Large clique is hard on average for resolution

Shuo Pang*

University of Chicago, Mathematics Department

Abstract. We prove an $\exp(\Omega(k^{(1-\epsilon)}))$ resolution size lower bound for the k-Clique problem on random graphs, for (roughly speaking) $k < n^{1/3}$. Towards an optimal resolution lower bound of the problem (i.e. of type $n^{\Omega(k)}$), we also extend the $n^{\Omega(k)}$ bound in [2] on regular resolution to a stronger model called *a-irregular resolution*, for $k < n^{1/3}$. This model is interesting in that all known CNF families separating regular resolution from general [1,24] have short proofs in it.

Keywords: Resolution· k-Clique · Random graphs· Regular resolution

1 Introduction

The *k-Clique* problem, given an input graph G and a number k, asks to decide if G contains a k-clique. As one of the fundamental NP-complete problems, its computational hardness has been intensively studied in both algorithmic and lower bound worlds ([16,19,13,25,21,23,11]). 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 the *Cook-Reckhow* systems). Given such a system Λ, the proof-theoretic version of the k-Clique problem is thus, "is there a short Λ-refutation of the CNF encoding of the fact 'G contains a k-clique'?" In this paper, Λ will be resolution or 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. (trivially there is no refutation of a correct claim, short or long); 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 [4], which is meaningful for $k > n^{5/6}$; the optimal $n^{\Omega(k)}$ size lower bounds are known for tree-like resolution [5] and regular resolution [2] (for $k < n^{\frac{1}{4}-o(1)}$).

* spang@uchicago.edu

Our results. We prove an $\exp(k^{1-\epsilon})$ average-case resolution size lower bound of k-Clique problem, when $G \sim G(n,p)$ as above (Corollary 1). This result holds for $k < n^{1/3}$, thus complements the result of [4] for smaller k's (more precisely, it holds for $k = n^{c_0}$ where c_0, ϵ are arbitrary parameters s.t. $\min\{\frac{1}{3} - c_0,\ \epsilon c_0\} > (\log n)^{-1/5}$). Our second result (Theorem 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. Like in almost all previous work, both results are stated and proved for a "strong" encoding of the problem.

Some words on the model. It is a Cook-Reckhow subsystem of resolution 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 a variant of width), so 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, it requires

> *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.

Somewhat surprisingly, it turns out (Remark 3) that all known CNF families separating regular resolution from general separate, in fact, regular resolution from this model, with a as small as $n^{-\Omega(1)}$. (On the contrary, the second result holds for constant a.)

Previously, [7] considered another extension of regular resolution called the *δ-regular resolution*, which restricts the number of irregularly-resolved variables on any path. Our restriction seems simpler in the sense that the resulting system is Cook-Reckhow. The two seem incomparable, but 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, if travel down the proof DAG with some strategy, one always ends in such a clause. By division, there are many such clauses in C (cf. the *bottleneck counting* method [12,17]). It might be possible to translate this proof into a random restriction-based argument; the current language is chosen since it works consistently for the second result, too.

The second result is built on [2] in a straightforward manner. In a given refutation, we find *one* small clause C (in the above sense) s.t. the sub-proof deriving

[1] More precisely, it is a product-subset of $[n/k]^k$; the reason is clear after seeing the strong encoding (section 2) where the vertex set is partitioned into k parts.

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 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 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.

Paper structure. We give the necessary preliminaries in section 2. In section 3 we prove the first result. In section 4 we introduce the model and then prove the second result. The paper is concluded in section 5 with some open problems.

2 Preliminaries

Graphs. $G = (V, E)$ denotes a simple, undirected graph. For $v \in V$, $N(v) = \{u \mid (u, v) \in E\}$ is the set of *neighbors of* v. 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 simplifies to $\hat{N}(B)$. A k-*clique* in G is a set $C \subseteq V$ with size k and $\forall u, v \in C, u \neq v \Rightarrow \{u, v\} \in E$. $\mathbf{G}$ denotes the n-vertex *Erdős-Rényi graph* $G(n, p)$, $0 < p < 1$, which places an edge between any two vertices with probability p independently. For $1 < k < n$, $n^{-\frac{2}{k-1}}$ is the well-known *threshold probability* [6]: $G(n, p)$ 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 paper.

Resolution and the encoding. A *literal* over a Boolean variable x is either x or its negation $\neg x$, x called the *variable* of the literal. 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 $w(C)$. $\perp$ is the contradiction/empty clause. A *CNF formula* $\tau = C_1 \wedge .... \wedge C_m$ is a conjunction of clauses. A *resolution proof from a CNF* τ is an ordered sequences $\Gamma = (D_1, ..., D_L)$ where 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*: $A \vee x,\ B \vee \neg x \vdash A \vee B$, 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*. The *size* of Γ is L, denoted by $|\Gamma|$. Γ is a *resolution refutation* if $D_L = \perp$. A resolution proof is *tree-like* if its underlying top-down proof DAG ($\perp$ at top/root) is a tree, and is *regular* if along any path from the root to axioms, no variable is resolved more than once.

