Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 129 (2026)

Monotone circuit lower bounds from spread matchings

Anup Rao*
anuprao@cs.washington.edu

July 31, 2026

Abstract

We show that $\exp(\widetilde{\Omega}(n^{1/2}))$ gates are required to detect bipartite perfect matchings in n-vertex graphs. Our lower bounds are based on a new spread matching lemma.

1. Introduction

A monotone Boolean circuit is a circuit that only uses the monotone gates $\wedge, \vee$; negations are not allowed. One of the beautiful success stories of complexity theory has been the achievement of exponential monotone circuit lower bounds. In this paper, we prove new monotone circuit lower bounds for detecting matchings, and simplify the proofs of some other monotone circuit lower bounds for natural functions.

In a foundational paper, Razborov [20] proved that computing matching and detecting cliques both require monotone circuits of size $n^{\Omega(\log n)}$. Alon and Boppana [1] later improved the lower bound for clique to $\exp(\widetilde{\Omega}(n^{1/3}))$. These early results leveraged the combinatorial concept of *sunflowers*, namely a collection of sets whose pairwise intersections are identical. Erdős and Rado [10] showed that every large collection of small sets must contain a large sunflower, and Razborov used this sunflower lemma to approximate the gates of a given monotone circuit with simpler functions, yielding circuit lower bounds. Since then, similar monotone circuit lower bounds were also proved by appealing to the switching lemma or other methods which avoided the use of sunflowers altogether [13, 5, 14]. Another direction leveraged the connection to communication complexity to prove optimal lower bounds of $\Omega(n)$ on the depth of the monotone circuits computing clique or matching [19, 18].

1.1. Robust sunflowers and spreadness

A significant advance in the study of these monotone circuit lower bounds was made by Rossman [21] when he introduced the notion of *robust sunflowers*. Loosely speaking, a robust sunflower is a DNF, namely a formula in disjunctive normal form, with the property that the DNF can be approximated by a single term. Rossman's work revealed that robust sunflowers could be used to prove new monotone circuit lower bounds. For example, he gave

ISSN 1433-8092

exponential monotone circuit lower bounds for the task of distinguishing graphs with cliques of size k from Erdős–Rényi random graphs that do not have such cliques.

In a breakthrough, Alweiss, Lovett, Wu and Zhang [2] established an essentially optimal robust sunflower lemma. The proof crucially used the concept of a *spread* set, first considered by Talagrand [22]. We say that a random set Z is r-spread if for all sets S,

$$p(S \subseteq Z) \leq r^{-|S|}.$$

Let $\mathcal{Z}$ denote the support of Z. The key contribution of [2] is a nice encoding argument to show that a random set must contain some element of a spread family $\mathcal{Z}$ with high probability. Subsequent work by the author [16], Frankston, Kahn, Narayanan and Park [11], and Bell, Chueluecha and Warnke [4] cleaned up the bounds to obtain the following version (see [17] for the easiest proof):

Lemma 1 (Spread Set Lemma)**.** *There is a universal constant $\alpha > 0$ such that the following holds. Let $\varepsilon \leq 1/2$, $r = \alpha \log(t/\varepsilon)/\gamma$ and Z be a random r-spread set of size at most t. Then if X_0 is a random set including each element independently with probability γ,*

$$p(\exists z \in \mathcal{Z}, z \subseteq X_0) > 1 - \varepsilon.$$

If a monotone DNF has terms that correspond to $\mathcal{Z}$, then the conclusion of Lemma 1 is that the DNF can be approximated by the function 1 from the perspective of a random input X_0. Lemma 1 is tight [2]. Let $[n] = \{1, 2, \dots, n\}$, let $f : [t] \to [\lceil \log(t/\varepsilon)/\gamma \rceil]$ be a uniformly random function, and let $Z = \{(i, f(i))\}$ be its graph. Then Z is r-spread with $r = \lceil \log(t/\varepsilon)/\gamma \rceil$, but if X_0 includes each element with probability γ, the probability that X_0 is disjoint from $[i] \times [\lceil \log(t/\varepsilon)/\gamma \rceil]$ is

$$(1-\gamma)^{\lceil \log(t/\varepsilon)/\gamma \rceil} \approx e^{-\gamma \lceil \log(t/\varepsilon)/\gamma \rceil} \approx \varepsilon/t,$$

so X_0 does not contain the graph of any f with probability $\approx \varepsilon$.

These results led to several new monotone circuit lower bounds, as well as new connections to so-called *lifting* results by Garg, Göös, Kamath and Sokolov [12], Lovett, Meka, Mertz, Pitassi and Zhang [15] and by de Rezende and Vinyals [9]. For example, Cavalar, Kumar and Rossman [8] used Lemma 1 to prove a lower bound of $\exp(\widetilde{\Omega}(\sqrt{n}))$ for an explicit function of n variables, beating the prior record of $\exp(\widetilde{\Omega}(n^{1/3}))$ due to Andreev [3] and Harnik and Raz [14]. They also gave a lower bound of $\exp(\widetilde{\Omega}(k))$ for detecting cliques up to size $k \leq n^{1/3}$, by proving a *robust clique sunflower lemma*. Blasiok and Meierhöfer [6] and de Rezende and Vinyals [9] proved lower bounds of the type $\exp(\widetilde{\Omega}(\sqrt{n}))$ for monotone circuits computing whether or not a graph on n vertices contains a clique of size $\approx \sqrt{n}$. The stronger bounds of [6] followed from a better robust clique sunflower lemma. Implicit in their work is the following *spread clique lemma* (see Section 4 for the proof). For a set S, let $\mathcal{C}_S$ denote the clique on the vertices of S.

Lemma 2 (Spread Clique Lemma)**.** *There is a universal constant $\alpha > 0$ such that the following holds. Let $\varepsilon \leq 1/2$, $r = \alpha \log(t/\varepsilon)/p^{t+s}$ and $Z \subseteq [n]$ be a random r-spread set of*

size at most t. Then if X_0 is a graph on the vertex set $[n]$ sampled by including each edge independently with probability p and $S \subseteq [n]$ is an arbitrary set of size s,

$$p(\exists z \in \mathcal{Z}, \mathcal{C}_{z \cup S} \subseteq X_0 \cup \mathcal{C}_S) > 1 - \varepsilon.$$

Razborov's $n^{\Omega(\log n)}$ bound remained the best monotone circuit lower bound for matching until Cavalar, Göös, Riazanov, Sofronova, and Sokolov [7] used Lemma 1 as well as the concept of *blocky matchings* to prove a robust matching sunflower lemma and used it to show that any monotone circuit distinguishing graphs with a perfect matching from graphs with maximum matching size $n/2 - 2$ must have size $\exp(\widetilde{\Omega}(n^{1/3}))$.

1.2. Our results

In this paper, we give new monotone circuit lower bounds for detecting matchings.

Theorem 3. *For $q < k \leq n/2$, any monotone circuit that can distinguish n-vertex bipartite graphs with matchings of size k from graphs that do not have matchings of size q must have $\exp(\Omega(q/(\sqrt{k}\log n)))$ gates.*

Setting $k = n/2$, $q = n/4$ yields:

Corollary 4. *Any monotone circuit that can distinguish n-vertex bipartite graphs with a perfect matching from graphs that do not have matchings of size $n/4$ must have $\exp(\Omega(\sqrt{n}/\log n))$ gates.*

Corollary 4 improves on the results of [7] in two ways: the exponent is larger, and the lower bound applies for distinguishing perfect matchings from graphs with no small matchings, rather than distinguishing perfect matchings from graphs with matchings of size 1 less than perfect. Theorem 3 gives exponential lower bounds even for circuits that distinguish graphs with matchings of size $n^{1/5}$ from graphs that do not have matchings of size $n^{1/9}$.

