THE MONOTONE COMPLEXITY OF K-CLIQUE ON RANDOM GRAPHS

BENJAMIN ROSSMAN*

Abstract. We present lower and upper bounds showing that the average-case complexity of the k-Clique problem on monotone circuits is $n^{k/4+O(1)}$. Similar bounds for AC^0 circuits were shown in [18, 5].

Key words. clique, monotone circuits, average-case complexity, quasi-sunflowers

AMS subject classifications. 68Q17, 68Q87

1. Introduction.

For a fixed constant $k \geq 3$, the *k-clique problem* (denoted k-Clique) is the problem of determining whether a graph of size n contains a complete subgraph of size k. Razborov [16] in 1985 showed that the *worst-case* complexity of k-Clique on monotone circuits is $\widetilde{\Omega}(n^k)$, nearly matching the trivial $O(n^k)$ upper bound. In this paper, we prove the first (and nearly optimal) lower bounds for the *average-case* complexity of k-Clique on monotone circuits. For the average-case analysis, we consider Erdős-Rényi random graphs $G(n,p)$ where $p = p(n)$ is a *threshold* for the existence of k-cliques (i.e., such that $\Pr[G(n,p)$ contains a k-clique$]$ is bounded away from 0 and 1). In previous work [18], we showed a lower bound of $\Omega(n^{k/4})$ on the size of AC^0 circuits (i.e., polynomial-size constant-depth Boolean circuits) which solve k-Clique with high probability on $G(n,p)$ for any single threshold p. Here we show a similar $\Omega(n^{k/4})$ lower bound for monotone circuits which solve k-Clique with high probability on $G(n,p)$ at two sufficiently separated thresholds p, such as $n^{-2/(k-1)}$ and $2n^{-2/(k-1)}$. In both results, the exponent $k/4$ is tight up to an additive constant, as shown by Amano [5] for AC^0 circuits and here for monotone circuits.

Our results support a widely held belief that Erdős-Rényi random graphs are a source of hard instances for clique problems. This idea goes back to a question raised by Karp [15] in 1976. It is well-known that the uniform random graph $G(n,1/2)$ has maximum cliques of expected size $(2-o(1))\log n$. While finding the *maximum* cliques in $G(n,1/2)$ appears to be hard, Karp pointed out that *maximal* cliques of expected size $(1-o(1))\log n$ are easy to find via a simple greedy algorithm: starting with any vertex v_1, choose any neighbor v_2 of v_1, then any common neighbor v_3 of v_1 and v_2, etc., in this way building up a clique as far as possible. Karp asked whether any polynomial-time algorithm finds a clique of size $(1+\varepsilon)\log n$ in $G(n,1/2)$ with high probability for any constant $\varepsilon > 0$. This question remains wide open today, despite a lot of research on algorithms for finding cliques in $G(n,1/2)$ (including in the setting of a large planted clique, see [2]). The failure to find efficient algorithms has even led cryptographic protocols (for example [13]) based on the hypothesis that finding hidden cliques is hard-on-average. Our results give the first strong evidence for this hypothesis by way of unconditional lower bounds.

1.1. Previous Bounds for k-Clique on Monotone Circuits.

It has long been observed that k-Clique is solved by monotone DNFs (OR-AND circuits) of size $O(n^k)$. The first (worst-case) lower bounds for k-Clique on monotone circuits were shown by Razborov in a seminal paper [16], which introduced the technique

[*] Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8550, Japan. Partially supported by NSF MSPRF grant DMS-1004484.

known as Approximation Method. For constant values of k, Razborov's bound of $\Omega((n/\log^2 n)^k)$ was later improved to $\Omega((n/\log n)^k)$ by Alon and Boppana [1]; these papers also give lower bounds in the setting where $k = k(n)$ is a growing function of n. Applying the Approximation Method to mildly non-monotone circuits, Amano and Maruoka [6] proved lower bounds for k-Clique on Boolean circuits with a small number ($(1/6)\log\log n$) of NOT gates. A different approach via communication complexity was used by Goldmann and Håstad [10] to bound the size of monotone formulas solving k-Clique.

1.2. Our Results. We now state our results (for formal definitions, see §2). Let k be a fixed but arbitrary integer ≥ 3. Let $p(n) = \Theta(n^{-2/(k-1)})$ be a fixed threshold function for the existence of k-cliques in the Erdős-Rényi random graph $G(n,p)$ (i.e., such that $\Pr[G(n,p)$ contains a k-clique] is bounded away from 0 and 1). Let $p^+ = p + p^{1+(1/k^2)}$ and note that p^+ is also a threshold for the existence of k-cliques (see §2.4).

We consider monotone circuits with arbitrary depth and AND and OR gates of unbounded fan-in, where *size* refers to the number of gates. We say that a circuit C *solves* k-Clique *w.h.p. (with high probability) on* $G(n,p)$ if

$$\lim_{n\to\infty} \Pr_{\boldsymbol{G}\sim G(n,p)}[\mathsf{C} \text{ outputs 1 on } \boldsymbol{G} \Leftrightarrow \boldsymbol{G} \text{ contains a } k\text{-clique}] = 1.$$

The following theorems first appeared in conference papers [18, 20] and the author's Ph.D. thesis [19].

Theorem 1.1 (Lower Bound for Bounded-Depth Circuits). *Boolean circuits of size $O(n^{k/4})$ and depth at most $k^{-2}\log n/\log\log n$ cannot solve k-Clique w.h.p. on $G(n,p)$.*

Theorem 1.2 (Lower Bound for Monotone Circuits). *Monotone circuits of size $O(n^{k/4})$ cannot solve k-Clique w.h.p. on both $G(n,p)$ and $G(n,p^+)$.*

Theorem 1.3 (Matching Upper Bound). *There exist monotone circuits of size $n^{k/4+O(1)}$ and depth $3k$ which solve k-Clique w.h.p. on $G(n,q)$ for all functions $q : \mathbb{N} \to [0,1]$.*

In this paper, we present complete proofs of Theorems 1.2 and 1.3. Some remarks on these results:

(a) Theorems 1.1, 1.2 and 1.3 respectively concern circuits which solve k-Clique w.h.p.
   (i) on $G(n,p)$ (i.e., at a single threshold),
   (ii) on $G(n,p)$ and $G(n,p^+)$ (i.e., at two thresholds with a "gap" of $p^{1+(1/k^2)}$),
   (iii) on $G(n,q)$ for all functions $q : \mathbb{N} \to [0,1]$.

   Clearly (iii) ⇒ (ii) ⇒ (i). Condition (i) is perhaps the most natural interpretation of "average case" in the context of k-Clique. However, condition (iii) is also reasonable to consider, especially for showing upper bounds. In fact, to pin down the average-case complexity of k-Clique in a very strong sense, it is desirable to have matching lower and upper bounds for circuits satisfying (i) and (iii), respectively. Note that Theorems 1.1 and 1.3 give precisely such a pair of bounds for the class of AC^0 circuits.

(b) The intermediate condition (ii) is introduced as a technical hypothesis in order to state Theorem 1.2 (our lower bound for monotone circuits) in the strongest terms that the proof entails. Together with Theorem 1.3, this establishes that $n^{k/4+O(1)}$ is the average-case complexity of k-Clique in the sense of condition (iii).

(c) We conjecture that $n^{k/4+O(1)}$ is the average-case complexity of k-Clique in the sense of condition (i) as well, i.e., that monotone circuits of size $O(n^{k/4})$ cannot solve k-Clique w.h.p. on $G(n,p)$. This conjecture and the related challenge of reducing the "gap" $p^+ - p$ $(= p^{1+(1/k^2)})$ in Theorem 1.2 are discussed in §11.

(d) Random graphs $G(n,p)$ and $G(n,p^+)$ have statistical distance $1-o(1)$ as probability distributions. They are nevertheless "close" from the standpoint of the k-Clique problem: the numbers of k-cliques in $G(n,p)$ and $G(n,p^+)$ are asymptotically equivalent Poisson random variables (see §2.4).

(e) Condition (ii) is equivalent to solving k-Clique w.h.p. on a single distribution, namely the random graph $G(n,q)$ where the parameter q is uniform in $\{p,p^+\}$ (or, alternatively, uniform in $[p,p^+]$). In this way, Theorem 1.2 can be restated in terms of a single distribution.

(f) The monotone circuits constructed in the proof of Theorem 1.3 are based on non-monotone AC^0 circuits due to Amano [5] (which we describe in §10).

(g) Although the lower bounds for AC^0 and monotone circuits (Theorems 1.1 and 1.2) rely on different combinatorial techniques, the exponent $k/4$ arises from a common bottleneck (the "medium patterns" described in §5).

Preliminary to proving Theorem 1.2, we first show a result involving a different pair of random graphs. Let $\delta = 1/k^2$ and note that the random graph $G(n,p^{1+\delta})$ is almost surely k-clique-free, i.e., $p^{1+\delta} = o(n^{-2/(k-1)})$ is sub-critical for the existence of k-cliques (see Lemma 2.2).

Theorem 1.4. *Let* C *be a monotone circuit of size* $O(n^{k/4})$ *and suppose that* C *outputs* 1 *on almost all k-cliques (i.e., n-vertex graphs consisting of a single k-clique with no additional edges). Then* C *outputs* 1 *on* $G(n,p^{1+\delta})$ *almost surely (in fact, with probability* $1-\exp(-\Omega(n^\delta))$*).*

Remark 1.5. Unpacking the asymptotic notation, Theorem 1.4 says: for all constants $c_1, \varepsilon > 0$, there is a constant $c_2 > 0$ such that if C is a monotone circuit of size $\leq c_1 n^{k/4}$ which outputs 1 on $1-\varepsilon$ fraction of k-cliques, then C outputs 1 on $G(n,p^{1+\delta})$ with probability $1-\exp(-c_2 n^\delta)$.

Our proof of Theorem 1.4 uses the Approximation Method of Razborov [16]. A key technical step in the proof involves a new combinatorial notion of *quasi-sunflowers*, a relaxation of sunflowers in which petals may overlap to a limited extent. A "Quasi-sunflower Lemma" (Theorem 4.4) plays a role in our proof analogous to the role of the Erdős-Rado Sunflower Lemma in previous worst-case monotone lower bounds for k-Clique. Our results also rely on subtle properties of Erdős-Rényi random graphs at the k-Clique threshold, as well as a special class of bottleneck shapes ("medium patterns") that also play a role in the AC^0 setting [18]. In addition, we introduce a technique for converting lower bounds for circuits with fan-in 2 into nearly equivalent lower bounds for circuits with unbounded fan-in.

1.3. Outline of the Paper.

In §2 we state basic definitions and a few probabilistic lemmas. In §3 we give an overview of the general Approximation Method. In §4 we define *quasi-sunflowers* and prove a "Quasi-sunflower Lemma". In §5 we introduce a convenient classification of graphs into three "sizes" (small, medium and large). Our lower bounds (Theorems 1.2 and 1.4) are proved in §6–§8 for the special case of monotone circuits in which all gates have fan-in 2. In §9 we remove the fan-in restriction, extending our lower bounds to arbitrary monotone circuits. Our matching upper bound (Theorem 1.3) is proved in §10. We state some conclusions and open questions in §11.

2. Preliminaries. Let $k \geq 3$ be an arbitrary but fixed integer. Let n be an arbitrary (but "growing") integer and let $[n] = \{1, \dots, n\}$. Expressions *with high probability* (*w.h.p.*) and *almost surely* mean with probability tending to 1 as $n \to \infty$. For a set X and integer $t \geq 0$, $\binom{X}{t}$ denotes the set of t-element subsets of X. $\log(\cdot)$ denotes the base-2 logarithm and $\ln(\cdot)$ denotes the natural logarithm.

2.1. Graphs and patterns. Graphs in this paper are finite simple graphs. Formally, a graph is a pair $G = (V_G, E_G)$ where V_G is a finite set and $E_G \subseteq \binom{V_G}{2}$. We denote by $\mathscr{G}_n$ the set of graphs with vertex set $[n]$. By default, ***graphs*** are elements of $\mathscr{G}_n$. The term ***pattern*** refers to a (constant-size) graph with no isolated vertices; all patterns we consider in this paper have size $\leq k$. (Unlike graphs in $\mathscr{G}_n$, patterns are only important up to isomorphism.)

For $\ell \in \mathbb{N}$, K_ℓ denotes the complete pattern with vertex set $\{1, \dots, \ell\}$ and edge set $\binom{\{1,\dots,\ell\}}{2}$. An *$\ell$-clique* in a graph G is a set of ℓ vertices with all $\binom{\ell}{2}$ possible edges present (i.e., a copy of the pattern K_ℓ in G). For graphs as well as patterns, $\cup$ denotes the union operation and $\subseteq$ denotes the subgraph/subpattern relation.

2.2. Monotone functions and minterms. A *(boolean) graph function* is a function from $\mathscr{G}_n$ to $\{0,1\}$. A graph function f is *monotone* if $f(G_1) \leq f(G_2)$ whenever $G_1 \subseteq G_2$.

A graph H is a *minterm* of monotone graph function f if $f(H) = 1$ and $f(H') = 0$ for every proper subgraph $H' \subset H$. For a pattern P, a minterm H of f is a *P-minterm* of f if the induced pattern on the non-isolated vertices of H is isomorphic to P. The set of minterms (resp. P-minterms) of f is denoted $\mathcal{M}(f)$ (resp. $\mathcal{M}(f,P)$).

We will frequently refer to the following basic fact about minterms:

Lemma 2.1. *For all monotone graph functions f and g,*

$$\begin{aligned} \mathcal{M}(f \vee g) &\subseteq \mathcal{M}(f) \cup \mathcal{M}(g), \\ \mathcal{M}(f \wedge g) &\subseteq \{F \cup G : F \in \mathcal{M}(f),\ G \in \mathcal{M}(g)\}. \end{aligned}$$

That is, every minterm of $f \vee g$ is a minterm of f or a minterm of g and every minterm of $f \wedge g$ is the union of a minterm of f and a minterm of g.

2.3. Monotone circuits. A *monotone circuit* on m variables is an acyclic directed graph C with m sources (called *inputs*) and a unique sink (called the *output*). Non-source nodes (called *gates*) are labelled either $\wedge$ or $\vee$. C computes a monotone function $\{0,1\}^m \to \{0,1\}$ in the natural way. For $m = \binom{n}{2}$, we view C as computing a monotone graph function. $\mathsf{C}(G)$ denotes the value of C on a graph G. $\mathcal{M}(\mathsf{C})$ (resp. $\mathcal{M}(\mathsf{C},P)$) denotes the set of minterms (resp. P-minterms) of the function computed by C.