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

$$\bigvee_{v \in V} x_{i,v} \qquad \forall i \in [k]; \tag{1}$$

$$\neg x_{i,u} \vee \neg x_{j,v} \qquad \forall i, j \in [k], u, v \in V \ s.t.\ i \neq j,\ \{u, v\} \notin E; \tag{2}$$

$$\neg x_{i,u} \vee \neg x_{i,v} \qquad \forall i \in [k], u, v \in V \ s.t.\ u \neq v. \tag{3}$$

[2] There is also the so-called *binary* encoding ([15]), which we will not discuss here.

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 $\forall l \in [k]$, $|C \cap V_l| \leq 1$.

$$\bigvee_{v \in V_i} x_v \qquad \forall i \in [k]; \tag{4}$$

$$\neg x_u \vee \neg x_v \qquad \forall i \neq j \in [k], u \in V_i, v \in V_j \text{ s.t. } \{u,v\} \notin E; \tag{5}$$

$$\neg x_u \vee \neg x_v \qquad \forall i \in [k],\ u,v \in V_i \text{ s.t. } u \neq v. \tag{6}$$

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 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. [20]). Finally, note a random graph from $G(n, \frac{2\xi}{k-1})$ contains $\Omega(k)$-cliques with high probability.

Remark 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 [4]). In the rest of the paper, 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 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, 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 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*

$$P_1(l) := \{\ v \in V_l \mid\ (l,v)^{yes} \in P\} \qquad P_0(l) := \{\ v \in V_l \mid\ (l,v)^{no} \in P\}. \quad (7)$$

$$P_{Live}(l) := V_l \backslash P_0(l) \qquad P_{Live} := \bigcup_{l \in [k]} P_{Live}(l). \quad (8)$$

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, such 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 2^k-type lower bound for resolution

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

$$\begin{aligned} &\xi > 1 \text{ a constant;} \\ &k = n^{c_0} \text{ where } c_0, \epsilon \in (0, 1/3) \text{ arbitrary parameters s.t.} \\ &\qquad \min\{\epsilon c_0, 1/3 - c_0\} > (\log n)^{-1/5}; \\ &N = 1 + \max\{\frac{1}{1-3c_0},\ \frac{1}{\epsilon c_0}\},\quad t = \frac{18\xi \cdot N}{1/3 - c_0}; \\ &r = \frac{k}{t},\ q = \frac{1}{2} n^{1-c_0-2\delta r} \text{ where } \delta = \frac{2\xi}{k-1}. \end{aligned} \quad (9)$$

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 2 and (27) to go through.

3.1 Graph properties

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

Definition 2. *A subset $A \subseteq V$ is called (r, q)-neighbor-dense ([5], [2]) 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 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 $W \subseteq V$, $|W| \leq a_2$,

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

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

Lemma 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 (9).*

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

$$\begin{aligned} \Pr[\ |\hat{N}_{V_j}(R)| < \frac{1}{2}q\ ] &\leq \exp(-\frac{n^{1-c_0-2\delta r}}{48}) \\ &< \exp(-n^{2c_0+\delta r}) \quad \text{since } \delta r < 1/3 - c_0 \text{ by (9).} \end{aligned} \tag{10}$$

The first "$\leq$" 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 $n^{2r} < \exp(0.5n^{2c_0} \log n)$, and $\exp(-n^{2c_0+\delta r}) \cdot \exp(0.5n^{2c_0} \log n) < \exp(-0.5\sqrt{\log n})$ since $\delta r > (\log n)^{-1/2}$ in (9).

Remark 2. Some particular graph family is also neighbor-dense, yet being far from pseudo-random. For example, consider a complete $(k-1)$-partite graph G where $2r < k_1 < k$ (r, k as in (9)), 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. [5]) 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. [5].

3.2 The lower bound proof

Theorem 2. *For parameters as in* (9) *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 1. *(of Theorem 2 and Lemma 2) Within the same parameters as in Theorem 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 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. [17]).

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. Random part. Choose a set of $\frac{r}{2}$ pigeons from $[k]$ uniformly randomly, 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:

(Distribution of $\boldsymbol{\alpha}$*) Suppose the chosen pigeons are* $l_1, ..., l_{\frac{r}{2}} \in [k]$. *Choose* $\alpha(l_1)$ *uniformly from* V, *then* $\alpha(l_2)$ *uniformly from* $\hat{N}_{V_{l_2}}(\{\alpha(l_1)\})$, $\alpha(l_3)$ *uniformly from* $\hat{N}_{V_{l_3}}(\{\alpha(l_1),\alpha(l_2)\})$ *and so on till* $\alpha(l_{\frac{r}{2}})$ *is chosen.* (11)

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. *(Narrow pigeons) Given an object* P, *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* $dom(P_1) \cup \{$*narrow pigeons in* $P\}$.

Intuitively, an object is small if it contains $\geq \frac{r}{2}$ many useful pigeons. The **invariance** 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. 1).

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

Claim 1 *If for an object P the above $(*)$ holds, then P is not an axiom.*

Proof. Direct check.

