THE UNIVERSITY OF CHICAGO

SOME RESULTS IN PROOF COMPLEXITY AND SAT-SOLVING

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

BY

SHUO PANG

CHICAGO, ILLINOIS

JUNE 2022

To my teachers

In the case of all things which have several parts and in which the totality is not, as it were, a mere heap, but the whole is something besides the parts, there is a cause.

Aristotle (384–322 BC)

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I wish to express my deepest gratitude to my adviser Alexander Razborov for his support and supervision. It is his teachings on conventional wisdom, self-discipline, and perseverance that saved me from drowning in the sea of freedom.

I am indebted to Aaron Potechin for the invitation to the robust Gaussian learning project among the influence he has on my SoS-related research, the seeds of which were sown by his excellent topic course and to which his feedback has been crucial.

I want to thank Nathan Mull for bringing the topic of CDCL-solvers with ordered-decision strategies to us and educating me on SAT-solvers.

The inclusive and comfortable study environment at the UChicago math department and CS/TTIC theory group has been a source of inspiration. I want to thank the professors, colleagues, and friends here, including Laci Babai, Madhur Tulsiani, Maryanthe Malliaris, Bohdan Kivva, Chris Jones, Sarah Reitzes, Bingjin Liu, Boming Jia, Weinan Lin, Noah Taylor, Leo Coregliano, Dylan Quintana, Nat Mayer, Jon DeWitt, and many others, for the valuable communications and help.

Outside the Chicago circle, I am grateful to Jakob Nordström for hosting me during the Lund-Copenhagen visit in 2019, where I was lucky to know researchers such as he, Dmitry Sokolov, and Kilian Risse. Jakob also invited me to the 2020 Banff workshop, a feast in the field—thank you again, Jakob.

I cannot express how much I love: my father, mother, sisters, and girlfriend Bingjin. Their (well, almost) unconditional love is what I live on.

ABSTRACT

This thesis studies two NP-complete problems, *Clique* and *Boolean Satisfiability* (SAT), under the proof complexity view.

For Clique, we study its average-case hardness. We show that with high probability over an Erdös-Rényi random graph G, the proof system under consideration has no short proof of the true statement "G contains no k-clique". Here k is a suitable parameter, and the shortness of proof is defined by natural complexity measures such as size, width, degree, etc. Specifically, we prove an exponential-in-k size lower bound for the *Resolution* system, and an almost optimal degree lower bound for the *Sum-of-Squares* (SoS) system.

For SAT, we study a different aspect, that is the proof-theoretic power and limitation of *Conflict-Driven Clause-Learning Algorithms* (CDCL-solvers), a standard class of modern SAT-solving algorithms whose often surprising performances call for explanation. We define proof systems modeling CDCL-solvers and, for solvers with the ordered-decision strategies, show their equivalence to either resolution or ordered resolution, depending on the learning scheme employed.

CHAPTER 1

INTRODUCTION

1.1 Proof complexity

Assume there is a fast algorithm A for an NP-complete problem, say the *Boolean Satisfiability* problem (SAT), then on any formula τ, the "running trace" of A gives a short proof of τ's (un)satisfiability. This is a nontrivial consequence, as a priori, there seems no reason that short proofs should always exist. (If τ is satisfiable, they surely exist.) Indeed, the existence of short proofs as such can be rephrased as NP=coNP [39], if "proofs" are in the Cook-Reckhow sense, i.e., any string that passes a pre-fixed, sound, polynomial-time computable "proof checker".

We do not believe short proofs always exist. Although proving such a general lower bound seems out of reach at present, there are many concrete proof systems for us to study and prove lower bounds for, which arise naturally from fields such as logic, algorithms, optimization, etc. The proofs can be in the sequential, Hilbert style (e.g., deduce B from $A,\ A \to B$), or they can operate with algebraic expressions (not necessarily boolean) and have the magical one-line style (e.g., $x_1^3 + x_2^3 + x_3^3 - 3x_1x_2x_3 = \big(x_1 + x_2 + x_3\big)\big(x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_2x_3 - x_3x_1\big)$ refutes $\big(x_1+x_2+x_3 = 0\big) \wedge \big(x_1^3+x_2^3+x_3^3-3x_1x_2x_3 = 1\big)$), or in other mixed styles. Some familiar examples of proof systems include *Resolution* and subsystems, *bounded-depth Frege*, *Frege*, *Polynomial Calculus*, *Cutting-Planes*, *Nullstelensatz*, *Sum-of-Squares*, and so on. Fixing such a system S, we can ask whether there is a "simple" S-proof for a given statement τ that is encoded in the language of S. Out of convenience, we study refutations of wrong statements (still call them proofs). Some examples of τ are the (negation of) counting-related principles such as pigeonhole and Tseitin tautologies, as well as statements from co-NP problems such as "graph G contains a clique of size k" (given an instance G and parameter k), "function f can be computed by a size-t circuit" (given the truth table of a function f), etc. As for the

simplicity of a proof, it can be measured in various ways, the usual ones being the length, size, width, degree, space, and so on, depending on the proof system and our interests.

Questions as above (among others) are studied by proof complexity. It turns out to be a fruitful direction for developing lower bound techniques, with deep technical connections to communication and circuit complexity (see e.g. [69, 91, 94, 60, 49, 48]) and fundamental mutual influences to fields like algorithms and optimization. In fact, the two main systems studied in this thesis, *resolution* and *Sum-of-Squares* (SoS), have strong motivation from and direct applications to the field of SAT-solving and optimization, respectively; for more details see the introduction of chapter 4 and 5.

Our focus is on the so-called non-uniform proof complexity. The uniform counterpart, which studies certain fragments of first- and second-order arithmetic theories (thus also called *bounded arithmetics*, see e.g. [34, 70, 96]), will not be discussed.

1.2 Results and techniques

We study proof complexity-questions for two NP problems, Clique and SAT.

For Clique, we study its average-case hardness on the Erdös-Rényi random graph $G(n, p)$. This means to show that w.h.p. over G, the given proof system has no short proof of the true statement "G contains k-clique", for suitable k.

A few words on average-case hardness. For many problems, if the underlying distribution of inputs has many independent components, then the so-called *statistical threshold* phenomenon will appear. For instance, if $G \sim G(n, 1/2)$, then as long as k is not in a thin range $(2 \pm \epsilon) \log n$, it is trivial to tell correctly w.h.p. whether G has a k-clique—e.g., if $k > 2.1 \log n$ then just say "no" ([29]). However, to prove the "no" answer seems difficult most of the time, and our task is to prove such intuition on weak proof systems.[1]

1. This is reminiscent of the *Shannon effect* in circuit complexity: a simple counting shows that random function has no small circuit, while proving this for a given function seems almost always difficult.

Chapter 3: Resolution size lower bound on *dense* graphs. We prove an $2^{\Omega(k^{1-\epsilon})}$ resolution size lower bound, where $k = n^{\epsilon}$, $\epsilon \in (0, \frac{1}{3})$. (The parameter p is $n^{-\frac{2\xi}{k-1}}$ for some large constant $\xi > 1$.) This extends the previous lower bound that is for $k > n^{\frac{5}{6}}$ [16] and the bounds on resolution subsystems for roughly the same range of k as here [24, 8]. But note that our bound is not as optimal as $n^{\Omega(k)}$ for subsystems [24, 8], and the difference is significant for small k's (say $k = \text{poly}(\log n)$).

Our method is the classic bottleneck-counting/random-restriction, the key being a variant of the clause width measure defined from graph-theoretic neighborhood density. The idea is a common one in complexity theory: if the system operates with only the class of local, partial information (low-"width" clauses) then its deduction closure is very limited, so it has to produce and use the more accurate, deep information (high-"width" clauses), and we show that the final contradiction is essentially a piece-by-piece aggregate of all such high-accuracy information thus the proof needs at least to deduce all of them.

Chapter 4: Almost tight SoS degree lower bound on $G(n, \frac{1}{2})$. Let us now follow the convention in the optimization literature and use letter ω to represent the size of an intended clique (whose existence we want to refute). It is well-known that degree d-SoS can solve the problem w.h.p. if degree $d > 2.1 \log n$ or $\omega = O(\sqrt{n})$, so an optimal lower bound is expected to be $d = \Omega(\log n)$ for $\omega = n^{\frac{1}{2}-\epsilon}$. Previous lower bounds have two kinds: either in the form $d = \Omega(\log_{\omega} n)$ [47, 79, 43, 57], or in the optimal form $d = O(\epsilon^2 \log n)$, $\omega = n^{\frac{1}{2}-\epsilon}$ but weakens the clique-size axiom to an inequality [13]. Note the latter formulation is potentially significantly weaker, as all polynomial multiple of that axiom are removed from constraints. We prove an almost optimal bound $d = \Omega(\frac{\epsilon^2 \log n}{\log \log n})$, $\omega = n^{\frac{1}{2}-\epsilon}$ for the original problem.

This time, we are dealing with the "degree d-SoS deduction closure" of the axioms, i.e. all possible polynomials that is a sum of multiples of the axioms and squares (all of degree $\leq d$). The fundamental method here, as is in many cases in optimization theory, is *duality*, which turns non-existence problems into constructive ones. It works by designing dual assignments

to monomials (called *pseudo-expectations*) and proving the resulting *pseudo-moment matrix* is PSD (positive semi-definite). Within this framework substantially more needs to be done, which is the nontrivial part. For the clique problem, our method intuitively is to combine the previous vertex-based technique (Johnson schemes) and edge-based technique (Fourier character-matrix factorization) in the analysis, achieved via using Hadamard product and Euler transform. At the heart of the pseudo-expectation design is a special matrix family which we term as the *factorial Hankel matrices*.

Next, we turn to the SAT problem. Due to its convenient formulation, SAT has quite a few practical applications and it's no wonder there are numerous algorithms and heuristics for solving it, all sharing the name *SAT-solvers*. A dominating class in modern SAT-solving is the *Conflict-Driven Clause-Learning algorithms (CDCL-solvers)* which has gained considerable theoretical interests (see e.g. [64, 26, 37]). Roughly speaking, they are algorithms that use resolution to find a satisfying assignment/refutation, possibly incorporating nondeterminism or randomness in various aspects, such as how to do a so-called *unit propagation*, how to decide to which variable to assign a value (*decision strategy*), and how to derive a new clause when the current assignments result in a contradiction (*learning scheme*).

Chapter 5: Proof-theoretic power and limitation of CDCL-solvers with the ordered-decision strategies. Decision strategies are often a non-trivial, non-deterministic or random part of CDCL-solvers in the literature for achieving the best theoretical power. How about the deterministic, simple, yet popular *ordered-decision strategy*? This means when the solver chooses a variable to assign a value, it always chooses the first unassigned one in a prefixed variable order. Since CDCL-solvers are based on resolution, with ordered-decision strategies they are naturally expected to fall between ordered and general resolution. We show, somewhat surprisingly, that with two different natural learning schemes inspired from practice, both extremes can be achieved: the resulting system modeling these solvers is equivalent to either resolution or ordered resolution, both regardless of the order in use.

Both results are proved by non-trivial simulations, where we use surgery-like processes to get a fine-grained understanding of the structure of a proof. One of the proof systems encountered here is non-closed under variable restrictions, and a fresh technique we introduce to analyze such systems is the *variable deletion* operator. When viewed semantically, it amounts to a projection of boolean cubes; we use it to break a proof into two subproofs, say one for $x_1 = 0$ and one for $x_1 = 1$, without overlap and without assuming the proof to be tree-like.

CHAPTER 2

NOTATION

$G = (V, E)$ will always denote a simple, undirected graph. The set of *neighbors* of a vertex $v \in V$ is $N(v) = \{u \mid (u, v) \in E\}$. A *k-clique* in G is a set $C \subset V$ with size k s.t. $\forall u, v \in C, u \neq v \Rightarrow \{u, v\} \in E$. The *Erdős-Rényi graph* $G(n, p)$, with $0 < p < 1$, is a random n-vertex graph that places an edge between any two vertices with probability p independently.

A *literal* over a Boolean variable x is either x or its negation $\neg x$ (also denoted as $\bar{x}$), where x is the underlying *variable* of the literal. We sometimes use the abbreviation x^0 for the negation of x and x^1 for x (so that the Boolean assignment $x = a$ *satisfies* the literal x^a). A *clause* $C = l_1 \vee ... \vee l_t$ is a disjunction of distinct literals where there is no appearance of $x, \neg x$ together for any variable x (otherwise the clause is 1). t is the *width* of C, denoted as $w(C)$, and $\mathrm{Var}(C)$ is the set of variables appearing in C. The empty clause is denoted by 0 or $\perp$. A *CNF formula* $\tau = C_1 \wedge .... \wedge C_m$ is a conjunction of clauses. For a CNF τ, $\mathrm{Var}(\tau)$ is the set of variables appearing in τ, i.e., the union of $\mathrm{Var}(C)$ for all $C \in \tau$. A *w-CNF* is a CNF in which all clauses have width $\leq w$.

A *resolution proof of clause C from a CNF* τ is an ordered sequences $\Gamma = (D_1, ..., D_L)$ where $D_L = C$ and, for all $i \in [L]$, D_i is either a clause in τ (called an *axiom*) or is derived from D_j, D_k, $j, k < i$ by the *resolution rule*:

$$\frac{C \vee x_i^a \qquad D \vee x_i^{1-a}}{C \vee D}, \ a \in \{0, 1\}. \tag{2.1}$$

where $D_j = A \vee x, D_k = B \vee \neg x, D_i = A \vee B$, $D_i \neq 1$. x is the *resolved variable*. We will sometimes make use of the notation $\mathrm{Res}(A \vee x, B \vee \neg x)$ for the conclusion clause $A \vee B$. The *size* of Γ is L, denoted by $|\Gamma|$. If $C = 0$, then Γ is called a *refutation*. Let $\mathrm{Var}(\Gamma)$ denote the set of variables appearing in Γ, i.e., the union of $\mathrm{Var}(C)$ for C appearing in Γ. For a CNF τ and a clause C, we let $S_R(\tau \vdash C)$ be the minimal possible size of a resolution proof

of the clause C from clauses in τ (∞ if C is not implied by τ). Likewise, $w(\tau \vdash C)$ is the minimal possible width of such a proof, defined as the maximal width of a clause in it. A resolution proof $\tau \vdash C$ is *tree-like* if its underlying proof graph—the natural *directed acyclic graph* (DAG) whose nodes correspond to the clauses in Γ, C at the top/root—is a tree, and it is *regular* if along any path from axioms to root, no variable is resolved more than once.

The *Sum-of-Squares* (SoS) proof system[1] works with polynomials over $\mathbb{R}$, where given a set of polynomial identities (axioms) $f_1(x) = 0, ..., f_k(x) = 0$ on variables $x = (x_1, ..., x_n)$, a *SoS proof of* $f_1, ..., f_k$, is an identity

$$-1 = \sum_{i=1}^{k} f_i q_i + \sum_j r_j^2 \quad \text{in} \quad \mathbb{R}[x_1, ..., x_n], \tag{2.2}$$

where $q_1, ..., q_k, r_1, ...$ are arbitrary real polynomials on $x_1, ..., x_n$. Note this actually *refutates* the existence of a solution, but for convenience we still call it a proof. The *degree-d SoS proof system* carries the obvious degree restriction on identity (2.2):

$$\max_{i,j}\{\deg(f_i) + \deg(q_i),\ 2\deg(r_j)\} \leq d. \tag{2.3}$$

For any real matrix M, $\|M\|$ denotes its L_2-norm.

"$\sqcup$" denotes the disjoint union of sets.

Similar to the conventional abbreviation "w.h.p." for "with high probability", "w.p." will stand for "with probability".

1. It is also known as the *Positivstellensatz* system [51].

CHAPTER 3

RESOLUTION LOWER BOUND OF CLIQUE

The content of this chapter is from the work [86] that appeared at the 16th International Computer Science Symposium in Russia (CSR 2021).

3.1 Introduction

The k-Clique problem is one of the fundamental NP-complete problems and its computational hardness has been intensively studied in both algorithmic and lower bound worlds ([82, 95, 55, 108, 99, 105, 53]). Proof complexity studies, among many other aspects, the hardness of proving $f(x) = 0$ for a boolean function f and input x, which is a natural and necessary step for understanding the computational hardness of f. The underlying proof system should be sound and efficiently checkable (called *Cook-Reckhow* systems). Given such a system Λ, the proof-theoretic version of the k-Clique problem is, "is there a short Λ-refutation of the CNF encoding of the fact 'G contains a k-clique'?" In this chapter, Λ will be resolution and its sub-systems, and we study the average-case problem, i.e. when G is a random graph and we ask if there a short refutation with high probability. The random graph should be k-clique-free w.h.p. (otherwise, there is no refutation of a correct claim, short or long), and the most studied setting is the Erdős-Rényi random graph $G(n, p)$, with p below the so-called threshold of containing a k-clique, usually taken as $p = n^{-\frac{2\xi}{k-1}}$ where $\xi > 1$ is a constant.

Previous work. An $n^{O(k)}$-sized tree-like resolution refutation is not hard to see when G doesn't contain a k-clique. For lower bounds, a $2^{\Omega(k^6/n^5)}$ size lower bound for resolution is known [16], which is meaningful for $k > n^{5/6}$; the optimal $n^{\Omega(k)}$ size lower bounds are known for tree-like resolution [24] and regular resolution [8] (for $k < n^{\frac{1}{4}-o(1)}$).

Our results. Like in almost all previous work, we state and prove the results for a strong encoding of the problem, the "transversal clique" formulation (equation (3.2)). Our main result is an $\exp(k^{1-\epsilon})$ average-case resolution size lower bound of the k-Clique problem in this encoding, when $G \sim G(n,p)$ as above (Corollary 3.1). This result holds for k's that do not exceed $n^{1/3}$ thus complements the result of [16] (which requires $k > n^{5/6}$). More precisely, it holds for $k = n^{c_0}$ where c_0, ϵ are arbitrary positive parameters s.t. $\min\{\frac{1}{3} - c_0, \epsilon c_0\} > (\log n)^{-1/5}$.

Our second result (Theorem 3.3) extends the $n^{\Omega(k)}$ average-case lower bound to a new model called *a-irregular* resolution, for $k < n^{1/3-\epsilon}$, as a possible step towards the same bound for resolution.

A few words on the second model. It is a Cook-Reckhow system with the following motivation: imagine that in general, the "hard part" of a short resolution proof is the derivation of some clauses with nontrivial width (or some variant) such that, once they are in place, the rest is easy. Then how hard is it to derive these clauses? In particular, if in deriving *any* wide clause we can't be too irregular, is there still a short refutation? Formally, we restrict that *in deriving any clause of large (block-)width, few (blocks of) variables are irregularly resolved.* Here, *large* and *few* will be characterized by the parameter $a \in (0,1)$ ($a = 0/1$ means regular/general resolution), and *block* is used in the main version where a variable partition is part of the input. It turns out (Remark 3.3) that all known CNF families separating regular resolution from general separate, in fact, regular resolution from this model with $a = n^{-\Omega(1)}$. (Our result holds for constant a.) Previously, [30] considered an extension of regular resolution called *δ-regular resolution* by restricting the number of irregularly-resolved variables on any path. Our restriction is simpler in the sense that the resulting system is clearly Cook-Reckhow, but the two seem incomparable, and it will be interesting to know their exact relation.

Proof idea. For the first result, we consider a class of clauses (not depending on the refutation) where each one is very small (under certain "measure" on clauses), while we show that in any refutation, the clauses from this class together "have measure 1". Such a clause C has the property that its associated set of *falsifying* assignments, when regarded as a k-product subset in $[n]^k$ in the natural way[1], has many indices $i \in [k]$ s.t. the i-th component is small in a certain sense. The empty clause has full measure 1. We show that, when traveling down the proof DAG with some strategy, one always ends in such a small clause, and thus there are many such clauses in C. This argument is similar to the *bottleneck counting* method as in [54, 92] and might be possible to be translated into a random restriction-based argument, while the current language is chosen since it works consistently for the second result too.

The second result is built on [8] in a straightforward manner. In a given refutation, we find *one* small clause C (in the above sense) s.t. the sub-proof deriving C is regular after a suitable restriction. The useful graph-theoretic property used in the regular case seems not inheritable to sub-graphs (which occurs from the restriction), but this can be fixed by using a relativized property (section 3.4.3).

The proof of the first result has the merit of simplicity and the drawback is there, too: the pseudorandom graph-theoretic property used is insufficient for an $n^{\Omega(k)}$ lower bound (Remark 3.2). On the other hand, we don't know of a similar limitation of the property used in the regular case and the second result.

Chapter structure. After giving preliminaries in section 3.2, we prove the first result in section 3.3. In section 3.4 we introduce the new model and prove the second result.

1. More precisely, it is a product-subset of $[n/k]^k$; the reason is clear after seeing the strong encoding (section 3.2) where the vertex set is partitioned into k parts.

3.2 Preliminaries

Recall we use $G = (V, E)$ to denote a simple, undirected graph. For $A, B \subseteq V$, $\hat{N}_A(B) = A \cap (\cap_{v \in B} N(v))$ denotes the set of *common neighbors of B in A*; when $A = V$ it will be simplified as $\hat{N}(B)$. $\mathbf{G}$ will denote the n-vertex Erdős-Rényi random graph $G(n, p)$, $0 < p < 1$. For $1 < k < n$, $n^{-\frac{2}{k-1}}$ is the well-known *threshold probability* [29]: $G(n, p)$ contains a k-clique (or not) w.h.p. as $n \to \infty$ if $p > n^{-(1-O(1))\frac{2}{k-1}}$ (or $p < n^{-(1+O(1))\frac{2}{k-1}}$). We take $p = n^{-\frac{2\xi}{k-1}}$, $\xi > 1$ a constant, throughout the chapter.

We now introduce the two natural k-Clique CNFs from the literature[2]. $Clique(G, k)$ is the encoding of "G contains a k-clique", on variables $x_{i,v}$ ($i \in [k]$, $v \in V$):

$$\begin{aligned} \bigvee_{v \in V} x_{i,v} \qquad & \forall i \in [k]; \\ \neg x_{i,u} \vee \neg x_{j,v} \qquad & \forall i, j \in [k], u, v \in V \text{ } s.t. \text{ } i \neq j, \text{ } \{u, v\} \notin E; \\ \neg x_{i,u} \vee \neg x_{i,v} \qquad & \forall i \in [k], u, v \in V \text{ } s.t. \text{ } u \neq v. \end{aligned} \tag{3.1}$$

The other one, $Clique_{block}(G, k)$, is the encoding of "G contains a k-transversal clique" w.r.t any fixed balanced vertex-partition:

$$V = V_1 \sqcup ... \sqcup V_k, \quad |V_i| - |V_j| \in \{0, \pm 1\} \text{ for all } i, j \in [k],$$

where a clique C is *transversal* if $\forall l \in [k]$, $|C \cap V_l| \leq 1$.

$$\begin{aligned} \bigvee_{v \in V_i} x_v \qquad & \forall i \in [k]; \\ \neg x_u \vee \neg x_v \qquad & \forall i \neq j \in [k], u \in V_i, v \in V_j \text{ } s.t. \text{ } \{u, v\} \notin E; \\ \neg x_u \vee \neg x_v \qquad & \forall i \in [k], \text{ } u, v \in V_i \text{ } s.t. \text{ } u \neq v. \end{aligned} \tag{3.2}$$

2. There is also the so-called *binary* encoding ([73]), which we will not discuss here.

In both encodings, the first group of axioms is called *clique axioms*, the second group *edge axioms*, and the third group *functionality axioms*. Clearly, the block encoding claims something stronger (hence is easier to refute) so a lower bound on its refutation length is stronger, too. We have the following observation which seems to be folklore among researchers.[3]

Theorem 3.1. *For any graph G that contains an $\Omega(k)$-clique, the $\exp(\Omega(k))$ resolution size lower bound holds for $Clique(G,k)$. In particular, the bound holds for the random graph $G(n, \frac{2\xi}{k-1})$ ($\xi > 1$ constant) with high probability.*

Proof. By a reduction to the *functional pigeonhole principle* $FPHP$. More precisely, if G contains a clique C, take the restriction ρ which sets $x_{i,v}$ to 0 for all $i \in [k], v \notin C$, then the refutation refutes $FPHP^k_{|C|}$. But an $\exp(|C|)$ lower bound for the latter is known (e.g. [97]). Finally, note a random graph from $G(n, \frac{2\xi}{k-1})$ contains $\Omega(k)$-cliques with high probability. □

Remark 3.1. *The encoding $Clique(G,k)$ inherits hardness from $FPHP^k_{\Omega(k)}$ which has little to do with the underlying graph. For $Clique_{block}(G,k)$, however, such a reduction on random graphs seems unlikely*[4] *as it just prohibits permutation on $[k]$. This is one reason $Clique_{block}(G,k)$ is regarded as more technically appropriate (cf. a similar remark in [16]). In the rest of the chapter, we concentrate on the CNF $Clique_{block}(G,k)$.*

Notation. We view a resolution proof Γ, i.e. a refutation of a CNF τ as a top-down DAG with the $\bot$ on top, and identify a clause C with the partial-assignment that minimally falsifies it. For example, $\{x_1 = 1, x_2 = 0\}$ represents clause $C = \neg x_1 \vee x_2$, and the empty assignment represents $\bot$. For clarity, we call such a representation an *object* and use letter P to denote it. Any non-leaf $P \in \Gamma$ is labeled by a query "x =?" on a variable x, and an *answer* is $x = 1$ or $x = 0$, leading to one child whose object contains the answer. For the clique problem, more conveniently, we can denote a query by "*(l,v)?*" intended for

3. For complete $(k-1)$-partite graphs, a similar reduction is observed earlier by Alexander Razborov (personal communication).

4. For some specially structured G this is possible; see Remark 3.2.

"is x_v=1?" where $l \in [k]$, $v \in V_l$, and the answer is $(l,v)^{yes}$ or $(l,v)^{no}$, which chooses a child whose representation includes $x_v = 1$, $x_v = 0$ respectively. For distinction (and inspired by the pigeonhole principle), let us call $l \in [k]$ a *pigeon* and $v \in V_l$ a *vertex*; the semantics of $Clique_{block}(G,k)$ is, therefore, "assign to each pigeon a vertex so that they form a k-transversal-clique".

Definition 3.1. *Given object P, let $P_1 := \{(l,v) \mid (l,v)^{yes} \in P\}$, $P_0 := \{(l,v) \mid (l,v)^{no} \in P\}$. For a pigeon $l \in [k]$, denote*

$$P_1(l) := \{\ v \in V_l \mid\ (l,v)^{yes} \in P\} \qquad P_0(l) := \{\ v \in V_l \mid\ (l,v)^{no} \in P\}. \tag{3.3}$$

$$P_{Live}(l) := V_l \backslash P_0(l) \qquad P_{Live} := \bigcup_{l \in [k]} P_{Live}(l). \tag{3.4}$$

By definition, $P_1(l) \cap P_0(l) = \emptyset$, $P_1 = \bigcup_{l\in[k]} \{l\} \times P_1(l)$, and $P_0 = \bigcup_{l\in[k]} \{l\} \times P_0(l)$. We use $\mathrm{dom}(P_1), \mathrm{dom}(P_0)$ to denote the projection to $[k]$ from P_1, P_0. A *live-clique in P* is a transversal clique in P_{Live}. A **partial** function $f : [k] \to V$ is a *live-clique assignment in P* if $f(l) \in V_l$ whenever it is defined, and its image is a live-clique in P.

In most situations, each $P_1(l)$ has size 0 or 1. Intuitively, an object P gives a product set $P(1) \times ... \times P(k) \subseteq V_1 \times ... \times V_k$ where $P(l) = P_1(l)$ if $P_1(l) \neq \emptyset$ and $P(l) = V_l \backslash P_0(l)$ otherwise. For example, if P is the empty assignment (i.e. the $\perp$ clause) then this set is the full $V_1 \times ... \times V_k$; while if $P_1(l)$ is nonempty for many l's, then the corresponding set has many coordinates of size 1. We will think of the "largeness" of P by measuring this set in a certain way (see the discussion under Definition 3.3).

3.3 2^k-type lower bound for resolution

Parameter regime. Throughout section 3.3, we use the following parameter regime.

$\xi > 1$ a constant;

$k = n^{c_0}$ where $c_0, \epsilon \in (0, 1/3)$ arbitrary parameters s.t.

$$\min\{\epsilon c_0, 1/3 - c_0\} > (\log n)^{-1/5}; \tag{3.5}$$

$$N = 1 + \max\{\frac{1}{1-3c_0}, \frac{1}{\epsilon c_0}\}, \quad t = \frac{18\xi \cdot N}{1/3 - c_0};$$

$$r = \frac{k}{t}, \; q = \frac{1}{2}n^{1-c_0-2\delta r} \text{ where } \delta = \frac{2\xi}{k-1}.$$

W.l.o.g. we can assume k, r, q are integers. The meaning of k, c_0, ϵ is self-evident. r is a sufficiently small portion of k, and q is appropriately below the expected number of common neighbors of an r-subset in a random graph G. N, t are used only for technical reason. Note $(\log n)^{-1/2} < \delta r < \frac{1/3-c_0}{4N}$.

The reader can assume for simplicity the parameters are in the "typical" case, i.e. ϵ, c_0 and N, t are all constants. We do not try to optimize the parameter range, e.g. the number $(\log n)^{-1/5}$ is just a convenient choice for the estimates in Lemma 3.2 and (3.22) to go through.

3.3.1 Graph properties

Fix a balanced vertex partition $V = V_1 \sqcup ... \sqcup V_k$.

Definition 3.2. *A subset $A \subseteq V$ is called (r, q)-neighbor-dense ([24], [8]) if for any $U \subseteq V$ with size $\leq r$, it holds that $|\hat{N}_A(U)| \geq q$. G is called $(r, q)^{block}$-neighbor-dense if for every $j \in [k]$, V_j is (r, q)-neighbor-dense.*

Lemma 3.1. *(Inheritability of neighbor-denseness) For any integers a_1, a_2, b_1, b_2 and fixed G, if $A \subseteq V$ is $(a_1 + a_2, b_1 + b_2)$-neighbor-dense and $A_1 \subseteq A$ is not (a_1, b_1)-neighbor-dense, then $A \backslash A_1$ is (a_2, b_2)-neighbor-dense.*

Proof. Take a witness W_1 of size a_1 for A_1 s.t. $|\hat{N}_{A_1}(W_1)| < b_1$. For any $W \subseteq V$, $|W| \le a_2$,

$$|\hat{N}_{A\setminus A_1}(W)| \ge |\hat{N}_{A\setminus A_1}(W_1 \cup W)| = |\hat{N}_A(W_1 \cup W)| - |\hat{N}_{A_1}(W_1 \cup W)| \ge (b_1 + b_2) - b_1,$$

where the second inequality used $|W_1 \cup W| \le a_1 + a_2$ and A is $(a_1 + a_2, b_1 + b_2)$-neighbor-dense. □

Lemma 3.2. *W.p.* $> 1 - \exp(-0.5\sqrt{\log n})$, $G \sim G(n, n^{-\frac{2\xi}{k-1}})$ *is* $(2r, q)^{block}$*-neighbor-dense with parameters in* (3.5).

Proof. By standard use of Chernoff bound and union bound. For any fixed $j \in [k]$, any $R \subseteq V$ with $|R| = 2r$, $\mathrm{E}[\ |\hat{N}_{V_j}(R)|\ ] \ge (n/k - |R|) \cdot n^{-\delta r} > \frac{2}{3} n^{1-c_0-\delta r} > q$. So

$$\begin{aligned} \Pr[\ |\hat{N}_{V_j}(R)| < \frac{1}{2}q\ ] &\le \exp(-\frac{n^{1-c_0-2\delta r}}{48}) \\ &< \exp(-n^{2c_0+\delta r}) \quad \text{since } \delta r < 1/3 - c_0 \text{ by (3.5).} \end{aligned} \tag{3.6}$$

The first "$\le$" in above uses Chernoff bound as all different edges are independent. Finally, take a union bound over R's whose total number is at most $n^{2r} < \exp(0.5 n^{2c_0} \log n)$, and $\exp(-n^{2c_0+\delta r}) \cdot \exp(0.5 n^{2c_0} \log n) < \exp(-0.5\sqrt{\log n})$ since $\delta r > (\log n)^{-1/2}$ in (3.5). □

Remark 3.2. *Some particular graph family is also neighbor-dense, yet being far from pseudorandom. For example, consider a complete* $(k-1)$*-partite graph* G *where* $2r < k_1 < k$ *(*r, k *as in* (3.5)*), with partition* $V = W_1 \sqcup ... \sqcup W_{k_1}$ *where* $|W_i \cap V_j| \approx \frac{n}{k_1 k}$ *for all* $i \in [k_1], j \in [k]$*. Notice, however, for these graphs there is a* $2^k n^2 k^2$ *refutation (e.g. [24]) which is regular, and thus to obtain strong lower bound* $n^{\Omega(k)}$ *the property of neighbor-denseness is not enough, even for regular resolution.*[5]

5. Although a variant of it seems sufficient for tree-like resolution, cf. [24].

3.3.2 Lower bound proof

Theorem 3.2. *For parameters as in* (3.5) *where* $k = n^{c_0}$*, if* G *is* $(2r, q)^{block}$*-neighbor-dense then any resolution refutation of* $Clique_{block}(G, k)$ *has size* $\geq \exp(\Omega(k^{1-\epsilon})/t^2)$*, where* $\Omega(\cdot)$ *only relies on some absolute constant. In particular, if* $c_0, \epsilon \in (0, 1/3)$ *are constant, then the bound is* $\exp(\Omega(k^{1-\epsilon}))$*.*

Corollary 3.1. *(of Theorem 3.2 and Lemma 3.2) Within the same parameters as in Theorem 3.2,* $Clique_{block}(G, k)$ *is sub-exponentially hard for* $G(n, n^{-\delta})$ *on average, where* $\delta = \frac{2\xi}{k-1}$*,* $\xi > 1$ *constant.*

The rest of this section is devoted to the proof of Theorem 3.2. To show size lower bound, we design an answering strategy that finds many different objects in Γ. We call this an *adversary strategy* (against the prover Γ; cf. [92]).

Fix any resolution proof Γ of $Clique_{block}(G, k)$. We will first describe an adversary strategy and then analyze the size bound from it.

Adversary strategy.

1. Probabilistic part. Choose a set of $\frac{r}{2}$ pigeons from $[k]$ uniformly at random, each with probability $\binom{k}{r/2}^{-1}$. Then choose an $\boldsymbol{\alpha}$, a transversal clique assignment to the chosen pigeons, according to the following distribution:

$$\begin{aligned} &\textit{(Distribution of } \boldsymbol{\alpha}\textit{) Suppose the chosen pigeons are } l_1, ..., l_{\frac{r}{2}} \in [k]\textit{. Choose } \alpha(l_1) \\ &\quad \textit{uniformly from } V\textit{, then } \alpha(l_2) \textit{ uniformly from } \hat{N}_{V_{l_2}}(\{\alpha(l_1)\})\textit{, } \alpha(l_3) \textit{ uniformly} \\ &\quad \textit{from } \hat{N}_{V_{l_3}}(\{\alpha(l_1), \alpha(l_2)\}) \textit{ and so on till } \alpha(l_{\frac{r}{2}}) \textit{ is chosen.} \end{aligned} \tag{3.7}$$

Denote this distribution by $\mathcal{D}$, which is well-defined when G is $(2r, q)^{block}$-neighbor-dense. The strategy is deterministic after α is chosen.

2. Deterministic part. Fix a sample α from above.

Definition 3.3. *(Narrow pigeons) Given an object P, pigeon $l \in [k]$ is* **narrow in** *P if:*

$$P_0(l) \text{ is } (r, \frac{1}{2}q)\text{-neighbor-dense.}$$

The set of **useful pigeons for** *P is defined to be dom$(P_1) \cup \{$narrow pigeons in $P\}$.*

Intuitively, an object is small if it contains $\geq \frac{r}{2}$ many useful pigeons. The **property** the strategy keeps is: as long as the number of useful pigeons in the current object is $< r/2$,

$(*)$:
1. α, P_1 are compatible as functions;
2. $\exists$ function β: {narrow pigeons in P} $\to V$ s.t. α, P_1, β are consistent and together is a live-clique assignment for P (Def. 3.1).

Note at the beginning of any path (top node), $(*)$ trivially holds.

Claim 3.1. *If for an object P the above $(*)$ holds, then P is not an axiom.*

Proof. This follows from a direct check. □

The strategy continues as follows. Suppose the property $(*)$ holds for current object P where the query is (l, v)?. Answer according to the following:

(1) If |useful pigeons in $P| \geq r/2$, then *halt*. Otherwise,
(2) (2a) If $l \in \text{dom}(\alpha \cup P_1 \cup \beta)$, answer according to $\alpha \cup P_1 \cup \beta$; (3.8)
(2b) Otherwise, say "No".

Lemma 3.3. *Suppose the current object P satisfies $(*)$. Then either we halt, or after extending the path by one more step we still keep $(*)$.*

Proof. For item 1 in $(*)$, it holds for the next object because of (2a) of the strategy. Now we prove item 2. If P has $\geq r/2$ many narrow pigeons then we would halt by (1) of the strategy.

Otherwise, by assumption there is β for P_0 as in $(*)$. We prove that the "intermediate" object

$$Q := P \cup \{\text{the new answer}\}$$

satisfies $(*)$, and the lemma follows because $(*)$ is monotone w.r.t. the object.

Assume the new query is $(l, v)?$. In case (2a), the same β for P suffices for Q, trivially from inductive hypothesis. In case (2b), either $P_0(l) \cup \{v\}$ is $(r, \frac{1}{2}q)$-neighbor-dense in G, or it isn't. In the latter case, the pigeon l is still not narrow in Q, and thus $(*)$ holds for Q. In the former case, let $R := \mathrm{Im}(\alpha \cup \beta \cup P_1)$. By assumption,

$$|R| \leq |\alpha| + |\beta \cup P_1| = \frac{r}{2} + |\{\text{useful pegions}\} < \frac{r}{2} + \frac{r}{2} = r. \tag{3.9}$$

Moreover, $P_0(l) \cup \{v\}$ is not $(r, \frac{1}{2}q + 1)$-neighbor-dense by the case assumption. So by Lemma 3.1, where we take $A := V_l$, $A_1 := P_0(l) \cup \{v\}$, and $a_1 = a_2 = \frac{1}{2}q$, we get that $V_l \backslash (P_0(l) \cup \{v\}) = V_l \backslash Q_0(l) = Q_{\mathrm{Live}}(l)$ is $(r, \frac{1}{2}q - 1)$-neighbor-dense. In particular, as $\frac{1}{q} >> 1$, we can choose a $w \in \hat{N}_{Q_{\mathrm{Live}}(l)}(R)$. Extend β to $\beta \cup \{\beta(l) = w\}$ will keep $(*)$ for Q. □

The answering strategy is now completed: we extend β so that $(*)$ holds until we halt.

Lower bound analysis.

Since Γ is a correct proof, the query process must stop. By Claim 3.1, it could only be halted in Case (1) of (3.8). Let T be the set of all such halting objects (over all α) in Γ.

Definition 3.4. *We say a $\frac{r}{2}$ transversal clique assignment α leads to object P (in T) if when chosen α in the beginning, the adversary strategy halts at P.*

Lemma 3.4. *Given the distribution $\boldsymbol{\alpha} \sim \mathcal{D}$ (3.7), for any fixed $P \in T$*

$$\Pr[\ \boldsymbol{\alpha} \textit{ leads to } P\ ] \leq \exp(-\Omega(k^{1-\epsilon})) \tag{3.10}$$

where the parameters are as in (3.5).

Proof. By definition of T and Lemma 3.3, for P we have $|\{\text{useful pigeons}\}| \geq r/2$. Recall $r = k/t$ in (3.5). Take another parameter $\epsilon' = \frac{1}{40}\frac{r}{k} = \frac{1}{40t}$ and denote $a_0 := \lceil \epsilon' r \rceil$. By the first part of definition of $\boldsymbol{\alpha}$,

$$\Pr[\ |\mathrm{dom}(\boldsymbol{\alpha}) \cap \{\text{useful pigeons}\}| < \epsilon' r\ ] \tag{3.11}$$

$$= \sum_{a<a_0} \binom{r/2}{a}\binom{k-r/2}{r/2-a}/\binom{k}{r/2} < a_0 \cdot \binom{r/2}{a_0}\binom{k-r/2}{r/2-a_0}/\binom{k}{r/2}. \tag{3.12}$$

Denote $f(a) = \binom{r/2}{a}\binom{k-r/2}{r/2-a}$ then $f(a+1) = f(a)\cdot\frac{(r/2-a)^2}{(a+1)(k-r+a)}$, so $\frac{f(a+1)}{f(a)} = \frac{(r/2-a)^2}{(a+1)(k-r+a)} > \frac{(1/2-2\epsilon')^2 r^2}{2\epsilon' rk} > 2$ when $a < 2a_0$. Also note $\binom{k}{r/2} = \sum_{a=0}^{r/2} f(a)$. Thus (3.12) $< a_0 \cdot \frac{f(a_0)}{f(2a_0)} < \epsilon' r \cdot 2^{-\epsilon' r} < \exp(-\Omega(k/t^2))$. Therefore,

$$\Pr[\ \boldsymbol{\alpha} \text{ leads to } P\ ] \leq$$

$$\exp(-\Omega(k/t^2)) + \Pr[\ \boldsymbol{\alpha} \text{ leads to } P,\ |\mathrm{dom}(\boldsymbol{\alpha}) \cap \{\text{useful pigeons}\}| \geq \epsilon' r\ ]$$

We bound the second term below. There are two cases:

$$|\mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1)| \geq \frac{\epsilon' r}{2}, \quad \text{Or} \tag{3.13}$$

$$|\mathrm{dom}(\boldsymbol{\alpha}) \cap (\{\text{narrow pigeons}\} \backslash \mathrm{dom}(P_1))| \geq \frac{\epsilon' r}{2}. \tag{3.14}$$

Here as usual, $\mathrm{dom}(\boldsymbol{\alpha})$ denotes the domain of $\boldsymbol{\alpha}$ (a subset of $[k]$). In the following, α' will denote an arbitrary choice of $\boldsymbol{\alpha}$ that satisfies the item's condition.

1. In the first case, (3.13), α' has to assign exactly the same vertices as P_1 to pigeons in $\mathrm{dom}(P_1) \cap \mathrm{dom}(\alpha')$. Since G is $(2r, q)^{block}$-neighbor-dense where $q = \frac{1}{2}n^{1-2\delta r}$, so in particular, there are $\geq \frac{1}{2}n^{1-c_0-2\delta r}$ many choices of vertices for *each* such pigeon. By definition

(3.7), $\boldsymbol{\alpha}$ chooses among them uniformly. Thus

$$\Pr[\ \boldsymbol{\alpha} \text{ leads to } P \text{ and } |\mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1)\}| \geq \epsilon' r/2\ ] \tag{3.15}$$

$$\leq \sum_{S \subseteq [k],\ |S| \geq \epsilon' r/2} \Pr[\mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1) = S\ \wedge\ \text{for all } i \in S,\ \boldsymbol{\alpha}(i) = P_1(i)] \tag{3.16}$$

$$= \sum_{S \subseteq [k],\ |S| \geq \epsilon' r/2} \Pr[\mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1) = S\ ] \cdot \Pr[\ \text{for all } i \in S,\ \boldsymbol{\alpha}(i) = P_1(i)] \tag{3.17}$$

$$\leq \sum_{S \subseteq [k],\ |S| \geq \epsilon' r/2} \Pr[\ \mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1) = S\ ] \cdot (\frac{1}{2} n^{1-c_0-2\delta r})^{\epsilon' r/2}$$

$$\leq 1 \cdot n^{-c_0 \epsilon' r} = n^{-\Omega(c_0 k/t^2)} \tag{3.18}$$

where (3.17) is from the independence of the two parts in the definition of $\boldsymbol{\alpha} \sim \mathcal{D}$.

2. In the latter case, (3.14), let B denote $\{\text{narrow pigeons (in } P)\} \backslash \mathrm{dom}(P_1)$. In the process of choosing vertices to a pigeon $i \in \mathrm{dom}(\alpha') \cap B$, vertices in $P_0(i)$ must not be chosen (by (2a) in the strategy). On the other hand, for any such pigeon i, it is narrow in P so $P_0(i)$ is $(r, \frac{1}{2}q)$-neighbor-dense. Therefore,

$$\hat{N}_{P_0(i)}(\mathrm{Im}(\alpha'|_{\mathrm{dom}(\alpha' \backslash \{i\})})) \geq \frac{1}{2} q = \frac{1}{4} n^{1-c_0-2\delta r}. \tag{3.19}$$

So for such i, as $|V_i| = n^{1-c_0}$,

$$\Pr[\ \boldsymbol{\alpha}(i) \notin P_0(i)\ |\ i \in \mathrm{dom}(\boldsymbol{\alpha})\ ] \leq 1 - \frac{n^{1-c_0-2\delta r}}{4n^{1-c_0}} = 1 - \frac{1}{4} n^{-2\delta r}. \tag{3.20}$$

Now we can bound the overall probability of this case by

$$\sum_{S \subseteq B,\ |S| \geq \epsilon' r/2} \Pr[\ \mathrm{dom}(\boldsymbol{\alpha}) \cap B = S \text{ and } \boldsymbol{\alpha}(i) \notin P_0(i) \text{ for all } i \in S\ ] \tag{3.21}$$

Similar to estimation (3.15), from (3.20) we have

$$(3.21) \leq (1 - \frac{1}{4}n^{-2\delta r})^{\epsilon' r/2} < \exp(-\Omega(k^{1-\epsilon}/t^2)), \tag{3.22}$$

where the last inequality uses $k = n^{c_0}$, $2\delta r < \epsilon c_0$ in (3.5).

Finally, note $c_0 < \log n$ so the sum of probability is $\exp(-\Omega(k^{1-\epsilon}/t^2))$. □

Since any choice of $\boldsymbol{\alpha}$ results in halting at some object in T, Lemma 3.4 implies $|T| \geq \exp(\Omega(k^{1-\epsilon})) = \exp(\Omega(n^{(1-\epsilon)c_0}))$. In particular, there are at least this many different objects in Γ. Theorem 3.2 is proved.

3.4 n^k-type lower bounds for a-irregular resolution

3.4.1 The model

Like before, let us view a resolution proof Γ as a top-down DAG ($\perp$ on top). A variable x is called *irregular* on a path L in Γ if it is queried more than once on L. For a node (clause) C in Γ, x is *irregular under* C if there is *some* path down from C on which x is irregular.

We are going to introduce the model of a-irregular resolution. Its main version assumes a variable partition in input. Let's start with a simpler one.

Definition 3.5. *For $a \leq 1$, a resolution proof Γ on m variables is* **unblocked a-irregular** *if for any clause $C \in \Gamma$, $w(C) \geq am \Rightarrow |\{\text{variables irregular under } C\}| \leq am$*

So regular resolution is 0-irregular, and general resolution is 1-irregular.

We continue to the main version. Given m variables and $\kappa : \text{Var} \to [k]$ a partition of variables ($1 \leq k \leq m$), we say x *belongs to block* $\kappa(x)$. Define the *block-size* of a variable set to be $|X|^b := |\kappa(X)|$, and the *block-width* to be

$$w^b(C) = |\text{Var}(C)|^b. \tag{3.23}$$

Definition 3.6. *(***Main model***) For $a \leq 1$, κ as above, a resolution proof Γ is* a**-irregular for** κ *if for any clause $C \in \Gamma$, $w^b(C) \geq ak \Rightarrow |\{\text{variables irregular under } C\})|^b \leq ak$.*

It is easy to see that this model is at least as strong as "resolution refutations with small block-width (for the same variable partition)"; and it always subsumes the unblocked $\frac{ak}{m}$-irregular model, regardless of the partition.

The unblocked a-irregular resolution (Definition 3.5) is already exponentially stronger than regular even for $a = k^{-\Omega(1)}$, and the situation is clearer for the main model. It turns out that the known exponential separations between the regular and general resolution ([2, 107]) are, actually, separations between regular and the a-irregular resolution with a natural partition κ and $a = k^{-\Omega(1)}$.

Remark 3.3. *We next give the details of how the a-irregular resolution can handle the hard instances from the known general-regular separations. The instances are Stone formulas ([2]), Lifted pebbling formulas ([107]), and a variation of the Ordering principle ([2]).*

1. **Stone formulas**. *Under the notation of [2], the $m = \Omega(n^2)$ many variables are $\{P_{i,s} \mid t \in S\}$ for each $i \in V(G)$ and $\{R_t \mid t \in S\}$, where $|S| = \Omega(|V(G)|) = \Omega(n)$. The variables are naturally partitioned into $k = n + 1$ blocks according to the vertex index, plus a block of all stones. Axioms have block-width ≤ 4, and the short resolution in [2] (their Lemma 4.1) is $5/k$-irregular for κ, since every clause in that resolution has block-width ≤ 4.*

This short resolution proof is also unblocked $m^{-1/2}$-irregular; actually, only the stone variables $\{R_t\}$ are irregularly resolved since a path in the proof naturally corresponds to a path in G and G is acyclic. There are $O(n) = O(m^{1/2})$ many stone variables.

2. **Lifted pebbling formulas**. *It is noted in [107] that the Stone formulas can be regarded as a "lifted" version of the so-called Pebbling formulas, Pebb_G, on the same graph G. They give a similar but different family of CNFs: in short, given boolean variables $x_1, ..., x_n$, consider a variable change by encoding every literal x_i^ϵ by $\wedge_{j \in N(i)}(\neg s_{i,j} \vee r_j^\epsilon)$ ($\epsilon \in \{0, 1\}$ and $x^0 := \neg x$), where $\{s_{i,j}, r_j^b\}$ are fresh variables corresponding to a bipartite*

graph H on components $[n]$, J ($[n] \cap J = \emptyset$), and we add the default axioms $\vee_{j \in N(i)} s_{i,j}$ for all i. If the left degree of H is d, then there are $nd + |J|$ many variables. The Stone Formulas are the resulting CNF expression from this variable change on $Pebb_G$, when H is complete; [107] showed the same separation holds if take H to be a more economic sparse bipartite expanders[6]*, with $d = \Theta(n/|J|)$ (their Theorem 12). For us, the short resolution refutation in example 1 now only simplifies, so the block width is still constant where blocks are the same $\{s_{i,j}\}$ (for each $i \in V(G)$ and $\{r_j\}$.*

Similar to example 1, the short proof is also unblocked $1/d$-irregular, and in applications $d \geq \Theta(\log \log n)$ (their Theorem 13).

3. **A variant of the Ordering principle**, *denoted by GT'_n. It has $m = n(n-1)$ variables $x_{i,j}$, $i \neq j \in [n]$, with the intended meaning $x_{i,j} \Leftrightarrow$ element i (in some n-element set) is greater than element j. We refer the reader to [2] to this CNF family; what's important for us is that if partition the variables according to the second subscript j, into $k = n$ blocks, then the axioms have constant block-width, and the short refutation (Corollary 3.4 in [2]) is $4/k$-irregular. Namely, that refutation first resolves $x_{i_1,i_2} \vee x_{i_2,i_3} \vee x_{i_3,i_1} \vee \rho(i_1, i_2, i_3)$ with $x_{i_1,i_2} \vee x_{i_2,i_3} \vee x_{i_3,i_1} \vee \neg\rho(i_1, i_2, i_3)$ for all i_1, i_2, i_3, where $\rho(\cdot)$ refers to some literal and all clauses have block-width ≤ 4, then it uses the short refutation from [102] to finish, in which all clauses are either the so-called $C_m(j)$'s (in notation of [102]) or axioms, all with block-width ≤ 4. So, the refutation is $4/k$-irregular for this partition.*

Remark 3.4. *In all the examples above, the variable partition not only has a natural semantic meaning but also makes axioms have constant block-width.*[7] *This might be considered together with the technique of variable substitutions in form $x_i = f(y_{i,1}, ..., y_{i,t})$ with $y_{i,j}$'s being distinct new variables (a.k.a. lifting; see e.g. [94, 60, 48]), where "blocks of variables" appear naturally. For the lifted CNF, it is reasonable to expect that the block-width measure*

6. The actual construction has one more twist called *mirroring*, which we ignore here.

7. Other partitions might also seem natural but fail the second property, and we do not know the power of the model with them.

on proofs w.r.t. this variable partition reflects the hardness of the original CNF which itself is often narrow. In our context, this perspective explains the power of the model in examples 1, 2. It seems to say nothing about example 3, though.

The main theorem of this section is the following.

