Electronic Colloquium on Computational Complexity, Report No. 68 (2019)

LARGE CLIQUE IS HARD ON AVERAGE FOR RESOLUTION

SHUO PANG

Abstract. We prove resolution lower bounds for k-Clique on the Erdos-Renyi random graph $G(n, n^{\frac{-2\xi}{k-1}})$ (where $\xi > 1$ is constant). First we show for $k = n^{c_0}$, $c_0 \in (0, 1/3)$, an $\exp(\Omega(n^{(1-\epsilon)c_0}))$ average lower bound on resolution where ϵ is arbitrary constant.

We then propose the model of a-irregular resolution. Extended from regular resolution, this model is interesting in that the power of general-over-regular resolution from all *known* exponential separations is below it. We prove an $n^{\Omega(k)}$ average lower bound of k-Clique for this model, for *any* $k < n^{1/3-\Omega(1)}$.

1. Introduction

The *Clique problem*, given input (G, k), asks whether a graph G contains a clique of size k. As one of the fundamental NP-complete problems ([19]), its computational hardness has been intensively studied in both algorithmic and lower bound worlds ([22, 24, 15, 31, 27, 30, 13]). In computational complexity, the case $k = n^{\Omega(1)}$ (where n is the number of vertices in G) is complete as other cases poly-time reduce to it by a simple padding.

Translated to proof complexity, the problem becomes about proving (the CNF translation of) the nonexistence of k-cliques in a k-clique-free graph. Instead of particular graphs, a more interesting setting is where the underlying graph is *random*, and we ask whether the CNF is hard on average (=*w.h.p.*, with high probability). This somewhat reflects the experience in complexity world that, random input of the problem is hard, and we want to know what "quasi-random[1]" feature makes it hard—here, it is in the sense of why familiar proof systems fail to efficiently prove "G is k-clique-free". To make sense, the graph should be k-clique-free w.h.p. (as there is no short proof for a wrong claim). The most studied such setting is the *Erdos-Renyi random graph* $G(n, p)$ with p below the so-called *threshold* (take $p = n^{-\frac{2\xi}{k-1}}$, with $\xi > 1$ constant for instance). Lower bounds in this setting are known for some proof systems. For example there are degree bounds on SOS ([20, 16, 3], for the *planted k-clique* version), and size lower

University of Chicago, Department of Mathematics, spang@math.uchicago.edu.

[1]This strict term is defined by density conditions; we borrow it here only to mean "random-like".

ISSN 1433-8092

bounds on subsystems of resolution like tree-like resolution ([7]) and regular resolution ([2]). But the problem remains widely open, in particular, for resolution. In general, the question of lower bounds of CNF instances for resolution is made more interesting by the fact that nearly all temporary algorithms (usually called *SAT-solvers*) for CNF satisfiability can be formulated within this system ([8, 4, 17, 21]).

As is usual for weak systems, here the encoding matters. There are two natural CNF encodings from the literature, which are denoted as $Clique(G, k)$ and $Clique_{block}(G, k)$ (Section 2). Roughly speaking, the two differ by whether allowing permutations of the k vertices of the clique. Among them, $Clique_{block}(G, k)$ is the one prohibiting such permutations, and it is the "stronger" one (*i.e.*, its lower bound easily implies that for $Clique(G, k)$). With Theorem 2.1, we will see that actually it is the proper encoding, in capturing hardness of k-Clique from the underlying graph G.

Our results. Our first result is for $k = n^{\Omega(1)}$, the k-clique problem is hard on average for resolution. More precisely, we prove an $\exp(k^{1-\epsilon})$ lower bound ($\epsilon > 0$ is arbitrary constant) for $Clique_{block}(n, k)$, for $k = n^{c_0}$, $c_0 \in (0, 1/3)$, on the Erdos-Renyi random graph (Corollary 3.1). The bound applies to graphs with some certain "quasi-random" combinatorial property (*neighbor-denseness*).

Our second result, Theorem 4.1, is an $n^{\Omega(k)}$-type average lower bound (for the same CNF but *any* k this time), for the model which we call *a-irregular resolution*, $a \in (0, 1)$, which sits between regular and general resolution. The significance of such model is that, as we will see in Section 4.1, it captures the known power of general-over-regular resolutions. *I.e.*, for known CNFs exponentially separating the two, they have short resolution proofs actually in this model for small a (Remark 4.1, 4.2, 4.3). In other words, the model is not less powerful than general resolution from the view of current knowledge. Therefore, for a target CNF, particularly those whose hardness for regular resolution is known (e.g., the situation of k-Clique and n^k-type lower bound), testing hardness in this model seems legitimate, and helps realize if we are faced with some "novel power" of general-over-regular resolution.

We now describe this model (loosely). It allows "irregularities", but requires them to be structured in the following way: viewing a resolution as a top-down DAG,

> *If a clause P has large (block-) width, then (blocks of) variables irregularly resolved after P are not too many.*

Here, both *large* and *many* are characterized by parameter $a \in (0, 1)$; the word *block* is used as the model assumes a variable partition in input (Definition 4.2). In Section 4.1, we show how this model captures the power of general-over-regular resolution; with the

concept of *blcok-width* (which is defined for any CNF) we also ask there, if it is possible to generalize the well-known width-size relation.

Proof method. The proofs are formulated in the top-down view of resolution (see Section 2. See also the paragraph below the next, for the possibility of using restrictions instead). We formalize properties of random graph first. Then we design the answering strategy based on these properties, and analyze in the classical bottleneck counting framework ([14]). For the first result, the strategy flips random coins *before* the process starts, then it forces the process to recover clauses at which, significant amount of information of the random coins is released. The idea is to branch to clause that is not "dead" but in "danger" (*i.e.*, no axiom is violated, but for many $i \in [k]$, pigeon i has few vertices to go for maintaining a clique; see Definition 3.2).

For the second result, suppose the resolution is Γ. The answering strategy is similarly to force the process to *any* clause P with similar tension as above, due to which: 1. The limitation of a-irregularity emerges; 2. There is a restriction, say ρ, under which the related induced sub-graph is still "quasi-random". This gives an almost "self-reduction" of the instance, and with $\Gamma|_\rho$ (under P) regular, we can finish by a slightly modified proof for regular case ([2]).

One curious aspect of proofs here is that, the answering strategy itself is apparently computationally hard (Remark 4.5). Previous ones used in the literature (for the pigeonhole principle ([23]), and for k-Clique in regular case) are, on the contrary, computationally simple. We have no idea whether such hardness is necessary (for proving lower bounds).

Another aspect worth mentioning is, since proof of the first bound uses the classical bottleneck counting, it appears possible that it can be translated into restriction-based language (in the sense of [5]). For example, one might define some "width" (computed from Definition 3.2), prove a "width" lower bound (from Lemma 3.3), and apply random restrictions (defined from distribution (3.3)) to remove "large-width" clauses, *etc.*. We do not work in detail of this, with an excuse that the adopted top-down argument consistently works for the second result[2].

Future problems. 1. A highlighted one is to get average lower bound of type $n^{\Omega(k)}$, for general resolution. This improvement (from 2^k to n^k) is especially meaningful for small values of k, say, $O(\log n)$ or constant, and it would match many current state-of-the-art algorithms up to a constant factor in the exponent. As a remark, there is some

[2]It is less clear how, to translate even the proof for regular case into the restriction-based language.

belief in such lower bound for *any* algorithm, whether or not it is based on resolution. E.g. in *parametrized complexity*, k-Clique is so-called $W[1]$-complete [11, 13].

2. Regarding models. In defining the new model we propose the concept *block-width* (Definition 4.2), which can be defined for any CNF. The following question might be of interest: can one extend the well-known size-width relation ([6]) to block-width in some way, in hope to find a unified way to study CNFs of large width (by making it of small block-width)? Also, to better understand short resolution proofs, it might be interesting to consider other "structurally irregular" models. For example, in *branching programs* there is so-called *s-regular* model ([18]), whose direct analogue in resolution is similar to, but different from (and apparently incomparable) the a-irregular model here. Can one prove $n^{\Omega(k)}$-type lower bound on it?

3. The problem of extending the average 2^k-type to stronger systems. For example, the system *Res(k)* (e.g., [26]), and algebraic systems like *cutting-plane* ([10]), which have similar top-down characterizations ([28, 12]).

The paper is organized as follows. Section 2 are preliminaries. Section 3 is for the first lower bound, Theorem 3.1, where subsection 3.1 is graph properties, 3.2 is the proof. Section 4 is for the second result Theorem 4.1, where subsection 4.1 defines the model of a-irregular resolution, 4.2 is (more) graph properties and 4.3 is the proof.

2. Preliminaries

Graphs. In this paper, a graph $G = (V, E)$ is always undirected, simple (with no self-loops or multiple edges). For $v \in V$, $N(v) = \{u \mid u \in V \text{ and } (u, v) \in E\}$ is the set of *neighbors of* v in G. For a subsets $A, B \subset V$, $\hat{N}_A(B) = A \cap (\cap_{v \in B} N(v))$ is the set of *common neighbors of* B *in* A. In case $A = V$, it simplifies to $\hat{N}(B)$.

Erdos-Renyi random graph $G(n, p)$, $0 < p < 1$, is the random variable which place and edge between $\{u, v\}$ with probability p independently for all pairs $u \neq v$ in a fixed n-element set V. Throughout this paper $\mathbf{G}$ denotes this random graph (when n, p is fixed). A *k-clique* in G is a subset C of V with size k such that $\forall u, v \in C, u \neq v \Rightarrow \{u, v\} \in E$. For positive integers $1 < k < n$, it is well-known that there exists the so-called *threshold probability*, $n^{-\frac{2}{k-1}}$, such that: $G(n, p)$ contains a k-clique (or not) with overwhelming probability as $n \to \infty$, when $p > n^{-(1-O(1))\frac{2}{k-1}}$ (or $p < n^{-(1+O(1))\frac{2}{k-1}}$). To see one direction (which is we need), note edges in $\mathbf{G}$ are i.i.d. *Bernoulli random variables* with probability p of being 1, by taking the union bound, the probability that $\mathbf{G}$ contains a k-clique is $< n^{-\Omega(k)}$ whenever $p \leq n^{\frac{-2\xi}{k-1}}$ for constant $\xi > 1$. We will take $\xi > 1$ as a

constant throughout the paper. A *p-biased coin* is the Bernoulli random variable which takes value 1 with probability p, and 0 with probability $1-p$.