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

$$\begin{aligned}&(1)\ \text{If } |\text{useful pigeons in } P| \geq r/2, \text{ then } \textit{halt}. \text{ Otherwise,}\\ &(2)\ (2a)\ \text{If } l \in \mathrm{dom}(\alpha \cup P_1 \cup \beta), \text{ answer according to } \alpha \cup P_1 \cup \beta;\\ &\qquad (2b)\ \text{Otherwise, say "No".}\end{aligned} \tag{12}$$

Lemma 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,

$$|R| \leq |\alpha| + |\beta \cup P_1| = \frac{r}{2} + |\{\text{useful pegions}\} < \frac{r}{2} + \frac{r}{2} = r. \tag{13}$$

Moreover, $P_0(l) \cup \{v\}$ is not $(r, \frac{1}{2}q + 1)$-neighbor-dense by the case assumption. So by Lemma 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 can be now completed: we extend β so that $(*)$ holds until we halt.

The analysis. Since Γ is a correct proof, the query process must stop. By Claim 1, it could only be halted in Case (1) of (12). Let T be the set of all such halting objects (over all α) in the Γ.

Definition 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 4. *Given the distribution $\boldsymbol{\alpha} \sim \mathcal{D}$ (11), for any fixed $P \in T$*

$$\Pr[\ \boldsymbol{\alpha} \text{ leads to } P\ ] \le \exp(-\Omega(k^{1-\epsilon})) \tag{14}$$

where the parameters are as in (9).

Proof. By definition of T and Lemma 3, for P we have $|\{\text{useful pigeons}\}| \ge r/2$. Recall $r = k/t$ in (9). 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 $\boldsymbol{\alpha}$,

$$\Pr[\ |\mathrm{dom}(\boldsymbol{\alpha}) \cap \{\text{useful pigeons}\}| < \epsilon' r\ ] \tag{15}$$

$$= \sum_{a<a_0} \binom{r/2}{a}\binom{k-r/2}{r/2-a}\Big/\binom{k}{r/2} < a_0 \cdot \binom{r/2}{a_0}\binom{k-r/2}{r/2-a_0}\Big/\binom{k}{r/2}. \tag{16}$$

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 (16) $< a_0 \cdot \frac{f(a_0)}{f(2a_0)} < \epsilon' r \cdot 2^{-\epsilon' r} < \exp(-\Omega(k/t^2))$. Therefore,

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

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

$$|\mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1)| \ge \frac{\epsilon' r}{2}, \quad \text{Or} \tag{17}$$

$$|\mathrm{dom}(\boldsymbol{\alpha}) \cap (\{\text{narrow pigeons}\} \backslash \mathrm{dom}(P_1))| \ge \frac{\epsilon' r}{2}. \tag{18}$$

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, (17), 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 $\ge \frac{1}{2}n^{1-c_0-2\delta r}$ many choices of vertices for *each* such pigeon. By definition (11), $\boldsymbol{\alpha}$ chooses among them uniformly. Thus

$$\Pr[\ \boldsymbol{\alpha} \text{ leads to } P \text{ and } |\mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1)\}| \ge \epsilon' r/2\ ] \tag{19}$$

$$\le \sum_{S\subseteq[k]:\ |S|\ge\epsilon' r/2} \Pr[\mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1) = S\ \wedge\ \text{for all } i \in S,\ \boldsymbol{\alpha}(i) = P_1(i)] \tag{20}$$

$$= \sum_{S\subseteq[k]:\ |S|\ge\epsilon' r/2} \Pr[\mathrm{dom}(\boldsymbol{\alpha}) \cap \mathrm{dom}(P_1) = S\ ] \cdot \Pr[\ \text{for all } i \in S,\ \boldsymbol{\alpha}(i) = P_1(i)] \tag{21}$$

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

$$\le 1 \cdot n^{-c_0\epsilon' r} \tag{22}$$

$$= n^{-\Omega(c_0 k/t^2)}, \tag{23}$$

where equation (21) uses the independence of the two parts of $\boldsymbol{\alpha}$, and inequality (22) uses $\frac{1}{2}n^{1-c_0-2\delta r} > n^{2c_0}$ from (9).

2. In the latter case, (18), let B denote {narrow pigeons (in P)}\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,

$$\hat{N}_{P_0(i)}(\mathrm{Im}(\alpha'|_{\mathrm{dom}(\alpha'\setminus\{i\})})) \geq \frac{1}{2}q = \frac{1}{4}n^{1-c_0-2\delta r}. \tag{24}$$

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

$$\Pr[\ \boldsymbol{\alpha}(i) \notin P_0(i) \mid i \in \mathrm{dom}(\boldsymbol{\alpha})\ ] \leq 1 - \frac{n^{1-c_0-2\delta r}}{4n^{1-c_0}} = 1 - \frac{1}{4}n^{-2\delta r}. \tag{25}$$

Now we can bound the overall probability of this case by

$$\sum_{S\subseteq B,\ |S|\geq \epsilon' r/2} \Pr[\ \mathrm{dom}(\boldsymbol{\alpha}) \cap B = S \text{ and } \boldsymbol{\alpha}(i) \notin P_0(i) \text{ for all } i \in S\ ] \tag{26}$$

Similar to estimation (19), from (25) we have

$$(26) \leq (1 - \frac{1}{4}n^{-2\delta r})^{\epsilon' r/2} < \exp(-\Omega(k^{1-\epsilon}/t^2)), \tag{27}$$

where the last inequality uses $k = n^{c_0}$, $2\delta r < \epsilon c_0$ in (9).