Theorem 3.3. *Fix the natural partition $\kappa_0 : x_v \mapsto i$ if $v \in V_i$ in $V_1 \sqcup ... \sqcup V_k$. Let $\xi > 1$ be constant and $\epsilon > 0$ be any parameter s.t. $(\log n)^{-1/2} < \epsilon < 1/200$. Then for any k s.t. $\xi^2(100/\epsilon)^3 < k < n^{1/3-40\epsilon}$, w.h.p. over $\boldsymbol{G} \sim G(n, n^{-2\xi/(k-1)})$, any $\frac{\epsilon}{\xi}$-irregular resolution proof for $Clique_{block}(G,k)$ has size $n^{k\epsilon^3/(200\xi)^2}$.*

3.4.2 More graph properties

Definition 3.7. *(relativized neighbor-denseness, Definition 3.2) Given G and $a, b \in \mathbb{N}_+$, for $A, B \subseteq V$, B is called $(a,b)^A$-neighbor-dense if $\forall U \subseteq A$, $|U| \leq a \Rightarrow |\hat{N}_B(U)| \geq b$. When $A = V$, we simply say B is (a,b)-neighbor-dense.*

Note $A' \subseteq A$, then $(a,b)^A$-neighbor-denseness implies $(a,b)^{A'}$-neighbor-denseness.

Another pseudorandom property which played an important role in the proof for regular case says: for any (r,q)-neighbor-dense sets in G, all witness sets of its non-(tr, q')-neighbor-denseness are non-trivially concentrated (for suitable t, q').

Definition 3.8. *([8]) $W \subseteq V$ is called (tr, r, q', s)-mostly-dense in G, if $\exists S \subseteq V$, $|S| = s$ such that: $\forall U \subseteq V$ of size $\leq tr$, $|\hat{N}_W(U)| < q' \Rightarrow |U \cap S| \geq r$. For convenience, we say G itself is (tr, r, q', s)-mostly-dense if* **every** *(r,q)-neighbor-dense set is (tr, r, q', s)-mostly-dense (when q is clear from the context).*

Proposition 3.1. *(mostly-denseness is inheritable w.r.t witness S) Suppose $A \subseteq V$, and W is (tr, r, q', s)-mostly-dense. Then $\exists S_1 \subseteq A$ of size $\leq s$ such that, for any $U \subseteq A$, $|U| \leq tr$, if $|\hat{N}_W(U)| < q'$ then $|U \cap S_1| \geq r$.*

Proof. Take S_1 to be $S \cap A$, where S is as in Definition 3.8. □

As usual, denote $\frac{2\xi}{k-1}$ by δ. For simplicity, we always take $\xi > 1$ to be constant. The main result of [8] is the following.

Theorem 3.4. *For any parameter $\epsilon \in (0, 1/2)$ and constant $\xi > 1$, if $k < n^{1/4-\epsilon}$ and $k\sqrt{\xi} < n^{1/2-\epsilon}$, then:*
(1) (their Theorem 6.1) W.h.p., $\boldsymbol{G} \sim G(n, n^{-\frac{2\xi}{k-1}})$ is (tr, tq)-neighbor-dense and (tr, r, q', s)-mostly-dense, with $t = \frac{64\xi}{\epsilon}$, $r = \frac{4k}{t^2}$, $q = \frac{n^{1-\delta tr}}{4t}$, $s = (\frac{n}{\xi})^{1/2}$ and $q' = 3\epsilon s^{1+\epsilon} \log s$.
(2) (their theorem 5.4) Let $t: \ 4 \le t \le k$ be any parameter and $r = 4k/t^2$. If G is (tr, tq)-neighbor-dense and (tr, r, q', s)-mostly-dense, then any regular refutation of $Clique(G, k)$ requires size $\frac{1}{2}\min\{s^{\epsilon r/2}, \ (1 - rs^{-(1+\epsilon)}/2ek)^{-q'}\}$.

We will need Theorem 3.4(1) for the following parameters. Theorem 3.4(2) will be actually re-proved and refined following the original method (Lemma 3.8, 3.9).

Parameter regime. In the rest of section 3.4, we use a parameter regime that is similar to that of [8]. As before, let $\xi > 1$ be a constant and $\delta = \frac{2\xi}{k-1}$.

$$\begin{aligned} &\epsilon = \text{any parameter in } \Big((\log n)^{-1/2}, \ 1/200\Big); \\ &t = \frac{64\xi}{\epsilon}, \quad k \in \left(\frac{3t^2}{\epsilon}, \ n^{1/3-40\epsilon}\right); \\ &r = \frac{4k}{t^2}, \quad q = \frac{1}{32t} n^{1-8\delta tr}/k, \quad q' = \frac{1}{4} q n^{-\delta tr}; \\ &s = k^2 n^{9\delta tr+\epsilon}, \quad p = n^{-(9\delta tr+2\epsilon)}/k. \end{aligned} \tag{3.24}$$

We can assume k, r, q, q', s are integers whose meaning is clear from Definition 3.8; p is used for a biased-coin in the argument. As before, the "typical" case is when ϵ is a small constant, and the bound is $n^{\Omega(k/\xi^2)}$. Our choice of $p = n^{-(9\delta tr+2\epsilon)}/k$ is larger than that in the original Theorem 3.4(2) (which is roughly $n^{-(1+\epsilon)/2}$); this makes the two bounds in the proof of Lemma 3.9 more balanced thus slightly improves the range of k from $n^{1/4}$ to $n^{1/3}$.

Theorem 3.5. *With parameter regime* (3.24)*, w.h.p.* $\boldsymbol{G} \sim G(n, n^{-\delta})$ *is*

$$\begin{aligned} &(i).\ (8tr, 4tq)^{block}\text{-neighbor-dense; and} \\ &(ii).\ (tr, r, q', s)\text{-mostly-dense.} \end{aligned} \tag{3.25}$$

Proof. (i) is proved identically to Lemma 3.2. (ii) is Theorem 3.4(1) except for a difference in parameters; we only have to point out that parameters (3.24) satisfy $n^{\epsilon/2+1} < qn^{-\delta tr}s/tr$ so can be safely replaced to their proof. □

Theorem 3.3 thus reduces to the following.

Theorem 3.6. *Recall* $V(G) = V_1 \sqcup ... \sqcup V_k$*, and* κ_0 *is the "canonical" partition that maps* v *to* i *if* $v \in V_i$*. If* G *satisfies* (3.25) *with parameters* (3.24)*, then any* $\frac{1}{t}$*-irregular resolution for* $(Clique_{block}(G, k), \kappa_0)$ *requires size* $n^{\epsilon k/6t^2}$*.*

3.4.3 Lower bound proof (Theorem 3.6)

Proof overview.

As described in the introduction, the idea is simple: use a suitable restriction to reduce to the regular case. The induced sub-graph is not quite pseudorandom, but not far: the only additional observation is to use a weaker, relative notion of pseudorandomness (Lemma 3.6, 3.9).

As before, we give an adversary strategy followed by its analysis, where we will need to open up the argument in the regular case.

Definition 3.9. *(Narrow pigeons, with new parameters (cf. Def. 3.3) Suppose* Γ *is a resolution proof,* $P \in \Gamma$ *an object. A pigeon* $l \in [k]$ *is* **narrow in** P *if*

$$P_0(l) \text{ is } (4tr, 2tq)\text{-neighbor-dense, where recall } 2tq = \frac{1}{4}n^{1-8t\delta r}/k.$$

We use narrow$_P$ to denote the set of narrow pigeons in P.

Adversary strategy.

Stage I (find a restriction). Travel down the proof, and keep a live-clique assignment β_P (Definition 3.1) s.t.

$$\beta_P \supseteq P_1, \qquad \mathrm{dom}(\beta_P) = \mathrm{dom}(P_1) \cup \mathrm{narrow}_P. \tag{3.26}$$

where P is the current object. Suppose the query at P is "(l_1, v_1)?". If

$$|\mathrm{narrow}_P \cup \mathrm{dom}(P_1)| \geq tr \tag{3.27}$$

then go to Stage II; otherwise if $l_1 \in \mathrm{dom}(P_1) \cup \mathrm{narrow}_P$, answer according to β_P; otherwise, answer No. Let us show that during Stage I the property (3.26) always holds.

Claim 3.2. *If G is $(8\delta tr, 4tq)^{block}$-neighbor-dense, $l \notin$ narrow$_P$, then $P_{Live}(l)$ is $(4\delta tr, 2tq)$-neighbor-dense.*

Proof. Apply Lemma 3.1 to $A \leftarrow V_l$, $A_1 \leftarrow P_0(l)$, $a_1 = a_2 = 4\delta tr$, $b_1 = b_2 = 2tq$. □

Denote the next node by P^+. There is at most one new narrow pigeon l_1, so by Claim 3.2, $|\hat{N}_{P_{Live}(l_1)}(\mathrm{Im}\ \beta_P)| \geq 2tq > 1$. Take a $v \in \hat{N}_{P_{Live}(l_1)}(\mathrm{Im}\ \beta_P) \backslash \{v_1\}$, extend β_P by $l \to v$ then restrict it to narrow$_{P^+} \cup \mathrm{dom}(P_1^+)$ as β_{P^+}. (3.26) holds for P^+.

This completes Stage I.

Claim 3.3. *The query-answer process must transit to Stage II at some node P.*

Proof. Similar to Claim 3.1: if (3.27) fails then P falsifies no axiom. □

Stage II (reduction to the regular case). Suppose we arrive at this stage at node P^*. We find a variable restriction as follows. Note $|P_1 \cup \mathrm{narrow}_P|$ increases by at most 1 per

step in Stage I (it might decrease), so it must be the case that $|\text{narrow}_{P^*} \cup P_1^*| = tr = k/t$. Now $|P^*|^b \geq k/t$ and since Γ is $\frac{1}{t}$-irregular, all irregular variables below P^* belong to some fixed block set I_{P^*} of size $\leq tr$.

Claim 3.4. *There exists a live-clique assignment $\widetilde{\beta}$ for P^* s.t.*

$$\widetilde{\beta} \text{ extends } \beta_{P^*} \quad \text{and} \quad dom(\widetilde{\beta}) = dom(\beta_{P^*}) \cup I_{P^*}. \tag{3.28}$$

Proof. Extend the function β_{P^*} on $\mathrm{I}_{P^*} \backslash \mathrm{dom}(\beta_{P^*}) \subseteq \mathrm{I}_{P^*} \backslash \mathrm{narrow}_{P^*}$ one by one. In each step, the function to be extended has image size $\leq (|\mathrm{dom}((P^*)_1)| + |\mathrm{narrow}_{P^*}|) + |\mathrm{I}_{P^*}| \leq 2tr$, so it is possible to find a common neighbor in $P_{\mathrm{Live}}(l)$ for any $l \notin \mathrm{narrow}_{P^*}$ by Claim 3.2. □

Now we make a self-reduction of the problem to $\widetilde{G}$. Fix a $\widetilde{\beta}$ in Claim 3.4. Let

$$\widetilde{G} := G\,[\bigcup_{l \in [k] \backslash \mathrm{dom}(\widetilde{\beta})} \widetilde{V}_l], \qquad \text{where } \widetilde{V}_l = \hat{N}_{P^*_{\mathrm{Live}}(l)}(\mathrm{Im}\ \widetilde{\beta}),\ l \in [k] \backslash \mathrm{dom}(\tilde{\beta}). \tag{3.29}$$

Restrict more appropriate variables to 0 so that axioms become $Clique_{block}(\widetilde{G},\ k - |\mathrm{dom}(\tilde{\beta})|)$. The restricted proof under P^* is regular. Denote it by Γ^*.

Finally, we use a strategy on Γ^* from the regular case [8]. Suppose we travel down Γ^* from the root P^* along a path L to node Q, and is faced by a query "(l_1, v_1)?".

1. If $\exists v \in \widetilde{V}_{l_1}$ s.t. (l_1, v) was answered Yes along L, answer No (*forgotten-forced* answer);
2. Otherwise, if $v_1 \notin \hat{N}(\mathrm{Im}\ Q_1)$, answer No (*edge-forced* answer);
3. Otherwise, answer Yes w.p. p, No w.p. $1 - p$ independently (*random* answer).

This completes the adversary strategy.

Pseudorandomness of $\widetilde{G}$.

Recall $\widetilde{G}$ is the induced subgraph (3.29). Assume w.l.o.g. $\mathrm{dom}(\widetilde{\beta}) = [\tilde{k}+1, k]$. The lower bound depends only on the pseudorandomness of $\widetilde{G}$ in Lemma 3.5, 3.6 below.

Lemma 3.5. *Assume G is $(8tr, 4tq)^{block}$-neighbor-dense (t, q as in (3.24)). Then $\forall l \in [\widetilde{k}]$, $\widetilde{V}_l$ is $(2tr, 2tq)^V$-neighbor-dense in G (the upper "V" stressed here).*

In particular, $\widetilde{G}$ itself is $(2tr, 2tq)^{block}$-neighbor-dense.

Proof. Like in Claim 3.2, we apply Lemma 3.1 to $A \leftarrow V_l$ and $A_1 \leftarrow (P^*)_0(l)$ with $a_1 = a_2 = 4tr$, $b_1 = b_2 = 2tq$, where $l \notin \mathrm{dom}(\widetilde{\beta}) \supseteq \mathrm{dom}(\mathrm{narrow}_{P^*})$. As a result we have

$$P^*_{\mathrm{Live}}(l) \text{ is } (4tr, 2tq)\text{-neighbor-dense in } V. \tag{3.30}$$

Now for any $R \subseteq V$ of size $\leq 2tr$, $|\mathrm{Im}(\widetilde{\beta}) \cup R| \leq 2tr + 2tr = 4tr$, so $|\hat{N}_{\widetilde{V}_l}(R)| \overset{\text{by def.}}{=} |\hat{N}_{\hat{N}_{P^*_{\mathrm{Live}}(l)}(\mathrm{Im}(\widetilde{\beta}))}(R)| = |\hat{N}_{P^*_{\mathrm{Live}}(l)}(\mathrm{Im}\ \widetilde{\beta}\ \cup R)| \overset{\text{by (3.30)}}{\geq} 2tq$. □

Lemma 3.6. *Assume G is (tr, r, q', s)-mostly-dense. The relativized mostly-denseness holds for $(G, \widetilde{G})$: for all $(r, q)^V$-neighbor-dense set $W \subseteq \widetilde{V}$, $\exists S \subseteq \widetilde{V}$ of size $\leq s$ s.t. $\forall U \subseteq \widetilde{V}$, if $|U| \leq tr$ and $|\hat{N}_W(U)| < q'$ then $|S \cap U| \geq r$.*

Proof. Since G is (tr, r, q', s)-mostly-dense and W is $(r, q)^V$-neighbor-dense, W is (tr, r, q', s)-mostly-dense. In Proposition 3.1 take $A \leftarrow \widetilde{V}$, as a result there exists $S_1 \subseteq A = \widetilde{V}$ that satisfies the condition in the lemma. □

Remark 3.5. *This relative property is apparently weaker than (tr, r, q', s)-mostly-denseness of $\tilde{G}$ since $\{(r, q)^V$-neighbor-dense sets in $\widetilde{V}\} \subseteq \{(r, q)^{\widetilde{V}}$-neighbor-dense sets in $\widetilde{V}\}$).*

Lower bound analysis.

Now we use the method in [8] to show regular resolution lower bound on $\widetilde{G}$.

Notation. Let $\boldsymbol{L}$ denote the random path from P^* to axioms in *strategy on* Γ^*. A path (not necessarily from P^* to axioms) is *eligible* if it can be traveled through with nonzero probability. If Z is a node on L, $L(Z)$ denotes the sub-path from Z. For an eligible L, similar to Definition 3.1, let

$$L_1 := \{\ (l,v) \mid (l,v)^{yes} \text{ is answered along } L\ \}, \text{ and similarly } L_0; \tag{3.31}$$

$$\text{rand}(L) := \{\ (l,v) \mid (l,v)? \text{ is answered randomly along } L\ \}. \tag{3.32}$$

$L_0(l) := \{v \mid (l,v) \in L_0\}$. A subset of $\{(l,v) \mid v \in \widetilde{V}_l, l \in [\widetilde{k}]\}$ is called a *query set*.

Definition 3.10. *Let X be a query set. A path L is X^{yes}-compatible if $X \cap L_0 = \emptyset$, and is X^{no}-compatible if $X \cap L_1 = \emptyset$.*

So, if Γ^* is regular then $L_1 \cap L_0 = \emptyset$, meaning L is L_1^{yes}- and L_0^{no}-compatible. It's easy to verify that any eligible path L to axioms must end in a *clique axiom* $C_l := \bigvee_{v \in V_l} x_v$, $l \in [\widetilde{k}]$.

Lemma 3.7. *If L is an eligible path to axiom C_l as above, then along L there is no forgotten-forced answer to l. In particular, L is X^{no}-compatible for $X = \{l\} \times \widetilde{V}_l$.*

Proof. By regularity. □

So it suffices to upper bound the probability $\Pr[\ \boldsymbol{L} \text{ ends in } C_l\ ]$, $\forall l \in [\tilde{k}]$, which is done by the following two lemmas. Note Lemma 3.8 actually holds without assuming regularity.

Lemma 3.8. *For any query set X and eligible path L' from P^* to Z,*

$$\Pr\left[\boldsymbol{L}(Z) \text{ is } X^{\theta}\text{-compatible}, |\text{rand}(\boldsymbol{L}(Z)) \cap X| \geq a \mid \boldsymbol{L} \supseteq L'\right] \leq \begin{cases} p^a, & \text{if } \theta = yes, \\ (1-p)^a, & \text{if } \theta = no. \end{cases}$$

Proof. We prove for $\theta = no$; the other is the same. Note if L is in the support of the event on the LHS, then on L any query $(l,v)?$ in X must be answered *no* by compatibility. Let

$\Pr_{L',Z,a}$ denote the probability on the LHS (X fixed). If Z is an axiom, then $a = 0$ so the conclusion is obvious.

We pass the probability $\Pr_{L',Z,a}$ to the one or two possible successor(s) of Z, and so use reverse-induction on the length of L'. Suppose the query at Z is (l, v)?. If $(l, v) \notin X$ or the answer is a forced-No (which can be decided given L', Z), then the probability passes to the successor(s) with a unchanged. Otherwise, the answer is a random-No, and $\Pr_{L',Z,a} = (1-p) \cdot \Pr_{L'',Z',a-1}$, where L'' extends L' by $Z \to Z'$ and Z' is the unique possible successor. The inductive hypothesis on L' completes the proof. □

Lemma 3.9. $\forall l \in [\ \widetilde{k}\ ]$,

$$\Pr[\ \boldsymbol{L} \textit{ ends in axiom } C_l,\ (\forall Z \textit{ on } \boldsymbol{L})\ |Z_1| < r/2\ ] < |\Gamma^*|^2 \cdot n^{-\epsilon k/3t^2-1}. \tag{3.33}$$

Proof. (cf. [8]) Due to item (1) in Stage II's strategy, there are at most $\widetilde{k}$ Yes-answers along any support of $\boldsymbol{L}$. Given such a L, divide it into consecutive segments $L^1 \cup ...L^{2t}$, such that $|(L^i)_1| \leq \lceil \frac{\widetilde{k}}{2t} \rceil \leq tr/2$, $\forall i \in [2t]$. Here recall $(L^i)_1$ is defined by (3.31). Below we consider $(L^i)_0(l)$; note by choice of l, $\bigcup_{i\in[2t]}(L^i)_0(l) = \widetilde{V}_l$.

We can see by contradiction that one of $(P^i)_0(l)$, say $(L^{i^*})_0(l)$, is $(r, q)^V$-neighbor-dense: otherwise, they give a union of $2t$ many sets of size r, together having $< q \cdot 2t$ many common neighbors in $\widetilde{V}_l$, contradicting Lemma 3.5. Fix such an i^* for L.

Let Z, Z' be the start and end nodes of L^{i^*} (decided by L). For simplicity, denote (Z, Z') by pair(L), and let $A = \mathrm{Im}(Z_1) \cup \mathrm{Im}((L^{i*})_1)$. Also, abbreviate the event

"$\boldsymbol{L}$ ends in C_l, and $(\forall P$ on $\boldsymbol{L})\ |P_1| < r/2$" (i.e. the event in the lemma)

as $\boldsymbol{L}^<$. Since L ends in C_l, by regularity of Γ^*, $(L^{i*})_0(l) = Z'_0(l) \backslash Z_0(l)$. So,

$$\text{LHS of (3.33)} = \Pr[\ \boldsymbol{L}^<,\ |\hat{N}_{\boldsymbol{Z'}_0 \backslash \boldsymbol{Z}_0}(\boldsymbol{A})| \geq q'\ ] + \Pr[\ \boldsymbol{L}^<,\ |\hat{N}_{\boldsymbol{Z'}_0 \backslash \boldsymbol{Z}_0}(\boldsymbol{A})| < q'\ ] \tag{3.34}$$

$$= \sum_{Z,Z' \in \Gamma} \Big(\Pr[\, \boldsymbol{L}^{<},\ \mathrm{pair}(\boldsymbol{L}) = (Z,Z'), |\hat{N}_{Z_0' \setminus Z_0}(\boldsymbol{A})| \geq q' \,] + \Pr[\, \boldsymbol{L}^{<}, \mathrm{pair}(\boldsymbol{L}) = (Z,Z'), |\hat{N}_{Z_0' \setminus Z_0}(\boldsymbol{A})| < q' \,] \Big).$$

For fixed $(Z, Z') \in \Gamma$, we bound the above two terms separately.

First term. By Lemma 3.7, any No-answer in $(L^i)_0(l)$ is random or edge-forced. By definition of A, the $\geq q'$ many No-answers to $\hat{N}_{Z_0' \setminus Z_0}(\boldsymbol{A})$ along $\boldsymbol{L}^{0,i^*}(l)$ are all random. Also, by Lemma 3.7, any path to C_l is X^{no}-compatible, $X := \{l\} \times \widetilde{V}$. So the event of this term implies event $E :=$ "$\boldsymbol{L}$ is X^{no}-compatible, $|\mathrm{rand}(\boldsymbol{L}) \cap X| \geq q'$." By Lemma 3.8 ($Z \leftarrow P^*$),

$$\Pr[E] \leq (1-p)^{q'} < \exp(-pq') < \exp(-n^{1-2\epsilon-20\delta tr}/(64tk^2)) < n^{-\epsilon k} \tag{3.35}$$

where we used $\delta tr < \epsilon$, $k < n^{1/3-40\epsilon}$, $\epsilon > (\log n)^{-1/3}$ by (3.24).

Second term. By choice of i^*, $Z_0' \setminus Z_0$ is $(r,q)^V$-neighbor-dense. Now $|\boldsymbol{A}| \leq r/2 + tr/2 < tr$, so by the (tr, r, q', s)-mostly-denseness of G and Lemma 3.6, $\exists S \subseteq \widetilde{V}$, $|S| \leq s$ s.t. $|\boldsymbol{A} \cap S| \geq r$. As $|\mathrm{Im}(Z_1)| \leq r/2$ in the event $\boldsymbol{L}^{<}$, if let $\boldsymbol{S}_1 = \mathrm{Im}((\boldsymbol{L}^{i^*})_1) \cap S$ then $\boldsymbol{L}^{<} \Rightarrow |\boldsymbol{S}_1| \geq r/2$. Therefore, as every Yes-answer is random, this term is bounded by

$$\sum_{S_1 \subseteq S,\ |S_1| = r/2} \Pr[\, \{l_1\} \times S_1 \subseteq\ \boldsymbol{L}(Z)_1 \cap \mathrm{rand}(\boldsymbol{L}(Z)) \,]. \tag{3.36}$$

For any fixed S_1, this is $< p^{r/2}$ by Lemma 3.8 (the compatibility condition is from the fact after Definition 3.10). Now $\binom{s}{\frac{r}{2}} p^{r/2} < (2et^2 n^{-\epsilon})^{k/t^2} < n^{-\epsilon k/3t^2 - 10}$, by (3.24).

The lemma follows by a union bound over $Z, Z' \in \Gamma^*$ in (3.34). □

Theorem 3.6 is now a straightforward corollary.

Proof. (*of Theorem 3.6*) Recall G is $(8tr, 4tq)^{block}$-neighbor-dense and (tr, r, q', s)-mostly-dense, and Γ is $\frac{1}{t}$-irregular resolution w.r.t. the canonical partition. By Claim 3.3, we only need to bound $|\Gamma^*| (\leq |\Gamma|)$. Consider an eligible path L down from P^*. If for some Q on L,

$|Q_1| \geq r/2$, we call L *type-1*; otherwise it is *type-2*.

For a type-1 L, fix such a node Q. L is Q_1^{yes}-compatible (by $Q_1 \subseteq L_1$ and the fact after Def. 3.10), $|Q_1| \geq \frac{r}{2}$. Yes-answers are random in Stage II so Lemma 3.8 applies to the sub-path from P^* to Q (with $X \leftarrow Q_1$). By a union bound over $Q \in \Gamma^*$, a type-1 path appears w.p. $\leq |\Gamma^*| \cdot p^{\frac{r}{2}} < |\Gamma^*| \cdot n^{-\epsilon k/t^2}$.

For a type-2 L, by Lemma 3.9 it appears w.p. $< k|\Gamma^*|^2 n^{-\epsilon k/3t^2-1}$ (unioned over $l \in [k]$). Together, type 1,2 appear with probability 1, so $|\Gamma^*| \geq n^{\epsilon k/6t^2}$. □

CHAPTER 4

SUM-OF-SQUARES LOWER BOUND OF CLIQUE

The content of this chapter is from the work [87] that appeared at the 36th Computational Complexity Conference (CCC 2021).

4.1 Introduction

A variant of the clique problem on random graphs $G(n, 1/2)$ was proposed in [62, 71], known as the *planted clique problem*: if we additionally and independently plant a random clique X of size $\omega \gg \log n$ to G, can X be recovered? Information-theoretically it is possible, since for any fixed choice $X \subset [n]$, w.h.p. over G it holds that $|N(v) \cap X| < (\text{say})0.51|X|$ for all $v \notin X$. But computationally, the problem is still widely believed to be hard on average after being intensively studied, and it has inspired a broad range of research directions (cryptography [6], learning [23], mathematical finance [7], computational biology [89], etc.). So far, the best known polynomial-time algorithm works only when $\omega = \Omega(\sqrt{n})$ [3], which is a so-called spectral algorithm (see e.g. [59]).

The *sum-of-squares hierarchy* (SoS) [101, 88, 72] is a stronger family of semidefinite programming algorithms (SDP) which, roughly speaking, is SDP on the extended set of variables $\{x_S \mid S \subseteq [n],\ |S| \leq d\}$ according to the degree parameter d. They can be significantly more powerful than spectral algorithms and traditional SDPs (see e.g. [11, 59]), and the recent years have witnessed rapid development on SoS-based algorithms that turns out to provide a characterization of a large class of algorithmic techniques ([14, 59]). The *SoS proof system* as described in chapter 2 is the natural proof-theoretic counterpart of these algorithms. It is known that in most cases, including when all variables are boolean (i.e. $x_i^2 = x_i$ are axioms), such a refutation exists if the axioms have no common solution; see [85, 93] for more on the relation between SoS proofs and algorithms.

The average-case hardness of the planted clique problem has a very simple form in proof complexity, and a lower bound would automatically give the hardness on any class of algorithms based on the proof system. Given that the decision version of the spectral algorithm of [3] corresponds to a degree-2 SoS proof, a SoS degree lower bound potentially can bring us a much better understanding of algorithmic hardness. The standard problem formulation is the following.

Definition 4.1. *Given an n-vertex simple graph G and a number ω, the* **Clique Problem** *for degree-d SoS proof system has the following* **axioms**.

$$\begin{aligned} \text{(Boolean)} \qquad & x_i^2 = x_i \quad \forall i \in [n] \\ \text{(Clique)} \qquad & x_i x_j = 0 \quad \forall \{i,j\} \text{ non-edge} \\ \text{(Size)} \qquad & x_1 + ... + x_n = \omega \end{aligned} \tag{4.1}$$

A fundamental feature of SoS systems is the duality: to prove degree lower bounds it suffices to find a *pseudo-expectation* whose *moment matrix*[1] is positive semi-definite (PSD). With boolean variables (which is our case), this can be demonstrated on multi-linear polynomials as below. Let $\mathcal{X}^{\leq d} = \{x_S \mid S \subseteq [n],\ |S| \leq d\}$ for any $d \in \mathbb{N}$.

Definition 4.2. *A* **degree-d pseudo-expectation** *for the Clique Problem on G is a map $\widetilde{E} : \mathcal{X}^d \to \mathbb{R}$ satisfying the following four* **constraints** *when extended by $\mathbb{R}$-linearity.*

$$\text{(Default)} \qquad \widetilde{E} x_\emptyset = 1 \tag{4.2}$$

$$\text{(Clique)} \qquad \widetilde{E} x_S = 0, \quad \forall S : |S| \leq d,\ G|_S \text{ non-clique} \tag{4.3}$$

$$\text{(Size)} \qquad \widetilde{E}\Big((x_1 + ... + x_n) x_S\Big) = \omega \cdot \widetilde{E} x_S \quad \forall S :\ |S| \leq d-1 \tag{4.4}$$

where in (4.4), *$x_A \cdot x_B := x_{A \cup B}$. To define the last constraint, define the* **moment matrix**

1. The name is simplified from the more cautious one, *pseudo-moment matrix*.

M to be the $\binom{[n]}{\leq d/2} \times \binom{[n]}{\leq d/2}$ matrix[2] *with $M(A,B) = \widetilde{E}x_{A\cup B}$, then:*

$$\text{(PSDness)} \quad M \text{ is positive semi-definite.} \tag{4.5}$$

It is not hard to see that, if a degree-d pseudo-expectation exists, then there will be no degree-d SoS refutation as in (2.2), (2.3) for the Clique Problem.

A relaxation of the problem was studied in [13], asking if $\widetilde{E}$ like above exits except with one change by weakening the Size Constraints (4.4) to a single inequality $\widetilde{E}(x_1+...+x_n) \geq \omega$. Henceforth, we call the Clique Problem (Definition 4.1) **Exact Clique** and this relaxation **Non-Exact Clique**.[3]

How to deal with the exact problem is a subtle but important open problem. On itself, lower bounds on the non-exact (weak) formulation indeed gave an important algorithmic message, but still, they do not rule out the possibility that SoS algorithms, when equipped with the additional constraint family $f \cdot (x_1 + ... + x_n - \omega) = 0$ (arbitrary f), become stronger and output "infeasible"; cf. the similar discussion in the case of random CSP [65]. This "weak vs. strong" distinction also involves how one thinks *the* SoS SDP optimization problem should be formulated.

Perhaps more importantly, it is about the techniques for average-case SoS lower bounds. The current so-called *pseudo-calibration heuristic* [13] tends to deal successfully with "soft" constraints (inequalities, or usually a threshold on the dual objective value) while being poor at handling "hard" constraints (polynomial identities generated from a fixed objective value); we want to find techniques to deal with the latter. Progress toward this goal is made in [65] for random CSPs, where the idea is that the hard constraint is a sum of "local" ones, each of which can be satisfied by a distribution on "local" variables, where locality is

2. d is always assumed to be even.

3. There is no "planted clique" in the problem formulation now, but traditionally this is still called the planted clique problems due to the algorithmic motivation behind.

formulated from a familiar notion of *graph closure* on expanders (cf. [50, 100, 22, 12, 68]). For Exact Clique, whose constraints do not have a similarly clear global-local structure, it seems unlikely a similar strategy could work.

There are also some concrete applications of lower bounds on Exact Clique, e.g. to the approximated Nash-Welfare [67], and a successful technique here might help deal with the related problems [65, 66, 63] (graph coloring, stochastic block models, etc.).

Previous work

For lower bounds, on Exact Clique, [47] showed that the (weaker) *d-round Lovasz-Schrijver* system cannot refute it for $\omega = O(\sqrt{n/2^d})$, [79] proved degree-d lower bound on SoS for $\omega = \widetilde{O}(n^{1/d})$ which was later improved to $\widetilde{O}(n^{1/3})$ for $d = 4$ [43] and further to $\widetilde{O}(n^{\frac{1}{\lfloor d/2 \rfloor + 1}})$ for general d [57]. For Non-Exact Clique, [13] proved the almost tight lower bound $d = \Omega(\epsilon^2 \log n)$ for $\omega = n^{1/2-\epsilon}$, $\epsilon > 0$ arbitrary.

For upper bounds, if $\omega = \Omega(\sqrt{n})$ then degree-2 SoS can refute Exact Clique with high probability [46]. On the other hand, if $\omega > d \geq 2.1 \log n$, a degree-$d$ SoS refutation for Exact Clique is not hard to see, which we include below for completeness.

Observation 4.1. *(Upper bound for Exact Clique if $\omega > d = 2.1 \log n$) Note that $(x_1 + ... + x_n)^d = \omega^d$ modulo the Size Axiom. The LHS can be multi-linearly homogenized to degree-d by $x_S = \frac{1}{\omega - |S|} \sum_{i \notin S} x_{S \cup \{i\}}$ by this axiom again, after which w.h.p. all terms are 0 by Clique Axioms since there is no size-$2.1 \log n$ clique in $G \sim G(n, 1/2)$ w.h.p.. This gives the contradiction $0 = 1$. Note the proof is actually in the weaker system Nullstellensatz (see e.g. [15]).*

Results of the chapter

Our main result is the following.

Theorem 4.1. *Let $\epsilon > 0$ be any parameter, $\omega = n^{1/2-\epsilon}$. With probability (w.p.) at least $1 - n^{-4\log n}$ over $G \sim G(n, \frac{1}{2})$, any SoS refutation of Exact Clique requires degree at least $\epsilon' \log n / \log\log n$, where $\epsilon' = \min\{\epsilon^2, \frac{1}{40^2}\}/2000$.*

We also have the following result. It does not allow to improve the lower bound but provides a new, hopefully simplifying, perspective on certain techniques that were used for the non-exact problem.

Theorem 4.2. *(Informal) For the Non-Exact Clique problem,*

(1). There is a way to define the correct pseudo-expectation from simple incidence algebra on the vertex-set;

(2). For the resulting moment matrix M, there is a weakened version of the quadratic equation $M = NN^\top$ whose solvability is given by, and actually equivalent to, a general graph-decomposition fact from which a "first-approximate" diagonalization of M can be deduced.

4.2 Proof overview

The two results use almost completely different ideas, so we treat them separately in this proof overview. The first two subsections 4.2.1 and 4.2.2 are for the proof of the main result, Theorem 4.1. The proof of Theorem 4.2 is sketched in subsection 4.2.3.

Let us start with a common idea for designing pseudo-expectations. Suppose we deal with degree-d SoS i.e. deal with size $\leq d$-subsets of $[n]$, then as is usual in complexity theory, we take a parameter $\tau \gg d$ (think of $d \ll \tau \ll \log n$) and make our construction on all size $\leq \tau$-subsets, in hope to later have a good control on its behavior on all size $\leq d$ subsets. This idea is most clearly demonstrated in the non-exact case (section 4.3.1), and is also the reason for the τ-parameter for the exact case (in (4.6) below).

4.2.1 Exact pseudo-expectation

The constraints force us to design the pseudo-expectations in a top-down manner, as follows. Fix $\widetilde{E}x_S$ for all $|S| = d$ first, then recursively set $\widetilde{E}x_S \leftarrow \frac{1}{\omega-|S|}\sum_{i\notin S}\widetilde{E}x_{S\cup\{i\}}$ if $|S| < d$. The Clique Constraints (4.3) will be satisfied if $\widetilde{E}_d x_S$ factors through $1_{G \text{ is clique on } S}$ as functions on G. Inspired by (almost all) previous work in the literature, we use Fourier characters and consider

$$\widetilde{E}x_S = \sum_{T:|V(T)\cup S|\le\tau} F(|V(T)\cup S|)\cdot\chi_T \quad \forall S\subseteq[n],\ |S| = d \tag{4.6}$$

for some function $F:\mathbb{N}\to\mathbb{R}$. We call F a **d-generating function**.[4] Thus

$$\widetilde{E}x_S = \frac{1}{\binom{w-d+u}{u}}\sum_{T:|V(T)\cup S|\le\tau}\chi_T\cdot\Bigg[\sum_{c=0}^{u}\binom{|V(T)\cup S|-d+u}{c}\binom{n-|V(T)\cup S|}{u-c} \cdot F(|V(T)\cup S|+u-c)\Bigg]$$

where $u := d-|S|$, for all S with $|S|\le d$. One key novelty we bring is the choice

$$F(x) = \frac{(x+8\tau^2)!}{(8\tau^2)!}\cdot(\frac{\omega}{n})^x. \tag{4.7}$$

The moment matrix $\widetilde{M}$ will be $\widetilde{M}(A,B) = \sum_{T:|V(T)\cup A\cup B|\le\tau}\widetilde{M}(A,B;T)\chi_T$ for $A,B\subseteq[n]$, $|A|,|B|\le d/2$, where $\widetilde{M}(A,B;T) =$

$$\frac{1}{\binom{\omega-d+u}{u}}\Bigg[\sum_{c=0}^{u}\binom{|V(T)\cup A\cup B|-(d-u)}{c}\binom{n-|V(T)\cup A\cup B|}{u-c} \cdot\underbrace{\frac{\big(|V(T)\cup A\cup B|+u-c+8\tau^2\big)!}{(8\tau^2)!}\cdot(\frac{\omega}{n})^{|(V(T)\cup A\cup B)|+u-c}}_{F\left(|V(T)\cup A\cup B|+u-c\right)}\Bigg], \tag{4.8}$$

4. To be distinguished from the usual generating functions for sequences.

where $u = d - |A \cup B|$.

This seemingly mysterious choice of F is ultimately for proving the PSDness of $\widetilde{M}$, but it probably can be seen only after a series of technical transformations (Remark 4.1, 4.4). It will be very interesting to know if there is *a priori* an explanation of it. See Remark 4.3, 4.11 for why some traditional choices from the literature that simulate some planted distributions apparently cannot work here.

4.2.2 Moment matrix analysis

1. Hadamard decomposition and Euler transform. For the exact problem, by the standard SoS homogeneity reduction (Lemma 4.9), it suffices to prove PSDness of the $\binom{[n]}{d/2} \times \binom{[n]}{d/2}$ principal minor of $\widetilde{M}$. Denote this minor by M. One unpleasant feature of M is that in its expression (4.8) the parameter $u = |A \cap B|$ appears in a deeply nested way. To analyze M (in particular, get a clue of how to diagonalize it), we resolve this intricacy in two steps.

First, $M = \sum_{c=0}^{\frac{d}{2}} m_c \circ M_c$ where "$\circ$" is the Hadamard product, and m_c, M_c are matrices as follows. For all $|I|, |J| = d/2$,

$$m_c(I, J) = \frac{1}{\binom{\omega - d + u}{u}} \omega^{u-c} \quad \text{where } u \text{ denotes } |I \cap J|; \tag{4.9}$$

$$M_c(I, J) = \begin{cases} \sum_{T : |V(T) \cup I \cup J| \le \tau} \chi_T \cdot M_c(|I \cap J|, |V(T) \cup I \cup J|), & \text{if } |I \cap J| \ge c; \\ 0, & \text{o.w.} \end{cases} \tag{4.10}$$

whose coefficients are

$$M_c(u, a) = \binom{a - (d-u)}{c} \binom{n-a}{u-c} n^{-(u-c)} \frac{(a + u - c + 8\tau^2)!}{(8\tau^2)!} (\frac{\omega}{n})^a$$

where $u = |I \cap J|$, $a = |V(T) \cup I \cup J|$.

The intuition is to let m_c carry (as much as possible) the "purely" vertex-set-based

information, $|I \cap J|$, so that the second factor M_c will be left with (mainly) edge-set-based information. As can be expected, in the analysis we will also treat m_c, M_c's separately.

The more difficult part is M_c. In fact, we will further remove the dependence on $|I \cap J|$ in $M_c(I, J)$ by one more step: a decomposition $M_c = \sum_{R \in \binom{[n]}{\leq \frac{d}{2}}} M_c^R$ where each M_c^R is supported on rows and columns whose index contains R, and the expression of M_c^R's can be derived from M_c by *Euler transform*. In summary, we will prove:

Lemma 4.1. *($\Sigma\Pi$-decomposition of M, Lemma 4.13)*

$$M = \sum_{c=0}^{\frac{d}{2}} m_c \circ \left(\sum_{R \in \binom{[n]}{\leq d/2}} M_c^R \right) = \sum_{R \in \binom{[n]}{\leq d/2}} \left(\sum_{c=0}^{|R|} m_c \circ M_c^R \right) \tag{4.11}$$

where each m_c is by (4.9) and M_c^R has the following expression. First, $M_c^R = 0$ if $|R| < c$. Also if $R \not\subseteq I \cap J$ then $M_c^R(I, J) = 0$. Finally, if $|R| \geq c$ and $R \subseteq I \cap J$, then $M_c^R(I, J) = \sum_{T: |V(T) \cup I \cup J| \leq \tau} M_c^R(I, J; T)\chi_T$ where, denoting $a = |V(T) \cup I \cup J|$, $M_c^R(I, J; T) = (\frac{\omega}{n})^a \cdot Y_c(|R|, a)$ and

$$Y_c(r, a) = \begin{cases} \sum_{l=c}^{r} (-1)^{r-l} \binom{r}{l} \binom{a+l-d}{c} \binom{n-a}{l-c} n^{-(l-c)} \frac{(a+l-c+8\tau^2)!}{(8\tau^2)!}, & \text{if } r \geq c; \\ 0, & \text{o.w.} \end{cases} \tag{4.12}$$

Moreover, for all $0 \leq c \leq r \leq d/2$ and $0 \leq a \leq \tau$, $|Y_c(r, a)| < \tau^{5\tau}$.

The intuition behind (4.11) is that, the first factor m_c "decreases" in c and m_0 is "very positive", while for fixed R, M_0^R is positive and other M_c^R's ($c > 0$) are "not too large". This is expounded by the following two lemmas.

Lemma 4.2. *For each $c = 0, ..., d/2$, $m_0 = \omega m_1 = ... = \omega^{\frac{d}{2}} m_{\frac{d}{2}} \succ \frac{d}{2\omega}\mathrm{Id}$.*

Lemma 4.3. (Main Lemma) *In* (4.11), *w.p.* $> 1 - n^{-5\log n}$ *the following hold. For all* $R \in \binom{[n]}{\leq d/2}$, *let* $P^R = \{I \in \binom{[n]}{d/2} \mid R \subseteq I\}$,

$$(1). \quad M_0^R \succeq n^{-d}\mathrm{diag}(\widetilde{\mathrm{Cl}})_{P^R \times P^R}; \tag{4.13}$$

$$(2). \quad \pm\omega^{-c} M_c^R \preceq n^{-c/6} \cdot M_0^R, \quad \forall 0 < c \leq |R|. \tag{4.14}$$

These two lemmas directly imply $M(G) \succeq n^{-d-1}\mathrm{diag}(\widetilde{\mathrm{Cl}}(G))_{\binom{[n]}{d/2}\times\binom{[n]}{d/2}}$ w.h.p., and Theorem 4.1 is an easy corollary of this (Cor. 4.1, 4.2).

The proof of Lemma 4.2 is relatively easier using *Johnson schemes* (similar to [79], see Lemma 4.12). Below we give the idea for proving the Main Lemma.

2. Recursive factorization: an extension. To prove the Main Lemma, an important first step is to derive an approximate diagonalization of M_c^R, for which we use the *recursive factorization* technique of [13]. In section 4.7 we will derive an approximate PSD factorization $M^R \approx \widetilde{L^R}\,(-)\left(\widetilde{L^R}\right)^\top$. This we roughly describe as below.

Lemma 4.4. *(Recursive factorization, Lemma 4.20) For any* $R \in \binom{[n]}{\leq d/2}$ *and* $0 \leq c \leq |R|$, *we have the following decomposition.*

$$M_c^R = \widetilde{L^R} \cdot \left[D^\tau \left(Q_{c,0}^R - Q_{c,1}^R + ... \pm Q_{c,d}^R\right) D^\tau\right] \cdot \left(\widetilde{L^R}\right)^\top + \mathcal{E}_c^R \tag{4.15}$$

where $\widetilde{L^R}$ *is some matrix of dimension* $\binom{[n]}{\frac{d}{2}} \times \left(\binom{[n]}{\leq \frac{d}{2}} \times (\tau+1)\right)$, D^τ *is the diagonal matrix* $\mathrm{diag}\left((\frac{\omega}{n})^{\frac{|A|}{2}}\right)_{A\subseteq[n],|A|\leq d/2} \otimes \mathrm{Id}_{\{0,...,\tau\}\times\{0,...,\tau\}}$, *and the "middle matrices"* $Q_{c,k}^R$*'s are* $(\tau+1)\times(\tau+1)$*-blocked, each block of dimension* $\binom{[n]}{\leq \frac{d}{2}} \times \binom{[n]}{\leq \frac{d}{2}}$. *The "error"* $\mathcal{E}_c^R(G)$ *is supported within rows and columns that contains* R *and is clique (given* G*), and w.p.* $> 1 - n^{-9\log n}$, $\left\|\mathcal{E}_c^R\right\| < n^{-\epsilon\tau/2}$.

For the reason of the "larger" dimension of matrices, see Remark 4.11.

3. Proving PSDness: encounter with Hankel matrices. With Lemma 4.2 and 4.4 at hand, the following is the key step towards the Main Lemma.

Lemma 4.5. *W.p.* $> 1 - n^{-8\log n}$ *over* G*, the following holds: for all* $R \in \binom{[n]}{\leq d/2}$*,*

(1). $Q^R_{0,0} - Q^R_{0,1} + ... \pm Q^R_{0,\frac{d}{2}} \succeq \tau^{-7\tau} \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right)_{S^R \times S^R}$*, where* $S^R = \{(A,i) \in \binom{[n]}{\leq d/2} \times \{0,...,\tau\} \mid A \supseteq R, |A| + i \geq \frac{d}{2}\}$*;*

(2). $\forall 0 < c \leq |R|$*,* $\pm\omega^{-c}\left(Q^R_{c,0} - Q^R_{c,1} + ... \pm Q^R_{c,\frac{d}{2}}\right) \preceq n^{-c/4} \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right)_{S^R \times S^R}$*.*

To prove this lemma, modulo somewhat standard steps (three Lemmas 4.23, 4.24, 4.25) the final technical challenge is: *show the positiveness of* $\mathbb{E}[Q^R_{0,0}]$ (Corollary 4.3).

We describe below how this is done. After simplification, the real task is to analyze the positiveness of the following matrix[5]:

$$\sum_{l=0}^{r} (-1)^{r-l} \frac{\binom{r}{l}}{l!} \cdot H_{\tau,\ l+8\tau^2} \quad \text{for any } 0 \leq r \leq d/2 \tag{4.16}$$

where $\{H_{m,t}\}$ is the family of $(m+1) \times (m+1)$-matrices

$$H_{m,t}(i,j) = (i+j+t)! \quad \forall 0 \leq i,j \leq m.$$

This is a special family of the so-called *Hankel matrices* whose (i,j)th element depends only on $i+j$. General Hankel matrices seem to arise naturally in moment problems but are notoriously wild-behaving in many aspects (see e.g. [103]). Fortunately enough, for the special family here we can manage to get a relatively fine understanding; we term this family **factorial Hankel matrices**. The key observation is that they have a concrete recursive diagonalization (Proposition 4.8), resulting in the following.

5. The subscripts are not exactly as in the problem but suffice to demonstrate the spirit.

Proposition 4.1. *If parameters m, t, r satisfy*

$$t + 1 > 8 \cdot \max\{r^2, m\}, \tag{4.17}$$

then $H_{m,t+1} \succeq 2r^2 H_{m,t}$.

Remark 4.1. *Condition* (4.17) *is why "$8\tau^2$" is used in the numerator of F,* (4.7)*.*

With this proposition, it is relatively easy to complete the proof of the Lemma 4.5, hence the Main Lemma. This completes the proof overview of Theorem 4.1.

4.2.3 A new perspective

We now explain Theorem 4.2, that is, to give a different perspective on certain techniques used in the non-exact case.

On defining the pseudo-expectation. Previously, the pseudo-expectation was obtained via the so-called *pseudo-calibration* method. We define the same $\widetilde{E}$ but from a different perspective, the incidence algebra on the vertex-set, which is also a simple refinement of the construction in [47].

The *ζ-matrix* on $[n]$ is the $2^{[n]} \times 2^{[n]}$ 0-1 matrix with $\zeta(A, B) = 1$ iff $A \subseteq B$. We observe that ζ reveals the basic linear structure of the true expectation on cliques if G is a single planted clique. So we use ζ to define $\widetilde{E}$. That is, we define a *degree-τ* approximate-distribution vector $p_\tau(G)$ first—it approximates the distribution of τ cliques inside a planted clique, with a standard twist so that it is only supported on cliques of the given G (4.25)—then take the vector $\zeta_{d,\tau} \cdot p_\tau(G)$ as $\widetilde{E}x$ (Def. 4.5). Here, $(\cdot)_\tau$ means to truncate the matrix or vector to indices of size $\leq \tau$. In this way, $\widetilde{E}$ inherits the linear structure posed by ζ too.

On deducing the first-approximate diagonalization. The goal is to come up with a coarse, "first-approximate" diagonalization of the moment matrix. We deduce its form in two steps: 1. Analyze the expectation of the matrix; 2. Observe that the (imaginary)

diagonalization of the matrix is in essence a quadratic equation, which we weaken to a proper "modular" version to solve.

We call step 2 the **mod-order analysis** (see section 4.6.1). The underlying idea is inspired by and similar to the more broad dimension-analysis in physical sciences: weaken the equation to its most significant part in a well-defined way (Def. 4.19). The main ingredient for defining the weakening is the norm information on certain pseudo-random matrices (the *graph matrices*), and the resulting equation has a nice structure to work with (see Lem. 4.16 and Cor. 4.6). Using standard techniques for studying algebraic equations—a simple *polarization* (Appendix)—we can deduce a solvability condition for the polarized equation, which translates to the existence of a general graph-theoretic structure (equation (4.163), Fact 4.9.1). The "coarse" diagonalization is then formulated based on this structure.

To demonstration this, it suffices to concentrate on the $\binom{[n]}{d/2} \times \binom{[n]}{d/2}$-minor of the moment matrix: $M'(I,J) = \sum_{T:|V(T)\cup I\cup J|\le\tau} (\frac{\omega}{n})^{|V(T)\cup I\cup J|}\chi_T$ where $|I| = |J| = d/2$.

Step 1: expectation. By using *Johnson schemes* as in [79], we get an explicit decomposition $\mathbb{E}[M'] = CC^\top$ where C is $\binom{[n]}{d/2} \times \binom{[n]}{\le d/2}$, and actually with a fine understanding of the spectrum of $\mathbb{E}[M']$.

Step 2: mod-order analysis. Given that $\mathbb{E}[M'] = CC^\top$, ideally we hope to solve the quadratic matrix equation (about the matrix variable N)

$$M' = NN^\top \tag{4.18}$$

and $\mathbb{E}[N] = C$, N extending C by non-trivial Fourier characters. Two observations follow.

(1) Order in $\frac{\omega}{n}$. Entries of M' all have a clear order in $\frac{\omega}{n}$. Like in fixed-parameter problems, we treat $\frac{\omega}{n}$ as a distinguished structural parameter and try to solve the correct power of $\frac{\omega}{n}$ in N first.

(2) Norm-match. A closer look into $CC^\top$ shows

$$\left\|C_r C_r^\top\right\| \approx \binom{d/2}{r} \cdot (\frac{\omega}{n})^{d-r} n^{d/2-r}, \quad r = 0, ..., d/2, \tag{4.19}$$

where $C = (C_0, ..., C_{d/2})$, each C_r having column dimension $\binom{[n]}{r}$. Assume $N = (N_0, ..., N_{d/2})$. Then we expect $N_r N_r^\top$ to concentrate around $C_r C_r^\top$ for each r, and so expect the norm of the non-constant part of $N_r N_r^\top$ to be bounded by (4.19). Under this condition, the known tight norm bounds on related matrices would tell us, for each possible appearing term in N, the least order of $\frac{\omega}{n}$ in its coefficient.

With these two observations, we can weaken equation (4.18) to a simple "modular version" that is more informative about the (imaginary) N. Namely, abstract $(\frac{\omega}{n})$ as a fresh variable α and work in ring $\mathbb{R}[\alpha, \{\chi_T\}]$, consider

$$(M' \mod \text{high order}) = (N \mod \text{high order}) \cdot (N^\top \mod \text{high order}) \tag{4.20}$$

where "order" means power of α (think of α as an "infinitesimal"). We call (4.20) the *mod-order equation* and its analysis the *mod-order analysis*. For details see Definition 4.19.

We feel that this approach leads us more naturally to the realization of using the graph-theoretic structure beyond guesses, and the simple idea behind the mod-order analysis might hopefully find other applications.

Structure of the chapter

In section 4.3 we define the pseudo-expectations and prove Theorem 4.2(1). In section 4.4 we recall some fundamental tools for analysis. The proof of the main Theorem 4.1 consists of three steps: section 4.5 the first step (combinatorial transforms), section 4.6, 4.7 the second (recursive factorization), and section 4.8 the last (structural and pseudo-random matrices).

The proof of Theorem 4.2(2) can be read independently and is in section 4.6.1.

Notation. I, J, A, B, S will stand for vertex-sets, and T for edge-sets. $E(S) := \binom{S}{2}$. "$\subseteq E([n])$" will be omitted in summation over edge sets on $[n]$ when there is no confusion.