Resolution, the k-Clique CNF. A *literal* l over a Boolean variable x is either x (*positive literal*) or its negation $\neg x$ (*negative literal*). x is called the *variable of* l. A *clause* $C = l_1 \vee ... \vee l_t$ is a disjunction of literals among which there is no appearance of $x, \neg x$ together for any variable x (otherwise the clause is simply 1). t is the *width* of C, denoted as $w(C)$. 0 is the empty clause. A *CNF formula* $\tau = C_1 \wedge .... \wedge C_m$ is a conjunction of clauses. A *resolution proof from CNF* τ is an ordered sequences $\Gamma = (D_1, ..., D_L)$ where for all $i \in [L]$, either D_i is a clause in τ (which is called an *axiom*) or it is derived from D_j, D_k where $j, k < i$, by the *resolution rule*:

$$\frac{A \vee x \qquad B \vee \neg x}{A \vee B}$$

$C_j = A \vee x, C_k = B \vee \neg x, C_i = A \vee B$. x is the *resolved variable*. The *size* of Γ is L, denoted as $|\Gamma|$. Γ is a *resolution refutation* if $D_L = 0$.

Equivalently, a resolution refutation is a DAG (directed acyclic graph) with a single source node on top (*the root*), and each non-leaf node has out degree 2 and is attached a clause. The root is attached the 0-clause; a leaf is attached an axiom. Directed edges $(a, b), (a, c)$ mean a resolution step from clauses of b, c to that of a. We say the resolved variable *is queried at* a. A resolution is *tree-like* if its DAG is a tree, and is *regular* if along any path from the root, no variable is queried more than once.

We now introduce two k-Clique CNFs from literature (e.g., [2]). The most direct one, $Click(G, k)$, is the propositional encoding of "G contains a k-clique". It has variables $x_{i,v}$ ($i \in [k]$, $v \in V$), and consists of the following groups of clauses:

$$\bigvee_{v \in V} x_{i,v} \qquad \forall i \in [k]; \tag{2.1}$$

$$\neg x_{i,u} \vee \neg x_{j,v} \qquad \forall i, j \in [k], u, v \in V \ s.t. \ i \neq j, \ \{u, v\} \notin E; \tag{2.2}$$

$$\neg x_{i,u} \vee \neg x_{i,v} \qquad \forall i \in [k], u, v \in V \ s.t. \ u \neq v. \tag{2.3}$$

The other, $Click_{blcok}(G, k)$, is the encoding of "G contains a k-clique, one vertex per block", fixing any a balanced vertex-decomposition:

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

$$\bigvee_{v \in V_i} x_{i,v} \qquad \forall i \in [k]; \tag{2.4}$$

$$\neg x_{i,u} \vee \neg x_{j,v} \qquad \forall i, j \in [k], u \in V_u, v \in V_j \ s.t. \ \{u, v\} \notin E; \tag{2.5}$$

$$\neg x_{i,u} \vee \neg x_{i,v} \qquad \forall i \in [k], \ u, v \in V_i \ s.t. \ u \neq v. \tag{2.6}$$

In both encoding, the first group of axioms is called the *clique axioms*, the second group the *edge axioms*, and the third group the *functionality axioms*. Clearly, the block encoding claims something stronger (hence easier to prove false), so whose lower bound is stronger—which formally can be seen from an easy restriction.

First of all, for the weak encoding, we have the following observation[3].

Theorem 2.1. For any graph G that contains an $\Omega(k)$-clique, the $\exp(\Omega(k))$ size lower bound holds for $Clique(G,k)$ on resolution. In particular, the bound holds for the random graph $G(n, \frac{2\xi}{k-1})$ ($\xi > 1$ constant) w.h.p..

Proof. Use a direct reduction to the *functional pigeonhole principle*, $FPHP$ (e.g., see [25]). More precisely, if G contains a clique C, take the restriction ρ which sets $x_{i,v}$ to 0 for all $i \in [k], v \notin C$. Any resolution proof of $Clique(G,k)$ restricted by ρ becomes a shorter one, which exactly refutes $FPHP^k_{|C|}$—with k pigeons and $|C|$ holes. But an $\exp(|C|)$ lower bound for the latter is known ([25]). Finally, notice that a random graph from $G(n, \frac{2\xi}{k-1})$ ($\xi > 1$ constant) contains $\Omega(k)$-cliques with high probability (e.g., [9]). □

Remark 2.1. Theorem 2.1 says the weak encoding "borrows hardness" from $FPHP^k_{\Omega(k)}$, while telling little about the hardness from the underlying graph. It is, however, unclear how to make a similar reduction for $Clique_{block}(G,k)$ on random graphs[4] , which by definition just prohibits permutations of pigeons and emphasizes more on the graph. This is the reason we think $Clique_{block}(G,k)$ is the "right" encoding of the problem.

Therefore, in the rest of the paper, we solely concentrate on the CNF $Clique_{block}(G,k)$. The following notion is for the "appropriate" cliques in G.

Definition 2.1. Assume $B \subset V = V_1 \coprod ... \coprod V_k$. A clique C is a *B-block-clique* if $C \subset B$, and $\forall l \in [k]$, $|C \cap V_l \cap B| \leq 1$. A *block-clique* is an V-block-clique (in particular, $C = \phi$ is a block-clique).

Query-answer language (*cf.* [23]) As we have mentioned, a resolution proof Γ of CNF τ can be regarded as a top-down DAG, querying a variable at each non-leaf node. We further specify some notations for convenience. A *record* is the negation of a clause in Γ, treated as a partial assignment. At a *round* (=a node/clause of Γ; the first round is the top 0), the query is "*Is variable* $x = 1$*?*", and an *answer* chooses Yes or No. The repeated such process thus forms a downward path that stops when arriving at

[3]For complete $(k-1)$-partite graphs, a similar reduction has been observed by Alexander Razborov earlier (personal communication). See the example in Remark 3.2.

[4]For some specially structured G's, see Remark 3.2.

an axiom in τ. This language naturally applies also to regular resolution and the later a-irregular model (Section 4.1). To show size lower bound under this view, one way is to design answering sequences that can find many different records in Γ. We call this an *Adversary strategy* (against the "Prover", Γ).

For the k-Clique problem, for convenience, denote queries as *(l,v)?*, and answers as $(l,v)^{yes}$ or $(l,v)^{no}$, $l \in [k], v \in V$. An $l \in [k]$ is called a *pigeon*, $v \in V$ is called a *vertex*. So the semantics of $Clique_{block}(G,k)$ is: "assign a vertex to each pigeon so that they form a k-block-clique."

Definition 2.2. (some notions for the k-Clique) On a record P, let $P_1 := \{(l,v) \mid (l,v)^{yes} \in P\}$, corresponding to the negative literals in the clause; and let $P_0 := \{(l,v) \mid (l,v)^{no} \in P\}$, corresponding to positive literals in the clause. Intuitively, P_1, P_0 are the pigeon-vertex assignments and rejections in P, respectively. Use $\mathrm{dom}(P_1), \mathrm{dom}(P_0)$ to denote the projection to $[k]$ from P_1, P_0, respectively. For each pigeon $l \in [k]$, its assignment(s) and rejections in P form the following sets:

$$P_1(l) := \{\ v \in V_l \mid\ (l,v)^{yes} \in P\}, \tag{2.7}$$

$$P_0(l) := \{\ v \in V_l \mid\ (l,v)^{no} \in P\}. \tag{2.8}$$

Note $P_1(l) \cap P_0(l) = \phi$ (by definition of a clause), and $P_1 = \bigcup_{l\in[k]}\{l\} \times P_1(l)$, $P_0 = \bigcup_{l\in[k]}\{l\} \times P_0(l)$. The non-rejected ("live") vertices for l (in P) is defined by:

$$P_{\mathrm{Live}}(l) := V_l \backslash P_0(l), \quad \text{and } P_{\mathrm{Live}} := \bigcup_{l\in[k]} P_{\mathrm{Live}}(l). \tag{2.9}$$

Finally, a *live-clique in P* is defined as a P_{Live}-block-clique (Definition 2.1). A function $f : [k] \to V$ is a *live-clique assignment in P* if f is injective and the image is a live-clique in P. For convenience, identify $[n]$ with the vertex set V when there is no confusion.

3. 2^k-type lower bound for resolution

Parameter regime. Throughout Section 3, we use the following parameter regime.

$$\begin{aligned}
&c_0 \in (0,1/2) \text{ constant}, k = n^{c_0}, \xi > 1 \text{ constant}.\\
&0 < \epsilon << 1 \text{ any small constant}.\\
&N > \max\{\frac{1}{1-3c_0},\ \frac{1}{\epsilon c_0}\},\ t = \frac{18\xi \cdot N}{1/3 - c_0} \text{ large constants}.\\
&r = \frac{k}{t},\ q = \frac{1}{2}n^{1-c_0-2\delta r}, \text{ where } \delta := \frac{2\xi}{k-1}.
\end{aligned} \tag{3.1}$$

(Notice $2\delta r < \frac{1/3-c_0}{2N}$.)

3.1. **Graph properties.** We define the combinatorial property which $\mathbf{G} \sim G(n, n^{-\delta})$ satisfies w.h.p.. It will also be used in Section 4 (but with drastically different parameters).

In a fixed graph $G = (V, E)$, recall $\hat{N}_A(B)$ is the set of common neighbors to B in A, where $A, B \subset V$. We always fix a balanced partition of V as $V = V_1 \coprod ... \coprod V_k$. $\boldsymbol{G}$ will abbreviate $\boldsymbol{G} \sim G(n, n^{\delta})$ with parameters (3.1).