Following the usual pattern, these new results are a consequence of a new *spread matching lemma* with essentially optimal parameters. We say that a random matching Z is r-spread if for every matching m,

$$p(m \subseteq Z) \leq r^{-|m|}.$$

Let $G(W_0)$ denote the graph that contains exactly those edges that are incident to W.

Lemma 5 (Spread Matching Lemma)**.** *There is a universal constant $\alpha > 0$ such that the following holds. Let $\varepsilon < 1/2$, $t > 1$, $r = \alpha \cdot (\log t)^2 \cdot (t + \log^2(1/\varepsilon))/\gamma^2$, and Z be a random r-spread matching on the set of vertices $[n]$, with $|Z| \leq t$. Then if $W \subseteq [n]$ is a uniformly random set with $|W| = \gamma n$,*

$$p(\exists z \in \mathcal{Z}, z \subseteq G(W)) > 1 - \varepsilon.$$

Remark 6. Lemma 5 also holds when W includes each element independently with probability γ. To prove this, add dummy elements to the universe until the probability that W contains $< \gamma n/2$ elements is much less than ε, and then apply Lemma 5.

A consequence of Lemma 5 is the following robust spread matching lemma.

Corollary 7 (Robust Spread Matching Lemma)**.** *There is a universal constant $\alpha > 0$ such that the following holds. Let $\varepsilon < 1/2$, $t > 1$, $r = \alpha \cdot (\log t)^2 \cdot (t + \log^2(1/\varepsilon))/\gamma^2$, and let $\mathcal{Z}$ be a family of r^t matchings of size at most t. Then there is a matching m such that if $W \subseteq [n]$ is a uniformly random set with $|W| = \gamma n$,*

$$p(\exists m' \in \mathcal{Z}, m \subseteq m', m' \subseteq G(W) \cup m) > 1 - \varepsilon.$$

Corollary 7 looks closer to a statement proved in [7]. To prove it, let $Z \in \mathcal{Z}$ be uniform, and pick the largest matching m violating r-spreadness. Then $Z \setminus m \mid m \subseteq Z$ is guaranteed to be r-spread by the choice of m, so we can apply Lemma 5 to derive the conclusion. The main improvement of Lemma 5 and Corollary 7 over the corresponding statement of [7] is the dependence of r on t and ε. Our dependence is of the type $t + \log^2(1/\varepsilon)$, while theirs is $t \log^2(1/\varepsilon)$. Our results apply using the graph $G(W)$, which contains a matching of size at most γn, while their result required the use of graphs that contain matchings of size $n/2 - 2$.

The proof of Lemma 5 is not as easy as the proof of Lemma 1. It uses a new encoding argument tailored for matchings that builds on the one used for sets, and the argument is, unfortunately, quite subtle. We prove the lemma in Section 2, where we also give several examples that verify the (near) optimality of its parameters. One of the examples given there shows that $r \geq \Omega(\log^2(1/\varepsilon))$ is necessary to obtain error ε.

In an effort to unify all known monotone circuit lower bounds into a single nice framework, one that we prefer over the other known ways of reasoning about these things, we reprove the results of [8, 6, 9]. For detecting cliques, we use Lemma 2 to prove the following in Section 4:

Theorem 8. *There is a universal constant $\beta > 0$ such that if $q < k$, $\beta k \log q \leq n$, any monotone circuit distinguishing n-vertex graphs that contain a clique of size k from graphs that have no clique of size q must have size $\left(\frac{\beta n}{qk}\right)^{q/\log n}$.*

Setting $k = \beta\sqrt{n}/2, q = k/2$ proves a lower bound of $\exp(\Omega(\sqrt{n}/\log n))$. We reproduce the bound proved by [8] in Section 5. Without loss of generality, assume n is a prime. Let D_d denote the set of univariate polynomials of degree d over $\mathbb{F}_n$. Define

$$F_{k,d}(x) = \bigvee_{\substack{w \in D_d \\ |w([k])| \geq k/2}} \bigwedge_{i \in w([k])} x_i.$$

We prove

Theorem 9. *There is a universal constant $\beta > 0$ such that if $\beta k \log d \leq n$ and $3d \log n \leq k$, then $F_{k,d}$ requires monotone circuits of size $\exp(\Omega(\min\{d, n/k\}))$.*

Setting $k = \sqrt{n}, d = k/\log n$ yields $F_{k,d} \in \mathsf{NP}$, but $F_{k,d}$ requires monotone circuits of size $\exp(\Omega(\sqrt{n}/\log n))$.

1.3. Acknowledgements

Thanks to Albert Atserias, Paul Beame, Shreya Gupta, Toby Escarez, Felix Moreno Penarrubia, Dante Tjowasi and Michael Whitmeyer for useful conversations.

2. Spread matching lemma

In this section, we prove Lemma 5. Here are some examples that show why Lemma 5 must have the form that it does:

1. Let A and B be disjoint sets, each of size $\log(1/\varepsilon)/2$, and Z be a single random edge from A to B. Let $\gamma = 1/2$. Then Z is r-spread with $r = \log(1/\varepsilon)^2/4$, yet with probability $\approx \varepsilon$, $G(W)$ does not include any edge in the support of Z. This shows that $r \geq \Omega(\log^2(1/\varepsilon))$ is required.

2. Let A and B be disjoint sets of size t, and Z be a uniformly random perfect matching from A to B. Then Z is r-spread with $r = t/2$. If $\gamma = 1/3$, with probability $> 1/2$, W contains less than t of the vertices of $A \cup B$, so the probability that $G(W)$ contains one of the matchings is at most $1/2$. This shows that $(t/2)$-spreadness is necessary, even to achieve error $1/2$.

3. Let A and B be disjoint sets of size $n/2$, and let Z be a uniformly random matching of size t from A to B. Then Z is $\Theta(n^2/t)$-spread. However, if $\gamma n = t/2$, we see that $G(W)$ cannot contain any matching of size t, even though Z is $\Theta(t/\gamma^2)$-spread. This shows that $r \ll t/\gamma^2$ is insufficient.

4. Let Z be a uniformly random edge from the star graph, namely the set of edges $\{\{1, j\} : j > 1\}$. We see that Z is $(n-1)$-spread, yet W contains an edge of $\mathcal{Z}$ only if it contains 1, and this happens with probability at most γ. This example shows why edges not contained in W need to be included in $G(W)$.

2.1. Proof of Lemma 5

Let q be the smallest number such that $2^q \geq t$, and sample a family of uniformly random mutually disjoint sets $\{W_{i,j}\}$, with

$$i \in [q], \qquad j \in [\lceil 2^{i-q} \log(q/\varepsilon) \rceil], \qquad |W_{i,j}| = \left\lfloor \frac{\gamma n}{q \cdot \lceil 2^{i-q} \log(q/\varepsilon) \rceil} \right\rfloor.$$

Let $W = \cup_{i,j} W_{i,j}$. We have $|W| \leq \gamma n$. Sample $W_{i,j}$ in the order

$$W_{1,1}, W_{1,2}, \ldots, W_{1,\lceil 2^{1-q} \log(q/\varepsilon) \rceil}, W_{2,1}, W_{2,2}, \ldots, W_{q,\lceil \log(q/\varepsilon) \rceil}.$$