Parameter regime. Throughout the chapter,

$$\begin{aligned}
&\epsilon = \text{any positive parameter (wlog } \epsilon < \frac{1}{40}\text{)};\\
&\omega = n^{1/2-4\epsilon};\\
&\tau = \frac{\epsilon}{200}\log n/\log\log n;\\
&d = \frac{\epsilon}{100}\tau.
\end{aligned}$$

4.3 Pseudo-expectations

As a warm-up, in section 4.3.1 we construct the non-exact pseudo-expectation. In section 4.3.2 we give the construction for the exact case.

4.3.1 Non-exact case

Given a graph G we can think of a degree-d pseudo-expectation as assigning a number $\widetilde{E}x_S$ to each subset $S \subseteq [n]$ of size $\leq d$, so that the resulting vector $\widetilde{E}x$ *looks indistinguishable* to the expectation resulted from the case when a random-ω clique is planted, from the view of degree-d SoS. As explained at the beginning of section 4.2, to make such an assignment we first go beyond to slightly larger subsets of size τ, define an "approximate distribution" on size $\leq \tau$-cliques, then use it to generate pseudo-expectation on all size $\leq d$-subsets.

ζ-function and Möbius inversion

Given n-vertex graph G, let $p(G) \in \mathbb{R}^{2^{[n]}}$ be the max-clique-indicator vector. Then $q(G) := \zeta \cdot p(G)$ is a vector supported exactly on all cliques in G, where ζ is the $2^{[n]} \times 2^{[n]}$ matrix

$$\zeta(A, B) = 1 \text{ iff } A \subseteq B, \quad \forall A, B \subseteq [n]. \tag{4.21}$$

In particular, if G is a single clique then $q(G)$ is the clique-indicator. We will use $\zeta_{a,b}$ to denote the submatrix of ζ on rows $\binom{[n]}{\leq a}$ and columns $\binom{[n]}{\leq b}$, and use similar notation on all related vectors. Consider the when G is just a randomly planted clique, whose distribution can be represented by a *plant-distribution* vector $p_{\text{plant}} \in \mathbb{R}^{2^{[n]}}$, and let the *output-expectation* q_{out} be the vector of cliques in G in expectation. Then $q_{\text{out}} = \zeta \cdot p_{\text{plant}}$. We call such a pair $(p_{\text{plant}}, q_{\text{out}})$ a **plant-setting**.

Definition 4.3. *(Two plant-settings) The* **exact plant-setting** (p_0, q_0) *is*

$$p_0(S) = \frac{1}{\binom{n}{\omega}} \text{ if } |S| = \omega \text{ and } 0 \text{ otherwise}, \quad q_0(S) = (\zeta p_0)(S) = \frac{\binom{n-|S|}{\omega-|S|}}{\binom{n}{\omega}}. \tag{4.22}$$

I.e. in this setting a random size-ω subseteq is chosen to be the planted clique.

The **independent plant-setting** (p_1, q_1) *is*

$$p_1(S) = (\frac{\omega}{n})^{|S|}(1 - \frac{\omega}{n})^{n-|S|}, \quad q_1(S) = (\zeta p_1)(S) = (\frac{\omega}{n})^{|S|} \tag{4.23}$$

for all $S \subseteq [n]$. I.e. any vertex is included in the planted clique w.p. $\frac{\omega}{n}$ independently.

Thus the matrix ζ reveals the basic linear relations between $(p_{\text{plant}}, q_{\text{out}})$. It is upper-triangular (with row- and column-indices ordered in a size-ascending way), invertible, with the inverse the **Möbius inversion** matrix: $\zeta^{-1}(A, B) = (-1)^{|B \setminus A|}$ if $A \subseteq B$, and 0 otherwise. Note $(\zeta_{a,a})^{-1} = (\zeta^{-1})_{a,a}$, $\forall a \leq n$. Moreover, if let the pseudo-expectation be defined

as $\widetilde{E}x = p \in \mathbb{R}^{2^{[n]}}$ for some vector p, then the "full" $2^{[n]} \times 2^{[n]}$ moment matrix is

$$M_{SOS} = \zeta \mathrm{diag}(p) \zeta^\top. \tag{4.24}$$

In particular, if p is a nonnegative vector then M_{SOS} is immediately PSD.

Non-exact pseudo-expectation for (p_1, q_1)

Given G, we first construct a *degree-τ* "approximate plant-distribution", $p_\tau(G)$, that simulates the plant-distribution **and** that $p_\tau(G)$ is supported on size $\leq \tau$-cliques in G. Then we can take $\widetilde{E}x = \zeta_{d,\tau} \cdot p_\tau(G)$ so that the result inherits the linear structure posed by ζ.

What is this $p_\tau(G)$? From the view of approximation it seems taking $\zeta_{\tau,\tau}^{-1}(q_1)_\tau$ would suffice, while to make it supported on cliques, same as in [47] we add a clique-indicator factor, thus

$$p_\tau(G)(S) = \left(2^{|\binom{S}{2}|} \mathrm{Cl}_S(G) \cdot \zeta_{\tau,\tau}^{-1}(q_1)_\tau\right)(S) \quad \forall S \subseteq [n] \text{ of size} \leq \tau \tag{4.25}$$

where $\mathrm{Cl}_S(\cdot)$ is the clique indicator function and $2^{|\binom{S}{2}|}$ is for re-normalization.

Definition 4.4. *For any $S \subseteq [n]$, the* **scaled clique-indicator** *is $\widetilde{\mathrm{Cl}}_S(G) := 2^{|\binom{S}{2}|}\mathrm{Cl}_S(G)$, which is a function on G. $\widetilde{\mathrm{Cl}}(G)$ is the (column) vector of them over a family of S's, which will always be clear from the context.*

Definition 4.5. *The* **non-exact pseudo-expectation** *is*

$$\widetilde{E}_{\text{nonexact}} = \zeta_{d,\tau} \cdot p_\tau(G) = \zeta_{d,\tau} \cdot (\widetilde{\mathrm{Cl}}(G) \circ \zeta_{\tau,\tau}^{-1}) \cdot (q_1)_\tau \quad \in \mathbb{R}^{\binom{[n]}{\leq d}} \tag{4.26}$$

where "$\circ$" is the Hadamard product[6].

6. In general $(M_1 \circ M_2) \cdot M_3 \neq M_1 \circ (M_2 \cdot M_3)$, but they are equal if M_1 is a column vector.

In short, $\widetilde{E}_{\text{nonexact}}$ refined the construction in [47] by one step: factor through size-τ subsets (in the *only* non-trivial way) so that the size-d output inherits linear relations posed by ζ. Similarly to (4.24), the resulting moment matrix is

$$M_{\text{nonexact}}(G) = \zeta_{d/2,\tau} \cdot \operatorname{diag}\left(p_\tau(G)\right) \cdot \left(\zeta_{d/2,\tau}\right)^\top. \tag{4.27}$$

Remark 4.2. *$\widetilde{E}_{\text{nonexact}}$ looks like a true expectation on cliques in G, namely, if $p_\tau(G)$ were nonnegative then the PSDness of $M_{\text{nonexact}}(G)$ would be immediate. Alas, this is not true by computation*[7]*. That the PSDness could still possibly hold is because $\zeta_{d/2,\tau}$ in (4.27) is degenerate.*

Lemma 4.6. *(Theorem 4.2(1)) For all $S \subseteq [n]$ s.t. $|S| \le d$,*

$$\widetilde{E}_{\text{nonexact}} x_S = \sum_{T:|V(T)\cup S|\le\tau} \left(\frac{\omega}{n}\right)^{|V(T)\cup S|} \chi_T. \tag{4.28}$$

Proof. Note $\widetilde{\text{Cl}}_S = \sum_{T\subseteq E(S)} \chi_T$ for all S. Now for S, S' with appropriate size bound,

$$\left(\widetilde{\text{Cl}} \circ \zeta_{\tau,\tau}^{-1}\right)(S, S') = \begin{cases} \sum_{T\in E(S)} \chi_T \cdot (-1)^{|S'\setminus S|}, & \text{if } S \subseteq S' \\ 0, & \text{o.w.} \end{cases};$$

$$\begin{aligned} \left(\zeta_{d,\tau} \cdot (\widetilde{\text{Cl}} \circ \zeta_{\tau,\tau}^{-1})\right)(S, S') &= \sum_{S'':S\subseteq S''\subseteq S'} \left(\sum_{T\subseteq E(S'')} \chi_T \cdot (-1)^{|S'\setminus S''|} \right) \\ &= \sum_{T:V(T)\cup S\subseteq S'} \chi_T \cdot \left(\sum_{S'':V(T)\cup S\subseteq S''\subseteq S'} (-1)^{|S'\setminus S''|} \right) \\ &= \sum_{T:V(T)\cup S\subseteq S'} \chi_T \cdot \delta_{S'=V(T)\cup S} = \sum_{T:V(T)\cup S=S'} \chi_T. \end{aligned}$$

7. One intuition, suggested by a referee, is that any true expectation on cliques has objective value $\sum_{i=1}^n x_i = O(\log n)$ w.h.p., now if $p_\tau(G)$ were nonnegative then it would be almost a distribution since $\widetilde{E}_{\text{nonexact}}(x_\phi) \approx 1$ (can be checked by (4.28)) with a problematically big objective value $n^{\frac{1}{2}-\epsilon}$.

Therefore, $\widetilde{E}_{\text{nonexact}} x_S =$

$$\begin{aligned}\left(\zeta_{d,\tau} \cdot (\widetilde{\text{Cl}} \circ \zeta_{\tau,\tau}^{-1})(q_1)_\tau\right)(S) &= \sum_{S':|S'|\leq\tau} \left(\sum_{T:V(T)\cup S=S'} \chi_T \cdot (\frac{\omega}{n})^{|S'|} \right) \\ &= \sum_{T:|V(T)\cup S|\leq\tau} \chi_T \cdot (\frac{\omega}{n})^{|V(T)\cup S|}\end{aligned}$$

for all S with $|S| \leq d$. □

4.3.2 Exact case

Now we construct a pseudo-expectation for the exact problem.

First, there is a generic way to generate possible candidates. That is, the Size Constraints (4.4) suggests to define $\widetilde{E}x_S$ in a top-down fashion: fix $\widetilde{E}x_S$ for all $|S| = d$ first, then recursively set

$$\widetilde{E}x_S \leftarrow \frac{1}{\omega - |S|} \sum_{i \notin S} \widetilde{E}x_{S\cup\{i\}} \tag{4.29}$$

for smaller-sized S's. If denote by $\widetilde{E}_d x$ the vector of the assignments for S's s.t. $|S| = d$, then this amounts to multiplying $\widetilde{E}_d x$ by the following matrix.

Definition 4.6. *The d-***filtration matrix** $\text{Fil}_{d,=d}$*, of dimension* $\binom{[n]}{\leq d} \times \binom{[n]}{d}$*, is*

$$\text{Fil}_{d,=d}(A,B) = \begin{cases} \binom{\omega-|A|}{d-|A|}^{-1}, & \text{if } A \subseteq B \text{ (where } |B| = d\text{);} \\ 0, & \text{otherwise.} \end{cases} \tag{4.30}$$

Definition 4.7. *Given vector $\widetilde{E}_d x$ which assigns a value to each d-subseteq $S \subseteq [n]$, the* **exact pseudo-expectation generated by** $\widetilde{E}_d x$ *is*

$$\widetilde{E}x := \text{Fil}_{d,=d} \cdot \widetilde{E}_d x. \tag{4.31}$$

Lemma 4.7. *The pseudo-expectation in Definition 4.7 satisfies Size Constraints* (4.4)*, regardless of the choice of* $\widetilde{E}_d x$*.*

Proof. For $|S| < d$, take vector v_S by $v_S(S') = \begin{cases} \omega - |S|, & \text{if } S' = S; \\ -1, & \text{if } S' \supseteq S,\ |S' \backslash S| = 1; \\ 0, & \text{otherwise} \end{cases}$ which is in $\mathbb{R}^{\binom{[n]}{\leq d}}$. Then it suffices to show $v_S^\top \mathrm{Fil}_{d,=d} = 0$, which is a direct check. □

The $\widetilde{E}$ generated like so should further satisfy:

1. Clique Constraints (4.3);
2. PSDness Constraint (4.5);
3. Default Constraint (4.2) (so far we only have $\omega \cdot \widetilde{E}x_\emptyset = \widetilde{E}x_1 + ... + \widetilde{E}x_n$).

Item (3) is not a problem as long as $\widetilde{E}x_\emptyset > 0$, since we can always rescale everything by $(\widetilde{E}x_\emptyset)^{-1}$ without affecting other constraints.

Remark 4.3. (Example) *The following construction seems natural. Combining Def. 4.7 with the perspective from section 4.3.1, we can take* (4.26) *with the exact plant-setting* (p_0, q_0)*, followed by multiplying* $\mathrm{Fil}_{d,=d}$*:*

$$\widetilde{E}_{\text{example}} x_S = \mathrm{Fil}_{d,=d} \cdot \left(\zeta_{d,\tau} \cdot (\widetilde{\mathrm{Cl}}(G) \circ \zeta_{\tau,\tau}^{-1}) \cdot (q_0)_\tau \right).$$

As can be checked, this satisfies the Clique Constraints. It also has a nice Fourier expression: by some computation which we omit here, modulo provably negligible error the resulting matrix is $M_{\text{example}}(I, J) = \sum_{\substack{T: \\ |V(T) \backslash (I \cup J)| \leq \tau - d}} \frac{\binom{n - |V(T) \cup I \cup J|}{\omega - |V(T) \cup I \cup J|}}{\binom{n}{\omega}} \chi_T$*. The only problem, however, is that we don't know how to prove the PSDness. Despite a transparent similarity to the previous expression* (4.28)*, a similar proof breaks down seriously here due to the loss of*

nice arithmetic structure when changing from function $(\frac{\omega}{n})^x$ *(in* (4.28)*) to* $\frac{\binom{n-x}{\omega-x}}{\binom{n}{\omega}}$*. See also Remark 4.11.*

Now we construct an $\widetilde{E}_d$ in Definition 4.7. With the motivation stated in section 4.2.1, we give the construction matter-of-factly here. First, take the pseudo-expectation for $|S| = d$ in the form $\widetilde{E}x_S = \sum_{T:|V(T)\cup S|\le\tau} \chi_T \cdot F(|V(T)\cup S|)$ for some function F. We call F a ***d*-generating function**, to be chosen shortly after. For now, for any $|S| \le d$, by (4.30) the pseudo-expectation has form: denote $u = d - |S|$,

$$\widetilde{E}x_S = \frac{1}{\binom{w-d+u}{u}} \sum_{T:|V(T)\cup S|\le\tau} \chi_T \cdot \Bigg[\sum_{c=0}^{u} \binom{|V(T)\cup S| - d + u}{c} \binom{n - |V(T)\cup S|}{u-c} \cdot F(|V(T)\cup S| + u - c)\Bigg]. \tag{4.32}$$

Lemma 4.8. (4.32) *always satisfy Clique and Size Constraints* (4.3),(4.4)*.*

Proof. It satisfies Size Constraints by Lemma 4.7. For Clique Constraints, fixing S, the "[...]"-part in (4.32) only depends on $|V(T)\cup S|$, so $\widetilde{E}x_S$ has the form

$$\sum_{T:|V(T)\cup S|\le\tau} a_{|V(T)\cup S|}\chi_T = \sum_k \sum_{T:|V(T)\cup S|=k} a_k \chi_T,$$

the inner sum factors through $\widetilde{\mathrm{Cl}}_S = \sum_{T\subseteq E(S)} \chi_T$. Thus, $M(I,J)(G) = 0$ if $\widetilde{\mathrm{Cl}}_{I\cup J}(G) = 0$. □

Definition 4.8. *(Exact d-generating function) We choose*

$$F(x) := \frac{(x+8\tau^2)!}{(8\tau^2)!} \cdot (\frac{\omega}{n})^x.$$

Remark 4.4. *As already mentioned in section 4.2.1, the design of F, especially its first factor, is technical; the goal is to make the resulting M positive. The numerator* $(x+8\tau^2)!$

will be used in Prop. 4.9, where the $8\tau^2$ can be replaced by larger polynomials in τ. The $(8\tau^2)!$ in denominator is added for convenience (see Remark 4.5).

Definition 4.9. *The* **exact moment matrix** $\widetilde{M}$ *is defined as*

$$\widetilde{M}(A,B) = \sum_{T:|V(T)\cup A\cup B|\le\tau} \widetilde{M}(A,B;T)\chi_T \text{ for all } A,B\subseteq[n],\ |A|,|B|\le d/2,$$

where $\widetilde{M}(A,B;T) =$

$$\frac{1}{\binom{\omega-d+u}{u}}\Bigg[\sum_{c=0}^{u}\binom{|V(T)\cup A\cup B|-(d-u)}{c}\binom{n-|V(T)\cup A\cup B|}{u-c} \underbrace{\cdot\frac{\big(|V(T)\cup A\cup B|+u-c+8\tau^2\big)!}{(8\tau^2)!}\cdot(\frac{\omega}{n})^{|(V(T)\cup A\cup B)|+u-c}}_{f\left(|V(T)\cup A\cup B|+u-c\right)}\Bigg]. \tag{4.33}$$

Here we denoted $d-|A\cup B|$ by u.

Remark 4.5. *In* (4.33)*, the "most significant" factor is $(\frac{\omega}{n})^{|V(T)\cup A\cup B|}\cdot\omega^{-c}$, if notice $\frac{\binom{n-|V(T)\cup A\cup B|}{u-c}}{\binom{\omega-d+u}{u}}\omega^u n^{-(u-c)}\ll\omega,n$, and that factors like $\frac{(|V(T)\cup A\cup B|+u-c+8\tau^2)!}{(8\tau^2)!}$ are qualitatively smaller than ω in our parameter regime.*

4.4 Some preparation

Homogenization for Exact Clique

With the Size Constraints (4.4) satisfied, any moment matrix can be reduced to its $\binom{[n]}{d/2}$-principal minor, which is slightly more convenient to work with. The following homogeneity trick is standard in the SoS literature.

Given any degree-d moment matrix $M_{dSOS}(G)$ that satisfies the Size Constraints (4.4), let $M(G)$ be its principal minor on $\binom{[n]}{d/2}\times\binom{[n]}{d/2}$.

Lemma 4.9. *$M_{dSOS}(G)$ is PSD $\Leftrightarrow$ $M(G)$ is PSD.*

Proof. The $\Rightarrow$ part is trivial. Now suppose M_{dSOS} is not PSD, then $\exists a \in \mathbb{R}^{\binom{[n]}{\leq d/2}}$ s.t. $a^\top M_{dSOS} a = -1$. With the presence of boolean constraints (i.e. we can additionally define $\widetilde{E}(x_i^2 \cdot p) := \widetilde{E}(x_i \cdot p)$ for all i and all polynomial p of degree $\leq d-2$), this is equivalent to $\widetilde{E}(g^2) = -1$ for some multi-linear polynomial $g = a^\top x = \sum_{|S| \leq d/2} a_S x_S$. Now substitute every x_S ($|S| < d/2$) in g by the corresponding linear combination of $\{x_{S'} \mid |S'| = d/2\}$ from (4.29), we get a multi-linear, degree-$d/2$ homogeneous g_1. Since $g - g_1$ thus $g^2 - g_1^2$ is a multiple of the constraints,

$$\widetilde{E}(g_1^2) = \widetilde{E}(g^2) = -1. \tag{4.34}$$

Assume $g_1 = b^T x$ where x denotes $(x_S)_{|S|=d/2}$. Then (4.34) says $b^\top M b = -1$, so M is not PSD. □

Concentration bound on polynomials

The following bound on random polynomials is standard.

Lemma 4.10. *Suppose $a < \log n$, and p is a polynomial*

$$p = \sum_{T:\ |V(T)|=a} c(T)\chi_T \quad c_T \in \mathbb{R}$$

and $C > 0$ is a number s.t. $|c(T)| \leq C$ for all T. Then W.p. $1 - n^{-10 \log n}$ over G,

$$|p(G)| < C \cdot n^{a/2} 2^{a^2} n^{4 \log\log n}. \tag{4.35}$$

Proof. For all $k \in \mathbb{N}$,

$$p^{2k} = \sum_{T_1,\ldots,T_{2k}:\ |V(T_i)|=a} c(T_1)\ldots c(T_{2k})\chi_{T_1}\cdots\chi_{T_{2k}}, \tag{4.36}$$

and we take the expectation of this. Each $\mathbb{E}[\chi_{T_1}\cdots\chi_{T_{2k}}(G)] \neq 0$ (i.e. equals 1) iff every edge

appears even times in $T_1, ..., T_{2k}$, which implies $|V(T_1 \cup ... \cup T_{2k})| \leq \frac{1}{2} \cdot 2ka = ka$. There are at most $ka\binom{n}{ka} < n^{ka}$ many choices of $V(T_1 \cup ... \cup T_{2k})$. For each choice, there are at most $\binom{ka}{a} \cdot 2^{\binom{a}{2}} < (ka)^a \cdot 2^{a^2/2}$ many ways to choose each T_i. Therefore,

$$\mathbb{E}[p^{2k}] \leq C^{2k} \cdot n^{ka} \left((ka)^a 2^{a^2/2}\right)^{2k} := N^{2k} \quad \text{where} \quad N = Cn^{a/2} \cdot (ka)^a \cdot 2^{a^2/2}.$$

By Markov inequality, $\Pr\left[p^{2k} > (2N)^{2k}\right] < 2^{-2k}$. Take $k := 10 \log^2 n$, we get that w.p. $> 1 - n^{-10 \log n}$, $|p(G)| < 2N < C \cdot n^{a/2} 2^{a^2} n^{4 \log \log n}$ for all large enough n. □

Norm concentration of pseudo-random matrices

Like in almost all previous work on the subject, the norm bound on certain pseudo-random matrices called *graph matrices* ([1]) will be a fundamental tool for us. Intuitively, such a matrix collects all possible Fourier characters from embeddings of a fixed small graph.

Definition 4.10. *(cf. [1, 79, 58, 63]) A* **ribbon** $\mathcal{R}$ *is a triple* $(A, B; T)$ *where* A, B *are vertex-sets and* T *is an edge set.* A, B *are called the* **side sets***, or individually the left and right set of* $\mathcal{R}$*, respectively. The* **size** *of* $\mathcal{R}$ *is* $|V(\mathcal{R})| = |V(T) \cup A \cup B|$.

By definition, a ribbon as a graph always has no isolated vertex outside of $A \cup B$.

Definition 4.11. *We say* $\mathcal{R} = (A, B; T)$ *is* **left-generated** *if every vertex in* $V(\mathcal{R})$ *is either in* B *or can be reached by paths*[8] *from* A *without touching* B*. Being* **right-generated** *is symmetrically defined.*

Definition 4.12. *A* **shape** *is a equivalent class of ribbons, where two ribbons* $(A, B; T)$*,* $(A', B'; T')$ *are equivalent or "of the same shape" if there is an isomorphism* σ *between the corresponding graphs s.t.* $\sigma(A) = A'$ *and* $\sigma(B) = B'$*. Denote a shape by* $\mathcal{U}$*, represented by a ribbon* $(A, B; T)$*.* $V(\mathcal{U}) := A \cup B \cup V(T)$ *and its* **size** *is* $|V(\mathcal{U})|$.

8. We always stick to the convention of including degenerate paths (one-point path).

Thus we may speak of **the shape of a ribbon** $\mathcal{R}$. We say a function f defined on a set of ribbons is **symmetric w.r.t. shapes** if, whenever $\mathcal{R}$ and $\mathcal{R}'$ are of the same shape and f is defined on them, $f(\mathcal{R}) = f(\mathcal{R}')$.

Definition 4.13. *([1]) Fix n and shape $\mathfrak{U} = (A, B; T)$. The* **graph matrix of shape** $\mathfrak{U}$ *is the following $2^{[n]} \times 2^{[n]}$-matrix $M_{\mathfrak{U}}$:*

$$\forall I, J \subseteq [n], \quad M_{\mathfrak{U}}(I, J) = \sum_{\substack{T_1: \\ \exists \text{injective } \phi : V(\mathfrak{U}) \to [n] \text{ s.t.} \\ \phi(A)=I,\ \phi(B)=J,\ \phi(T)=T_1}} \chi_{T_1}$$

($= 0$ if no such ϕ exists). Here, ϕ on T means the natural induced map on edges.

In [1], the matrices have columns and rows indexed by *tuples* with elements in $[n]$, instead of *subsets* (which is our case), but our matrix is always a sub-matrix of it, e.g. ours can be viewed as supported on strictly increasing tuples.

Theorem 4.3. *(Norm bounds on $M_{\mathfrak{U}}$, [1]) For any shape $\mathfrak{U} = (A, B; T)$ of size $t < \log n$, w.p. $> 1 - n^{-10 \log n}$ over G,*

$$\|M_{\mathfrak{U}}(G)\| \leq n^{\frac{t-p}{2}} \cdot 2^{O(t)} \cdot (\log n)^{O(t+p-2r)} \tag{4.37}$$

where $r = |A \cap B|$ and p is the max number of vertex-disjoint paths between (A, B) in $\mathfrak{U}$. Moreover, under the same notation, if further denote $s = \frac{|A|+|B|}{2}$ then

$$\|M_{\mathfrak{U}}(G)\| \leq n^{\frac{t-p}{2}} \cdot 2^{O(t)} \cdot (\log n)^{O(t-s)}. \tag{4.38}$$

The bound in Theorem 4.3 is almost tight ([1]). It is proved by a careful estimation of the trace-power $\mathbb{E}[\mathrm{tr}(M_{\mathfrak{U}}^{2k})]$ (for some $k > 0$) which we omit here. Its "moreover" part follows from (4.37) since $t \geq |A \cup B| = 2s - r$, $p \leq s$, so $t + p - 2r \leq t + s - 2(2s - t) = 3(t - s)$.

Some notions on graphs

Definition 4.14. *(Vertex-separator) For a graph H and $A, B \subseteq V(H)$, we say $S \subseteq V(H)$ is an (A,B)-***vertex-separator***, or S separates A, B in H, if any path from A to B in H must pass through S. Let*

$$s_{A,B}(H) := \min\{|S| \mid S \text{ is an } (A,B)\text{-vertex-separator}\}.$$

A vertex-separator achieving this minimum is a **min-separator**. *Let* $\mathrm{mSep}_{A,B}(H)$ *denote the set of all min-separators.*

The definition naturally applies to a ribbon $\mathcal{R} = (A, B; T)$, with A, B being the two vertex-sets. In that case, we can write the corresponding min-separator size as $s_{A,B}(T)$ and set of the min-separators as $\mathrm{mSep}_{A,B}(T)$ *or* $\mathrm{mSep}(\mathcal{R})$.

Theorem 4.4. *(Menger's theorem) For any finite graph H, $s_{A,B}(H)$ equals to the maximum number of vertex-disjoint paths from A to B in H.*

Definition 4.15. *For ribbon $\mathcal{R} = (A, B; T)$, define its* **reduced size** *to be*

$$e_{A,B}(T) := |V(T) \cup A \cup B| - s_{A,B}(T). \tag{4.39}$$

The reduced size is double of the exponent in n in the bound of Theorem 4.3, hence is the controlling parameter of the norm of the graph matrix.

A fundamental fact is that the set of all min-separators has a lattice structure.

Theorem 4.5. *([45]) For a ribbon $(A, B; T)$,* $\mathrm{mSep}_{A,B}(T)$ *has a natural* **poset** *structure: min-separators $A_1 \leq A_2$ iff A_1 separates $(A, A_2; T)$, or equivalently as it can be checked, iff A_2 separates $(A_1, B; T)$. The set is actually a* **lattice** *under this partial-ordering: $\forall A_1, A_2 \in$* $\mathrm{mSep}_{A,B}(T)$ *their join and meet exist. In particular, there exist unique* **minimum** *and* **maximum**.

We denote the minimum in the above theorem by $S_l(A,B;T)$ and the maximum by $S_r(A,B;T)$, meant to be the **leftmost** and **rightmost** min-separator, respectively.

Johnson schemes

We only need a minimal amount of knowledge here.

Definition 4.16. *([42]) Fix natural numbers $n \geq k$, $n > 0$. A* **Johnson scheme** $\mathfrak{J}$ *is an $\binom{[n]}{k} \times \binom{[n]}{k}$-matrix that satisfies $\mathfrak{J}(I,J) = \mathfrak{J}(I',J')$ whenever $|I \cap J| = |I' \cap J'|$.*

It can be checked that (fix n,k) all Johnson schemes are symmetric matrices and form a commutative $\mathbb{R}$-algebra, so they are simultaneously diagonalizable. In below we fix n and $k = d/2$. An obvious $\mathbb{R}$-basis for Johnson schemes is $D_0, ..., D_{d/2}$ where

$$D_r(I,J) = \begin{cases} 1, & \text{if } |I \cap J| = r \\ 0, & \text{o.w.} \end{cases} \qquad \forall I, J \in \binom{S}{d/2}. \tag{4.40}$$

Another basis which we denote by $\mathfrak{J}_0, ..., \mathfrak{J}_{d/2}$ is

$$\mathfrak{J}_r(I,J) = \binom{|I \cap J|}{r}, \quad \forall I, J \in \binom{[n]}{\frac{d}{2}}. \tag{4.41}$$

$\mathfrak{J}_0, ..., \mathfrak{J}_{d/2}$ are PSD matrices since

$$\mathfrak{J}_r = \sum_{A \subseteq [n], |A| = r} u_A u_A^\top \quad \text{where} \quad u_A \in \mathbb{R}^{\binom{[n]}{k}},\ u_A(B) = 1_{A \subseteq B}. \tag{4.42}$$

Also, clearly, $\mathfrak{J}_{d/2} = \mathrm{Id}$. A basis-change from D to $\mathfrak{J}$ is given by the following.

Lemma 4.11. $D_r = \sum_{r'=r}^{d/2} (-1)^{r'-r} \binom{r'}{r} \cdot \mathfrak{J}_{r'}$.

Proof. The $RHS(I,J) = \sum_{r'=r}^{d/2} (-1)^{r'-r} \binom{r'}{r} \binom{|I \cap J|}{r'} = \sum_{r'=r}^{|I \cap J|} (-1)^{r'-r} \binom{|I \cap J|}{r} \binom{|I \cap J| - r}{r'-r} = \binom{|I \cap J|}{r} \cdot 1_{|I \cap J| = r} = 1_{|I \cap J| = r}$. □

4.5 PSDness analysis, I: Hadamard product and Euler transform

Notation. Henceforth throughout the chapter, M exclusively refers to the $d/2$-homogeneous minor of the moment matrix $\widetilde{M}$ in Definition 4.9.

Our main theorem is the following.

Theorem 4.6. *W.p.* $> 1 - n^{-5\log n}$, $M(G) \succeq n^{-d-1}\mathrm{diag}\left(\widetilde{\mathrm{Cl}}(G)\right)_{\binom{[n]}{d/2}\times\binom{[n]}{d/2}}$.

Corollary 4.1. *W.p.* $> 1 - n^{-5\log n}$, $\widetilde{E}x_{\emptyset} > 0$.

Proof. By construction (4.29), $\widetilde{E}x_{\emptyset} = \frac{\binom{\omega-d/2}{d-d/2}}{\binom{\omega}{d}\binom{d}{d/2}} \sum_{S:|S|=d/2} \widetilde{E}x_S = \frac{\binom{\omega-d/2}{d-d/2}}{\binom{\omega}{d}\binom{d}{d/2}}\mathrm{Tr}(M)$, and by Theorem 4.6 this is positive with high probability. □

Proof. (of Theorem 4.1 from Theorem 4.6) Lemma 4.9 and Theorem 4.6 proves the PSDness of the moment matrix from Definition 4.9, which also satisfies the Default Constraint (Corollary 4.1 and the discussion above Remark 4.3) and the Clique and Size Constraints (Lemma 4.7). The degree-d lower bound follows. □

In the rest of the chapter, we prove Theorem 4.6. We will use three steps to achieve it, and this section makes the first step.

To begin with, by definition of $M(I,J)$ (Def. 4.9, (4.33)),

$$M(I,J;T) = \sum_{c=0}^{u}\Bigg[\frac{1}{\binom{\omega-d+u}{u}}\omega^{u-c}\cdot \underbrace{\left(\binom{a-(d-u)}{c}\binom{n-a}{u-c}n^{-(u-c)}\frac{(a+u-c+8\tau^2)!}{(8\tau^2)!}(\frac{\omega}{n})^a\right)}_{:=M_c(u,a)}\Bigg] \tag{4.43}$$

where $u = |I\cap J|, a = |V(T)\cup I\cup J|$. In this expression the parameter u appears nestedly and makes it difficulty to analyze. (It doesn't appear in the non-exact case (4.28) at all.) To resolve the issue, we express M in a $\Sigma\Pi$-form, i.e. a sum of Hadamard products, so that

in each leaf matrix the dependence on u is removed to some degree:

$$M = \sum_{c=0}^{\frac{d}{2}} m_c \circ M_c \tag{4.44}$$

where m_c, M_c are matrices as follows. For all $|I|, |J| = d/2$,

$$m_c(I,J) = \frac{1}{\binom{\omega-d+u}{u}} \omega^{u-c} \quad \text{where } u = |I \cap J| \tag{4.45}$$

$$M_c(I,J) = \begin{cases} \sum_{T:|V(T)\cup I\cup J|\leq\tau} M_c(|I\cap J|, |V(T)\cup I\cup J|)\chi_T & \text{, if } |I\cap J| \geq c; \\ 0 & \text{, o.w.} \end{cases} \tag{4.46}$$

Remark 4.6. *It is important to note that m_c is supported on all (I,J) while $M_c(I,J) = 0$ if $|I \cap J| < c$, so that (4.44) holds.*

To analyze (4.44), we would hope that the second factor M_c is "close" to each other for varying c, while the first factor m_c is qualitatively decreasing in c. This, if true, would make it possible for us to concentrate on showing the PSDness in the main case $c = 0$. The next Lemma 4.12 proves the second half of the above intuition; the other half will be stated more precisely in the Main Lemma 4.14.

Lemma 4.12. *For each $c = 0, ..., d/2$, $m_c = \omega^{-c} \sum_{k=0}^{d/2} b_k \cdot \mathfrak{J}_k$ where $\mathfrak{J}_k$'s are the Johnson basis (4.41), $b_k/k! \in [\frac{d}{2\omega}, 1 + \frac{2dk}{\omega}]$. In particular,*

$$m_0 = \omega m_1 = ... = \omega^{\frac{d}{2}} m_{\frac{d}{2}} \succ \frac{1}{\omega}\mathrm{Id}. \tag{4.47}$$

Proof. By definition, $m_c = \omega^{-c} \sum_{l=0}^{d/2} \frac{\omega^l}{\binom{\omega-d+l}{l}} D_l$, where D_l $(l = 0, ..., d/2)$ are the simple basis

of Johnson schemes (4.40). By basis-change (Lem. 4.11),

$$m_c = \omega^{-c} \sum_{k=0}^{d/2} \mathfrak{J}_k \cdot k! \left(\sum_{l=0}^{k} (-1)^{k-l} \cdot \underbrace{\left[\frac{\omega}{\omega-(d-l)} \cdot \ldots \cdot \frac{\omega}{\omega-(d-1)} \cdot \frac{1}{(k-l)!} \right]}_{:=f_k(l), \text{ which is } 1/k! \text{ if } l=0} \right).$$

For fixed k, $f_k(l)$ is increasing in l so $\sum_{l=0}^{k}(-1)^{k-l} f_k(l) \geq f_k(k) - f_k(k-1) > \frac{d/2}{\omega} \cdot (1 + \frac{d/2}{\omega})^{k-1} \geq \frac{d}{2\omega}$. Note for $k = d/2$, $\mathfrak{J}_{d/2} = \mathrm{Id}$, so we get (4.47). □

Euler transform. Fixing c, now we look into the second factor M_c in (4.44). For fixed $(I, J; T)$ denote $u = |I \cap J|$, $a = |V(T) \cup I \cup J|$, then by (4.43) we have that

$$M_c(u,a) = \binom{a-(d-u)}{c} \binom{n-a}{u-c} n^{-(u-c)} \frac{(a+u-c+8\tau^2)!}{(8\tau^2)!} (\frac{\omega}{n})^a \tag{4.48}$$

is the coefficient of χ_T in $M_c(I, J)$ for $c \leq u$.

Definition 4.17. *(***Extended** $M_c(u,a)$*) For fixed $c \geq 0$, the function $M_c(u,a)$ in* (4.48) *is partial, defined for $(u,a) \in \mathbb{N}^2$ s.t. $u \geq c$, $u + a \geq d + c$. It can be naturally* **extended to** $\mathbb{N}^2$ *by letting*

$$\binom{n-a}{u-c} = 0 \quad \textit{if } u < c, \tag{4.49}$$

and using the convention on binomial coefficients: $\binom{-m}{k} = (-1)^k \cdot \binom{m+k-1}{k}$ for all $m > 0$, $k \geq 0$; $\binom{m}{0} = 1$ for all $m \in \mathbb{Z}$; and

$$\binom{m}{k} = 0 \textit{ for all } 0 \leq m < k. \tag{4.50}$$

In the rest of the chapter, we will use $M_c(u,a)$ to mean this extended function.

In particular, if $0 \leq a - (d-u) < c$ then $M_c(u,a) = 0$ since $\binom{a-(d-u)}{c} = 0$.

One trouble with M_c is that, still, $u = |I \cap J|$ appears in it in an unpleasant way. To further remove the dependence on u, we consider a decomposition

$$M_c = \sum_{R \in \binom{[n]}{\leq \frac{d}{2}}} M_c^R \tag{4.51}$$

where for each $R \in \binom{[n]}{\leq \frac{d}{2}}$ the matrix M_c^R is supported on rows and columns whose index contains R. More explicitly, for any $(I, J; T)$ let $a = |V(T) \cup I \cup J|$, suppose

$$M_c^R(I,J) := \begin{cases} (\frac{\omega}{n})^a \sum_{T: |V(T) \cup I \cup J| \leq \tau} Y_c(|R|, a) \cdot \chi_T & \text{, if } R \subseteq I \cap J; \\ 0 & \text{, o.w.} \end{cases} \tag{4.52}$$

for some function $Y_c(u, a)$ to be chosen, then comparing for every tuple $(I, J; T)$ we see that equation (4.51) is equivalent to the following: for any fixed c, a,

$$\sum_{r=0}^{u} \binom{u}{r} Y_c(r, a) (\frac{\omega}{n})^a = M_c(u, a). \tag{4.53}$$

This suggests to take $Y_c(u, a) \cdot (\frac{\omega}{n})^a$ to be the **inverse Euler transform** (w.r.t. variable u) of the **extended** function $M_c(u, a)$.

Fact 4.1. [9] *If $x(m), y(m)$ are two sequences defined on $\mathbb{N}$ s.t. for all m, $x(m) = \sum_{l=0}^{m} \binom{m}{l} y(l)$, then $x(m)$ is called the* **Euler transform** *of $y(m)$. The inverse transform is given by that for all m, $y(m) = \sum_{l=0}^{m} (-1)^{m-l} \binom{m}{l} x(l)$.*

Definition 4.18. *(Coefficients in M_c^R) For every fixed $c \geq 0$, define*

$$Y_c(r,a) = \begin{cases} \sum_{l=c}^{r} (-1)^{r-l} \binom{r}{l} \binom{a+l-d}{c} \binom{n-a}{l-c} n^{-(l-c)} \frac{(a+l-c+8\tau^2)!}{(8\tau^2)!} & \text{, if } r \geq c; \\ 0 & \text{, o.w.} \end{cases} \tag{4.54}$$

9. Coincidentally, this fact can be seen as an application of ζ-matrix and its inverse.

Then as a clear-up summary, we prove the following the main result of this section.

Lemma 4.13. *(The Hadamard-product decomposition of M)*

$$M = \sum_{c=0}^{\frac{d}{2}} m_c \circ \left(\sum_{R:R\in\binom{[n]}{\leq d/2}} M_c^R \right) \tag{4.55}$$

$$= \sum_{R\in\binom{[n]}{\leq d/2}} \underbrace{\left(\sum_{c=0}^{|R|} m_c \circ M_c^R \right)}_{:=M^R} \tag{4.56}$$

where each m_c is as in Lemma 4.12 and each M_c^R has the following expression.

1. *$M_c^R = 0$ if $|R| < c$;*

2. *If $R \not\subseteq I \cap J$, $M_c^R(I,J) = 0$;*

3. *If $|R| \geq c$ and $R \subseteq I \cap J$, $M_c^R(I,J) = \sum_{T:|V(T)\cup I\cup J|\leq\tau} M_c^R(I,J;T)\chi_T$ where if denote $a = |V(T)\cup I\cup J|$, then $M_c^R(I,J;T) =$*

$$(\frac{\omega}{n})^a \underbrace{\sum_{l=c}^{|R|}(-1)^{|R|-l}\binom{|R|}{l}\binom{a+l-d}{c}\binom{n-a}{l-c}n^{-(l-c)}\frac{(a+l-c+8\tau^2)!}{(8\tau^2)!}}_{Y_c(|R|,a)\ (4.54)}. \tag{4.57}$$

4. *For all $0 \leq c \leq r \leq d/2$ and $0 \leq a \leq \tau$, $|Y_c(r,a)| < \tau^{5\tau}$.*

Proof. (1), (2), (3) is by definition. To check (4.55) i.e. $M_c = \sum_R M_c^R$, we check for every $(I,J;T)$ where $|I| = |J| = d/2$, $|V(T)\cup I\cup J| \leq \tau$. Let $u = |I\cap J|$, $a = |V(T)\cup I\cup J|$, then note $a - (d-u) \geq 0$, and

$$\sum_{R:} M_c^R(I,J;T) = \sum_{R:R\subseteq I\cap J} M_c^R(I,J;T) = (\frac{\omega}{n})^a \sum_{r=0}^{|I\cap J|}\binom{|I\cap J|}{r} Y_c(r,a).$$

By the Euler transform and (4.53), the RHS equals the extended $M_c(u,a)$. Thus, we only need to see $M_c(u,a)=0$ if further $u<c$ or $a-(d-u)<c$ (in particular, in such cases $c>0$), and this is by (4.49), (4.50).

For (4),

$$\begin{aligned}|Y_c(u,a)| &= \left|\sum_{l=c}^{r}(-1)^{r-l}\binom{r}{l}\binom{a+l-d}{c}\Big[\binom{n-a}{l-c}n^{-(l-c)}\Big]\frac{(a+l-c+8\tau^2)!}{(8\tau^2)!}\right| \\ &< r\cdot 2^r\cdot(2\tau)^r\cdot 1\cdot(9\tau^2)^{2\tau} < \tau^{5\tau}\end{aligned}$$

where note $r\le d/2\ll\tau$ in our parameter regime. □

Lemma 4.14. (Main Lemma) *In the decomposition* (4.56)*, w.p.* $>1-n^{-5\log n}$ *the following hold. For all* $R\in\binom{[n]}{\le d/2}$*, denote* $P^R=\{I\in\binom{[n]}{d/2}\mid R\subseteq I\}$*,*

(1). $M_0^R\succeq n^{-d}\mathrm{diag}(\widetilde{\mathrm{Cl}})_{P^R\times P^R}$*;*

(2). $\pm\omega^{-c}M_c^R\preceq n^{-c/6}\cdot M_0^R,\quad\forall 0<c\le|R|$*.*

Corollary 4.2. *(Theorem 4.6) W.p.* $>1-n^{-5\log n}$ *over* G*,*

$$M(G)\succeq n^{-d-1}\mathrm{diag}(\widetilde{\mathrm{Cl}}(G))_{\binom{[n]}{d/2}\times\binom{[n]}{d/2}}.$$

Proof. Fix an R, $M^R=\sum_{c=0}^{|R|}m_c\circ M_c^R$. Suppose Lemma 4.14 (1), (2) hold (w.p. probability $>1-n^{-5\log n}$). Since Hadamard product with a PSD matrix presevres PSDness (Schur product theorem), we have $\sum_{c=1}^{|R|}m_c\circ M_c^R\preceq\sum_{c=1}^{|R|}m_c\circ\left(\omega^c n^{-c/6}\cdot M_0^R\right)$ by Lemma 4.14(2). The latter equals $\left(\sum_{c=1}^{|R|}n^{-c/6}\cdot m_0\right)\circ M_0^R$ by Lemma 4.12 which then $\preceq\ n^{-1/6}m_0\circ M_0^R$. Similarly, $\sum_{c=1}^{|R|}m_c\circ M_c^R\succeq -n^{-1/6}m_0\circ M_c^R$. Thus

$$M^R\succeq(1-n^{-1/6})m_0\circ M_0^R\succeq n^{-d-1}\mathrm{diag}(\widetilde{\mathrm{Cl}})_{P^R\times P^R}\quad\text{(Lem. 4.12 and 4.14(2))}.$$

So in (4.56), $M = M^{\emptyset} + \sum_{\emptyset \neq R \in \binom{[n]}{\leq d/2}} M^R \succeq M^{\emptyset} \succeq n^{-d-1}\mathrm{diag}(\widetilde{\mathrm{Cl}})_{\binom{[n]}{d/2}\times\binom{[n]}{d/2}}$. □

The rest of the chapter is devoted to proving the Main Lemma 4.14.

4.6 Recursive factorization technique

In this section, we introduce the *recursive approximate factorization* technique of [13]. It will be formalized and properly extended in section 4.6.2 (for later use in section 4.7).

Notation. Throughout section 4.6, for simplicity, we discuss the non-exact moment matrix which suffices to lay the ground for the technique, denoted by M'. It is the $\binom{[n]}{\frac{d}{2}}\times\binom{[n]}{\frac{d}{2}}$-minor[10] of the non-exact moment matrix:

$$M'(I,J) = \sum_{T:|V(T)\cup I\cup J|\leq\tau} (\frac{\omega}{n})^{|V(T)\cup I\cup J|}\chi_T \quad \forall I,J \in \binom{[n]}{d/2}. \tag{4.58}$$

The goal of section 4.6 is to diagonalize M' approximately in the "$LQL^\top$" form s.t. the difference matrix is negligible w.h.p. (when plugging in G).

4.6.1 A detour

This subsection is independent and only for showing Theorem 4.2(2); the reader can safely skip it and proceed to 4.6.2 for the proof of the Main Lemma 4.14. The goal of this subsection is to deduce a "coarse" factorization of M' via *mod-order analysis*.

10. Strictly speaking, PSDness of this minor is not sufficient as we do not have a homogeneity reduction in non-exact case. Nevertheless, it suffices to demonstrate the factorization.

Step 1: Diagonalization of $\mathbb{E}[M']$

Proposition 4.2. *$\mathbb{E}[M'] = CC^\top$, where C is the $\binom{[n]}{d/2} \times \binom{[n]}{\leq d/2}$-matrix*

$$C = (\zeta^\top)_{d/2,\leq d/2} \cdot \mathrm{diag}\left(\sqrt{t(|A|)}\right)_{A \in \binom{[n]}{\leq d/2}} \tag{4.59}$$

and $t(r) = (1 - O(\frac{d\omega}{n})) \cdot (\frac{\omega}{n})^{d-r}$ for all $r = 0, ..., d/2$.

We show it by a similar calculation as in [79], using Johnson schemes (Def. 4.16).

Fact 4.2. *(See e.g. (4.29) in [42]) The Johnson schemes (for $(n, d/2)$) have shared eigenspace-decomposition $\mathbb{R}^{\binom{[n]}{d/2}} = V_0 \oplus ... \oplus V_{d/2}$, and*

$$\mathfrak{J}_r = \bigoplus_{i=0}^{\frac{d}{2}} \lambda_r(i) \cdot \Pi_i \quad \text{for } r = 0, ..., d/2$$

where Π_i is the orthogonal projection to V_i w.r.t. the Euclidean inner product, and the eigenvalues are

$$\lambda_r(i) = \binom{\frac{d}{2} - i}{r - i} \binom{n - \frac{d}{2} - i}{\frac{d}{2} - r}, \quad 0 \leq i \leq \frac{d}{2}.$$

Lemma 4.15. *$\mathbb{E}[M'] = \sum_{r=0}^{d/2} t(r)\mathfrak{J}_r$ where each $t(r) = (1 - O(\frac{d\omega}{n})) \cdot (\frac{\omega}{n})^{d-r}$.*

Proof. By definition, $\mathbb{E}[M'] = \sum_{r=0}^{d/2} (\frac{\omega}{n})^{d-r} D_r$. By Lemma 4.11, $\mathrm{D}_r = \sum_{r'=r}^{d/2} (-1)^{r'-r} \binom{r'}{r} \cdot \mathfrak{J}_{r'}$ so

$$\begin{aligned}
\mathbb{E}[M'] &= \sum_{r=0}^{d/2} (\frac{\omega}{n})^{d-r} \left(\sum_{r'=r}^{d/2} (-1)^{r'-r} \binom{r'}{r} \mathfrak{J}_{r'} \right) \\
&= \sum_{r'=0}^{d/2} \mathfrak{J}_{r'} \cdot \left(\sum_{r=0}^{r'} (\frac{\omega}{n})^{d-r} (-1)^{r'-r} \binom{r'}{r} \right) \\
&= \sum_{r'=0}^{d/2} \mathfrak{J}_{r'} \cdot (\frac{\omega}{n})^{d-r'} (1 - \frac{\omega}{n})^{r'}
\end{aligned} \tag{4.60}$$

which proves the lemma. □

By Lemma 4.15 and (4.42), if let $t(r) = (\frac{\omega}{n})^{d-r'}[1-\frac{\omega}{n}]^{r'}$ then

$$\mathbb{E}[M'] = \sum_{A:|A|\le d/2} t(|A|)u_A u_A^\top = (\zeta^\top)_{d/2,\le d/2} \cdot \mathrm{diag}\Big(t(|A|)\Big) \cdot \zeta_{\le d/2,d/2} = CC^\top,$$

where used that the matrix $(\zeta^\top)_{d/2,\le d/2}$ has columns $\{u_A \mid |A| \le d/2\}$. This proves Proposition 4.2.

Step 2: Mod-order analysis

Reminder. This subsection is only for Theorem 4.2(2). The reader can safely skip it if he/she wants to proceed directly to proof of Theorem 4.1.

Given $\mathbb{E}[M'] = CC^\top$ in Step 1, ideally we hope to continue to solve for

$$M' = NN^\top \tag{4.61}$$

with $\mathbb{E}[N] = C$, and N extending C by non-trivial Fourier characters. Also, we restrict ourselves to symmetric solutions w.r.t. shapes. Toward this goal, we start with a relaxed equation as Definition 4.19, with the following motivation.

(1) Order in $\frac{\omega}{n}$. Entries of M' all have a clear order in $\frac{\omega}{n}$. Like in fixed-parameter problems, we treat $\frac{\omega}{n}$ as a distinguished structural parameter and try to solve the correct power of $\frac{\omega}{n}$ in the terms of N.

(2) Norm-match. Let's have a closer look into $\mathbb{E}[M'] = CC^\top = \sum_{r=0}^{d/2}(1-O(\frac{d\omega}{n}))\cdot(\frac{\omega}{n})^{d-r}\mathfrak{J}_r$. By fact 4.2, each $\mathfrak{J}_r$ b has norm $\binom{d/2}{r}\cdot n^{d/2-r}$ so

$$\Big\|C_r C_r^\top\Big\| \approx \binom{d/2}{r}\cdot(\frac{\omega}{n})^{d-r}n^{d/2-r}, \quad r=0,...,d/2. \tag{4.62}$$

We expect $N_r(N_r)^\top$ to concentrate around $C_r(C_r)^\top$, so the norm of the "random" part, i.e. matrix of nontrivial Fourier characters in $N_r(N_r)^\top$, is expected to be bounded by (4.62).

The essentially tight bound from Theorem 4.3 (cf. [1]) tells how this may happen, as below.

It is convenient to scale the variables: let $L = (L_0, ..., L_{\frac{d}{2}}) = (N_r \cdot (\frac{\omega}{n})^{\frac{-|A|}{2}})_{0 \le r \le \frac{d}{2}}$, then

$$M' = L \cdot \mathrm{diag}\left((\frac{\omega}{n})^{|A|}\right) \cdot L^\top \quad \text{with} \quad \mathbb{E}[L] = (\ C_r \cdot (\frac{\omega}{n})^{-r/2}\ )_{r=0,1,...,d/2.} \tag{4.63}$$

Now suppose $L_r(I, A) = \sum_{\text{small } T} \beta_{I,A}(T)\chi_T$, $A \in \binom{[n]}{r}$, where assuming as in (1) that the order of $\frac{\omega}{n}$ can be separated:

$$\beta_{I,A}(T) = \underbrace{(\frac{\omega}{n})^x}_{\text{main-order term}} \cdot (\text{ factor} \ll \frac{n}{\omega} \text{ and} \gg \frac{\omega}{n}\ ). \tag{4.64}$$

Fix I, A, T, we are looking for the condition on x to control the expected norm of $L_r(\frac{\omega}{n})^r(L_r)^\top$. Ignore for a moment the cross-terms, such a single graph matrix square in $L_r(\frac{\omega}{n})^r L_r^\top$ is

$$(\frac{\omega}{n})^{2x} R_{(I,A;T)} \cdot (\frac{\omega}{n})^r \cdot R_{(I,A;T)}^\top$$

with norm[11]

$$\lessapprox (\frac{\omega}{n})^{2x+r} \cdot n^{\mathrm{e}_{I,A}(T)} \cdot 2^{O(|V(T) \cup I \cup A|)} \cdot (\log n)^{>0}$$

by Theorem 4.3. Here recall $e_{I,A}(T) = |V(T) \cup I \cup A| - s_{I,A}(T) (\ge |I| - |A| = \frac{d}{2} - r)$. Compare this with (4.62), we need $(\frac{\omega}{n})^{2x} n^{e_{I,A}(T)} < \binom{d/2}{r} (\frac{\omega}{\sqrt{n}})^{d/2-r}$. If think of 2^d as qualitatively smaller than any positive constant power of ω, n, the natural bound to put is $x \ge e_{I,A}(T)$ which actually is the limit requirement when $\frac{\log \omega}{\log n} \to \frac{1}{2}$. Suggested by this, we will set the restriction $x \ge e_{I,A}(T)$ right from the start in the relaxed equation.