Size is the number of gates in a circuit. *Fan-in* is the maximum in-degree among gates. In §6–§8, we prove our lower bounds (Theorems 1.2 and 1.4) for monotone circuits with fan-in 2. In §9, we extend these results to monotone circuits with unbounded fan-in.

2.4. Random graphs. We consistently represent random objects using boldface symbols ($\boldsymbol{G}$, $\boldsymbol{W}$, etc.). For a set X and $p \in [0,1]$, notation $\boldsymbol{W} \subseteq_p X$ expresses that $\boldsymbol{W}$ is a random subset of X where each $x \in X$ belongs to $\boldsymbol{W}$ independently with probability p. For a function $p : \mathbb{N} \to [0,1]$, we denote by $\boldsymbol{G} \sim \mathrm{G}(n,p)$ the *Erdős-Rényi random graph* on n vertices, in which each pair of vertices has an edge independently with probability $p(n)$ (i.e., $V_{\boldsymbol{G}} = [n]$ and $E_{\boldsymbol{G}} \subseteq_p \binom{[n]}{2}$). We denote by $\boldsymbol{K}_k$ ($= \boldsymbol{K}_k(n)$)

the *random planted k-clique* on n vertices (i.e., $V_{\boldsymbol{K}_k} = [n]$ and $E_{\boldsymbol{K}_k} = \binom{\boldsymbol{U}}{2}$ where $\boldsymbol{U}$ is uniform random k-element subset of $[n]$).

We now state two lemmas concerning k-cliques in $G(n,p)$ (for proofs and additional background, see Ch. 10 of [3], Ch. 4 of [7], or Ch. 3 of [12]). The first lemma establishes that $\Theta(n^{-2/(k-1)})$ is precisely the class of threshold functions for the existence of k-cliques in $G(n,p)$.

Lemma 2.2.

- *If $p(n) = o(n^{-2/(k-1)})$ then $G(n,p)$ is almost surely k-clique-free.*
- *If $p(n) = \omega(n^{-2/(k-1)})$ then $G(n,p)$ has a k-clique almost surely.*
- *If $p(n) = \Theta(n^{-2/(k-1)})$ then $\Pr[G(n,p)$ has a k-clique$]$ is bounded away from 0 and 1.*

When $p = \Theta(n^{-2/(k-1)})$, the number of k-cliques in $G(n,p)$ is asymptotically Poisson, as the next lemma shows. To state the lemma, let $\mathrm{Pois}(\lambda)$ denote the Poisson distribution with mean λ, let $d_{\mathrm{TV}}(\cdot,\cdot)$ denote the total variation distance ($= 1/2$ the ℓ_1-distance between two distributions), and let $\kappa(G)$ denote the number of k-cliques in a graph G.

Lemma 2.3. *Fix $c > 0$ and let $\lambda = c^{\binom{k}{2}}/k!$ and $\boldsymbol{G} \sim G(n, cn^{-2/(k-1)})$. For $t \in \mathbb{N}$, let $\boldsymbol{G}_t$ denote $\boldsymbol{G}$ conditioned on $\kappa(\boldsymbol{G}) = t$.*

1. *$\kappa(\boldsymbol{G})$ and $\mathrm{Pois}(\lambda)$ converge in distribution (i.e., $\lim_{n\to\infty} d_{\mathrm{TV}}(\kappa(\boldsymbol{G}), \mathrm{Pois}(\lambda)) = 0$).*
2. *$\boldsymbol{G}_{t+1}$ and $\boldsymbol{G}_t \cup \boldsymbol{K}_k$ converge in distribution.*
3. $\lim_{n\to\infty} d_{\mathrm{TV}}(\kappa(\boldsymbol{G}), \kappa(\boldsymbol{G} \cup \boldsymbol{K}_k)) = d_{\mathrm{TV}}(\mathrm{Pois}(\lambda), \mathrm{Pois}(\lambda) + 1) < 1$.

Proof. [Proof sketch] Proofs of (1) can be found in any of [3, 7, 12]. For (2), let $\mathcal{S} \subseteq \mathscr{G}_n$ be the set of graphs with exactly $t+1$ k-cliques such that no two k-cliques have a vertex in common. W.h.p., $\boldsymbol{G}_{t+1} \in \mathcal{S}$ and $\boldsymbol{G}_t \cup \boldsymbol{K}_k \in \mathcal{S}$. Further, for every $G \in \mathcal{S}$, we have $\Pr[\boldsymbol{G}_{t+1} = G \mid \boldsymbol{G}_{t+1} \in \mathcal{S}] = \Pr[\boldsymbol{G}_t \cup \boldsymbol{K}_k = G \mid \boldsymbol{G}_t \cup \boldsymbol{K}_k \in \mathcal{S}]$. It follows that $\boldsymbol{G}_{t+1}$ and $\boldsymbol{G}_t \cup \boldsymbol{K}_k$ converge in distribution. For (3), note that (1) and (2) imply that $\kappa(\boldsymbol{G} \cup \boldsymbol{K}_k)$ and $\mathrm{Pois}(\lambda) + 1$ converge in distribution. Hence $d_{\mathrm{TV}}(\kappa(\boldsymbol{G}), \kappa(\boldsymbol{G} \cup \boldsymbol{K}_k))$ converges to $d_{\mathrm{TV}}(\mathrm{Pois}(\lambda), \mathrm{Pois}(\lambda)+1)$, which is a constant less than $1 - \Pr[\mathrm{Pois}(\lambda) = 0]$ $(= 1 - e^{-\lambda})$. □

3. Razborov's Approximation Method.

Razborov proved the first lower bounds on the worst-case monotone complexity of k-Clique in a seminal paper [16] which introduced the technique known as the Approximation Method. A slight quantitative improvement to Razborov's bounds was later given by Alon and Boppana [1].

Theorem 3.1 ([1, 16]). *For every constant $k \geq 3$, k-Clique has worst-case monotone complexity $\Omega((n/\log n)^k)$.*

Theorem 3.1 is derived from a more general lower bound stated in terms of two random graphs (similar to the statement of Theorem 1.4). Let $\boldsymbol{P}_{k-1}$ denote the uniform distribution on complete $(k-1)$-partite graphs in $\mathscr{G}_n$. The following theorem is implicit in [1, 16].

Theorem 3.2. *If C is a monotone circuit of size $o((n/\log n)^k)$ such that $\mathrm{E}[\mathsf{C}(\boldsymbol{K}_k)] = 1 - o(1)$, then $\mathrm{E}[\mathsf{C}(\boldsymbol{P}_{k-1})] = 1 - o(1)$.*

We now describe the basic Approximation Method used to prove Theorem 3.2. Suppose we want to prove a lower bound the size of monotone circuits C which *separate* two probability distributions Δ_0 and Δ_1 on $\{0,1\}^n$ in the sense that $\mathrm{E}[\mathsf{C}(\Delta_0)] = o(1)$ and $\mathrm{E}[\mathsf{C}(\Delta_1)] = 1 - o(1)$. In the Approximation Method, we consider a class $\mathfrak{A}$ of monotone functions $\{0,1\}^n \to \{0,1\}$ (called "approximators") such that

- $\mathfrak{A}$ contains the i-coordinate function $x \mapsto x_i$ for every $i \in [n]$,
- $\mathfrak{A}$ is a lattice with respect to the natural partial order on monotone functions (i.e. $f \le g$ iff $f(x) \le g(x)$ for all $x \in \{0,1\}^n$).

We denote by $\overline{\wedge}$ and $\overline{\vee}$ the g.l.b. and l.u.b. operations in $\mathfrak{A}$ (note that $\overline{\wedge}$ and $\overline{\vee}$ are not necessarily the AND and OR operations). Now, for any monotone circuit C on $\binom{n}{2}$ variables, we may consider the corresponding circuit $\{\overline{\wedge}, \overline{\vee}\}$-circuit $\overline{\mathsf{C}}$ in which the $\wedge$ and $\vee$ gates are replaced by $\overline{\wedge}$ and $\overline{\vee}$ gates. Note that every gate in $\overline{\mathsf{C}}$ computes a function in $\mathfrak{A}$.

To establish that no monotone circuit C of size S separates Δ_0 and Δ_1, it suffices to show the following:

1. no $f \in \mathfrak{A}$ satisfies $\mathrm{E}[f(\Delta_0)] = o(1)$ and $\mathrm{E}[f(\Delta_1)] = 1 - o(1)$,
2. for all $f, g \in \mathfrak{A}$,

$$\begin{aligned} \mathrm{E}[(f \mathbin{\overline{\vee}} g)(\Delta_0)] - \mathrm{E}[(f \vee g)(\Delta_0)] &= o(1/S), \\ \mathrm{E}[(f \wedge g)(\Delta_1)] - \mathrm{E}[(f \mathbin{\overline{\wedge}} g)(\Delta_1)] &= o(1/S). \end{aligned}$$

By bounding "local errors", (2) implies that for any monotone circuit C of size S,

$$\begin{aligned} \mathrm{E}[\mathsf{C}(\Delta_0)] &\le \mathrm{E}[\overline{\mathsf{C}}(\Delta_0)] + o(1), \\ \mathrm{E}[\mathsf{C}(\Delta_1)] &\ge \mathrm{E}[\overline{\mathsf{C}}(\Delta_1)] - o(1). \end{aligned}$$

It follows that C cannot satisfy both $\mathrm{E}[\mathsf{C}(\Delta_0)] = o(1)$ and $\mathrm{E}[\mathsf{C}(\Delta_1)] = 1 - o(1)$.

Of course, showing (1) and (2) for given Δ_0 and Δ_1 depends on a clever choice of the lattice $\mathfrak{A}$. To prove Theorem 3.2 (with respect to $\Delta_0 = \boldsymbol{P}_{k-1}$ and $\Delta_1 = \boldsymbol{K}_k$), Razborov defines a lattice $\mathfrak{A}$ where the l.u.b. operation $\overline{\vee}$ involves "plucking" large sunflowers among the minterms of the function $f \vee g$. (See [16] for the precise definition of $\mathfrak{A}$.)

Having outlined the standard Approximation Method framework, we caution the reader that our proof of Theorem 1.4 does not follow this framework precisely. Rather, we work with a "one-sided" version of the Approximation Method presented in terms of a closure operator on the lattice of all monotone graph functions (see §6). However, this difference is merely a matter of presentation, as our proof could alternatively be formulated in terms of a suitable lattice $\mathfrak{A}$ of approximator functions.

4. Quasi-sunflowers. In this section we introduce a new relaxation of sunflowers called *quasi-sunflowers*. Like sunflowers, quasi-sunflowers are a special class of hypergraphs. Recall that a *hypergraph* on a set X is a family $\mathcal{F}$ of subsets of X. Elements of $\mathcal{F}$ are called *hyperedges*. The *size* $|\mathcal{F}|$ of $\mathcal{F}$ refers to the number of hyperedges. We say that $\mathcal{F}$ is *s-uniform* if every hyperedge has size s (i.e., $\mathcal{F} \subseteq \binom{X}{s}$).

A *sunflower* is a nonempty hypergraph $\mathcal{F}$ such that the intersection of any two distinct hyperedges equals the intersection $\bigcap \mathcal{F}$ $(= \bigcap_{U \in \mathcal{F}} U)$ of all hyperedges. The set $\bigcap \mathcal{F}$ is called the *core* of $\mathcal{F}$ and sets $U \setminus \bigcap \mathcal{F}$ where $U \in \mathcal{F}$ are called *petals* of $\mathcal{F}$ (note that petals are mutually disjoint). The following result, known as the Erdős-Rado Sunflower Lemma, plays a key role in many applications of sunflowers.

Theorem 4.1 (Sunflower Lemma [9]). *Every s-uniform hypergraph $\mathcal{F}$ of size $> s!(N-1)^s$ contains a sunflower of size N.*

We now define our new notion of quasi-sunflowers. Quasi-sunflowers are a relaxation of sunflowers in which petals may overlap in a limited way (for other variants of sunflowers studied in extremal combinatorics, see Ch. 7 of [14]).

Definition 4.2 (Quasi-sunflowers). *Let $\mathcal{F}$ be a nonempty hypergraph on a set X and let $Y = \bigcap \mathcal{F}$. For $p \in [0,1]$ and $\gamma \geq 0$, we say that $\mathcal{F}$ is* (p,γ)-quasi-sunflower *if for the random set $\boldsymbol{W} \subseteq_p X$,*

$$\Pr\big[\boldsymbol{W} \cup Y \textit{ contains no hyperedge of } \mathcal{F}\big] \leq e^{-\gamma}.$$

Remark 4.3. Every sunflower is a (p,γ)-quasi-sunflower for suitable p and γ. Specifically, suppose $\mathcal{F}$ is a sunflower of size n such that each hyperedge has size $\leq s$. Then for every $p \in [0,1]$, $\mathcal{F}$ is a (p, np^s)-quasi-sunflower. To see this, let $Y = \bigcap \mathcal{F}$ and note that for $\boldsymbol{W} \subseteq_p X$,

$$\Pr\big[\boldsymbol{W} \cup Y \text{ contains no hyperedge of } \mathcal{F}\big] \leq (1 - p^{s-|Y|})^n \leq \exp(np^{s-|Y|}) \leq \exp(np^s).$$

We now give a result on quasi-sunflowers analogous to the Sunflower Lemma. This lemma plays a key role in our lower bounds.

Theorem 4.4 (Quasi-sunflower Lemma). *For all $p \in [0,1]$ and $\gamma \geq 1$, every s-uniform hypergraph of size $\geq s!(c\gamma/p)^s$ contains a (p,γ)-quasi-sunflower where $c = 1/\ln(3/2) < 2.47$.*

Remark 4.5. The standard Sunflower Lemma (Theorem 4.1) directly implies a weaker version of Theorem 4.4. Suppose $\mathcal{F}$ is a s-uniform hypergraph of size $\geq s!(\gamma/p^s)^s$. Then $\mathcal{F}$ contains a sunflower of size γ/p^s by Theorem 4.1, which is a (p,γ)-quasi-sunflower by Remark 4.1.

Our proof of Theorem 4.4 relies on Janson's Inequality [11] (see also Ch. 2 of [12] and Ch. 8 of [3]).