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 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 2 is proved.

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

4.1 The model

Like before, let us view a resolution proof Γ as a top-down DAG ($\bot$ on top). A variable x is called *irregular* on a path $\mathfrak{p}$ in Γ if it is queried more than once on $\mathfrak{p}$. x is *irregular under clause* C if there is *some* path 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 5. *For $a \leq 1$, a resolution proof Γ on m variables is* **unblocked a-irregular** *if for any clause $C \in \Gamma$,*

$$w(C) \geq am \Rightarrow |\{\textit{variables irregular under } C\}| \leq am \tag{28}$$

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

We continue to the main version. Given m variables and $\kappa : \mathrm{Var} \to [k]$ a partition of variables ($1 \le k \le m$), 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

$$w^b(C) = |\mathrm{Var}(C)|^b. \tag{29}$$

Definition 6. *(***Main model***) For $a \le 1$, κ as above, a resolution proof Γ is* a**-irregular for** κ *if for any clause $C \in \Gamma$,*

$$w^b(C) \ge ak \Rightarrow |\{\textit{variables irregular under } C\})|^b \le ak. \tag{30}$$

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 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 ([1,24]) are, actually, separations between regular and the a-irregular resolution with a natural partition κ and $a = k^{-\Omega(1)}$.

Remark 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* ([1]), *Lifted pebbling formulas* ([24]), and a variation of the *Ordering principle* ([1]).

1. *Stone formulas.* Under the notation of [1], 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 [1] (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 realized in [24] 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; [24] 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

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

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 $\{r_j\}$.

Similarly 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. GT'_n, a variation of the so-called *Ordering principle*. 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 [1] 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 [1]) 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 [22] to finish, in which all clauses are either the so-called $C_m(j)$'s (in notation of [22]) or axioms, all with block-width ≤ 4. So, the refutation is $4/k$-irregular for this partition.

Remark 4. In all the examples above, the variable partition we work with 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 [18,14,10,8] and the references therein), where "blocks of variables" appear naturally. For the lifted CNF, it is reasonable to expect that the block-width measure on proofs w.r.t. this variable partition (i.e. according to the i-index) reflects the hardness of the easier, unlifted CNF which itself is often narrow. In our context, this explains the power of the model in examples 1, 2: with the correct variable partition, it has sufficient power to recover and handle the unlifted CNF, which is just easy for regular resolution. This perspective seems to say nothing about example 3, though.

The main theorem of this section is the following.

Theorem 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 $n^{k\epsilon^3/(200\xi)^2}$.*

4.2 More graph properties

Definition 7. *(relativized neighbor-denseness, Definition 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').

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

Definition 8. *([2]) $W \subseteq V$ 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 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 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 [2] is the following.

Theorem 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 $t:\ 4 \leq t \leq k$ 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 4(1) for the following parameters. Theorem 4(2) will be actually re-proved and refined following the original method (Lemma 8, 9).

Parameter regime. In the rest of Section 4, we use a parameter regime that is similar to that of [2]. As before, let $\xi > 1$ be a constant and $\delta = \frac{2\xi}{k-1}$.

$$\begin{aligned} &\epsilon = \text{any parameter in } \Big((\log n)^{-1/2},\ 1/200\Big); \\ &t = \frac{64\xi}{\epsilon}, \quad k \in \left(\frac{3t^2}{\epsilon},\ n^{1/3-40\epsilon}\right); \\ &r = \frac{4k}{t^2}, \quad q = \frac{1}{32t}n^{1-8\delta tr}/k, \quad q' = \frac{1}{4}qn^{-\delta tr}; \\ &s = k^2 n^{9\delta tr+\epsilon}, \quad p = n^{-(9\delta tr+2\epsilon)}/k. \end{aligned} \tag{31}$$

Again, we can assume k, r, q, q', s are integers, and their meaning is clear from Definition 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 compared to the original choice for Theorem 4(2) (which is about $n^{-(1+\epsilon)/2}$); this makes the two bounds in proof of Lemma 9 more balanced thus allows to slightly improve the range of k from $n^{1/4}$ to $n^{1/3}$.

Theorem 5. *With parameter regime (31), w.h.p. $\boldsymbol{G} \sim G(n, n^{-\delta})$ is*

$$\begin{aligned} &(i).\ (8tr, 4tq)^{block}\text{-neighbor-dense; and} \\ &(ii).\ (tr, r, q', s)\text{-mostly-dense.} \end{aligned} \tag{32}$$

Proof. (i) is identically proved as Lemma 2. (ii) is Theorem 4(1) except for a difference in parameters; we only have to point out that parameters (31) satisfy $n^{\epsilon/2+1} < qn^{-\delta tr}s/tr$ so can be safely replaced to their proof.