The above motivation leads to the following definition. Take a ring $\mathbb{A}$ by adding fresh variables α and χ_T's to $\mathbb{R}$ for all $T \in \binom{[n]}{2}$, with only relations $\{\chi_{T'} \cdot \chi_{T''} = \chi_T : T' \oplus T'' = T\}$.

11. Here the matrix is truncated from size $2^{[n]} \times 2^{[n]}$, which doesn't change anything since the original matrix is always 0 elsewhere.

Definition 4.19. *The* **mod-order equation** *is*

$$L_\alpha \cdot \mathrm{diag}\left(\alpha^{|A|}\right) \cdot (L_\alpha)^\top = M_\alpha \qquad \mod (*) \tag{4.65}$$

on the $\binom{[n]}{d/2} \times \binom{[n]}{\leq d/2}$ *matrix variable* L_α *in* $\mathbb{A}$*, where* $M_\alpha(I,J) := \sum_{T:|V(T)\cup I\cup J|\leq\tau} \alpha^{|V(T)\cup I\cup J|}\chi_T$*, and* $\mod (*)$ *is the* **modularity***, which means position-wise mod the ideal*

$$\left(\{\alpha^{|V(T)\cup I\cup J|+1}\chi_T\},\ \{\chi_T : |V(T)\cup I\cup J| > \tau\}\right).$$

Moreover, if denote $L_\alpha(I,A) = \sum_T \beta_{I,A}(T)\chi_T$ *where* $\beta_{I,A}(T) \in \mathbb{R}[\alpha]$*, then*[12]

$$\alpha^{e_{I,A}(T)} \mid \beta_{I,A}(T) \quad \forall I, A, T. \tag{4.66}$$

We are interested in solutions that are **symmetric***, i.e.* $\beta_{I,A}(T') = \beta_{J,B}(T'')$ *whenever* $(I, A; T')$*,* $(J, B; T'')$ *are of the same shape.*

The following is the key observation, whose proof is presented in the Appendix.

Lemma 4.16. *(Order match) If a product* $\alpha^{|A|} \cdot \beta_{I,A}(T') \cdot \beta_{J,A}(T'')$ *from the LHS of* (4.65) *is nonzero mod* $(*)$*, then both of the following hold:*

$$A \text{ is a min-separator for both } (I, A; T'),\ (J, A; T''); \tag{4.67}$$

$$\big(V(T') \cup I \cup A\big)\ \cap\ \big(V(T'') \cup J \cup A\big) = A. \tag{4.68}$$

Moreover, (4.67)*,* (4.68) *imply that*

$$A \text{ is a min-separator of } (I, J; T) \text{ (where } T = T' \oplus T''); \tag{4.69}$$

$$|V(T') \cup I \cup A|,\ |V(T'') \cup J \cup A| \leq \tau. \tag{4.70}$$

12. Recall $e_{I,A}(T')$ is the reduced size $|V(T') \cup I \cup A| - s_{I,A}(T')$ (Def. 4.15).

By this lemma, in an imagined solution we should assume $\beta_{I,A}(T') \neq 0$ only when it satisfies its part in conditions (4.67), (4.70). Using this information, plus a further weakening as *polarization*, we can deduce the following Proposition 4.3 which is the main takeaway. In the deduction, the graph-theoretic fact—the "in particular" of Theorem 4.5—appears exactly as the solvability condition. We leave details to the Appendix.

Proposition 4.3. *(Mod-order diagonalization) Let*

$$L_\alpha(I,A) := \sum_{\substack{T':\ |V(T')\cup I\cup A|\le\tau \\ A=S_l(I,A;T') \\ T'\cap E(A)=\emptyset \\ (I,A;T') \text{ left-generated (Def. 4.11)}}} \alpha^{e_{I,A}(T')}\chi_{T'},$$

$$Q_{0,\alpha}(A,B) := \sum_{\substack{T_m:\ |T\cup A\cup B|\le\tau \\ A,B\in \mathrm{mSep}_{A,B}(T_m)}} \alpha^{e_{A,B}(T_m)}\chi_{T_m}$$

(T_m to indicate "middle"). Then

$$L_\alpha \cdot [\mathrm{diag}\left(\alpha^{\frac{|A|}{2}}\right)\cdot Q_{0,\alpha}\cdot \mathrm{diag}\left(\alpha^{\frac{|A|}{2}}\right)]\cdot L_\alpha^\top = M_\alpha \qquad \mathrm{mod}\ (*) \tag{4.71}$$

where recall $(*)$ means ideal $(\{\alpha^{|V(T)\cup I\cup J|+1}\chi_T\},\ \{\chi_T : |V(T)\cup I\cup J| > \tau\})$ entry-wise.

Equation (4.71) is weaker than (4.65) but is sufficient for all use since we are only concerned with PSDness. In particular, it gives the first-approximate diagonalization of the matrix M', recast as Definition 4.20 below. This shows Theorem 4.2(2).

4.6.2 Recursive technique

In this subsection, we give a systematic treatment of the recursive factorization technique. We formulate it on matrix-products (Def. 4.22, 4.23) with simplification (Lem. 4.18) and an extension (Prop. 4.5) that will be used in Section 4.7 for the exact case.

The goal is to refine the coarse diagonalization (4.71), recast below.

Definition 4.20. *Let L be the $\binom{[n]}{\frac{d}{2}} \times \binom{[n]}{\leq \frac{d}{2}}$-matrix*

$$L(I,A) := \sum_{\substack{T' \colon |V(T')\cup I\cup A|\leq \tau \\ A=S_l(I,A;T') \\ T'\cap E(A)=\emptyset \\ (I,A;T') \text{ left-generated}}} (\frac{\omega}{n})^{|V(T')\cup I\cup A|-|A|}\chi_{T'}, \tag{4.72}$$

and Q_0 be the $\binom{[n]}{\leq \frac{d}{2}} \times \binom{[n]}{\leq \frac{d}{2}}$-matrix

$$Q_0(A,B) := \sum_{\substack{T_m:|T_m\cup A\cup B|\leq \tau \\ A,B\in \mathrm{mSep}_{A,B}(T_m)}} (\frac{\omega}{n})^{|V(T_m)\cup A\cup B|}\chi_{T_m}. \tag{4.73}$$

Finally, let

$$D := \mathrm{diag}\left((\frac{\omega}{n})^{\frac{|A|}{2}}\right)_{A\in\binom{[n]}{\leq d/2}}. \tag{4.74}$$

We call $L(DQ_0)L^\top$ the **first-approximate diagonalization** *of M'.*

Despite its name ("approximate"), the difference $M'-L(DQ_0D)L^\top$ is far from negligible. This is where the recursive factorization will be applied, and in the end it will give

$$M' = L\cdot[D\cdot(Q_0 - Q_1 + Q_2 ... \pm Q_{d/2})\cdot D]\cdot L^\top + \mathcal{E} \tag{4.75}$$

for some negligible error-matrix $\mathcal{E}$.

Remark 4.7. *The use of D in the above is superficial. We only keep it to make the middle matrices Q_i have slightly more convenient expressions.*

Let us start with some necessary notions.

More notion on graphs

Definition 4.21. *([13] Def. 6.5) For ribbon $\mathcal{R} = (I, J; T)$, the* **canonical decomposition** *is a ribbon triple $(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r) = ((I, A; T_l), (A, B; T_m), (B, J; T_r))$ as follows. $A = S_l(I, J; T)$, $B = S_r(I, J; T)$. $V(\mathcal{R}_l)$ is A unioned with the set of vertices reachable by paths from I in T without touching A, and $T_l = T|_{V(\mathcal{R}_l)} \backslash E(A)$. Symmetricallywe define $V(\mathcal{R}_l)$ and T_r. Finally, $T_m = T \backslash (T' \sqcup T'')$. R_l, R_m, R_r are called the* **left, middle, right ribbon of** $\mathcal{R}$*, respectively.*

Remark 4.8. *For better clarity, we list a few properties that follow from the definition of the canonical decomposition.*

1. $A = S_l(I, A; T_l)$, $B = S_r(B, J; T_r)$ (so they are unique min-separators of $\mathcal{R}_l, \mathcal{R}_r$, respectively);

2. $T_l \cap E(A) = \emptyset = T_r \cap E[A]$;

3. $\mathcal{R}_l$ is left-generated, $\mathcal{R}_r$ is right-generated;

4. $A, B \in \mathrm{mSep}_{A,B}(T_m)$ (in particular, $|A| = |B|$).

The above are properties about $\mathcal{R}_l$, $\mathcal{R}_m$, $\mathcal{R}_m$ individually ("inner" properties). There is also an intersection property on pairs of them ("outer" properties):

5. $V(\mathcal{R}_l) \cap V(\mathcal{R}_m) \subseteq A$, $V(\mathcal{R}_m) \cap V(\mathcal{R}_r) \subseteq B$, $V(\mathcal{R}_l) \cap V(\mathcal{R}_r) \subseteq A \cap B$. This implies $e(\mathcal{R}_l) + |V(\mathcal{R}_m)| + e(\mathcal{R}_r) = |V(\mathcal{R})|$.

The canonical decomposition can be *reversely* described, as follows.

Definition 4.22. *(Inner-, outer-canonicality) For a ribbon triple*

$$(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r) = \Big((I, A; T_l), (A, B; T_m), (B, J; T_r) \Big),$$

their **ribbon-sum** *is ribbon $(I, J; T)$ where $T = T_l \oplus T_m \oplus T_r$ (i.e. each edge mod 2 sum). The triple is called* **inner-canonical***, if they satisfy the "inner" conditions: items 1—4 in*

Remark 4.8. The triple is **outer-canonical** *if they satisfy the "outer" condition: item 5 in Remark 4.8. The triple is* **canonical** *if it is both inner- and outer-canonical.*

Proposition 4.4. *Canonical triples are 1-1 correspondent to their ribbon-sum, via ribbon sum and canonical decomposition.*

Proof. This follows directly by checking the definition. □

The above notions can be extended to related matrix products. Denote by $\mathbb{R}[\{\chi_T\}]$ the ring by adding fresh variables ("characters") χ_T's into $\mathbb{R}$ for every $T \subseteq \binom{[n]}{2}$ (fixing an n), with relations $\{\chi_{T'} \cdot \chi_{T''} = \chi_T \mid T' \oplus T'' = T\}$.

Definition 4.23. *(Approximate form) Suppose matrices X, Y have their rows and columns indexed by subsets of $[n]$ and entries in $\mathbb{R}[\{\chi_T\}]$. A character in an entry of such matrix can be regarded as a ribbon on the side sets row and column. Assume all ribbons have size $\leq \tau$ and X, Y have dimensions s.t. $XYX^\top$ is defined.*

Then every triple product (without collecting like-terms) in $XYX^\top$ has form

$$\underbrace{X(I, A; T_l)Y(A, B; T_m)X(J, B; T_r)}_{\text{nonzero in } \mathbb{R}} \chi_{T_l \oplus T_m \oplus T_r}, \tag{4.76}$$

and can be identified with a ribbon triple $(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r)$ in the natural way. We say (4.76) *is the* **resulting term** *of the ribbon triple; it is an* **outer-canonical product** *if the ribbon triple is outer-canonical. The* **approximation form** *of $XYX^\top$ is:*

$$XYX^\top = (XYX^\top)_{\text{can}} + (XYX^\top)_{\text{non-can}} \tag{4.77}$$

where $\left(XYX^\top\right)_{\text{out-can}}$ collects all terms of outer-canonical products, $(XYX^\top)_{\text{non-can}}$ collects all terms of non-outer-canonical products.

Machinery of recursion

Using the above notion, the first-approximate factorization (Def. 4.20) can be recast as

$$M' = [L(DQ_0D)L^\top]_{\text{can}} - \mathcal{E}_{\text{deg}} = L(DQ_0D)L^\top - [L(DQ_0D)L^\top]_{\text{non-can}} - \mathcal{E}_{\text{deg}} \quad (4.78)$$

where $\mathcal{E}_{\text{deg}}$ consists of all terms in $[L(DQ_0D)L^\top]_{\text{can}}$ with $|V(T) \cup I \cup J| > \tau$. $\mathcal{E}_{\text{deg}}$ is actually negligible in matrix norm[13], and the main task is to analyze the "main error", $[L(DQ_0D)L^\top]_{\text{non-can}}$. The key insight is:

$$[L(DQ_0D)L^\top]_{\text{non-can}} \text{ itself factors through } L, L^\top \text{ approximately, too.} \quad (4.79)$$

That is, $\exists Q_1$ s.t. $[L(DQ_0D)L^\top]_{\text{non-can}} = [L(DQ_1D)L^\top]_{\text{can}} + \mathcal{E}_{1;\text{negl}}$ for some $\mathcal{E}_{1;\text{negl}}$ where $[L(DQ_1D)L^\top]_{\text{can}} = L(DQ_1D)L^\top - [L(DQ_1D)L^\top]_{\text{non-can}}$ by (4.76); then we recurse on $[L(DQ_1D)L^\top]_{\text{non-can}}]$. We need the following notation to describe this.

Definition 4.24. *([13]) An* **improper ribbon** *is a ribbon plus with a new set of isolated vertices. In symbol, denote it as $\mathcal{R}^* = (A, B; T^*)$ with $T^* = T \sqcup \mathcal{I}$, T an edge-set and $\mathcal{I}$ a vertex set* d*isjoint from $V(T) \cup A \cup B$. $\mathcal{I}$ is called the* **isolated vertex-set of** *$\mathcal{R}^*$, denoted by $\mathcal{I}(\mathcal{R}^*)$. $V(\mathcal{R}^*) := V(T) \cup A \cup B \cup \mathcal{I}$. $(A, B; T)$ is called the (unique) largest ribbon in $\mathcal{R}^*$. Note a usual ribbon is an improper ribbon with $\mathcal{I} = \emptyset$.*

Note $\mathcal{I}(\mathcal{R}^*)$ could be different from the set of isolated vertices of the underlying graph, since there can be isolated vertices in $A \cup B$.

Definition 4.25. *The triple $\big(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r\big) = \big((I, A; T_l), (A, B; T_m), (B, J; T_r)\big)$ is called* **side-inner-canonical** *if the left and right ribbons, $\mathcal{R}_l$, $\mathcal{R}_r$ satisfy the inner-canonical conditions on their part (item 1–3 in Remark 4.8), and $\mathcal{R}_m$ is just a ribbon.*

13. They are supported on rows and columns where G is a clique.

Suppose a triple $(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r) = ((I, A; T_l),\ (A, B; T_m),\ (B, J; T_r))$ is side-inner-canonical and non-outer-canonical. Let $T := T_l \oplus T_m \oplus T_r$ and Z be the multi-set of "unexpected" intersections, i.e. the multi-set of vertices from $(\mathcal{R}_l \cap \mathcal{R}_m) - A$, $(\mathcal{R}_m \cap \mathcal{R}_r) - B$, $(\mathcal{R}_l \cap \mathcal{R}_r) - (A \cap B)$. Call $|Z|$ their **intersection size**, denoted as $z(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r)$. Note

$$|V(\mathcal{R}_l) \cup V(\mathcal{R}_m) \cup V(\mathcal{R}_r)| = |V(\mathcal{R}_l)| + |V(\mathcal{R}_m)| + |V(\mathcal{R}_r)| - |A| - |B| - z. \tag{4.80}$$

We further separate this triple into an "outer-canonical" one by the following operation, which is the core of recursive factorization.

Definition 4.26. *(Separating factorization, [13]) Let S'_l be the leftmost min-separator of $(I, A \cup (Z \cap V(\mathcal{R}_l)); T_l)$, similarly S'_r the right-most min-separator of $(B \cup (Z \cap V(\mathcal{R}_r)), J; T_r)$. Note $S'_l, S'_r \subseteq V(T) \cup I \cup J$.*

Define $\mathcal{R}'_l := (I, S'_l; T'_l)$, whose vertex set $V(\mathcal{R}'_l)$ is S'_l unioned with the set of vertices in $\mathcal{R}_l$ reachable from I by paths in T_l without touching S'_l, and T'_l is $T_l \backslash E(S'_l)$ restricted on $V(\mathcal{R}'_l)$. Ribbon $\mathcal{R}'_r$ is symmetrically defined. In particular, $T'_l \cap T'_r = \emptyset$. Then let $\mathcal{R}^*_m$ be the **improper** *ribbon $(S'_l, S'_r; T^*_m)$, $T^*_m := \big(T \backslash (T'_l \sqcup T'_r)\big) \sqcup \mathfrak{I}(\mathcal{R}^*_m)$ where $\mathfrak{I}(\mathcal{R}^*_m)$ collects all the rest isolated vertices:*

$$\mathfrak{I}(\mathcal{R}^*_m) = V(\mathcal{R}_l) \cup V(\mathcal{R}_m) \cup V(\mathcal{R}_r) \ - \ V(T) \cup I \cup J. \tag{4.81}$$

$(\mathcal{R}'_l, \mathcal{R}^*_m, \mathcal{R}'_r)$ is called the **separating factorization** *of $(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r)$, denoted as*

$$(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r) \to (\mathcal{R}'_l, \mathcal{R}^*_m, \mathcal{R}'_r). \tag{4.82}$$

Remark 4.9. *Let $(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r) \to (\mathcal{R}'_l, \mathcal{R}^*_m, \mathcal{R}'_r)$ be as above. We list some basic properties of this operation that are direct from the definition.*

(1). $(\mathcal{R}'_l, R^*_m, \mathcal{R}'_r)$ is side-inner- and outer-canonical. The latter means their pair-wise

vertex intersections are in S'_l, S'_r and $S'_l \cap S'_r$, respectively. So if replace R^*_m by its largest ribbon, the triple would be canonical.

(2). $\mathcal{R}'_l \subseteq \mathcal{R}_l$, S'_l separates $(V(\mathcal{R}'_l),\ V(\mathcal{R}_l) - V(\mathcal{R}'_l))$ in $\mathcal{R}_l$. So we can talk about the part of $\mathcal{R}_l$ that is strictly to the right of S'_l, which is disjoint from R'_l and is further contained in $\mathcal{R}^*_m$. The similar fact holds for $\mathcal{R}_r$.

(3). In $\mathcal{R}_l$, since S'_l separates (I, A) and A is the unique min-separator of $\mathcal{R}_l$, there are $|A|$ many vertex-disjoint paths between A and S'_l. Similarly for $\mathcal{R}_r$.

Lemma 4.17. *Under the notation of Def. 4.26,*

(1). $|S'_l| + |S'_r| \geq |A| + |B| + 1$;

(2).[14] *Let $s = \frac{|A|+|B|}{2}$, p' be the max number of vertex-disjoint paths from S'_l to S'_r in $\mathcal{R}^*_m$, and p be the max number of vertex-disjoint paths from A to B in $\mathcal{R}_m$, then*

$$2(s' - s) + (p - p') + |\mathfrak{I}(\mathcal{R}^*_m)| \leq z(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r).$$

Proof. (1): by definition, there must be some unexpected pair-wise intersection between the triple $(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r)$. In either of the three cases of breaking the *outer condition* (Def. 4.22), there exists some $v \in Z$ that is in $V(\mathcal{R}_l) - A$ or $V(\mathcal{R}_r) - B$. W.l.o.g., suppose the first case happens. Then $S'_l \neq A$ since v can be reached from I without passing A by the left-generated condition on $\mathcal{R}_l$. Similarly, if $|S'_l| = |A|$ then it is A as A is the unique min-separator separating (I, A), so this is impossible. Thus $S'_l > A$.

(2). This is Lemma 7.14 of [13]. We omit the proof here. □

Apply to M'

Now we analyze $[L(DQ_0D)L^\top]_{\text{non-can}}$ in (4.78). Conceptually, the separating factorization allows us to "cancel" $[L(DQ_0D)L^\top]_{\text{non-can}}$ using $L, L^\top$. Namely, a term $(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r)$ in

14. Recall in our setting $\mathcal{R}_m$ is always a ribbon, without any isolated vertex.

$[L(DQ_0D)L^\top]_{\text{non-can}}$ at the (I,J)-th position can be "countered" by the term $-(\mathcal{R}'_l, \mathcal{R}^*_m, \mathcal{R}'_r)$ in a new matrix product $[L(DQ_1D)L^\top]_{\text{can}}$: R'_l at entry (I, S'_l) in L, R'_r at entry (S'_r, J) in $L^\top$, and the largest ribbon of $\mathcal{R}^*_m$ at (S'_l, S'_r) in a new middle matrix DQ_1D.

Of course, there are other triples whose separating factorization is the same, and each entry of L is a sum of many different R'_ls, so we need to insure that this cancellation works for them simultaneously. This is by the following proposition. We state a refined version (distinguishing the (i,j) parameter) which will be fully needed later (in Lem. 4.21).

Proposition 4.5. *(Solvability condition, cf. Claim 6.12 in [13]) Fix (I, J, S'_l, S'_r) and a improper ribbon $\mathcal{R}^*_m$ with side sets (S'_l, S'_r). Let $(\mathcal{R}'_l, \mathcal{R}'_r)$ be inner-canonical left and right ribbons with side sets $(I, S'_l), (S'_r, J)$ respectively, as in Def. 4.22. Let $(\mathcal{R}''_l, \mathcal{R}''_r)$ be another such ribbon pair, with the same reduced size $e(\mathcal{R}'_l) = e(\mathcal{R}''_l)$, $e(\mathcal{R}'_r) = e(\mathcal{R}''_r)$ (the same size, equivalently). Then for every fixed (i,j,z) the following holds: $\exists$ 1-1 matching between triples*

$$(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r) \text{ s.t. } \begin{cases} (\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r) \to (\mathcal{R}'_l, \mathcal{R}^*_m, \mathcal{R}'_r), \\ (e(\mathcal{R}_l),\ e(\mathcal{R}_r),\ z(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r)) = (i,j,z). \end{cases} \tag{4.83}$$

and

$$(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r) \text{ s.t. } \begin{cases} (\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r) \to (\mathcal{R}''_l, \mathcal{R}^*_m, \mathcal{R}''_r), \\ (e(\mathcal{R}_l),\ e(\mathcal{R}_r),\ z(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r)) = (i,j,z). \end{cases} \tag{4.84}$$

Moreover, this matching fixes every middle $\mathcal{R}_m$.

Proof. We give a reversible map from (4.83) onto (4.84). Take a $(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r)$ from (4.83). By Remark 4.9 (2), the part of $\mathcal{R}_l$ to the right of S'_l is in $\mathcal{R}^*_m$ hence is disjoint from both R'_l and R''_l. Similarly for $\mathcal{R}'_r$, $\mathcal{R}_r$. Now take a map $(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r) \mapsto (\phi(\mathcal{R}_l), \mathcal{R}_m, \phi(\mathcal{R}_r))$, where $\phi(\mathcal{R}_l)$ replace $\mathcal{R}'_l$ by $\mathcal{R}''_l$ in $\mathcal{R}_l$, $\phi(\mathcal{R}_r)$ replaces $\mathcal{R}'_r$ by $\mathcal{R}''_r$ in $\mathcal{R}_r$; so $\mathcal{R}^*_m$ (thus $\mathcal{R}_m$) is unchanged.

Since $\mathcal{R}'_l$, $\mathcal{R}''_l$ have the same size by assumption, by the disjointness property in Remark 4.9

(2), the replacement operation keeps the size of $\mathcal{R}_l$. Moreover, $\mathcal{R}_l$, $\phi(\mathcal{R}_l)$ have the same right set which is the unique min-separator of both, so $e(\mathcal{R}_l) = e(\phi(R_l))$. Similarly for $\mathcal{R}_r, \phi(\mathcal{R}_r)$, so the parameter (i, j) is unchanged by ϕ. The intersection parameter z is unchanged too, since the changed part is disjoint from $Z(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r)$. Finally, the inverse map is given the same way by changing the role of $(\mathcal{R}'_l, \mathcal{R}'_r)$ and $(\mathcal{R}''_l, \mathcal{R}''_r)$. □

We are going to define **one round of factorization**. Let L be as Def. (4.20), Q be any $\binom{[n]}{\leq d/2} \times \binom{[n]}{\leq d/2}$-matrix with $Q(A, B) = \sum_{T_m:\ |V(T_m)\cup A\cup B|\leq\tau} (\frac{\omega}{n})^{|V(\mathcal{R}_m)|} q(\mathcal{R}_m) \cdot \chi_{T_m}$, where $\mathcal{R}_m$ denotes $(A, B; T_m)$ and $q(\cdot)$ is a function symmetric w.r.t. shapes. Let us define matrices $Q', \mathcal{E}_{\text{negl}}$ as follows so that

$$(LQL^\top)_{\text{non-can}} = (LQ'L^\top)_{\text{can}} + \mathcal{E}_{\text{negl}}. \tag{4.85}$$

Let $Q'(A, B) := \sum_{T_m:\ |V(T_m)\cup A\cup B|\leq\tau} (\frac{\omega}{n})^{|V(\mathcal{R}_m)|} q'(\mathcal{R}_m)\chi_{T_m}$, $q'(\mathcal{R}_m)$ defined as below. For any $\mathcal{R}_m = (A, B; T_m)$, let $t = |V(\mathcal{R}_m)| (\leq \tau)$, $s = \frac{|A|+|B|}{2}$; then for every improper $\mathcal{R}^*_m$ that contains $\mathcal{R}_m$ as its largest ribbon and $|V(\mathcal{R}^*_m)| \leq \tau$, **fix** any pair $(\mathcal{R}'_l, \mathcal{R}'_r)$ s.t. $(\mathcal{R}'_l, \mathcal{R}^*_m, \mathcal{R}'_r)$ is the separating factorization for some triple with $|V(\mathcal{R}'_l)|, |V(\mathcal{R}'_r)| \leq \tau$ (if there is none, exclude $\mathcal{R}^*_m$ in the summation below) and let

$$\begin{aligned} q'(\mathcal{R}_m) &= \sum_{\substack{\mathcal{R}^*_m:\ \text{improper ribbon on } (A,B) \\ |V(\mathcal{R}^*_m)|\leq\tau \\ \text{largest ribbon is } \mathcal{R}_m}} (\frac{\omega}{n})^{|\mathfrak{I}(\mathcal{R}^*_m)|} \cdot q''(\mathcal{R}^*_m) \quad \text{where} \\ q''(\mathcal{R}^*_m) &= \sum_{1\leq z\leq d/2} \sum_{\substack{\mathcal{P}=(\mathcal{R}_l,\mathcal{R},\mathcal{R}_r):\ \text{side-inn. can.} \\ \mathcal{P}\to(\mathcal{R}'_l,\mathcal{R}^*_m,\mathcal{R}'_r)\ \text{for the fixed } \mathcal{R}'_l,\mathcal{R}'_r \\ z(\mathcal{P})=z}} (\frac{\omega}{n})^z \cdot q(\mathcal{R}). \end{aligned} \tag{4.86}$$

Note $q'(\mathcal{R}_m)$ doesn't depend on the choice $(\mathcal{R}'_l, \mathcal{R}'_r)$ by Prop. 4.5, so $q'(\cdot)$ is also symmetric w.r.t. shapes. Now define $\mathcal{E}_{\text{negl}}$ such that (4.85) holds.

Lemma 4.18. *(One round) In the above notation,*

(1). W.p. $> 1 - n^{-9\log n}$ *over* G, $\left\|\mathcal{E}_{\text{negl}}\right\| \leq \max\{q(A,B;T)\} \cdot n^{-\epsilon\tau}$;

(2). Given an $\mathcal{R}_m$*, let* p *be the max number of vertex-disjoint paths in it between the two side sets. If there is a number* C *s.t.*

$$\forall \mathcal{R}_m,\ |q(\mathcal{R}_m)| \leq C \cdot (\frac{\omega}{n^{1-\epsilon}})^{s-p} \tag{4.87}$$

then $|q'(\mathcal{R}_m)| \leq C \cdot (\frac{\omega}{n^{1-\epsilon}})^{s-p+1/3}$ *for all* $\mathcal{R}_m$.

Proof. We compare $[LQ'L^\top]_{\text{can}}$, $[LQL^\top]_{\text{non-can}}$ as step (0), then prove (1), (2).

(0). For any fixed (I,J), recall $[LQL^\top]_{\text{non-can}}(I,J)$ is

$$\sum_{\substack{(\mathcal{R}_l,\mathcal{R}_m,\mathcal{R}_r)\text{: side. inn. can.}\\ \text{non-outer-can.}\\ \text{all three have size } \leq\tau}} (\frac{\omega}{n})^{|V(\mathcal{R}_l)|+|V(\mathcal{R}_m)|+|V(\mathcal{R}_r)|-|A|-|B|} q(\mathcal{R}_m)\chi_{T_l\oplus T_m\oplus T_r} \tag{4.88}$$

where we denote the side sets of $\mathcal{R}_m$ by (A,B). For each $(\mathcal{R}_l,\mathcal{R}_m,\mathcal{R}_r)$ in the sum, there is a unique $(\mathcal{R}'_l,\mathcal{R}^*_m,\mathcal{R}'_r)$ that is its separating factorization: $(\mathcal{R}_l,\mathcal{R}_m,\mathcal{R}_r) \to (\mathcal{R}'_l,\mathcal{R}^*_m,\mathcal{R}'_r)$. There are two cases of a term in (4.88).

First case: $|V(\mathcal{R}^*_m)| \leq \tau$. In this case, there is the corresponding term

$$(\frac{\omega}{n})^{|V(\mathcal{R}'_l)|+|V(\mathcal{R}'_m)|+V(\mathcal{R}'_r)|-|S'_l|-|S'_r|} \cdot (\frac{\omega}{n})^{z+|\mathcal{I}(\mathcal{R}^*_m)|} \cdot q(\mathcal{R}'_m)\chi_{T'_l\oplus T^*_m\oplus T'_r} \tag{4.89}$$

in $(LQ'L^\top)_{\text{can}}(I,J)$, where $\mathcal{R}'_m$ denotes the largest ribbon of $\mathcal{R}^*_m$, T^*_m means the edges of $\mathcal{R}'_m$, and $z \geq 1$ is the intersection size of $(\mathcal{R}_l,\mathcal{R}_m,\mathcal{R}_r)$. In the separating factorization, recall $T'_l \oplus T^*_m \oplus T'_r = T_l \oplus T_m \oplus T_r$, $V(\mathcal{R}_l) \cup V(\mathcal{R}_m) \cup V(\mathcal{R}_r)| = |V(\mathcal{R}'_l)| + |V(\mathcal{R}^*_m)| + |V(\mathcal{R}'_r)| - |S'_l| - |S'_r| = |V(\mathcal{R}_l)| + |V(\mathcal{R}_m)| + |V(\mathcal{R}_r)| - |A| - |B| - z$ and $|V(R^*_m)| = |V(\mathcal{R}'_m)| + |\mathcal{I}(\mathcal{R}^*_m)|$, so the coefficient in (4.89) equals the one in (4.88) for $(\mathcal{R}'_l,\mathcal{R}^*_m,\mathcal{R}'_r)$. Conversely, at a position $(\mathcal{R}'_l,\mathcal{R}'_r)$, $[LQ'L^\top]_{\text{can}}$ by (4.86) and Prop. 4.5 collects exactly all terms from a

triple $(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r)$ in $[LQL^\top]_{\text{non-can}}$ whose separating factors have $(\mathcal{R}'_l, \mathcal{R}'_r)$ as the left, right part and whose $\mathcal{R}^*_m$ has size $\le \tau$.

Therefore, $\mathcal{E}_{\text{negl}}$ will collect exactly all terms in the next case.

Second case: $|V(\mathcal{R}^*_m)| > \tau$. By the above explanation, $\mathcal{E}_{\text{negl}}(I,J) =$

$$\sum_{\substack{(\mathcal{R}_l,\mathcal{R}_m,\mathcal{R}_r)\text{: side. inn. can.}\\ \text{non-outer-can.}\\ \text{all three has size } \le\tau\\ \text{resulting } |V(\mathcal{R}^*_m)|>\tau}} (\frac{\omega}{n})^{|V(\mathcal{R}_l)|+|V(\mathcal{R}_m)|+|V(\mathcal{R}_r)|-|A|-|B|} q(\mathcal{R}_m)\chi_{T_l\oplus T_m\oplus T_r}. \tag{4.90}$$

where we omit writing the sum condition "$\mathcal{R}_l$ ($\mathcal{R}_r$) has left (right) vertex-set as I (J)".

(1). Fix any $(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r)$ in (4.90). Note $|\mathcal{I}(\mathcal{R}^*_m)| \le z + d/2$ as a quick corollary of Lemma 4.17. Fix $T = T_l \oplus T_m \oplus T_r$ and $a > \tau - |V(T)\cup I\cup J|$, we count the number of triples in (4.90) resulting in $(\frac{\omega}{n})^{|V(T)\cup I\cup J|+a}\cdot\chi_T$ (ignoring $q(\mathcal{R}_m)$ for the moment): to create such a triple, we choose a set as $\mathcal{I}(\mathcal{R}^*_m)$ of size $\le a/2+d/4$, a intended to be $|\mathcal{I}(\mathcal{R}^*_m)|+z$ so $a \ge 2\mathcal{I}(\mathcal{R}^*) - d/2$ (by the above), then decide the triple over the vertex set in $< 3^{3\tau}\cdot 2^{3\binom{\tau}{2}}$ many ways. So, if let $B_0 := \max\{q(\cdot)\}$, then $\big|\text{coefficient of } \chi_T \text{ in (4.90)}\big| \le B_0(\frac{\omega}{n})^{|V(T)\cup I\cup J|+a} n^{\frac{(a+d)}{2}} 2^{2\tau^2} = B_0(\frac{\omega}{n^{1-2\epsilon}})^{|V(T)\cup I\cup J|} n^{-2\epsilon(|V(T)\cup I\cup J|)}(\frac{\omega}{\sqrt{n}})^a n^{\frac{d}{2}} 2^{2\tau^2} \le B_0 n^{-\frac{|V(T)\cup I\cup J|}{2} - 2\epsilon(|V(T)\cup I\cup J|+a)+\frac{d}{2}} 2^{2\tau^2}$ $\le B_0(n^{-1/2})^{|V(T)\cup I\cup J|} n^{-1.5\epsilon\tau}$, where we used $\omega \le n^{1/2-4\epsilon}$, $|V(T)\cup I\cup J| + a > \tau$ (case condition) and $d < \epsilon\tau/10$, $2^{2\tau} < n^{\epsilon/10}$. Also, all χ_T appearing in (4.90) has $|V(T)| \le 3\tau$. By Lemma 4.10, for any (I,J), w.p.$> 1 - n^{-10\log n}$,

$$|\mathcal{E}_{\text{negl}}(I,J)| < \sum_{a=0}^{3\tau} B_0 n^{-a/2} n^{-1.5\epsilon\tau} n^{a/2} n^{4\log\log n} 2^{a^2} < n^{-1.4\epsilon\tau}.$$

By union bound on (I,J), w.p.$> 1 - n^{-9\log n}$, $\big\|\mathcal{E}_{\text{negl}}\big\| < n^d \cdot n^{-1.4\epsilon\tau} < n^{-\epsilon\tau}$.

(2). $q'(\mathcal{R}_m) = \sum_{\substack{z,\mathcal{R}^*_m:\\ \text{largest ribbon } = \mathcal{R}_m}} (\frac{\omega}{n})^{|\mathcal{I}(\mathcal{R}^*_m)|+z} \sum_{\substack{\mathcal{P}=(\mathcal{R}_l,\mathcal{R},\mathcal{R}_r)\text{: side-inn. can.}\\ \mathcal{P}\to(\mathcal{R}'_l,\mathcal{R}^*_m,\mathcal{R}'_r) \text{ for the fixed } \mathcal{R}'_l,\mathcal{R}'_r\\ z(\mathcal{P})=z}} q(\mathcal{R})$ for any fxied $\mathcal{R}_m$, by (4.86). For a fixed $\mathcal{R}^*_m$, there are $\le 8^{z\tau} < n^{\epsilon z}$ many triples in the inner sum

(recall $\mathcal{R}'_l, \mathcal{R}'_r$ are fixed), as after fixing how each vertex appears in all three ribbons and fixing side sets $A, B \subseteq \mathcal{R}^*_m$, we only need to decide the edges that appear more than once in the original triple; such an edge must has at least one end in the already fixed (multi-set) Z. So by Lem. 4.17(2), (4.87), $\big|\text{inner sum}\big| \leq n^{\epsilon z}(\frac{\omega}{n})^{z+|\mathcal{I}(\mathcal{R}^*_m)|} \cdot |q(\mathcal{R})| \leq (\frac{\omega}{n^{1-\epsilon}})^{2(s'-s)+(p-p')+2|\mathcal{I}(\mathcal{R}^*_m)|}$ $\cdot C \cdot (\frac{\omega}{n^{1-\epsilon}})^{s-p} \leq C \cdot (\frac{\omega}{n})^{2|\mathcal{I}(\mathcal{R}^*_m)|} \cdot (\frac{\omega}{n^{1-\epsilon}})^{s'-p'+1/2}$, where the parameters (s,p) for $\mathcal{R}$ and (s',p') for $\mathcal{R}_m$ have the same meaning as in the lemma, and $s'-s \geq 1/2$ by Lem. 4.17(1).

Finally, in the outer sum, for any i_0 there are $< n^{i_0}$ many $\mathcal{R}^*_m$ s.t. $|\mathcal{I}(\mathcal{R}^*_m)| = i_0$ and $1 \leq z \leq 3\tau$. So $|q'(\mathcal{R}_m)| \leq 3\tau \sum_{i_0=0}^{d/2} C \cdot n^{i_0}(\frac{\omega}{n})^{2i_0} \cdot (\frac{\omega}{n^{1-\epsilon}})^{s'-p'+1/2} \leq C \cdot (\frac{\omega}{n^{1-\epsilon}})^{s'-p'+1/3}$. □

Apply Lemma 4.18 to $[L(DQ_0D)L^\top]_{\text{non-can}}$ with $Q \leftarrow (DQ_0D)$, then repeat as described under (4.79), we get the **recursive approximate factorization** of M':

$$M' = L\bigg(D(Q_0 - Q_1 + Q_2 - ... \pm Q_d)D\bigg)L^\top - \mathcal{E}_{\text{deg}} + \bigg(-\mathcal{E}_{1;\text{negl}} + ... \pm \mathcal{E}_{1+d;\text{negl}}\bigg). \quad (4.91)$$

Here it implicitly used:

Proposition 4.6. *([13] Claim 6.15)* $Q_{d+1} = 0$.

Proof. First we use induction in k to show that, in Q_k every appearing ribbon $R_m = (A, B; T_m)$ has $|A| + |B| \geq k$. The base case $k = 0$ is trivial. For $k+1$, by Lemma 4.18 every $\mathcal{R}'_m = (A', B'; T'_m)$ in Q_{k+1} is the largest ribbon of some $\mathcal{R}^*_m$ in the separating factorization of some non-outer-canonical triple in $L(DQ_kD)L^\top$. Suppose that triple has the middle part $\mathcal{R}_m = (A, B; T_m)$, then by inductive hypothesis $|A| + |B| \geq k$. By Lemma 4.17(1), $|A'| + |B'| \geq |A| + |B| + 1 \geq k + 1$, completing induction. For $k = 1 + d$, no ribbon with both side sets in $\binom{[n]}{d/2}$ can satisfy this. □

We have completed the preparation of the recursive factorization technique.

Remark 4.10. *PSDness of M' would follow from* (4.91) *by some standard steps (similar to the arguments in section 4.8), which we omit here.*

4.7 PSDness analysis, II: Exact recursive factorization

Now we apply the recursive approximate factorization to matrices M_c^R in (4.56).

The high-level steps are the same as in section 4.6: define the **first-approximate** factorization (Def. 4.27, 4.29 and Lem. 4.19), then refine it recursively to get the eventual factorization, Lemma 4.20, which is the main result of this section.

Definition 4.27. *Fix $R \in \binom{[n]}{\leq \frac{d}{2}}$. For every $i = 0, ..., \tau$ define matrix $L^{R,i}$ as*

$$L^{R,i}(I,A) = \begin{cases} 0 & \text{, if } R \not\subseteq I \cap A; \\ \sum\limits_{\substack{T:\ |V(T)\cup I\cup A|\leq\tau \\ A=S_l(I,A;T) \\ T\cap E(A)=\emptyset \\ (I,A;T)\ \text{left-generated} \\ e_{I,A}(T)=i}} (\frac{\omega}{n})^i \chi_T & \text{, o.w.} \end{cases} \tag{4.92}$$

of dimension $\binom{[n]}{\frac{d}{2}} \times \binom{[n]}{\leq \frac{d}{2}}$. Let $\widetilde{L^R} := (L^{R,0}, ..., L^{R,\tau})$ the **left factor**, *$(\widetilde{L^R})^\top$ the* **right factor**. *Note these matrices do not depend on "c".*

Definition 4.28. $D^\tau := \operatorname{diag}\left((\frac{\omega}{n})^{\frac{|A|}{2}}\right)_{A\subseteq[n]:\ |A|\leq d/2} \otimes \mathrm{Id}_{\{0,...,\tau\}\times\{0,...,\tau\}}$.

Our goal is to find a middle, $\left(\binom{[n]}{\leq \frac{d}{2}} \times (\tau+1)\right) \times \left(\binom{[n]}{\leq \frac{d}{2}} \times (\tau+1)\right)$-matrix Q_c^R s.t. $M_c^R \approx \underbrace{(L^{R,0}, ..., L^{R,\tau})}_{\widetilde{L^R}} \cdot \left(D^\tau \cdot Q_c^R \cdot D^\tau\right) \cdot \underbrace{(L^{R,0}, ..., L^{R,\tau})^\top}_{\left(\widetilde{L^R}\right)^\top}$, achived as Lemma 4.20.

Remark 4.11. *Here the middle matrix has "larger" dimension ($\times\{0, ..., \tau\}$) compared to the non-exact case. The reason is that in* (4.54)*, or more broadly in any exact pseudo-expectation generated by the method in section 4.3.2, the parameter $a = |V(T) \cup I \cup J|$ appears nestedly in an essential way—in the non-exact case* (4.28)*, $(\frac{\omega}{n})^a = (\frac{\omega}{n})^{e(\mathcal{R}_l)+|V(\mathcal{R}_m)|+e(\mathcal{R}_r)}$ (Remark 4.8) is a product of the "local" left, middle, right terms; but now terms like $\binom{a+l-d}{c} \cdot \binom{n-a}{l-c}$ are no longer log-additive in a, losing the product structure. Our method will need to consider additional parameters as $(e(\mathcal{R}_l),\ e(\mathcal{R}_r)) \in \{0, ...\tau\} \times \{0, ...\tau\}$.*

The $(\frac{\omega}{n})^a$ factor in (4.57) can be separated into left, right, middle factors as before, $(\frac{\omega}{n})^a = (\frac{\omega}{n})^{e(\mathcal{R}_l)} \cdot (\frac{\omega}{n})^{|V(\mathcal{R}_m)|} \cdot (\frac{\omega}{n})^{e(\mathcal{R}_r)}$; we leave the "hard" factor $Y_c(r,a)$ to the middle matrix $Q_c^R\Big((\cdot,e_l),(\cdot,e_r)\Big)$ where e_l, e_r are the "intended" reduced sizes, as below.

Definition 4.29. *(First-approximate factorization) Define $Q_{c,0}^R$ to be the $\{0,...,\tau\}\times\{0,...,\tau\}$-block matrix, each block of dimension $\binom{[n]}{\leq d/2}\times\binom{[n]}{\leq d/2}$, that is 0 outside of the principal minor $S^R \times S^R$ where*

$$S^R = \{(A,i) \in \binom{[n]}{\leq d/2} \times \{0,...,\tau\} \mid A \supseteq R, |A| + i \geq \frac{d}{2}\}, \tag{4.93}$$

and on this principal minor, $Q_{c,0}^R\Big((A,i),(B,j)\Big) =$

$$\sum_{\substack{T_m: |V(T_m)\cup A\cup B| \leq \tau \\ A,B\in \mathrm{mSep}_{A,B}(T_m)}} (\frac{\omega}{n})^{|V(T_m)\cup A\cup B| - \frac{|A|+|B|}{2}} \cdot \underbrace{Y_c\big(|R|,\ |V(T_m)\cup A\cup B| + (i+j)\big)}_{\text{defined by (4.54)}} \cdot \chi_{T_m} \tag{4.94}$$

$\widetilde{L^R} \cdot \Big(D^\tau \cdot Q_{c,0}^R \cdot D^\tau\Big) \cdot \Big(\widetilde{L^R}\Big)^\top$ is called the **first approximate factorization** *of M_c^R.*

Remark 4.12. *(Intended meaning of parameters in $Q_{c,0}^R$.)*

(1). The set S^R (4.93) is defined independently of c, where the condition $|A| + i \geq d/2$ is by the intended meaning of i as $|V(T')\backslash A| \geq |I| - |A|$ for some ribbon $(I, A; T')$ in $\widetilde{L^R}$. If $|A| + i < d/2$ the corresponding column in $\widetilde{L^R}$ is always 0. Similarly for j.

(2). $Q_{c,0}^R$ is supported only on those $((A,i),(B,j)) \in S^R \times S^R$ with $|A| = |B|$.

(3). (cf. Remark 4.8) Regarding (4.94), in "canonical" situations (i.e. for outer-canonical products in $\widetilde{L^R} \cdot \Big(D^\tau \cdot Q_{c,0}^R \cdot D^\tau\Big) \cdot \Big(\widetilde{L^R}\Big)^\top$) it holds that

$$|V(T_m)\cup A\cup B| + (i+j) = |V(T)\cup I\cup J|$$

for any ribbon $\mathcal{R} = (I, J; T)$ that has $(A, B; T_m)$ as the middle part of its canonical decom-

position and $e(\mathcal{R}_l) = i$, $e(\mathcal{R}_r) = j$.

Lemma 4.19. *($Q^R_{c,0}$ gives the first-approximation) Fix R, $c \le |R|$. For every $(I, J; T)$ s.t. $|V(T) \cup I \cup J| \le \tau$ and $R \subseteq I \cap J$, there is exactly one outer-canonical product in the $XYX^\top$-type matrix product*

$$\underbrace{\widetilde{L^R}}_{\text{as ``X''}} \cdot \underbrace{\left(D^\tau \cdot Q^R_{c,0} \cdot D^\tau\right)}_{\text{as ``Y''}} \cdot \left(\widetilde{L^R}\right)^\top. \tag{4.95}$$

It is from the canonical decomposition of $(I, J; T)$, and results in term $M^R_c(I, J; T)\chi_T$.

Proof. Suppose $R \subseteq I \cap J$. First, note every triple in (4.95) is inner-canonical by definition of $\widetilde{L^R}, Q^R_{c,0}$, so all outer-canonical triples there 1-1 correspond to their triple-product $(I, J; T)$ via the canonical decomposition.

Fix an $(I, J; T)$ and its canonical decomposition, where $|V(T) \cup I \cup J| \le \tau$. $(I, A; T')$ appears exactly once in $\widetilde{L^R}(I, A)$ in block L^{R,e_l}, where $e_l = e_{I,A}(T')$; similarly for $(J, B; T'')$ and $e_r = e_{J,B}(T'')$. Further, there is exactly one outer-canonical product in (4.95) corresponding to this triple, with coefficient

$$L^{R,e_l}(I, A; T') \cdot (\frac{\omega}{n})^{\frac{|A|}{2}} \cdot Q^R_{c,0}(A, B; T_m) \cdot (\frac{\omega}{n})^{\frac{|B|}{2}} \cdot L^{R,e_r}(J, B; T''). \tag{4.96}$$

By definition (4.92), (4.94), if let $a := |V(T) \cup I \cup J|$ then the above coefficient is $(\frac{\omega}{n})^a \cdot Y_c(|R|, a) = M^R_c(I, J; T)$. Compare (4.54), (4.57), where note $a = |V(T) \cup I \cup J| = e_l + |V(T_m) \cup A \cup B| + e_r$ by canonicality, we see that the lemma holds. □

Definition 4.30. *Let $\mathcal{E}^R_{c;\deg}$ be the matrix that collects all products in $[\widetilde{L^R} \cdot \left(D^\tau Q^R_{c,0} D^\tau\right) \cdot \left(\widetilde{L^R}\right)^\top]_{\text{can}}$ with $|V(T) \cup I \cup J| > \tau$ (cf. (4.78)), and $[\widetilde{L^R} \cdot (D^\tau Q^R_{c,0} D^\tau) \cdot (\widetilde{L^R})^\top]_{\text{non-can}}$ collects all terms from triples that are non-outer-canonical.*

Summarizing, we have the first-approximate factorization:

$$M_c^R = \widetilde{L^R} \cdot \left(D^\tau Q_{c,0}^R D^\tau\right) \cdot \left(\widetilde{L^R}\right)^\top - [\widetilde{L^R} \cdot \left(D^\tau Q_{c,0}^R D^\tau\right) \cdot \left(\widetilde{L^R}\right)^\top]_{\text{non-can}} - \mathcal{E}_{c;\deg}^R. \quad (4.97)$$

The crucial fact is that again matrix $[\widetilde{L^R} \cdot \left(D^\tau Q_{c,0}^R D^\tau\right) \cdot \left(\widetilde{L^R}\right)^\top]_{\text{non-can}}$ factorizes through $\widetilde{L^R}, (\widetilde{L^R})^\top$ approximately, allowing us to factorize recursively (cf. (4.91)).

Definition 4.31. *For a fixed $R \subseteq [n]$, we say a function f defined on ribbons on the ground set $[n]$ is R-**symmetric w.r.t. shapes**, if f takes the same values on isomorphic ribbons whose side sets both contain R.*

The main conclusion of this section is the following.

Lemma 4.20. *(Recursive factorization, exact case) $\forall R \in \binom{[n]}{\leq d/2}$, $0 \leq c \leq |R|$,*

$$M_c^R = \widetilde{L^R} \cdot \left[D^\tau \left(Q_{c,0}^R - Q_{c,1}^R + ... \pm Q_{c,d}^R\right) D^\tau\right] \cdot \left(\widetilde{L^R}\right)^\top + \mathcal{E}_c^R \quad \textit{where} \quad (4.98)$$

(1). All $Q_{c,k}^R$'s are supported on the principal minor $S^R \times S^R$ ((4.93));

(2). $Q_{c,0}^R$ is by Definition 4.29;

(3). $\forall 1 < k \leq d/2$, $Q_{c,k}^R$ is a $(\tau+1) \times (\tau+1)$-block-matrix supported on $S^R \times S^R$,

$$Q_{c,k}^R\Big((A,i),(B,j)\Big) = \sum_{T_m : |V(T_m) \cup A \cup B| \leq \tau} q_{c,k}^R(\mathcal{R}_m, i, j) \cdot \chi_{T_m} \quad (4.99)$$

where we denote $\mathcal{R}_m = (A, B; T_m)$, $q_{c,k}^R(\cdot, i, j)$'s are R-symmetric w.r.t. shapes, and

$$\forall (i,j) \quad |q_{c,k}^R(\mathcal{R}_m, i, j)| \leq \tau^{5\tau} \cdot (\frac{\omega}{n^{1-\epsilon}})^{s-p+k/3} \quad (4.100)$$

where $s = \frac{|A|+|B|}{2}$, p is the max number of vertex-disjoint paths between A, B in $\mathcal{R}_m$.

(4). For any G, $\mathcal{E}_c^R(G)$ is supported within rows and columns that is clique in G and contains R. Moreover, w.p. $> 1 - n^{-9\log n}$, $\left\|\mathcal{E}_c^R\right\| < n^{-\epsilon\tau/2}$.

