Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 181 (2020)

Monotone Circuit Lower Bounds from Robust Sunflowers

Bruno Pasqualotto Cavalar [*] University of Warwick

Mrinal Kumar [†] IIT Bombay

Benjamin Rossman [‡] Duke University

August 5, 2022

Abstract

Robust sunflowers are a generalization of combinatorial sunflowers that have applications in monotone circuit complexity [24], DNF sparsification [11], randomness extractors [17], and recent advances on the Erdős-Rado sunflower conjecture [3,18,21]. The recent breakthrough of Alweiss, Lovett, Wu and Zhang [3] gives an improved bound on the maximum size of a w-set system that excludes a robust sunflower. In this paper, we use this result to obtain an $\exp(n^{1/2-o(1)})$ lower bound on the monotone circuit size of an explicit n-variate monotone function, improving the previous best known $\exp(n^{1/3-o(1)})$ due to Andreev [5] and Harnik and Raz [12]. We also show an $\exp(\Omega(n))$ lower bound on the monotone *arithmetic* circuit size of a related polynomial via a very simple proof. Finally, we introduce a notion of robust clique-sunflowers and use this to prove an $n^{\Omega(k)}$ lower bound on the monotone circuit size of the CLIQUE function for all $k \leqslant n^{1/3-o(1)}$, strengthening the bound of Alon and Boppana [1].

Contents

[*]Email: Bruno.Pasqualotto-Cavalar@warwick.ac.uk
[†]Email: mrinalkumar08@gmail.com
[‡]Email: benjamin.rossman@duke.edu

ISSN 1433-8092

1 Introduction

A monotone Boolean circuit is a Boolean circuit with AND and OR gates but no negations (NOT gates). Although a restricted model of computation, monotone Boolean circuits seem a very natural model to work with when computing *monotone* Boolean functions, i.e., Boolean functions $f : \{0,1\}^n \to \{0,1\}$ such that for all pairs of inputs $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in \{0,1\}^n$ where $a_i \leqslant b_i$ for every i, we have $f(a_1, a_2, \ldots, a_n) \leqslant f(b_1, b_2, \ldots, b_n)$. Many natural and well-studied Boolean functions such as Clique and Majority are monotone.

Monotone Boolean circuits have been very well studied in Computational Complexity over the years, and continue to be one of the few seemingly largest natural sub-classes of Boolean circuits for which we have exponential lower bounds. This line of work started with an influential paper of Razborov [23] from 1985 which proved an $n^{\Omega(k)}$ lower bound on the size of monotone circuits computing the $\mathsf{Clique}_{k,n}$ function on n-vertex graphs for $k \leqslant \log n$; this bound is super-polynomial for $k = \log n$. Prior to Razborov's result, super-linear lower bounds for monotone circuits were unknown, with the best bound being a lower bound of $4n$ due to Tiekenheinrich [29]. Further progress in this line of work included the results of Andreev [4] who proved an exponential lower bound for another explicit function. Alon and Boppana [1] extended Razborov's result by proving an $n^{\Omega(\sqrt{k})}$ lower bound for $\mathsf{Clique}_{k,n}$ for all $k \leqslant n^{2/3-o(1)}$. A second paper of Andreev [5] from the same time period proved an $2^{\Omega(n^{1/3}/\log n)}$ lower bound for an explicit n-variate monotone function. Using a different technique, Harnik and Raz [12] proved a lower bound of $2^{\Omega((n/\log n)^{1/3})}$ for a family of explicit n-variate functions defined using a small probability space of random variables with bounded independence. However, modulo improvements to the polylog factor in this exponent, the state of art monotone circuit lower bounds have been stuck at $2^{\Omega(n^{1/3-o(1)})}$ since 1987.[1] To this day, the question of proving truly exponential lower bounds for monotone circuits (of the form $2^{\Omega(n)}$) for an explicit n-variate function) remains open! (Truly exponential lower bounds for monotone *formulas* were obtained only recently [20].)

[1] Stasys Jukna (personal communication) observed that Andreev's bound [5] can be improved to $2^{\Omega((n/\sqrt{\log n})^{1/3})}$ using the lower bound criterion of [16].

In the present paper, we are able to improve the best known lower bound for monotone circuits by proving an $2^{\Omega(n^{1/2}/\log n)}$ lower bound for an explicit n-variate monotone Boolean function (Section 2). The function is based on the same construction first considered by Harnik and Raz, but our argument employs the approximation method of Razborov with recent improvements on robust sunflower bounds [3, 21]. By applying the same technique with a variant of robust sunflowers that we call clique-sunflowers, we are able to prove an $n^{\Omega(k)}$ lower bound for the $\mathsf{Clique}_{k,n}$ function when $k \leqslant n^{1/3-o(1)}$, thus improving the result of Alon and Boppana when k is in this range (Section 3). Finally, we are able to prove truly exponential lower bounds in the monotone arithmetic setting to a fairly general family of polynomials, which shares some similarities to the functions considered by Andreev and Harnik and Raz (Section 4).