Theorem 3 thus reduces to the following.

Theorem 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* (32) *with parameters* (31)*, then any $\frac{1}{t}$-irregular resolution for $(Clique_{block}(G,k), \kappa_0)$ requires size $n^{\epsilon k/6t^2}$.*

4.3 The lower bound proof (Theorem 6)

Proof overview. As briefed in the introduction the idea is simple–use a suitable restriction to simplify the refutation to be regular. This would finish the proof (by a self-reduction) if the induced sub-graph were also pseudo-random, which is not the case. It is not far, though: the only additional observation is to use a weaker, relative pseudo-randomness (Lemma 6, 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 9. *(Narrow pigeons, with new parameters (cf. Def. 3) Suppose Γ is a resolution proof, $P \in \Gamma$ an object. A pigeon $l \in [k]$ is* **narrow in** *P if*

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

Let narrow_P denote the set of narrow pigeons in P.

Adversary strategy. Stage I (to find a restriction). Travel down the proof, and keep a live-clique assignment β_P (Definition 1) s.t.

$$\beta_P \supset P_1, \qquad \text{dom}(\beta_P) = \text{dom}(P_1) \cup \text{narrow}_P. \tag{33}$$

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

$$|\text{narrow}_P \cup \text{dom}(P_1)| \geq tr \tag{34}$$

then go to Stage II; otherwise if $l_1 \in \text{dom}(P_1) \cup \text{narrow}_P$, answer according to β_P; otherwise, answer No.

When not transit to Stage II, we show (33) holds for the next node.

Claim 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 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 2, $|\hat{N}_{P_{Live}(l_1)}(\text{Im } \beta_P)| \geq 2tq > 1$. Take a $v \in \hat{N}_{P_{Live}(l_1)}(\text{Im } \beta_P) \backslash \{v_1\}$, extend β_P by $l \to v$ then restrict it to $\text{narrow}_{P^+} \cup \text{dom}(P_1^+)$ as β_{P^+}. (33) holds for P^+.

This completes Stage I.

Claim 3 *The query-answer process must transit to Stage II at some node P.*

Proof. Similar to Claim 1: if (34) fails then P falsifies no axiom.

Stage II. Suppose we transit to this stage at node P^*.

(i). The restriction. Note $|P_1 \cup \text{narrow}_P|$ 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 4 *There exists a live-clique assignment $\widetilde{\beta}$ for P^* s.t.*

$$\widetilde{\beta} \text{ extends } \beta_{P^*} \quad \text{and} \quad \text{dom}(\widetilde{\beta}) = \text{dom}(\beta_{P^*}) \cup I_{P^*}. \tag{35}$$

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

(ii). Self-reduction to $\widetilde{G}$. Fix a $\widetilde{\beta}$ in Claim 4. Let

$$\widetilde{G} := G\,[\bigcup_{l \in [k] \backslash \text{dom}(\widetilde{\beta})} \widetilde{V}_l], \qquad \text{where } \widetilde{V}_l = \hat{N}_{P^*_{\text{Live}}(l)}(\text{Im } \widetilde{\beta}),\ l \in [k] \backslash \text{dom}(\tilde{\beta}). \tag{36}$$

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

(iii). Strategy on Γ^* (the regular case; cf. [2]). Suppose we travel down Γ^* from the root P^* along a path $\mathfrak{p}$ 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 $\mathfrak{p}$, answer No (*forgotten-forced* answer);
2. Otherwise, if $v_1 \notin \hat{N}(\text{Im } Q_1)$, 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 (36). Assume w.l.o.g.

$$\text{dom}(\widetilde{\beta}) = [\tilde{k} + 1, k].$$

The vertex-set size $|\widetilde{V}|$ will not be important, as the lower bound depends only on the pseudorandomness from Lemma 5, 6.

Lemma 5. *Assume G is $(8tr, 4tq)^{block}$-neighbor-dense (t, q as in (31)). 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. Fix such an l. As in the proof of Claim 2, we apply Lemma 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 $l \notin \mathrm{dom}(\widetilde{\beta}) \supset \mathrm{dom}(\mathrm{narrow}_{P^*})$. As a result we have

$$P^*_{\mathrm{Live}}(l) \text{ is } (4tr, 2tq)\text{-neighbor-dense in } V. \tag{37}$$

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

$$|\hat{N}_{\widetilde{V}_l}(R)| \overset{\text{by def.}}{=} |\hat{N}_{\hat{N}_{P^*_{\mathrm{Live}}(l)}(\mathrm{Im}(\widetilde{\beta}))}(R)| = |\hat{N}_{P^*_{\mathrm{Live}}(l)}(\mathrm{Im}\ \widetilde{\beta}\ \cup R)| \overset{\text{by (37)}}{\geq} 2tq. \tag{38}$$

The Lemma is proved.

Lemma 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 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 5. This relative property is weaker than (tr, r, q', s)-mostly-denseness of $\tilde{G}$: $\{(r,q)^V\text{-neighbor-dense sets in } \widetilde{V}\} \subseteq \{(r,q)^{\widetilde{V}}\text{-neighbor-dense sets in } \widetilde{V}\}$).