Definition 3.1. In G, $A \subset V$ is called (r, q)-*neighbor-dense* ([2]) if for any $C \subset V$ with size $\leq r$, it holds that $|\hat{N}_A(C)| \geq q$. G is called $(r, q)^{block}$-*neighbor-dense* if for every $j \in [k]$, V_j is (r, q)-neighbor-dense.

Remark 3.1. If a set of vertices is (r, q)-neighbor-dense, then *a priori* it has size $\geq q$.

Lemma 3.1. (*"flip" of neighbor-denseness*) For any integers a_1, a_2, b_1, b_2 and fixed G, if $A \subset V$ is $(a_1 + a_2, b_1 + b_2)$-neighbor-dense and $A_1 \subset A$ 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 such that $|\hat{N}_{A_1}(W_1)| < b_1$. For any $W \subset V$ of size $\leq a_2$, we have

$$\begin{aligned} |\hat{N}_{A\backslash A_1}(W)| &\geq |\hat{N}_{A_1\backslash A_1}(W_1 \cup W)| \\ &= |\hat{N}_A(W_1 \cup W)| - |\hat{N}_{A_1}(W_1 \cup W)| \\ &\geq (b_1 + b_2) - |\hat{N}_{A_1}(W_1)| \\ &\geq b_2 \end{aligned}$$

where the third line uses the assumption that $|W_1 \cup W| \leq a_1 + a_2$ and A is $(a_1 + a_2, b_1 + b_2)$-neighbor-dense. □

Lemma 3.2. W.h.p., $\boldsymbol{G}$ is $(2r, q)^{block}$-neighbor-dense, with parameters (3.1).

Proof. Use the Chernoff bound and union bound, as follows. Note for any fixed $j \in [k]$, any $R \subset V$ with $|R| = 2r$,

$$\mathrm{E}[\ |\hat{N}_{V_j}(R)|\ ] \geq (n/k - |R|) \cdot n^{-\delta r} > \frac{2}{3} n^{1-c_0-2\delta r} > q.$$

So

$$\begin{aligned} \Pr[\ |\hat{N}_{V_j}(R)| < \frac{1}{2}q\ ] &\leq \exp(-\frac{n^{1-c_0-2\delta r}}{48}) \\ &< \exp(-n^{2c_0+\delta r}) \quad \text{since } 3\delta r < 1 - 3c_0 \text{ by (3.1).} \end{aligned} \tag{3.2}$$

where the first "$\leq$" is by Chernoff bound since all different edges are independent. Now take the union bound over all such R's, whose total number of different choices is $\leq n^{2r} < \exp(n^{2c_0} \log n)$. □

For convenience, we call a graph G *good* if it is $(2r, q)^{block}$-neighbor-dense. By Lemma 3.2, $\mathbf{G} \sim G(n, n^{-\delta})$ is good with high probability.

Remark 3.2. Some particularly structured graphs are also good, though being far from "quasi-random". For example, consider a graph $G = (V, E)$ that contains a complete k_1-partite sub-graph, where $2r < k_1 < k$ (r, k as in (3.1)), with "transversal" partition $V = W_1 \coprod ... \coprod W_{k_1}$; *i.e.*, $|W_i \cap V_j| \approx \frac{n}{k_1 k}$ for all $i \in [k_1], j \in [k]$. G is good by straightforward verification. But for $Clique_{block}(G, k)$, there already exists reduction to FPHP (the *functional pigeonhole principle*, as in Theorem 2.1), by the variable substitution: $x_{i,v} \in V_i \cap W_j \mapsto y_{i,j}$ where $y_{i,j}$ are the variables of FPHP. The reduction clearly preserves resolution proofs. While as is mentioned, $2^{\Omega(k)}$-type lower bound for such FPHP is known. As a side remark, on complete $(k-1)$-partite graphs, the $2^{\Omega(k)}$ lower bound is actually tight, since there is the natural $2^k n^2 k^2$ size resolution (and which is regular); e.g., see Prop. 3.1 in [2].

3.2. **Size lower bound.**

Theorem 3.1. For $c_0 \in (0, 1/3)$, $k = n^{c_0}$ and any $\epsilon > 0$, any resolution refutation of $Clique_{block}(G, k)$ on a good graph G must have size $\geq \exp(\Omega(k^{1-\epsilon}))$. Here "good" is with respect to the parameters (3.1).

An immediate corollary of this and section 3.1 is the following.

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

The rest of Section 3 is for the proof of Theorem 3.1.

Fix any a resolution proof Γ of $Clique_{block}(G, k)$. We first describe the Adversary strategy (recall this is just the answering strategy), and then do bottleneck counting.

3.2.1. *The Adversary strategy. Random part.* At the beginning of the query-answer process, choose $\frac{r}{2}$ different pigeons from $[k]$ uniformly from the $\binom{k}{r/2}$ such choices. After this, further choose an α, a block-clique (Definition 2.1) assignment to the chosen

pigeons, randomly according to the following distribution:

(3.3) *Suppose the pigeons chosen are* $l_1, ..., l_{\frac{r}{2}} \in [k]$. *Choose* $\alpha(l_1)$ *uniformly from* V, *then choose* $\alpha(l_2)$ *uniformly from* $\hat{N}_{V_{l_2}}(\{\alpha(l_1)\})$, *and then* $\alpha(l_3)$ *uniformly from* $\hat{N}_{V_{l_3}}(\{\alpha(l_1), \alpha(l_2)\})$ *and so on till* $\alpha(l_{\frac{r}{2}})$ *is chosen.*

Denote this distribution of $\boldsymbol{\alpha}$ by $\mathcal{D}$. Note when G is $(2r, q)^{block}$-neighbor-dense, the above $\alpha(l_j)$ always has non-zero support, for all $j \in [\frac{r}{2}]$.

After choosing α, the strategy will be deterministic.

Deterministic part. Fix a sample α as defined above.

Definition 3.2. (*narrow pigeons*) Given a record P, suppose α and P_1 are compatible as functions from $[k]$ to $[n]$. Pigeon $l \in [k]$ is called *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 $\mathrm{dom}(P_1) \cup \{\text{narrow pigeons in } P\}$.

The **invariance** the strategy will keep is the following: as long as the number of useful pigeons on the record is $< r/2$,

($*$): 1. α and P_1 are compatible functions; and
2. There exists function β defined all narrow pigeons in P, such that $\alpha \cup P_1 \cup \beta$ is injective and has image a live-clique for P (Definition 2.2).

Note in the beginning (top node), ($*$) trivially holds because $P = \phi$ and α 1-1 maps to a block-clique.

Claim 3.1. If for a record P the above ($*$) holds, then P is not an axiom (*i.e.*, the process does not stop unless is halted).

Proof. Direct check. The domain and range condition on β assures that P does not falsify the *clique axioms*, the well-definedness of P_1 assures that P does not falsify the *functionality axioms*. Finally from ($*$), P_1 is injective with $\mathrm{Im}(P_1)$ a block-clique, which assures that P does not falsify the *edge axioms*. □

We continue the construction of the strategy. Suppose at some round, the invariance ($*$) has been kept for the current record P, and the query is (l, v)?. Answer according to the following:

(3.4)
(1) If |useful pigeons in P| $\geq r/2$, then *halt*. Otherwise,
(2) (2a) If $l \in \mathrm{dom}(\alpha \cup P_1 \cup \beta)$, answer honestly according to $\alpha \cup P_1 \cup \beta$;
(2b) Otherwise, say "No".

Lemma 3.3. Suppose the the current record P satisfies $(*)$. Then either we halt, or after the round we still keep $(*)$.

Proof. For item 1 in $(*)$, it holds for the new record because of (2a) of the above strategy. Next we prove item 2. Suppose the current record is P. If P has $\geq r/2$ many narrow pigeons, then we will halt by (1) in the strategy. Otherwise, by assumption there is β for P_0 as in $(*)$. We prove that for the "intermediate" record

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

still satisfies $(*)$. Note Q always subsumes the record at the next node, and so the new record will satisfy $(*)$ because $(*)$ is anti-monotone in the amount of information on the record.

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), there are two possibilities: 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,

$$\begin{aligned} |R| &\leq |\alpha| + |\beta \cup P_1| \\ &= \frac{r}{2} + |\{\text{useful pegions}\}| \\ &< \frac{r}{2} + \frac{r}{2} = r. \end{aligned} \tag{3.5}$$

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. □

Now the Adversary strategy can be completed: as long as not halted, we additionally extend β to keep $(*)$ in any deterministic way.

Remark 3.3. Before bottleneck counting, here is a remark regarding Definition 3.2 (the reader can safely skip this to continue the proof). In Section 4 we will encounter

again the notion of narrow pigeons, but with very different parameter regime (Definition 4.5, equation (4.4)). We will not attempt to unify the parameters in the two sections, so we can preserve the lighter parameter regime (3.1) and the cleaner argument.

3.2.2. *Bottleneck counting.* Since Γ is a correct proof, the query process must stop. By Claim 3.1, it could only be halted in Case (1) of (3.4). Let T be the set of all such halting records (over all α) in the Γ.

Definition 3.3. We say a $\frac{r}{2}$-block-clique assignment α *leads to record P (in T)* if when chosen α in the beginning, the Adversary strategy halts at P.

Lemma 3.4. Given the distribution $\boldsymbol{\alpha} \sim \mathcal{D}$ (3.3), for any fixed $P \in T$

$$\Pr[\ \boldsymbol{\alpha} \text{ leads to } P\ ] \leq \exp(-\Omega(k^{1-\epsilon})) \tag{3.6}$$

where the parameters are as in (3.1).

Proof. Let $P \in T$ be such a record. Recall (Definition 3.2) useful pigeons are those in $P_1 \cup \{\text{narrow pigeons}\}$. By definition of T and Lemma 3.3, for P we have $|\{\text{useful pigeons}\}| \geq r/2$.