To prove it, as before, we first describes a single round of factorization using an analogue of Lemma 4.18. Fix an $R \subseteq \binom{[n]}{d/2}$ and for ease of notation denote $n_1 := \binom{[n]}{d/2} \times (\tau+1)$. Let $\widetilde{L^R}$ be from Definition 4.27, Q^R be any $n_1 \times n_1$-matrix supported on $S^R \times S^R$ and

$$Q^R((A,i),(B,j)) = \sum_{T_m:\ |V(T_m)\cup A\cup B|\le\tau} (\frac{\omega}{n})^{|V(\mathcal{R}_m)|} q(\mathcal{R}_m,i,j)\cdot\chi_{T_m} \tag{4.101}$$

where $\mathcal{R}_m$ denotes $(A,B;T_m)$, and $q(\cdot,i,j)$ is R-symmetric w.r.t. shapes for any fixed (i,j). We define matrix $Q', \mathcal{E}_{\text{negl}}$ so that

$$[\widetilde{L^R}\cdot Q\cdot(\widetilde{L^R})^\top]_{\text{non-can}} = [\widetilde{L^R}\cdot Q'\cdot(\widetilde{L^R})^\top]_{\text{can}} + \mathcal{E}_{\text{negl}}. \tag{4.102}$$

Namely, let $Q'((A,i),(B,j)) = \sum_{T_m:\ |V(T_m)\cup A\cup B|\le\tau} (\frac{\omega}{n})^{|V(\mathcal{R}_m)|} q'(\mathcal{R}_m,i,j)\chi_{T_m}$ and be only supported on $S^R\times S^R$, with $q'(\mathcal{R}_m,i,j)$ as follows. For a fixed $\mathcal{R}_m=(A,B;T_m)$ and (i,j), let $t=|V(\mathcal{R}_m)|\le\tau$, $s=\frac{|A|+|B|}{2}$, and for every improper ribbon $\mathcal{R}^*_m$ that contains $\mathcal{R}_m$ as its largest ribbon and $|V(\mathcal{R}^*_m)|\le\tau$, fix any a ribbon pair $(\mathcal{R}'_l,\mathcal{R}'_r)$ so that $(\mathcal{R}'_l,\mathcal{R}^*_m,\mathcal{R}'_r)$ is the separating factorization of some ribbon triple, $|V(\mathcal{R}'_l)|,|V(\mathcal{R}'_r)|\le\tau$ *and*

$$(e(\mathcal{R}'_l),e(\mathcal{R}'_r)) = (i,j). \tag{4.103}$$

If there is no such choice, exclude this $\mathcal{R}^*_m$ in the summation below. Define

$$q'(\mathcal{R}_m,i,j) = \sum_{\substack{\mathcal{R}^*_m\text{: improper ribbon on }(A,B)\\ |V(\mathcal{R}^*_m)|\le\tau\\ \text{largest ribbon is }\mathcal{R}_m}} (\frac{\omega}{n})^{|\mathfrak{I}(\mathcal{R}^*_m)|}\cdot q''(\mathcal{R}^*_m,i,j) \quad \text{where}$$

$$q''(\mathcal{R}^*_m,i,j) = \sum_{\substack{(z,i_1,j_1):\\ 1\le z\le d/2}} \sum_{\substack{\mathcal{P}=(\mathcal{R}_l,\mathcal{R},\mathcal{R}_r)\text{: side-inn. can.}\\ \mathcal{P}\to(\mathcal{R}'_l,\mathcal{R}^*_m,\mathcal{R}'_r)\text{ for the fixed }\mathcal{R}'_l,\mathcal{R}'_r\\ z(\mathcal{P})=z,\ e(\mathcal{R}_l)=i_1,e(\mathcal{R}_r)=j_1}} (\frac{\omega}{n})^z\cdot q(\mathcal{R},i_1,j_1).$$

Here, $q''(\mathcal{R}_m, i, j)$ doesn't depend on the choice $(\mathcal{R}'_l, \mathcal{R}'_r)$ by (**the full of**) Prop. 4.5, so $q'(\cdot, i, j)$ is also R-symmetric w.r.t. shapes. Finally, $\mathcal{E}_{\text{negl}}$ is defined s.t. (4.102) holds.

Lemma 4.21. *(One round of factorization, exact case)*

(1). W.p. $> 1 - n^{-9\log n}$ *over* G, $\left\|\mathcal{E}_{\text{negl}}\right\| \le \max\{q(\cdot)\} \cdot n^{-\epsilon\tau}$;

(2). If there is a number C *for which*

$$\forall \mathcal{R}_m, i, j \quad |q(\mathcal{R}_m, i, j)| \le C \cdot (\frac{\omega}{n^{1-\epsilon}})^{s-p} \tag{4.104}$$

where p *is the max number of vertex-disjoint paths between* A, B *in* $\mathcal{R}_m$*, then*

$$\forall \mathcal{R}_m, i, j \quad |q'(\mathcal{R}_m)| \le C \cdot (\frac{\omega}{n^{1-\epsilon}})^{s-p+1/3}.$$

Proof. (of Lemma 4.21) The proof is almost the same as that of Lemma 4.18; we point out and explain the differences below. First, note the support condition (i.e. only on $S^R \times S^R$) doesn't affect anything since $\widetilde{L^R}$ is automatically 0 on columns and rows not in S^R.

In step (0), we expand $[\widetilde{L^R} \cdot Q' \cdot (\widetilde{L^R})^\top]_{\text{can}}$ to compare with $[\widetilde{L^R} \cdot Q \cdot (\widetilde{L^R})^\top]_{\text{non-can}}$ term-wise, using Prop. 4.5. Here, notice that when (i, j) and $\mathcal{R}^*_m$ are fixed, the size of any choice of $(\mathcal{R}'_l, \mathcal{R}'_r)$ satisfying (4.103) are also fixed, so the proposition is applicable.

The comparison of orders on $(\frac{\omega}{n})$ between the two is the same as in step (0) in the proof of Lem. 4.18, and we get that $\mathcal{E}_{\text{negl}}$ collects all products in $[\widetilde{L^R} \cdot Q \cdot (\widetilde{L^R})^\top]_{\text{non-can}}$ whose $\mathcal{R}^*_m$ in separating factorization exceeds size τ. I.e. $\mathcal{E}_{\text{negl}}(I, J)) =$

$$\sum_{i,j} \sum_{\substack{(\mathcal{R}_l, \mathcal{R}_m, \mathcal{R}_r)\text{: side inn. can.} \\ \text{non-outer-can.} \\ \text{all three has size} \le \tau \\ |V(\mathcal{R}^*_m)| > \tau,\ (e(\mathcal{R}_l), e(\mathcal{R}_r)) = (i,j)}} (\tfrac{\omega}{n})^{|V(\mathcal{R}_l)| + |V(\mathcal{R}_m)| + |V(\mathcal{R}_r)| - |A| - |B|} q(\mathcal{R}_m, i, j) \chi_T,$$

where $T = T_l \oplus T_m \oplus T_r$ and we omitted writing the default condition in the summation that $\mathcal{R}_l$ ($\mathcal{R}_r$) has the left (right) side vertex set I (J).

Conclusions (1), (2) follow from the same estimates as in Lem. 4.18 (after (4.90)). Note the norm bound from Theorem 4.3 is still applicable to our case where a graph matrix can be nonzero only on (A, B) s.t. $R \subseteq A \cap B$; this is because we can process the original graph matrix by $\mathrm{diag}(1_R) \cdot (-) \cdot \mathrm{diag}(1_R)$ where $1_R(A) = 1$ iff $R \subseteq A$, which does not increase norm. Finally, for (1) we have an extra $(1+\tau)^2$-factor compared with before (occurring from a union bound on blocks), but the estimate in Lem. 4.18 is loose enough that when multiplied by this additional factor it is still $< n^{-\epsilon\tau}$. □

Proof. (of Lemma 4.20) As before, we apply Lemma 4.21 to $[\widetilde{L^R} \cdot \left(D^\tau Q^R_{c,0} D^\tau\right) \cdot \left(\widetilde{L^R}\right)^\top]_{\text{non-can}}$ repeatedly. As the result, M^R_c is decomposed as:

$$\widetilde{L^R}\left(D^\tau \left(Q^R_{c,0} - Q^R_{c,1} + ... \pm Q^R_{c,d}\right) D^\tau\right) \left(\widetilde{L^R}\right)^\top - \mathcal{E}^R_{c;\text{deg}} + \left(-\mathcal{E}^R_{c,1;\text{negl}} + ... \pm \mathcal{E}^R_{c,d+1;\text{negl}}\right) \tag{4.105}$$

where again it uses that $Q^R_{c,d+1} = 0$, by the same Prop. 4.6.

(1). All $Q^R_{c,k}$ is supported within $S^R \times S^R$ by definition of a round (Lem. 4.21).

(2). This is by definition.

(3). The coefficients $\{q^R_{c,k}(\cdot, i, j)\}$ of each $Q^R_{c,k}$ $(k = 0, 1, ..., d)$ are always R-symmetric w.r.t. shapes by Lem. 4.21. By (4.94) and Lem. 4.13(4), $|q^R_{c,0}(\mathcal{R}_m)| = |Y_c(|R|, |\mathcal{R}_m|)| \cdot (\frac{\omega}{n})^{|V(T) \cup A \cup B|} \leq \tau^{5\tau} \cdot 1$ for all $\mathcal{R}_m, i, j$. Note $Q^R_{c,0}$ is special in that for all $\mathcal{R}_m = (A, B; T_m)$ in it, there are $|A| = |B|$ many vertex-disjoint paths between A, B in $\mathcal{R}_m$, i.e. $s = p$ (as usual $s := \frac{|A|+|B|}{2}$ and p denotes the max number of vertex-disjoint paths between A, B). So the above can be equivalently written as $|q^R_{c,0}(\mathcal{R}_m)| \leq (\frac{\omega}{n^{1-\epsilon}})^{s-p} \tau^{5\tau}$. Now we use Lem. 4.21(2), whose "$q(\cdot)$" is $q^R_{c,k}$ here, the "Q" matrix is $D^\tau Q^R_{c,k} D$, the "$(\frac{\omega}{n})^{|V(\mathcal{R}_m)|} q(\cdot)$" is $(\frac{\omega}{n})^{|V(\mathcal{R}_m)|-s} \cdot (\frac{\omega}{n})^s \cdot q^R_{c,k}$. As the result, $|q^R_{c,k}(\mathcal{R}_m, i, j)| \leq \tau^{5\tau} \cdot (\frac{\omega}{n^{1-\epsilon}})^{s-p+k/3}$.

(4). When plugging in G, both M^R_c $\widetilde{L^R}\left[D^\tau\left(Q^R_{c,0} - Q^R_{c,1} + ... \pm Q^R_{c,d}\right)D^\tau\right]\left(\widetilde{L^R}\right)^\top$ are supported on clique rows and columns that contain R by definition. So it is the case for the difference, $\mathcal{E}^R_c$, too. We only need to bound $\|\mathcal{E}^R_c\| := \|-\mathcal{E}^R_{c;\text{deg}} + \left(-\mathcal{E}^R_{c,1;\text{negl}} + ... \pm \mathcal{E}^R_{c,d+1;\text{negl}}\right)\|$.

By Lem. 4.21(2) and induction on $k = 0, ..., d$, it always holds that $|q^R_{c,k}| < \tau^{5\tau}$. Also for each $\mathcal{E}^R_{k;\mathrm{negl}}$, by Lem. 4.21(1) w.p. $> 1 - n^{-9\log n}$, $\left\|\mathcal{E}^R_{k;\mathrm{negl}}\right\| < \tau^{5\tau} n^{-\epsilon\tau} < n^{-0.9\epsilon\tau}$.

As for $\mathcal{E}^R_{c;\deg}$, recall by Def. 4.23, its (I,J)-th entry is the sum of outer-canonical products in $\widetilde{L^R} \cdot \left(D^\tau Q^R_{c,0} D^\tau\right) \cdot \left(\widetilde{L^R}\right)^\top$ at (I,J) where $|V(T) \cup I \cup J| > \tau$. Thus

$$\mathcal{E}^R_{c;\deg}(I,J) = \sum_{\substack{(\mathcal{R}_l,\mathcal{R}_m,\mathcal{R}_r)\text{: side-inn.can.}\\ \text{outer.can.}\\ \text{all three has size } \le\tau\\ |V(T)\cup I\cup J|>\tau}} (\tfrac{\omega}{n})^{|V(T)\cup I\cup J|} \cdot q^R_{c,0}(\mathcal{R}_m, e(\mathcal{R}_l), e(\mathcal{R}_r))\chi_T$$

where $T = T_l \oplus T_m \oplus T_r$, and in the summation R_l (R_r) should have I (J) as the left (right) set. Note this equation uses $|V(T) \cup I \cup J| = e_l + e_r + |V(\mathcal{R}_m)|$, a fact from outer- and side-inner-canonicality. By canonicality again, the sum contributes to a $(I, J; T)$ by at most $3^{3\tau}$ triples. Since $3\tau \ge |V(T) \cup I \cup J| > \tau$ and $|q^R_{c,0}(\cdot)| < \tau^{5\tau}$, we have by Lem. 4.10 that $\left|\mathcal{E}^R_{c;\deg}(I,J)\right| < \tau^{6\tau} \cdot \sum_{c=0}^{3\tau} (\frac{\omega}{n})^{\max\{\tau,c\}} (n^{c/2} 2^{c^2} n^{4\log\log n}) < n^{-2\epsilon\tau}$ w.p. $> 1 - n^{-10\log n}$. So, by union bound over (I,J), $\left\|\mathcal{E}^R_{c;\deg}\right\| < n^{-d/4} n^{-2\epsilon\tau} < n^{-\epsilon\tau}$ w.p. $> 1 - n^{-9.5\log n}$.

Together, summing the bounds on $\left\|\mathcal{E}^R_{c,k;\mathrm{negl}}\right\|$ and $\left\|\mathcal{E}^R_{c;\deg}\right\|$, by union bound over $k = 1, ..., d$, we get that w.p. $> 1 - n^{-9\log n}$, $\left\|\mathcal{E}^R_c\right\| < n^{-\epsilon\tau/2}$. □

4.8 PSDness analysis, III: Structural and pseudorandom matrices

In this section, we prove the Main Lemma 4.14. Recall for each R, $c \le |R|$ by Lemma 4.20,

$$M^R_c = \widetilde{L^R} \cdot \left[D^\tau \underbrace{\left(Q^R_{c,0} - Q^R_{c,1} + ... \pm Q^R_{c,d}\right)}_{:=Q^R_c} D^\tau \right] \cdot \left(\widetilde{L^R}\right)^\top + \mathcal{E}^R_c.$$

The key is the following lemma.

Lemma 4.22. *W.p.* $> 1 - n^{-8\log n}$ *over* G*, the following holds.*

(1). $\forall R \in \binom{[n]}{\leq d/2}$, $Q^R_{0,0} - Q^R_{0,1} + ... \pm Q^R_{0,\frac{d}{2}} \succeq \tau^{-7\tau} \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right)_{S^R \times S^R}$*, where recall* $S^R = \{(A,i) \in \binom{[n]}{\leq d/2} \times \{0,...,\tau\} \mid A \supseteq R, |A| + i \geq \frac{d}{2}\}$.

(2). $\forall R$, $0 < c \leq |R|$, $\pm\omega^{-c}\left(Q^R_{c,0} - Q^R_{c,1} + ... \pm Q^R_{c,\frac{d}{2}}\right) \preceq n^{-c/4}\mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right)_{S^R \times S^R}$.

Proof plan of Lemma 4.22. Fix an $R \in \binom{[n]}{\leq d/2}$. We will prove the lemma by three ingredients: Corollary 4.5, Lemma 4.24, Lemma 4.25.

Proof plan. Corollary 4.5 (section 4.8.1, 4.8.2): Positiveness of $Q^R_{0,0}$. This is the last real technical challenge. We use a natural "*structural part + pseudo-random part*" decomposition of $Q^R_{0,0}$ (Def. 4.33), aiming to show that on their common support, the structural part is positive enough and the pseudo-random part is small enough in norm. The main difficulty here is in analyzing $\mathbb{E}[Q^R_{0,0}]$ which, ultimately, is about the choice of generating function F in Definition 4.8.

Lemma 4.24, 4.25 (section 4.8.2): Other $Q^R_{c,k}$'s ($k > 0$ or $c > 0$), when timed with ω^{-c}, are small and appropriately supported. These are proved by standard means.

We carry out this plan in the upcoming two subsections 4.8.1, 4.8.2.

Definition 4.32. *Define the* **root diagonal-clique matrix** *as*

$$D_{\mathrm{Cl}}(A,B) = \begin{cases} 0 & \text{, if } A \neq B; \\ 2^{-\binom{|A|}{2}/2} \cdot \widetilde{\mathrm{Cl}}_A = 2^{-\binom{|A|}{2}/2} \sum_{T \subseteq E[A]} \chi_T & \text{, o.w.} \end{cases} \tag{4.106}$$

of dimension $\binom{[n]}{\leq d/2} \times \binom{[n]}{\leq d/2}$*, so that* $D^2_{\mathrm{Cl}}(A,A) = \widetilde{\mathrm{Cl}}(A)$ *for all* $A \in \binom{[n]}{d/2}$*. Also let* $D^\tau_{\mathrm{Cl}} := D_{\mathrm{Cl}} \otimes \mathrm{Id}_{\{0,...,\tau\}\times\{0,...,\tau\}}$ *which is again diagonal.*

Definition 4.33. *The* **structural-pseudorandom decomposition** *of* $Q^R_{0,0}$ *is*

$$Q^R_{0,0} = D^\tau_{\mathrm{Cl}} \cdot \mathbb{E}[Q^R_{0,0}] \cdot D^\tau_{Cl} + \left(Q^R_{0,0} - D^\tau_{\mathrm{Cl}} \cdot \mathbb{E}[Q^R_{0,0}] \cdot D^\tau_{Cl}\right), \tag{4.107}$$

where the summand $D^{\tau}_{\mathrm{Cl}} \cdot \mathbb{E}[Q^R_{0,0}] \cdot D^{\tau}_{Cl}$ *is called the* **structural part**, *and the summand* $\Big(Q^R_{0,0} - D^{\tau}_{\mathrm{Cl}} \cdot \mathbb{E}[Q^R_{0,0}] \cdot D^{\tau}_{Cl}\Big)$ *the* **pseudo-random part**.

4.8.1 Positiveness of structural part

Proposition 4.7. *Fix* $R \in \binom{[n]}{\leq d/2}$ *and* $0 \leq c \leq |R|$, *let* $r := |R|$.

(1). $\mathbb{E}[Q^R_{c,0}]$ *is supported on the blockwise partial-diagonals* $\{\Big((A,i),(A,j)\Big) \in S^R \times S^R\}$, *where* S^R *is by* (4.93) *(i.e. requires* $R \subseteq A$ *and* $|A| + \min\{i,j\} \geq d/2$*).*

(2). For all $\Big((A,i),(A,j)\Big) \in S^R \times S^R$, $\mathbb{E}[Q^R_{c,0}]\Big((A,i),(A,j)\Big) =$

$$\sum_{l=c}^{r} (-1)^{r-l} \frac{\binom{r}{l}}{(l-c)!} \binom{|A|+i+j+l-d}{c} \frac{\Big(|A| + 8\tau^2 + (l-c) + (i+j)\Big)!}{(8\tau^2)!} + O\left(\frac{\tau^{1.5\tau}}{n}\right). \tag{4.108}$$

In particular, for $c = 0$,

$$\mathbb{E}[Q^R_{0,0}]\Big((A,i),(A,j)\Big) = \sum_{l=0}^{r} (-1)^{r-l} \frac{\binom{r}{l}}{l!} \cdot \frac{\Big(|A| + 8\tau^2 + l + (i+j)\Big)!}{(8\tau^2)!} + O\left(\frac{\tau^{1.5\tau}}{n}\right). \tag{4.109}$$

(3). For every $A \in \binom{[n]}{\leq d/2}$ *let* $1_{A,A}$ *be the* $\binom{[n]}{\leq d/2} \times \binom{[n]}{\leq d/2}$*-matrix with a single 1 on position* (A,A). *Then*

$$\mathbb{E}[Q^R_{0,0}] = \sum_{\substack{A \subseteq \binom{[n]}{\leq d/2} \\ A \supseteq R}} 1_{A,A} \otimes \left[\left(\sum_{l=0}^{r} (-1)^{r-l} \frac{\binom{r}{l}}{l!} \cdot P_{|A|+l}\right) + E^R_A\right] \tag{4.110}$$

where for every fixed A, $P_{|A|+l}, E^R_A$ *are* $(\tau+1) \times (\tau+1)$*-matrices both supported on the principal minor* $\{i \mid d/2 - |A| \leq i \leq \tau\} \times \{i \mid d/2 - |A| \leq i \leq \tau\}$, *satisfying* $\left\|E^R_A\right\| < \frac{\tau^{2\tau}}{n}$

and

$$P_{|A|+l}(i,j) = \frac{\Big(|A|+l+8\tau^2+(i+j)\Big)!}{(8\tau^2)!}, \quad d/2-|A| \le i,j \le \tau. \tag{4.111}$$

Proof. For (1), the constant terms in (4.94) correspond to $T_m = \emptyset$, which is nonzero only when $A = B$ for A, B in S^R.

For (2), by definition (4.94) notice again $T_m = \emptyset$ and $A = B$. $\mathbb{E}[Q^R_{c,0}((A,i),(A,j))]$ $= Y_c(\underbrace{|R|}_{:=r}, \underbrace{|A|+i+j}_{:=a})$, which expands to:

$$\sum_{l=c}^{r}(-1)^{r-l}\binom{r}{l}\underbrace{\binom{a+l-d}{c}}_{\text{Def. 4.17}}\binom{n-a}{l-c}n^{-(l-c)}\frac{(a+l-c+8\tau^2)!}{(8\tau^2)!}. \tag{4.112}$$

Now use $\binom{n-a}{l-c}n^{-(l-c)} = \frac{1}{(l-c)!}\frac{(n-a)\ldots(n-a-(l-c)+1)}{n^{l-c}} = \frac{1}{(l-c)!}(1-O(d^2/n))$ and

$$\left|\binom{r}{l}\binom{a+l-d}{c}\binom{n-a}{l-c}n^{-(l-c)}\frac{(a+l-c+8\tau^2)!}{(8\tau^2)!}\right| < (4d)^d\cdot(9\tau^2)^d < \tau^\tau$$

to (4.112), we get (4.108). Further, in (4.112) when $c = 0$ we have $\binom{a+l-d}{0} = 0$ regardless of $a+l-d$ (any value of it, positive, negative or 0). And the same analysis gives (4.109).

For (3), each E^R_A has dimension $(\tau+1)\times(\tau+1)$ and each entry is absolutely $< \tau^{1.5\tau}/n$ from part (2). The expression of $P_{|A|+l}$ is directly from (4.109). □

Remark 4.13. *(Specialty of $c = 0$). Comparing $\mathbb{E}[Q^R_{0,0}]$ and $\mathbb{E}[Q^R_{c,0}]$ (4.108), (4.109), the specialty of the case $c = 0$ is that the factor $\binom{|A|+l-d}{0}$ is* **always** *1, which is important for $\mathbb{E}[Q^R_{0,0}]$ to be positive. In cases $c > 0$, $\binom{|A|+l-d}{c}$ might be 0 or negative depending on the order between $0, c, |A|+l-d$, making $\mathbb{E}[Q^R_{c,0}]$ possibly not PSD.*

Definition 4.34. *For every $m, t \in \mathbb{N}$, define the* **factorial Hankel matrix** *to be*

$$H_{m,t}(i,j) = (i+j+t)! \quad \forall 0 \le i,j \le m. \tag{4.113}$$

The following is our key observation on the structure of these matrices.

Proposition 4.8. *(Almost common decomposition of $\{H_{m,t}\}$)*

(1). $H_{m,t} = L_m \cdot \left(N_{m,t} \cdot D_{m,t} \cdot (N_{m,t})^\top\right) \cdot (L_m^\top)$ where $L_m, D_{m,t}$ are diagonal and $N_{m,t}$ is lower-triangular, with expressions

$$L_m(i,i) = i! \qquad D_{m,t}(i,i) = \prod_{t'=1}^{t}(i+t') \qquad N_{m,t}(i,j) = \binom{i+t}{i-j}.$$

In particular, L_m is independent of t, and $H_{m,t}$ is positive.

(2). Let J_m be the usual $(1+m)\times(1+m)$ lower-triangular Jordan block

$$J_m(i,j) = \begin{cases} 1 & , \text{ if } i = j \text{ or } i = j+1; \\ 0 & , \text{ o.w.} \end{cases}$$

Then the "left factors" $N_{m,t}$ satisfy the recursive relation $N_{m,t+1} = N_{m,t} \cdot J_m$.

Proof. The two items follow from a direct inspection of the definition. □

Proposition 4.9. *If parameters m, t, r satisfy*

$$t + 1 > 8 \cdot \max\{r^2, m\} \tag{4.114}$$

then it holds that $H_{m,t+1} \succeq 2r^2 H_{m,t}$.

Proof. By Proposition 4.8 it suffices to show that under (4.114),

$$J_m \cdot D_{m,t+1} \cdot J_m^\top \succeq 2r^2 D_{m,t}.$$

Equivalently, we need to compare the quadratic forms for fixed m:

$$q_{t+1}(x) := (x^\top J_m) D_{m,t+1} (J_m^\top x) \quad v.s. \quad q_t(x) := 2r^2 \cdot x^\top D_{m,t} x \tag{4.115}$$

where $x^\top = (x_0, ..., x_m)$ is the formal variable row-vector. Define two polynomials

$$\alpha(y) = 2r^2 \prod_{t'=1}^{t} (y + t'), \quad \beta(y) = \prod_{t'=1}^{t+1} (y + t').$$

Then we have $q_{t+1}(x) = \sum_{i=0}^{m} \beta(i)(x_i + x_{i+1})^2$ ($x_{m+1} := 0$) and $q_t(x) = \sum_{i=0}^{m} \alpha(i) x_i^2$.

To compare $q_t(x)$, $q_{t+1}(x)$, note $q_{t+1}(x) = \sum_{i=0}^{m} \beta(i) \cdot (x_i + x_{i+1})^2$

$$\sum_{i=0}^{m} \left[\alpha(i) x_i^2 + \Big(\beta(i) - \alpha(i) \Big) \cdot (x_i + \frac{\beta(i)}{\beta(i) - \alpha(i)} x_{i+1})^2 \; - \; \frac{\beta(i)^2}{\beta(i) - \alpha(i)} x_{i+1}^2 \right]$$

So if for $1 \le i \le m$ let $b_i := 1 - \frac{\alpha(i)}{\beta(i)} - \frac{\beta(i-1)}{\beta(i)} \frac{1}{b_{i-1}}$, $b_0 = 1 - \frac{\alpha(0)}{\beta(0)}$, then

$$q_{t+1}(x) = \underbrace{\sum_{i=0}^{m} \alpha(i) x_i^2}_{q_t(x)} \; + \; \sum_{i=0}^{m} \beta(i) b_i (x_i + \frac{1}{b_i} x_{i+1})^2. \tag{4.116}$$

Claim 4.1. *For all $i \le m$ we have $b_i > 1/2$.*

Proof. (of the claim) By definition, $b_0 = 1 - \frac{2r^2}{(t+1)}$ and

$$b_i = 1 - \frac{2r^2}{(t+1+i)} - \frac{i}{(t+1+i)} \cdot \frac{1}{b_{i-1}}, \quad i \ge 1. \tag{4.117}$$

Use induction for the claim: $b_0 = 1 - \frac{2r^2}{t+1} > 1/2$ by (4.114). For $1 \le i \le m$, $b_i = 1 - \frac{2r^2}{t+1+i} - \frac{i}{t+1+i} \cdot \frac{1}{b_{i-1}} \ge 1 - \frac{2r^2}{t+1} - \frac{m}{t+1} \cdot 2 > 1/2$ by (4.114) and inductive hypothesis. □

By (4.116) and positiveness of each b_i (Claim 4.1), $q_{t+1}(x) \ge q_t(x)$. This proves (4.115) and thus the proposition. □

Now we apply Proposition 4.9 to matrices $P_{|A|+l}$ (4.111). Note

$$P_{|A|+l} = \frac{1}{(8\tau^2)!} H_{\tau-(d/2-|A|),\, d-|A|+8\tau^2+l}$$

where A is fixed, l varies. We have the following:

Corollary 4.3. *(Positiveness of $\mathbb{E}[Q^R_{0,0}]$) In the decomposition* (4.110) *of $\mathbb{E}[Q^R_{0,0}]$,*

$$\left(\sum_{l=0}^{r}(-1)^{r-l}\frac{\binom{r}{l}}{l!}\cdot P_{|A|+l}\right) + E^R_A \;\succ\; \operatorname{diag}\left(\tau^{-6\tau}\right)_{0\le i\le \tau-(d/2-|A|)} \tag{4.118}$$

where we regard the matrices' support as $\{i \mid d/2-|A| \le i \le \tau)\}^2 \cong \{0,...,\tau-(d/2-|A|)\}^2$. In particular, by (4.110)

$$\mathbb{E}[Q^R_{0,0}] \;\succ \sum_{\substack{A\subseteq \binom{[n]}{\le d/2} \\ A\supseteq R}} 1_{A,A}\otimes \operatorname{diag}\left(\tau^{-6\tau}\right)_{d/2-|A|\le i\le \tau} = \operatorname{diag}\left(\tau^{-6\tau}\right)_{S^R\times S^R} \tag{4.119}$$

where recall $S^R = \{(A,i) \mid R\subseteq A, |A|+i \ge d/2\}$.

Proof. The "in particular" part is straightforward from (4.118) by checking the support, and noticing that tensoring with a nonzero PSD matrix preserves the relation $\succ$. Below we prove for (4.118).

Fix A, let $\tau_0 = \tau-(d/2-|A|)$, $t_0 = d-|A|+8\tau^2$. Then

$$\sum_{l=0}^{r}(-1)^{r-l}\frac{\binom{r}{l}}{l!}\cdot P_{|A|+l} = \frac{1}{(8\tau^2)!}\cdot(X_r + X_{r-2} + ...) \tag{4.120}$$

where, $\forall 0 \le v \le \lfloor r/2\rfloor$, $X_{r-2v} = \frac{\binom{r}{r-2v}}{(r-2v)!}\Big(H_{\tau_0,t_0+r-2v} - \underbrace{\frac{(r-2v)^2}{(2v+1)}}_{\le r^2} H_{\tau_0,t_0+r-2v-1}\Big)$ and

$H_{\tau_0,-1} := 0$. Since $t_0 > 8\max\{r^2, \tau_0\}$, by Proposition 4.9

$$X_{r-2v} \succeq \frac{\binom{r}{r-2v}}{(r-2v)!} \cdot \max\{\frac{1}{2}H_{\tau_0,t_0+r-2v},\ r^2 H_{\tau_0,t_0+r-2v-1}\} \quad \forall 0 \le v \le r/2.$$

So in (4.120), in particular,

$$\sum_{l=0}^{r}(-1)^{r-l}\frac{\binom{r}{l}}{l!} \cdot P_{|A|+l} \ \succeq\ \frac{1}{(8\tau^2)!} \cdot H_{\tau_0,t_0} \overset{\text{Prop. 4.8}}{=} L\left(N_{t_0} \cdot \frac{D_{t_0}}{(8\tau^2)!} \cdot (N_{t_0})^\top\right)L \qquad (4.121)$$

where we temporarily abuse the notation by omitting the index τ_0 in the RHS.

Using the following claim, we can finish the proof of (4.118):

$$\begin{aligned}\text{RHS of (4.121)} &\succ L \cdot \operatorname{diag}\left(\tau^{-5\tau}\right)_{0\le i\le\tau_0} \cdot L \qquad \text{(by Claim 4.2)}\\ &\succeq \operatorname{diag}\left(\tau^{-5\tau}\right)_{0\le i\le\tau_0},\end{aligned}$$

while by Proposition 4.7 (3), $\left\|E_A^R\right\| < \frac{\tau^{2\tau}}{n} < \tau^{-6\tau}$ (using the parameter regime). So LHS of (4.118) $\succeq$ $\operatorname{diag}\left(\tau^{-5\tau} - \tau^{-6\tau}\right)_{0\le i\le\tau_0}$ $\succeq$ RHS of (4.118). □

Claim 4.2. *Under the notation of Cor. 4.3, the following holds:*

$$N_{t_0}^{-1}(i,j) = (-1)^{i-j}\binom{i+t_0}{i-j} \quad 0 \le i,j \le \tau_0 \qquad (4.122)$$

(which is defined as 0 if $i < j$);

$$N_{t_0} \cdot \frac{D_{t_0}}{(8\tau^2)!} \cdot (N_{t_0})^\top \succ \operatorname{diag}\left(\tau^{-5\tau}\right)_{0\le i\le\tau_0}. \qquad (4.123)$$

Proof. For (4.122), multiply this matrix with N_{t_0} then the (i,j)th entry is

$$\sum_{j\le k\le i}(-1)^{i-k}\binom{i+t_0}{i-k}\binom{k+t_0}{k-j} = \sum_{k'=0}^{i'}(-1)^{i'-k'}\binom{i'+j+t_0}{i'-k'}\binom{k'+j+t_0}{k'}$$

where $i' = i - j,\ k' = k - j$. To see it is the identity matrix, we use a generating function. Let $D_m[(1+x)^a]$ denote the coefficient of x^m in $(1+x)^a$, $m \geq 0, a \in \mathbb{Z}$, the above RHS $= (-1)^{i'} \sum_{k'=0}^{i'} D_{i'-k'}[(1+x)^{i'+j+t_0}] \cdot D_{k'}[(1+x)^{-(t_0+j+1)}] = (-1)^{i'} D_{i'}[(1+x)^{i'+j+t_0-(t_0+j+1)}] = (-1)^{i'} D_{i'}[(1+x)^{i'-1}] = 1_{i'=0}$.

As for (4.123), note it is equivalent to:

$$\frac{D_{t_0}}{(8\tau^2)!} \ \succ \ N_{t_0}^{-1} \cdot \tau^{-5\tau} \cdot (N_{t_0}^{-1})^\top. \tag{4.124}$$

To upper bound the RHS, let $a_0 = \tau^{-5\tau}$, consider the quadratic form

$$x^\top N_{t_0}^{-1} \cdot a_0 \cdot (N_{t_0}^{-1})^\top x = a_0 \sum_{j=0}^{\tau_0} y_j^2, \tag{4.125}$$

where by (4.122), $y_j = \left(x^\top N_{t_0}^{-1}\right)_j = \sum_{i=j}^{\tau_0} (-1)^{i-j} \binom{i+t_0}{i-j} x_i$. By Cauchy-Schwartz, $y_j^2 \leq \tau_0 \cdot \sum_{i=j}^{\tau_0} \binom{i+t_0}{i-j}^2 x_i^2$, thus RHS of (4.125) $= a_0 \sum_{j=0}^{\tau_0} y_j^2 \leq \ a_0 \sum_{i=0}^{\tau_0} x_i^2 \cdot \left(\tau_0 \sum_{j=0}^{i} \binom{i+t_0}{i-j}^2\right)$ $< \sum_{i=0}^{\tau_0} \left(\tau^{-5\tau} \cdot (9\tau^2)^{2i+2}\right) x_i^2$. Now (4.124) follows since, for each i, in the LHS of (4.124) $= \frac{D_{t_0}(i,i)}{(8\tau^2)!} \geq (8\tau^2)^{-(d/2-|A|)}$ by definition, and the latter $> \tau^{-2d} > \tau^{-5\tau} \cdot (9\tau^2)^{2i+2}$ using $i \leq \tau_0 < \tau$, $d \ll \tau$. Combining these two conclusions, we get (4.124). □

We arrive at the main conclusion of this subsection.

Corollary 4.4. *(Positiveness of the structural part of $Q_{0,0}^R$ (Def. 4.33))*

$$\underbrace{D_{\mathrm{Cl}}^\tau \cdot \mathbb{E}[Q_{0,0}^R] \cdot D_{\mathrm{Cl}}^\tau}_{\text{stractural part of } Q_{0,0}^R} \ \succeq \ \tau^{-6\tau} \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right)_{S^R \times S^R}.$$

Proof. It follows from Corollary 4.3 and the fact that $D_{\mathrm{Cl}}^2(A,A) = \widetilde{\mathrm{Cl}}(A)$ in Definition 4.32. □

4.8.2 Bounds on rest matrices

In this subsection, we bound the rest matrices:

$$\underbrace{Q^R_{0,0} - D^\tau_{\mathrm{Cl}} \cdot \mathbb{E}[Q^R_{0,0}] \cdot D^\tau_{\mathrm{Cl}}}_{\text{pseudo-random part of } \mathrm{Q}^{\mathrm{R}}_{0,0} \text{ (Def. 4.33)}} \quad , \quad Q^R_{0,k}\ (k>0), \quad \omega^{-c} \cdot Q^R_{c,k}\ (c>0, k \geq 0)$$

by three Lemmas 4.23, 4.24, 4.25, respectively, which would prove Lemma 4.22.

The arguments are standard but somewhat lengthy, as we need to be careful about the block structure and the support of matrices. Like in the proof of Lem. 4.21, when fixing an $R \subseteq [n]$ we only consider ribbons whose both side sets contain R, so the corresponding graph matrices will be multiplied by $\mathrm{diag}(1_R)$ from left and right, where $1_R(A) = 1$ iff $R \subseteq A$; this does not affect the norm bound in Thm 4.3.

Definition 4.35. *Recall the (blocked) root diagonal-clique matrix D^τ_{Cl}, Def. 4.32. Denote by D' its 0-1 valued version. I.e., D' is diagonal and $D'((A,i),(A,i)) = \mathrm{Cl}_A$ for all $A \in \binom{[n]}{\leq d/2}$ and $0 \leq i \leq \tau$.*

Lemma 4.23. *W.p. $> 1 - n^{-9\log n}$ the following holds: $\forall R \in \binom{[n]}{\leq d/2}$,*

$$\pm \underbrace{(Q^R_{0,0} - D^\tau_{\mathrm{Cl}} \cdot \mathbb{E}[Q^R_{0,0}] \cdot D^\tau_{\mathrm{Cl}})}_{\text{pseudo-random part of } Q^R_{0,0}}(G) \ \preceq\ n^{-\epsilon} \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}}(G)\right)_{S^R \times S^R} \tag{4.126}$$

Proof. **Fix R. In this proof abbreviate** $Q_{\mathrm{ps}} := Q^R_{0,0} - D^\tau_{\mathrm{Cl}} \cdot \mathbb{E}[Q^R_{0,0}] \cdot D^\tau_{\mathrm{Cl}}$ ("ps" for pseudo-random). It is $(\tau+1)\times(\tau+1)$-blocked with blocks $\left(Q_{\mathrm{ps},(i,j)}\right)_{0\leq i,j\leq\tau}$.

In block (i,j), by Def. 4.29 and Prop. 4.7, $Q_{\mathrm{ps},(i,j)}$ is supported within $S_{i,j} \times S_{i,j}$, where $S_{i,j} := \{A \mid |A| + \min\{i,j\} \geq d/2\}$. For each $A \neq B$, by Prop. 4.7 (1), $Q_{\mathrm{ps},(i,j)}(A,B) =$

$Q^R_{0,0}((A,i),(B,j)) =$

$$\sum_{\substack{T_m:\ |V(T_m)\cup A\cup B|\le\tau \\ A,B\in \mathrm{mSep}_{A,B}(T_m)}} (\frac{\omega}{n})^{|V(T_m)\cup A\cup B|-\frac{|A|+|B|}{2}} \cdot q(A,B;T_m)\cdot \chi_{T_m} \tag{4.127}$$

and

$$Q_{\mathrm{ps},(i,j)}(A,A) = \sum_{T_m:\ 1\le|V(T_m)\setminus A|\le\tau-|A|} (\frac{\omega}{n})^{|V(T_m)\cup A|-|A|}\cdot q(A,A;T_m)\cdot\chi_{T_m}. \tag{4.128}$$

Here we have abbreviated $q(A,B;T_m) := Y_0\Big(|R|, |V(T_m)\cup A\cup B| + (i+j)\Big)$ ((4.94)) and have omitted the indices $|R|, i+j$ when they are fixed. Two properties we need:

$$q(A,B;T_m) \text{ depends only on } |V(T_m)\cup A\cup B| \text{ when fixing } (A,B); \tag{4.129}$$

$$\Big|q(A,B;T_m)\Big| < \tau^{5\tau} \qquad (\text{by Lemma 4.13 (4)}). \tag{4.130}$$

By (4.129), $Q_{\mathrm{ps},(i,j)}(A,B)$ always factors through $\mathrm{Cl}_{A\cup B}$ thus $\mathrm{Cl}_A\mathrm{Cl}_B$. In particular,

$$Q_{\mathrm{ps}} = D'\cdot Q_{\mathrm{ps}}\cdot D' \quad (D' \text{ from Def. 4.35}). \tag{4.131}$$

Claim 4.3. *W.p.* $> 1-n^{-9.5\log n}$, $\pm Q_{\mathrm{ps},(i,j)} \prec n^{-1.1\epsilon}\mathrm{diag}\left(2^{\binom{|A|}{2}}\right)_{S_l^R\times S_l^R}$ *for all* (i,j), *where* $l := \min\{i,j\}$ *and* $S_l^R := \{A\in\binom{[n]}{\le d/2} \mid A\supseteq R,\ |A|+l\ge d/2\}$.

The lemma follows from this claim and (4.131), as follows. We consider a different decomposition of Q_{ps}: for every $b\in[0,\frac{d}{2}]$, let $I_b := \{i \mid d/2-b\le i\le\tau\}$, and let $Q_{\mathrm{ps};b}$ be the principal minor on $W_b := \Big(P_b^R\times I_b\Big)\times\Big(P_b^R\times I_b\Big)$ of Q_{ps} (0 elsewhere), where $P_b^R = \{A\subseteq[n] \mid R\subseteq A, |A|=b\}$. Then

$$\{((A,i),(B,j))\in S^R\times S^R \mid 0\le|A|=|B|\le d/2\} = \bigsqcup_{b=0}^{d/2} W_b \quad (\text{disjoint union}).$$

Note $Q^R_{c,0}$ is supported only on those $((A,i),(B,j)) \in S^R \times S^R$ with $|A| = |B|$ (Remark 4.12(2)); in particular for $c = 0$, we have a decomposition $Q_{ps} = \sum_{b=0}^{d/2} Q_{\mathrm{ps};b}$.

Now inside block $I_b \times I_b$, $Q_{\mathrm{ps};b}$ is further block-wise, each block a principal minor of $Q_{\mathrm{ps},(i,j)}$. By Claim 4.3, $(\pm)$ all such blocks $\prec n^{-1.5\epsilon} \cdot \mathrm{diag}\left(2^{\binom{b}{2}}\right)_{P_b^R \times P_b^R}$ together w.p. $> 1 - n^{-9.5\log n}$, which implies $\pm Q_{\mathrm{ps};b} \prec \tau^2 \cdot n^{-1.5\epsilon}\mathrm{diag}\left(2^{\binom{b}{2}}\right)_{W_b} \prec n^{-\epsilon}\mathrm{diag}\left(2^{\binom{b}{2}}\right)_{W_b}$. So, summing over b, $\pm Q_{\mathrm{ps}} \prec n^{-\epsilon}\mathrm{diag}\left(2^{\binom{|A|}{2}}\right)_{S^R \times S^R}$ w.p. $1 - n^{-9\log n}$. Insert this to the middle of (4.131), where $\widetilde{\mathrm{Cl}}_A = 2^{\binom{|A|}{2}} \cdot \mathrm{Cl}_A$, $\mathrm{Cl}_A = \mathrm{Cl}_A^2$, we get (4.126). □

Proof. (of Claim 4.3) We use the norm bounds from section 4.4. Fix (i,j), consider $Q^{\mathrm{diag}}_{\mathrm{ps},(i,j)}$ and $Q^{\mathrm{off}}_{\mathrm{ps},(i,j)} = Q_{\mathrm{ps},(i,j)} - Q^{\mathrm{diag}}_{\mathrm{ps},(i,j)}$ separately.

Diagonal part. For any (A,A) in the support (i.e. $|A| + i \geq d/2$, $|A| + j \geq d/2$), $Q^{\mathrm{diag}}_{\mathrm{ps},(i,j)}(A,A) = \widetilde{\mathrm{Cl}}_A \underbrace{\left(\sum_{\substack{T_m:\ 1 \leq |V(T_m)\backslash A| \leq \tau - |A| \\ T_m \cap E[A] = \emptyset}} (\frac{\omega}{n})^{|V(T_m)\backslash A|} q(A,A;T_m)\chi_{T_m} \right)}_{:= g(A)}$ by (4.128). This $g(A)$ can be bounded by norms of diagonal graph matrices as follows. First, $q(A,A;T_m)$ depends only on $|V(T_m)\backslash A|$ (we have fixed R,i,j,A), so temporarily denote it as $q(|V(T_m)\backslash A|)$. For any $1 \leq v \leq \tau - |A|$ let $\mathcal{U}^v_1, ..., \mathcal{U}^v_{h(v)}$ be all different shapes $(A,A;T)$ (Def. 4.13) s.t. $T \cap E[A] = \emptyset$, $|V(T)\backslash A| = v$. Note

$$h(v) \leq 2^{|A|v+v^2} \quad \text{since we required } T \cap E[A] = \emptyset. \tag{4.132}$$

So w.p. $> 1 - n^{-9.6\log n}$, $|g(A)| = \left| \sum_{v=1}^{\tau-|A|} (\frac{\omega}{n})^v q(v) \cdot \left(\sum_{x=1}^{h(v)} \underbrace{\sum_{\substack{T_m:(A,A;T_m) \text{ has} \\ \text{shape } \mathcal{U}^v_x}} \chi_{T_m}}_{= M_{\mathcal{U}^v_x}(A,A) \text{ by Def. 4.13}} \right) \right|$

$\leq \sum_{v=1}^{\tau-|A|} (\frac{\omega}{n})^v q(v) \cdot \sum_{x=1}^{h(v)} \left\| M_{\mathcal{U}^v_x} \right\| \leq \sum_{v=1}^{\tau-|A|} (\frac{\omega}{n})^v \tau^{5\tau} \sum_{x=1}^{h(v)} \left\| M_{\mathcal{U}^v_x} \right\|$ by (4.130) and that each $M_{\mathcal{U}^v_x}$ is

diagonal; this is further $< \sum_{v=1}^{\tau} (\frac{\omega}{n})^v \tau^{5\tau} \cdot 2^{|A|v+v^2} \cdot n^{\frac{v}{2}} 2^{O(|A|+v)}$ by (4.132) and Theorem 4.3, which is $< \sum_{v=1}^{\tau} n^{-3\epsilon v} \cdot n^{\epsilon v} < n^{-1.2\epsilon}$ in our parameter regime.

Off-diagonal part. By R-symmetry of coefficients (4.129), $Q^{\text{off}}_{\text{ps},(i,j)}$ is a sum of graph matrices. Let $\mathcal{U}^{s,t}_1, ..., \mathcal{U}^{s,t}_{h(s,t)}$ be all shapes $(A, B; T)$ s.t. $|A| = |B| = s$, $A \neq B$, $A, B \in \text{mSep}_{A,B}(T)$ and $|V(T) \cup A \cup B| = t$, then by (4.127), $Q^{\text{off}}_{\text{ps},(i,j)}$ is a block-diagonal matrix, with blocks $s = d/2 - i, ..., d/2$ according to $s = |A| = |B|$, the sth block being $Q^{\text{off}}_{\text{ps},(i,j)}(s) = \sum_{t:\ s<t\le\tau} (\frac{\omega}{n})^{t-s} \sum_{x=1}^{h(s,t)} q(\mathcal{U}^{s,t}_x) M_{\mathcal{U}^{s,t}_x}$. Here naturally, we denote $q(A, B; T_m) = q(\mathcal{U}^{s,t}_x)$ if $(A, B; T_m)$ has shape $\mathcal{U}^{s,t}_x$. By Theorem 4.3,

$$\left\| Q^{\text{off}}_{\text{ps},(i,j)}(s) \right\| \le \sum_{s<t\le\tau} (\frac{\omega}{n})^{t-s} \cdot h(t,s) \cdot n^{\frac{t-s}{2}} 2^{O(t)} (\log n)^{O(t-s)} \tag{4.133}$$

w.p. $> 1 - n^{-9.8 \log n}$. Also clearly, $h(t,s) \le 2^{\binom{t}{2}+O(t)}$. So with the same probability, the RHS of (4.133) $\le \sum_{\substack{d/2-\max\{i,j\}\le s\le d/2 \\ s<t\le\tau}} (\frac{\omega}{n})^{t-s} 2^{\binom{t}{2}+O(t)} n^{\frac{t-s}{2}} (\log n)^{O(t-s)}$ where note $(\frac{\omega}{n})^{t-s} 2^{\binom{t}{2}+O(t)} n^{\frac{t-s}{2}} (\log n)^{O(t-s)} \le n^{-2\epsilon(t-s)} 2^{O(t)} 2^{\binom{s}{2}} (2^{t+s} \log n)^{O(t-s)} < 2^{\binom{s}{2}} n^{-1.95\epsilon}$. Now taking the blocks together, we get $\pm Q^{\text{off}}_{\text{ps},(i,j)} \prec n^{-1.9\epsilon} \cdot \text{diag}\left(2^{\binom{|A|}{2}}\right)_{S^R_{\min\{i,j\}} \times S^R_{\min\{i,j\}}}$.

By a union bound on the two parts in the above, w.p. $> 1 - n^{-9.5 \log n}$ it holds that $\pm Q_{\text{ps},(i,j)} = \pm(Q^{\text{diag}}_{\text{ps},(i,j)} + Q^{\text{off}}_{\text{ps},(i,j)}) \prec n^{-1.5\epsilon} \cdot \text{diag}\left(2^{\binom{|A|}{2}}\right)_{S^R_{\min\{i,j\}} \times S^R_{\min\{i,j\}}}$. □

Corollary 4.5. *(Positiveness of $Q^R_{0,0}$) For any $R \in \binom{[n]}{\le d/2}$, w.p. $> 1 - n^{-8 \log n}$,*

$$Q^R_{0,0}(G) \succeq \tau^{-6.1\tau} \cdot \text{diag}\left(\widetilde{\text{Cl}}(G)\right)_{S^R \times S^R}.$$

Proof. This is by Lem. 4.23, Cor. 4.4, and the fact that $\tau^{-6.1\tau} \gg n^{-\epsilon/10}$. □

Lemma 4.24. *(Bounds on $Q^R_{0,k}$) W.p. $> 1 - n^{-9 \log n}$ the following holds. For all $R \in \binom{[n]}{\le d/2}$ and all $1 \le k \le d/2$, $\pm Q^R_{0,k}(G) \preceq n^{-k/10} \cdot \text{diag}\left(\widetilde{\text{Cl}}(G)\right)_{S^R \times S^R}$.*

Proof. We will use union bound over (R,k), so fix one first and **abbreviate** $Q^R_{0,k}$ **by** Q.

Recall the definition of $Q^R_{0,k}$ (Lem. 4.20 (3)): Q is supported within $S^R \times S^R$,

$$Q\bigg((A,i),(B,j)\bigg) = \sum_{T_m:|V(T_m)\cup A\cup B|\le\tau} (\frac{\omega}{n})^{t-s} q^R_{0,k}(\mathcal{R}_m,i,j)\cdot\chi_{T_m}. \tag{4.134}$$

where $t = |A\cup B|$, $s = \frac{|A|+|B|}{2}$. Abbreviate $q^R_{0,k}$ as q_k. By Lemma 4.20(3), $q_k(\cdot,i,j)$ is R-symmetric w.r.t. shapes for all fixed (i,j) (the *R-symmetry condition*), and also $|q_k(\mathcal{R}_m,i,j)| \le \tau^{5\tau}(\frac{\omega}{n^{1-\epsilon}})^{s-p+k/3}$ (the *coefficient-size condition*) where $t = |A\cup B|$, $s = \frac{|A|+|B|}{2}$ and p is the max number of vertex-disjoint paths from A to B in T_m. By symmetry of q_k's, $Q((A,i),(B,j))$ factors through $\mathrm{Cl}(A)\mathrm{Cl}(B)$, so

$$Q = D'\cdot Q\cdot D' \tag{4.135}$$

where D' is by Definition 4.35. It suffices to show that

$$\text{w.p. } > 1-n^{-9.5\log n} \quad \pm Q \prec n^{-k/10}\cdot \mathrm{diag}\left(2^{\binom{|A|}{2}}\right)_{S^R\times S^R}. \tag{4.136}$$

This is because, like in the proof of Lemma 4.23, we can insert (4.136) to the middle of (4.135) which proves the lemma for the fixed R,k. Below, we prove (4.136).