Lemma 4.6 (Janson's Inequality [11]). *Let $\mathcal{F}$ be a nonempty hypergraph on a set X. Let $\boldsymbol{W}$ be a random subset of X such that events $x \in \boldsymbol{W}$ are mutually independent for $x \in X$ (for example, $\boldsymbol{W} \subseteq_p X$). Define μ and Δ by*

$$\mu = \sum_{U \in \mathcal{F}} \Pr\big[U \subseteq \boldsymbol{W}\big],$$
$$\Delta = \sum_{\substack{U,V \in \mathcal{F}:\\ U \neq V,\ U \cap V \neq \emptyset}} \Pr\big[U \cup V \subseteq \boldsymbol{W}\big].$$

Then $$\Pr\Big[\bigwedge_{U \in \mathcal{F}} U \not\subseteq \boldsymbol{W}\Big] \leq \exp(-\min(\frac{\mu}{2}, \frac{\mu^2}{2\Delta})).$$

Our proof of Theorem 4.4, below, uses Janson's Inequality within an inductive argument that resembles proofs of the Sunflower Lemma.

Proof. [Proof of the Quasi-sunflower Lemma (Theorem 4.4)] Define the sequence $\ell_1, \ell_2, \ldots$ inductively by $\ell_1 = 1$ and $\ell_s = 2\sum_{t=1}^{s-1}\binom{s}{t}\ell_t$ for $s \geq 2$. We have $\ell_s \leq s!\ln^{-s}(3/2)$ by induction: for $s \geq 2$, if we assume that $\ell_t \leq t!\ln^{-t}(3/2)$ for all

$t \in \{1, \dots, s-1\}$, then

$$\begin{aligned}
\ell_s &\le 2 \sum_{t=1}^{s-1} \binom{s}{t} t! \ln^{-t}(3/2) \\
&= 2\Bigg(\sum_{t=1}^{s-1} \frac{\ln^{s-t}(3/2)}{(s-t)!} \Bigg) s! \ln^{-s}(3/2) \\
&\le 2\Bigg(-1 + \sum_{j=0}^{\infty} \frac{\ln^{j}(3/2)}{j!} \Bigg) s! \ln^{-s}(3/2) \\
&= s! \ln^{-s}(3/2).
\end{aligned}$$

Suppose $\mathcal{F}$ is an s-uniform hypergraph of size $\ge \ell_s(\gamma/p)^s$. Arguing by induction on s, we claim that $\mathcal{F}$ contains an (p,γ)-quasi-sunflower (proving the theorem). In the base case where $s = 1$, let $\boldsymbol{W} \subseteq_p X$ and note that events $U \subseteq \boldsymbol{W}$ for $U \in \mathcal{F}$ are mutually independent. Therefore,

$$\Pr\big[\bigwedge_{U \in \mathcal{F}} U \nsubseteq \boldsymbol{W} \big] = (1-p)^{|\mathcal{F}|} \le (1-p)^{\gamma/p} \le e^{-\gamma},$$

so $\mathcal{F}$ itself is a (p,γ)-quasi-sunflower.

For the induction step, let $s \ge 2$ and assume the claim holds for $t \in \{1, \dots, s-1\}$. For all $A \subseteq X$ with $1 \le |A| \le s-1$, let

$$\mathcal{F}_A = \{U \setminus A : U \in \mathcal{F} \text{ such that } A \subseteq U\}.$$

Note that $\mathcal{F}_A$ is an $(s-|A|)$-uniform hypergraph. We now consider two cases.

Case 1:. Suppose there exist $t \in \{1, \dots, s-1\}$ and $A \in \binom{X}{t}$ such that $|\mathcal{F}_A| \ge \ell_{s-t}(\gamma/p)^{s-t}$. By the induction hypothesis, $\mathcal{F}_A$ contains a (p,γ)-quasi-sunflower $\mathcal{F}'$. Observe that $\{U \cup A : U \in \mathcal{F}'\} \subseteq \mathcal{F}$ is a (p,γ)-quasi-sunflower.

Case 2:. Suppose $|\mathcal{F}_A| \le \ell_{s-t}(\gamma/p)^{s-t}$ for all $t \in \{1, \dots, s-1\}$ and $A \in \binom{X}{t}$. We will show that $\mathcal{F}$ itself is a (p,γ)-quasi-sunflower. Let $\boldsymbol{W} \subseteq_p X$ and let μ and Δ be as in the statement of Janson's Inequality (Lemma 4.6), whereby we have

$$\Pr\big[\bigwedge_{U \in \mathcal{F}} U \nsubseteq \boldsymbol{W} \big] \le \exp(-\min(\frac{\mu}{2}, \frac{\mu^2}{2\Delta})).$$

Thus, to show that $\mathcal{F}$ is a (p,γ)-quasi-sunflower, it suffices to show that $\mu/2 \ge \gamma$ and $\mu^2/2\Delta \ge \gamma$.

We have $\mu = |\mathcal{F}|p^s$ since $\Pr[U \subseteq \boldsymbol{W}] = p^s$ for all $U \in \mathcal{F}$. Since $|\mathcal{F}| \ge \ell_s(\gamma/p)^s$ and $\ell_s \ge 2$ (as $s \ge 2$) and $\gamma^s \ge \gamma$ (as $\gamma \ge 1$), it follows that $\mu/2 \ge \gamma$.

It remains to show that $\mu^2/2\Delta \ge \gamma$. For all $t \in \{1, \dots, s-1\}$, we have $\sum_{A \in \binom{X}{t}} |\mathcal{F}_A| = \binom{s}{t}|\mathcal{F}|$ as each hyperedge of $\mathcal{F}$ is counted $\binom{s}{t}$ times in this summation. Therefore,

$$\sum_{A \in \binom{X}{t}} |\mathcal{F}_A|^2 \le |\mathcal{F}| \sum_{A \in \binom{X}{t}} |\mathcal{F}_A| \le \mu \binom{s}{t} \ell_{s-t} \gamma^{s-t} p^{t-2s}$$

(using $|\mathcal{F}| = \mu p^{-s}$ and $|\mathcal{F}_A| \le \ell_{s-t}(\gamma/p)^{s-t}$). Noting that $\Pr\big[U \cup V \subseteq \boldsymbol{W}\big] =$

$p^{2s-|U\cap V|}$ for all $U, V \in \mathcal{F}$, we bound Δ as follows:

$$\begin{aligned}
\Delta &= \sum_{\substack{A\subseteq X:\\ 1\le|A|\le s-1}} \sum_{\substack{U,V\in\mathcal{F}:\\ U\cap V=A}} \Pr\big[U\cup V\subseteq \boldsymbol{W}\big]\\
&\le \sum_{t=1}^{s-1}\Big(\sum_{A\in\binom{X}{t}} |\mathcal{F}_A|^2\Big)p^{2s-t}\\
&\le \mu\sum_{t=1}^{s-1}\binom{s}{t}\ell_{s-t}\gamma^{s-t}\\
&\le \mu\gamma^{s-1}\sum_{t=1}^{s-1}\binom{s}{t}\ell_t \qquad \text{(using } \gamma^t\le\gamma^{s-1}\text{)}\\
&= \frac{\mu\gamma^{s-1}\ell_s}{2} \qquad \text{(by definition of } \ell_s\text{).}
\end{aligned}$$

Completing the proof, we have

$$\frac{\mu^2}{2\Delta} \ge \frac{\mu}{\gamma^{s-1}\ell_s} = \frac{|\mathcal{F}|p^s}{\gamma^{s-1}\ell_s} \ge \gamma$$

(using the assumption that $|\mathcal{F}| \ge \ell_s(\gamma/p)^s$). □

5. Small, Medium, Large.

Let $\boldsymbol{G} \sim G(n, \Theta(n^{-2/(k-1)}))$ be a random graph at a threshold for k-Clique. It is instructive to calculate the expected number of ℓ-cliques in $\boldsymbol{G}$ for $\ell \in \{0,\dots,k\}$:

$$\mathrm{E}[\#\text{ of } \ell\text{-cliques in } \boldsymbol{G}] = \Theta\big(n^{\ell-\frac{2}{k-1}\binom{\ell}{2}}\big).$$

Letting $\lambda = \ell/k$, we have

$$\ell - \frac{2}{k-1}\binom{\ell}{2} = \lambda(1-\lambda)k + O(1).$$

Note that $\lambda(1-\lambda)k$ has maximum value $k/4$ for $\lambda = 1/2$. (Indeed, $\ell - \frac{2}{k-1}\binom{\ell}{2}$ is maximal for $\ell \in \{\lfloor k/2\rfloor, \lceil k/2\rceil\}$.)

Related to the fact that $\boldsymbol{G}$ has many cliques of size around $k/2$ and much fewer cliques of size $\le \varepsilon k$ or $\ge (1-\varepsilon)k$ for $\varepsilon > 0$, it will be convenient to classify patterns into three "sizes".

Definition 5.1. *A pattern P is:*

- small *if $|V_P| < k/2$,*
- medium *if $|V_P| \ge k/2$ and there exist small patterns P_1, P_2 such that $P = P_1 \cup P_2$,*
- large *otherwise.*

A graph is small, medium *or* large *according to the induced pattern on its non-isolated vertices.*

A few observations about this definition: The union of two small patterns/graphs is small or medium (but never large). The complete pattern K_ℓ is small if $\ell < k/2$ and large otherwise (but never medium). An important example of medium pattern is $K_{\lceil k/2\rceil} - \{\text{single edge}\}$ (which is the union of two overlapping copies of $K_{\lceil k/2\rceil-1}$).

Lemma 5.2. *For every medium pattern P,*

$$|V_P| - \frac{2}{k-1}|E_P| \geq \frac{k+1}{4} + \frac{2}{k-1}.$$

Proof. Let P be a medium pattern which minimizes $|V_P| - \frac{2}{k-1}|E_P|$. By definition of medium, P is the union of two small patterns P_1 and P_2. We can assume that P_1 and P_2 are complete, since we only decrease $|V_{P_1 \cup P_2}| - \frac{2}{k-1}|E_{P_1 \cup P_2}|$ by replacing P_1 and P_2 with the (also small) complete patterns with the same vertices. Let $a = |V_P|$, $b = |V_{P_1}|$ and $c = |V_{P_2}|$ and note that $|V_P| - \frac{2}{k-1}|E_P| = a - \frac{2}{k-1}(\binom{b}{2} + \binom{c}{2} - \binom{b+c-a}{2})$.

First, consider the case that k is odd and let $t = \frac{k-1}{2}$. Note that integers a, b, c satisfy $1 \leq b, c \leq t$ and $t + 1 \leq a \leq b + c$. Relaxing integrality, let α, β, γ be real numbers minimizing $\alpha - \frac{1}{t}(\binom{\beta}{2} + \binom{\gamma}{2} - \binom{\beta+\gamma-\alpha}{2})$ subject to $1 \leq \beta, \gamma \leq t$ and $t + 1 \leq \alpha \leq \beta + \gamma$. Note that $\beta = \gamma$ since, if not, by replacing both β and γ with their mean $(\beta + \gamma)/2$ we could reduce the objective function while still satisfying the constraints. Our task is now to minimize the function $f(\alpha, \beta)$ defined by

$$f(\alpha, \beta) = \alpha + \frac{1}{t}\binom{2\beta - \alpha}{2} - \frac{2}{t}\binom{\beta}{2}$$

subject to $1 \leq \beta \leq t$ and $t + 1 \leq \alpha \leq 2\beta$. Since $\frac{d}{d\alpha} f(\alpha, \beta) > 0$ and $\frac{d}{d\beta} f(\alpha, \beta) < 0$ for all α, β in this range, it follows that $\alpha = t + 1$ and $\beta = t$. Therefore,

$$|V_P| - \frac{2}{k-1}|E_P| \geq f(t+1, t) = \frac{t+1}{2} + \frac{1}{t} = \frac{k+1}{4} + \frac{2}{k-1}.$$

In the case where k is even, we get

$$|V_P| - \frac{2}{k-1}|E_P| \geq \frac{k+1}{4} + \frac{9}{4(k-1)} > \frac{k+1}{4} + \frac{2}{k-1}$$

by a similar calculation. □

We point out that Lemma 5.2 is tight when P is the medium pattern $K_{\lceil k/2 \rceil} - \{\text{single edge}\}$.

Remark 5.3. The dominant term $k/4$ in Lemma 5.2 is the same $k/4$ that appears in the exponent of $n^{k/4}$ in our main theorems. In fact, Lemma 5.2 also accounts for the exponent in the $n^{k/4}$ lower bound on the average-case complexity of k-Clique on AC^0 circuits from [18]. It is notable that the same bottleneck arises in the distinct settings of AC^0 circuits and monotone circuits.

6. The Approximation via a Closure Operator. In this section, we define a closure operator in the lattice of monotone graph functions. For a monotone graph function f, its closure $\mathbf{cl}(f)$ is a good approximation for f (Lemma 6.6). A key property of closed functions is that they have few P-minterms for small and medium patterns P (Lemma 6.9).

Remark 6.1. The approximation of f by $\mathbf{cl}(f)$ is a variation of the standard Approximation Method as described in §3. To fit that framework exactly (define the lattice of approximator functions, etc.), it becomes necessary to work with an additional "truncation" operator which cuts out large minterms (as in [16]). We find it more natural to work with a closure operator alone, so our presentation differs from the framework described in §3.

From now through §8, fix $p = n^{-2/(k-1)}$ and $\delta = k^{-2}$ and let $\boldsymbol{G} \sim G(n, p)$ and $\boldsymbol{G}^- \sim G(n, p^{1+\delta})$. Keep in mind that:

- p is a fixed threshold function for the existence of k-cliques (our results in fact hold for any $p = \Theta(n^{-2/(k-1)})$),
- δ is a sufficiently small constant (this happens to mean $\leq k^{-2}$),
- $\boldsymbol{G}$ is random graph at k-clique threshold p, and
- $\boldsymbol{G}^-$ is a random graph which is slightly subcritical for the existence of k-cliques. That is, $\boldsymbol{G}^-$ is almost surely k-clique-free since $p^{1+\delta} = o(n^{-2/(k-1)})$, but for instance $\boldsymbol{G}^-$ contains many cliques of size $k-1$ since $p^{1+\delta} = \omega(n^{-2/(k-2)})$.