First, recall $r = k/t$ ((3.1)) and let $\epsilon' = (\frac{1}{100}\frac{r}{k})^2 = (\frac{1}{100t})^2$ which is a small constant. By the first part of $\boldsymbol{\alpha}$, we have:

$$Pr[\ |\mathrm{dom}(\boldsymbol{\alpha}) \cap \{\text{useful pigeons}\}| < \epsilon' r\ ] \tag{3.7}$$

$$\leq \sum_{a<\epsilon' r} \binom{\frac{r}{2}}{a} \cdot \binom{k-\frac{r}{2}}{\frac{1}{2}r-a} / \binom{k}{\frac{r}{2}} \tag{3.8}$$

$$\leq \epsilon' r \cdot \big(\frac{e}{2\epsilon'}\big)^{\epsilon' r} \cdot \big(\frac{e(k-\frac{r}{2})}{(\frac{1}{2}-\epsilon')r}\big)^{r/2-\epsilon' r} \cdot \big(e(\frac{k}{\frac{r}{2}}-\frac{1}{2})\big)^{-r/2} \tag{3.9}$$

$$= \epsilon' r \cdot \exp(r\epsilon' \ln \frac{e}{2\epsilon'}) \cdot \big(\frac{t-\frac{1}{2}}{(2t-\frac{1}{2})(\frac{1}{2}-\epsilon')}\big)^{\frac{r}{2}-\epsilon' r} \tag{3.10}$$

$$\leq \epsilon' r \cdot \exp(r \cdot 2\sqrt{\epsilon'}) \cdot (1-\frac{1}{10t})^{r/3} \tag{3.11}$$

$$< \epsilon' r \cdot \exp(-r/75t) = \exp(-\Omega(k)) \tag{3.12}$$

where (3.9) is by the monotonicity in a ($a \leq \epsilon' r$) and binomial coefficient approximation

$$\big(e(\frac{n}{b}-\frac{1}{2})\big)^b \leq \binom{n}{b}\sqrt{2\pi b} \leq (\frac{en}{b})^b, \quad \text{when } n >> b;$$

(3.11) is because $\epsilon' \ln \frac{1}{\epsilon'} < \sqrt{\epsilon'}$ when ϵ' is small enough, and $\frac{t-\frac{1}{2}}{(2t-\frac{1}{2})(\frac{1}{2}-\epsilon')} < 1 - \frac{1}{10t}$ noticing $\epsilon' < \frac{1}{20t}$; the last "=" uses $r = \Omega(k)$ and t is constant.

Therefore,

$$\Pr[\ \boldsymbol{\alpha} \text{ leads to } P\ ] \le \exp(-\Omega(k)) +$$

$$\Pr[\ \boldsymbol{\alpha} \text{ leads to } P \text{ and } |\mathrm{dom}(\boldsymbol{\alpha}) \cap \{\text{useful pigeons}\}| \ge \epsilon' r\ ] \tag{3.13}$$

Below we bound the probability in (3.13). There are two cases:

$$|\mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1)| \ge \frac{\epsilon' r}{2}, \quad \text{Or} \tag{3.14}$$

$$|\mathrm{dom}(\boldsymbol{\alpha}) \cap (\{\text{narrow pigeons}\} \backslash \mathrm{dom}(P_1))| \ge \frac{\epsilon' r}{2}. \tag{3.15}$$

Here as usual, $\mathrm{dom}(\boldsymbol{\alpha})$ denotes the domain of $\boldsymbol{\alpha}$ (a subset of $[k]$).

Recall $\frac{\epsilon' r}{2} = \Omega(k)$, and both $|\mathrm{dom}(P_1)|$ and $|\text{narrow pigeons}|$ are subsets of $[k]$ that are decided by P (independently of $\boldsymbol{\alpha}$). Suppose α' is an arbitrary choice of $\boldsymbol{\alpha}$ that satisfies the condition in (3.13). Below we bound the probability (3.14), (3.15) separately.

1. In the first case, (3.14), 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 by Remark 3.1(a) there are $\ge \frac{1}{2} n^{1-c_0-2\delta r}$ many choices of vertices for *each* such pigeon. By definition (3.3), $\boldsymbol{\alpha}$ chooses among them uniformly. Thus

$$\Pr[\ \boldsymbol{\alpha} \text{ leads to } P \text{ and } |\mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1)\}| \ge \epsilon' r/2\ ] \tag{3.16}$$

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

$$= \sum_{S \subset [k],\ |S| \ge \epsilon' r/2} \Pr[\mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1) = S\ ] \cdot \Pr[\text{ for all } i \in S,\ \boldsymbol{\alpha}(i) = P_1(i)] \tag{3.18}$$

$$\le \sum_{S \subset [k],\ |S| \ge \epsilon' r/2} \Pr[\ \mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1) = S\ ] \cdot (\frac{1}{2} n^{1-c_0-2\delta r})^{\epsilon' r/2} \le\ 1 \cdot n^{-\Omega(k)} \tag{3.19}$$

where (3.17) is from the independence between the choosing $\mathrm{dom}(\boldsymbol{\alpha})$ and choosing their images in the definition of $\boldsymbol{\alpha}$, and (3.18) is from the uniform choice of each image independently, and the discussion above (3.16); the last inequality is from parameter choice (3.1) and that ϵ' is a constant.

2. In the latter case, (3.15), let B denote $\{\text{narrow pigeons (in } P)\} \backslash \mathrm{dom}(P_1)$. Note in the process of choosing vertices to pigeons in

$$i \in \mathrm{dom}(\alpha') \cap B$$

to define $\alpha'(i)$, vertices in $P_0(i)$ cannot be chosen. This is because of (2a) of (3.4) in the strategy. On the other hand, for any such pigeon i, by assumption it is narrow in

P so $P_0(i)$ is $(r, \frac{1}{2}q)$-neighbor-dense. Hence by Remark 3.1, we have

$$\begin{aligned}\hat{N}_{P_0(i)}(\mathrm{Im}(\alpha'|_{\mathrm{dom}(\alpha'\setminus\{i\})})) &\geq \frac{1}{2}q \\ &= \frac{1}{4}n^{1-c_0-2\delta r}.\end{aligned} \tag{3.20}$$

So for such i, by definition of $\mathcal{D}$ and $|V_i| = n^{1-c_0}$,

$$\begin{aligned}\Pr[\, \boldsymbol{\alpha}(i) \notin P_0(i) \mid i \in \mathrm{dom}(\boldsymbol{\alpha}) \,] &\leq 1 - \frac{n^{1-c_0-2\delta r}}{4n^{1-c_0}} \\ &= 1 - \frac{1}{4}n^{-2\delta r}.\end{aligned} \tag{3.21}$$

Now we can bound the overall probability that this case happens, by

$$\sum_{S\subset B,\ |S|\geq \epsilon' r/2} \Pr[\, \mathrm{dom}(\boldsymbol{\alpha}) \cap B = S \text{ and } \boldsymbol{\alpha}(i) \notin P_0(i) \text{ for all } i \in S \,] \tag{3.22}$$

By the independence of the two stages in the distribution $\mathcal{D}$, similar to the estimation to (3.16), we have from (3.21) that

$$(3.22) \leq (1 - \frac{1}{4}n^{-2\delta r})^{\epsilon' r/2} = (1 - \frac{1}{4}n^{-2\delta r})^{\Omega(k)} \leq \exp(-\Omega(k^{1-\epsilon})), \tag{3.23}$$

where the last "$\leq$" is from the fact that $2\delta r < \epsilon c_0$ in (3.1). □

Since any choice of $\boldsymbol{\alpha}$ must halt in some record in T (the first paragraph of section 3.2.2), 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 records in Γ. Theorem 3.1 is proved.

4. n^k-type lower bounds for a-irregular resolutions

4.1. a-irregular resolution.

Recall a resolution proof Γ is viewed as a top-down DAG. We say a variable x is *irregularly queried on* $\mathcal{P}$, where $\mathcal{P}$ is a directed path in Γ, if x is queried more than once on $\mathcal{P}$ (the query at the end of $\mathcal{P}$, if exists, doesn't count).

We are going to introduce the model of a-irregular resolution. Its main version, Definition 4.2, assumes a variable partition in input. Let's start with a lighter one, subsumed by the main.

Definition 4.1. Let $0 \leq a \leq 1$. A resolution proof Γ on m variables is *a-irregular*, if for any clause $C \in \Gamma$ with width $\geq am$, there is a set irr_C of size $\leq am$, that contains all irregularly-queried variables after C. In other words,

$$\begin{aligned}&\text{if } w(C) \geq am, \text{ then } \exists \mathrm{irr}_C \subset [m],\ |\mathrm{irr}_C| \leq am, \text{ such that on any path} \\ &\text{starting from } C, \text{ its irregularly queried variables belong to } \mathrm{irr}_C.\end{aligned} \tag{4.1}$$

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

We continue to the main version, starting with some additional motivation. For many CNFs of interests, which express tautologies or principles, there are "naturally" associated partitions of variables (by their semantical meanings, etc.). On the other hand, for general satisfiability problem or random CNFs where there is no natural candidate partition, *any* variable partition can be added as additional input, to pose structural control on the proof or algorithm. (An analogue is, for example, the ordered resolution, where a variable order is added as structural limitation.) The model of *a-irregular resolution for* κ takes this into consideration.

(*Main model*) Given m variables and $\kappa : [m] \twoheadrightarrow [k]$ a partition of variables into k blocks ($1 \leq k \leq m$), we say x *belongs to* $S \subset [k]$ if $\kappa(x) \in S$. The *block-width* of clause C is

$$w^b(C) := |\{\ i \in [k] \mid \kappa^{-1}(i) \cap Var(C) \neq \phi\}|. \tag{4.2}$$

Definition 4.2. (*main model*) For $a \leq 1$, κ as above, a resolution proof Γ on m variables is *a-irregular for* κ if for any clause $C \in \Gamma$,

$$\begin{aligned} &\text{If } w^b(C) \geq am, \text{ then } \exists \mathrm{irr}_C \subset [k] \text{ of size} \leq ak \text{ s.t. along any path} \\ &\text{starting from } C, \text{ its irregularly queried variables belong to } \mathrm{irr}_C. \end{aligned} \tag{4.3}$$

As a reminder, both definitions 4.1, 4.2 have no limitation on the number of irregular queries on any variable, nor queries before encountering a clause like C. Note by definition, the blocked a-irregular model subsumes the unblocked $\frac{ak}{m}$-irregular one, for *any* $\kappa :\ [m] \twoheadrightarrow [k]$.