Let $k(i,j)$ be the location of the set $W_{i,j}$ in the above ordering: $k(1,1) = 1, k(1,2) = 2$ and so on. We write $W_k = W_{i,j}$ and $W^k = \bigcup_{l=1}^{k} W_l$. Let $W^0 = W_0 = \emptyset$. During this random

process, we need to keep track of the matchings of $\mathcal{Z}$ that have been partially covered by $G(W^k)$. To this end, define the map π_k as follows. Set $\pi_0(z) = z$, and

$$\pi_k(z) = \pi_{k-1}(\mu_k(z)) \setminus G(W^k),$$

where $\mu_k(z) \in \mathcal{Z}$ is the lexicographically first matching that minimizes $|\pi_{k-1}(\mu_k(z)) \setminus G(W^k)|$ subject to the constraints

$$\pi_{k-1}(\mu_k(z)) \subseteq G(W^k) \cup \pi_{k-1}(z),$$

and

$$|\pi_{k-1}(\mu_k(z))| \leq 2^{q-i+1}.$$

This choice ensures that $\pi_k(z) \subseteq \pi_{k-1}(z)$, and in particular $\pi_k(z) \subseteq z$. The map π_k is determined by $W_1, \ldots, W_k$. Given W^k, $\pi_k(z)$ is a matching that is easier to cover than $\pi_{k-1}(z)$, and if $\pi_k(z)$ is eventually covered by $G(W^k)$, then some matching of $\mathcal{Z}$ must also be covered. If $\pi_k(z)$ is empty, then $\mathcal{Z}$ must contain a matching that has been covered by $G(W^k)$.

For $k = k(i,j)$, let $a \geq 2^{q-i}$, and fix $W_1, \ldots, W_{k-1}$. Let E_k denote the event:

$$E_k : \qquad |\pi_{k-1}(Z)| \leq 2^{q-i+1} \text{ and } |\pi_k(Z)| \geq 2^{q-i}.$$

The key technical bound of the proof is that over the random choice of the pair (W_k, Z) we have

$$p(E_k) \leq \kappa^{-2^{q-i}}, \tag{1}$$

where $\kappa = \alpha/2^{17}$, for α as in the statement of Lemma 5.

Let us see how to use Equation (1) to finish the proof. Applying Markov's inequality to Equation (1), we conclude that

$$p_{W_k}(p_Z(E_k) > \kappa^{-2^{q-i-1}}) < \kappa^{-2^{q-i-1}},$$

and recall that this bound holds for all fixed values of $W_1, \ldots, W_{k-1}$. So, for any fixed i and fixed $W_1, \ldots, W_{k(i,1)-1}$,

$$p_W(\forall j, p_Z(E_{k(i,j)}) > \kappa^{-2^{q-i-1}}) < (\kappa^{-2^{q-i-1}})^{\lceil 2^{q-i}\log(q/\varepsilon)\rceil} \leq \kappa^{-\log(q/\varepsilon)/2} < \varepsilon/q,$$

for α chosen large enough. By the union bound, we conclude that with probability at least $1-\varepsilon$, W satisfies the condition that for each i there is some $j = j'(i)$ such that over the choice of Z

$$p_Z(E_{k(i,j')}) \leq \kappa^{-2^{q-i-1}}.$$

We claim that this implies that there must be $z \in \mathcal{Z}$ with $z \subseteq G(W_0)$. That is because we can bound

$$\begin{aligned} p_Z(|\pi_{k(q,\lceil\log(q/\varepsilon)\rceil)}(Z)| > 0) &\leq \sum_{i=1}^{q} p_Z\Big(\bigwedge_{j=1}^{\lceil 2^{i-q}\log(q/\varepsilon)\rceil} E_{k(i,j)}\Big) \\ &\leq \sum_{i=1}^{q} p_Z\Big(E_{k(i,j'(i))}\Big) \leq \sum_{i=1}^{q} \kappa^{-2^{q-i-1}} \leq \sum_{i=1}^{\infty} \kappa^{-i/2} < 1, \end{aligned}$$

for α chosen large enough.

It only remains to prove Equation (1). Recall again that the choice of $W_1, \ldots, W_{k-1}$ is fixed. Let $E_{k,a}$ denote the following event, which is determined by (W_k, Z):

$$E_{k,a}: \qquad |\pi_{k-1}(Z)| \leq 2^{q-i+1} \text{ and } |\pi_k(Z)| = a.$$

So, $E_k = \bigvee_{a=2^{q-i}}^{2^{q-i+1}} E_{k,a}$. Given a matching z of size a, let $V(z)$ denote the set of $2a$ vertices that are incident to z. For $z \in \mathcal{Z}$, say that a pair (W^k, z), with $|\pi_{k-1}(z)| \leq 2^{q-i+1}, |\pi_k(z)| = a$ is *consistent* with a subset $S \subseteq [n]$ and a function $f : [n] \to [a]$ if the following conditions hold:

1. For all edges $\{u, v\} \in \pi_{k-1}(\mu_k(z))$, either
   (a) $\{u, v\} \subseteq S$, $\{u, v\} \in \pi_k(z)$ and $f(u) = f(v)$, or
   (b) $\{u, v\} \cap S = \emptyset$ and $\{u, v\} \notin \pi_k(z)$.
2. If u, v belong to distinct edges of $\pi_k(z)$, then $f(u) \neq f(v)$.

Given any fixed pair $(W_k, z) \in E_{k,a}$, if S and f are chosen uniformly at random, then the probability that the pair is consistent with S, f is at least

$$2^{-2^{q-i+2}} \cdot (1/a^2)^a \cdot a! \geq 2^{-2^{q-i+2}} \cdot (ea)^{-a}.$$

Therefore, if $D_{S,f}$ denotes the event that the pair is consistent with S, f, there is some choice of S, f such that

$$p(E_{k,a} \wedge D_{S,f}) \geq p(E_{k,a}) \cdot 2^{-2^{q-i+2}} \cdot (ea)^{-a}. \tag{2}$$

Fix such a choice of S, f.

With Equation (2) in mind, our goal is to bound $p(E_{k,a} \wedge D_{S,f})$. To do this, we count the number of possible pairs $(W_k, \pi_k(z))$ that can be produced within the event $E_{k,a} \wedge D_{S,f}$. For a matching m, let $V(m)$ denote the vertices incident to m. Given W_k and $\pi_k(z)$, the number of choices for $W_k \cup V(\pi_k(z))$ is

$$\begin{aligned}\binom{n - |W^{k-1}|}{|W_k| + 2a} &\leq \binom{n - |W^{k-1}|}{|W_k|} \cdot \left(\frac{n - |W^{k-1}|}{|W_k|}\right)^{2a} \\ &\leq \binom{n - |W^{k-1}|}{|W_k|} \cdot \left(\frac{2q \cdot \lceil 2^{i-q} \cdot \log(q/\varepsilon) \rceil}{\gamma}\right)^{2a}. \end{aligned} \tag{3}$$

For each choice of $W_k \cup V(\pi_k(z))$, let $z' \in \mathcal{Z}$ be the lexicographically first matching satisfying the following conditions:

1. $|\pi_{k-1}(z')| \leq 2^{q-i+1}$, $\pi_{k-1}(z') \subseteq G(W^k \cup V(\pi_k(z)))$,
2. For all $\{u, v\} \in \pi_{k-1}(z')$, either

(a) $\{u, v\} \subseteq S$, $f(u) = f(v)$ and $\{u, v\} \subseteq W_k \cup V(\pi_k(z))$, or
(b) $\{u, v\} \cap S = \emptyset$.

The conditions given above are satisfied by $\mu_k(z)$, so the choice of z' is well-defined.

Claim 10. $\pi_k(z) \subseteq \pi_{k-1}(z')$.