In addition, from now through §8, monotone circuits are assumed to have fan-in 2. That is, we first prove Theorems 1.2 and 1.4 for monotone circuits with fan-in 2. In §9, we extend these theorems to monotone circuits with unbounded fan-in.

We now present the key definition of this section:

Definition 6.2. *A monotone graph function $f : \mathscr{G}_n \to \{0,1\}$ is* closed *if for every small-or-medium graph H,*

$$\mathrm{E}[f(\boldsymbol{G}^- \cup H)] \geq 1 - e^{-n^\delta} \implies f(H) = 1.$$

In order words, the expectation $\mathrm{E}[f(\boldsymbol{G}^- \cup H)]$ $(= \Pr[f(\boldsymbol{G}^- \cup H) = 1])$ never lies in the interval $[1 - e^{-n^\delta}, 1)$; it is either $< 1 - e^{-n^\delta}$ or $= 1$. Note that if both f and g are closed, then the conjunction $f \wedge g$ is also closed.

Definition 6.3. *For a monotone graph function f, we denote by $\mathbf{cl}(f)$ the unique minimal closed function such that $f \leq \mathbf{cl}(f)$; this is well-defined since the constant function 1 is closed and conjunctions of closed functions are closed. We call $\mathbf{cl}(f)$ the* closure *of f.*

Remark 6.4. Viewed as an operation on the set of monotone graph functions, $\mathbf{cl}(\cdot)$ is a closure operator in the usual sense. That is, it satisfies:

- (increasing) $f \leq \mathbf{cl}(f)$,
- (monotone) $f \leq g \implies \mathbf{cl}(f) \leq \mathbf{cl}(g)$,
- (idempotent) $\mathbf{cl}(\mathbf{cl}(f)) = \mathbf{cl}(f)$.

Definition 6.5. *We denote by $\overline{\vee}$ the operation on monotone graph functions defined by $f \mathbin{\overline{\vee}} g = \mathbf{cl}(f \vee g)$. For a monotone circuit C, let $\overline{\mathsf{C}}$ be the corresponding circuit with basis $\{\wedge, \overline{\vee}\}$ in which the $\vee$-gates in C are replaced by $\overline{\vee}$-gates. For a node ν in C, we denote by $\overline{\nu}$ the corresponding node in $\overline{\mathsf{C}}$.*

Note that $\mathbf{cl}(\mathsf{C})$ (i.e., $\mathbf{cl}(f)$ where f is the function computed by C) is not necessarily the same function as $\overline{\mathsf{C}}$, although $\overline{\mathsf{C}}$ is indeed a closed function satisfying $\mathsf{C} \leq \overline{\mathsf{C}}$ (i.e., $\mathsf{C}(G) \leq \overline{\mathsf{C}}(G)$ for all graphs G).

Lemma 6.6. *For every monotone graph function f,*

$$\Pr\left[f(\boldsymbol{G}^-) \neq (\mathbf{cl}(f))(\boldsymbol{G}^-)\right] \leq 2^{k^2} n^k e^{-n^\delta}.$$

Proof. We claim that there exist $t \in \mathbb{N}$ and small-or-medium graphs $H_1, \dots, H_t$ and monotone functions $f_0, \dots, f_t : \mathscr{G}_n \to \{0,1\}$ such that

- $f_0 = f$,
- $\mathrm{E}[f_{i-1}(\boldsymbol{G}^- \cup H_i)] \in [1 - e^{-n^\delta}, 1)$,
- $f_i = f_{i-1} \vee \mathsf{Ind}_{H_i}$ where $\mathsf{Ind}_{H_i} : \mathscr{G}_n \to \{0,1\}$ is the function $\mathsf{Ind}_{H_i}(G) = 1$ iff $H_i \subseteq G$,
- f_t is closed.

We can generate such a sequence simply by choosing any suitable H_{i+1} so long as f_i is not closed; this process eventually terminates, since each small or medium graph

H appears at most once in the sequence $H_1, H_2, \dots$. Note that

$$t \leq |\{\text{small and medium graphs in } \mathscr{G}_n\}| \leq 2^{k^2} n^k.$$

We argue by induction that $f_i \leq \mathbf{cl}(f)$ for all $i \in \{0, \dots, t\}$. This is true for $i = 0$ since $f_0 = f$. Let $i \geq 1$ and assume $f_{i-1} \leq \mathbf{cl}(f)$. We have $\mathrm{E}[(\mathbf{cl}(f))(\boldsymbol{G}^- \cup H_i)] \geq \mathrm{E}[f_{i-1}(\boldsymbol{G}^- \cup H_i)] \geq 1 - e^{-n^\delta}$. Therefore $\mathbf{cl}(f)(H_i) = 1$ (by definition of $\mathbf{cl}(f)$ being closed). Since f_i $(= f_{i-1} \vee \mathsf{Ind}_{H_i})$ is minimal among monotone graph functions g such that $f_{i-1} \leq g$ and $g(H_i) = 1$, we have $f_i \leq \mathbf{cl}(f)$.

It follows that $f_t = \mathbf{cl}(f)$ since f_t is closed and $f \leq f_t \leq \mathbf{cl}(f)$. Concluding the proof of the lemma, we have

$$\begin{aligned}
\Pr\left[f(\boldsymbol{G}^-) \neq (\mathbf{cl}(f))(\boldsymbol{G}^-)\right] &\leq \sum_{i=1}^{t} \Pr\left[f_{i-1}(\boldsymbol{G}^-) \neq f_i(\boldsymbol{G}^-)\right] \\
&= \sum_{i=1}^{t} \Pr\left[f_{i-1}(\boldsymbol{G}^-) = 0 \text{ and } H_i \subseteq \boldsymbol{G}^-\right] \\
&\leq \sum_{i=1}^{t} \Pr\left[f_{i-1}(\boldsymbol{G}^- \cup H_i) = 0\right] \\
&\leq 2^{k^2} n^k e^{-n^\delta}.
\end{aligned}$$

□

The next two lemmas follow immediately from Lemma 6.6.

Lemma 6.7. *For every monotone graph function f, $\mathcal{M}(\mathbf{cl}(f)) \setminus \mathcal{M}(f)$ contains only small and medium graphs.*

Proof. The proof of Lemma 6.6 shows that there exist small-or-medium graphs $H_1, \dots, H_t$ such that $\mathbf{cl}(f) = f \vee \bigvee_{i=1}^{t} \mathsf{Ind}_{H_i}$. Thus, $\mathcal{M}(\mathbf{cl}(f)) \subseteq \mathcal{M}(f) \cup \{H_1, \dots, H_t\}$. □

Lemma 6.8. *For every monotone circuit C of size $\exp(o(n^\delta))$,*

$$\mathrm{E}[\overline{\mathsf{C}}(\boldsymbol{G}^-)] - \mathrm{E}[\mathsf{C}(\boldsymbol{G}^-)] = \exp(-\Omega(n^\delta)).$$

Proof. For any graph H, note that if $\mathsf{C}(H) \neq \overline{\mathsf{C}}(H)$ then there exists an $\vee$-gate ν with children μ_1 and μ_2 in C such that $\overline{\nu}(H) \neq (\overline{\mu_1} \vee \overline{\mu_2})(H)$ (equivalently: $f(H) \neq (\mathbf{cl}(f))(H)$ where f is the function $\overline{\mu_1} \vee \overline{\mu_2}$). It follows that

$$\begin{aligned}
\mathrm{E}[\overline{\mathsf{C}}(\boldsymbol{G}^-)] - \mathrm{E}[\mathsf{C}(\boldsymbol{G}^-)] &= \Pr\left[\mathsf{C}(\boldsymbol{G}^-) \neq \overline{\mathsf{C}}(\boldsymbol{G}^-)\right] \\
&\leq \sum_{\substack{\vee\text{-gates } \nu \text{ in } \mathsf{C} \text{ with} \\ \text{children } \mu_1 \text{ and } \mu_2}} \Pr\left[\overline{\nu}(\boldsymbol{G}^-) \neq (\overline{\mu_1} \vee \overline{\mu_2})(\boldsymbol{G}^-)\right] \\
&\leq \mathsf{size}(\mathsf{C}) 2^{k^2} n^k e^{-n^\delta} \qquad \text{(by Lemma 6.6)} \\
&= \exp(-\Omega(n^\delta)).
\end{aligned}$$

□

The next lemma gives a key property of closed functions that relies on the Quasi-sunflower Lemma (Theorem 4.4).

Lemma 6.9. *A closed monotone graph function has at most $k^{k^2}(n^\delta/p^{1+\delta})^{|E_P|}$ P-minterms for every small or medium pattern P.*

Proof. Let f be a closed monotone graph function and let P be a small or medium pattern. Toward a contradiction, assume that $|\mathcal{M}(f,P)| \geq k^{k^2}(n^\delta/p^{1+\delta})^{|E_P|}$. Let $X = \binom{[n]}{2}$ and consider the $|E_P|$-uniform hypergraph $\mathcal{F} \subseteq \binom{X}{|E_P|}$ defined by $\mathcal{F} = \{E_F : F \in \mathcal{M}(f,P)\}$. Since $|E_P| \leq k^2/4$ (i.e., no medium pattern has more than $k^2/4$ edges), we have $|E_P|!2.47^{|E_P|} \leq k^{k^2}$ and hence

$$|\mathcal{F}| = |\mathcal{M}(f,P)| \geq |E_P|!2.47^{|E_P|}(n^\delta/p^{1+\delta})^{|E_P|}.$$

By Theorem 4.4, there exists a $(p^{1+\delta}, n^\delta)$-quasi-sunflower $\mathcal{F}_0 \subseteq \mathcal{F}$. Let $Y = \bigcap \mathcal{F}$ and let H be the graph with edge set $E_H = Y$. Let $\boldsymbol{W} \subseteq_{p^{1+\delta}} X$ and note that $\boldsymbol{W}$ has the same distribution as $E_{\boldsymbol{G}^-}$. We have

$$\begin{aligned} \mathrm{E}[f(\boldsymbol{G}^- \cup H)] &\geq \Pr\left[\boldsymbol{G}^- \cup H \text{ contains a } P\text{-minterm of } f\right] \\ &\geq \Pr\left[\boldsymbol{W} \cup Y \text{ contains a hyperedge of } \mathcal{F}_0\right] \\ &\geq 1 - e^{-n^\delta}. \end{aligned}$$

Since f is closed and H is small or medium, it follows that $f(H) = 1$. Note that H has fewer than $|E_P|$ edges, so in particular H is a proper subgraph of some $F \in \mathcal{M}(f,P)$ with $E_F \in \mathcal{F}_0$. However, this contradicts the fact that F is a minterm of f. □

Our final lemma on closed functions concerns the pattern $K_k - \{\text{single edge}\}$.

LEMMA 6.10. *Suppose f is a closed monotone graph function. Let $\boldsymbol{Q}$ be a random planted copy of $K_k - \{\text{single edge}\}$ among n vertices. Then either f is the constant function 1 or else $\mathrm{E}[f(\boldsymbol{Q})] = o(1)$.*

Proof. Assume that $\mathrm{E}[f(\boldsymbol{Q})] \geq \varepsilon$ for some constant $\varepsilon > 0$. We will show that f is the constant function 1 using Janson's Inequality (Lemma 4.6). Let $\mathcal{F}$ be the family of graphs H such that $f(H) = 1$ and the induced subgraph on non-isolated vertices of H is isomorphic to Q ($= K_k - \{\text{single edge}\}$). We have $|\mathcal{F}| = \varepsilon\binom{n}{k} = \Omega(n^k)$. Viewing $\mathcal{F}$ as a $|E_Q|$-uniform hypergraph on $\binom{[n]}{2}$, we bound μ and Δ in the statement of Lemma 4.6:

$$\mu = \sum_{H \in \mathcal{F}} \Pr\left[H \subseteq \boldsymbol{G}^-\right], \quad \Delta = \sum_{H_1, H_2 \in \mathcal{F} \,:\, H_1 \neq H_2,\ H_1 \cap H_2 \neq \emptyset} \Pr\left[H_1 \cup H_2 \subseteq \boldsymbol{G}^-\right].$$

Recalling that $p = n^{-2/(k-1)}$ and $\delta = k^{-2}$, we have $\mu = |\mathcal{F}|p^{(1+\delta)(\binom{k}{2}-1)} = \varepsilon n^{(2/(k-1))-(1/k)}$. Note that Δ is dominated by terms where H_1, H_2 are copies of Q which overlap on a single edge (so that $H_1 \cup H_2$ has $2k-2$ vertices and $2\binom{k}{2} - 3$ edges). Thus, we have $\Delta = O(n^{2k-2}p^{(1+\delta)(2\binom{k}{2}-3)})$ and hence $\mu^2/\Delta = \Omega(n^2p^{1+\delta}) = \Omega(n^{2-\frac{2}{k-1}(1+k^{-2})})$. Noting that μ and μ^2/Δ are both $\Omega(n^{1/k})$, Lemma 4.6 implies $\Pr[\boldsymbol{G}^-$ contains no Q-minterm of $f] = \exp(-\Omega(n^{1/k}))$. It follows that $\mathrm{E}[f(\boldsymbol{G}^-)] \geq \Pr[\boldsymbol{G}^-$ has a subgraph in $\mathcal{F}] \geq 1 - \exp(-n^\delta)$ for sufficiently large n. The assumption that f is closed now implies that $\mathrm{E}[f(\boldsymbol{G}^-)] = 1$, that is, f is the constant function 1. □

7. K vs. G⁻. In the previous section, we defined a closure operator $\mathbf{cl}(\cdot)$ on monotone graph functions and an operation transforming a monotone circuit C into a $\{\wedge, \triangledown\}$-circuit $\overline{\mathsf{C}}$. In this section, we prove Theorem 1.4.

LEMMA 7.1. *Let C be a monotone circuit. For every $H \in \mathcal{M}(\overline{\mathsf{C}}, K_k)$, there exist a gate ν in C and a medium subgraph H' of H such that $H' \in \mathcal{M}(\overline{\nu})$.*

Proof. Suppose $H \in \mathcal{M}(\overline{\mathsf{C}}, K_k)$ and let

$$\mathcal{H} = \{\text{subgraphs of } H\}, \quad \mathcal{A} = \{\text{small graphs}\}, \quad \mathcal{B} = \{\text{medium graphs}\}.$$

Toward a contradiction, assume that $\mathcal{M}(\overline{\nu}) \cap \mathcal{H} \cap \mathcal{B} = \emptyset$ for every gate ν in C. We will show, arguing by induction on ν, that $\mathcal{M}(\overline{\nu}) \cap \mathcal{H} \subseteq \mathcal{A}$ for every node ν in C. This yields a contradiction since $H \in (\mathcal{M}(\overline{\nu_{\text{out}}}) \cap \mathcal{H}) \setminus \mathcal{A}$ where ν_{out} is the output gate of C.