As a blocked matrix $Q = (Q_{(i,j)})_{0\le i,j\le\tau}$, $Q_{(i,j)}$ supported on A's s.t. $|A|+i \ge d/2$. **For any fixed** (i,j), any $(s_1,s_2)\in\{0,...,d/2\}^2$ s.t. $s_1+i\ge d/2$, $s_2+j\ge d/2$, and any $t\ge\max\{s_1,s_2\}$, let $\mathfrak{U}_1^{t;s_1,s_2},...,\mathfrak{U}_{h(t;s_1,s_2)}^{t;s_1,s_2}$ be all different shapes $(A,B;T)$ where $|A|=s_1$, $|B|=s_2$, $|V(T)\cup A\cup B|=t$. Then by (4.134) and R-symmetry,

$$Q_{(i,j)} = \sum_{\substack{(t;s_1,s_2)\\ s_1+i,s_2+j\ge d/2\\ \tau\ge t\ge s_1,s_2}} \sum_{x=1}^{h(t;s_1,s_2)} q_k(\mathfrak{U}_x^{(t;s_1,s_2)},i,j)\cdot M_{\mathfrak{U}_x^{(t;s_1,s_2)}}.$$

This can be alternatively expressed as $Q_{(i,j)} = \sum_{\substack{s_1,s_2 \\ s_1+i,s_2+j\geq d/2}} Q_{(s_1,i),(s_2,j)}$ where

$$Q_{(s_1,i),(s_2,j)} := \sum_{\substack{t: \\ s_1,s_2\leq t\leq \tau}} \sum_{x=1}^{h(t;s_1,s_2)} q_k(\mathcal{U}_x^{(t;s_1,s_2)}, i, j) \cdot M_{\mathcal{U}_x^{(t;s_1,s_2)}}. \tag{4.137}$$

$Q_{(s_1,i),(s_2,j)}$ is a $\binom{[n]}{s_1} \times \binom{[n]}{s_2}$-matrix on the (i,j)th block, and w.p. $> 1 - n^{-10\log n}$

$$\left\|Q_{(s_1,i),(s_2,j)}\right\| \leq \sum_{\substack{t:\ t\leq\tau \\ t\geq s_1,s_2}} h(t;s_1,s_2) \cdot (\frac{\omega}{n})^{t-s} (\frac{\omega}{n^{1-\epsilon}})^{s-p+k/3} \cdot n^{\frac{t-p}{2}} 2^{O(t)} (\log n)^{O(t-s)} \tag{4.138}$$

by Thm. 4.3 and *coefficient-size condition*, where $s = \frac{s_1+s_2}{2}$ and p is the max number of vertex-disjoint paths between the two side sets. Since $h(t;s_1,s_2) \leq 2^{\binom{t}{2}+O(t)} = 2^{\binom{s}{2}+O(t)+(t+s)\cdot(t-s)}$, (4.138) implies (note $k>0$, $2^{O(t)} < n^{\epsilon/10}$, $\tau^{5\tau} < n^{1/30}$)

$$\left\|Q_{(s_1,i),(s_2,j)}\right\| < 2^{\binom{s}{2}} \cdot \tau^{5\tau} n^{-k/6} n^{-\epsilon(t-s)} < 2^{\binom{s}{2}} n^{-k/8}. \tag{4.139}$$

Finally, we sum over all double-blocks and use Cauchy-Schwartz. Namely, regard each $Q_{(s_1,i),(s_2,j)}$ as on $S^R \times S^R$ (extended by 0's), $Q = \sum_{\substack{(s_1,i),(s_2,j) \\ s_1+i,s_2+j\geq d/2}} Q_{(s_1,i),(s_2,j)}$ where

$$\pm Q_{(s_1,i),(s_2,j)} \ \prec\ n^{-k/8} \cdot \left(2^{\binom{s_1}{2}} \mathrm{Id}_{(s_1,i),(s_1,i)} \ +\ 2^{\binom{s_2}{2}} \mathrm{Id}_{(s_2,j),(s_2,j)}\right)/2$$

by (4.139) and Cauchy-Schwartz. Summing over $(s_1,i),(s_2,j)$, w.p. $> 1 - n^{-9.5\log n}$, we get $\pm Q \ \prec\ \tau^2 n^{-k/8} \mathrm{diag}\left(2^{\binom{|A|}{2}}\right)_{S^R\times S^R} \ \prec\ n^{-k/10} \mathrm{diag}\left(2^{\binom{|A|}{2}}\right)_{S^R\times S^R}$.

□

Lemma 4.25. *(Bounds on $Q^R_{c,k}$, $c>0$) W.p. $> 1 - n^{-9\log n}$ the following holds: for all $R \in \binom{[n]}{\leq d/2}$, $0 < c \leq |R|$ and $0 \leq k \leq d/2$, $\pm\omega^{-c} \cdot Q^R_{c,k} \ \preceq\ n^{-c/3} \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right)_{S^R\times S^R}$.*

Proof. The proof is almost the same as the previous one (Lemma 4.24). First, by a union bound over all such (R, c, k), it suffices to show that w.p. $> 1 - n^{-9.5 \log n}$ the inequality holds for a fixed (R, c, k), which we prove below.

Fix (R, c, k) as in the lemma. If $k > 0$ then the proof is identical to that of Lemma 4.24 ($c = 0$), as the same *R-symmetry* and *coefficient-size* conditions hold (by Lem. 4.20), and moreover, the matrix $Q^R_{c,k}$ is supported within $S^R \times S^R$ too.

So we only need to deal with the case $c > 0$, $k = 0$, i.e. $Q^R_{c,0}$. By Definition 4.29, it is supported on $S^R \times S^R$ with expression $Q^R_{c,0}\Big((A,i),(B,j)\Big) =$

$$\sum_{\substack{T_m : |V(T_m)\cup A\cup B| \le \tau \\ A,B \in \mathrm{mSep}_{A,B}(T_m)}} (\frac{\omega}{n})^{|V(T_m)\cup A\cup B| - \frac{|A|+|B|}{2}} \cdot Y_c\big(|R|,\ |V(T_m)\cup A\cup B| + (i+j)\big) \cdot \chi_{T_m} \quad (4.140)$$

where $\big|Y_c\big(|R|,\ |V(T_m) \cup A \cup B| + (i+j)\big)\big| < \tau^{5\tau}$ by Lemma 4.13 (4). For a fixed $(A, B; T_m)$ denote $t = |V(T_m) \cup A \cup B|$, $s = \frac{|A|+|B|}{2} (= |A| = |B|$ in this case), then the coefficient in (4.140) is bounded by $(\frac{\omega}{n})^{t-s} \cdot \tau^{5\tau}$ in absolute value. So we have the support condition, the R-symmetry and coefficient-size conditions as in Lemma 4.24; we proceed the same as there till (4.137), and a single term on the RHS now is $h(t; s_1, s_2) \cdot (\frac{\omega}{n})^{t-s} \tau^{5\tau} \cdot n^{\frac{t-p}{2}} 2^{O(t)} (\log n)^{O(t-s)}$. Note in (4.140) any appearing ribbon $\mathcal{R}_m = (A, B; T_m)$ has $A, B \in \mathrm{mSep}_{A,B}(T_m)$ so $p = s$ (the specialty of $k = 0$). So we can replace the bound on the RHS of (4.139) by $\tau^3 2^{\binom{s}{2}} \cdot n^{-3\epsilon(t-s)} \tau^{5\tau} 2^{O(t)} < 2^{\binom{s}{2}} \tau^{6\tau}$ and then proceed to get $\pm Q^R_{c,0} \prec \tau^{7\tau} \cdot \mathrm{diag}\left(2^{\binom{|A|}{2}}\right)_{S^R \times S^R}$. Now $c \ge 1$, $\omega = n^{\frac{1}{2} - 4\epsilon}$ ($\epsilon < 1/40$), $\tau^{7\tau} < n^{1/15}$, so

$$\pm \omega^{-c} Q^R_{c,0} \prec n^{-c/3} \mathrm{diag}\left(2^{\binom{|A|}{2}}\right)_{S^R \times S^R}.$$

Once again by $Q^R_{c,0} = D' Q^R_{c,0} D'$, we have $\pm \omega^{-c} Q^R_{c,0} \preceq n^{-c/3} \mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right)_{S^R \times S^R}$. □

Lemma 4.22 follows immediately from Corollary 4.5, Lemma 4.24, 4.25.

4.8.3 Put together

Now we prove the Main Lemma 4.14 thus Theorem 4.6. For any fixed R, recall the definition of $P^R = \{I \in \binom{[n]}{d/2} \mid R \subseteq I\}$, D^τ (Def. 4.28) and S^R (4.93).

Lemma 4.14 recast: W.p. $1 - n^{-5\log n}$ it holds that for all $R \subseteq \binom{[n]}{d/2}$:

$$M_0^R \succeq n^{-d} \cdot \mathrm{diag}(\widetilde{\mathrm{Cl}})_{P^R \times P^R}; \tag{4.141}$$

$$\pm\, \omega^{-c} M_c^R \preceq n^{-c/6} \cdot M_0^R, \quad \forall 0 < c \le |R|. \tag{4.142}$$

The following lemma will be handy.

Lemma 4.26. $\widetilde{L^R} D^\tau \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right)_{S^R \times S^R} \cdot D^\tau (\widetilde{L^R})^\top \succeq (\frac{\omega}{n})^{d/2} \mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right)_{P^R \times P^R}$ *for any* $R \in \binom{[n]}{\le d/2}$*, when evaluated on any* G*.*

Proof. Fix any $R \in \binom{[n]}{\le d/2}$. Without confusion, we omit subscript $S^R \times S^R$ by regarding the supports as the vertex-set $[n'] = [n] - R$ and regarding the corresponding matrix indices as $\binom{[n']}{d'/2}$ or $\binom{[n']}{\le d'/2}$, where $d'/2 = d/2 - |R|$. τ is unchanged. We will still use $\widetilde{\mathrm{Cl}}(X)$ to mean $\widetilde{\mathrm{Cl}}(X \sqcup R)$ for $X \subseteq [n']$.

Since $D^\tau \mathrm{diag}(\widetilde{\mathrm{Cl}}) D^\tau$ is nonnegative and diagonal for any G, we have

$$\widetilde{L^R} \left(D^\tau \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right) \cdot D^\tau \right) (\widetilde{L^R})^\top \succeq L^{R,0} \left(D^\tau \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right) \cdot D^\tau \right) (L^{R,0})^\top, \tag{4.143}$$

where recall $\widetilde{L^R} = (L^{R,0}, ..., L^{R,\tau})$. Further, $L^{R,0} = (L_0^{R,0}, ..., L_{d'/2}^{R,0})$, where $L_t^{R,0}$ is the matrix on column set $\binom{n'}{t}$. This means $L_{d/2-|R|}^{R,0} = \left(0, ..., 0, \mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right)_{\binom{[n']}{d'/2} \times \binom{[n']}{d'/2}}\right)$ since in $L^{R,0}$ (Def. 4.27) only ribbons $\mathcal{R} = (I, A; T')$ with 0-reduced size can occur, forcing $A = I$ and $T' \subseteq E(I)$. In particular, this implies RHS of (4.143) $\succeq (\frac{\omega}{n})^{d/2} \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}}\right)_{\binom{[n']}{d'/2} \times \binom{[n']}{d'/2}}$. Translated back to $[n]$ and $d/2$, this is exactly the bound in the lemma. □

Proof. (for Lemma 4.14) Fix $R \in \binom{[n]}{\leq d/2}$. By Lemma 4.20, for all $c \leq |R|$

$$M_c^R = \widetilde{L^R} \cdot \left[D^\tau \left(Q_{c,0}^R - Q_{c,1}^R + ... \pm Q_{c,d}^R \right) D^\tau \right] \cdot \left(\widetilde{L^R} \right)^\top + \mathcal{E}_c^R. \tag{4.144}$$

The following bounds all hold w.p. $> 1 - n^{-8\log n}$ from the corresponding lemmas, and we take union bound so the overall probability is $> 1 - n^{-5\log n}$. First,

$$\begin{aligned}
M_0^R &= \widetilde{L^R} \cdot \left[D^\tau \left(Q_{0,0}^R - Q_{0,1}^R + ... \pm Q_{0,d}^R \right) D^\tau \right] \cdot \left(\widetilde{L^R} \right)^\top + \mathcal{E}_0^R \\
&\succeq \tau^{-7\tau} \left[\widetilde{L^R} \cdot D^\tau \mathrm{diag}\left(\widetilde{\mathrm{Cl}} \right)_{S^R \times S^R} D^\tau \cdot \left(\widetilde{L^R} \right)^\top \right] + \mathcal{E}_0^R \quad \text{(Lem. 4.22(1))} \\
&\succeq \tau^{-7\tau} (\frac{\omega}{n})^{d/2} \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}} \right)_{P^R \times P^R} + \mathcal{E}_0^R \quad \text{(Lemma 4.26)} \\
&\succeq (\tau^{-7\tau} (\frac{\omega}{n})^{d/2} - n^{-\epsilon\tau/2}) \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}} \right)_{P^R \times P^R} \quad \text{(Lemma 4.20(4))} \\
&\succeq n^{-d} \cdot \mathrm{diag}(\widetilde{\mathrm{Cl}})_{P^R \times P^R} \quad \text{(parameter regime)}
\end{aligned}$$

Then for (4.142), fix R and let $1 \leq c \leq |R|$, we have:

$$\begin{aligned}
M_c^R &= \widetilde{L^R} \cdot \left[D^\tau \left(Q_{c,0}^R - Q_{c,1}^R + ... \pm Q_{c,d}^R \right) D^\tau \right] \cdot \left(\widetilde{L^R} \right)^\top + \mathcal{E}_c^R \\
&\preceq \omega^c n^{-c/4} \left[\widetilde{L^R} D^\tau \cdot \mathrm{diag}\left(\widetilde{\mathrm{Cl}} \right)_{S^R \times S^R} \cdot D^\tau \left(\widetilde{L^R} \right)^\top \right] + \mathcal{E}_c^R \quad \text{(Lem. 4.22(2))} \\
&\preceq \omega^c n^{-c/4} \left[\tau^{7\tau} (M_0^R - \mathcal{E}_0^R) \right] + \mathcal{E}_c^R \quad \text{(Lem. 4.22(1) and (4.144))} \\
&\preceq \omega^c n^{-c/5} M_0^R + \left(\omega^c n^{-c/4} + 1 \right) n^{-\epsilon\tau/2} \mathrm{diag}\left(\mathrm{Cl} \right)_{P^R \times P^R} \quad \text{(Lem. 4.20(4))}
\end{aligned}$$

So together,

$$\begin{aligned}
\omega^{-c} M_c^R &\preceq n^{-c/5} M_0^R + 2n^{-\epsilon\tau/2} \cdot \mathrm{diag}\left(\mathrm{Cl} \right)_{P^R \times P^R} \\
&\preceq (n^{-c/5} + 2n^d n^{-\epsilon\tau/2}) M_0^R \quad \text{((4.141) and } \widetilde{\mathrm{Cl}} \geq \mathrm{Cl}) \\
&\preceq n^{-c/6} \cdot M_0^R \quad (c \leq |R| \leq d/2 \text{ and parameter regime})
\end{aligned}$$

The same analysis holds for $-\omega^{-c}M_c^R$. $\square$

4.9 Appendix. Mod-order analysis

Set-up recap

We complete the deductions in section 4.6.1 now. Recall the ring $\mathbb{A}$ is got by adding fresh variables α and χ_T's to $\mathbb{R}$, where T ranges over edge sets on $[n]$ and with only the relations $\{\chi_{T'} \cdot \chi_{T''} = \chi_T \text{ whenever } T' \oplus T'' = T\}$. The **mod-order equation** is

$$L_\alpha \cdot \operatorname{diag}\left(\alpha^{|A|}\right) \cdot (L_\alpha)^\top = M_\alpha \qquad \text{mod } (*) \tag{4.145}$$

on the $\binom{[n]}{d/2} \times \binom{[n]}{\leq d/2}$-matrix variable L_α in ring $\mathbb{A}$, where

$$M_\alpha(I,J) = \sum_{T:|V(T)\cup I\cup J|\leq\tau} \alpha^{|V(T)\cup I\cup J|}\chi_T \quad \forall I,J : |I| = |J| = d/2,$$

and mod $(*)$ means to mod the ideal $(\{\alpha^{|V(T)\cup I\cup J|+1}\chi_T\},\ \{\chi_T : |V(T)\cup I\cup J| > \tau\})$ position-wise on each (I,J). We call $(*)$ the **modularity**. Moreover, if denote

$$L_1'(I,A) = \sum_{T'} \beta_{I,A}(T')\chi_{T'}, \quad \beta_{I,A}(T') \in \mathbb{R}[\alpha]$$

then we require

$$\alpha^{e_{I,A}(T')} \mid \beta_{I,A}(T') \quad \forall I, A, T' \tag{4.146}$$

where $e_{I,A}(T')$ is the reduced size $|V(T')\cup I\cup A| - s_{I,A}(T')$ (Def. 4.15).

Expressed in terms, equations (4.145), (4.146) become the following.

$$\sum_{A\in\binom{[n]}{\leq d/2}} \sum_{\substack{T',T'':\\ T'\oplus T''=T}} \alpha^{|A|}\cdot\beta_{I,A}(T')\cdot\beta_{J,A}(T'') = \alpha^{|V(T)\cup I\cup J|} \mod \alpha^{|V(T)\cup I\cup J|+1} \tag{4.147}$$

for every $(I, J; T)$ with $|V(T) \cup I \cup J| \leq \tau$, and

$$\alpha^{e_{I,A}(T')} \mid \beta_{I,A}(T') \tag{4.148}$$

for every $(I, A; T')$.

The main observation is the following (Lemma 4.16 recast).

Lemma 4.27. *(Order match) In the LHS of equation* (4.147)*, only products* $\alpha^{|A|} \cdot \beta_{I,A}(T') \cdot \beta_{J,A}(T'')$ *that satisfies the following are non-zero modulo* $(*)$*.*

$$A \text{ is a min-separator for both } (I, A; T'),\ (J, A; T''); \tag{4.149}$$

$$\big(V(T') \cup I \cup A\big) \ \cap \ \big(V(T'') \cup J \cup A\big) = A. \tag{4.150}$$

Moreover, (4.149)*,* (4.150) *imply that*

$$A \text{ is a min-separator of } (I, J; T) \text{ (where } T = T' \oplus T''); \tag{4.151}$$

$$|V(T') \cup I \cup A|,\ |V(T'') \cup J \cup A| \leq \tau. \tag{4.152}$$

Proof. Pick a term $\alpha^{|A|} \cdot \beta_{I,A}(T') \cdot \beta_{J,A}(T'')$ form the LHS of (4.147). By (4.148),

$$\text{its order in } \alpha \geq |A| + |V(T') \cup I \cup A| - s_{I,A}(T') + |V(T'') \cup A \cup J| - s_{J,A}(T'').$$

By modularity on the RHS of (4.147), the term is non-zero only if: (its order in α)$\leq$ $|V(T) \cup I \cup J|$ and $|V(T) \cup I \cup J| \leq \tau$, where $T = T' \oplus T''$. This implies

$$|V(T') \cup I \cup A| + |V(T'') \cup J \cup A| \leq \underbrace{|V(T) \cup I \cup J|}_{①} + \underbrace{(s_{I,A}(T') + s_{J,A}(T'') - |A|)}_{②} \tag{4.153}$$

Note ② $\leq |A|$ and "=" holds iff $s_{I,A}(T') = s_{J,A}(T'') = |A|$. While the LHS above

$$= \underbrace{|(V(T') \cup I \cup A) \cup (V(T'') \cup J \cup A)|}_{\geq |V(T) \cup I \cup J| = ①} + \underbrace{|(V(T') \cup I \cup A) \cap (V(T'') \cup J \cup A)|}_{\geq |A| \geq ②}.$$

Therefore, (4.153) could hold only when all "="'s hold, which means: (1). A is a min-separator of $(I, A; T')$, $(J, A; T'')$; (2). $(V(T') \cup I \cup A) \cup (V(T'') \cup J \cup A) = V(T) \cup I \cup J$; (3). $(V(T') \cup I \cup A) \cap (V(T'') \cup J \cup A) = A$.

Next, we show (1),(3) imply $A \in \mathrm{mSep}_{I,J}(T)$ (and also (2), actually). By (3), T', T'' could overlap only in $E(A)$. Now $T = T' \oplus T''$, so

$$T = T' \sqcup T'' \quad \text{modulo } E(A) \tag{4.154}$$

(also $\Rightarrow V(T') \cup V(T'') \subseteq V(T) \cup A$). By (1) there are $|A|$ many vertex-disjoint paths $p_1, , , .p_{|A|}$ from I to A in T', and similarly $q_1, ..., q_{|A|}$ from J to A in T''. These paths are also present in T by (4.154)—where it naturally assumes every path touches A only once at its endpoint. By (3) again, any p_i, q_j do not intersect beside endpoint in A so they are paired to $|A|$ many vertex-disjoint paths from I to J in T, all passing A (this also implies $A \subseteq V(T) \cup I \cup J$). On the other hand, if p is a path in T from I not passing A, then it is a path on $I \cup V(T')$ by induction using (3). Now by (3) again we have $(V(T') \cup I) \cap J \subseteq A$, so p can't reach J. So $A \in \mathrm{mSep}_{I,J}(T)$.

Finally, under the above implications, $V(T') \cup I \cup A \subseteq V(T) \cup I \cup J$ and similarly for $V(T'') \cup J \cup A$, so both have size $\leq \tau$. □

By this lemma, we can assume that in an imagined solution, $\beta_{I,A}(T') \neq 0$ only when it satisfies the conditions (4.149), (4.152) on its part. If assume further that the solution is *symmetric* (which looks plausible), i.e. $\beta_{I,A}(T') = \beta_{J,B}(T'')$ whenever $(I, A; T')$, $(J, B; T'')$ are of the same shape, then this lemma is particularly informative about some special $(I, J; T)$'s.

Corollary 4.6. *If $(I, J; T)$ has a* **unique** *min-separator A, then*

$$\sum_{\substack{T', T'': T' \oplus T'' = T \\ (4.149),\ (4.150)\ \text{hold}}} \beta_{I,A}(T') \cdot \beta_{J,A}(T'') = \alpha^{e_{I,J}(T)} \tag{4.155}$$

where $e_{I,J}(T) = |V(T) \cup I \cup J| - s_{I,J}(T)$. In particular, in symmetric solution,

$$\sum_{T_1 \subseteq E(A)} \beta_{I,A}(T_1 \oplus T')^2 = \alpha^{2 \cdot e_{I,A}(T')} \tag{4.156}$$

for all $(I, A; T')$ such that

$$A \text{ is the unique min-separator of } (I, A; T'). \tag{4.157}$$

Proof. The first part is directly from Lemma 4.16. For the "in particular" part, let $(I, A; T')$ satisfy (4.157). By mirroring $(I, A; T')$ through A, we get a $(J, A; T'')$ that satisfies the same condition and they together satisfy (4.149), (4.150). There are always enough vertices in $[n]$ to carry out this mirroring operation. By the symmetry assumption, $\beta_{I,A}(T') = \beta_{J,A}(T'')$. From mirroring it is not hard to see that A is the unique min-separator of $(I, J; T = T' \oplus T'')$, so for this triple $(I, J; T)$ equation (4.155) holds, giving that $\sum_{T_1 \subseteq E(A)} \beta_{I,A}(T' \oplus T_1)^2 = \alpha^{|V(T) \cup I \cup J| - |A|} = \alpha^{2(|V(T') \cup I \cup A| - |A|)}$. □

Summarizing what we got so far, let all $\beta_{I,A}(T' \oplus T_1)$'s in (4.156) be equal (which is a plausible assumption) then $\beta_{I,A}(T') = 2^{-\binom{|A|}{2}/2} \cdot \alpha^{e_{I,A}(T')}$ (taken all + signs); collecting these terms, we get a matrix L_1': $L_1'(I, A) = \sum_{\substack{T': |V(T') \cup I \cup A| \le \tau \\ (4.157)\ \text{holds} \\ T' \cap E(A) = \emptyset}} 2^{-\binom{|A|}{2}/2} \alpha^{|V(T') \cup I \cup A| - |A|} \chi_{T'} \cdot \widetilde{\mathrm{Cl}}_A$, where $\widetilde{\mathrm{Cl}}_A = \sum_{T \subseteq E(A)} \chi_T$. To see how far this is from a solution, notice $\widetilde{\mathrm{Cl}}_A^2 = 2^{\binom{|A|}{2}} \widetilde{\mathrm{Cl}}_A$ and consider

$$L_1' \cdot \mathrm{diag}\left(\alpha^{|A|}\right) \cdot (L_1')^\top = L_1 \cdot \mathrm{diag}\left(\alpha^{|A|} \cdot \widetilde{\mathrm{Cl}}_A\right) \cdot L_1^\top \tag{4.158}$$

where L_1 is the matrix in $\mathbb{A}$ as below (which is cleaner than L_1' to use).

Definition 4.36. $\forall I \in \binom{[n]}{d/2}$, $A \in \binom{[n]}{\leq d/2}$,

$$L_1(I,A) := \sum_{\substack{T' \colon |V(T')\cup I\cup A|\leq\tau \\ (4.157) \text{ holds} \\ T'\cap E(A)=\emptyset}} \alpha^{|V(T')\cup I\cup A|-|A|}\chi_{T'}. \tag{4.159}$$

Surely L_1' is not a solution to the mod-order equation, since (4.158) equals (mod (*)) only the part of M_α consisting of the special $(I,J;T)$'s from Cor. 4.6. For a general $(I,J;T)$, Lemma 4.27 only says:

$$\sum_{\substack{A,T',T'' \colon T'\oplus T''=T \\ A\in \mathrm{mSep}_{I,J}(T) \\ (4.149),(4.150) \text{ hold}}} \beta_{I,A}(T')\beta_{J,A}(T'') = \alpha^{e_{I,J}(T)} \mod \alpha^{e_{I,J}(T)+1}. \tag{4.160}$$

To see how to proceed further, we inspect a further weakening: polarization.

Polarized solution

Roughly speaking, polarization weakens linear equations with "x_i^2's" by replacing these terms with multi-linear "x_iy_i's", where $\vec{y}$ are fresh variables, and we plug in a "tentative" solution $\vec{x_0}$ and solve for $\vec{y}$ (the equations become in $\vec{y}$) then see how to modify $\vec{x_0}$ further.

Definition 4.37. *The* **polarized** *mod-order equation w.r.t.* L_1 *is:*

$$L_1 \cdot \mathrm{diag}\left(\alpha^{|A|}\cdot \widetilde{\mathrm{Cl}}_A\right)\cdot L_2^\top = M_\alpha \qquad \mod (*) \tag{4.161}$$

where $(*)$ *is the modularity in* (4.145), L_1 *is by* (4.159), L_2 *is a matrix*

$$L_2(I,A) = \sum_{T' \colon |V(T')\cup I\cup A|\leq\tau} \beta^{(2)}_{I,A}(T')\chi_{T'} \tag{4.162}$$

with variables $\{\beta^{(2)}_{I,A}(T')\}$ *required to satisfy* $\alpha^{e_{I,A}(T')} \mid \beta^{(2)}_{I,A}(T'), \forall (I,A,T')$.

In this polarized form, the essential condition (4.160) becomes

$$\sum_{\substack{A,T',T'':\ T'\oplus T''=T \\ (I,A;T') \text{ appears in } L_1 \\ (4.149),(4.150) \text{ hold}}} \alpha^{e_{I,A}(T')} \cdot \beta^{(2)}_{J,A}(T'') = \alpha^{e_{I,J}(T)} \mod \alpha^{e_{I,J}(T)+1}. \tag{4.163}$$

By (4.163), existence of a solution L_2 requires at least the following condition: for general $(I,J;T)$, there always exist "$(I,A;T')$ appearing in L_1" and T'' which satisfy the condition in the LHS of (4.163). By a direct (but careful) check, this is actually equivalent to the "In particular" part of the graph-theoretic fact 4.5 due to Escalante, restated below.

Fact 4.9.1. *For any ribbon* $(I,J;T)$*, the set of all min-separators,* $\mathrm{mSep}_{I,J}(T)$*, has a natural poset structure: min-separators* $A_1 \le A_2$ *iff* A_1 *separates* $(I,A_2;T)$*, or equivalently as can be checked, iff* A_2 *separates* $(J,A_1;T)$*. The set is further a* **lattice** *under this partial-ordering:* $\forall A_1, A_2 \in \mathrm{mSep}_{I,J}(T)$ *their join and meet exist. In particular, there exist a unique* **minimum** *and* **maximum**.

Denote the minimum by $S_l(I,J;T)$ *and the maximum by* $S_r(I,J;T)$*, which is the "leftmost" and "rightmost" min-separator, respectively.*

By this fact, some $(I,A;T')$ indeed appears in (4.163) with $A = S_l(I,J;T)$. Moreover, (4.163) is naturally satisfied if take

$$L_2(J,A) = \sum_{\substack{T'':\ |V(T'')\cup J\cup A|\le\tau \\ A\in \mathrm{mSep}_{J,A}(T'') \\ T''\cap E(A)=\emptyset \\ (J,A;T'') \text{ left-generated}}} \alpha^{e_{J,A}(T'')}\chi_{T''}. \tag{4.164}$$

Here, recall being left-generated means every vertex is either in A or can be connected from J without touching A. Also, with this L_2 only one product in the LHS of (4.163) contributes

to the right modulo $\alpha^{e_{I,J}(T)+1}$. We get:

Proposition 4.10. *The pair (L_1, L_2) is a solution to the polarized mod-order equation* (4.161), (4.162).

Remove the polarization. One more use of fact 4.9.1 actually shows that, if move the "left-generated" condition from L_2 to L_1, then L_2 itself factors through L_1—that is, we can replace $\mathrm{diag}(\widetilde{\mathrm{Cl}}) \cdot L_2^\top$ by some $X \cdot L_1^\top$ in (4.161), and this finally gives the following.

Proposition 4.11. *(Mod-order diagonalization; Prop. 4.3 recast) Let*

$$L_\alpha(I,A) := \sum_{\substack{T' \colon |V(T')\cup I\cup A|\le\tau \\ A=S_l(I,A;T') \\ T'\cap E(A)=\emptyset \\ (I,A;T') \text{ left-generated}}} \alpha^{e_{I,A}(T')}\chi_{T'},$$

$$Q_{0,\alpha}(A,B) := \sum_{\substack{T_m \colon |T\cup A\cup B|\le\tau \\ A,B\in \mathrm{mSep}_{A,B}(T_m)}} \alpha^{e_{A,B}(T_m)}\chi_{T_m}$$

(where T_m indicates "middle"). Then

$$L_\alpha \cdot [\mathrm{diag}\left(\alpha^{\frac{|A|}{2}}\right) \cdot Q_{0,\alpha} \cdot \mathrm{diag}\left(\alpha^{\frac{|A|}{2}}\right)] \cdot L_\alpha^\top = M_\alpha \qquad \mathrm{mod}\ (*) \tag{4.165}$$

where $(*)$ is the modularity in (4.145).

Proof. Given Fact 4.9.1, we immediately have the *canonical decomposition* of graphs as in Definition 4.21 and Remark 4.8. This implies that in the LHS of (4.165) only the products from canonical triples are non-zero modulo $(*)$, and they give M_α. □

Thus we get a "$L(-)L^\top$"-shape decomposition of M_α, meaning that we do not lose much from the polarization step since our goal is only to prove the PSDness of the matrix. Indeed, (4.165) gives the "first-approximate" decomposition in Definition 4.20.

CHAPTER 5

ON CDCL WITH ORDERED-DECISION STRATEGY

The content of this chapter is from a joint work with Nathan Mull and Alexander Razborov, whose abbreviated version appeared at the 23rd International Conference on Theory and Applications of Satisfiability Testing (SAT 2020) [81].

5.1 Introduction

SAT-solvers have become standard tools in many application domains such as hardware verification, software verification, automated theorem proving, scheduling and computational biology (see [52, 61, 33, 78, 38] among the others). Since their conception in the early 1960s, SAT-solvers have become significantly more efficient, but they have also become significantly more complex. Consequently, there has been increasing interest in understanding the theoretical limitations and strengths of contemporary SAT-solvers. Much of the recent literature has focused on the connections between SAT-solvers and subsystems of the resolution proof system originally introduced in [27, 98].

This connection essentially started with the Davis-Putnam-Logemann-Loveland procedure (DPLL) [41, 40], a backtracking search algorithm that builds partial assignments one literal at a time until a satisfying assignment is found or all assignments have been exhausted. Since DPLL is sound and complete, its computational trace when applied to an unsatisfiable formula is a *proof* of unsatisfiability. It is generally accepted as a folklore result that the computational trace of DPLL on an unsatisfiable formula can be converted into a tree-like resolution refutation. Thus, tree-like resolution lower bounds imply DPLL running time lower bounds. And in some sense, these lower bounds are tight: DPLL, given oracle access to a tree-like resolution refutation Π of the input formula, can run in time that is polynomial in the length of Π. That is, DPLL is essentially equivalent to tree-like resolution and thus

can be viewed as a propositional proof system in the Cook-Reckhow sense [39].

Nearly all contemporary SAT-solvers are variants of DPLL augmented with modern algorithmic techniques and heuristics. The technique most often credited for their success is *conflict-driven clause learning* (CDCL) [64, 77], so these solvers are interchangeably called CDCL SAT-solvers, CDCL solvers, or simply CDCL (for further information regarding the design of SAT-solvers, see the *Handbook of Satisfiability* [26]). Just as with DPLL, the computational trace of CDCL can be converted into a resolution refutation, but may no longer be tree-like or even regular. Thus, general resolution lower bounds imply CDCL running time lower bounds, but it is unclear *a priori* whether these bounds are tight in the same sense as above.

The line of work on the question of whether CDCL solvers simulate general resolution was initiated by Beame et al. [18] and continued by many others [104, 83, 56, 35, 20, 90, 9, 44]. The primary difference between all these papers is in the details of the model, the models considered by Pipatsrisawat and Darwich [90] and Atserias et al. [9] being perhaps the most faithful to actual implementations of CDCL SAT-solvers. But almost all models appearing in the literature make a few nonstandard assumptions.

1. *Very frequent restarts.* The solver restarts roughly $O(n^2)$ times for every clause in the given resolution refutation Π (where n is the total number of variables). Though many solvers do restart frequently in practice [25], it is unclear if this is really necessary for the strength of CDCL.

2. *No clause deletion policy.* The solver has to keep every learned clause. In practice, some solvers periodically remove half of all learned clauses [10].

3. *Nondeterministic decision strategy.* The solver uses oracle access to Π to construct a very particular decision strategy. In practice, solvers use heuristics [76, 80, 75].

It is natural to ask whether these assumptions can be weakened or removed entirely. In

this respect, the first two assumptions have become topics of recent interest. With regards to the first, much research has been dedicated to the study of *nonrestarting* SAT-solvers [104, 35, 36, 31, 19, 74]. The exact strength of CDCL without restarts is still unknown and, arguably, makes for the most interesting open problem in the area. With regards to the second, Elffers et al. [44] proved size-space tradeoffs in a very tight model of CDCL, which may be interpreted as results about aggressive clause deletion policies.

In this chapter we are primarily concerned with the third assumption, i.e., how much does the efficiency of CDCL-solvers depend on the nondeterminism in the decision strategy? We study a simple decision strategy that we call the *ordered* decision strategy which is identical to the strategy studied by Beame et al. [17] in the context of DPLL without clause learning. It is defined naturally: when the solver has to choose a variable to assign, the ordered decision strategy dictates that it chooses the smallest unassigned variable according to some fixed order. There is still a choice in whether to fix the variable to 0 (*false*) or 1 (*true*), and we allow the solver to make this choice nondeterministically. If unit propagation is used, the solver may assign variables out of order; a unit clause does not necessarily correspond to the smallest unassigned variable. This possibility to "cut the line" is precisely what makes the situation much more subtle and nontrivial.

Thus, our motivating question is the following:

Is there a family of contradictory CNFs $\{\tau_n\}_{n=1}^{\infty}$ *that possess polynomial size resolution refutations but require superpolynomial time for CDCL with any ordered decision strategy?*

Before describing our contributions towards this question, let us briefly review analogous separations in the context of proof and computational complexities. Bonet et al. [32] proved that a certain family of formulas requires exponential-sized ordered resolution refutations but has polynomial-sized regular resolution refutations. Bollig et al. [28] proved that a certain boolean function requires exponential-sized ordered binary decision diagrams (OBDDs) but have polynomial-sized general BDDs. These results tell us that order tends to be a strong

restriction, and the above question asks whether this same phenomenon occurs for CDCL. It is also worth noting that this question may be motivated as a way of understanding the strength of *static* decision strategies such as MINCE [4] and FORCE [5]. But since such decision strategies are rarely used in practice we will not dwell on this anymore.

Our contributions

Per the discussion above, a proof system that captures any class of CDCL solvers should be no stronger than general resolution. It can also be reasonably expected (and in two particular situations will be verified below as easy directions of Theorems 5.2, 5.3) that with any ordered decision strategy, they should be at least as strong as ordered resolution with respect to the same order. Our main results show that, for a nondetermistic model of CDCL in which the solver may arbitrarily choose conflict/unit clauses if there are several, may elect not to do conflict analysis/unit propagations at all, and may restart at any time, both extremes are attained. In this setting, the strength of the system depends on the *learning scheme* employed; that is, it depends on the method used to determine which clauses are learned after conflict analysis. More specifically, we prove

1. CDCL with the ordered decision strategy and a learning scheme we call DECISION-L is equivalent to ordered resolution (Theorem 5.2). In particular, it does not simulate general resolution.

2. CDCL with the ordered decision strategy and a learning scheme we call FIRST-L is equivalent to general resolution (Theorem 5.3).

Remark 5.1. *As the name suggests,* DECISION-L *is the same as the so-called DECISION learning scheme used in practice.*[1] *Hence these two results, taken together, go somewhat against the "common wisdom." Namely, it turns out that in the case of ordered decision*

1. We use this slightly different name so that it fits our naming conventions below.

strategy, an assertive learning scheme is badly out-performed by a scheme that, to the best of our knowledge, has not been used before. That said, FIRST-L *is similar to the learning scheme FirstNewCut [18], and both schemes have the property that they are designed somewhat artificially to target particular resolution steps in a given refutation.*

We also prove linear width lower bounds for CDCL with the ordered decision strategy (Theorem 5.4), which are in sharp contrast with the size-width relationship for general resolution proved by Ben-Sasson and Wigderson [21].

With the ability of possibly postponing conflict analysis and unit propagation, the model of CDCL we consider differs in these aspects from solvers that occur in practice. This is in part because our intention is to focus on the impact of decision strategies. But this substantial amount of nondeterminism also allows us to identify two proof systems that are, more or less straightforwardly, *equivalent* to the corresponding CDCL variant. (This correspondence is very much like the correspondence between *regWRTI* and a variant of CDCL with similar nonstandard features called *DLL-LEARN*, both introduced by Buss et al. [36, 31].) Determining the exact power of these systems constitutes the main technical part of this chapter.

The first proof system might be of independent interest; we call it *half-ordered resolution*. For a given order on the variables, ordered resolution can be alternatively described by the requirement that in every application of the resolution rule, the resolved variable is larger than any other variable appearing in both of the two antecedent clauses. We relax this requirement by asking that this property holds for *at least one* of them, which reflects the inherent asymmetry in resolution rules resulting from clause learning in CDCL solvers. Somewhat surprisingly (at least to us), it turns out (Theorem 5.1) that this relaxation does not add any extra power, and half-ordered resolution is polynomially equivalent to ordered resolution with respect to the same order.

The second proof system, which we call *trail resolution*, extends half-ordered resolution

and is more auxiliary in nature. It is based on the observation that with the amount of nondeterminism we allow, all trails[2] that a CDCL solver manages to create can be easily recreated when needed. Accordingly, the system works with lines of two types, one for clauses and another for trails. Clauses entail nontrivial trails via a unit propagation rule while trails can be used to enhance the half-ordered resolution rule. We show that trail resolution is polynomially equivalent to resolution (Theorem 5.5), and since it is by far our most difficult result, let us reflect a bit on the ideas in its proof.

Like other CDCL-based proof systems, trail resolution is not closed under restrictions or weakening, so many standard methods do not apply. Instead, we use two operations on resolution proofs (lifting and variable deletion) in tandem with some additional structural information to give us a fine-grained understanding of the size and structure of the general resolution refutation being simulated. The properties of these operators allow for a surgery-like process; we simulate small local pieces of the refutation and then stitch them together into a new global refutation.

Finally, in order to aid the above work (and, perhaps, even facilitate further research in the area), we present a model and language for studying CDCL-based proof systems. This model is not meant to be novel, and is heavily influenced by previous work [83, 9, 44]. However, the primary goal of our model is to *highlight* possible nonstandard sources of nondeterminism in variants of CDCL, as opposed to creating a model completely faithful to applications. For example, Theorem 5.3 can be written in this language as:

For any order π, CDCL(FIRST-L, π-D) *is equivalent to general resolution.*

We will also try to pay a special attention to finer details of the model sometimes left implicit in previous works. This entails several subtle choices to be made, and we interlace the mathematical description of our model with informal discussion of these choices.

2. A *trail* is essentially an ordered partial assignment constructed by CDCL during its execution.

The chapter is organized as follows. In Section 5.2 we give all necessary definitions and formulate our main results as we go along.

In Section 5.3 we prove Theorem 5.2 on the power of CDCL with the ordered decision strategy and the DECISION-L learning strategy. Section 5.3.1 contains proof-complexity theoretic arguments about half-ordered resolution, while in Section 5.3.2 we establish its translation to the language of CDCL.

In Section 5.4 we prove Theorem 5.3 on the power of CDCL with the ordered decision strategy and the FIRST-L learning strategy. To that end, in Section 5.4.1 we show the equivalence of this system to trail resolution (mentioned above) and in Section 5.4.2 we establish that trail resolution is actually equivalent to general resolution (Theorem 5.5).

In Section 5.5 we prove Theorem 5.4 that, roughly speaking, states that the simulation provided by Theorem 5.3 fails extremely badly with respect to width. Among other things, this implies that there does not seem to exist any useful width-size relation in the context of CDCL with ordered decision strategy.

Related works

The recent work of Vinyals [106] also studied the strength of decision heuristics in CDCL, where it was shown that CDCL with the popular VSIDS decision strategy (among others) cannot simulate ordered resolution.

5.2 Preliminaries and main results

Throughout the chapter, we assume that the set of propositional variables is fixed as $V \stackrel{\text{def}}{=} \{x_1, \ldots, x_n\}$. Recall the *resolution proof system* is a Hilbert-style proof system whose lines

are clauses and that has only one *resolution rule* (2.1). Note that the *weakening rule*

$$\frac{C}{C \vee D}$$

is *not* included by default. In the full system of resolution it is admissible in the sense that $S_R(\tau \vdash 0)$ does not change if we allow it. But this will not be the case for some of the CDCL-based fragments we will be considering below.

Remark 5.2. *Despite the above distinction, it is often convenient to consider systems that do allow the weakening rule. We make it clear when we do this by adding the annotation '+ weakening' to the system. For example, resolution + weakening is the resolution proof system with the weakening rule included.*

Resolution graphs

Our results depend on the careful analysis of the structure of resolution proofs. For example, it will be useful for us to maintain structural properties of the proof while changing the underlying clauses and derivations. We build up the following collection of definitions for this analysis, to which we will refer throughout the later sections. The reader may skip this section for now and return to it in the future as needed.

Definition 5.1. *For a resolution + weakening proof* Π*, its resolution graph,* $G(\Pi)$*, is a directed acyclic graph (DAG) representing* Π *in the natural way: each clause in* Π *has a distinguished node, and for each node there are incoming edges from the nodes corresponding to the clauses from which it is derived. Every node has in-degree 0, 1, or 2 if its corresponding clause is an axiom, derived by weakening, or derived by resolving two clauses, respectively. Denote the set of nodes by* $V(\Pi)$*, and the clause at* $v \in V(\Pi)$ *by* $c_\Pi(v)$*. We do* not *assume that* c_Π *is injective, that is we allow the same clause to appear in the proof several times.*

There is a natural partial order on $V(\Pi)$ reflecting the order of appearances of clauses in Π: $v > u$ if and only if v is a descendant of u, or equivalently, there is a (directed) path from u to v. We sometimes say that v is above (resp. below) u if $v > u$ (resp. $v < u$). If, moreover, (u, v) is an edge (directed from u to v), we say that u is a parent *of v. A set of nodes is independent if any two nodes in the set are incomparable. Note that we have defined this order so that we naturally view resolution graphs in bottom-up orientation, where axioms appear at the bottom and derivations flow upwards.*

Maximal and minimal nodes of any nonempty $S \subseteq V(\Pi)$ are defined with respect to this partial order: $\max_\Pi S \stackrel{\text{def}}{=} \{v \in S : \forall u \in S \neg(v < u)\}$, *and similarly for* $\min_\Pi S$.

Definition 5.2. *Let $S \subseteq V(\Pi)$. The upward closure and downward closure of S in $G(\Pi)$ are* $\mathrm{ucl}_\Pi(S) \stackrel{\text{def}}{=} \{v \in V(\Pi) : \exists w \in S(v \geq w)\}$ *and* $\mathrm{dcl}_\Pi(S) \stackrel{\text{def}}{=} \{v \in V(\Pi) : \exists w \in S(v \leq w)\}$, *respectively. A subset of nodes S is parent-complete if for any $v \in S$ of in-degree 2, one parent of v being in S implies that the other parent of v is also in S. It is path-complete if for any directed path p in $G(\Pi)$, the two end points of p being in S implies all nodes of p are.*

Remark 5.3. *The following are some basic facts about these definitions.*

- *The upward closure* $\mathrm{ucl}_\Pi(S)$ *is path-complete but need not be parent-complete.*
- *The downward closure* $\mathrm{dcl}_\Pi(S)$ *is always both path-complete and parent-complete.*
- *Path-completeness does not imply upward-closedness.*
- *The complement of any upward-closed set is downward-closed.*

Also, these definitions behave naturally, as demonstrated by the following proposition.

Proposition 5.1. *Let $S \subseteq V(\Pi)$ be a nonempty set of nodes that is both parent-complete and path-complete. Then the induced subgraph on S in $G(\Pi)$ is the graph of a proof which derives* $\max_\Pi S$ *from* $\min_\Pi S$.

Proof. Let $S^* \subseteq S$ be the set of all nodes in S "provable" from $\min_\Pi S$ inside S. Formally, it is the closure of $\min_\Pi S$ according to the following rule: if $v \in S$ and all its parents are in S^* then v is also in S^*. We need to show that $S^* = S$.

Assume not, and fix an arbitrary $v \in \min_\Pi(S \setminus S^*)$. Since $v \notin \min_\Pi S$, there exists $w \in S$ below v. Since S is path-complete, we can assume w.l.o.g. that w is a parent of v, and since S is parent-complete, all parents of v are in S. Now, since v is minimal in $S \setminus S^*$, all of them must be actually in S^*. Hence $v \in S^*$, a contradiction. □

In the sequel, we refer to a proof (refutation) defined on a subgraph in this way as a *subproof* (*subrefutation*).

Definition 5.3. *A resolution graph is connected if* $|\max_\Pi V(\Pi)| = 1$*, i.e., there is a unique sink.*

This is **not** the usual definition of connectedness for directed graphs. But it implies that every node can be connected to the unique sink by a directed path, and thus implies the weak connectedness in the usual sense (i.e., there is an undirected path between any two nodes).

Remark 5.4. *For a resolution proof* Π *and* $v \in V(\Pi)$*, the subgraph on* $\mathrm{dcl}_\Pi(\{v\})$ *is a connected resolution graph whose axiom nodes are among axiom nodes of* $G(\Pi)$*.*

Ordered and half-ordered resolution

Fix now an order $\pi \in S_n$. For any literal $l = x_k^a$, $\pi(l) \stackrel{\text{def}}{=} \pi(k)$. For $k \in [n]$, let Var_π^k denote the k smallest variables according to π. A clause C is *k-small* with respect to π if $\mathrm{Var}(C) \subseteq \mathrm{Var}_\pi^k$.

The proof system *π-ordered resolution* is the subsystem of resolution defined by imposing the following restriction on the resolution rule (2.1):

$$\forall l \in C \vee D \ (\pi(l) < \pi(x_i)).$$

That is, the two antecedents are i-small. We note that in the literature this system is usually defined differently, namely in a top-down manner (see e.g. [32]). It is easy to see, however, that our version is equivalent.

Definition 5.4. π-half-ordered resolution *is the subsystem of resolution in which the rule* (2.1) *is restricted by the requirement*

$$\forall l \in C \ (\pi(l) < \pi(x_i)). \tag{5.1}$$

That is, at least one of the antecedents is i-small.

Recall [39] that a proof system P *p*-simulates another proof system Q if there exists a polynomial time algorithm that takes any Q-proof to a P-proof from the same axioms (in particular, the size of the P-proof is bounded by a polynomial in the size of the original proof). Two systems P and Q are *polynomially equivalent* if they *p*-simulate each other.

We are now ready to state our first result.

Theorem 5.1. *For any order $\pi \in S_n$, π-ordered resolution is polynomially equivalent to π-half-ordered resolution.*

The next proof system, *π-trail resolution*, is even more heavily motivated by CDCL solvers. For this reason we interrupt our proof-complexity exposition to define the corresponding model. As we noted in the introduction, we will try to highlight certain subtle points in the definition of the model by injecting informal remarks.

5.2.1 CDCL-based proof systems

A *unit clause* is a clause consisting of a single literal. An *assignment* is an expression of the form $x_i = a$ $(1 \leq i \leq n,\ a \in \{0,1\})$. A *restriction* ρ is a set of assignments in which all variables are pairwise distinct. We denote by $\mathrm{Var}(\rho)$ the set of all variables appearing

in ρ. Restrictions naturally act on clauses, CNFs, resolution proofs, etc.; we denote by $C|_\rho,\ \tau|_\rho,\ \Pi|_\rho \ldots$ the result of this action. Note that both π-ordered resolution and π-half-ordered resolution are closed under restrictions, i.e., if Π is a π-(half)-ordered resolution proof, then $\Pi|_\rho$ is a $\pi|_\rho$-(half)-ordered resolution proof of no-bigger size, where $\pi|_\rho$ is the order induced by π on $V \setminus \mathrm{Var}(\rho)$.

Remark 5.5. *Restrictions of proofs also act on resolutions graphs, i.e., they give rise to a transformation from $G(\Pi)$ to $G(\Pi|_\rho)$. For example, if a clause is satisfied by a restriction ρ, its node will be immediately removed. And even if a clause is not satisfied, its node still might be not used in constructing $G(\Pi|_\rho)$ since e.g. a parent is removed.*

An *annotated assignment* is an expression of the form $x_i \stackrel{*}{=} a$ $(1 \leq i \leq n,\ a \in \{0,1\}, * \in \{d,u\})$. Informally, a CDCL solver builds (ordered) restrictions one assignment at a time, and the annotation indicates in what way the assignment is made: 'd' means by a decision, and 'u' means by unit propagation. See Definition 5.6 and Remark 5.8 below for details about these annotations.

Definition 5.5. *A* trail *is an ordered list of annotated assignments in which all variables are again pairwise distinct. A trail acts on clauses, CNFs, etc., just in the same way as does the restriction obtained from it by disregarding the order and the annotations on assignments. For a trail t and an annotated assignment $x_i \stackrel{*}{=} a$ such that x_i does not appear in t, we denote by $[t, x_i \stackrel{*}{=} a]$ the trail obtained by appending $x_i \stackrel{*}{=} a$ to its end. $t[k]$ is the kth assignment of t. A* prefix *of a trail $t = [x_{i_1} \stackrel{*_1}{=} a_1, \ldots, x_{i_r} \stackrel{*_r}{=} a_r]$ is any trail of the form $[x_{i_1} \stackrel{*_1}{=} a_1, \ldots, x_{i_s} \stackrel{*_s}{=} a_s]$ $(0 \leq s \leq r)$ denoted by $t[\leq s]$. Λ is the empty trail.*

A state *is a pair $(\mathbb{C}, t)$, where $\mathbb{C}$ is a CNF and t is a trail. The state $(\mathbb{C}, t)$ is* terminal *if either $C|_t \equiv 1$ for all $C \in \mathbb{C}$ or $\mathbb{C}$ contains 0. All other states are nonterminal. We let $\mathbb{S}_n$ denote the set of all states (recall that n is reserved for the number of variables), and let $\mathbb{S}_n^o \subset \mathbb{S}_n$ be the set of all nonterminal states.*

Remark 5.6. *As unambiguous as Definition 5.5 may seem, it already reflects one important choice, to consider only* positional[3] *solvers, i.e., those that are allowed to carry along only CNFs and trails, but not any other auxiliary information. The only mathematical ramification of this restriction is that we will have to collapse the whole clause learning stage into one step, but that is a sensible thing to do anyway.*

Remark 5.7. *We are now about to describe the core of our (or, for that matter, any other) model, which can be viewed as a labeled transition system consisting of the state space* $\mathbb{S}_n$ *and possible labeled transitions between states. But since this definition is the longest one, we prefer to change gears and* precede *it with some informal remarks rather than give them after the definition.*

Proof systems attempting to capture performance of modern CDCL solvers are in general much bulkier than their logical counterparts and are built from several heterogeneous blocks. At the same time, most papers highlight the impact of one or a few of the features, with a varying degrees of nondeterminism allowed, while the features out of focus are treated in often unpredictable and implicit ways. We have found this state of affairs somewhat impending for the effort of trying to compare different results to each other or to build useful structure around them of the kind existing in "pure" proof complexity. Therefore, we adapt an approach that in a sense is the opposite. Namely, we rigorously describe a basic *model that is very liberal and nondeterministic and intends to approximate the union of most conceivable features of CDCL solvers. Then models of actual interest will be defined by their* deviations *from the basic model. These deviations will take the form of "amendments" forbidding certain forms of behavior or, potentially, allowing for new ones.*

Besides this point, there are only few (although sometimes subtle) differences from the previous models, so our description is given more or less matter-of-factly.