To prove Claim 10, observe that if $\{u, v\} \in \pi_{k-1}(z')$ and $u, v \in V(\pi_k(z))$, then $u, v \in S$, so the choice of z' implies that $f(u) = f(v)$ and $\{u, v\} \in \pi_k(z)$, because this must be true in $D_{S,f}$. There is no edge $\{u, v\} \in \pi_{k-1}(z')$ such that $u \in V(\pi_k(z)), v \notin W^k \cup V(\pi_k(z))$, because such an edge must have $u \in S$, which forces $v \in S$, and hence by 2(a) we get $v \in W_k \cup V(\pi_k(z))$. We conclude that any edge of $\pi_{k-1}(z')$ that is not in $\pi_k(z)$ must be incident to W_k. So, if there is an edge $\{u, v\} \in \pi_k(z)$ that is missing in $\pi_{k-1}(z')$, we must have $\pi_{k-1}(z') \subseteq G(W^k) \cup \pi_k(z)$ and $|\pi_{k-1}(z') \setminus G(W^k)| < |\pi_k(z)|$, but $\mu_k(z)$ is the minimizer, so this cannot happen.

By Claim 10, given $W_k \cup V(\pi_k(z))$ and the event $E_{k,a} \wedge D_{S,f}$, the number of possible choices for $\pi_k(z)$ is bounded by the number of subsets of $\pi_{k-1}(z')$, which is at most $2^{2^{q-i+1}}$. Given $\pi_k(z)$ and $W_k \cup V(\pi_k(z))$, W_k is also determined. Putting these calculations together, and using the spreadness condition of Z applied to the matching $\pi_k(z)$, we conclude that for $2^{q-i+1} \geq a \geq 2^{q-i}$,

$$\begin{aligned}
&p(E_{k,a} \wedge D_{S,f}) \\
&= \sum_{(W_k, \pi_k(z)) \in E_{k,a} \wedge D_{S,f}} p(W_k, \pi_k(z)) \\
&= \sum_{(W_k, \pi_k(z)) \in E_{k,a} \wedge D_{S,f}} \binom{n - |W^{k-1}|}{|W_k|}^{-1} \cdot r^{-a} \\
&\leq \binom{n - |W^{k-1}|}{|W_k|} \cdot \Big(\frac{2q \cdot \lceil 2^{i-q} \cdot \log(q/\varepsilon) \rceil}{\gamma}\Big)^{2a} \cdot 2^{4 \cdot 2^{q-i}} \cdot \binom{n - |W^{k-1}|}{|W_k|}^{-1} \cdot r^{-a} \\
&\leq \Big(\frac{2^6 q^2 \cdot \lceil 2^{i-q} \cdot \log(q/\varepsilon) \rceil^2}{r \cdot \gamma^2}\Big)^a.
\end{aligned}$$

Using Equation (2) yields the bound

$$p(E_{k,a}) \leq \Big(\frac{e 2^8 q^2 \cdot a \cdot \lceil 2^{i-q} \cdot \log(q/\varepsilon) \rceil^2}{r \cdot \gamma^2}\Big)^a.$$

Observe that when $2^{i-q} \cdot \log(q/\varepsilon) < 1$, we have

$$a \cdot \lceil 2^{i-q} \cdot \log(q/\varepsilon) \rceil^2 < a,$$

and when $2^{i-q} \cdot \log(q/\varepsilon) \geq 1$, because $a \leq 2^{q-i+1}$, we have

$$\begin{aligned}
a \cdot \lceil 2^{i-q} \cdot \log(q/\varepsilon) \rceil^2 \leq 4a \cdot (2^{i-q} \cdot \log(q/\varepsilon))^2 \leq 8 \log^2(q/\varepsilon) &= 8(\log(q) + \log(1/\varepsilon))^2 \\
&\leq 16(\log^2(q) + \log^2(1/\varepsilon)).
\end{aligned}$$

Recall that $r = \alpha \cdot ((\log t)^2 \cdot (t + \log^2(1/\varepsilon))/\gamma^2$ and $q = \lceil \log t \rceil$, so in all cases we obtain the bound $p(E_{k,a}) \le (\alpha/2^{16})^{-a}$. Finally, we bound

$$p(E_k) \le \sum_{a=2^{q-i}}^{2^{q-i+1}} p(E_{k,a}) \le (\alpha/2^{17})^{-2^{q-i}},$$

as required.

3. Exponential lower bounds for matching

Here we prove Theorem 3. Let X_1 be a uniformly random matching of size k from $[n/2]$ to $[n] \setminus [n/2]$, and let $\mathcal{X}_1$ denote its support. Let $X_0 = G(W_0)$ (recall that this is the set of edges incident to W_0), where W_0 is a uniformly random subset of $[n]$ of size q. Note that X_0 has maximum matching size q. Let $\mathcal{X}_0$ denote the support of X_0.

If $|m| > k$, then $p(m \subseteq X_1) = 0$, and if $|m| \le k$, then by the arithmetic-mean geometric-mean inequality,

$$\begin{aligned} p(m \subseteq X_1) &= \left(\frac{\binom{n/2}{k}}{\binom{n/2-|m|}{k-|m|}}\right)^{-2} \frac{1}{(k)(k-1)\cdots(k-|m|+1)} \\ &\le \left(\frac{n}{2k}\right)^{-2|m|} \cdot (k - |m|/2 + 1/2)^{-|m|} \\ &\le \left(\frac{n^2}{8k}\right)^{-|m|}, \end{aligned}$$

so X_1 is $(n^2/(8k))$-spread. For $\eta = 1/(1600\alpha)$, we set

$$\begin{aligned} &t = \min\{q/8, \eta q^2/(k \log^2 n)\}, \qquad \varepsilon = \exp(-\eta q/(\sqrt{k} \log n)), \\ &r = \alpha \cdot (\log^2(2t)) \cdot (2t + \log^2(1/\varepsilon)) \cdot (2n/q)^2 \\ &\quad \le 100\alpha\eta \cdot n^2/k \\ &\quad \le n^2/(16k). \end{aligned}$$

3.1. Approximation method

Given any set of matchings M, define

$$f_M(x) = \begin{cases} 1 & \text{if } \exists m \in M, m \subseteq x \\ 0 & \text{otherwise.} \end{cases}$$

For each gate g of a given monotone circuit, we compute a set of matchings M_g, such that every $m \in M_g$ is of size at most t. Our approximator for g is f_{M_g}. We define the sets of errors:

$$E_g^1 = \{x \in \mathcal{X}_1 : g(x) = 1, f_{M_g}(x) = 0\},$$

$$E_g^0 = \{x \in \mathcal{X}_0 : g(x) = 0, f_{M_g}(x) = 1\}.$$

We prove that if the circuit has at most $\min\{2^t, 1/\varepsilon\}/2 = \min\{q/8, \eta q/(\sqrt{k}\log n)\}/2$ gates and g is the output gate, then one can compute M_g with

$$p(X_1 \in E_g^1) \leq 1/2, \text{ and } p(X_0 \in E_g^0) \leq 1/2. \tag{4}$$

Given Lemma 5, this is enough to complete the proof of the theorem. Indeed, if the circuit is correct, then when $X_1 \notin E_g^1$, there must be some matching $Z(X_1) \in M_g$ such that $Z(X_1) \subseteq X_1$, $|Z(X_1)| \leq t$. For any matching m, we have

$$p(m \subseteq Z(X_1) | X_1 \notin E_g^1) \leq \frac{p(m \subseteq Z(X_1) \subseteq X_1, X_1 \notin E_g^1)}{p(X_1 \notin E_g^1)} \leq 2 \cdot (2r)^{-|m|} \leq r^{-|m|},$$

so $Z(X_1)$ is r-spread. Lemma 5 then implies that

$$p(g(X_0) = 1) \geq p(\exists z \in \mathcal{Z}, z \subseteq X_0) - p(X_0 \in E_g^0) \geq 1/2 - \varepsilon,$$

proving that the circuit is not correct. A correct circuit must have more than $1/(2\varepsilon)$ gates.