Consider first the base case where ν is an input node labelled by 0 or 1 or the indicator function for some edge $e \in \binom{[n]}{2}$. Note that $\mathcal{M}(\nu)$ is respectively the empty set or $\{$the empty graph$\}$ or $\{$the graph with only edge $e\}$. In any case, ν has only small minterms. Since $\overline{\nu} = \nu$, we have $\mathcal{M}(\overline{\nu}) \cap \mathcal{H} \subseteq \mathcal{A}$ as required.

For the induction step, suppose ν is a gate in C with children μ_1 and μ_2 and assume that $\mathcal{M}(\overline{\mu_i}) \cap \mathcal{H} \subseteq \mathcal{A}$ for $i \in \{1,2\}$. If ν is an $\wedge$-gate, then

$$\begin{aligned}
\mathcal{M}(\overline{\nu}) \cap \mathcal{H} &= \mathcal{M}(\overline{\mu_1} \wedge \overline{\mu_2}) \cap \mathcal{H} \\
&= \{F_1 \cup F_2 : F_1 \in \mathcal{M}(\overline{\mu_1}),\ F_2 \in \mathcal{M}(\overline{\mu_2})\} \cap \mathcal{H} \qquad \text{(Lemma 2.1)} \\
&= \{F_1 \cup F_2 : F_1 \in \mathcal{M}(\overline{\mu_1}) \cap \mathcal{H},\ F_2 \in \mathcal{M}(\overline{\mu_2}) \cap \mathcal{H}\} \\
&\subseteq \{F_1 \cup F_2 : F_1, F_2 \in \mathcal{A}\} \qquad \text{(since } \mathcal{M}(\overline{\mu_i}) \cap \mathcal{H} \subseteq \mathcal{A}\text{)} \\
&\subseteq \mathcal{A} \cup \mathcal{B} \qquad \text{(the union of two small graphs cannot be large)} \\
&\subseteq \mathcal{A} \qquad \text{(by assumption } \mathcal{M}(\overline{\nu}) \cap \mathcal{H} \cap \mathcal{B} = \emptyset\text{).}
\end{aligned}$$

Finally, if ν is a $\vee$-gate, then

$$\begin{aligned}
\mathcal{M}(\overline{\nu}) \cap \mathcal{H} &= \mathcal{M}(\overline{\mu_1} \mathbin{\overline{\vee}} \overline{\mu_2}) \cap \mathcal{H} \\
&= \mathcal{M}(\mathbf{cl}(\overline{\mu_1} \vee \overline{\mu_2})) \cap \mathcal{H} \qquad \text{(definition of } \overline{\vee}\text{)} \\
&\subseteq \big(\mathcal{M}(\overline{\mu_1} \vee \overline{\mu_2}) \cup \mathcal{A} \cup \mathcal{B}\big) \cap \mathcal{H} \qquad \text{(Lemma 6.7)} \\
&\subseteq \big(\mathcal{M}(\overline{\mu_1}) \cup \mathcal{M}(\overline{\mu_2}) \cup \mathcal{A} \cup \mathcal{B}\big) \cap \mathcal{H} \qquad \text{(Lemma 2.1)} \\
&\subseteq \mathcal{A} \cup \mathcal{B} \qquad \text{(since } \mathcal{M}(\overline{\mu_i}) \cap \mathcal{H} \subseteq \mathcal{A} \text{ for } i \in \{1,2\}\text{)} \\
&\subseteq \mathcal{A} \qquad \text{(by assumption } \mathcal{M}(\overline{\nu}) \cap \mathcal{H} \cap \mathcal{B} = \emptyset\text{).}
\end{aligned}$$

□

LEMMA 7.2. *For every monotone circuit* C*, there exists a medium pattern* P *such that*

$$\mathsf{size}(\mathsf{C}) \geq \frac{|\mathcal{M}(\overline{\mathsf{C}}, K_k)|}{(2k)^{k^2} n^{k-|V_P|} (n^{\delta}/p^{1+\delta})^{|E_P|}}.$$

Proof. By Lemma 7.1, for each $H \in \mathcal{M}(\overline{\mathsf{C}}, K_k)$, there exists a gate μ_H in C and a medium subgraph H' of H such that $H' \in \mathcal{M}(\overline{\mu_H})$. Fix choices of μ_H and H' for all $H \in \mathcal{M}(\overline{\mathsf{C}}, K_k)$. For every gate ν in C and medium pattern P, let

$$t(\nu, P) = |\{H \in \mathcal{M}(\overline{\mathsf{C}}, K_k) : \mu_H = \nu \text{ and } H' \in \mathcal{M}(\overline{\nu}, P)\}|.$$

By a simple counting argument, there exist ν and P such that

$$\frac{|\mathcal{M}(\overline{\mathsf{C}}, K_k)|}{\mathsf{size}(\mathsf{C})|\{\text{medium patterns up to isomorphism}\}|} \leq t(\nu, P).$$

For each $H' \in \mathcal{M}(\overline{\nu}, P)$, there are at most $n^{k-|V_P|}$ different $H \in \mathcal{M}(\overline{\mathsf{C}}, K_k)$ of which H' is a subgraph. It follows that

$$t(\nu, P) \leq n^{k-|V_P|} |\mathcal{M}(\overline{\nu}, P)|.$$

Since $\overline{\nu}$ is closed and P is medium, Lemma 6.9 implies

$$|\mathcal{M}(\overline{\nu}, P)| \leq k^{k^2}(n^{\delta}/p^{1+\delta})^{|E_P|}.$$

The result follows by combining these three inequalities, together with the bound 2^{k^2} on the number of medium patterns up to isomorphism. $\square$

We are ready now to prove Theorem 1.4.

Proof. [Proof of Theorem 1.4] Suppose $f : \mathscr{G}_n \to \{0,1\}$ is computed by monotone circuits of size $O(n^{k/4})$ and satisfies $\mathrm{E}[f(\boldsymbol{K}_k)] = 1 - o(1)$. We must show that $\mathrm{E}[f(\boldsymbol{G}^-)] = 1 - \exp(-\Omega(n^{\delta}))$.

Let C be the circuit computing f. By Lemma 6.8, we have

$$\mathrm{E}[\overline{\mathsf{C}}(\boldsymbol{G}^-)] - \mathrm{E}[f(\boldsymbol{G}^-)] = \Pr[f(\boldsymbol{G}^-) \neq \overline{\mathsf{C}}(\boldsymbol{G}^-)] = \exp(-\Omega(n^{\delta})).$$

Therefore, it suffices to show that $\mathrm{E}[\overline{\mathsf{C}}(\boldsymbol{G}^-)] = 1$ (i.e., $\overline{\mathsf{C}}$ is the constant function 1).

We now assume that $\mathrm{E}[\overline{\mathsf{C}}(\boldsymbol{G}^-)] \neq 1$ and derive a contradiction. Lemma 6.10 implies that $\mathrm{E}[\overline{\mathsf{C}}(\text{random planted copy of } K_k - \{\text{single edge}\}] = o(1)$. Since $\mathrm{E}[\overline{\mathsf{C}}(\boldsymbol{K}_k)] \geq \mathrm{E}[f(\boldsymbol{K}_k)] = 1 - o(1)$, it follows that almost all k-cliques are minterms of $\overline{\mathsf{C}}$, that is, $|\mathcal{M}(\overline{\mathsf{C}}, K_k)| = (1 - o(1))\binom{n}{k}$.

For the following calculations, recall that $p = n^{-2/(k-1)}$ and $\delta = k^{-2}$. By Lemma 7.2, there is a medium pattern P such that

$$\mathsf{size}(\mathsf{C}) \geq \frac{|\mathcal{M}(\overline{\mathsf{C}}, K_k)|}{(2k)^{k^2} n^{k-|V_P|}(n^{\delta}/p^{1+\delta})^{|E_P|}} = \Omega\left(\frac{n^{|V_P| - (\frac{2}{k-1}(1+\delta)+\delta)|E_P|}}{k^k(2k)^{k^2}}\right).$$

Note that $|E_P| < k^2/4$ (since among medium patterns, the disjoint union of two $\lfloor \frac{k-1}{2} \rfloor$-cliques has the most edges). By Lemma 5.2, $|V_P| - \frac{2}{k-1}|E_P| \geq \frac{k}{4} + \frac{1}{4} + \frac{2}{k-1}$. Thus,

$$|V_P| - \left(\frac{2}{k-1}(1+\delta) + \delta\right)|E_P| > |V_P| - \frac{2}{k-1}|E_P| - \frac{1}{4}\left(1 + \frac{2}{k-1}\right) > \frac{k}{4} + \frac{1}{k}.$$

So we have $\mathsf{size}(\mathsf{C}) = \Omega(k^{-k}(2k)^{-k^2}n^{(k/4)+(1/k)})$. But since k is a constant, this contradicts the assumption that $\mathsf{size}(\mathsf{C}) = O(n^{k/4})$. $\square$

8. $\mathbf{G} \cup \mathbf{K}$ vs. $\mathbf{G} \cup \mathbf{G}^-$. In this section, we prove Theorem 1.2 using Theorem 1.4 together with the following lemma. Recall that $\boldsymbol{G} \sim G(n,p)$ and $\boldsymbol{G}^- \sim G(n, p^{1+\delta})$. Note that $\boldsymbol{G} \cup \boldsymbol{G}^- \sim G(n, p + (1-p)p^{1+\delta})$ and $p + (1-p)p^{1+\delta} = p + o(n^{-2/(k-1)})$, which is also a threshold function for k-Clique.

Lemma 8.1. *Let f be a graph function (not necessarily monotone) and let $\boldsymbol{G}_0 \sim G(n,p)$ conditioned on $\boldsymbol{G}_0$ being k-clique-free.*

1. *If f solves k-Clique w.h.p. on $\boldsymbol{G}$, then* $\mathrm{E}[f(\boldsymbol{G}_0 \cup \boldsymbol{K}_k)] = 1 - o(1)$.
2. *If f solves k-Clique w.h.p. on $\boldsymbol{G} \cup \boldsymbol{G}^-$, then* $\mathrm{E}[f(\boldsymbol{G}_0 \cup \boldsymbol{G}^-)] = o(1)$.

Proof. Let $\kappa(G)$ denote the number of k-cliques in a graph G.

(1): Suppose f solves k-Clique w.h.p. on $\boldsymbol{G}$. This means, in particular, that $\mathrm{E}[f(\boldsymbol{G}) \mid \kappa(\boldsymbol{G}) = 1] = 1 - o(1)$. Let $\boldsymbol{G}_1 \sim G(n,p)$ conditioned on $\kappa(\boldsymbol{G}_1) = 1$. Note that $\mathrm{E}[f(\boldsymbol{G}_1)] = 1 - o(1)$ (using the fact that $\Pr[\kappa(\boldsymbol{G}) = 1] = \Omega(1)$). By Lemma 2.3, random graphs $\boldsymbol{G}_0 \cup \boldsymbol{K}_k$ and $\boldsymbol{G}_1$ have total variation distance $o(1)$. Therefore, w.h.p. $\mathrm{E}[f(\boldsymbol{G}_0 \cup \boldsymbol{K}_k)] = 1 - o(1)$.

(2): Suppose f solves k-Clique w.h.p. on $\boldsymbol{G} \cup \boldsymbol{G}^-$. In particular,

$$(*) \qquad \mathrm{E}[f(\boldsymbol{G} \cup \boldsymbol{G}^-) \mid \kappa(\boldsymbol{G} \cup \boldsymbol{G}^-) = 0] = o(1).$$

Since $\boldsymbol{G} \sim G(n,p)$ and $\boldsymbol{G} \cup \boldsymbol{G}^- \sim G(n, p+o(p))$, random variables $\kappa(\boldsymbol{G})$ and $\kappa(\boldsymbol{G} \cup \boldsymbol{G}^-)$ converge in distribution to the same Poisson distribution by Lemma 2.3. In particular, we have

$$(**) \qquad \Pr[\kappa(\boldsymbol{G}) = 0] = (1+o(1)) \Pr[\kappa(\boldsymbol{G} \cup \boldsymbol{G}^-) = 0].$$

Thus, we have

$$\begin{aligned}
\mathrm{E}[f(\boldsymbol{G}_0 \cup \boldsymbol{G}^-)] &= \Pr[f(\boldsymbol{G} \cup \boldsymbol{G}^-) = 1 \mid \kappa(\boldsymbol{G}) = 0] \\
&= \frac{\Pr[f(\boldsymbol{G} \cup \boldsymbol{G}^-) = 1 \text{ and } \kappa(\boldsymbol{G}) = 0]}{\Pr[\kappa(\boldsymbol{G}) = 0]} \\
&\geq \frac{\Pr[f(\boldsymbol{G} \cup \boldsymbol{G}^-) = 1 \text{ and } \kappa(\boldsymbol{G} \cup \boldsymbol{G}^-) = 0]}{\Pr[\kappa(\boldsymbol{G}) = 0]} \\
&\overset{(**)}{=} \frac{\Pr[f(\boldsymbol{G} \cup \boldsymbol{G}^-) = 1 \text{ and } \kappa(\boldsymbol{G} \cup \boldsymbol{G}^-) = 0]}{(1+o(1)) \Pr[\kappa(\boldsymbol{G} \cup \boldsymbol{G}^-) = 0]} \\
&= (1-o(1)) \Pr[f(\boldsymbol{G} \cup \boldsymbol{G}^-) = 1 \mid \kappa(\boldsymbol{G} \cup \boldsymbol{G}^-) = 0] \\
&\overset{(*)}{=} 1 - o(1).
\end{aligned}$$

□

Proof. (of Theorem 1.2) Let C be a monotone circuit of size $O(n^{k/4})$. Toward a contradiction, assume that C solves k-Clique w.h.p. on both $\boldsymbol{G}$ and $\boldsymbol{G} \cup \boldsymbol{G}^-$. For a graph G, let C^G be the circuit obtained from C by substituting 1 for each input corresponding to an edge in G. Note that C^G computes the function $\mathsf{C}^G(H) = \mathsf{C}(G \cup H)$.