We give some evidence of the usefulness of the model, via three remarks below. As a beforehand reminder, all short proofs mentioned below actually fall in the model with extremely small parameter a as $m^{-\Omega(1)}$; our lower bound in Theorem 4.1, on the other hand, holds for constant a (for any k).

Remark 4.1. Let us see by example that (unblocked) a-irregular resolution (Definition 4.1) is exponentially stronger than regular, even a is merely $m^{-\Omega(1)}$. We can take the *Stone-formula* in [1], which has $m = \Theta(n^2)$ variables. For G with large *pebbling number*, these formulas are exponentially hard for regular resolution (see [1] for detail), while the short resolution (their Theorem 4.1) is $m^{-\frac{1}{2}}$-irregular. Actually, the set of all irregularly queried variables are only the "stone variables", whose size is $O(n)$.

Remark 4.2. The situation is even more clear in the main model, Definition 4.2. To the best of the author's knowledge, known exponential separations between the regular

and general resolution are the two classes from [1]. And they are, as we will see, all separations between regular and the a-irregular model for some κ, where a is only $m^{-\Omega(1)}$ and κ is naturally associated with the CNF.

We examine these examples below. They are the Stone Formulas, which is already mentioned in Remark 4.1, and a variation of the *Ordering Principle*, denoted as GT'_n. For the Stone-formula, the variables are naturally partitioned into $k = n + 1$ blocks according to vertices of G. Axioms have block-width 4. Using the notation in [1], $\kappa = \{ \{P_{i,u}\}_{a\in S}\ (i \in G),\ \{R_t\}_{t\in S}\ \}$. The short resolution in [1] is $\frac{5}{k}$-irregular for κ, since every clause in that resolution has block-width ≤ 4.

For the variation of the Ordering Principle, GT'_n, under the notation in [1], it has $m = n(n-1)$ variables $x_{i,j}$, $i \neq j \in [n]$, with the intended semantical meaning $x_{i,j} \Leftrightarrow$ *element i is greater than element j*. They are naturally partitioned according to the second subscript j, into $k = n$ blocks. Denote this partition by κ. Axioms will again have constant block-width. The short resolution (Corollary 3.4 in [1]) 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 all clauses have block-width ≤ 4; and then uses a resolution from [29], in which all clauses are $C_m(j)$'s (in notation of [29]) or axioms, and so all have block-width ≤ 4. So in particular, it is $4/k$-irregular for κ.

Remark 4.3. Finally, we give some remarks about the additional input—a variable partition κ. Full freedom in choosing κ seems hard to control, yet we provide some suggestion on "reasonable" ones. All examples in above remarks have somewhat natural choice of κ, from the semantics of the CNF (and we will explain below, why some other plausible partitions are not chosen). This "natural choice" is certainly not guaranteed for general CNFs, but in that case we can consider the following.

First, recall CNFs with small width are well-studied for resolution in a unified way via the width-size relation ([6]). This naturally stimulates the hope to extend this relation to some variation of width, as there are CNFs of interests that have large width. If consider this in our model, then it highlights a plausible "principle":

Choose κ under which, axioms have small block-width.

Second, to be useful to help understand short proofs, the limited model should be strong enough to contain short proofs. The above "principle" has a merit: clauses with large block-width are "nontrivial" (or "far from axioms"), so at least apparently, the structural requirement (4.3) seems not to make this system oversimple.

As the reader might have noticed, choices of κ in examples of Remark 4.1, 4.2 followed this principle, and somehow witnessed the mentioned merit. It is now also clear why

we omit some other choices: in GT'_n, for example, κ' that partitions variables according to the first subscript also seems natural at the first sight, but axioms already have linear block-width. In the Stone formula, the partition by stones similarly causes large block-width in axioms. Under this angle, for our target $Clique_{block}(G,k)$ the choice $\kappa : x_{l,v} \mapsto l$ is appropriate, as axioms have block-width ≤ 2 (while having large width).

From now on, by "a-irregular resolution" we insist to the model by Definition 4.2. The main theorem of this section is the following.

Theorem 4.1. Let $\tau := Clique_{block}(G,k)$, $\kappa : x_{i,v} \to i \in [k]$. For $\xi > 1$ constant, if $\log_n k \leq \frac{1}{3} - 200\epsilon$ for some constant $\epsilon > 0$, then for $\boldsymbol{G} \sim G(n, n^{-2\xi/(k-1)})$, w.h.p. any $\frac{\epsilon}{\xi}$-irregular resolution proof for (τ,κ) requires size $n^{\Omega(k)}$, where Ω depends on ξ,ϵ.

In particular, the same bound holds for (unblocked) $\frac{\epsilon k}{\xi n}(=O(\frac{k}{n}))$-irregular resolution.

4.2. **More graph properties.** Recall the neighbor-denseness (Definition 3.1). Here is a relativzation of it.

Definition 4.3. Given a graph G, $a,b \in \mathbb{N}_+$. For $A,B \subset V$, B is called $(a,b)^A$-*neighbor-dense* if for any $Q \subset A$, $|Q| \leq a$ it holds that $|\hat{N}_B(Q)| \geq b$. When $A = V$, we omit the upper index and simply say B is (a,b)-*neighbor-dense*.

Remark 4.4. (*inheritability of neighbor-denseness*) If $A' \subset A$ and B is $(a,b)^A$-neighbor-dense, then B is $(a,b)^{A'}$-neighbor-dense. In particular, an (a,b)-neighbor-dense set is $(a,b)^A$-neighbor-denseness for any A.

Recall the "flip" property of neighbor-denseness (Lemma 3.1). For convenience we recast it here as:

Lemma 4.1. (*"flip" of neighbor-denseness*) For any integers a_1,a_2,b_1,b_2 and fixed G, if $A \subset V$ is (a_1+a_2,b_1+b_2)-neighbor-dense and $A_1 \subset A$ is not (a_1,b_1)-neighbor-dense, then $A \backslash A_1$ is (a_2,b_2)-neighbor-dense.

Another "quasi-random" property of G which plays an important rule in the proof of regular case is the following. It says for any (r,q)-neighbor-dense set in G, all witness sets of its non-(tr,q')-neighbor-denseness (if exist) are non-trivially concentrated (for suitable suitable parameters r,q,q').

Definition 4.4. $W \subset V$ is called (tr,r,q',s)-*mostly-dense in* G ([2]), if $\exists S \subset V$ of size $\leq s$, such that $\forall Q \subset V$ of size $\leq tr$, $|\hat{N}_W(Q)| < q'$ implies $|Q \cap S| \geq r$. 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.

The following simple proposition says mostly-denseness is also inheritable (with respect to the concentrating set S).

Proposition 4.1. Suppose $A \subset V$, and W is (tr, r, q', s)-mostly-dense. Then $\exists S_1 \subset A$ of size $\leq s$ such that, for any $Q \subset A$, $|Q| \leq tr$, if $|\hat{N}_W(Q)| < q'$ then $|Q \cap S_1| \geq r$.

Proof. Simply take S_1 to be $S \cap A$, where S is as in the definition of mostly-denseness of W. □

As usual, denote $\frac{2\xi}{k-1}$ by δ. The main result of [2] is the following.

Theorem 4.2. Suppose $\xi > 1$, $k < n^{\frac{1}{4}-\epsilon}$, $\epsilon \in (0, \frac{1}{2})$. Then:

(1) (their Theorem 6.1) W.h.p., $\boldsymbol{G} \sim G(n, n^{-\delta})$ 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) If G satisfies the two properties in (1), then any regular refutation of $Clique_{block}(G, k)$ requires size $n^{\Omega(k/\xi^2)}$.

Below we fix the parameter regime for the rest of the paper; then state a form of Theorem 4.2(1) (as Theorem 4.3) that will be of use.

Parameter regime. In the rest of Section 4, we set parameters as:

$$\begin{aligned} &\xi > 1 \text{ constant}, \ \ 0 < \epsilon < 1/15 \text{ constant}, \ \delta = \frac{2\xi}{k-1}; \\ &t = \frac{40\xi}{\epsilon}, \ \ \frac{3t^2}{\epsilon} < k < n^{\frac{1}{3}-5\epsilon}; \\ &r = \frac{k}{t^2}, \quad q = \frac{1}{8tk} n^{1-8\delta tr}, \quad q' = \frac{1}{4} q n^{-\delta tr}; \\ &s = k^2 n^{9\delta tr+\epsilon}, \ p = n^{-(9\delta tr+2\epsilon)}/k. \end{aligned} \tag{4.4}$$

In below, recall the $(\cdot,\cdot)^{block}$-neighbor-denseness in Definition 3.1.

Theorem 4.3. With parameter regime (4.4), w.h.p. $\boldsymbol{G} \sim G(n, n^{-\delta})$ is

$$\begin{aligned} &(8tr, 4tq)^{block}\text{-neighbor-dense; and} \\ &(tr, r, q', s)\text{-mostly-dense.} \end{aligned} \tag{4.5}$$

Proof. The proof of first part is identical to that of Lemma 3.2. For the second part, the original technical proof of Theorem 4.2(1) applies directly; we only point out parameters (4.4) make $n^{\epsilon/2+1} < qn^{-\delta tr}s/tr$, making their argument go through smoothly. □

Therefore, to prove Theorem 4.1 it suffices to prove the following.

Theorem 4.4. Suppose G satisfies (4.5) with parameters (4.4). $\tau := Clique_{block}(G, k)$, $\kappa : x_{l,v} \mapsto i \in [k]$. For large n, any $\frac{1}{t}$-irregular resolution for (τ, κ) requires size $n^{\epsilon k/6t^2}$.