3. The name is suggested by a similar term "positional strategy" in game theory.

Definition 5.6. *For a nonterminal state $S = (\mathbb{C}, t) \in \mathbb{S}_n^o$, we define the finite set Actions(S) and the function Transition$_S$: Actions$(S) \longrightarrow \mathbb{S}_n$; the fact Transition$_S(A) = S'$ will be usually abbreviated to $S \overset{A}{\Longrightarrow} S'$. Those are described as follows:*

$$\mathit{Actions}(S) \overset{\text{def}}{=} D(S) \,\dot\cup\, U(S) \,\dot\cup\, L(S),$$

where the letters D, U, and L naturally stand for decision, unit propagation, and learning.[4]

- *$D(S)$ consists of all annotated assignments $x_i \overset{d}{=} a$ such that x_i does not appear in t and $a \in \{0, 1\}$. We naturally let*

$$(\mathbb{C}, t) \overset{x_i \overset{d}{=} a}{\Longrightarrow} (\mathbb{C}, [t, x_i \overset{d}{=} a]). \tag{5.2}$$

- *$U(S)$ consists of all those assignments $x_i \overset{u}{=} a$ for which $\mathbb{C}|_t$ contains the unit clause x_i^a; the transition function is given by the same formula (5.2) but with a different annotation:*

$$(\mathbb{C}, t) \overset{x_i \overset{u}{=} a}{\Longrightarrow} (\mathbb{C}, [t, x_i \overset{u}{=} a]). \tag{5.3}$$

- *As should be expected, $L(S)$ is the most sophisticated part of the definition (cf. [9, Section 2.3.3]). It consists of clause-trail pairs (C, t^*) where C is a learnable clause and t^* is a prefix of t with the assignments that persist after learning C and backtracking. The exact class of such pairs is given in Definition 5.7. The transition function is then defined naturally:*

$$(\mathbb{C}, t) \overset{(C, t^*)}{\Longrightarrow} (\mathbb{C} \cup \{C\}, t^*).$$

Definition 5.7. *Given $(\mathbb{C}, t) \in \mathbb{S}_n^o$, the set of learnable clauses from S is defined as follows. Let $t = [x_{i_1} \overset{*_1}{=} a_1, \ldots, x_{i_r} \overset{*_r}{=} a_r]$. By reverse induction on $k = r + 1, \ldots, 1$ we define the*

4. Restarts will be treated as a part of the learning scheme.

set $\mathbb{C}_k(S)$ that, intuitively, is the set of clauses that can be learned by backtracking up to the prefix $t[\leq k]$.

We let

$$\mathbb{C}_{r+1}(S) \stackrel{\text{def}}{=} \{\, D \in \mathbb{C} \mid D|_t = 0 \,\}$$

be the set of all conflict clauses.

For $1 \leq k \leq r$, we do the following: if the k-th assignment of t is of the form $x_{i_k} \stackrel{d}{=} a_k$, then $\mathbb{C}_k(S) \stackrel{\text{def}}{=} \mathbb{C}_{k+1}(S)$. Otherwise, it is of the form $x_{i_k} \stackrel{u}{=} a_k$, and we build up $\mathbb{C}_k(S)$ by processing every clause $D \in \mathbb{C}_{k+1}(S)$ as follows.

- *If D does not contain the literal $\overline{x_{i_k}^{a_k}}$ then we include D into $\mathbb{C}_k(S)$ unchanged.*
- *If D contains $\overline{x_{i_k}^{a_k}}$, then we resolve D with all clauses $C \in \mathbb{C}$ such that $C|_{t[\leq k-1]} = x_{i_k}^{a_k}$ and include into $\mathbb{C}_k(S)$ all the results $Res(C, D)$. D itself is not included.*

To make sure that this definition is sound, we have to guarantee that C and D are actually resolvable (that is, they do not contain any other conflicting variables but x_{i_k}). For that we need the following observation, easily proved by reverse induction on k, simultaneously with the definition:

Claim 5.1. *$D|_t = 0$ for every $D \in \mathbb{C}_k(S)$.*

Finally, we let

$$\mathbb{C}(S) \stackrel{\text{def}}{=} \bigcup_{k=1}^{r} \mathbb{C}_k(S),$$

and

$$L(S) \stackrel{\text{def}}{=} \begin{cases} \{(0, \Lambda)\} \text{ if } 0 \in \mathbb{C}(S); \\ \{\, (C, t^*) \mid C \in (\mathbb{C}(S) \setminus \mathbb{C}),\ t^* \text{ a prefix of } t \text{ such that } C|_{t^*} \neq 0 \,\} \text{ otherwise.} \end{cases} \tag{5.4}$$

Example 1. *Consider the scenario in which*

$$\mathbb{C} = \{x_1 \vee \overline{x_4},\ \overline{x_3} \vee x_4,\ x_1 \vee x_3 \vee x_4,\ x_1 \vee \overline{x_3} \vee x_4\}$$
$$t = [x_1 \stackrel{d}{=} 0,\ x_4 \stackrel{u}{=} 0,\ x_3 \stackrel{u}{=} 1]$$
$$S = (\mathbb{C}, t).$$

Then

$$\mathbb{C}_4(S) = \{\overline{x_3} \vee x_4,\ x_1 \vee \overline{x_3} \vee x_4\}$$
$$\mathbb{C}_3(S) = \{x_1 \vee x_4\}$$
$$\mathbb{C}_2(S) = \{x_1\}$$
$$\mathbb{C}_1(S) = \mathbb{C}_2(S)$$

so $\mathbb{C}(S) = \{x_1,\ x_1 \vee x_4\}$ *and, finally,*

$$L(S) = \{(x_1, \Lambda),\ (x_1 \vee x_4, \Lambda),\ (x_1 \vee x_4, (x_1 \stackrel{d}{=} 0))\}.$$

This completes the description of the basic model.

Remark 5.8. *For nearly all modern implementations of CDCL, the annotations are redundant because CDCL solvers typically require unit propagation always to be performed when it is applicable (in our language of amendments, this feature will be called* ALWAYS-U*). Nevertheless, the presence of annotations makes the basic model flexible enough to carry on various, sometimes subtle, restrictions and extensions. In particular, we consider solvers that are not required to* record *unit propagations as such. This allows for the situation in which* $x_i \stackrel{d}{=} a$ and $x_i \stackrel{u}{=} a$ *are in Actions*(S)*, and the set of learnable clauses is sensible to this.*

Remark 5.9. *In certain pathological cases, mostly resulting from neglecting to* do *unit prop-*

agation, the set Actions$(\mathbb{C}, t)$ *may turn out to be empty even if* $(\mathbb{C}, t)$ *is nonterminal and* $\mathbb{C}$ *is contradictory. But for the reasons already discussed above, we prefer to keep the basic model as clean as possible* syntactically*, postponing such considerations for later.*

The *transition graph* Γ_n is the directed graph on $\mathbb{S}_n$ defined by erasing the information about actions; thus $(S, S') \in E(\Gamma_n)$ if and only if $S' \in \mathrm{im}(\mathrm{Transition}_S)$. It is easy to see (by double induction on $(|\mathbb{C}|, n - |t|)$) that Γ_n is acyclic. Moreover, both the set $\{\,(S, A) \mid A \in \mathrm{Actions}(S)\,\}$ and the function $(S, A) \mapsto \mathrm{Transition}_S(A)$ are polynomial-time[5] computable. These observations motivate the following definition.

Definition 5.8. *Given a CNF* $\mathbb{C}$*, a partial run on* $\mathbb{C}$ *from the state* S *to the state* T *is a sequence*

$$S = S_0 \overset{A_0}{\Longrightarrow} S_1 \overset{A_1}{\Longrightarrow} \dots S_{L-1} \overset{A_{L-1}}{\Longrightarrow} S_L = T, \tag{5.5}$$

where $A_k \in \mathit{Actions}(S_k)$*. In other words, a partial run is a path in* Γ_n*, with annotations restored. A successful run is a partial run from* $(\mathbb{C}, \Lambda)$ *to a terminal state. A* CDCL solver *is a partial function*[6] μ *on* $\mathbb{S}_n^o$ *such that* $\mu(S) \in \mathit{Actions}(S)$ *whenever* $\mu(S)$ *is defined. The above remarks imply that when we apply a CDCL solver* μ *to any initial state* $(\mathbb{C}, \Lambda)$*, it will always result in a finite sequence like* (5.5)*, with* T *being a terminal state (successful run) or such that* $\mu(T)$ *is undefined (failure).*

Remark 5.10. *Theoretical analysis usually deals with* classes *(i.e., sets) of individual solvers rather than with individual implementations, and there might be several different approaches to defining such classes. One might consider for example various complexity restrictions like demanding that* μ *be polynomial-time computable. But in this chapter we are more interested in classes defined by prioritizing and restricting various actions.*

5. in the size of the state S, not in n

6. It is possible for $\mathrm{Actions}(S)$ to be empty, see Remark 5.9.

Definition 5.9. *A* local *class of CDCL solvers is defined by a collection AllowedActions*$(S) \subseteq$ *Actions*(S), $S \in \mathbb{S}_n^o$. *It consists of all those solvers* μ *for which* $\mu(S) \in$ *AllowedActions*(S), *whenever* $\mu(S)$ *is defined.*

We will describe local classes of solvers in terms of *amendments* prescribing what actions should be *removed* from the set Actions(S) to form AllowedActions(S). Without further ado, let us give a few examples illustrating how familiar restrictions look in this language. Throughout the description, we fix a nonterminal state $S = (\mathbb{C}, t)$.

ALWAYS-C If $\mathbb{C}|_t$ contains the empty clause, then $D(S)$ and $U(S)$ are removed from Actions(S). In other words, this amendment requires the solver to perform conflict analysis if it can do so.

ALWAYS-U If $\mathbb{C}|_t$ contains a unit clause, then $D(S)$ is removed from Actions(S). This amendment insists on unit propagation, but leaves to nondeterminism the choice of the unit to propagate if there are several choices. Note that as defined, ALWAYS-U is a lower priority amendment than ALWAYS-C: under the latter, if both a conflict and a unit clause are present, the solver must do conflict analysis while under the former both unit propagation and conflict analysis are permitted.

ALWAYS-R In definition (5.4) of $L(S)$ we keep only those (C, t^*) for which $t^* = \Lambda$.

NEVER-R In definition (5.4) of $L(S)$, we require that t^* is the *longest* prefix of t satisfying $C|_{t^*} \neq 0$ (in which case $C|_{t^*}$ is necessarily a unit clause). As described, this amendment does not model nonchronological backtracking or require that the last assignment in the trail is a decision. However, this version is easier to state and it is not difficult to modify to have the aforementioned properties. Furthermore, all open questions pertaining to this amendment remain open for either version.

ASSERTING-L In definition (5.4) of $L(S)$, we shrink $\mathbb{C}(S) \setminus \mathbb{C}$ to $\left(\bigcup_{k=1}^{s} \mathbb{C}_k(S)\right) \setminus \mathbb{C}$, where $s < r$ is the largest index for which $x_{i_s} = a_s$ is annotated as 'd' in t. This amendment

is meaningful (and mostly used) only when combined with ALWAYS-C and ALWAYS-U, in which case we can state expected properties like the fact that every learned clause contains the literal $x_{i_s}^{1-a_s}$ (we do not need this fact, so we leave its proof to the reader).

DECISION-L In definition (5.4) of $L(S)$, we shrink $\mathbb{C}(S)\backslash\mathbb{C}$ to $\mathbb{C}_1(S)\backslash\mathbb{C}$. This amendment has appeared in practice as a natural asserting learning scheme. By induction on length of the trail t, it is not hard to see that the learned clause according to this amendment is falsified by just the decisions in t. The clause could consist of a strict subset of those decided variables.

FIRST-L In definition (5.4) of $L(S)$, we shrink $\mathbb{C}(S) \setminus \mathbb{C}$ to those clauses that are obtained by resolving, in the notation of Definition 5.6, between pairs C and D with $D \in \mathbb{C}$. As noted in the introduction, this is similar to the scheme FirstNewCut [18] but one is not a generalization of the other. FIRST-L is applicable in more settings (FirstNewCut was designed in a setting with mandatory conflict analysis). And the "New" in First-NewCut refers to its ability to perform more resolutions in order to derive a clause not currently in the formula, which is not modeled by FIRST-L.

π-D, **where** $\pi \in S_n$ **is an order on the variables** We keep in $D(S)$ only the two assignments $x_i \stackrel{d}{=} 0$, $x_i \stackrel{d}{=} 1$, where x_i is the *smallest* variable w.r.t. π that does not appear in t. Note that this amendment does not have any effect upon $U(S)$, and our main technical contributions can be also phrased as determining under which circumstances this "loophole" can circumvent the severe restriction placed on the set $D(S)$.

WIDTH-w, **where** w **is an integer** In definition (5.4) of $L(S)$, we keep in $\mathbb{C}(S) \setminus \mathbb{C}$ only clauses of width $\leq w$. Note that this amendment still allows us to use wide clauses as intermediate results *within* a single clauses learning step.

SPACE-s, **where** s **is an integer** If $|\mathbb{C}| \geq s$, then $L(S)$ is entirely removed from Actions(S). This amendment makes sense when accompanied by the possibility to do bookkeeping

by removing "unnecessary" clauses. We will briefly discuss positive amendments in Remark 5.12 below.

Thus, our preferred way to specify local classes of solvers and the corresponding proof systems is by listing one or more amendments, with the convention that their effect is cumulative: an action is removed from Actions(S) if and only if it should be removed according to at least one of the amendments present.

Definition 5.10. *For a finite set $\mathcal{A}_1, \dots, \mathcal{A}_r$ of poly-time computable amendments,*[7] *we let* CDCL($\mathcal{A}_1, \dots, \mathcal{A}_r$) *be the (possibly incomplete) proof system whose proofs are those successful runs* (5.5) *in which none of the actions A_i is affected by any of the amendments $\mathcal{A}_1, \dots, \mathcal{A}_r$.*

Remark 5.11. *The amendments* ALWAYS-C, ALWAYS-U *are present in most previous work and, arguably, it is precisely what distinguishes conflict-driven clause learning techniques. Nonetheless, we have decided against including them into the basic model as they may be distracting in theoretical studies focusing on other features; our work is one example.*

Remark 5.12. *Let us briefly discuss the possibility of extending the basic model rather than restricting it. The most substantial deviation would be to forfeit the assumption of positionality (see Remark 5.6) or, in other words, to allow the solver to carry along more information than just a set of clauses and a trail. Two such examples are dynamic variable ordering and phase saving.*

For positional solvers, extending the basic model amounts to introducing positive amendments *enlarging the sets Actions(S) instead of decreasing them. Here are a few suggestions we came across during our deliberations.*

CLAUSE DELETION *For $S = (\mathbb{C}, t) \in \mathbb{S}^o_n$, we add to Actions($S$) all subsets $\mathbb{C}_0 \subseteq \mathbb{C}$. The*

7. An amendment is poly-time computable if determining whether an action $\mu(S)$ is in AllowedActions(S) is poly-time decidable given S and $\mu(S)$.

transition function is obvious:

$$(\mathbb{C}, t) \stackrel{\mathbb{C}_0}{\Longrightarrow} (\mathbb{C}_0, t).$$

This is the space model whose study was initiated in [44], and like in that paper, we do not see compelling reasons to differentiate between original clauses and the learned ones.

MULTI-CLAUSE LEARNING *In the definition* (5.4) *of* $L(S)$*, we can allow arbitrary nonempty subsets* $\mathbb{C}_0 \subseteq \mathbb{C}(S) \setminus \mathbb{C}$ *instead of a single clause* C *and require that* $C|_{t^*} \neq 0$ *for* any $C \in \mathbb{C}$*, with the obvious transition*

$$(\mathbb{C}, t) \stackrel{(\mathbb{C}_0, t^*)}{\Longrightarrow} (\mathbb{C} \cup \mathbb{C}_0, t^*).$$

Though existing SAT-solver implementions tend not to do this, it is natural to consider when thinking of Pool resolution or RTL proof systems as variants of CDCL (see e.g. [104, 36]).

INCOMPLETE LEARNING *In the definition* (5.4) *of* $L(S)$*, we could remove the restriction* $C|_{t^*} \neq 0$ *on the prefix* t^**. This positive amendment could make sense in the absence of* ALWAYS-C*, that is, if we are prepared for delayed conflict analysis.*

In this language, the (nonalgorithmic part of the) main result from [9, 90] can be roughly summarized as

CDCL(ALWAYS-C, ALWAYS-U, ALWAYS-R, ASSERTING-L) *is polynomially equivalent to resolution.*[8]

8. Their result is actually stronger in that the choice of which unit to propagate and which clause to learn can be made adversarially.

The algorithmic part from [9] roughly says that *any* CDCL solver in the associated class, subject to the only condition that the choice of actions from $D(S)$ (when it is allowed by the amendments) is random, polynomially simulates bounded-width resolution[9]. The open question asked in [9, Section 2.3.4] can be reasonably interpreted as whether CDCL(ALWAYS-C, ALWAYS-U, WIDTH-w) is as powerful as width-w resolution, perhaps with some gap between the two width constraints (We took the liberty to remove those amendments that do not appear to be relevant to the question.) Finally, we would like to abstract the "no-restarts" question as

Does CDCL(ALWAYS-C, ALWAYS-U, NEVER-R) (*or at least* CDCL(NEVER-R)) *simulate general resolution?*

where we have again removed all other amendments in the hope that this will make the question more clean mathematically.

5.2.2 Technical contributions

As they had already been discussed in the introduction, here we formulate our results (in the language just introduced) without additional exposition.

Theorem 5.2. *For any fixed order π on the variables, the system* CDCL(π-D, DECISION-L) *is polynomially equivalent to π-ordered resolution.*

Theorem 5.3. *For any fixed order π on the variables, the system* CDCL(π-D, FIRST-L) *is polynomially equivalent to general resolution.*

Theorem 5.4. *For any fixed order π on the variables and every $\epsilon > 0$ there exist contradictory CNFs τ_n with $w(\tau_n \vdash 0) = O(1)$ not provable in* CDCL(π-D, WIDTH-$(1-\epsilon)n$).

9. That is, has running time $n^{O(w(\tau_n \vdash 0))}$ with high probability, given a contradictory CNF τ_n as an input.

Finally, let us mention that while $\mathsf{CDCL}(\mathcal{A}_1, \ldots, \mathcal{A}_r)$ can be naturally regarded as a (possibly incomplete) proof system where proofs are efficiently checkable, it need not necessarily be a Hilbert-style proof system, operating with "natural" lines and inference rules. Assume, however, that the set AllowedActions(S) additionally satisfies the following two properties:

1. whenever AllowedActions(S) $\cap\, L(S) \neq \emptyset$, it contains an action leading to a state of the form $(\mathbb{C}, \Lambda)$ (i.e, restarts are allowed);

2. (monotonicity) If $S = (\mathbb{C}, t)$, $S' = (\mathbb{C}', t)$ and $\mathbb{C} \subseteq \mathbb{C}'$ then AllowedActions(S)$\cap(D(S) \,\dot\cup\, U(S)) \subseteq$ AllowedActions(S') $\cap\, (D(S') \,\dot\cup\, U(S'))$.

Then every trail t that appears in a run can always be *recreated*, at a low cost, when it is needed again. Thus, under these restrictions we get a "normal" proof system with nice properties.

Note that property 2) might not hold in the presence of ALWAY-C, ALWAYS-U, and this is the main reason why we do not include them in the basic model for studying CDCL as a proof system. Let us now formulate this system explicitly for the case π-D we are mostly interested in.

Definition 5.11. *Fix an order π on the variables. π-trail resolution is the following (two-typed) proof system. Its lines are either clauses or trails (where the empty trail is an axiom), and it has the following rules of inference:*

$$\frac{t}{[t, x_i \overset{d}{=} a]}, \quad \textit{(Decision rule)}$$

where x_i is the π-smallest index such that x_i does not appear in t and $a \in \{0, 1\}$ is arbitrary;

$$\frac{t \qquad C}{[t, x_i \overset{u}{=} a]}, \quad \textit{(Unit propagation rule)}$$

where $C|_t = x_i^a$*;*

$$\frac{C \vee x_i^a \qquad D \vee x_i^{1-a} \qquad t}{C \vee D}, \quad \textit{(Learning rule)}$$

where $(C \vee D)|_t = 0$*,* $(x_i \overset{*}{=} a) \in t$ *and all other variables of* C *appear before* x_i *in* t*.*

It is straightforward to see that without the unit propagation rule, this is just π-half-ordered resolution.

Then, the main technical part in proving Theorem 5.3 is the following.

Theorem 5.5. *For every fixed order* π *on the variables,* π*-trail resolution is polynomially equivalent to general resolution.*

5.3 CDCL(π-D, DECISION-L) $=_p$ π-ordered

In this section we prove Theorem 5.2. The proof is made up of two parts (Theorem 5.1, Theorem 5.6), with half-ordered resolution as the intermediary.

5.3.1 π-half-ordered $=_p$ π-ordered

Half-ordered resolution trivially p-simulates ordered resolution, so the core of Theorem 5.1 is the other direction. In this section we will depend heavily on resolution graphs (Definition 5.1) and related definitions from Section 5.2.

Definition 5.12. *A resolution refutation* Π *is ordered up to* k *(with respect to an order* π*) if it satisfies the property that if any two clauses are resolved on a variable* $x_i \in \mathrm{Var}_\pi^k$*, then all resolution steps above it are on variables in* $\mathrm{Var}_\pi^{\pi(i)-1}$*. We note that* π*-ordered resolution proofs are precisely those that are ordered up to* $n-1$*.*

We now prove the main part of Theorem 5.1, namely that π-ordered resolution p-simulates π-half-ordered resolution.

Proof. (of theorem 5.1) Let Π be a π-half-ordered resolution refutation of τ. Without loss of generality, assume that $\pi = \mathrm{id}$ (otherwise rename variables).

We will construct by induction on k ($0 \leq k \leq n-1$) a half-ordered resolution refutation Π_k of τ, which is ordered up to k. For the base case, let $\Pi_0 = \Pi$. Suppose Π_k has been constructed; without loss of generality we can assume that Π_k is connected (otherwise take the subrefutation below any occurrence of 0).

Consider the set of nodes whose clauses are k-small. Note this set is parent-complete. We claim it is also upward-closed. Indeed, let u be any node in this set (i.e., $c(u) = c_{\Pi_k}(u)$ is k-small) and v be a child of u. Then $c(v)$ is obtained by resolving a variable $x_i \in \mathrm{Var}_\pi^k$ since we disallow weakenings. The fact that Π_k is ordered up to k implies $\mathrm{Var}(c(v)) \subseteq \mathrm{Var}_\pi^{i-1} \subseteq \mathrm{Var}_\pi^k$ (otherwise, some variable in $c(v)$ would have remained unresolved on a path connecting v to the sink by connectedness), thus $c(v)$ is also k-small i.e. v is in this set. Therefore, by induction, any node above u is in the set.

Upward-closedness implies path-completeness (see Remark 5.3), so by Proposition 5.1, the set $\{v \mid c(v) \text{ is } k\text{-small}\}$ defines a subrefutation of the clauses labeling the independent set

$$\mathcal{L}_k \stackrel{\text{def}}{=} \min_{\Pi_k}\{v|\ c(v) \text{ is } k\text{-small}\}. \tag{5.6}$$

Denote $\mathcal{U} := \mathrm{ucl}_{\Pi_k}(\mathcal{L}_k)$ $(= \{v|\ c(v) \text{ is } k\text{-small}\})$ and $\mathcal{D} := \mathrm{dcl}_{\Pi_k}(\mathcal{L}_k)$ where $\mathcal{D}, \mathcal{U}, \mathcal{L}$ stands for *downward*, *upward*, and *layer*, respectively. Then we have the following.

- $\mathcal{U} \cap \mathcal{D} = \mathcal{L}_k$ (from the independence of nodes in $\mathcal{L}_k$);
- $\mathcal{D}$ is also a subproof (by Remark 5.3 and Proposition 5.1);
- $\Pi_k = \mathcal{U} \cup \mathcal{D}$. To see this, note by connectedness any node v can be connected by a directed path p in Π_k to the unique sink—the empty clause which belongs to $\mathcal{U}$. Consider the first $u \in p$ that is in $\mathcal{U}$. If $u = v$ then $v \in \mathcal{U}$, otherwise $u \in \mathcal{L}_k$ (since $\mathcal{U}$ is path- and parent-complete) and then $v \in \mathcal{D}$.

That is, the "layer" $\mathcal{L}_k$ splits Π_k into two subproofs $\mathcal{U}$, $\mathcal{D}$ and they meet at $\mathcal{L}_k = \min_{\Pi_k}(\mathcal{U}) = \max_{\Pi_k}(\mathcal{D})$. $\mathcal{U}$ contains all nodes labeled by a k-small clause, and $\mathcal{D}$ is the union of $\mathcal{L}_k$ and the set of all nodes whose labeled clause is not k-small. In particular, all axioms are in $\mathcal{D}$, all resolutions in $\mathcal{U}$ are on the variables in Var_π^k and, since Π_k is ordered up to k, all resolutions in $\mathcal{D}$ are on the variables not in Var_π^k.

Define

$$M \stackrel{\text{def}}{=} \min_{\mathcal{D}}\{w|\ c(w) \text{ is the result of resolving two clauses on } x_{k+1}\} \tag{5.7}$$

where $\min_{\mathcal{D}}$ is taken with respect to the topological order in the proof $\mathcal{D}$ (cf. the last paragraph in Definition 5.1). If M is empty, $\Pi_{k+1} \stackrel{\text{def}}{=} \Pi_k$. Otherwise, suppose $M = \{w_1, \ldots, w_s\}$ (where $w_1, \ldots, w_s$ are independent nodes in $\mathcal{D}$), and define

$$A_i \stackrel{\text{def}}{=} \mathrm{ucl}_{\mathcal{D}}(\{w_i\}). \tag{5.8}$$

We will eliminate all resolutions on x_{k+1} in $\mathcal{D}$ by the following process; it should be emphasized that *the set of nodes stays the same* during this process. Only the edges and clause-labeling function change. More precisely, we update $\mathcal{D}$ in s rounds, defining π-half-ordered resolution + *weakening* proofs $\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_s$. Initially $\mathcal{D}_0 = \mathcal{D}$, $i = 1$. Let c_{i-1} denote the clause-labeling $c_{\mathcal{D}_{i-1}}$. To define the transition $\mathcal{D}_{i-1} \to \mathcal{D}_i$, we need the following structural properties of $\mathcal{D}_{i-1}$ (that will also be proved by induction simultaneously with the definition).

Claim 5.2. *Let u and v be arbitrary vertices in $V(\mathcal{D})$.*

a. If v is not above u in $\mathcal{D}$, then the same is true in $\mathcal{D}_{i-1}$;

b. $c_{i-1}(v)$ is equal to $c_{\mathcal{D}}(v)$, $c_{\mathcal{D}}(v) \vee x_{k+1}$ or $c_{\mathcal{D}}(v) \vee \overline{x_{k+1}}$;

c. *If* $v \notin \bigcup_{j=1}^{i-1} A_j$ *then* $c_{i-1}(v) = c_{\mathcal{D}}(v)$*, and* $c_{i-1}(v)$ *is obtained in* $\mathcal{D}_{i-1}$ *via application of the same resolution rule as in* $\mathcal{D}_i$*;*

d. $\mathcal{D}_{i-1}$ *is a* π*-half-ordered resolution + weakening proof.*

In the base case ($i = 1$), Claim 5.2 holds simply because $\mathcal{D}_0 = \mathcal{D}$.

Let us construct $\mathcal{D}_i$. By Claim 5.2(c), the resolution step at w_i (which is not in $\bigcup_{j=1}^{i-1} A_j$ by independence) is unchanged from $\mathcal{D}$ to $\mathcal{D}_{i-1}$. Assume that it resolves $c_{\mathcal{D}}(w') = B \vee x_{k+1}$ and $c_{\mathcal{D}}(w'') = C \vee \overline{x_{k+1}}$. Since Π_k is half-ordered, either B or C is k-small. Assume without loss of generality that B is k-small.

Recall that there is no resolution in $\mathcal{D}$ on variables in Var_π^k. Thus, for all $v \in A_i$, it follows that B is a subclause of $c_{\mathcal{D}}(v)$, and by Claim 5.2(b), we get the following crucial property:

$$\text{For all } v \in A_i,\ B \text{ is a subclause of } c_{i-1}(v). \tag{5.9}$$

Note that A_i is upward closed in $\mathcal{D}_{i-1}$ by Claim 5.2(a). Accordingly, as the first step, for any $v \notin A_i$ we set $c_i(v) \coloneqq c_{i-1}(v)$ and do not change its incoming edges.

Next, we update vertices $v \in A_i$ in an arbitrary $\mathcal{D}$-topological order maintaining the property $c_i(v) \in \{c_{i-1}(v),\ c_{i-1}(v) \vee \overline{x_{k+1}}\}$ (in particular, $c_i(v) = c_{i-1}(v)$ whenever $c_{i-1}(v)$ contains the variable x_{k+1}). First we set $c_i(w_i) \coloneqq c_{i-1}(w_i) \vee \overline{x_{k+1}}$ (recall that $c_{i-1}(w_i) = c_{\mathcal{D}}(w_i)$ by Claim 5.2(c) and hence does not contain x_{k+1} by (5.7)), and replace incoming edges by a weakening edge from w''.

For $v \in A_i \setminus \{w_i\}$ (as a reminder, it might be that $v \in \bigcup_{j<i} A_j$), we proceed as follows.

1. If $x_{k+1} \in c_{i-1}(v)$, keep the clause but replace incoming edges with a weakening edge (w', v). This is well-defined by (5.9), and note for the record that $w' <_{\mathcal{D}} w_i <_{\mathcal{D}} v$.

2. If $c_{i-1}(v) = \mathrm{Res}(c_{i-1}(u), c_{i-1}(w))$ on x_{k+1} where $\overline{x_{k+1}} \in c_{i-1}(u)$, set $c_i(v) \coloneqq c_{i-1}(v) \vee \overline{x_{k+1}}$, and replace incoming edges by a weakening edge (u, v).

3. If $c_{i-1}(v)$ is weakened from $c_{i-1}(u)$ (and $x_{k+1} \notin c_{i-1}(v)$), set $c_i(v) \coloneqq c_{i-1}(v) \vee c_i(u)$. In other words, we append the literal $\overline{x_{k+1}}$ to $c_i(v)$ if and only if this was previously done for $c_i(u)$.

4. Otherwise, $x_{k+1} \notin c_{i-1}(v)$ and $c_{i-1}(v) = \mathrm{Res}(c_{i-1}(u), c_{i-1}(w))$ on some x_ℓ where $\ell > k+1$. In particular, $x_{k+1} \notin \{c_{i-1}(u), c_{i-1}(w)\}$. Set $c_i(v) \coloneqq \mathrm{Res}(c_i(u), c_i(w))$ that is, like in the previous item, we append $\overline{x_{k+1}}$ if and only if it was previously done for either $c_i(v)$ or $c_i(w)$. Note that since $\ell > k+1$, this step remains π-half-ordered.

This completes our description of $\mathcal{D}_i$; we have to check Claim 5.2 for it. For (a), note that the only new edges were added in item 1, and see the remark made there. The items (b) and (c) are straightforward. For (d), the only different resolution steps were introduced in item 4; again, see the remark made there.

The next claim summarizes the necessary properties of the end result, $\mathcal{D}_s$.

Claim 5.3.

a. $\mathcal{D}_s$ is a π-half-ordered resolution + weakening proof without resolutions on x_{k+1}.

b. If $c_s(v) \neq c_{\mathcal{D}}(v)$ for some $v \in \mathcal{D}$, then there is a vertex w in $\mathrm{dcl}_{\mathcal{D}}(M) \setminus \{M\}$ such that $c_{\mathcal{D}}(v) = Res(c_s(w), c_s(v))$ on x_{k+1}, and this resolution is half-ordered. In fact, w is a parent (in $\mathcal{D}$'s topology) of some node in M.

Proof.

a. No new resolution on the variable x_{k+1} has been introduced, while all old ones are in $A_1 \cup \cdots \cup A_s$ and thus have been eliminated. The conclusion follows from this observation together with Claim 5.2(d).

b. Suppose $c(v)$ was changed in $\mathcal{D}_{i-1} \to \mathcal{D}_i$ (and hence stayed unchanged afterwards by Claim 5.2(b)) then in particular $v \in A_i$. Set $w \coloneqq w'$ where w' is the parent of w_i we chose in the paragraph above (5.9). Note that $c_s(w) = c_{\mathcal{D}}(w)$ since the latter contains the literal

(say) x_{k+1}. Then we readily have $c_{\mathcal{D}}(v) = c_{\mathcal{D}_{i-1}}(v) = \mathrm{Res}(B \vee x_{k+1}, c_{\mathcal{D}}(v) \vee \overline{x_{k+1}})$ by (5.9), and it is half-ordered since B is k-small. □

Now to get Π_{k+1}, we try to reconnect $\mathcal{D}_s$ with $\mathcal{U}$ along $\mathcal{L}_k$ (again, their node sets have been unchanged so far), then clear out weakenings. The problem with this approach is the added appearances of x_{k+1}^a (where a may be 0 or 1) in $c_s(v)$ for $v \in \mathcal{L}_k$, as in Claim 5.2(b). We introduce new nodes to deal with them. Namely, let $\mathcal{L}_k^{bad} := \{v \in \mathcal{L}_k \mid c_s(v) \neq c_{\mathcal{D}}(v)\}$, and for each node $v \in \mathcal{L}_k^{bad}$, keeping in mind Claim 5.3(b), create a **new** node denoted by $\widetilde{v}$ labeled with the clause $\mathrm{Res}(c_s(w), c_s(v)) = c_{\mathcal{D}}(v)$. Denote the set of new vertices by $\mathcal{N}$. Define $\widetilde{\Pi}_{k+1}$ to be the result of connecting $\mathcal{D}_s \sqcup \mathcal{N}$ and $\mathcal{U}$ along $(\mathcal{L}_k \backslash \mathcal{L}_k^{bad}) \sqcup \mathcal{N}$.[10]

Before this operation neither $\mathcal{D}_s$ nor $\mathcal{U}$ contained resolutions on x_{k+1}, and hence $\widetilde{\Pi}_{k+1}$ is a half-ordered refutation (with weakenings) that is *ordered up to* $k+1$. Let Π_{k+1} be obtained by contracting[11] all weakening rules in $\widetilde{\Pi}_{k+1}$. Then Π_{k+1} is also half-ordered up to $k+1$ since contracting weakening rules preserves this property. It only remains to analyze the size, $|\Pi_{k+1}|$ (note that *a priori* it can be doubled at every step, which is unacceptable).

Since

$$|\Pi_{k+1}| \leq |\Pi_k| + |\mathcal{L}_k|, \tag{5.10}$$

we only have to control $|\mathcal{L}_k|$. For that we will keep track of the invariant $|\mathrm{dcl}_{\Pi_k}(\mathcal{L}_k)|$; more precisely, we claim that

$$|\mathrm{dcl}_{\Pi_{k+1}}(\mathcal{L}_{k+1})| \leq |\mathrm{dcl}_{\Pi_k}(\mathcal{L}_k)|. \tag{5.11}$$

10. For example, suppose $v \in \mathcal{L}_k$ and $c_{\mathcal{D}}(v) = x_1 \vee x_2$ but $c_s(v) = x_1 \vee x_2 \vee \overline{x_{k+1}}$ (assuming $k > 1$). By Claim 5.3(b), there is a vertex w with $c_s(w) \subseteq x_1 \vee x_2 \vee x_{k+1}$ and

$$c(\widetilde{v}) := \mathrm{Res}(c_s(w), c_s(v)) = x_1 \vee x_2 = c_{\mathcal{D}}(v),$$

so we will use $\widetilde{v}$ instead of v in connecting $\mathcal{D}_s$ and $\mathcal{U}$ to construct $\widetilde{\Pi}_{k+1}$.

11. By contraction here we mean the process implicit in showing that weakening rules can be eliminated in a resolution refutation without increasing its size.

Let us prove this by constructing an injection from $\mathrm{dcl}_{\Pi_{k+1}}(\mathcal{L}_{k+1})$ to $\mathrm{dcl}_{\Pi_k}(\mathcal{L}_k)$; we will utilize the previous notation.

First note that the resolution + weakening refutation $\widetilde{\Pi}_{k+1}$ and its weakening-free contraction Π_{k+1} can be related as follows. For every node $v \in V(\Pi_{k+1})$ there exists a node $v^* \in V(\widetilde{\Pi}_{k+1})$ with $c_{\widetilde{\Pi}_{k+1}}(v^*) \supseteq c_{\Pi_{k+1}}(v)$ which is *minimal* among those contracting to v. If v is an axiom node of Π_{k+1} then so is v^* in $\widetilde{\Pi}_{k+1}$. Otherwise, if u and w are the two parents of v, and if u' and w' are the corresponding parents of v^* (v^* may not be obtained by weakening due to the minimality assumption), then $c_{\widetilde{\Pi}_{k+1}}(u^*)$ is a subclause of $c_{\widetilde{\Pi}_{k+1}}(u')$ and $c_{\widetilde{\Pi}_{k+1}}(w^*)$ is a subclause of $c_{\widetilde{\Pi}_{k+1}}(w')$. We claim that $(v \mapsto v^*)\,|_{\mathrm{dcl}_{\Pi_{k+1}}(\mathcal{L}_{k+1})}$ (which is injective by definition) is the desired injection. We have to check that its image is contained in $\mathrm{dcl}_{\Pi_k}(\mathcal{L}_k)$.

Fix $v \in \mathrm{dcl}_{\Pi_{k+1}}(\mathcal{L}_{k+1})$. Then *either v is an axiom or both its parents are not $(k+1)$-small* (by (5.6)). By the above mentioned facts about the contraction $\widetilde{\Pi}_{k+1} \to \Pi_{k+1}$, this property is inherited by v^*. In particular, $v^* \notin \mathcal{N}$ (the set of the newly added nodes when constructing Π_k) because all nodes in this set have at least one $(k+1)$-small parent (the w node in Claim 5.3(b)). Finally, since the corresponding clauses in $\mathcal{D}$ and $\mathcal{D}_s$ differ only in the variable x_{k+1}, v^* cannot be in U, for the same reason (recall that all axioms are in $\mathcal{D}$). Hence $v^* \in V(\mathcal{D}_s) = V(\mathcal{D}) = \mathrm{dcl}_{\Pi_k}(\mathcal{L}_k)$.

Having thus proved (5.11), we conclude by the obvious induction that $|\mathcal{L}_k| \le |\mathrm{dcl}_{\Pi_k}(\mathcal{L}_k)| \le |\mathrm{dcl}_{\Pi_0}(\mathcal{L}_0)| \le |\Pi|$. Then (5.10) implies $|\Pi_{n-1}| \le n|\Pi|$, as desired. □

5.3.2 π-half-ordered $=_p$ CDCL(π-D, DECISION-L)

In this section, we prove the following theorem.

Theorem 5.6. *The systems* CDCL(π-D, DECISION-L) *and π-half-ordered resolution are p-equivalent.*

One direction is almost trivial.

Proposition 5.2. CDCL(π-D, DECISION-L) *p-simulates π-half-ordered resolution.*

Proof. As usual, assume $\pi = \mathrm{id}$. Suppose $C \vee D = \mathrm{Res}(C \vee x_i,\ D \vee \overline{x_i})$ is any half-ordered resolution, and without loss of generality assume C is i-small. It is enough to present a partial run from (τ, Λ) to $(\tau \cup \{C \vee D\}, \Lambda)$ of length at most $n+1$, where τ is any clause set containing $C \vee x_i$ and $D \vee \overline{x_i}$.

Let x_j be the largest variable in C (thus $j < i$). Consider a trail of the form

$$t = [x_1 \stackrel{d}{=} a_1, \ldots, x_j \stackrel{d}{=} a_j, x_i \stackrel{u}{=} 1, x_{j+1} \stackrel{d}{=} a_{j+1}, \ldots, x_{i-1} \stackrel{d}{=} a_{i-1}, x_{i+1} \stackrel{d}{=} a_{i+1}, \ldots, x_n \stackrel{d}{=} a_n]$$

such that $(C \vee D)|_t = 0$. By definition, $t[l] \in \mathrm{AllowedActions}((\tau, t[\leq l-1]))$ for all $l \neq j+1$. But since C is i-small, $(C \vee x_i)|_{t[\leq j]} = x_i$ and thus $x_i \stackrel{u}{=} 1 \in \mathrm{AllowedActions}((\tau, t[\leq j]))$ as well. Therefore,

$$(\tau, \Lambda) \stackrel{t[1]}{\Longrightarrow} (\tau, t[\leq 1]) \stackrel{t[2]}{\Longrightarrow} (\tau, t[\leq 2]) \ldots \stackrel{t[n]}{\Longrightarrow} (\tau, t)$$

is a partial run from (τ, Λ) to (τ, t). It now suffices to show $(\tau \cup \{C \vee D\}, \Lambda) \in L((\tau, t))$. This follows by verifying Definition 5.6 directly: $(D \vee \overline{x_i})|_t = 0$ so $D \vee \overline{x_i} \in \mathbb{C}_{n+1}((\tau, t))$. For $j' > j+1$, the assignment $t[j']$ is a decision, so $D \vee \overline{x_i} \in \mathbb{C}_{j+2}((\tau, t))$. Since $(C \vee x_i)|_{t[\leq j]} = x_i$, $C \vee D = \mathrm{Res}(C \vee x_i, D \vee \overline{x_i}) \in \mathbb{C}_{j+1}((\tau, t))$. Finally, for $j' \leq j$, $t[j']$ is a decision, so $C \vee D \in \mathbb{C}_1(\tau, t)$ and $(\tau \cup \{C \vee D\}, \Lambda) \in \mathrm{AllowedActions}((\tau, t))$. □

The other direction of Theorem 5.6 is less obvious. We begin with some additional notation.

Previous works describe standard learning schemes like DECISION-L with respect to so-called *trivial resolution* on a set of particular clauses (e.g., in [90, 18]). We can recast this notion in our model by the following lemma. Let

$$D \circ^x C \stackrel{\mathrm{def}}{=} \begin{cases} \mathrm{Res}(D, C) & \text{if } C \text{ and } D \text{ are resolvable on } x \\ D & \text{otherwise (“null case”)} \end{cases}$$

and we extend this definition by left associativity:

$$C_0 \circ^{x_{i_1}} C_1 \circ^{x_{i_2}} \cdots \circ^{x_{i_k}} C_k \stackrel{\text{def}}{=} (\ldots (C_0 \circ^{x_{i_1}} C_1) \circ^{x_{i_2}} \ldots) \circ^{x_{i_k}} C_k.$$

Note if x_{i_j} appears maximally in C_j (according to π) for each $j \in [k]$, then all the resolutions are π-half-ordered.

Lemma 5.1. *Assume, in the notation of in Definition 5.6, a clause D is learned from state $S = (\mathbb{C}, t = [y_1 \stackrel{*_1}{=} a_1, \ldots, y_r \stackrel{*_r}{=} a_r])$.*

Assume $D \in \mathbb{C}_j(S)$ for some $j \in [r+1]$. Then there exist $k \leq r$, indices $j \leq i_1 < \cdots < i_k \leq r$ and clauses $C_1, \ldots, C_{k+1} \in \mathbb{C}$ such that $*_{i_1} = ... = *_{i_k} = u$ (i.e. the indices correspond to some unit propagations in t) and the following properties hold.

1. *$C_{k+1}|_t = 0$.*
2. *$C_\nu|_{t[\leq i_\nu - 1]} = y_{i_\nu}^{a_{i_\nu}}$ for $\nu \in [k]$.*
3. *$D = C_{k+1} \circ^{y_{i_k}} C_k \cdots \circ^{y_{i_1}} C_1$ where all operators are not null.*
4. *For any $\ell \in [j, r]$ with $*_\ell = u$, if variable y_ℓ appears in C_ν for some $\nu \in [k+1]$ then $\ell \in \{i_1, \ldots, i_k\}$.*

Proof. This is by directly tracing Definition 5.6. Suppose $D \in \mathbb{C}_j$, we use reverse induction on j to define the desired clauses and indices. If $j = r+1$, let $k = 0$ and $C_{k+1} = D$ (the conflict clause). If $j \leq r$, either $D \in \mathbb{C}_{j+1}(S)$, or there are clauses $D' \in \mathbb{C}_{j+1}(S)$, $C \in \mathbb{C}$ such that $C|_{t[\leq j-1]} = y_j^{a_j}$ and $D = \text{Res}(D', C)$ on y_j. In the first case, the clauses and indices are the same as for $D \in \mathbb{C}_{j+1}(S)$, and in the second case, enlarge the index list by adding j and the clause list by appending C to be the first. Items 1,2,3 follow immediately by this definition.

Now we can represent the learning of D as a sequence of clauses $X_{r+1}(= C_{k+1}) \stackrel{\text{step } r}{\longrightarrow} X_r \to ... \stackrel{\text{step } 1}{\longrightarrow} X_j(= D)$ where at each step $i_\mu \in \{i_1, ..., i_k\}$ a resolution $X_{i_\mu} = \text{Res}(X_{i_\mu + 1}, C_\mu)$

happens, and at each step $a \in [j, r] \backslash \{i_1, ..., i_k\}$, $X_a = X_{a+1}$. To prove item 4, assume $\ell \in [r]$, $\nu \in [k+1]$ satisfy the assumption there. Let $i_{k+1} := r + 1$ for convenience. First, it cannot be that $i_\nu < \ell$ since $\mathrm{Var}(C_\nu) \subset \mathrm{Var}(t[\leq i_\nu])$ but $y_\ell \notin \mathrm{Var}(t[\leq i_\nu])$. So assume $i_\nu > \ell$ (if $i_\nu = \ell$ then we are done). By items 1 and 2, for any ν' with $i_{\nu'} > \ell$, $C_{\nu'}$ does not contain $y_\ell^{a_\ell}$; so in particular, $y_\ell^{1-a_\ell} \in C_\nu$ by assumption. Then $y_\ell^{1-a_\ell} \in X_{i_\nu} = (C_{k+1} \circ^{y_{i_k}} C_k \cdots \circ^{y_{i_\nu}} C_\nu)$ (where all resolutions are not null), and the literal $y_\ell^{1-a_\ell}$ appears in $X_{i_\nu} ... X_{\ell+1}$. Hence, a resolution step on y_ℓ must happen at step ℓ, which means $\ell \in \{i_1, ..., i_k\}$. □

In short, C_{k+1} is a conflict clause and the other C_ν's are clauses in $\mathbb{C}$ chosen to do resolutions while backtracking in a learning step. These clauses are not necessarily unique, but we fix a choice arbitrarily.

Example 2. *Let us consider the same scenario as in Example 1 with $\pi = id$ (so that t is a legitimate trail). One way to learn the clause $x_1 \in \mathbb{C}_1(S)$ is to take the clauses*

$$C_1 = x_1 \vee \overline{x_4}$$

$$C_2 = x_1 \vee x_3 \vee x_4$$

$$C_3 = x_1 \vee \overline{x_3} \vee x_4$$

so that $(C_3 \circ^{x_3} C_2) \circ^{x_4} C_1 = x_1$.

The following Proposition 5.3 will complete the proof of Theorem 5.6, and with Theorem 5.1 this completes the proof of Theorem 5.2.

Proposition 5.3. *π-half-ordered resolution p-simulates* $\mathsf{CDCL}(\pi\text{-}\mathsf{D}, \mathsf{DECISION\text{-}L})$.

Proof. Fix a successful run in $\mathsf{CDCL}(\pi\text{-}\mathsf{D}, \mathsf{DECISION\text{-}L})$. Since the clause set only changes after a learning step, it suffices to show that for each learning step $S = (\mathbb{C}, t) \overset{(D,t^*)}{\Longrightarrow} (\mathbb{C} \cup \{D\}, t^*)$, there is a short half-ordered resolution proof of D from $\mathbb{C}$. Suppose $t = [y_1 \overset{*_1}{=}$

$a_1, \ldots, y_r \overset{*_r}{=} a_r]$ and assume $\pi = \mathrm{id}$, as usual. Fix the clauses C_ν for $\nu \in [k+1]$ and the set $\{i_1, ..., i_k\}$ as in Lemma 5.1 where we take $j = 1$ (that is, $D \in \mathbb{C}_1(S)$) due to DECISION-L.

Recall that

$$D = C_{k+1} \circ^{y_{i_k}} C_k \cdots \circ^{y_{i_1}} C_1. \tag{5.12}$$

The high-level idea is the following. The sequence of resolutions (5.12) is not all half-ordered only if some $y_{i_\nu}^{a_{i_\nu}}$ is not the largest in C_ν (which may happen since the assignments in t need not necessarily respect the order π). Our goal is thus to replace in (5.12), this time going from right to left, each clause C_ν for $\nu \in [k]$ by a clause C'_ν in which y_{i_ν} is the largest. This will give the desired half-ordered resolution.

First, let $C'_1 = C_1$. For $\nu \in [2, k+1]$, let

$$C'_\nu \overset{\text{def}}{=} C_\nu \circ^{y_{i_{\nu-1}}} C'_{\nu-1} \cdots \circ^{y_{i_1}} C'_1 \tag{5.13}$$

where this time some operators may be null.

It is immediate from (5.13) and Lemma 5.1(2) that

$$y_{i_\nu}^{a_\nu} \in C'_\nu \text{ for all } \nu \in [k] \tag{5.14}$$

and

$$C'_\nu \subseteq \bigcup_{\mu=1}^{\nu} C_\mu \text{ for all } \nu \in [k+1] \text{ (by induction on } \nu). \tag{5.15}$$

Lemma 5.2. *For any $\mu < \nu$, variable y_{i_μ} does not appear in the clause $C_\nu \circ^{y_{i_{\nu-1}}} C'_{\nu-1} \cdots \circ^{y_{i_\mu}} C'_\mu$.*

Proof. We first prove the fact that, for all $\nu \in [k+1]$ and $\mu \leq \nu$,

$$(C_\nu \circ^{y_{i_{\nu-1}}} C'_{\nu-1} \cdots \circ^{y_{i_\mu}} C'_\mu)|_{t[\leq i_\nu - 1]} = y_{i_\nu}^{a_{i_\nu}} \quad \text{where } y_{i_{k+1}}^{a_{i_{k+1}}} \coloneqq 0.$$

For this we use double induction, first on ν and then on $\mu = \nu \ldots 1$. For $\mu = \nu$, this is Lemma 5.1(2) (and Lemma 5.1(1) when $\mu = \nu = k+1$). For $\mu < \nu$ let $E \stackrel{\text{def}}{=} (C_\nu \circ^{y_{i_{\nu-1}}} C'_{\nu-1} \cdots \circ^{y_{i_{\mu+1}}} C'_{\mu+1})$; we have to prove that $(E \circ^{y_{i_\mu}} C'_\mu)|_{t[\leq i_\nu - 1]} = y_{i_\nu}^{a_{i_\nu}}$ from $E|_{t[\leq i_\nu - 1]} = y_{i_\nu}^{a_{i_\nu}}$. We can assume without loss of generality that this operator is not null, and then note $C'_\mu \mid_{t[\leq i_\mu - 1]} = y_{i_\mu}^{a_\mu}$ by the inductive assumption applied to the pair $\nu \coloneqq \mu,\ \mu \coloneqq 1$.

Now we prove the lemma. Again let $E = C_\nu \circ^{y_{i_{\nu-1}}} C'_{\nu-1} \cdots \circ^{y_{i_{\mu+1}}} C'_{\mu+1}$. Note that $y_{i_\mu}^{a_{i_u}} \in C'_{i_\mu}$ by (5.14) so $y_{i_\mu}^{a_{i_\mu}} \notin E$ (otherwise $E \mid_{t[\leq i_\nu - 1]} = 1$, contradicting the above fact), and the two clauses are consistent on other variables in C'_μ (according to $t[\leq i_\mu - 1]$). Then a simple case analysis on whether or not $E \circ^{y_{i_\mu}} C'_{i_\mu}$ is a null operator shows that the result does not contain y_{i_μ} or $\overline{y_{i_\mu}}$. □

Example 3. *Considering the same clauses as in Example 2, note that the resolution* $C_3 \circ^{x_3} C_2$ *is not (id)-half-ordered. The derivation from the above lemma would yield the clauses*

$$C'_1 = C_1$$
$$C'_2 = C_2 \circ^{x_4} C'_1 = x_1 \vee x_3$$
$$C'_3 = (C_3 \circ^{x_3} C'_2) \circ^{x_4} C'_1 = x_1$$

where all resolutions are now half-ordered.