1.1 Monotone circuit lower bounds and sunflowers

The original lower bound for $\mathsf{Clique}_{k,n}$ due to Razborov employed a technique which came to be known as the *approximation method*. Given a monotone circuit C of "small size", it consists into constructing gate-by-gate, in a bottom-up fashion, another circuit $\widetilde{C}$ that approximates C on most inputs of interest. One then exploits the structure of this *approximator circuit* to prove that it differs from $\mathsf{Clique}_{k,n}$ on most inputs of interest, thus implying that no "small" circuit can compute this function. This technique was leveraged to obtain lower bounds for a host of other monotone problems [1].

A crucial step in Razborov's proof involved the sunflower lemma due to Erdős and Rado. A family $\mathcal{F}$ of subsets of $[n]$ is called a *sunflower* if there exists a set Y such that $F_1 \cap F_2 = Y$ for every $F_1, F_2 \in \mathcal{F}$. The sets of $\mathcal{F}$ are called *petals* and the set $Y = \bigcap \mathcal{F}$ is called the *core*. We say that the family $\mathcal{F}$ is ℓ-uniform if every set in the family has size ℓ.

Theorem 1.1 (Erdős and Rado [8])**.** *Let $\mathcal{F}$ be a ℓ-uniform family of subsets of $[n]$. If $|\mathcal{F}| > \ell!(r-1)^\ell$, then $\mathcal{F}$ contains a sunflower of r petals.*

Informally, the sunflower lemma allows one to prove that a monotone function can be approximated by one with fewer minterms by means of the "plucking" procedure: if the function has too many (more than $\ell!(r-1)^\ell$) minterms of size ℓ, then it contains a sunflower with r petals; remove all the petals, replacing them with the core. One can then prove that this procedure does not introduce many errors.

The notion of *robust sunflowers* was introduced by the third author in [24], to achieve better bounds via the approximation method on the monotone circuit size of $\mathsf{Clique}_{k,n}$ when the negative instances are Erdős-Rényi random graphs $\boldsymbol{G}_{n,p}$ below the k-clique threshold.[2] A family $\mathcal{F} \subseteq 2^{[n]}$ is called a (p,ε)-*robust sunflower* if

$$\mathop{\mathbb{P}}_{\boldsymbol{W} \subseteq_p [n]} [\exists F \in \mathcal{F} : F \subseteq \boldsymbol{W} \cup Y] > 1 - \varepsilon,$$

where $Y := \bigcap \mathcal{F}$ and $\boldsymbol{W}$ is a p-random subset of $[n]$ (i.e., every element of $[n]$ is contained in $\boldsymbol{W}$ independently with probability p).

As remarked in [24], every ℓ-uniform sunflower of r petals is a (p, e^{-rp^ℓ})-robust sunflower. Moreover, as observed in [18], every $(1/r, 1/r)$-robust sunflower contains a sunflower of r petals.

[2] Robust sunflowers were called *quasi-sunflowers* in [11, 17, 18, 24] and *approximate sunflowers* in [19]. Following Alweiss *et al* [3], we adopt the new name *robust sunflower*.

A corresponding bound for the appearance of robust sunflowers in large families was also proved in [24].

Theorem 1.2 ([24]). *Let $\mathcal{F}$ be a ℓ-uniform family such that $|\mathcal{F}| \geqslant \ell!(2\log(1/\varepsilon)/p)^\ell$. Then $\mathcal{F}$ contains a (p,ε)-robust sunflower.*

For many choice of parameters p and ε, this bound is better than the one by Erdős and Rado, thus leading to better approximation bounds. In a recent breakthrough, this result was significantly improved by Alweiss, Lovett, Wu and Zhang [3]. Soon afterwards, alternative proofs with slightly improved bounds were given by Rao[3] [21] and Tao [28]. A more detailed discussion can be found in a note by Bell, Suchakree and Warnke [6].

Theorem 1.3 ([3, 6, 21, 28]). *There exists a constant $B > 0$ such that the following holds for all $p, \varepsilon \in (0, 1/2]$. Let $\mathcal{F}$ be an ℓ-uniform family such that $|\mathcal{F}| \geqslant (B\log(\ell/\varepsilon)/p)^\ell$. Then $\mathcal{F}$ contains a (p,ε)-robust sunflower.*

Theorem 1.3 can be verified by combining the basic structure of Rossman's original argument [24] with the main technical estimate of Rao [21]. Since the proof does not appear explicitly in any of those papers, for completeness we give a proof on Appendix A.

