritz Müller. *Parameterized Randomization*. PhD thesis, Albert-Ludwigs-Universität Freiburg, 2008.

36 Jaroslav Nešetřil, Patrice Ossona de Mendez, and David R Wood. Characterisations and examples of graph classes with bounded expansion. *European Journal of Combinatorics*, 33(3):350–373, 2012.

37 Oliver Riordan and Nicholas Wormald. The diameter of sparse random graphs. *Combinatorics, Probability and Computing*, 19(5-6):835–926, 2010.

38 Luc Segoufin and Alexandre Vigny. Constant Delay Enumeration for FO Queries over Databases with Local Bounded Expansion. In *LIPIcs-Leibniz International Proceedings in Informatics*, volume 68. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.

39 Larry J. Stockmeyer. *The Complexity of Decision Problems in Automata Theory*. PhD thesis, Dept. of Electrical Engineering, MIT, 1974.