Let $\boldsymbol{G}_0 \sim G(n,p)$ conditioned on $\boldsymbol{G}_0$ being k-clique-free. Lemma 8.1 implies that for every constant $\varepsilon > 0$,

$$\begin{aligned}
&\Pr_{\boldsymbol{G}_0}\big[\mathop{\mathrm{E}}_{\boldsymbol{K}_k}[\mathsf{C}^{\boldsymbol{G}_0}(\boldsymbol{K}_k)] \geq 1 - \varepsilon\big] = 1 - o(1), \\
&\Pr_{\boldsymbol{G}_0}\big[\mathop{\mathrm{E}}_{\boldsymbol{G}^-}[\mathsf{C}^{\boldsymbol{G}_0}(\boldsymbol{G}^-)] \leq \varepsilon\big] = 1 - o(1).
\end{aligned}$$

It follows that there is a sequence of monotone circuits of size $O(n^{k/4})$ (namely, $\mathsf{C}^{\boldsymbol{G}_0}$ for almost every $\boldsymbol{G}_0$) with expected value $1 - o(1)$ on $\boldsymbol{K}_k$ and $o(1)$ on $\boldsymbol{G}^-$. But Theorem 1.4 says this is impossible, which gives the desired contradiction. □

9. Removing the Fan-in Restriction. In this section, we remove the fan-in 2 restriction in our lower bounds (Theorem 1.2 and 1.4). Let C be a fixed monotone circuit of size $O(n^{k/4})$ with $\bigwedge$-gates and $\bigvee$-gates of *unbounded fan-in.* We will show that the lower bounds of Theorems 1.2 and 1.4 (on size, as defined by the number of gates) still hold in this setting.

We first note that there is an obvious generalization of the binary operation $\overline{\vee}$ (defined by $f \mathbin{\overline{\vee}} g = \mathbf{cl}(f \vee g)$) to a multi-ary operation $\overline{\bigvee}$ on functions $f_1, \dots, f_m$, which we define by $\overline{\bigvee}_{i=1}^m f_i = \mathbf{cl}\big(\bigvee_{i=1}^m f_i\big)$. Denote by $\overline{\mathsf{C}}$ the $\{\bigwedge, \overline{\bigvee}\}$-circuit obtained by replacing $\bigvee$-gates in C with $\overline{\bigvee}$-gates.

There is only one place in the proof of Theorem 1.4 where the fan-in 2 assumption comes into play: namely in Lemma 7.1. To be precise, this lemma relies on the fact that if f_1 and f_2 are monotone graph functions with only small minterms, then $f_1 \wedge f_2$ has no large minterms. This is a consequence of facts:

- the union of two small graphs is either small or medium, and

- $\mathcal{M}(f_1 \wedge f_2) \subseteq \{F_1 \cup F_2 : F_1 \in \mathcal{M}(f_1),\ F_1 \in \mathcal{M}(f_2)\}$ (Lemma 2.1).

The trouble is that the union of three or more small graphs can be large. So Lemma 7.1 is invalid for the circuit C.

We get around this problem as follows. Denote by $[k \log n]$ the set $\{1, \dots, \lceil k \log n \rceil\}$ and by $[n^{1/2k}]$ the set $\{1, \dots, \lceil n^{1/2k} \rceil\}$. For every $\bigwedge$-gate ν in C and $i \in [k \log n]$ and $j \in [n^{1/2k}]$, generate a random set $\boldsymbol{S}_{\nu,i,j} \subseteq_{2^{-i}}$ Children(ν) (that is, $\boldsymbol{S}_{\nu,i,j}$ independently contains each child of ν with probability 2^{-i}). We replace Lemma 7.1 with the following:

Lemma 9.1. *With probability* $1 - \exp(-\Omega(n^{1/3k}))$*, the following holds: for every* $H \in \mathcal{M}(\overline{\mathsf{C}}, K_k)$*, there exist a gate* ν *in* C *and a medium subgraph* H' *of* H *such that either*

- ν *is an* $\bigvee$*-gate and* $H' \in \mathcal{M}(\overline{\nu})$*, or*
- ν *is an* $\bigwedge$*-gate and* $H' \in \mathcal{M}(\bigwedge_{\mu \in \boldsymbol{S}_{\nu,i,j}} \overline{\mu})$ *for some* $i \in [k \log n]$ *and* $j \in [n^{1/2k}]$.

Proof. Suppose $H \in \mathcal{M}(\overline{\mathsf{C}}, K_k)$ and for notational convenience let

$$\mathcal{H} = \{\text{subgraphs of } H\}, \quad \mathcal{A} = \{\text{small graphs}\}, \quad \mathcal{B} = \{\text{medium graphs}\}.$$

An easy argument (along the lines of the proof of Lemma 7.1) shows that there exists a gate ν in C, with children $\mu_1, \dots, \mu_m$, such that

1. $\mathcal{M}(\overline{\mu_\ell}) \cap \mathcal{H} \subseteq \mathcal{A}$ for all $\ell \in [m]$, and
2. $\big(\mathcal{M}(\overline{\nu}) \cap \mathcal{H}\big) \setminus \mathcal{A}$ is nonempty.

Fix any $H' \in \big(\mathcal{M}(\overline{\nu}) \cap \mathcal{H}\big) \setminus \mathcal{A}$.

In the case where ν is $\bigvee$-gate, we have

$$\begin{aligned}
\mathcal{M}(\overline{\nu}) &= \mathcal{M}(\overline{\textstyle\bigvee}_{\ell \in [m]} \overline{\mu_\ell}) & \\
&= \mathcal{M}(\mathbf{cl}(\textstyle\bigvee_{\ell \in [m]} \overline{\mu_\ell})) & \text{(definition of } \overline{\textstyle\bigvee}) \\
&\subseteq \mathcal{M}(\textstyle\bigvee_{\ell \in [m]} \overline{\mu_\ell}) \cup \mathcal{A} \cup \mathcal{B} & \text{(Lemma 6.7)} \\
&\subseteq \textstyle\bigcup_{\ell \in [m]} \mathcal{M}(\overline{\mu_\ell}) \cup \mathcal{A} \cup \mathcal{B} & \text{(Lemma 2.1).}
\end{aligned}$$

Since $H' \notin \mathcal{A}$ and $\mathcal{M}(\overline{\mu_\ell}) \cap \mathcal{H} \subseteq \mathcal{A}$ for all $\ell \in [m]$, it follows that $H' \in \mathcal{B}$ (i.e., H' is medium, so we are done).

Now suppose ν is an $\bigwedge$-gate. We have

$$\begin{aligned}
\mathcal{M}(\overline{\nu}) &= \mathcal{M}(\textstyle\bigwedge_{\ell \in [m]} \overline{\mu_\ell}) \\
&\subseteq \{F_1 \cup \cdots \cup F_m : F_1 \in \mathcal{M}(\overline{\mu_1}),\ \dots,\ F_m \in \mathcal{M}(\overline{\mu_m})\} \qquad \text{(Lemma 2.1).}
\end{aligned}$$

Hence there exist $F_1 \in \mathcal{M}(\overline{\mu_1}),\ \dots,\ F_m \in \mathcal{M}(\overline{\mu_m})$ such that $H' = F_1 \cup \cdots \cup F_m$. Fix any such $F_1, \dots, F_m$.

We next fix an enumeration $H_1, \dots, H_t$ of the set $\{F_1, \dots, F_m\}$ subject to

$$|\{\ell \in [m] : H_{t'} = F_\ell\}| \geq |\{\ell \in [m] : H_{t'+1} = F_\ell\}|$$

for all $t' \in \{1, \dots, t-1\}$. (That is, $H_{t'}$ are ranked in decreasing order according to their frequency among $F_1, \dots, F_m$.) Note that $t \leq 2^{k^2}$ (even though m may be as large as $n^{k/4}$), since there are $\leq 2^{k^2}$ distinct subgraphs of H.

Let s be the least index in $\{2, \dots, t\}$ such that $H_1 \cup \cdots \cup H_s \notin \mathcal{A}$. (Such s is well-defined since $H_1 \cup \cdots \cup H_t = F_1 \cup \cdots \cup F_m = H' \notin \mathcal{A}$.) Note that $H_1 \cup \cdots \cup H_s \in \mathcal{B}$, since $H_1 \cup \cdots \cup H_{s-1} \in \mathcal{A}$ and $H_s \in \mathcal{A}$ (using the fact that the union of two small graphs is either small or medium). Let i be the unique integer in $[k \log n]$ such that

$$2^{i-1} \leq |\{\ell \in [m] : H_s = F_\ell\}| < 2^i.$$

(Such i exists since $m \leq \mathsf{fanin}(\mathsf{C}) \leq \mathsf{size}(\mathsf{C}) = O(n^{k/4})$.)

We now show that, with extremely high probability, there exists $j \in [n^{1/2k}]$ such that $H_1 \cup \cdots \cup H_s \in \mathcal{M}(\bigwedge_{\mu \in \boldsymbol{S}_{\nu,i,j}} \overline{\mu})$. Consider a random set $\boldsymbol{S} \subseteq_{2^{-i}} [m]$. For $t' \in \{1,\dots,t\}$, denote by $\boldsymbol{X}_{t'}$ the event that there exists $\ell \in \boldsymbol{S}$ such that $H_{t'} \in \mathcal{M}(\overline{\mu_\ell})$. Note the following:

- for $t' \in \{1,\dots,s\}$,

$$\Pr[\boldsymbol{X}_{t'}] = 1 - (1-2^{-i})^{|\{\ell \in [m] : H_{t'} = F_\ell\}|} \geq 1 - (1-2^{-i})^{2^{i-1}} > 1 - \frac{1}{\sqrt{e}} > \frac{1}{4},$$

- for $t' \in \{s+1,\dots,t\}$,

$$\Pr[\neg \boldsymbol{X}_{t'}] \geq (1-2^{-i})^{|\{\ell \in [m] : H_{t'} = F_\ell\}|} > (1-2^{-i})^{2^{i}} \geq \frac{1}{4}.$$

Note that $\boldsymbol{X}_1,\dots,\boldsymbol{X}_t$ are independent. It follows that

$$\begin{aligned}
\Pr\left[H_1 \cup \cdots \cup H_s \in \mathcal{M}(\textstyle\bigwedge_{\ell \in \boldsymbol{S}} \overline{\mu_\ell})\right] &\geq \Pr\left[(\boldsymbol{X}_1 \wedge \cdots \wedge \boldsymbol{X}_s) \wedge (\neg \boldsymbol{X}_{s+1} \wedge \cdots \wedge \neg \boldsymbol{X}_t)\right] \\
&= \Big(\prod_{t' \in \{1,\dots,s\}} \Pr[\boldsymbol{X}_{t'}]\Big)\Big(\prod_{t' \in \{s+1,\dots,t\}} \Pr[\neg \boldsymbol{X}_{t'}]\Big) \\
&\geq 4^{-t} \\
&\geq 4^{-2^{k^2}}.
\end{aligned}$$

By independence (for different $j \in [n^{1/2k}]$) of sets $\boldsymbol{S}_{\nu,i,j}$, we have

$$\begin{aligned}
&\Pr\left[\forall j \in [n^{1/2k}],\ H_1 \cup \cdots \cup H_s \notin \mathcal{M}(\textstyle\bigwedge_{\mu \in \boldsymbol{S}_{\nu,i,j}} \overline{\mu})\right] \\
&\qquad \leq \prod_{j \in [n^{1/2k}]} \Pr\left[H_1 \cup \cdots \cup H_s \notin \mathcal{M}(\overline{\boldsymbol{\sigma}_{\nu,i,j}})\right] \\
&\qquad \leq \left(1 - 4^{-2^{k^2}}\right)^{n^{1/2k}} \\
&\qquad \leq \exp(-4^{-2^{k^2}} n^{1/2k}).
\end{aligned}$$

Taking a union bound over all $\leq \binom{n}{k}$ graphs $H \in \mathcal{M}(\overline{C}, K_k)$, we upper bound the total failure probability by

$$\binom{n}{k} \exp(-4^{-2^{k^2}} n^{1/2k}) = \exp(-\Omega(n^{1/3k})),$$

which proves the lemma. □

We now get the following modified version of Lemma 7.2.

Lemma 9.2. *With probability* $1 - \exp(-\Omega(n^{1/3k}))$, *there exists a medium pattern* P *such that*

$$\mathsf{size}(\mathsf{C}) \geq \frac{1}{(k \log n) n^{1/2k}} \cdot \frac{|\mathcal{M}(\overline{\mathsf{C}}, K_k)|}{(2k)^{k^2} n^{k-|V_P|} (n^{\delta}/p^{1+\delta})^{|E_P|}}.$$

Proof. The argument is nearly identical to the proof of Lemma 7.2, with Lemma 9.1 playing the role of Lemma 7.1. □

Compared with Lemma 7.2, the bound in Lemma 9.2 incurs a loss of $1/(k \log n) n^{1/2k}$. To achieve a lower bound of $\omega(n^{k/4})$, this loss is tolerable since it is eaten up by the slack factor of $n^{1/k}/k^k(2k)^{k^2}$ in the actual bound $\mathsf{size}(\mathsf{C}) = \Omega(n^{(k/4)+(1/k)}/k^k(2k)^{k^2})$ given by the proof of Theorem 1.4. The fact that the bottleneck of Lemma 9.2 fails with probability $\exp(-\Omega(n^{1/3k}))$ is also tolerable, since the error $\mathrm{E}[\overline{\mathsf{C}}(\boldsymbol{G}^-)] - \mathrm{E}[\mathsf{C}(\boldsymbol{G}^-)]$ allowed by the proof of Theorem 1.4 is $\exp(-\Omega(n^\delta))$ where $\delta = 1/k^2 = o(1/3k)$. By this argument, it is seen that the lower bounds proved in this paper remain valid for monotone circuits with unbounded fan-in.

10. Matching Upper Bound.

In this section, we prove Theorem 1.3 (restated below). This theorem shows that the exponent $k/4$ in our lower bound (Theorem 1.2) is tight up to an additive constant.

THEOREM 10.1 (Theorem 1.3 restated). *There exist monotone circuits* C *of size* $n^{k/4+O(1)}$ *and depth* $3k$ *such that* C *solves* k-CLIQUE *w.h.p. on* $G(n,q)$ *for every function* $q : \mathbb{N} \to [0,1]$.