The rest of this section is for proving Theorem 4.4.

4.3. **Lower bound proof.** The following notion, as mentioned in Remark 3.3, is the same to Definition 3.2 but with different parameters. For compatibility we still use the name "narrow". Without confusion, in this Section 4 we always insist to this version.

Definition 4.5. (*narrow pigeons*) Suppose $P \in \Gamma$ is a record. A pigeon $l \in [k]$ is called *narrow in* P if

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

Let narrow_P denote the set of narrow pigeons in P.

4.3.1. *Proof outline.* The proof will combine the idea in Section 3 and Theorem 4.2, via a restriction. As usual, given a proof Γ we design an Adversary strategy. This time it is two-stage. In stage I, the strategy is similar to that of section 3.2 but even simpler: now we do not need random coin α at all, and the goal of this stage is to find *any* clause, say P^*, that satisfies:

- has block-width $\geq \frac{k}{t}$; and
- living vertices in P^* (Definition 2.2) for "many" pigeons are "many".

The two conditions will be balanced via Definition 4.5 (*"narrow"*). Then, stage II starts at P^*. In a $\frac{1}{t}$-irregular proof, by choice of P^*, there is a small set of blocks containing all irregularly-queried variables after P^*. We will be able to find a block-clique assignment $\widetilde{\beta}$ (equation (4.11)) which sets these variables, and concentrate on $\Gamma|_{\widetilde{\beta}}$ which is regular. The second condition for P^* insures that the instance almost has a *self-reduction* via this restriction: more precisely, the induced sub-graph keeps being (tr, tq)-neighbor-dense, and has a similar property to (tr, r, q', s')-mostly-denseness (Section 4.3.3). Therefore, we can use Theorem 4.2(2) to finish the proof. The only subtlety of the last part is that mostly-denseness is not completely inherited, but we find a relative version (Remark 4.6) that suffices.

Definition 4.6. (*Notation*) Recall in a resolution, a record is identified with a node/clause. Suppose the query process has continued to record P, then $\mathcal{P}$ denotes the path traveled from the root to P. We call the query-process so far as being *along* $\mathcal{P}$. P^+ denotes the next node according to the strategy, with Q the intermediate record $P \cup \{\text{new answer}\}$.

4.3.2. *Adversary strategy.*

Stage I.

The starting node 0 is in this stage; the strategy will be similar to that in Section 3. During this stage, we always keep a live-clique assignment β_P (Definition 2.2) for the

current record P, which is empty at the starting node, such that

$$\beta_P \supset P_1, \qquad \mathrm{dom}(\beta_P) = \mathrm{dom}(P_1) \cup \mathrm{narrow}_P. \tag{4.6}$$

In particular, P_1 will be a well-defined function. Suppose the process continues to P along $\mathcal{P}$ within this stage, and the query at P is:

$$(l_1, v_1)? \tag{4.7}$$

Answer by:

- If

$$|\mathrm{narrow}_P \cup \mathrm{dom}(P_1)| \geq tr, \tag{4.8}$$

  go to Stage II;
- Otherwise, to query (4.7),
  - if $l_1 \in \mathrm{dom}(P_1) \cup \mathrm{narrow}_P$, answer according to β_P;
  - otherwise, answer No.

If haven't transited to Stage II, we need to maintain (4.6) for the new node. Update for β_P to β_Q as follows. Notice $|\mathrm{dom}(\beta_Q)| \leq |\mathrm{dom}(\beta_P)| + 1 \leq tr$, and "+1" is needed if and only if $l_1 \in \mathrm{narrow}_Q \backslash \mathrm{narrow}_P$.

Claim 4.1. If G is $(8\delta tr, 4tq)^{block}$-neighbor-dense, $l \notin \mathrm{narrow}_P$, then $P_{\mathrm{Live}}(l)$ is $(4\delta tr, 2tq)$-dense.

Proof. Apply Lemma 4.1 to $A \leftarrow V_l$, $A_1 \leftarrow P_0(l)$ and $a_1 = a_2 = 4\delta tr$, $b_1 = b_2 = 2tq$. □

Claim 4.1 implies that if $l_1 \in \mathrm{narrow}_Q \backslash \mathrm{narrow}_P$ then

$$|\hat{N}_{P_{Live}(l_1)}(\mathrm{Im}(\beta_P))| \geq 2tq > 1.$$

Therefore, $\exists v \in \hat{N}_{P_{Live}(l_1)}(\mathrm{Im}(\beta_P)) \backslash \{v_1\}$, and β_Q extends β_P by sending l_1 to v. This settles Q for maintaining (4.6); as for P^+, take

$$\beta_{P^+} = \beta_Q|_{\mathrm{narrow}_{P^+} \cup \mathrm{dom}(P_1^+)} \tag{4.9}$$

where $\mathrm{narrow}_{P^+} \subset \mathrm{narrow}_Q$ and $P_1^+ \subset Q_1$ (a sub-function). This completes Stage I.

Claim 4.2. The query-answer process must transit to Stage II at some node P.

Proof. Similar to Claim 3.1. If P does not satisfy (4.8) then there is no violated axiom. Indeed, the *functionality axioms* and *edge axioms* are preserved by existence of β_P in (4.6). The *clique axioms* are preserved by β_P and the fact that, if $P_{\mathrm{Live}}(l) = \phi$ then *a priori* l is narrow, but this means $\beta(l) \in P_{\mathrm{Live}}(l)$ which is impossible in Stage I. □

Stage II.

Suppose the process transits to this stage at node P^* of Γ. Our goal is to find a new, regular protocol Γ^* by restricting Γ (under P^*), then use the result for regular resolution. This can be accomplished only if the instance after the restriction is still a Clique-CNF on a "quasi-random" graph, which is a bit too much to obtain. We find a weaker "quasi-randomness" instead, from a deterministic restriction. The analysis would require some detail of the strategy for regular case, so we also present it in "*Strategy on* Γ^*" in below.

Find the restriction. As $|P_1 \cup \text{narrow}_P|$ at most increases size by 1 per round in Stage I (while it might decrease), P^* must satisfy:

$$|\text{narrow}_{P^*} \cup \text{dom}((P^*)_1)| = tr. \tag{4.10}$$

If Γ is $\frac{1}{t}$-irregular (w.r.t. κ), there is a subset of $[k]$ with size tr, denoted as irr_{P^*}, that contains blocks (i.e., pigeons) of all possible irregularly-queried variables after P^*.

Claim 4.3. There exists a live-clique assignment for P^*, $\widetilde{\beta}$, such that

$$\widetilde{\beta} \text{ extends } \beta_{P^*}, \quad \text{dom}(\widetilde{\beta}) = \text{dom}(\beta_{P^*}) \cup \text{irr}_{P^*}. \tag{4.11}$$

Proof. We extend function β_{P^*} on $\text{irr}_{P^*} \backslash \text{dom}(\beta_{P^*}) \subset \text{irr}_{P^*} \backslash \text{narrow}_{P^*}$ one by one. In each step, the function to be extended has image size $\leq (|\text{dom}((P^*)_1)| + |\text{narrow}_{P^*}|) + |\text{irr}_{P^*}| \leq 2tr$, so it is possible to find their common neighborhood in $P_{\text{Live}}(l)$ for any $l \notin \text{narrow}_{P^*}$, by Claim 4.1. □

Get new instance $\widetilde{G}$ *and* Γ^*. Fix a $\widetilde{\beta}$ as in Claim 4.3. Let

$$\widetilde{G} := G\,[\bigcup_{l \in [k] \backslash \text{dom}(\widetilde{\beta})} \widetilde{V}_l], \qquad \text{where } \widetilde{V}_l := \hat{N}_{P^*_{\text{Live}}(l)}(\text{Im}(\widetilde{\beta})),\ l \in [k] \backslash \text{dom}(\tilde{\beta}). \tag{4.12}$$

Further restrict appropriate variables to 0, so that the k-Clique CNF on G becomes the $(k - |\text{dom}(\tilde{\beta})|)$-Clique CNF on $\widetilde{G}$. Moreover, by definition of irr_{P^*}, if Γ is $\frac{1}{t}$-irregular then the resulting restricted proof, denoted as Γ^*, is regular.

Strategy on Γ^*. Finally, we show the query process on Γ^*. Still use P^* to denote top node of Γ^* (a 0 clause now). Suppose the current node is $P \in \Gamma^*$, the query is (4.7), $l_1 \in [k] \backslash \text{dom}(\widetilde{\beta})$, $v_1 \in \widetilde{V}_{l_1}$, and $\mathcal{P}$ is the path from P^* to P *so far traveled*. Answer by:

(1) If $\exists v \in \widetilde{V}_{l_1}$ s.t. (l_1, v) was answered Yes along $\mathcal{P}$, answer No;
(2) Otherwise, if $v_1 \notin \hat{N}(\text{Im}(P_1))$, answer No;
(3) Otherwise, flip a p-biased coin (p in (4.4)), and answer Yes iff the coin is 1.

The No's in (1), (2) are called a *forgotten-forced* answer (to l_1) and a *edge-forced* answer, respectively. Answer in (3) is called *random*. Note item (1) depends on $\mathcal{P}$.

This completes Stage II, hence the whole Adversary strategy.

Remark 4.5. The above *Strategy on* Γ^*, as mentioned, is borrowed from the regular case ([2]), with minor adjustments (to make it simpler; see the end of the remark). It is defined regardless of regularity of Γ^*; and as we will see, some of its useful property, though not all, holds for general resolution (Lemma 4.5). As a side remark, compared to the "hard" strategies used in Theorem 3.1 and Stage I[5], here given G and the current query-path, an answer is easy to compute (*i.e.*, the deterministic part can be done in time $O(|\Gamma^*|)$) even if not knowing the whole Γ^*.

4.3.3. *Analysis.*

Properties of $\widetilde{G}$. Recall $\widetilde{G}$ is the induced subgraph (4.12).