The analysis. Now we use the method in [2] to show regular resolution lower bound on $\widetilde{G}$. The key part is Lemma 8 and Lemma 9 in below.

Notation. Let $\mathfrak{p}$ 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 a path $\mathfrak{p}$, $\mathfrak{p}(Z)$ denotes the sub-path from Z. For an eligible $\mathfrak{p}$, similar to Definition 1, let

$$\mathfrak{p}_1 = \{\ (l,v) \mid (l,v)^{yes} \text{ is answered along } \mathfrak{p}\ \}, \text{ and similarly } \mathfrak{p}_0; \tag{39}$$

$$\mathrm{rand}(\mathfrak{p}) = \{\ (l,v) \mid (l,v)? \text{ is answered randomly along } \mathfrak{p}\ \}. \tag{40}$$

$\mathfrak{p}_0(l) := \{v \mid (l,v) \in \mathfrak{p}_0\}$. A subset of $\{(l,v) \mid v \in \widetilde{V}_l, l \in [\widetilde{k}]\}$ is called a *query set.*

Definition 10. *Let X be a query set. A path $\mathfrak{p}$ is X^{yes}-compatible if $X \cap \mathfrak{p}_0 = \emptyset$, and is X^{no}-compatible if $X \cap \mathfrak{p}_1 = \emptyset$.*

So, if Γ^* is regular then $\mathfrak{p}_1 \cap \mathfrak{p}_0 = \emptyset$, meaning $\mathfrak{p}$ is $\mathfrak{p}_1^{yes}$- and $\mathfrak{p}_0^{no}$-compatible.

It is easy to verify: any eligible path $\mathfrak{p}$ to axioms must end in a *clique axiom*

$$C_l := \bigvee_{v \in V_l} x_v \qquad l \in [\ \widetilde{k}\ ]. \tag{41}$$

Lemma 7. *If $\mathfrak{p}$ is an eligible path to axiom C_l in* (41)*, then along $\mathfrak{p}$ there is no forgotten-forced answer to l. In particular, $\mathfrak{p}$ is X^{no}-compatible for $X = \{l\} \times \widetilde{V}_l$.*

Proof. By regularity.

So it suffices to upper bound the probability $\Pr[\ \mathfrak{p}$ ends in $C_l\ ]$, $\forall l \in [\tilde{k}]$, which is done by the following two lemmas. Note Lemma 8 actually holds without assuming regularity.

Lemma 8. *For any query set X and eligible path $\mathfrak{q}$ from P^* to Z,*

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

Proof. We prove for $\theta = no$; the other is the same. Suppose $\mathfrak{p}$ is in the support of the event in the Lemma. On $\mathfrak{p}(Z)$, any query (l, v)? with $(l, v) \in X$ must be answered No by compatibility. Let $\Pr_{\mathfrak{q},Z,a}$ denote the probability in the lemma (X fixed). When Z is an axiom then $a = 0$ so the conclusion is obvious.

We pass the probability $\Pr_{\mathfrak{q},Z,a}$ to the one or two possible successor(s) of Z, hence use reverse-induction on the length of $\mathfrak{q}$. Suppose the query at Z is (l_1, v_1)?. If $(l_1, v_1) \notin X$ or the answer is a forced-No (which can be decided given $\mathfrak{q}, Z$), then the probability passes to the successor(s) with a unchanged. Otherwise, the answer is a random-No, and $\Pr_{\mathfrak{q},Z,a} = (1-p) \cdot \Pr_{\mathfrak{q}',Z',a-1}$, where $\mathfrak{q}'$ extends $\mathfrak{q}$ by $Z \to Z'$, and Z' is the unique possible successor. The inductive hypothesis on $\mathfrak{q}'$ completes the proof.

Lemma 9. $\forall l \in [\ \widetilde{k}\ ]$,

$$\Pr[\ \mathfrak{p} \text{ ends in axiom } C_l, (\forall Z \text{ on } \mathfrak{p})\ |Z_1| < r/2\ ] < |\Gamma^*|^2 \cdot n^{-\epsilon k/3t^2 - 1}. \quad (42)$$

Proof. (cf. [2]) Due to item (1) in Stage II's strategy, there are at most $\widetilde{k}$ Yes-answers along any support of $\mathfrak{p}$. Given such a $\mathfrak{p}$, divide it into consecutive segments $\mathfrak{p}^1 \cup ... \mathfrak{p}^{2t}$, such that $|(\mathfrak{p}^i)_1| \leq \lceil \frac{\widetilde{k}}{2t} \rceil \leq tr/2$, $\forall i \in [2t]$. Here recall $(\mathfrak{p}^i)_1$ is defined by (39). Below we consider $(\mathfrak{p}^i)_0(l)$; note by choice of l, $\bigcup_{i \in [2t]} (\mathfrak{p}^i)_0(l) = \widetilde{V}_l$.