The monotone circuits C constructed in the proof of Theorem 1.3 are adapted from non-monotone AC^0 circuits for the average-case k-CLIQUE problem due to Amano [5]. We briefly describe the idea behind Amano's construction. Consider the random graph $\boldsymbol{G} \sim G(n,p)$ at a k-clique threshold $p = \Theta(n^{-2/(k-1)})$. Pick random sets $U_1, \dots, U_k \subseteq \{1, \dots, n\}$ such that U_i has size slightly less than $\min(p^{-i}, n)$. Let's say that $(U_1, \dots, U_k)$ *isolates a k-clique* if there exists a k-clique $\{u_1, \dots, u_k\}$ in $\boldsymbol{G}$ such that for all $i \in \{1, \dots, k\}$, u_i is the unique common neighbor in the set U_i of vertices $u_1, \dots, u_{i-1}$. The key observation is that, for any fixed choice of $U_1, \dots, U_k$, it's possible to test whether $(U_1, \dots, U_k)$ isolates a k-clique in $\boldsymbol{G}$ via AC^0 circuits of size $\widetilde{O}(n)$ and depth $O(k)$. Taking a disjunction of these circuits over $n^{k/4+O(1)}$ independent choices of $U_1, \dots, U_k$, we get an AC^0 circuit of size $n^{k/4+O(1)}$ and depth $O(k)$ which solves k-CLIQUE w.h.p. on $\boldsymbol{G}$. (The actual circuits from Amano's paper [5] have a different description, but the essential idea is the same.)

We will show how to carry out this construction with monotone circuits. One immediate challenge is that the graph property "$(U_1, \dots, U_k)$ isolates a k-clique" is non-monotone. We work around this problem using a technique that involves hash functions.

REMARK 10.2. A typical *maximal* (as opposed to *maximum*) clique in $\boldsymbol{G} \sim G(n, n^{-2/(k-1)})$ has size $\lfloor k/2 \rfloor$ or $\lceil k/2 \rceil$. Unlike maximum cliques, maximal cliques are easy to find: they can be sampled roughly uniformly at random in linear time via a simple greedy algorithm (cf. the discussion of Karp's question in §1). It turns out that $\boldsymbol{G}$ has $n^{k/4+O(1)}$ maximal cliques in expectation. By running the greedy algorithm $n^{k/4+O(1)}$ times (each time using fresh randomness to extend cliques as far as possible), we can enumerate all the maximal cliques (including the maximum cliques) with high probability. This gives a randomized $n^{k/4+O(1)}$ time algorithm for solving k-CLIQUE w.h.p. on $\boldsymbol{G}$. This observation is closely related to the above description of Amano's AC^0 circuits.

10.1. Subcircuits $\mathsf{A}_{U_1,\dots,U_\ell}$ and $\mathsf{B}^c_{U_1,\dots,U_\ell}$.

To define the circuit C in Theorem 1.3, we start by defining its principal subcircuits.

DEFINITION 10.3. *For a graph* $G \in \mathscr{G}_n$ *and sets* $U_1, \dots, U_\ell \subseteq [n]$ *where* $\ell \geq 1$, *define* $\Gamma_G(U_1, \dots, U_\ell) \subseteq U_\ell$ *inductively as follows:*

- $\Gamma_G(U_1) = U_1$,
- *for* $\ell \geq 2$, $\Gamma_G(U_1, \dots, U_\ell)$ *is the set of* $u_\ell \in U_\ell$ *such that for every* $i \in \{1, \dots, \ell - 1\}$, *there exists* $u_i \in \Gamma_G(U_1, \dots, U_i)$ *such that* $\{u_i, u_\ell\}$ *is an edge in* G.

Lemma 10.4. *If $\Gamma_G(U_1, \dots, U_i)$ is a singleton $\{u_i\}$ for each $i \in \{1, \dots, \ell\}$, then $u_1, \dots, u_\ell$ form an ℓ-clique in G.*

Proof. Immediate from the definition of $\Gamma_G(\cdot)$. □

Lemma 10.5. *There exist monotone circuits $\mathsf{A}_{U_1,\dots,U_\ell}$ of size $\le \ell^2 n^2$ and depth $3(\ell-1)$ with n output nodes, denoted $\mathsf{A}^v_{U_1,\dots,U_\ell}$ for $v \in [n]$, such that for every graph $G \in \mathscr{G}_n$ and vertex $v \in [n]$,*

$$\mathsf{A}^v_{U_1,\dots,U_\ell}(G) = 1 \iff v \in \Gamma_G(U_1, \dots, U_\ell).$$

Proof. The proof is by induction on ℓ. In the base case where $\ell = 1$, the circuit A_{U_1} consists of n isolated output nodes where $\mathsf{A}^v_{U_1}$ is labeled by the constant 1 if $v \in U_1$ and by the constant 0 otherwise.

For the induction step, assume $\ell \ge 2$. Starting with the circuit $\mathsf{A}_{U_1,\dots,U_{\ell-1}}$, for each $v \in [n]$ create new gates ν_v and $(\mu_{v,i})_{i \in \{1,\dots,\ell-1\}}$ and $(\xi_{v,i,w})_{i \in \{1,\dots,\ell-1\},\, w \in [n] \setminus \{v\}}$. The labels and wires are as follows:

- $\nu_v = \operatorname*{AND}_{i \in \{1,\dots,\ell-1\}} \mu_{v,i}$,
- $\mu_{v,i} = \operatorname*{OR}_{w \in [n] \setminus \{v\}} \xi_{v,i,w}$,
- $\xi_{v,i,w} = \text{AND}(X_{\{v,w\}}, \mathsf{A}^w_{U_1,\dots,U_i})$ where $X_{\{v,w\}}$ is the indicator variable for the edge $\{v,w\}$.

The output node $\mathsf{A}^v_{U_1,\dots,U_{\ell-1}}$ is of course ν_v.

It is easy to see that $\mathsf{A}_{U_1,\dots,U_\ell}$ correctly computes the set $\Gamma_G(U_1, \dots, U_\ell)$ (assuming that $\mathsf{A}_{U_1,\dots,U_i}$ correctly computes $\Gamma_G(U_1, \dots, U_i)$ for every $i \in \{1, \dots, \ell-1\}$). Note that we have added 3 to the depth and created $(\ell-1)n^2 + n \le \ell n^2$ new gates. Thus, as required we have

- $\mathsf{depth}(\mathsf{A}_{U_1,\dots,U_\ell}) = \mathsf{depth}(\mathsf{A}_{U_1,\dots,U_{\ell-1}}) + 3 = 3(\ell-1)$,
- $\mathsf{size}(\mathsf{A}_{U_1,\dots,U_\ell}) \le \mathsf{size}(\mathsf{A}_{U_1,\dots,U_{\ell-1}}) + \ell n^2 \le (\ell-1)^2 n^2 + \ell n^2 \le \ell^2 n^2$.

□

Next comes another useful definition, followed by a description of circuits $\mathsf{B}^c_{U_1,\dots,U_\ell}$.

Definition 10.6. *A sequence $(U_1, \dots, U_\ell)$ is* c-bounded *in graph G if for all $i \in \{1, \dots, \ell\}$ and distinct $u_1 \in U_1, \dots, u_{i-1} \in U_{i-1}$, there are at most c different $u_i \in U_i$ such that $\{u_j, u_i\}$ is an edge in G for all $j \in \{1, \dots, i-1\}$.*

Lemma 10.7. *For all $c, \ell \in \mathbb{N}$, there exist single-output monotone circuits $\mathsf{B}^c_{U_1,\dots,U_\ell}$ of size $O(n^2 \log n)$ and depth $3\ell - 1$ such that for every graph G, if $(U_1, \dots, U_\ell)$ is c-bounded in G then*

$$\mathsf{B}^c_{U_1,\dots,U_\ell}(G) = 1 \iff U_1 \times \cdots \times U_\ell \text{ contains an } \ell\text{-clique in } G.$$

(The hidden constant in this $O(\cdot)$ term is $\ell c^\ell 4^{\ell c^\ell}$.)

Proof. Let $\mathcal{H}$ be an ℓc^ℓ-perfect family of $O(4^{\ell c^\ell} \log n)$ hash functions from $[n]$ to $[\ell c^\ell]$. That is, $\mathcal{H}$ is a set of functions $[n] \to [\ell c^\ell]$ such that for every $X \subseteq [n]$ such that $|X| \le \ell c^\ell$, there exists $h \in \mathcal{H}$ such that $|h(X)| = |X|$. The existence of an ℓc^ℓ-perfect family $|\mathcal{H}|$ of size $O(4^{\ell c^\ell} \log n)$ is established by a probabilistic argument: simply choose $4^{\ell c^\ell} \log n$ functions at random for sufficiently large n (see [4]).

Define $\mathsf{B}^c_{U_1,\dots,U_\ell}$ by

$$\mathsf{B}^c_{U_1,\dots,U_\ell} = \operatorname*{AND}_{h \in \mathcal{H}} \ \operatorname*{OR}_{z_1,\dots,z_\ell \in [\ell c^\ell],\, v \in [n]} \mathsf{A}^v_{U_1 \cap h^{-1}(z_1),\dots,U_\ell \cap h^{-1}(z_\ell)}.$$

Finally, note that $\mathsf{B}^c_{U_1,\dots,U_\ell}$ has size $O(n^2 \log n)$ and depth $3\ell - 1$.

To see that $\mathsf{B}^c_{U_1,\dots,U_\ell}$ computes a suitable function, let G be any graph such that $(U_1,\dots,U_\ell)$ is c-bounded in G. We will now show that $\mathsf{B}^c_{U_1,\dots,U_\ell}(G) = 1 \iff U_1 \times \cdots \times U_\ell$ contains an ℓ-clique in G.

($\Longleftarrow$) Assume that $u_1,\dots,u_\ell$ form an ℓ-clique in G where $u_i \in U_i$ for every $i \in \{1,\dots,\ell\}$. To show that $\mathsf{B}^c_{U_1,\dots,U_\ell}(G) = 1$, let h be any function in $\mathcal{H}$ (chosen adversarially). Select any $z_i = h^{-1}(u_i)$ for each $i \in \{1,\dots,\ell\}$ and note that $\mathsf{A}^{u_\ell}_{U_1 \cap h^{-1}(z_1),\dots,U_\ell \cap h^{-1}(z_\ell)}(G) = 1$.

($\Longrightarrow$) Assume that $\mathsf{B}^c_{U_1,\dots,U_\ell}(G) = 1$. Let $X = \bigcup_{i\in\{1,\dots,\ell\}} \Gamma_{U_1,\dots,U_i}(G)$. Since $(U_1,\dots,U_\ell)$ is c-bounded in G, we have $|X| \le c + c^2 + \cdots + c^\ell \le \ell c^\ell$. Since $\mathcal{H}$ is an ℓc^ℓ-perfect family of hash functions, there exists $h \in \mathcal{H}$ such that $|h(X)| = |X|$. By definition of $\mathsf{B}^c_{U_1,\dots,U_\ell}$, there exist $z_1,\dots,z_\ell \in [\ell c^\ell]$ such that

$$\operatorname*{OR}_{v\in[n]} \mathsf{A}^v_{U_1\cap h^{-1}(z_1),\dots,U_\ell\cap h^{-1}(z_\ell)}(G) = 1.$$

An inductive argument shows that $\Gamma_G(U_1 \cap h^{-1}(z_1),\dots,U_i \cap h^{-1}(z_i))$ is a singleton for every $i \in \{1,\dots,\ell\}$. By Lemma 10.4, it follows that G contains an ℓ-clique in $U_1 \times \cdots \times U_\ell$. □

10.2. Random sets $\mathbf{U}^{(t)}_1,\dots,\mathbf{U}^{(t)}_k$.

Using the circuits $\mathsf{B}^c_{U_1,\dots,U_\ell}$ defined in the last section, we now present a monotone constant-depth circuit of size $n^{k/4+O(1)}$ which solves k-Clique on $G(n,p)$ for all functions $p : \mathbb{N} \to [0,1]$.

Definition 10.8. *For $i \in \{1,\dots,k\}$, let $p_i = \min\{n^{(i-2)\frac{2}{k}-1}, 1\}$ and let $\boldsymbol{U}_i \subseteq_{p_i} [n]$ (that is, $\Pr[v \in \boldsymbol{U}_i] = p_i$ independently for all $v \in [n]$).*

This definition of random sets $\boldsymbol{U}_i$ is motivated by the following lemma.

Lemma 10.9. *For all $\alpha \ge 2/k$ and $i \in \{1,\dots,k\}$ and distinct $v_1,\dots,v_{i-1} \in [n]$,*

$$\Pr_{\boldsymbol{G}\sim G(n,n^{-\alpha})}\big[\boldsymbol{U}_i \text{ contains} > c \text{ common neighbors of } v_1,\dots,v_{i-1} \text{ in } \boldsymbol{G}\big] = O(n^{-\frac{2}{k}(c+1)}).$$

Proof. For each $w \in [n]\backslash\{v_1,\dots,v_{i-1}\}$, the probability that w belongs to $\boldsymbol{U}_i$ and is a common neighbor of $v_1,\dots,v_{i-1}$ in $\boldsymbol{G}$ is precisely $p_i(n^{-\alpha})^{i-1}$. Since $p_i \le n^{(i-2)\frac{2}{k}-1}$ and $n^{-\alpha} \le n^{-\frac{2}{k}}$, we have $p_i(n^{-\alpha})^{i-1} \le n^{-1-\frac{2}{k}}$. By a union bound and independence,

$$\begin{aligned}
&\Pr\big[\boldsymbol{U}_i \text{ contains} > c \text{ common neighbors of } v_1,\dots,v_{i-1} \text{ in } \boldsymbol{G}\big]\\
&\qquad \le \sum_{\text{distinct } w_1,\dots,w_{c+1}\in[n]\backslash\{v_1,\dots,v_{i-1}\}} \Pr\begin{bmatrix} w_1,\dots,w_{c+1} \in \boldsymbol{U}_i \text{ are common}\\ \text{neighbors of } v_1,\dots,v_{i-1} \text{ in } \boldsymbol{G}\end{bmatrix}\\
&\qquad = \binom{n-i+1}{c+1}\left(n^{-1-\frac{2}{k}}\right)^{c+1}\\
&\qquad = O(n^{-\frac{2}{k}(c+1)}).
\end{aligned}$$

□

We proceed by stating four lemmas that give further properties of $\boldsymbol{U}_1,\dots,\boldsymbol{U}_k$.