To prove Equation (4), we need to describe how to construct M_g for each gate g. The input gates already correspond to f_{M_g} with M_g containing a single edge, so they are their own approximators. If g is computed from gates h_1, h_2, we show how to obtain M_g from M_{h_1}, M_{h_2}. If $g = h_1 \vee h_2$, we set $M_g = M_{h_1} \cup M_{h_2}$. This choice guarantees that $E_g^1 \subseteq E_{h_1}^1 \cup E_{h_2}^1$ and $E_g^0 \subseteq E_{h_1}^0 \cup E_{h_2}^0$, so no new errors are introduced.

The more interesting case is when $g = h_1 \wedge h_2$. Then the natural choice is to set

$$M_g' = \{m \cup m' : m \in M_{h_1}, m' \in M_{h_2}, m \cup m' \text{ is a matching}\}.$$

The problem is that M_g' may contain a matching of size $> t$. Given M_g, let

$$N_g^1 = E_g^1 \setminus (E_{h_1}^1 \cup E_{h_2}^1) \text{ and } N_g^0 = E_g^0 \setminus (E_{h_1}^0 \cup E_{h_2}^0)$$

denote the sets of new errors. If $X_1 \in N_g^1$, then there must be a matching $Z(X_1) \in M_g'$ with $Z(X_1) \subseteq X_1$ and $|Z(X_1)| \leq 2t$. We construct the final M_g using the following simple algorithm:

Algorithm 1 Computing M_g

$M_g \leftarrow \emptyset$

while $p(X_1 \in N_g^1) > 0$ **do**

  Find a largest matching m such that $p(m \subseteq Z(X_1) \mid X_1 \in N_g^1) \geq r^{-|m|}$.

  if $|m| \leq t$ **then**

    $M_g \leftarrow M_g \cup \{m\}$

  else

    halt ; `// Terminate if largest valid matching exceeds threshold t`

return M_g

At the end of this algorithm, M_g only contains matchings of size at most t, if any. Let us bound the measure of the new errors N_g^1.

Lemma 11. $p_{X_1}(X_1 \in N_g^1) \leq 2^{-t}$.

Proof. The non-trivial case is when the algorithm discovers a matching m with $|m| > t$. In this case we bound

$$p(X_1 \in N_g^1) = \frac{p(m \subseteq Z, X_1 \in N_g^1)}{p(m \subseteq Z | X_1 \in N_g^1)} \leq \frac{p(m \subseteq X_1)}{r^{-|m|}} \leq 2^{-|m|} \leq 2^{-t}.$$

□

Lemma 12. $p(X_0 \in N_g^0) \leq \varepsilon$.

Proof. If $f_{M_g}(X_0) = 1$, let $m(X_0) \in M_g$ be the lexicographically first element with $m(X_0) \subseteq X_0$. Let $V(m(X_0))$ denote the set of vertices incident to $m(X_0)$. If $p(f_{M_g}(X_0) = 1) = 0$, then $p(X_0 \in N_g^0) = 0$. Otherwise, we have

$$\begin{aligned} p(X_0 \in N_g^0) &\leq p(X_0 \in N_g^0 \mid f_{M_g}(X_0) = 1) \\ &= \sum_{m^*, S \subseteq [n]} p(X_0 \in N_g^0 \mid m(X_0) = m^*, V(m^*) \cap W_0 = S, f_{M_g}(X_0) = 1) \\ &\qquad \cdot p(m(X_0) = m^*, V(m^*) \cap W_0 = S \mid f_{M_g}(X_0) = 1). \end{aligned} \tag{5}$$

When m^* was added to M_g, it was chosen as a largest matching satisfying $p(m^* \subseteq Z \mid X_1 \in N_g^1) \geq r^{-|m^*|}$. Thus, for any matching m' with $V(m') \cap V(m^*) = \emptyset$, we have

$$p(m' \subseteq Z \mid m^* \subseteq Z, X_1 \in N_g^1) = \frac{p(m' \cup m^* \subseteq Z \mid X_1 \in N_g^1)}{p(m^* \subseteq Z \mid X_1 \in N_g^1)} \leq \frac{r^{-(|m^*|+|m'|)}}{r^{-|m^*|}} = r^{-|m'|}.$$

Therefore, $Z \setminus m^*$ conditioned on the event $(m^* \subseteq Z, X_1 \in N_g^1)$ is an r-spread matching of size at most $2t$. Conditioned on $m(X_0) = m^*$ and $V(m^*) \cap W_0 = S$, the random variable X_0 contains $G(W_0')$, where W_0' is a uniformly random subset of the complement of $V(m^*)$ of size

$$|W_0'| \geq q - |S| \geq q - 4t \geq q/2,$$

since $t \leq q/8$. Applying Lemma 5, we conclude that

$$\begin{aligned} &p(X_0 \in N_g^0 \mid m(X_0) = m^*, V(m^*) \cap W_0 = S, f_{M_g}(X_0) = 1) \\ &\leq 1 - p(\exists z \in \mathcal{Z}, z \subseteq X_0 \mid m(X_0) = m^*, V(m^*) \cap W_0 = S, f_{M_g}(X_0) = 1) \\ &< \varepsilon. \end{aligned}$$

Substituting this bound back into (8) yields

$$\begin{aligned} p(X_0 \in N_g^0) &\leq \sum_{m^*, S \subseteq [n]} \varepsilon \cdot p(m(X_0) = m^*, V(m^*) \cap W_0 = S \mid f_{M_g}(X_0) = 1) \\ &= \varepsilon, \end{aligned}$$

as required. □

Using the union bound with Lemmas 11 and 12, we find that if the circuit has size at most $\min\{2^t, 1/\varepsilon\}/2$, then

$$p\Big(X_1 \in \bigcup_g E_g^1\Big) \le 2^t \cdot 2^{-t}/2 \le 1/2, \qquad p\Big(X_0 \in \bigcup_g E_g^0\Big) \le (1/(2\varepsilon)) \cdot \varepsilon \le 1/2,$$

proving Equation (4).

4. Exponential lower bounds for clique

We start by reproducing the ideas of [6] to prove Lemma 2:

Proof of Lemma 2. Without loss of generality, assume that $S = \{n-s+1, \ldots, n\}$. For $i = 1, \ldots, n-s$, let W_i be a random subset of $[i]$, where each element is included independently with probability p^{t+s}, sampled independently of X_0. Let $W_0 = \emptyset$. Recall that $G(W_i)$ denotes the graph that includes all edges incident to W_i. Let $X_0^i = G(W_i) \cup (X_0 \setminus G([i]))$.

We use a coupling argument to prove that

$$p(\exists z \in \mathcal{Z}, \mathcal{C}_{z\cup S} \subseteq X_0^i \cup \mathcal{C}_S) \ge p(\exists z \in \mathcal{Z}, \mathcal{C}_{z\cup S} \subseteq X_0^{i+1} \cup \mathcal{C}_S). \tag{6}$$

X_0^0 has the same distribution as X_0, and by Lemma 1,

$$p(\exists z \in \mathcal{Z}, \mathcal{C}_{z\cup S} \subseteq X_0^{n-s} \cup \mathcal{C}_S) > 1 - \varepsilon$$

So, Equation (6) proves Lemma 2.

To prove Equation (6), sample W_i and $T = X_0 \setminus G([i+1])$ independently. Then sample $Q \subseteq \{i+1\}$ by including $i+1$ with probability p^{t+s}, and sample H as a subset of the edges $\{(i+1, i+2), (i+1, i+3), \ldots, (i+1, n)\}$ where each edge is included independently with probability p. Set $X_0^i = G(W_i) \cup H \cup T$ and set $X_0^{i+1} = G(W_i \cup Q) \cup T$.