We now complete the proof of Proposition 5.3. By Lemma 5.2, the variable y_{i_μ} does not appear in $C_\nu \circ^{y_{i_{\nu-1}}} C'_{\nu-1} \cdots \circ^{y_{i_\mu}} C'_\mu$ $(\mu < \nu)$. Also, it does not appear in $C_{\mu-1}, \ldots, C_1$ (by Lemma 5.1(2)) and thus not in $C'_{\mu-1}, \ldots, C'_1$ (by (5.15)). Hence it does not appear in C'_ν and we arrive at the following strengthening of (5.15):

$$\forall \nu \in [k+1],\ C'_\nu \subseteq (\bigcup_{\mu=1}^{\nu} C_\mu) \backslash (\bigcup_{\mu=1}^{\nu-1} \{y_{i_\mu}, \overline{y_{i_\mu}}\}). \tag{5.16}$$

By Lemma 5.1(4) and the fact that $j = 1$ (here we use DECISION-L), (5.16) means any

variable different from y_{i_ν} in C'_ν is labeled as d in $t_{[\leq i_\nu - 1]}$. This implies y_{i_ν} ($\nu \in [k]$) is maximal in C'_ν since we are in π-D. Thus for all $\nu \in [k+1]$ the sequence $C_\nu \circ^{y_{i_{\nu-1}}} C'_{\nu-1} \cdots \circ^{y_{i_1}} C'_1$ is half-ordered. Taken together, these sequences yield a half-ordered derivation of C'_{k+1} with $O(k^2)$ steps in total.

Finally, by (5.16) $C'_{k+1} \subseteq (\bigcup_{\mu=1}^{k+1} C_\mu) \setminus (\bigcup_{\mu=1}^{k} \{y_{i_\mu}, \overline{y_{i_\mu}}\}) \subset D$ where the latter inclusion follows by Lemma 5.1(3). This suffices for proving the proposition since the weakening rule is admissible in π-half-ordered resolution. □

5.4 CDCL(π-D, FIRST-L) $=_p$ resolution

In this section we prove Theorem 5.3. We first show that CDCL(π-D, FIRST-L) and π-trail resolution (see Definition 5.11) are p-equivalent and then prove size upper bounds for π-trail resolution.

5.4.1 π-trail resolution $=_p$ CDCL(π-D, FIRST-L)

Theorem 5.7. *For any fixed order π, the systems* CDCL(π-D), CDCL(π-D, FIRST-L) *and π-trail resolution are p-equivalent.*

Proof. Let Π be a π-trail resolution refutation of a contradictory CNF τ. We simulate Π step-by-step in CDCL(π-D, FIRST-L) by directly deriving each clause in Π. Suppose we have arrived at a state $(\mathbb{C}, \Lambda)$, where $\mathbb{C}$ contains both premises in the inference

$$\frac{C \vee x_i^a \qquad D \vee x_i^{1-a} \qquad t}{C \vee D}, \tag{5.17}$$

as well as all preceding clauses, and assume that all variables in C appear before x_i in t. Let $t = [x_{j_1} \overset{*_1}{=} a_1, \ldots, x_{j_r} \overset{*_r}{=} a_r, x_i \overset{*}{=} a, \ldots]$ and (for ease of notation) $t_s \overset{\text{def}}{=} t[\leq s]$. To derive $C \vee D$, we first build the trail t_r; note that since t might be derived in Π using the Unit

Propagation rule, the sequence $j_1, \ldots, j_r$ need not necessarily be π-increasing.

We build the trail t_r simply by performing the corresponding actions in CDCL(π-D, FIRST-L) for decisions and unit propagations. By induction, assume that we have already built t_{s-1}, $s \leq r$. If $*_s = d$ then x_{j_s} is the smallest variable according to π that is not in t_{s-1}, so by definition $x_{j_s} \stackrel{d}{=} a_s \in D((\mathbb{C}, t_{s-1}))$. In the case of the Unit Propagation rule ($*_s = u$), there is a clause E in Π preceding (5.17) such that $E|_{t_{s-1}} = x_{s-1}^{a_{s-1}}$. Since $E \in \mathbb{C}$ by assumption, $x_{j_s} \stackrel{u}{=} a_{j_s} \in U((\mathbb{C}, t_{s-1}))$.

Next, we build $[t_r, x_i \stackrel{u}{=} a]$ from t_r (note that it is different from t_{r+1} if $* = d$), which is possible since $C \vee x_i^a \in \mathbb{C}$ by our assumption. Then we further extend $[t_r, x_i \stackrel{u}{=} a]$ by making decisions in π-ascending order on the remaining variables $\{x_1, ..., x_n\} \setminus (\mathrm{Var}(t_s) \cup \{x_i\})$ until $D \vee x_i^{1-a}$ becomes a conflict clause. Denote the resulting state by $S = (\mathbb{C}, t')$.

Since all assignments after x_i in t' are decisions, $D \vee x_i^{1-a} \in \mathbb{C}_{r+2}(S)$, in the notation of Definition 5.6. Therefore, $C \vee D \in \mathbb{C}_{r+1}(S)$, and hence $(C \vee D, \Lambda)$ is in AllowedActions(S) even in the presence of FIRST-L. Induction completes the simulation.

The other direction is more straightforward: π-trail resolution p-simulates CDCL(π-D) by design. Whenever a run arrives at a state $(\mathbb{C}, t)$, we infer in π-trail resolution all clauses $C \in \mathbb{C}$ as well as all prefixes of t, including t itself. More specifically, for a transition $(\mathbb{C}, t) \stackrel{A}{\Longrightarrow} (\mathbb{C}', t')$, if A is a decision action or a unit propagation action, then we can derive prefixes of t' using the Decision rule and the Unit propagation rule, respectively. If A is a learning action, then it suffices to make the following simple observation: by construction, for any $\gamma \in [|t|]$, the clauses in $\mathbb{C}_\gamma((\mathbb{C}, t))$ can be derived from clauses in $\mathbb{C}$ and $\mathbb{C}_{\gamma+1}((\mathbb{C}, t))$ using the Learning rule with the trail t.

It is easy to see that both simulations increase size by at most a multiplicative factor n. □

5.4.2 π-trail resolution $=_p$ resolution

It remains to prove that π-trail resolution simulates resolution. This is the interesting direction of Theorem 5.5 and follows from Theorem 5.8 below.

Throughout this section, assume that $\pi = \mathrm{id}$. We first introduce operators for *lifting* π-trail resolution proofs to include appearances of the literal x_1 and *deleting variables* from resolution refutations, both of which we use extensively in the proof of Theorem 5.8.

The lifting operator is primarily a bookkeeping mechanism for managing auxiliary appearances of the literal x_1 in proofs.

Definition 5.13. *Let ψ and τ be CNFs such that $x_1 \notin \mathrm{Var}(\psi)$ and for each $C \in \psi$, τ contains either C or $C \vee x_1$. For $C \in \psi$, define $\mathrm{Lift}_\tau(C)$ to be C if $C \in \tau$, and $C \vee x_1$ otherwise. For a π-trail resolution proof Π from ψ define $\mathrm{Lift}_\tau(\Pi)$ to be the π-trail resolution proof resulting from the following operations on Π.*

- *Add the derivation of $[x_1 \stackrel{d}{=} 0]$ by the Decision rule to the beginning of Π.*
- *Replace each trail t in Π with $[x_1 \stackrel{d}{=} 0, t]$.*
- *Replace each axiom A appearing in Π with $\mathrm{Lift}_\tau(A)$ and then let the added appearances of x_1 be naturally inherited throughout the clauses of Π.*

It is straightforward to verify that $\mathrm{Lift}_\tau(\Pi)$ is a π-trail resolution proof and if Π derives C from ψ then $\mathrm{Lift}_\tau(\Pi)$ derives C or $C \vee x_1$ from τ. Note also that this is only possible because x_1 is the smallest variable according to π and hence does not interfere with the Learning rule. In the proof of Theorem 5.8, we will want to construct Π but will only be able to derive clauses in τ, so we construct $\mathrm{Lift}_\tau(\Pi)$ instead and then manage the additional appearances of x_1.

The second operator, *variable deletion*, is an analog of restriction for sets of variables (as opposed to assignments). Let $S \subseteq V$ be a set of variables. For a clause C, let $\mathrm{Del}_S(C)$

denote the result of removing from C all literals whose underlying variables are in S. For a CNF τ, define $\mathrm{Del}_S(\tau) \stackrel{\text{def}}{=} \{\mathrm{Del}_S(C) : C \in \tau\} \setminus \{0\}$. Here we see the first interesting feature of variable deletion, namely that we ignore clauses that become 0 after removing variables from S. But, as we show below, if τ is contradictory and the subset S is proper then $\mathrm{Del}_S(\tau)$ is also contradictory. This is not true in general for $\tau|_\rho \setminus \{0\}$ of course.

The action of variable deletion on refutations will be described in Definition 5.14. It is presented as a (linear time) algorithm that operates on the underlying resolution graph as its input, by recursively changing edges and clauses while nodes keep their identity (although some may be deleted). This is similar to the approach we took in Section 5.3.1. In order to more easily keep the node structure fixed, the algorithm first produces a proof in the subsystem of resolution + weakening in which all applications of the weakening rule are dummy (that is, are of the form $\dfrac{C}{C}$). We call proofs in this system *generalized resolution proofs*. We further emphasize that variable deletion is defined only on connected refutations, as connectedness is necessary for the output to be a refutation (cf. Claim 5.4(1)). Consequently, we ensure in the proof of Theorem 5.8 that we only apply it to connected refutations.

In the following, recall $c_\Pi(v)$ denotes the corresponding clause at node v in a proof Π.

Definition 5.14. *Let Π be a **connected** resolution refutation of τ and let S be a **proper** subset of $\mathrm{Var}(\Pi)$. Let Γ be the generalized resolution refutation of $\mathrm{Del}_S(\tau)$ whose resolution graph is output by the algorithm below. The resolution refutation $\mathrm{Del}_S(\Pi)$ is the result of contracting dummy applications of the weakening rule in Γ.*

Deletion Algorithm

1. *For each axiom node v, set $c(v) \coloneqq \mathrm{Del}_S(c_\Pi(v))$. If $c(v)$ becomes 0 (that is, when $\mathrm{Var}(c_\Pi(v)) \subseteq S$), delete it.*

2. *Processing nodes in topological order, let v be a resolution node and let v_1, v_2 be its parents.*

(a) *If* both v_1 *and* v_2 *were previously deleted, delete* v *as well.*

(b) *If only one of them was deleted or none was deleted but* $c(v_1), c(v_2)$ *are no longer resolvable, then one of them, say,* $c(v_1)$ *is a subclause of* $\mathrm{Del}_S(c(v))$ *(we will see this in Claim 5.4). Set* $c(v) \coloneqq c(v_1)$*, and replace incoming edges with a dummy weakening edge from* v_1*.*

(c) *If both* v_1 *and* v_2 *survived and* $c(v_1), c(v_2)$ *are resolvable, set* $c(v) \coloneqq \mathit{Res}(c(v_1), c(v_2))$*.*

After processing the root v *of* Π*, output the current downward-closure of* v*.*

We claim that this algorithm is well-defined (that is, the condition in step 2b is always met) and that the root vertex v is not deleted and $c(v) = 0$ (that is, the algorithm produces a generalized resolution refutation of $\mathrm{Del}_S(\tau)$). Both statements are immediate corollaries of the following claim.

Claim 5.4.

1. *A vertex* v *is deleted if and only if for every axiom node* $w \in \mathit{dcl}_\Pi(v)$ *it holds that* $\mathrm{Var}(c_\Pi(v)) \subseteq S$*. In particular:*
   - *The root vertex is not deleted (recall that* Π *is connected);*
   - *If* v *is deleted then* $\mathrm{Var}(c_\Pi(v)) \subseteq S$*.*
2. *For every remaining vertex* v*,* $c(v)$ *is a subclause of* $\mathrm{Del}_S(c_\Pi(v))$*.*
3. *In the situation of step 2b, there indeed exists* v_i *such that* $c(v_i)$ *is a subclause of* $\mathrm{Del}_S(c_\Pi(v))$*.*

Proof. These are proved by induction, simultaneously with the construction. In the base case, axioms, the three items clearly hold. In the inductive step, we prove them by analyzing each case in Deletion Algorithm. The only interesting case is step 2b. If precisely one of

the two vertices (say, v_2) was deleted, then $\mathrm{Var}(c_\Pi(v_2)) \subseteq S$ by Claim 5.4(1) and hence $c_\Pi(v)$ was obtained by resolving on a variable x_i in S. Applying Claim 5.4(2) to the other parent v_1, we see that $c(v_1)$ is a subclause of $\mathrm{Del}_S(c_\Pi(v_1))$ which in turn is a subclause of $\mathrm{Del}_S(c_\Pi(v))$ since $x_i \in S$. Similarly, if both parents of v are alive but become non-resolvable, then by Claim 5.4(2) the resolved variable is no longer in one of the parents (say v_1) and $c(v_1)$ is a subclause of $\mathrm{Del}_S(c_\Pi(v))$. □

One key difference between variable deletion and restriction is that $\Pi|_\rho$ may be trivial, in the sense that it is a single empty clause, while $\mathrm{Del}_{\mathrm{Var}(\rho)}(\Pi)$ is not. As a simple example, consider the CNF $\{x_1, \overline{x_1} \vee x_2, \overline{x_2}\}$ and the refutation

$$\dfrac{\dfrac{x_1 \qquad \overline{x_1} \vee x_2}{x_2} \qquad \overline{x_2}}{0}$$

If $\rho = \{x_1 = 0\}$, then $\Pi|_\rho$ is trivial, whereas $\mathrm{Del}_{\{x_1\}}(\Pi)$ is

$$\dfrac{x_2 \qquad \overline{x_2}}{0}$$

The final property of $\mathrm{Del}_S(\Pi)$ is that its size can be characterized with respect to the relationship between Π and S. This allows us to "slough off" parts of the Π that we might have already seen before.

Lemma 5.3. *Let Π be a connected resolution refutation and let $S \subsetneq \mathrm{Var}(\Pi)$. Let t denote the number of resolution steps $Res(C, D)$ in Π on variables in S. Then*

$$|\mathrm{Del}_S(\Pi)| \leq |\Pi| - t.$$

Proof. By Claim 5.4(2), all remaining resolution steps 2c are on variables that do not belong to S. □

Remark 5.13. *(Restriction as intersection, deletion as projection.) If we view a clause C semantically as the set $C^{-1}(0) \subset \{0,1\}^n$, then the restriction operator (say by ρ) on any*

clause C means to take intersection with the subcube $\rho^{-1}(1)$: $C^{-1}(0) \to C^{-1}(0) \cap \rho^{-1}(1)$; while the deletion operator $\mathrm{Del}_S(\cdot)$ corresponds to the projection $\{0,1\}^n \to \{0,1\}^{S^c}$ induced on $C^{-1}(0)$.

We now have sufficient machinery to prove Theorem 5.8. As is sometimes useful, the simulation we define is more ambitious than necessary. Rather than outputting a refutation, it outputs a proof that derives all literals (as unit clauses) appearing in the input. The motivation for this is twofold. First, unit clauses make π-trail resolution significantly more powerful because they grant more control over the trails that can be derived. In particular, if all literals appearing in a refutation Π have been derived, then Π can be simulated in $n|\Pi|$ steps by directly simulating each resolution appearing in it. Second, in reference to the deletion operator, all clauses of $\mathrm{Del}_S(\tau)$ can be derived using clauses of τ and unit clauses x^0 and x^1 for $x \in S$.

Our simulation algorithm is based on the obvious restrict-and-branch method, by which one recurses on $\Pi|_{\{x_i=0\}}$ and $\Pi|_{\{x_i=1\}}$, lifts the resulting proofs to have axioms in τ, and then derives 0 (if it has not been derived already) by resolving the unit clauses x_i and $\overline{x_i}$. The clear issue with this approach is that we cannot afford to recurse on *both* restricted proofs: there are parts of Π that are "double counted" as a consequence of its DAG structure and the size may blow up. But recursing on just $\Pi|_{\{x_i=0\}}$ may ignore relevant parts of Π, namely those resolutions on variables not even appearing in $\Pi|_{\{x_i=0\}}$. This is the purpose of the deletion operator. The refutation $\mathrm{Del}_{\mathrm{Var}(\Pi|_{\{x_i=0\}})}(\Pi)$ is a refutation with resolutions that correspond to resolutions in Π but not in $\Pi|_{\{x_i=0\}}$, so we can recurse on it without worrying about this double counting issue. This can be iterated so that we eventually see all literals appearing in Π without considering a particular resolution more than once. So an incomplete but instructive outline of our algorithm is this: recurse on $\Pi|_{\{x_i=0\}}$ and lift the proof to axioms of τ, iterate the deletion operator to derive all literals appearing in Π with possible additional appearances of x_i, and then simulate $\Pi|_{\{x_i=1\}}$ directly to derive $\overline{x_i}$ and

remove all additional appearances of x_i.

Before we finally state and prove Theorem 5.8, we present two simple lemmas that are factored out of the proof to simplify its presentation. The first essentially states that a variable in a connected refutation must play a nontrivial role, which intuitively should be true if we want to derive its corresponding literals. The second tells us that once we can directly simulate a connected π-trail refutation, we can also directly simulate a proof of all its literals; this is essentially a stronger version of the observation in the previous paragraphs that is more suited to the goal of deriving all literals.

Lemma 5.4. *Let Π be a connected resolution refutation of τ such that $x \in \mathrm{Var}(\Pi)$ and let Π' be the downward closure of any appearance of 0 in $\Pi|_{\{x=a\}}$. Then there is a clause $C \in \tau$ that contains x^{1-a} and appears restricted in Π'.*

Proof. Suppose for contradiction that there is no such clause. Then all axioms in Π' are axioms in Π not containing the variable x, so in the standard definition of restriction no edges are contracted and $G(\Pi')$ is a downward-closed subgraph of $G(\Pi)$ with identical labels. Since Π is connected it has a unique appearance of 0 (otherwise, 0 would be the premise of some resolution step that is impossible). Therefore $\Pi' = \Pi$ which contradicts the fact that $x \in \mathrm{Var}(\Pi)$. □

Lemma 5.5. *For any connected resolution refutation Π of τ, there is a resolution proof from τ of size at most $|\Pi| + 2n^2$ that derives, as unit clauses, all literals of variables in $\mathrm{Var}(\Pi)$.*

Proof. It suffices to note that if literals of all variables in $\mathrm{Res}(C \vee x_i^0, D \vee x_i^1)$ have been derived as unit clauses, then there is a proof of size at most $2n$ that derives x_i^0 and x_i^1. This process can be repeated on clauses in Π in reverse topological order (skipping clauses for which x_i^0 and x_i^1 have already been derived). Connectedness guarantees that every clause appearing in Π (and hence every variable) is processed. □

Theorem 5.8. *There is a polynomial time algorithm that, given a connected resolution refutation* Π *of* τ*, outputs a* π*-trail proof of size* $O(n^2|\tau||\Pi|)$ *that derives, as unit clauses, all literals of variables in* $\mathrm{Var}(\Pi)$.

Proof. We present the algorithm Sim which is recursively called on derivations with fewer variables.

Simulation Algorithm (Sim)

1. If $|\mathrm{Var}(\Pi)| = 1$, then for some variable x_i, Π contains only a resolution of x_i and $\neg x_i$. In this case, output the axioms x_i and $\overline{x_i}$.

2. Assume without loss of generality that all variables appear in Π. Define Π^0 to be the downward closure of some appearance of 0 in $\Pi|_{\{x_1=0\}}$. Derive $\mathrm{Lift}_\tau(\mathsf{Sim}(\Pi^0))$ (note that $|\mathrm{Var}(\Pi^0)| < |\mathrm{Var}(\Pi)|$, which justifies the recursive call to Sim) and let $l_{y,a} \in \{y^a, y^a \vee x_1\}$ for $y \in \mathrm{Var}(\Pi^0)$ denote the lifted unit clauses appearing in it. Note that Π^0 might be trivial, in which case x_1 is an axiom in τ and the next step can be skipped.

3. If x_1 appears in any $l_{y,a}$ from the previous step, then derive $x_1 = \mathrm{Res}(l_{y,0}, l_{y,1})$. Otherwise, by Lemma 5.4, there is a clause $C \in \tau$ containing the literal x_1. Derive x_1 by consecutively resolving C with literals $\overline{\ell_{y,a}}$, for all $\ell_{y,a}$ in C. We note here that these are half-ordered resolutions and hence admissible in π-trail resolution, but we refrain from pointing this out in similar cases below.

4. Derive the clauses $\{C \circ^{x_1} x_1 : C \in \tau\}$.

   At this point we have derived a set of clauses τ^* such that for every clause C in

$$\psi \stackrel{\text{def}}{=} \mathrm{Del}_{\{x_1\}}(\tau) \cup \bigcup_{y \in \mathrm{Var}(\Pi^0)} \{y^0, y^1\},$$

the set τ^* contains either C or $C \vee x_1$.

5. Set $\mathcal{S} \coloneqq \mathrm{Var}(\Pi^0)$. While $\mathcal{S} \cup \{x_1\} \neq V$ perform the following procedure constructing a π-trail resolution proof from the set of axioms ψ. We maintain that at the start of each iteration, all unit clauses in $\bigcup_{y \in \mathcal{S}} \{y^0, y^1\}$ have been derived. Also, to make clear, the proof constructed in this step is **not** part of the output, but its lifted verison will be (in step 6).

   (a) Construct the clauses of $\mathrm{Del}_{\mathcal{S} \cup \{x_1\}}(\tau)$ by resolving each clause in $\mathrm{Del}_{\{x_1\}}(\tau)$ with the unit clauses x^a for $x \in \mathcal{S}$. Then build $\mathrm{Del}_{\mathcal{S} \cup \{x_1\}}(\Pi)$ using the deletion algorithm.

   (b) Assume without loss of generality that $\mathrm{Del}_{\mathcal{S} \cup \{x_1\}}(\Pi)$ is connected; otherwise, as usual, take the downward closure of any appearance of 0. Construct the proof $\mathsf{Sim}(\mathrm{Del}_{\mathcal{S} \cup \{x_1\}}(\Pi))$. (This is the other recursive call to Sim.)

   (c) Set $\mathcal{S} \coloneqq \mathcal{S} \cup \mathrm{Var}(\mathrm{Del}_{\mathcal{S} \cup \{x_1\}}(\Pi))$.

6. Since $\mathrm{Del}_{\mathcal{S} \cup \{x_1\}}(\Pi)$ is always nontrivial when $\mathcal{S} \cup \{x_1\} \neq V$ (this follows from the well-definedness of the Deletion operator, Claim 5.4), the previous step terminates. Call the resulting proof Υ; it is the union of the proofs from step 5 (Υ need not be connected), which derives from ψ all unit clauses x_i^a for $i \in [2, n]$. Derive the proof $\mathrm{Lift}_{\tau^*}(\Upsilon)$, where τ^* is the set of clauses in step 4. This proof derives (this time from τ) $l_{i,a} \in \{x_i^a, x_i^a \vee x_1\}$ for $i \in [2, n]$. It remains to derive $\overline{x_1}$.

7. For that purpose, it is now possible to build any trail (up to annotations) that extends $[x_1 \overset{d}{=} 0]$ by using the Unit Propagation Rule with the lifted unit clauses from the previous step. Therefore, we can simulate any resolution proof not containing the variable x_1 by directly simulating each resolution step. Do this to the resolution proof extending $\Pi|_{\{x_1=1\}}$ that derives all literals appearing in it (Lemma 5.5).

8. By Lemma 5.4, there is a clause $C \in \tau$ containing $\overline{x_1}$ that appears restricted in $\Pi|_{\{x_1=1\}}$. Derive $\overline{x_1}$ by resolving C with all new literals from the previous step, when possible.

9. Derive all remaining literals by resolving $l_{i,a}$ with $\overline{x_1}$ when necessary.

Let $f(n,m)$ and $s(n,m)$ be upper bounds on the running time of Sim and the size of π-trail proof output by Sim, respectively, when Sim is run on a proof containing at most n variables and whose size is at most m. Our primary focus is on understanding the contributions of step 2 and 5 since the algorithm is called recursively in these steps. Step 2 adds at most $s(n-1,|\Pi^0|)$ to $s(n,|\Pi|)$ and

$$f(n-1,|\Pi^0|) + O(n \cdot s(n-1,|\Pi|))$$

to $f(n,|\Pi|)$.

Suppose that step 5 iterates T (which is $\leq n$) times. For $i \in [T]$, define $\mathcal{S}^i$ to be the state of $\mathcal{S}$ before the i^{th} iteration and define Π^i to be $\mathrm{Del}_{\mathcal{S}^i \cup \{x_1\}}(\Pi)$. Then steps 5-6 contribute at most $\sum_{i=1}^{T} s(n-1,|\Pi^i|)$ to the size bound and

$$\sum_{i=1}^{T} f(n-1,|\Pi^i|) + O(n|\tau| \cdot |\Pi|)$$

to the running time bound.

The most important fact here is that, by Lemma 5.3, $\sum_{i=0}^{T} |\Pi^i| \leq |\Pi|$. This is because the sets $\mathrm{Var}(\Pi^i)$ for $i \in [0,T]$ are pairwise disjoint and so the resolutions in each proof Π^i correspond to unique resolutions in Π. Note the special case of Π^0, which uses the fact that restrictions, like variable deletion, have the property that all resolutions in the resulting proof correspond to resolutions in Π on the same variable.

The auxiliary operations performed throughout the algorithm (e.g., recreating trails by

adding assignments to x_1 at the start) are clearly $O(n|\tau| \cdot |\Pi|)$ that yields the bounds

$$s(n, |\Pi|) \leq \sum_{i=0}^{T} s(n-1, |\Pi^i|) + O(n|\tau| \cdot |\Pi|)$$

and

$$f(n, |\Pi|) \leq \sum_{i=0}^{T} f(n-1, |\Pi^i|) + O\left(\sum_{i=0}^{T} s(n-1, |\Pi^i|)\right) + O(n^2|\tau| \cdot |\Pi|).$$

By induction on n, first for s and then f, it follows that $s(n, \Pi) = O(n^2|\tau| \cdot |\Pi|)$ and $f(n, |\Pi|) = O(n^3|\tau| \cdot |\Pi|)$. □

5.5 Width lower bound

Our last piece of technical work is Theorem 5.4, which demonstrates the limitations of bounded width clause learning in the presence of the ordered decision strategy. Using the connection to π-trail resolution from the previous section, Theorem 5.4 follows from a general width lower bound for the latter. Some of the formulas to which this bound applies have constant width (that implies polynomial size) refutations and hence, by Theorem 5.3, automatically have polynomial size π-trail refutations. Thus this result also shows that there is no size-width relationship for π-trail resolution like the one for resolution proved by Ben-Sasson and Wigderson [21].

Say that a clause C is *almost-k-small* with respect to π if $|\mathrm{Var}(C) \setminus \mathrm{Var}_\pi^k| \leq 1$, and that a trail $t = [x_{i_1} \overset{*_1}{=} a_1, \ldots, x_{i_r} \overset{*_r}{=} a_r]$ is *k-trivial* if for $s \overset{\text{def}}{=} \min(r, k)$, all assignments in $t[\leq s]$ are decisions on variables in Var_π^k in π-increasing order: $t[\leq s] = [x_{\pi(1)} \overset{d}{=} a_1, \ldots, x_{\pi(s)} \overset{d}{=} a_s]$.

Definition 5.15. *The order π is k-robust for a contradictory CNF τ if for any restriction ρ such that $|\mathrm{Var}(\rho) \setminus \mathrm{Var}_\pi^k| \leq 1$, the following properties hold:*

- *the formula $\tau|_\rho$ is minimally unsatisfiable, i.e., all strict subsets of $\tau|_\rho$ are satisfiable;*

- *for all $i \in [n]$, if $(x_i = a) \in \rho$ then there is a clause in τ that appears restricted in $\tau|_\rho$, i.e., it is not satisfied by ρ and contains the literal x_i^{1-a}.*

Example 4. *For a CNF τ_n, the r-ary parity substitution of τ_n, denoted by $\tau_n[\oplus_r]$, is the formula in which for all $i \in [n]$, each variable x_i is replaced with $\bigoplus_{j=1}^{r} y_{i,j}$ where the variables $y_{i,1}, y_{i,2}, \ldots, y_{i,r}$ are new and distinct. As described, $\tau_n[\oplus_r]$ is technically not a CNF, but its encoding as a CNF is straightforward and natural; see [84] for full details. It is also straightforward to check that whenever τ_n is minimally unsatisfiable and contains all variables $x_1, \ldots, x_n$, the order π on the variables of $\tau_n[\oplus_r]$ given by*

$$\begin{aligned}
&\pi(y_{1,1}) < \pi(y_{2,1}) < \cdots < \pi(y_{n,1}) < \\
&\pi(y_{1,2}) < \pi(y_{2,2}) < \cdots < \pi(y_{n,2}) < \cdots < \\
&\pi(y_{1,r}) < \pi(y_{2,r}) < \cdots < \pi(y_{n,r})
\end{aligned}$$

is $((r-2)n)$-robust. In fact, this readily follows from the observation that any restriction ρ that satisfies $|\mathrm{Var}(\rho) \backslash \mathrm{Var}_\pi^{(r-2)n}| \leq 1$ must leave unassigned at least one variable in each group $\{y_{i,1}, \ldots, y_{i,r}\}$.

The following theorem shows that robustness implies large width in π-trail resolution.

Theorem 5.9. *Let τ be a contradictory CNF formula and let π be a w-robust order for τ. Then the width of any π-trail refutation of τ is at least w.*

Proof. Assume without loss of generality that $\pi = \mathrm{id}$. Let Π be a π-trail refutation of τ and let C be the first almost-w-small clause appearing in Π. We will actually prove that $\mathrm{Var}_\pi^w \subseteq \mathrm{Var}(C)$.

First, we claim that all trails that appear before C in Π are $(w+1)$-trivial. Suppose otherwise and let t be the first trail in Π that is not. Since Π contains all prefixes of t, and all such prefixes precede t, it follows that t is of the form $[t', x_i \overset{u}{=} a]$, where $t' = [x_1 \overset{d}{=} a_1, x_2 \overset{d}{=}$

$a_2 \ldots, x_j \stackrel{d}{=} a_j]$, $i \geq j+2$ and $j \leq w$. Suppose that t follows from t' by the Unit Propagation rule with the clause D. This means $D|_{t'}$ is a unit clause, which implies D is almost-w-small, contradicting the assumption that C is the first almost-w-small clause in Π.

It then follows that all resolutions (corresponding to applications of the Learning rule) that appear before C are on variables not in Var_π^{w+1}. Indeed, suppose that the inference

$$\frac{D \vee x_i^a \qquad E \vee \overline{x_i^a} \qquad t}{D \vee E}$$

appears before C in Π. By the claim in the previous paragraph, t is $(w+1)$-trivial. Therefore if $x_i \in \mathrm{Var}_\pi^{w+1}$, then it is actually assigned in $t[\leq w+1]$ and so are all variables appearing in D. This implies D is almost-w-small, contradicting the assumption that C is the first such clause.

Finally let Π^* be the *resolution refutation* corresponding to Π; that is, the refutation constructed from Π by ignoring all trails. Let Γ be the connected subproof of C in Π^* on the downward closure of C. By the remark in the previous paragraph, all resolutions in Γ are on variables not in Var_π^{w+1}. Lastly, let ρ be any restriction with the domain $\mathrm{Var}_\pi^w \cup \mathrm{Var}(C)$ that falsifies C, so that $\Gamma|_\rho$ is a refutation of $\tau|_\rho$. By the first property in the definition of robustness, $\tau|_\rho$ is minimal, which implies that all clauses in $\tau|_\rho$ appear as axioms of $\Gamma|_\rho$. Therefore, there are paths from these clauses (unrestricted) to C in Γ. By the second property of robustness, each variable in Var_π^w appears in at least one of these clauses. Since all resolutions in Γ are on variables not in Var_π^{w+1}, it follows that $\mathrm{Var}_\pi^w \subseteq \mathrm{Var}(C)$. □

Finally, we prove Theorem 5.4, which is restated here for convenience. The proof is a simple variation of the one above (we only have to make sure that the variables in Var_π^w appear in a *learned* clause).

Theorem 5.10. *(Theorem 5.4 restated) For any fixed order π on the variables and every $\epsilon > 0$ there exist contradictory CNFs τ_n with $w(\tau_n \vdash 0) = O(1)$ not provable in* CDCL(π-D,

WIDTH-$(1-\epsilon)n$).

Proof. The formula used here is $\mathrm{Ind}_m[\oplus_r]$ where Ind_m is the *Induction principle*

$$x_1 \wedge \bigwedge_{i=1}^{m-1} (\overline{x_i} \vee x_{i+1}) \wedge \overline{x_m},$$

and r will be chosen as a sufficiently large constant. The natural resolution refutation of this formula has width $O(r)$.

Fix $\epsilon > 0$. Let R be a successful run in CDCL(π-D) on $\mathrm{Ind}_m[\oplus_r]$ and let Π be the natural π-trail simulation of this run given by Theorem 5.7. We begin with some observations about Π that are easily verified by examining the proof of Theorem 5.7. First, all clauses learned in R are derived exactly in Π, in the order they appear in R. Second, for any learning step (C, t') in R from the state $(\mathbb{C}, t)$, the proof Π contains the connected subproof of C from $\mathbb{C}$ corresponding exactly to the sequence of resolutions used to learn C (Lemma 5.1). Furthermore, the trail t appears before this subproof in Π.

Let $w = (r-2)m$ and let D be the first almost-w-small clause in Π. Similar to the proof of Theorem 5.9, it follows that $\mathrm{Var}_\pi^w \subseteq \mathrm{Var}(D)$ and all trails appearing before D in Π are $(w+1)$-trivial. If D is not a learned clause, then it appears in the subproof of some learned clause C. Suppose that C follows from the state $(\mathbb{C}, t)$ in R. As is made clear in Lemma 5.1, all resolutions in the subproof of C are on variables whose assignments are unit propagations in t. Since t appears before D, it is $(w+1)$-trivial, so none of the variables in Var_π^w are resolved on to derive C. This implies all variables in Var_π^w are inherited in C from D.

The result follows by taking $r > 2/\epsilon$ so that $(r-2)m > (1-\epsilon)rm$. □

REFERENCES

[1] Kwangjun Ahn, Dhruv Medarametla, and Aaron Potechin. Graph matrices: norm bounds and applications. *arXiv preprint arXiv:1604.03423*, 2016.

[2] Michael Alekhnovich, Jan Johannsen, Toniann Pitassi, and Alasdair Urquhart. An exponential separation between regular and general resolution. In *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, pages 448–456. ACM, 2002.

[3] Noga Alon, Michael Krivelevich, and Benny Sudakov. Finding a large hidden clique in a random graph. *Random Structures & Algorithms*, 13(3-4):457–466, 1998.

[4] Fadi A. Aloul, Igor L. Markov, and Karem A. Sakallah. MINCE: A Static Global Variable-Ordering for SAT and BDD. In *International Workshop on Logic and Synthesis*, pages 1167–1172, 2001.

[5] Fadi A. Aloul, Igor L. Markov, and Karem A. Sakallah. FORCE: A Fast & Easy-to-Implement Variable-Ordering Heuristic. In *Proceedings of the 13th ACM Great Lakes symposium on VLSI*, pages 116–119. ACM, 2003.

[6] Benny Applebaum, Boaz Barak, and Avi Wigderson. Public-key cryptography from different assumptions. In *Proceedings of the forty-second ACM symposium on Theory of computing*, pages 171–180, 2010.

[7] Sanjeev Arora, Boaz Barak, Markus Brunnermeier, and Rong Ge. Computational complexity and information asymmetry in financial products. *Communications of the ACM*, 54(5):101–107, 2011.

[8] Albert Atserias, Ilario Bonacina, Susanna F. de Rezende, Massimo Lauria, Jakob Nordström, and Alexander Razborov. Clique is hard on average for regular resolution. *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 866–877, 2018.

[9] Albert Atserias, Johannes Klaus Fichte, and Marc Thurley. Clause-Learning Algorithms with Many Restarts and Bounded-Width Resolution. *Journal of Artificial Intelligence Research*, 40:353–373, 2011.

[10] Gilles Audemard and Laurent Simon. Predicting learnt clauses quality in modern SAT solvers. In *IJCAI*, volume 9, pages 399–404, 2009.

[11] Boaz Barak, Fernando GSL Brandao, Aram W Harrow, Jonathan Kelner, David Steurer, and Yuan Zhou. Hypercontractivity, sum-of-squares proofs, and their applications. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 307–326, 2012.

[12] Boaz Barak, Siu On Chan, and Pravesh K Kothari. Sum of squares lower bounds from pairwise independence. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 97–106, 2015.

[13] Boaz Barak, Samuel Hopkins, Jonathan Kelner, Pravesh K Kothari, Ankur Moitra, and Aaron Potechin. A nearly tight sum-of-squares lower bound for the planted clique problem. *SIAM Journal on Computing*, 48(2):687–735, 2019.

[14] Boaz Barak and David Steurer. Sum-of-squares proofs and the quest toward optimal algorithms. In *Proceedings of International Congress of Mathematicians (ICM)*, 2014.

[15] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on hilbert's nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society*, 3(1):1–26, 1996.

[16] Paul Beame, Russell Impagliazzo, and Ashish Sabharwal. The resolution complexity of independent sets and vertex covers in random graphs. *computational complexity*, 16(3):245–297, 2007.

[17] Paul Beame, Richard Karp, Toniann Pitassi, and Michael Saks. The efficiency of resolution and Davis–Putnam procedures. *SIAM Journal on Computing*, 31(4):1048–1075, 2002.

[18] Paul Beame, Henry Kautz, and Ashish Sabharwal. Towards Understanding and Harnessing the Potential of Clause Learning. *Journal of Artificial Intelligence Research*, 22:319–351, 2004.

[19] Paul Beame and Ashish Sabharwal. Non-Restarting SAT Solvers with Simple Preprocessing Can Efficiently Simulate Resolution. In *Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence*, pages 2608–2615, 2014.

[20] Eli Ben-Sasson and Jan Johannsen. Lower Bounds for Width-Restricted Clause Learning on Small Width Formulas. In *Theory and Applications of Satisfiability Testing – SAT 2010*, pages 16–29. Springer, 2010.

[21] Eli Ben-Sasson and Avi Wigderson. Short Proofs Are Narrow – Resolution Made Simple. *Journal of the ACM*, 48(2):149–169, 2001.

[22] Siavosh Benabbas, Konstantinos Georgiou, Avner Magen, and Madhur Tulsiani. Sdp gaps from pairwise independence. *Theory of Computing*, 8(1):269–289, 2012.

[23] Quentin Berthet and Philippe Rigollet. Complexity theoretic lower bounds for sparse principal component detection. In *Conference on Learning Theory*, pages 1046–1066. PMLR, 2013.

[24] Olaf Beyersdorff, Nicola Galesi, and Massimo Lauria. Parameterized complexity of DPLL search procedures. *ACM Transactions on Computational Logic (TOCL)*, 14(3):20, 2013.

[25] Armin Biere and Andreas Fröhlich. Evaluating CDCL restart schemes. In *Proceedings POS-15. Sixth Pragmatics of SAT workshop*, 2015.

[26] Armin Biere, Marijn Heule, Hans van Maaren, and Toby Walsh, editors. *Handbook of Satisfiability*, volume 336 of *Frontiers in Artificial Intelligence and Applications*. IOS Press, 2021.

[27] Archie Blake. *Canonical expressions in boolean algebra*. PhD thesis, University of Chicago, 1938.

[28] Beate Bollig, Martin Löbbing, Martin Sauerhoff, and Ingo Wegener. On the complexity of the hidden weighted bit function for various BDD models. *RAIRO-Theoretical Informatics and Applications*, 33(2):103–115, 1999.

[29] Béla Bollobás and Paul Erdös. Cliques in random graphs. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 80, pages 419–427. Cambridge University Press, 1976.

[30] Ilario Bonacina and Navid Talebanfard. Strong eth and resolution via games and the multiplicity of strategies. *Algorithmica*, 79(1):29–41, 2017.

[31] Maria Luisa Bonet, Sam Buss, and Jan Johannsen. Improved Separations of Regular Resolution from Clause Learning Proof Systems. *Journal of Artificial Intelligence Research*, 49:669–703, 2014.

[32] Maria Luisa Bonet, Juan Luis Esteban, Nicola Galesi, and Jan Johannsen. On the Relative Complexity of Resolution Refinements and Cutting Planes Proof Systems. *SIAM Journal on Computing*, 30(5):1462–1484, 2000.

[33] Maria Luisa Bonet and Katherin St. John. Efficiently calculating evolutionary tree measures using SAT. In *International Conference on Theory and Applications of Satisfiability Testing*, pages 4–17. Springer, 2009.

[34] Samuel R Buss. *Bounded arithmetic*. Princeton University, 1985.

[35] Samuel R. Buss, Jan Hoffmann, and Jan Johannsen. Resolution Trees with Lemmas: Resolution Refinements that Characterize DLL-Algorithms with Clause Learning. *Logical Methods in Computer Science*, 4(4), 2008.

[36] Samuel R. Buss and Leszek Aleksander Kołodziejczyk. Small Stone in Pool. *Logical Methods in Computer Science*, 10(2), 2014.

[37] Samuel R. Buss and Jakob Nordström. Chapter 7. proof complexity and sat solving. 2021.

[38] Eldan Cohen, Guoyu Huang, and Christopher J. Beck. (I can get) satisfaction: Preference-based scheduling for concert-goers at multi-venue music festivals. In *International Conference on Theory and Applications of Satisfiability Testing*, pages 147–163. Springer, 2017.

[39] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, 1979.

[40] Martin Davis, George Logemann, and Donald Loveland. A machine program for theorem-proving. *Communications of the ACM*, 5(7):394–397, 1962.

[41] Martin Davis and Hilary Putnam. A computing procedure for quantification theory. *Journal of the ACM (JACM)*, 7(3):201–215, 1960.

[42] P Delsarte. An algebraic approach to association schemes of coding theory, phillips j, 1973.

[43] Yash Deshpande and Andrea Montanari. Improved sum-of-squares lower bounds for hidden clique and hidden submatrix problems. In *Conference on Learning Theory*, pages 523–562. PMLR, 2015.

[44] Jan Elffers, Jan Johannsen, Massimo Lauria, Thomas Magnard, Jakob Nordström, and Marc Vinyals. Trade-offs Between Time and Memory in a Tighter Model of CDCL SAT Solvers. In *Theory and Applications of Satisfiability Testing – SAT 2016*, pages 160–176. Springer, 2016.

[45] Fernando Escalante. Schnittverbände in graphen. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, volume 38, pages 199–220. Springer, 1972.

[46] Uriel Feige and Robert Krauthgamer. Finding and certifying a large hidden clique in a semirandom graph. *Random Structures & Algorithms*, 16(2):195–208, 2000.

[47] Uriel Feige and Robert Krauthgamer. The probable value of the lovász–schrijver relaxations for maximum independent set. *SIAM Journal on Computing*, 32(2):345–370, 2003.

[48] Ankit Garg, Mika Göös, Pritish Kamath, and Dmitry Sokolov. Monotone circuit lower bounds from resolution. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 902–911. ACM, 2018.

[49] Mika Göös, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for bpp. *SIAM Journal on Computing*, 49(4):FOCS17–441, 2020.

[50] Dima Grigoriev. Linear lower bound on degrees of positivstellensatz calculus proofs for the parity. *Theoretical Computer Science*, 259(1-2):613–622, 2001.

[51] Dima Grigoriev and Nicolai Vorobjov. Complexity of null-and positivstellensatz proofs. *Annals of Pure and Applied Logic*, 113(1-3):153–160, 2001.

[52] Aarti Gupta, Malay Ganai, and Chao Wang. SAT-based verification methods and applications in hardware verification. *Formal Methods for Hardware Verification*, pages 108–143, 2006.

[53] Mohammad T Hajiaghayi, Rohit Khandekar, and Guy Kortsarz. Fixed parameter inapproximability for clique and setcover in time super-exponential in opt. *arXiv preprint arXiv:1310.2711*, 2013.

[54] Armin Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[55] Johan Hastad. Clique is hard to approximate within $n^{1-\epsilon}$. In *Proceedings of 37th Conference on Foundations of Computer Science*, pages 627–636. IEEE, 1996.

[56] Philipp Hertel, Fahiem Bacchus, Toniann Pitassi, and Allen Van Gelder. Clause Learning Can Effectively P-Simulate General Propositional Resolution. In *Proceedings of the Twenty-Third AAAI Conference on Artificial Intelligence*, pages 283–290, 2008.

[57] Samuel B Hopkins, Pravesh Kothari, Aaron Henry Potechin, Prasad Raghavendra, and Tselil Schramm. On the integrality gap of degree-4 sum of squares for planted clique. *ACM Transactions on Algorithms (TALG)*, 14(3):1–31, 2018.

[58] Samuel B Hopkins, Pravesh K Kothari, and Aaron Potechin. Sos and planted clique: Tight analysis of mpw moments at all degrees and an optimal lower bound at degree four. *arXiv preprint arXiv:1507.05230*, 2015.

[59] Samuel B Hopkins, Pravesh K Kothari, Aaron Potechin, Prasad Raghavendra, Tselil Schramm, and David Steurer. The power of sum-of-squares for detecting hidden structures. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 720–731. IEEE, 2017.

[60] Trinh Huynh and Jakob Nordstrom. On the virtue of succinct proofs: Amplifying communication complexity hardness to time-space trade-offs in proof complexity. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 233–248, 2012.

[61] Franjo Ivančić, Zijiang Yang, Malay K. Ganai, Aarti Gupta, and Pranav Ashar. Efficient SAT-based bounded model checking for software verification. *Theoretical Computer Science*, 404(3):256–274, 2008.

[62] Mark Jerrum. Large cliques elude the metropolis process. *Random Structures & Algorithms*, 3(4):347–359, 1992.

[63] Chris Jones, Aaron Potechin, Goutham Rajendran, Madhur Tulsiani, and Jeff Xu. Sum-of-squares lower bounds for sparse independent set. *arXiv preprint arXiv:2111.09250*, 2021.

[64] Roberto J. Bayardo Jr. and Robert C. Schrag. Using CSP look-back techniques to solve real-world SAT instances. In *AAAI/IAAI*, pages 203–208, 1997.

[65] Pravesh Kothari, Ryan O'Donnell, and Tselil Schramm. Sos lower bounds with hard constraints: think global, act local. *arXiv preprint arXiv:1809.01207*, 2018.

[66] Pravesh K. Kothari and Peter Manohar. A Stress-Free Sum-Of-Squares Lower Bound for Coloring. In *36th Computational Complexity Conference (CCC 2021)*, volume 200 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 23:1–23:21, 2021.

[67] Pravesh K Kothari and Ruta Mehta. Sum-of-squares meets nash: Optimal lower bounds for finding any equilibrium. *arXiv preprint arXiv:1806.09426*, 2018.

[68] Pravesh K Kothari, Ryuhei Mori, Ryan O'Donnell, and David Witmer. Sum of squares lower bounds for refuting any csp. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 132–145, 2017.

[69] Jan Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997.

[70] Jan Krajicek, Jan Krajíček, et al. *Bounded arithmetic, propositional logic and complexity theory*. Cambridge University Press, 1995.

[71] Luděk Kučera. Expected complexity of graph partitioning problems. *Discrete Applied Mathematics*, 57(2-3):193–212, 1995.

[72] Jean B Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on optimization*, 11(3):796–817, 2001.

[73] Massimo Lauria, Pavel Pudlák, Vojtěch Rödl, and Neil Thapen. The complexity of proving that a graph is ramsey. *Combinatorica*, 37(2):253–268, 2017.

[74] Chunxiao Li, Noah Fleming, Marc Vinyals, Toniann Pitassi, and Vijay Ganesh. Towards a Complexity-theoretic Understanding of Restarts in SAT solvers. In *Theory and Applications of Satisfiability Testing – SAT 2020*, pages 233–249. Springer, 2020.

[75] Jia Hui Liang, Vijay Ganesh, Ed Zulkoski, Atulan Zaman, and Krzysztof Czarnecki. Understanding VSIDS branching heuristics in conflict-driven clause-learning SAT solvers. In *Haifa Verification Conference*, pages 225–241. Springer, 2015.

[76] João P. Marques-Silva. The impact of branching heuristics in propositional satisfiability algorithms. *Progress in Artificial Intelligence*, pages 850–850, 1999.

[77] João P. Marques-Silva and Karem A. Sakallah. GRASP: A search algorithm for propositional satisfiability. *IEEE Transactions on Computers*, 48(5):506–521, 1999.

[78] Ralph Eric McGregor. *Automated theorem Proving using SAT*. Clarkson University, 2011.

[79] Raghu Meka, Aaron Potechin, and Avi Wigderson. Sum-of-squares lower bounds for planted clique. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 87–96, 2015.

[80] Matthew W. Moskewicz, Conor F. Madigan, Ying Zhao, Lintao Zhang, and Sharad Malik. Chaff: Engineering an efficient SAT solver. In *Proceedings of the 38th Annual Design Automation Conference*, pages 530–535. ACM, 2001.

[81] Nathan Mull, Shuo Pang, and Alexander Razborov. On cdcl-based proof systems with the ordered decision strategy. In *International Conference on Theory and Applications of Satisfiability Testing*, pages 149–165. Springer, 2020.

[82] Jaroslav Nešetřil and Svatopluk Poljak. On the complexity of the subgraph problem. *Commentationes Mathematicae Universitatis Carolinae*, 026,2, 1985.

[83] Robert Nieuwenhuis, Albert Oliveras, and Cesare Tinelli. Solving SAT and SAT Modulo Theories: From an Abstract Davis–Putnam–Logemann–Loveland Procedure to DPLL(T). *Journal of the ACM*, 53(6):937–977, 2006.

[84] Jakob Nordström. Pebble games, proof complexity, and time-space trade-offs. *Logical Methods in Computer Science*, 9, 2013.

[85] Ryan O'Donnell. Sos is not obviously automatizable, even approximately. In *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.

[86] Shuo Pang. Large clique is hard on average for resolution. In *Computer Science – Theory and Applications*, pages 361–380. Springer International Publishing, 2021.

[87] Shuo Pang. Sos lower bound for exact planted clique. In *36th Computational Complexity Conference (CCC 2021)*, pages 26:1–26:63. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2021.

[88] Pablo A Parrilo. *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization*. PhD thesis, California Institute of Technology, 2000.

[89] Pavel A Pevzner, Sing-Hoi Sze, et al. Combinatorial approaches to finding subtle signals in dna sequences. In *ISMB*, volume 8, pages 269–278, 2000.

[90] Knot Pipatsrisawat and Adnan Darwiche. On the power of clause-learning SAT solvers as resolution engines. *Artificial Intelligence*, 175(2):512–525, 2011.

[91] Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *The Journal of Symbolic Logic*, 62(3):981–998, 1997.

[92] Pavel Pudlák. Proofs as games. *The American Mathematical Monthly*, 107(6):541–550, 2000.

[93] Prasad Raghavendra and Benjamin Weitz. On the bit complexity of sum-of-squares proofs. *arXiv preprint arXiv:1702.05139*, 2017.

[94] Ran Raz and Pierre McKenzie. Separation of the monotone nc hierarchy. In *Proceedings 38th Annual Symposium on Foundations of Computer Science*, pages 234–243. IEEE, 1997.

[95] Alexander Razborov. Lower bounds on the monotone complexity of some boolean functions. *English translation in Soviet Math. Doklady*, 31:354–357, 1985.

[96] Alexander A Razborov. Unprovability of lower bounds on circuit size in certain fragments of bounded arithmetic. *Izvestiya: mathematics*, 59(1):205, 1995.

[97] Alexander A Razborov. Proof complexity of pigeonhole principles. In *International Conference on Developments in Language Theory*, pages 100–116. Springer, 2001.

[98] John Alan Robinson. A machine-oriented logic based on the resolution principle. *Journal of the ACM (JACM)*, 12(1):23–41, 1965.

[99] Benjamin Rossman. On the constant-depth complexity of k-clique. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 721–730. ACM, 2008.

[100] Grant Schoenebeck. Linear level lasserre lower bounds for certain k-csps. In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 593–602. IEEE, 2008.

[101] Naum Z Shor. Class of global minimum bounds of polynomial functions. *Cybernetics*, 23(6):731–734, 1987.

[102] Gunnar Stålmarck. Short resolution proofs for a sequence of tricky formulas. *Acta Informatica*, 33(3):277–280, 1996.

[103] Evgenij E Tyrtyshnikov. How bad are hankel matrices? *Numerische Mathematik*, 67(2):261–269, 1994.

[104] Allen Van Gelder. Pool Resolution and Its Relation to Regular Resolution and DPLL with Clause Learning. In *Logic for Programming, Artificial Intelligence, and Reasoning – LPAR 2005*, pages 580–594. Springer, 2005.

[105] Virginia Vassilevska. Efficient algorithms for clique problems. *Information Processing Letters*, 109(4):254–257, 2009.

[106] Marc Vinyals. Hard Examples for Common Variable Decision Heuristics. In *Proceedings of the 34th AAAI Conference on Artificial Intelligence (AAAI'20)*, 2020.

[107] Marc Vinyals, Jan Elffers, Jan Johannsen, and Jakob Nordström. Simplified and improved separations between regular and general resolution by lifting. In *International Conference on Theory and Applications of Satisfiability Testing*, pages 182–200. Springer, 2020.

[108] David Zuckerman. Linear degree extractors and the inapproximability of max clique and chromatic number. In *Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, pages 681–690. ACM, 2006.