Lemma 10.10. $p_1 p_2 \cdots p_k \ge n^{-(k/4)-3}$.

Proof. We have $p_1 p_2 \cdots p_k = n^{-\beta}$ where

$$\beta = \sum_{i=1}^{k} \max\left\{0,\, 1-(i-2)\frac{2}{k}\right\} = \sum_{i=1}^{\lfloor \frac{k}{2}\rfloor+2} \left(1-(i-2)\frac{2}{k}\right)$$
$$= \left(\left\lfloor\frac{k}{2}\right\rfloor+2\right)\left(1+\frac{2}{k}\right) - \frac{2}{k}\binom{\lfloor\frac{k}{2}\rfloor+1}{2} < \frac{k}{4}+3.$$

□

Lemma 10.11. *For all $\alpha \geq 2/k$ and $\boldsymbol{G} \sim G(n, n^{-\alpha})$,*

$$\Pr\big[(\boldsymbol{U}_1,\dots,\boldsymbol{U}_k) \text{ is not } k^2\text{-bounded in } \boldsymbol{G}\big] = O(n^{-k}).$$

Proof. We have

$$\Pr\big[(\boldsymbol{U}_1,\dots,\boldsymbol{U}_k) \text{ is not } k^2\text{-bounded in } \boldsymbol{G}\big]$$
$$\leq \sum_{\text{distinct } v_1,\dots,v_k\in[n]} \sum_{i\in\{1,\dots,k\}} \Pr\begin{bmatrix}\boldsymbol{U}_i \text{ contains} > k^2 \text{ common}\\ \text{neighbors of } v_1,\dots,v_{i-1} \text{ in } \boldsymbol{G}\end{bmatrix}$$
$$\leq \binom{n}{k} k \cdot O(n^{-\frac{2}{k}(k^2+1)}) \qquad \text{(Lemma 10.9)}$$
$$= O(n^{-k}).$$

□

Definition 10.12. *Let $S = \lceil n^{(k/4)+4}\rceil$ and let $\boldsymbol{U}_1^{(t)},\dots,\boldsymbol{U}_k^{(t)}$ be independent copies of $\boldsymbol{U}_1,\dots,\boldsymbol{U}_k$ for $t \in \{1,\dots,S\}$.*

We choose S large enough so that the following lemma holds.

Lemma 10.13. *W.h.p.,* $\displaystyle\bigcup_{t\in\{1,\dots,S\}} \boldsymbol{U}_1^{(t)} \times \cdots \times \boldsymbol{U}_k^{(t)} = [n]^k$.

Proof. Another straightforward calculation:

$$\Pr\Big[\bigcup_{t\in\{1,\dots,S\}} \boldsymbol{U}_1^{(t)} \times\cdots\times \boldsymbol{U}_k^{(t)} \neq [n]^k\Big]$$
$$= \Pr\Big[\bigvee_{v_1,\dots,v_k\in[n]} \bigwedge_{t\in\{1,\dots,S\}} \bigvee_{i\in\{1,\dots,k\}} v_i \notin \boldsymbol{U}_i^{(t)}\Big]$$
$$\leq \sum_{v_1,\dots,v_k\in[n]} \Pr\Big[\bigwedge_{t\in\{1,\dots,S\}} \bigvee_{i\in\{1,\dots,k\}} v_i \notin \boldsymbol{U}_i^{(t)}\Big] \qquad \text{(union bound)}$$
$$= \sum_{v_1,\dots,v_k\in[n]} \Big(\Pr\Big[\bigvee_{i\in\{1,\dots,k\}} v_i \notin \boldsymbol{U}_i\Big]\Big)^S \qquad \text{(independence)}$$
$$= \sum_{v_1,\dots,v_k\in[n]} \Big(1-\Pr\Big[\bigwedge_{i\in\{1,\dots,k\}} v_i \in \boldsymbol{U}_i\Big]\Big)^S$$
$$= \sum_{v_1,\dots,v_k\in[n]} \Big(1-\prod_i p_i\Big)^S$$
$$\leq n^k\big(1-n^{-(k/4)-3}\big)^{n^{(k/4)+4}} \qquad \text{(Lemma 10.10)}$$
$$= o(1).$$

□

Lemma 10.14. *There exist sets $U_1^{(t)}, \dots, U_k^{(t)}$ $(t \in \{1, \dots, S\})$, such that*

1. $\displaystyle\bigcup_{t \in \{1,\dots,S\}} U_1^{(t)} \times \cdots \times U_k^{(t)} = [n]^k$, *and*
2. *for all $\alpha \geq 2/k$, w.h.p. for $\boldsymbol{G} \sim G(n, n^{-\alpha})$,*

$$(U_1^{(t)}, \dots, U_k^{(t)}) \text{ is } k^2\text{-bounded in } \boldsymbol{G} \text{ for all } t \in \{1, \dots, S\}.$$

Proof. Follows from Lemma 10.11 (taking a union bound over t) and Lemma 10.13.

□

10.3. Proof of Theorem 1.3. We now prove Theorem 1.3. Fix sets $U_1^{(t)}, \dots, U_k^{(t)}$ $(t \in \{1, \dots, S\})$ as in Lemma 10.14. Let $\mathcal{E}$ be an arbitrary subset $\binom{[n]}{2}$ of size $\lceil n^{2/(k-(1/2))} \rceil$. The circuit C is defined by

$$\mathsf{C} = \Big(\operatorname*{OR}_{t \in \{1,\dots,S\}} \mathsf{B}^{k^2}_{U_1^{(t)},\dots,U_k^{(t)}} \Big) \text{ OR } \Big(\operatorname*{OR}_{\{v,w\} \in \mathcal{E}} X_{\{v,w\}} \Big).$$

(Here the subcircuit $\mathrm{OR}_{\{v,w\}\in\mathcal{E}}\ X_{\{v,w\}}$ has value 1 on a graph G if, and only if, some element of $\mathcal{E}$ is an edge in G.)

We check that the circuit C has the correct size and depth. C has size $O(Sn^3 \log n) = n^{k/4+O(1)}$ as each B subcircuit has size $O(n^3 \log n)$. Combining the three OR gates at the top of C, we see that C has depth $3k$ as each B has depth $3k - 1$.

It remains to show that C solves k-Clique w.h.p. on $\boldsymbol{G} \sim G(n,p)$ for all functions $p : \mathbb{N} \to [0,1]$. We split the argument into three cases.

Case 1: $p \geq n^{-2/k}$.

W.h.p. $\boldsymbol{G}$ contains a k-clique (by Lemma 2.2 since $n^{-2/k} = \omega(n^{-2/(k-1)})$) as well as an edge in $\mathcal{E}$. So w.h.p. both $\mathsf{C}(\boldsymbol{G})$ and k-Clique$(\boldsymbol{G})$ equal 1.

Case 2: $n^{-2/(k-(1/4))} < p < n^{-2/k}$.

W.h.p. $\boldsymbol{G}$ contains a k-clique. Let $\checkmark$ $(= \checkmark(\boldsymbol{G}))$ be the event that $(U_1^{(t)}, \dots, U_k^{(t)})$ is k^2-bounded in $\boldsymbol{G}$ for all $t \in \{1, \dots, S\}$. Since $p \leq n^{-2/k}$, $\checkmark$ holds almost surely by Lemma 10.14(2). *We may therefore condition on $\checkmark$ and the event that $\boldsymbol{G}$ contains a k-clique.* It now suffices to show that $\mathsf{C}(\boldsymbol{G}) = 1$. Let $\{v_1, \dots, v_k\}$ be a k-clique in $\boldsymbol{G}$. By Lemma 10.14(1), there exists $t \in \{1, \dots, S\}$ such that $(v_1, \dots, v_k) \in U_1^{(t)} \times \cdots \times U_k^{(t)}$. Since $(U_1^{(t)}, \dots, U_k^{(t)})$ is k^2-bounded (by $\checkmark$), Lemma 10.7 implies that $\mathsf{B}^{k^2}_{U_1^{(t)},\dots,U_k^{(t)}}(G) = 1$ and hence $\mathsf{C}(\boldsymbol{G}) = 1$.

Case 3: $p \leq n^{-2/(k-(1/4))}$.

As in Case 2, $\checkmark$ holds almost surely. Since $p = o(n^{-2/(k-(1/2))})$, w.h.p. $\boldsymbol{G}$ contains no edge in $\mathcal{E}$. *We may therefore condition on $\checkmark$ and the event that $\boldsymbol{G}$ contains no edge in $\mathcal{E}$.* It suffices to show that $\mathsf{C}(\boldsymbol{G}) = 1$ if, and only if, $\boldsymbol{G}$ contains a k-clique. If $\boldsymbol{G}$ contains a k-clique $\{v_1, \dots, v_k\}$, then $\mathsf{C}(\boldsymbol{G}) = 1$ by same reasoning as in Case 2. For the converse direction, assume $\mathsf{C}(\boldsymbol{G}) = 1$. Then $B^{k^2}_{U_1^{(t)},\dots,U_k^{(t)}}(\boldsymbol{G}) = 1$ for some $t \in \{1, \dots, S\}$. Since $(U_1^{(t)}, \dots, U_k^{(t)})$ is k^2-bounded (by $\checkmark$), Lemma 10.7 implies that $U_1^{(t)} \times \cdots \times U_k^{(t)}$ contains a k-clique in $\boldsymbol{G}$.

11. Concluding Remarks. We point out that there is a trade-off in Theorem 1.2 between the strength of the lower bound and the size of the *gap* $p^+ - p$ $(= p^{1+(1/k^2)})$ between thresholds p and p^+. This trade-off is easily extracted from the proof of Theorem 1.2. We can express this trade-off as follows:

THEOREM 11.1. *For all* $\lambda \in [0,1]$, *monotone circuits of size* $O(n^{(1-\lambda)k/4})$ *cannot solve* k-CLIQUE *w.h.p. on both* $G(n,p)$ *and* $G(n, p + p^{1+(\lambda/k)})$.

We thus get non-trivial lower bounds for a gap of size $p^{1+((1+\varepsilon)/k)}$. It is a challenge for future research to reduce or eliminate this gap. In fact, we conjecture that the gap is unnecessary, i.e., that Theorem 1.2 applies to monotone circuits which solve k-CLIQUE w.h.p. at a single threshold.

CONJECTURE 11.2. *Monotone circuits of size* $O(n^{k/4})$ *cannot solve* k-CLIQUE *w.h.p. on* $G(n,p)$.

We view Theorem 1.2 as strong evidence for Conjecture 11.2. Unfortunately, the existing Approximation Method framework seems to require that the distributions on positive and negative instances be well separated, with the negative instances having significantly higher Hamming weight. For this reason, we speculate that entirely new techniques might be needed to prove Conjecture 11.2.

Finally, it would be interesting to find other applications of quasi-sunflowers. Given the many applications of sunflowers, we believe that quasi-sunflowers might be useful in a variety of settings.

Acknowledgements. I am grateful to Madhu Sudan, Sasha Razborov, Osamu Watanabe and Will Perkins for valuable discussions. Thanks also to the anonymous referees for their helpful comments.

REFERENCES

[1] Noga Alon and Ravi B. Boppana. The monotone circuit complexity of boolean functions. *Combinatorica*, 7(1):1–22, 1987.

[2] Noga Alon, Michael Krivelevich, and Benny Sudakov. Finding a large hidden clique in a random graph. *Random Structures and Algorithms*, 13(3-4):457–466, 1998.

[3] Noga Alon and Joel Spencer. *The Probabilistic Method, 3rd Edition.* John Wiley, 2008.

[4] Noga Alon, Raphael Yuster, and Uri Zwick. Color-coding. *Journal of the ACM*, 42(4):844–856, 1995.

[5] Kazuyuki Amano. k-Subgraph isomorphism on AC^0 circuits. *Computational Complexity*, 19(2):183–210, 2010.

[6] Kazuyuki Amano and Akira Maruoka. A superpolynomial lower bound for a circuit computing the clique function with at most $(1/6)\log\log n$ negation gates. *SIAM Journal on Computing*, 35(1):201–215, 2005.

[7] Béla Bollobás. *Random Graphs (2nd Edition).* Cambridge University Press, 2001.

[8] Coenraad Bron and Joep Kerbosch. Finding all cliques of an undirected graph (algorithm 457). *Commun. ACM*, 16(9):575–576, 1973.

[9] Paul Erdős and Richard Rado. Intersection theorems for systems of sets. *J. London Math. Soc.*, 35:85–90, 1960.

[10] Mikael Goldmann and Johan Håstad. A simple lower bound for the depth of monotone circuits computing clique using a communication game. *Information Processing Letters*, 41(4):221–226, 1992.

[11] Svante Janson. Poisson approximation for large deviations. *Random Structures and Algorithms*, 1(2):221–230, 1990.

[12] Svante Janson, Tomasz Łuczak, and Andrzej Ruciński. *Random Graphs.* John Wiley, 2000.

[13] Ari Juels and Marcus Peinado. Hiding cliques for cryptographic security. *Des. Codes Cryptography*, 20(3):269–280, 2000.

[14] Stasys Jukna. *Extremal Combinatorics with Applications in Computer Science.* Springer, Heidelberg, 2001.

[15] Richard M. Karp. Probabilistic analysis of some combinatorial search problems. In J. F.

Traub, editor, *Algorithms and Complexity: New Directions and Recent Results*, pages 1–19. Academic Press, 1976.

[16] Alexander A. Razborov. Lower bounds on the monotone complexity of some boolean functions. *Doklady Akademii Nauk SSSR*, 281:798–801, 1985. English translation in Soviet Math. Doklady 31 (1985), 354–357.

[17] Alexander A. Razborov. On the method of approximations. In *Proceedings of the 21st Annual ACM Symposium on the Theory of Computing*, pages 167–176, 1989.

[18] Benjamin Rossman. On the constant-depth complexity of k-clique. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC)*, pages 721–730, 2008.

[19] Benjamin Rossman. *Average-Case Complexity of Detecting Cliques*. PhD thesis, M.I.T., 2010.

[20] Benjamin Rossman. The monotone complexity of k-clique on random graphs. In *FOCS '10: Proceedings of 51st Annual IEEE Symposium on Foundations of Computer Science*, pages 193–201, 2010.