For each fixing of W_i, T, if there is $z \in \mathcal{Z}$ with $\mathcal{C}_{z\cup S} \subseteq G(W_i) \cup T \cup \mathcal{C}_S$, then $\mathcal{C}_{z\cup S} \subseteq X_0^i \cup \mathcal{C}_S$ and $\mathcal{C}_{z\cup S} \subseteq X_0^{i+1} \cup \mathcal{C}_S$. Similarly, $p(\mathcal{C}_{z\cup S} \subseteq X_0^i \cup \mathcal{C}_S | W_i, T) = 0$ if and only if $p(\mathcal{C}_{z\cup S} \subseteq X_0^{i+1} \cup \mathcal{C}_S | W_i, T) = 0$. The only interesting case is when both quantities are in $(0, 1)$. In this case, after fixing W_i, T, the probability that H includes the edges required to ensure $\mathcal{C}_{z\cup S} \subseteq G(W_i) \cup H \cup T \cup \mathcal{C}_S$ is at least as large as p^{t+s}, because in the worst case $i+1$ needs to connect to $t+s$ vertices, and those edges are included in X_0^{i+1} with probability at most p^{t+s}. This proves

$$p(\mathcal{C}_{z\cup S} \subseteq X_0^i \cup \mathcal{C}_S | W_i, T) \ge p(\mathcal{C}_{z\cup S} \subseteq X_0^{i+1} \cup \mathcal{C}_S | W_i, T)$$

and completes the proof of Equation (6).

□

Armed with Lemma 2, we can now prove Theorem 8. Let $W_1 \subseteq [n]$ be a uniformly random set of size k, and let $X_1 = \mathcal{C}_{W_1}$. Let X_0 be an Erdős–Rényi random graph where

each edge is included with probability $p = n^{-2/(q-1)}$. We have that W_1 is (n/k)-spread, and the probability that X_0 includes a clique of size q is at most

$$\binom{n}{q} \cdot p^{\binom{q}{2}} = \binom{n}{q} \cdot n^{-q} \leq 1/2,$$

for $q > 5$. Let α be as in Lemma 2, and set

$$t = \lceil 2(q-1)/\log n \rceil, \qquad \varepsilon = (n/(8\alpha t k \log n))^{-t}$$
$$r = \alpha \log((2t+1)/\varepsilon)/p^{2t+1} \leq 8\alpha t \log n.$$

4.1. Approximation method

For a family of sets A, define

$$f_A(x) = \begin{cases} 1 & \text{if } \exists S \in A \text{ and } \exists \mathcal{C}_T \subseteq x \text{ with } S \subseteq T, \\ 0 & \text{otherwise.} \end{cases}$$

Note that we may have $|S| \leq 1$ in the above definition. For each gate g of the circuit, we approximate it with a function f_{A_g}, with $|S| \leq t$ for all $S \in A$. We define the sets of errors:

$$E_g^1 = \{x \in \mathcal{X}_1 : g(x) = 1, f_{A_g}(x) = 0\}$$

$$E_g^0 = \{x \in \mathcal{X}_0 : g(x) = 0, f_{A_g}(x) = 1\}.$$

We prove that if the circuit has at most $\min\{2^t, 1/\varepsilon\}/3$ gates and g is the output gate, then one can compute A_g with

$$p(X_1 \in E_g^1) \leq 1/3, \text{ and } p(X_0 \in E_g^0) \leq 1/3. \tag{7}$$

Given Lemma 2, this is enough to complete the proof of the theorem. Indeed, if the circuit is correct, then when $X_1 \notin E_g^1$, there must be some set $Z(X_1) \in A_g$ such that $Z(X_1) \subseteq W_1$, $|Z(X_1)| \leq t$. For any set S, using the spreadness of W, we get

$$p(S \subseteq Z(X_1) | X_1 \notin E_g^1) \leq \frac{p(S \subseteq Z(X_1) \subseteq W, X_1 \notin E_g^1)}{p(X_1 \notin E_g^1)} \leq 3 \cdot (n/k)^{-|S|} \leq (n/(3k))^{-|S|},$$

So, $Z(X_1)$ is r-spread. Lemma 2 implies that

$$p(g(X_0) = 1) \geq p(\exists z \in \mathcal{Z}, \mathcal{C}_z \subseteq X_0) - p(X_0 \in E_g^0) \geq 1 - 1/3 - \varepsilon > 1/2,$$

proving that the circuit is not correct. A correct circuit must have at least $1/(3\varepsilon)$ gates, and that proves Theorem 8.

To prove Equation (7), we need to describe how to construct A_g for each gate g. The input gates already correspond to f_{A_g} with A_g containing a single set of size 2. If g is computed from gates h_1, h_2, we show how to obtain A_g from A_{h_1}, A_{h_2}. If $g = h_1 \vee h_2$, we set

$A_g = A_{h_1} \cup A_{h_2}$. This choice ensures that $E_g^1 \subseteq E_{h_1}^1 \cup E_{h_2}^1$ and $E_g^0 \subseteq E_{h_1}^0 \cup E_{h_2}^0$, so no new errors are generated. The more interesting case is when $g = h_1 \wedge h_2$. The natural choice is to set

$$A'_g = \{S_1 \cup S_2 : S_1 \in A_{h_1}, S_2 \in A_{h_2}\}.$$

The problem is that A'_g may contain a set of size $> t$. Given A_g, let

$$N_g^1 = E_g^1 \setminus (E_{h_1}^1 \cup E_{h_2}^1) \text{ and } N_g^0 = E_g^0 \setminus (E_{h_1}^0 \cup E_{h_2}^0)$$

denote the sets of new errors. If $X_1 \in N_g^1$, there must be a set $Z(X_1) \in A'_g$ with $Z(X_1) \subseteq W$ and $|Z(X_1)| \leq 2t$. We construct the final A_g using the following algorithm:

Algorithm 2 Computing A_g

$A_g \leftarrow \emptyset$

while $p(X_1 \in N_g^1) > 0$ **do**

  Find a largest set S such that $p(S \subseteq Z(X_1) \mid X_1 \in N_g^1) \geq r^{-|S|}$.

  if $|S| \leq t$ **then**

    $A_g \leftarrow A_g \cup \{S\}$

  else

    halt ; `// Terminate if largest valid set exceeds threshold t`

return A_g

At the end of this algorithm, A_g only contains sets of size at most t, if any.

Lemma 13. $p(X_1 \in N_g^1) \leq \varepsilon$.

Proof. The non-trivial case is when the algorithm discovers a set S with $2t \geq |S| > t$. In this case we bound

$$\begin{aligned} p(X_1 \in N_g^1) = \frac{p(S \subseteq Z, X_1 \in N_g^1)}{p(S \subseteq Z | X_1 \in N_g^1)} \leq \frac{p(S \subseteq W)}{r^{-|S|}} &\leq (n/(8\alpha tk \log n))^{-|S|} \\ &< (n/(8\alpha tk \log n))^{-t}. \end{aligned}$$

□

Lemma 14. $p(X_0 \in N_g^0) \leq \varepsilon$.