We claim that one of $(P^i)_0(l)$, say $(\mathfrak{p}^{i^*})_0(l)$, is $(r, q)^V$-neighbor-dense (similar to lemma 1). This can be seen by contradiction: 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 5. Fix such an i^* for $\mathfrak{p}$.

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

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

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

$$\text{LHS of (42)} = \Pr[\ \mathfrak{p}^<,\ |\hat{N}_{\boldsymbol{Z'}_0 \backslash \boldsymbol{Z}_0}(\boldsymbol{A})| \geq q'\ ] + \Pr[\ \mathfrak{p}^<,\ |\hat{N}_{\boldsymbol{Z'}_0 \backslash \boldsymbol{Z}_0}(\boldsymbol{A})| < q'\ ] \quad (43)$$

$$= \sum_{Z, Z' \in \Gamma} \Big(\Pr[\ \mathfrak{p}^<,\ \mathrm{pair}(\mathfrak{p}) = (Z, Z'), |\hat{N}_{Z'_0 \backslash Z_0}(\boldsymbol{A})| \geq q'\ ] + \Pr[\ \mathfrak{p}^<, \mathrm{pair}(\mathfrak{p}) = (Z, Z'), |\hat{N}_{Z'_0 \backslash Z_0}(\boldsymbol{A})| < q'\ ] \Big).$$

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

First term. By Lemma 7, any No-answer in $(\mathfrak{p}^i)_0(l)$ 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 $\mathfrak{p}^{0,i^*}(l)$ are all random. Also, by Lemma 7, any path to C_l is X^{no}-compatible, with $X := \{l\} \times \widetilde{V}$. So the event of this term implies event

$$E := \text{ “}\mathfrak{p} \text{ is } X^{no}\text{-compatible, } |\mathrm{rand}(\mathfrak{p}) \cap X| \geq q'\text{.”}$$

By Lemma 8 (with $Z \leftarrow P^*$),

$$\Pr[E] \leq (1-p)^{q'} < \exp(-pq') < \exp(-n^{1-2\epsilon-20\delta tr}/(64tk^2)) < n^{-\epsilon k} \tag{44}$$

by (31) since $\delta tr < \epsilon$, $k < n^{1/3-40\epsilon}$ and that $\epsilon > (\log n)^{-1/3}$.

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 6, $\exists S \subseteq \widetilde{V}$ of size $\leq s$ s.t. $|\boldsymbol{A} \cap S| \geq r$. As $|\mathrm{Im}(Z_1)| \leq r/2$ in the event $\mathfrak{p}^<$, if let $\boldsymbol{S}_1 = \mathrm{Im}((\mathfrak{p}^{i^*})_1) \cap S$ then $\mathfrak{p}^< \Rightarrow |\boldsymbol{S}_1| \geq r/2$. Therefore, as every Yes-answer is random, this term is bounded by

$$\sum_{S_1 \subseteq S,\ |S_1| = r/2} \Pr[\ \{l_1\} \times S_1 \subseteq\ \mathfrak{p}(Z)_1 \cap \mathrm{rand}(\mathfrak{p}(Z))\ ]. \tag{45}$$

For any fixed S_1, this is $< p^{r/2}$ by Lemma 8 (where the compatibility condition is from the fact after Definition 10). Now $\binom{s}{\frac{r}{2}} p^{r/2} < (2et^2 n^{-\epsilon})^{k/t^2} < n^{-\epsilon k/3t^2 - 10}$, by the choice of s, p in (31).

The lemma follows by a union bound over $Z, Z' \in \Gamma^*$ in (43).

Theorem 6 is now a straightforward corollary.

Proof. (*of Theorem 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, we only need to bound $|\Gamma^*| (\leq |\Gamma|)$. Consider an eligible path $\mathfrak{p}$ down from P^*. If for some Q on $\mathfrak{p}$, $|Q_1| \geq r/2$, we call $\mathfrak{p}$ *type-1*; otherwise it is *type-2*.

For a type-1 $\mathfrak{p}$, fix such a node Q. $\mathfrak{p}$ is Q_1^{yes}-compatible (by $Q_1 \subseteq \mathfrak{p}_1$ and the fact after Def. 10), $|Q_1| \geq \frac{r}{2}$. Yes-answers are random in Stage II so Lemma 8 applies to the sub-path from P^* to Q (with $X \leftarrow Q_1$). By a union bound over all possible Q's, this implies 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 $\mathfrak{p}$, by Lemma 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 $|\Gamma^*| \geq n^{\epsilon k/6t^2}$.

5 Conclusion and open Problems.

We proved the $\exp(\Omega(k^{1-\epsilon}))$ resolution lower bound for $Clique_{block}(G,k)$ on random graphs, for $k < n^{1/3}$. We also defined the model of a-irregular resolution, discussed its relative power to regular and general resolution and extended the $n^{\Omega(k)}$ lower bound to this model. Some open problems are in order.

1. Prove the $n^{\Omega(k)}$ lower bound for general resolution. This improvement (from 2^k to n^k) is especially meaningful for small values of k, say $O(\log n)$.