Lemma 4.2. Assume G is $(8tr, 4tq)^{block}$-neighbor-dense (t, q as in (4.4)). Then $\forall l \in [k]\backslash\mathrm{dom}(\widetilde{\beta})$, $\widetilde{V}_l$ is $(2tr, 2tq)^V$-neighbor-dense in G.

In particular, $\widetilde{G}$ itself is $(2tr, 2tq)^{block}$-neighbor-dense, by the inheritability (Remark 4.4) and the fact that it is induced.

Proof. Fix such an l. First, as in the proof of Claim 4.1, apply Lemma 4.1 to $A \leftarrow V_l$ and $A_1 \leftarrow (P^*)_0(l)$ with $a_1 = a_2 = 4\delta tr$, $b_1 = b_2 = 2tq$, where we notice that $l \notin \mathrm{dom}(\mathrm{Im}(\widetilde{\beta})) \supset \mathrm{dom}(\mathrm{narrow}_{P^*})$. As a result we have

$$P^*_{\mathrm{Live}}(l) \text{ is } (4\delta tr, 2tq)\text{-neighbor-dense.} \tag{4.13}$$

Now for any $R \subset V$ of size $\leq 2tr$, $|\mathrm{Im}(\widetilde{\beta}) \cup R| \leq 2tr + 2tr = 4tr$, so by (4.13),

$$\begin{aligned} |\hat{N}_{\widetilde{V}_l}(R)| &= |\hat{N}_{\hat{N}_{P^*_{\mathrm{Live}}(l)}(\mathrm{Im}(\widetilde{\beta}))}(R)| \\ &= |\hat{N}_{P^*_{\mathrm{Live}}(l)}(\mathrm{Im}(\widetilde{\beta}) \cup R)| \\ &\geq 2tq. \end{aligned}$$

The lemma is proved. □

Lemma 4.3. Assume G is (tr, r, q', s)-mostly-dense. Then: for all $(r, q)^V$-neighbor-dense set $W \subset \widetilde{V}$, $\exists S \subset \widetilde{V}$ of size $\leq s$ such that, for any $Q \subset \widetilde{V}$ of size tr, $|\hat{N}_W(Q)| < q'$ implies $|S \cap Q| \geq r$.

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 4.1, take $A \leftarrow \widetilde{V}$ and $W \leftarrow W$; as a result, there exists $S_1 \subset A = \widetilde{V}$ that satisfies the condition in the lemma. □

[5]where to efficiently check neighbor-denseness, one apparently needs an NP oracle

Remark 4.6. The content after "Then" in Lemma 4.3 is a *relative* property between G and $\widetilde{G}$. For $\tilde{G}$, this is weaker than (tr, r, q', s)-mostly-denseness itself, because of the obvious inclusion

$$\{(r,q)^V\text{-neighbor-dense sets in } \widetilde{V}\} \subset \{(r,q)^{\widetilde{V}}\text{-neighbor-dense sets in } \widetilde{V}\}.$$

As we will see, this weaker "quasi-randomness" suffices for the proof (in Lemma 4.6).

Bottleneck counting. Since Γ is a correct proof, the process must stop in Stage II by Claim 4.2. Without loss of generality, assume

$$\mathrm{dom}(\widetilde{\beta}) = [\tilde{k}+1, k], \quad \text{where } k - \tilde{k} = |\mathrm{dom}(\widetilde{\beta})| < 2tr \ (= \frac{2k}{t}).$$

We will not care much about $|\widetilde{V}|$; as will be seen, the lower bound actually depends on the "quasi-random" parameters of $\widetilde{G}$ from Lemma 4.2, 4.3. Denote by $\boldsymbol{\mathcal{P}}$ the random path from P^* to axioms (defined by the strategy on Γ^*). To any path $\mathcal{P}'$, "$\mathcal{P}' \subset \boldsymbol{\mathcal{P}}$" denotes the event "$\boldsymbol{\mathcal{P}}$ travels through $\mathcal{P}'$". By *eligible paths* we refer to paths in Γ^* (not necessarily from P^* to axioms) that can be traveled through with nonzero probability.

For any eligible path $\mathcal{P}$ in Γ^*, define

$$\mathcal{P}_1 = \{\ (l,v) \mid (l,v)^{yes} \text{ is answered along } \mathcal{P}\ \}, \text{ and similarly } \mathcal{P}_0; \tag{4.14}$$

$$\mathrm{random}(\mathcal{P}) = \{\ (l,v) \mid (l,v)? \text{ is answered randomly along } \mathcal{P}\ \}. \tag{4.15}$$

As usual, $\mathcal{P}_0(l) = \{\ v \mid (l,v) \in \mathcal{P}_0\ \}$ for $l \in [\ \widetilde{k}\ ]$. Note $\mathrm{random}(\mathcal{P})$ is well-defined.

Definition 4.7. Suppose $W \subset \{\ (l,v) \mid (l,v) \in [\ \widetilde{k}\ ] \times \widetilde{V}_l\ \}$. A path $\mathcal{P}$ in Γ^* is W^{yes}*-compatible* if $W \cap \mathcal{P}_0 = \phi$, and is W^{no}*-compatible* if $W \cap \mathcal{P}_1 = \phi$.

A related important fact is: if Γ^* is regular then $\mathcal{P}_1 \cap \mathcal{P}_0 = \phi$, meaning that $\mathcal{P}$ is $\mathcal{P}_1^{yes}$- and $\mathcal{P}_0^{no}$-compatible, for any path $\mathcal{P}$ in Γ^*.

Now we prove lower bounds on $|\Gamma^*|$. First it is easy to verify: *functionality* and *edge axioms* are never falsified by a record in Stage II. So any eligible path $\mathcal{P}$ that is down to axioms must end in a *clique axiom*

$$C_l := \bigvee_{v \in V_l} x_{l,v} \qquad l \in [\ \widetilde{k}\ ]. \tag{4.16}$$

In below, we only need to upper bound the probability $\Pr[\ \boldsymbol{\mathcal{P}}$ ends in $C_l\ ]$, $\forall l \in [\tilde{k}]$.

Lemma 4.4. If $\mathcal{P}$ is an eligible path to axiom C_l in (4.16), then along $\mathcal{P}$ there is no forgotten-forced answer to l. In particular, $\mathcal{P}$ is W^{no}-compatible for $W := l \times \widetilde{V}_l$.

Proof. By regularity. □

The next lemma does not need regularity of Γ^*. In below, $\mathcal{P}(Z)$ denotes the sub-path from node Z if $Z \in \mathcal{P}$; a subset W of $\{\ (l,v) \mid (l,v) \in [\widetilde{k}\ ] \times \widetilde{V}_l\ \}$ is called a *query set*.

Lemma 4.5. For any query set W, node Z and eligible path $\mathcal{R}$ from P^* to Z,

$$\Pr[\,\boldsymbol{\mathcal{P}}(Z) \text{ is } W^\theta\text{-compatible}, |\text{random}(\boldsymbol{\mathcal{P}}(Z)) \cap W| \geq a \mid \mathcal{R} \subset \boldsymbol{\mathcal{P}}] \leq \begin{cases} p^a, & \text{if } \theta = yes; \\ (1-p)^a, & \text{if } \theta = no. \end{cases}$$

Proof. We prove for $\theta = no$; the other is the same. Suppose $\mathcal{P}$ is in the support of the event in the Lemma. On $\mathcal{P}(Z)$, any query $(l,v)?$ with $(l,v) \in W$ must be answered No by compatibility. Let $\Pr_{\mathcal{R},Z,a}$ denote the probability in the lemma (with W fixed).

We pass the probability $\Pr_{\mathcal{R},Z,a}$ to the two or one possible successor(s) of Z. Suppose the query at Z is $(l_1,v_1)?$. If $(l_1,v_1) \notin W$ or the answer is forced-No (which can be decided given $\mathcal{R}, Z$), then the probability passes to the successor(s) with a unchanged. Otherwise the answer must be a random-No, and so $\Pr_{\mathcal{R},Z,a} = (1-p) \cdot \Pr_{\mathcal{R}',Z',a-1}$, with $\mathcal{R}'$ extending $\mathcal{R}$ by $Z \to Z'$, where Z' is the unique possible successor. Induction on Z (from below) completes the proof. □

We continue to bound probability of paths. As it turns out, if $\boldsymbol{\mathcal{P}}$ has a node P with large $|P_1|$, then it can be handled by Lemma 4.5 (*type-1* in the proof of Theorem 4.4). The other case is harder; we need a technical lemma, which follows the analysis in [2].

Lemma 4.6. Suppose n is large enough. Then $\forall l \in [\ \widetilde{k}\ ]$,

$$\Pr[\,\boldsymbol{\mathcal{P}} \text{ ends in } C_l, \forall P \text{ on } \boldsymbol{\mathcal{P}}\ |P_1| < r/2\ ] < |\Gamma^*|^2 \cdot n^{-\epsilon k/3t^2-1}. \tag{4.17}$$

Proof. Due to item (1) in Stage II's strategy, there are at most $\widetilde{k}$ Yes-answers along any support of $\boldsymbol{\mathcal{P}}$. Given such a $\mathcal{P}$, divide it into consecutive segments $\mathcal{P}^1 \cup ... \mathcal{P}^{2t}$, such that $|(\mathcal{P}^i)_1| \leq \lceil \frac{\widetilde{k}}{2t} \rceil \leq tr/2$, $\forall i \in [2t]$. Here recall $(\mathcal{P}^i)_1$ is defined by (4.14). Below we consider $(\mathcal{P}^i)_0(l)$; note by choice of l, $\bigcup_{i\in[2t]} (\mathcal{P}^i)_0(l) = \widetilde{V}_l$.

By Lemma 4.2, $\widetilde{V}_l$ is $(2tr, 2tq)^V$-neighbor-dense. We claim that, one of $(P^i)_0(l)$, say $(\mathcal{P}^{i^*})_0(l)$, is $(r,q)^V$-neighbor-dense. This can be seen by contradiction: otherwise, we can collect a union of $2t$ many sets all of which have size r, and together has $< q \cdot 2t$ many common neighbors in $\widetilde{V}_l$—contradicting the $(2tr, 2tq)^V$-neighbor-denseness.