Proof. If $f_{A_g}(X_0) = 1$, let $S(X_0) \in A_g$ and $T(X_0) \subseteq [n]$ be the lexicographically first pair of sets minimizing $|T(X_0)|$ and satisfying $S(X_0) \subseteq T$, $\mathcal{C}_{T(X_0)} \subseteq X_0$. If $p(f_{A_g}(X_0) = 1) = 0$, then $p(X_0 \in N_g^0) = 0$. Otherwise, we have

$$\begin{aligned} p(X_0 \in N_g^0) &\leq p(X_0 \in N_g^0 \mid f_{A_g}(X_0) = 1) \\ &= \sum_{S^*, T^* \subseteq [n]} p(X_0 \in N_g^0 \mid S(X_0) = S^*, T(X_0) = T^*, f_{A_g}(X_0) = 1) \\ &\qquad \cdot p(S(X_0) = S^*, T(X_0) = T^* \mid f_{A_g}(X_0) = 1). \end{aligned} \tag{8}$$

When S^* was added to A_g, it was chosen as a largest set satisfying

$$p(S^* \subseteq Z \mid X_1 \in N_g^1) \geq r^{-|S^*|}.$$

Thus, for any set S' with $S^* \cap S' = \emptyset$, we have

$$p(S' \subseteq Z \mid S^* \subseteq Z, X_1 \in N_g^1) = \frac{p(S' \cup S^* \subseteq Z \mid X_1 \in N_g^1)}{p(S^* \subseteq Z \mid X_1 \in N_g^1)} \leq \frac{r^{-(|S^*|+|S'|)}}{r^{-|S^*|}} = r^{-|S'|}.$$

Therefore, $Z \backslash S^* \mid (S^* \subseteq Z, X_1 \in N_g^1)$ is a random r-spread set of size at most $2t$. Conditioned on $S(X_0) = S^*, T(X_0) = T^*$, the random variable X_0 is the union of an Erdős–Rényi graph with $\mathcal{C}_{T^*}$. Applying Lemma 2, we conclude that

$$p(X_0 \in N_g^0 \mid S(X_0) = S^*, T(X_0) = T^*, f_{A_g}(X_0) = 1) \leq 1 - p(\exists z \in \mathcal{Z}, \mathcal{C}_{S^* \cup z} \subseteq X_0 \cup \mathcal{C}_{S^*}) < \varepsilon.$$

Substituting this bound back into (8) yields

$$p(X_0 \in N_g^0) \leq \sum_{S^*, T^*} \varepsilon \cdot p(S(X_0) = S^*, T(X_0) = T^*, f_{A_g}(X_0) = 1) = \varepsilon.$$

□

Using the union bound with Lemmas 13 and 14, we find that if the circuit has size at most $1/(3\varepsilon)$, then

$$p\Big(X_1 \in \bigcup_g E_g^1\Big) \leq (1/(3\varepsilon)) \cdot \varepsilon \leq 1/3, \qquad p\Big(X_0 \in \bigcup_g E_g^0\Big) \leq (1/(3\varepsilon)) \cdot \varepsilon \leq 1/3,$$

proving Equation (7).

5. Exponential lower bounds for an explicit function

In this section we prove Theorem 9. Let $w \in D_d$ be uniformly random, and let $X_1 = w([k])$. Let $X_0 \subseteq [n]$ be uniformly random. We have

$$\begin{aligned} p(|w([k])| \leq k/2) &\leq p(|\{i, j \in [k], i \neq j, w(i) = w(j)\}| \geq k/2) \\ &\leq \frac{\mathbb{E}_w[|\{i, j \in [k], i \neq j, w(i) = w(j)\}|]}{k/2} \\ &\leq \frac{\binom{k}{2}/n}{k/2} \\ &\leq k/n, \end{aligned}$$

So, $p(F_{k,d}(X_1) = 1) \geq 1 - p(|w([k])| \leq k/2) \geq 1 - k/n \geq 2/3$.

$$p(F(X_0)=1) \le \sum_{\substack{w\in D_d \\ |w([k])|\ge k/2}} 2^{-k/2} \le n^{d+1}\cdot 2^{-k/2} \le 1/3,$$

because $3d\log n < k$. By the d-wise independence of the evaluations of w, for a set S with $|S| \le d$, we have

$$p(S \subseteq X_1) \le p(S \subseteq w([k])) \le \binom{k}{|S|}\cdot \frac{|S|!}{n^{|S|}} \le \left(\frac{n}{k}\right)^{-|S|}, \tag{9}$$

so X_1 is (n/k)-spread, at least for sets of size at most d. Set $\beta = 32\alpha$ and

$$t = d/2, \qquad \varepsilon = \exp(-n/(32\alpha k))$$
$$r = \alpha\log(t/\varepsilon)/(1/2)^2 \le n/(8k) + \alpha\log d \le n/(4k).$$

5.1. Approximation method

For a family of sets A, define

$$f_A(x) = \begin{cases} 1 & \text{if } \exists S\in A, S\subseteq x, \\ 0 & \text{otherwise.}\end{cases}$$

For each gate g of the circuit, we approximate it with a function f_{A_g}, with $|S| \le t$ for all $S \in A$. We define the sets of errors:

$$E_g^1 = \{x \in \mathcal{X}_1 : g(x) = 1, f_{A_g}(x) = 0\},$$

$$E_g^0 = \{x \in \mathcal{X}_0 : g(x) = 0, f_{A_g}(x) = 1\}.$$

We prove that if the circuit has at most $\min\{2^t, 1/\varepsilon\}/2$ gates and g is the output gate, then one can compute A_g with

$$p(X_1 \in E_g^1) \le 1/2, \text{ and } p(X_0 \in E_g^0) \le 1/2. \tag{10}$$

Given Lemma 1, this is enough to complete the proof of the theorem. Indeed, if the circuit is correct, then when $X_1 \notin E_g^1$, there must be some set $Z(X_1) \in A_g$ such that $Z(X_1) \subseteq X_1$, $|Z(X_1)| \le t$. Because $2t \le d$, by Equation (9), for any set S

$$p(S \subseteq Z(X_1) | X_1 \notin E_g^1) \le \frac{p(S \subseteq Z(X_1) \subseteq X_1, X_1 \notin E_g^1)}{p(X_1 \notin E_g^1)} \le 2\cdot(n/k)^{-|S|} \le (n/(2k))^{-|S|},$$

So, $Z(X_1)$ is r-spread. Lemma 1 then implies that

$$p(F(X_0)=1) \ge p(\exists z \in \mathcal{Z}, z \subseteq X_0) - p(X_0 \in E_g^0) \ge 1 - 1/2 - \varepsilon > 1/3,$$

which is a contradiction. Thus, a correct circuit must have more than $\min\{2^t, 1/\varepsilon\}/2$ gates, proving Theorem 9.

To prove Equation (10), we need to describe how to construct A_g for each gate g. The input gates already correspond to f_{A_g} with A_g containing a single set of size 1, so they are their own approximators. If g is computed from gates h_1, h_2, we show how to obtain A_g from A_{h_1}, A_{h_2}. If $g = h_1 \vee h_2$, we set $A_g = A_{h_1} \cup A_{h_2}$. This choice guarantees that $E^1_g \subseteq E^1_{h_1} \cup E^1_{h_2}$ and $E^0_g \subseteq E^0_{h_1} \cup E^0_{h_2}$, so no new errors are introduced. The more interesting case is when $g = h_1 \wedge h_2$. Then the natural choice is to set

$$A'_g = \{S_1 \cup S_2 : S_1 \in A_{h_1}, S_2 \in A_{h_2}\}.$$

The problem is that A'_g may contain a set of size $> t$. Given A_g, let

$$N^1_g = E^1_g \setminus (E^1_{h_1} \cup E^1_{h_2}) \text{ and } N^0_g = E^0_g \setminus (E^0_{h_1} \cup E^0_{h_2})$$

denote the sets of new errors. If $X_1 \in N^1_g$, then there must be a set $Z(X_1) \in A'_g$ with $Z(X_1) \subseteq X_1$ and $|Z(X_1)| \leq 2t$. We construct the final A_g using the following algorithm:

Algorithm 3 Computing A_g

$A_g \leftarrow \emptyset$

while $p(X_1 \in N^1_g) > 0$ **do**

  Find a largest set S such that $p(S \subseteq Z(X_1) \mid X_1 \in N^1_g) \geq r^{-|S|}$.

  if $|S| \leq t$ **then**

    $A_g \leftarrow A_g \cup \{S\}$

  else

    halt ; `// Terminate if largest valid set exceeds threshold t`

return A_g

At the end of this algorithm, A_g only contains sets of size at most t, if any. Let us bound the measure of the new errors.