2. Are there candidate families separating $\Omega(1)$-irregular model from general resolution? A possible starting point is to note that the concept of *block-width* has appeared in special forms in the study of many interesting CNFs (see e.g. [3,9]), either with or without lifting (although it seems unclear, in this context, how useful the lifting technique is; see Remark 4). Regarding the relation with the model in [7], does their SETH result hold for our unblocked model?

3. Extend the 2^k-type result to stronger systems, for example, *Res(k)* (where k has a completely different meaning) and algebraic systems like *Polynomial Calculus* and *Cutting Planes*. Does it hold for resolution but with other pseudo-random graphs (e.g. *Ramsey graphs* [15])?

Acknowledgment. I am indebted to Alexander Razborov for many helpful communications and feedback on the early draft. My thanks also go to Aaron Potechin, Jakob Nordström, and Ilario Bonacina, for various comments and references, and to the anonymous referees for their extensive feedback and suggestions that undoubtedly help improve readability.

References

1. Alekhnovich, M., Johannsen, J., Pitassi, T., Urquhart, A.: An exponential separation between regular and general resolution. In: Proceedings of the thiry-fourth annual ACM symposium on Theory of computing. pp. 448–456. ACM (2002)
2. Atserias, A., Bonacina, I., de Rezende, S.F., Lauria, M., Nordström, J., Razborov, A.: Clique is hard on average for regular resolution. Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing pp. 866–877 (2018)
3. Atserias, A., Müller, M.: Automating resolution is np-hard. Journal of the ACM (JACM) **67**(5), 1–17 (2020)
4. Beame, P., Impagliazzo, R., Sabharwal, A.: The resolution complexity of independent sets and vertex covers in random graphs. computational complexity **16**(3), 245–297 (2007)
5. Beyersdorff, O., Galesi, N., Lauria, M.: Parameterized complexity of DPLL search procedures. ACM Transactions on Computational Logic (TOCL) **14**(3), 20 (2013)
6. Bollobás, B., Erdös, P.: Cliques in random graphs. In: Mathematical Proceedings of the Cambridge Philosophical Society. vol. 80, pp. 419–427. Cambridge University Press (1976)
7. Bonacina, I., Talebanfard, N.: Strong eth and resolution via games and the multiplicity of strategies. Algorithmica **79**(1), 29–41 (2017)
8. Garg, A., Göös, M., Kamath, P., Sokolov, D.: Monotone circuit lower bounds from resolution. In: Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing. pp. 902–911. ACM (2018)
9. Göös, M., Koroth, S., Mertz, I., Pitassi, T.: Automating cutting planes is np-hard. In: Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing. pp. 68–77 (2020)
10. Göös, M., Pitassi, T.: Communication lower bounds via critical block sensitivity. SIAM Journal on Computing **47**(5), 1778–1806 (2018)

11. Hajiaghayi, M.T., Khandekar, R., Kortsarz, G.: Fixed parameter inapproximability for clique and setcover in time super-exponential in opt. arXiv preprint arXiv:1310.2711 (2013)
12. Haken, A.: The intractability of resolution. Theoretical Computer Science **39**, 297–308 (1985)
13. Hastad, J.: Clique is hard to approximate within $n^{1-\epsilon}$. In: Proceedings of 37th Conference on Foundations of Computer Science. pp. 627–636. IEEE (1996)
14. Huynh, T., Nordstrom, J.: 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. pp. 233–248 (2012)
15. Lauria, M., Pudlák, P., Rödl, V., Thapen, N.: The complexity of proving that a graph is ramsey. Combinatorica **37**(2), 253–268 (2017)
16. Nešetřil, J., Poljak, S.: On the complexity of the subgraph problem. Commentationes Mathematicae Universitatis Carolinae **026,2** (1985)
17. Pudlák, P.: Proofs as games. The American Mathematical Monthly **107**(6), 541–550 (2000)
18. Raz, R., McKenzie, P.: Separation of the monotone nc hierarchy. In: Proceedings 38th Annual Symposium on Foundations of Computer Science. pp. 234–243. IEEE (1997)
19. Razborov, A.: Lower bounds on the monotone complexity of some boolean functions. English translation in Soviet Math. Doklady **31**, 354–357 (1985)
20. Razborov, A.A.: Proof complexity of pigeonhole principles. In: International Conference on Developments in Language Theory. pp. 100–116. Springer (2001)
21. Rossman, B.: On the constant-depth complexity of k-clique. In: Proceedings of the fortieth annual ACM symposium on Theory of computing. pp. 721–730. ACM (2008)
22. Stålmarck, G.: Short resolution proofs for a sequence of tricky formulas. Acta Informatica **33**(3), 277–280 (1996)
23. Vassilevska, V.: Efficient algorithms for clique problems. Information Processing Letters **109**(4), 254–257 (2009)
24. Vinyals, M., Elffers, J., Johannsen, J., Nordström, J.: Simplified and improved separations between regular and general resolution by lifting. In: International Conference on Theory and Applications of Satisfiability Testing. pp. 182–200. Springer (2020)
25. Zuckerman, D.: 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. pp. 681–690. ACM (2006)