Fix such an i^* for $\mathcal{P}$. Let Z, Z' be the start and end nodes of $\mathcal{P}^{i^*}$, decided by $\mathcal{P}$ in some fixed way. For simplicity, let $\text{sel}(\mathcal{P}) := (Z, Z')$, $A := \text{Im}(Z_1) \cup \text{Im}((\mathcal{P}^{i*})_1)$, and

$$\boldsymbol{\mathcal{P}}^< := \text{“}\boldsymbol{\mathcal{P}} \text{ ends in } C_l, \forall P \text{ on } \boldsymbol{\mathcal{P}}, |P_1| < r/2\text{”} \ (=\text{the event in the lemma}). \tag{4.18}$$

As $\mathcal{P}$ ends in C_l, by regularity of Γ^*, $(\mathcal{P}^{i*})_0(l) = Z'_0(l) \backslash Z_0(l)$. Thus,

$$\text{LHS of (4.17)} = \Pr[\,\boldsymbol{\mathcal{P}}^<,\ |\hat{N}_{\boldsymbol{Z'}_0 \backslash \boldsymbol{Z}_0}(\boldsymbol{A})| \geq q'\ ] + \Pr[\,\boldsymbol{\mathcal{P}}^<,\ |\hat{N}_{\boldsymbol{Z'}_0 \backslash \boldsymbol{Z}_0}(\boldsymbol{A})| < q'\ ] \tag{4.19}$$

(4.20)

$$\leq \sum_{Z,Z'\in\Gamma} \Pr[\ \boldsymbol{\mathcal{P}}^{<}, \mathrm{sel}(\boldsymbol{\mathcal{P}}) = (Z,Z'), |\hat{N}_{Z_0'\setminus Z_0}(\boldsymbol{A})| \geq q'\ ] + \Pr[\ \boldsymbol{\mathcal{P}}^{<}, \mathrm{sel}(\boldsymbol{\mathcal{P}}) = (Z,Z'), |\hat{N}_{Z_0'\setminus Z_0}(\boldsymbol{A})| < q'\ ]$$

For fixed $Z, Z' \in \Gamma$, we only need to bound the two terms of (4.20).

first term. By Lemma 4.4, any No-answer in $(\mathcal{P}^i)_0(l)$ 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 $\boldsymbol{\mathcal{P}}^{0,i^*}(l)$ are all random. Also, by Lemma 4.4, any path to C_l is W^{no}-compatible, with $W := \{l\} \times \widetilde{V}$. So the event of this term implies event

$$E := \text{ “}\boldsymbol{\mathcal{P}} \text{ is } W^{no}\text{-compatible, } \mathrm{random}(\boldsymbol{\mathcal{P}}) \cap W| \geq q'\text{.”}$$

By Lemma 4.5 (with $Z \leftarrow P^*$), $\Pr[E] \leq (1-p)^{q'} < \exp(-n^{2\epsilon k}/32t) < n^{-\epsilon k}$ by (4.4).

second term. By choice of i^*, $Z_0'\setminus Z_0$ is $(r,q)^V$-neighbor-dense. Now $|\boldsymbol{A}| \leq r/2 + tr/2 < tr$. By (tr, r, q', s)-mostly-denseness of G and Lemma 4.3, $\exists S \subset \widetilde{V}$ of size $\leq s$ s.t. $|\boldsymbol{A} \cap S| \geq r$. As $|\mathrm{Im}(\boldsymbol{Z}_1)| \leq r/2$ from the event $\boldsymbol{\mathcal{P}}^{<}$, if let $\boldsymbol{S}_1 := \mathrm{Im}((\boldsymbol{\mathcal{P}}^{i^*})_1) \cap S$ then $\boldsymbol{\mathcal{P}}^{<} \Rightarrow |\boldsymbol{S}_1| \geq r/2$. Therefore, as every Yes-answer is random, this term is bounded by:

$$\sum_{S_1\subset S,\ |S_1|=r/2} \Pr[\ \{l_1\} \times S_1 \subset\ \boldsymbol{\mathcal{P}}(Z)_1 \cap \mathrm{random}(\boldsymbol{\mathcal{P}}(Z))\ ] \tag{4.21}$$

For fixed S_1, the probability is $< p^{r/2}$ by Lemma 4.5 ($W \leftarrow \{l_1\} \times S_1$, weighted-summed over all paths $\mathcal{R}$ from P^* to Z; compatibility is from the fact after Definition 4.7). Now $\binom{s}{\frac{r}{2}} p^{r/2} < (2et^2 n^{-\epsilon})^{k/(2t^2)} < n^{-\epsilon k/3t^2 - 10}$, by choice of s, p in (4.4).

The Lemma follows by a union bound over $Z, Z' \in \Gamma^*$ in (4.20). □

Now we can prove Theorem 4.4.

Proof. (*of Theorem 4.4*) Let G be $(8tr, 4tq)^{block}$-neighbor-dense and (tr, r, q', s)-mostly-dense. Suppose Γ is $\frac{1}{t}$-irregular resolution w.r.t. κ, the canonical variable partition.

By Claim 4.2, the query-answer process on Γ must stop in Stage II at an axiom like (4.16). We only need to bound $|\Gamma^*| (\leq |\Gamma|)$. Consider any path $\mathcal{P}$ in the support of $\boldsymbol{\mathcal{P}}$ in Stage II. If $\exists P \in \mathcal{P}$ with $|P_1| \geq r/2$, we call it *type-1*; otherwise it is *type-2*.

For any type-1 $\mathcal{P}$ and such P, note $(P^*)_1 = \phi$, and $P_1 \subset \mathcal{P}_1$. So if take $W := P_1$, then $\mathcal{P}$ is W^{yes}-compatible (from the fact after Definition 4.7), $|W| \geq \frac{r}{2}$. All Yes answers are random in Stage II, so by Lemma 4.5 with $Z \leftarrow P^*$, the probability of type-1 path to appear, taken over all possible such node $P \in \Gamma^*$, is $\leq |\Gamma^*| \cdot p^{\frac{r}{2}} < n^{-\epsilon k/t^2}$.

For type-2 path $\mathcal{P}$, we can apply Lemma 4.6. As a result, the probability is $\leq k \cdot |\Gamma^*|^2 \cdot n^{-\epsilon k/3t^2 - 1}$, taken union over $l \in [k]$.

Together type-1, type-2 appear with probability 1, so $|\Gamma^*| \geq n^{\epsilon k/6t^2}$. □

5. Acknowledgements

The author is indebted to Alexander Razborov and Aaron Potechin for many useful feedbacks to the early version of the paper.

References

[1] 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.

[2] 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.

[3] B. Barak, S. B. Hopkins, J. A. Kelner, P. Kothari, A. Moitra, and A. Potechin. A nearly tight sum-of-squares lower bound for the planted clique problem. *FOCS*, pages 428–437, 2016.

[4] 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.

[5] Paul Beame and Toniann Pitassi. Simplified and improved resolution lower bounds. In *Proceedings of 37th Conference on Foundations of Computer Science*, pages 274–282. IEEE, 1996.

[6] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow—resolution made simple. *Journal of the ACM (JACM)*, 48(2):149–169, 2001.

[7] Olaf Beyersdorff, Nicola Galesi, and Massimo Lauria. Parameterized complexity of DPLL search procedures. *ACM Transactions on Computational Logic (TOCL)*, 14(3):20, 2013.

[8] Armin Biere, Marijn Heule, Hans van Maaren, and Toby Walsh, editors. *Handbook of Satisfiability*, volume 185 of *Frontiers in Artificial Intelligence and Applications*. IOS Press, 2009.

[9] 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.

[10] William Cook, Collette R Coullard, and Gy Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, 1987.

[11] Rod G Downey and Michael R Fellows. Fixed-parameter tractability and completeness ii: On completeness for w [1]. *Theoretical Computer Science*, 141(1-2):109–131, 1995.

[12] 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.

[13] 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.

[14] Armin Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[15] 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.

[16] S. Hopkins, P. Kothari, A. Potechin, P. Raghavendra, and T. Schramm. Tight lower bounds for planted clique in the degree-4 sos program. *SODA*, 2016.

[17] 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.

[18] Stasys Jukna and Alexander A Razborov. Neither reading few bits twice nor reading illegally helps much. *Discrete Applied Mathematics*, 85(3):223–238, 1998.

[19] Richard M Karp. Reducibility among combinatorial problems. In *Complexity of computer computations*, pages 85–103. Springer, 1972.

[20] R. Meka, Aaron Potechin, and Avi Wigderson. Sum-of-squares lower bounds for planted clique. *STOC*, pages 87–96, 2015.

[21] Nathan Mull, Shuo Pang, and Alexander Razborov. On CDCL-based proof systems with the ordered decision strategy. To appear.
[22] Jaroslav Nešetřil and Svatopluk Poljak. On the complexity of the subgraph problem. *Commentationes Mathematicae Universitatis Carolinae*, 026,2, 1985.
[23] Pavel Pudlák. Proofs as games. *The American Mathematical Monthly*, 107(6):541–550, 2000.
[24] Alexander Razborov. Lower bounds on the monotone complexity of some boolean functions. *English translation in Soviet Math. Doklady*, 31:354–357, 1985.
[25] Alexander A Razborov. Proof complexity of pigeonhole principles. In *International Conference on Developments in Language Theory*, pages 100–116. Springer, 2001.
[26] Alexander A Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. *Annals of Mathematics*, pages 415–472, 2015.
[27] 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.
[28] Dmitry Sokolov. Dag-like communication and its applications. In *International Computer Science Symposium in Russia*, pages 294–307. Springer, 2017.
[29] Gunnar Stålmarck. Short resolution proofs for a sequence of tricky formulas. *Acta Informatica*, 33(3):277–280, 1996.
[30] Virginia Vassilevska. Efficient algorithms for clique problems. *Information Processing Letters*, 109(4):254–257, 2009.
[31] 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.

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il