Lemma 15. $p(X_1 \in N^1_g) \leq 2^{-t}$.

Proof. The non-trivial case is when the algorithm discovers a set S with $2t \geq |S| > t$. In this case we bound

$$p(X_1 \in N^1_g) = \frac{p(S \subseteq Z, X_1 \in N^1_g)}{p(S \subseteq Z | X_1 \in N^1_g)} \leq \frac{p(S \subseteq X_1)}{r^{-|S|}} \leq 2^{-|S|} \leq 2^{-t},$$

by the choice of parameters. □

Lemma 16. $p(X_0 \in N^0_g) \leq \varepsilon$.

Proof. For every $f_{A_g}(X_0) = 1$, let $S(X_0) \subseteq X_0$ be the lexicographically first set such that $S(X_0) \in A_g$. If $p(f_{A_g}(X_0) = 1) = 0$, then $p(X_0 \in N_g^0) = 0$. Otherwise, we have

$$\begin{aligned} p(X_0 \in N_g^0) &\leq p(X_0 \in N_g^0 \mid f_{A_g}(X_0) = 1) \\ &= \sum_{S^* \subseteq [n]} p(X_0 \in N_g^0 \mid S(X_0) = S^*, f_{A_g}(X_0) = 1) \cdot p(S(X_0) = S^* \mid f_{A_g}(X_0) = 1). \end{aligned} \tag{11}$$

When S^* was added to A_g, it was chosen as a largest set satisfying

$$p(S^* \subseteq Z \mid X_1 \in N_g^1) \geq r^{-|S^*|},$$

so for any set S' with $S^* \cap S' = \emptyset$, we have

$$p(S' \subseteq Z \mid S^* \subseteq Z, X_1 \in N_g^1) = \frac{p(S' \cup S^* \subseteq Z \mid X_1 \in N_g^1)}{p(S^* \subseteq Z \mid X_1 \in N_g^1)} \leq \frac{r^{-(|S^*|+|S'|)}}{r^{-|S^*|}} = r^{-|S'|}.$$

Therefore, $Z \setminus S^* \mid (S^* \subseteq Z, X_1 \in N_g^1)$ is an r-spread set of size at most $2t$. Conditioned on $S(X_0) = S^*$, the random variable $X_0 \setminus S^*$ is a uniformly random subset of the complement of S^*. Applying Lemma 1, we conclude that

$$p(X_0 \in N_g^0 \mid S(X_0) = S^*, f_{A_g}(X_0) = 1) \leq 1 - p(\exists z \in \mathcal{Z}, z \subseteq X_0 \cup S^*) < \varepsilon.$$

Substituting this bound back into (11) yields

$$p(X_0 \in N_g^0) \leq \sum_{S^*} \varepsilon \cdot p(S(X_0) = S^* \mid f_{A_g}(X_0) = 1) = \varepsilon,$$

which completes the proof. □

Using the union bound with Lemmas 15 and 16, we find that if the circuit has size at most $\min\{2^t, 1/\varepsilon\}/2$, then

$$p\Big(X_1 \in \bigcup_g E_g^1\Big) \leq 2^t \cdot 2^{-t}/2 \leq 1/2, \qquad p\Big(X_0 \in \bigcup_g E_g^0\Big) \leq (1/(2\varepsilon)) \cdot \varepsilon \leq 1/2,$$

proving Equation (10).

References

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

[2] Ryan Alweiss, Shachar Lovett, Kewen Wu, and Jiapeng Zhang. Improved bounds for the sunflower lemma. *Annals of Mathematics*, 194(3):795–815, 2021.

[3] A. E. Andreev. A method for obtaining efficient lower bounds for monotone complexity. *Algebra and Logic*, 26(1):1–18, 1987.

[4] Tolson Bell, Suchakree Chueluecha, and Lutz Warnke. Note on sunflowers. *CoRR*, abs/2009.09327, 2020.

[5] Christer Berg and Staffan Ulfberg. Symmetric approximation arguments for monotone lower bounds without sunflowers. *Comput. Complex.*, 8(1):1–20, June 1999.

[6] Jaroslaw Blasiok and Linus Meierhöfer. Hardness of clique approximation for monotone circuits. In *40th Computational Complexity Conference, CCC 2025, Toronto, Canada, August 5-8, 2025*, volume 339 of *LIPIcs*, pages 4:1–4:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025.

[7] Bruno Cavalar, Mika Göös, Artur Riazanov, Anastasia Sofronova, and Dmitry Sokolov. Monotone circuit complexity of matching. In *Proceedings of the 58th Annual ACM Symposium on Theory of Computing, STOC 2026*, pages 1128–1132. ACM, 2026.

[8] Bruno Pasqualotto Cavalar, Mrinal Kumar, and Benjamin Rossman. Monotone circuit lower bounds from robust sunflowers. *Algorithmica*, 84(12):3655–3685, 2022.

[9] Susanna F. de Rezende and Marc Vinyals. Lifting with colourful sunflowers. In *40th Computational Complexity Conference, CCC 2025, Toronto, Canada, August 5-8, 2025*, volume 339 of *LIPIcs*, pages 36:1–36:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025.

[10] Paul Erdös and Richard Rado. Intersection theorems for systems of sets. *Journal of the London Mathematical Society*, 35:85–90, 1960.

[11] Keith Frankston, Jeff Kahn, Bhargav Narayanan, and Jinyoung Park. Thresholds versus fractional expectation-thresholds. *Annals of Mathematics*, 194(2):475–495, 2021.

[12] Ankit Garg, Mika Göös, Pritish Kamath, and Dmitry Sokolov. Monotone circuit lower bounds from resolution. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 902–911. ACM, 2018.

[13] Armin Haken. Counting bottlenecks to show monotone P <=> NP. In *36th Annual Symposium on Foundations of Computer Science, FOCS 1995, Milwaukee, Wisconsin, USA, 23-25 October 1995*, pages 36–40. IEEE Computer Society, 1995.

[14] Danny Harnik and Ran Raz. Higher lower bounds on monotone size. In F. Frances Yao and Eugene M. Luks, editors, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*, pages 378–387. ACM, 2000.

[15] Shachar Lovett, Raghu Meka, Ian Mertz, Toniann Pitassi, and Jiapeng Zhang. Lifting with sunflowers. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, Berkeley, CA, USA, January 31 - February 3, 2022*, volume 215 of *LIPIcs*, pages 104:1–104:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[16] Anup Rao. Coding for Sunflowers. *Discrete Analysis*, feb 25 2020.

[17] Anup Rao. The story of sunflowers. *Journal of the London Mathematical Society*, 113(1):e70380, 2026.

[18] Anup Rao and Amir Yehudayoff. *Communication Complexity: and Applications*. Cambridge University Press, 2020.

[19] Ran Raz and Avi Wigderson. Monotone circuits for matching require linear depth. *Journal of the ACM*, 39(3):736–744, 1992.

[20] Alexandr A. Razborov. Lower bounds for the monotone complexity of some boolean functions. *Soviet Mathematics Doklady*, 31(2):354–357, 1985.

[21] Benjamin Rossman. The monotone complexity of k-clique on random graphs. *SIAM J. Comput.*, 43(1):256–279, 2014.

[22] Michel Talagrand. Are many small sets explicitly small? In Leonard J. Schulman, editor, *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010*, pages 13–36. ACM, 2010.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il