1.2 Preliminaries

We denote by $\{0,1\}^n_{=m} \subseteq \{0,1\}^n$ the set of all n-bit binary vectors with Hamming weight exactly m. We extend the logical operators $\vee$ and $\wedge$ to binary strings $x, y \in \{0,1\}^n$, as follows:

- $(x \wedge y)_i = x_i \wedge y_i$, for every $i \in [n]$;
- $(x \vee y)_i = x_i \vee y_i$, for every $i \in [n]$.

We will say that a distribution $\boldsymbol{X}$ with support in $\{0,1\}^n$ is *p-biased* or *p-random* if the random variables $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n$ are mutually independent and satisfy $\mathbb{P}[\boldsymbol{X}_i = 1] = p$ for all i. If a distribution $\boldsymbol{U}$ has support in $2^{[n]}$, we will say that $\boldsymbol{U}$ is *p-biased* or *p-random* if the random Boolean string $\boldsymbol{X}$ such that $\boldsymbol{X}_i = 1 \iff i \in \boldsymbol{U}$ is p-biased. We sometimes write $\boldsymbol{U} \subseteq_p [n]$ to denote that $\boldsymbol{U}$ is a p-biased subset of $[n]$.

We consistently write random objects using boldface symbols (such as $\boldsymbol{W}$, $\boldsymbol{G}_{n,p}$, etc). Everything that is not written in boldface is not random. When taking probabilities or expectation, the underlying distribution is always the one referred to by the boldface symbol. For instance, when $i \in [n]$ and $\boldsymbol{W}$ is a p-biased subset of $[n]$, the event $\{i \in \boldsymbol{W}\}$ denotes that the *non-random* element i is contained in the *random* set $\boldsymbol{W}$.

For a Boolean function f and a probability distribution $\boldsymbol{\mu}$ on the inputs on f, we write $f(\boldsymbol{\mu})$ to denote the random variable which evaluates f on a random instance of $\boldsymbol{\mu}$.

In what follows, we will mostly ignore ceilings and floors for the sake of convenience, since these do not make any substantial difference in the final calculations.

[3] Rao's bound is also slightly stronger in the following sense. He shows that, if the random set $\boldsymbol{W}$ is chosen uniformly at random among all sets of size $\lfloor np \rfloor$, then we also have $\mathbb{P}[\exists F \in \mathcal{F} : F \subseteq \boldsymbol{W} \cup Y] > 1 - \varepsilon$. However, for our purposes, the p-biased case will suffice.

2 Harnik-Raz function

The strongest lower bound known for monotone circuits computing an explicit n-variate monotone Boolean function is $\exp\big(\Omega\big((n/\log n)^{1/3}\big)\big)$, and it was obtained by Harnik and Raz [12]. In this section, we will prove a lower bound of $\exp(\Omega(n^{1/2}/\log n))$ for the same Boolean function they considered. We apply the *method of approximations* [23] and the new *robust sunflower* bound [3, 21]. We do not expect that a lower bound better than $\exp(n^{1/2-o(1)})$ can be obtained by the approximation method with robust sunflowers. This limitation is discussed with more detail in Section 2.8.

We start by giving a high level outline of the proof. We define the Harnik-Raz function $f_{\mathrm{HR}} : \{0,1\}^n \to \{0,1\}$ and find two distributions $\boldsymbol{Y}$ and $\boldsymbol{N}$ with support in $\{0,1\}^n$ satisfying the following properties:

- f_{HR} outputs 1 on $\boldsymbol{Y}$ with high probability (Lemma 2.3);
- f_{HR} outputs 0 on $\boldsymbol{N}$ with high probability (Lemma 2.4).

Because of these properties, the distribution $\boldsymbol{Y}$ is called the *positive test distribution*, and $\boldsymbol{N}$ is called the *negative test distribution*. We also define a set of monotone Boolean functions called *approximators*, and we show that:

- every approximator commits many mistakes on either $\boldsymbol{Y}$ or $\boldsymbol{N}$ with high probability (Lemma 2.17);
- every Boolean function computed by a "small" monotone circuit agrees with an approximator on both $\boldsymbol{Y}$ and $\boldsymbol{N}$ with high probability (Lemma 2.18).

Together these suffice for proving that "small" circuits cannot compute f_{HR}. The crucial part where the robust sunflower result comes into play is in the last two items.

2.1 Notation for this section

For $A \subseteq [n]$, let $x_A \in \{0,1\}^n$ be the binary vector with support in A. For a set $A \subseteq [n]$, let $\lceil A \rceil$ be the indicator function satisfying

$$\lceil A \rceil(x) = 1 \iff x_A \leqslant x.$$

For a monotone Boolean function $f : \{0,1\}^n \to \{0,1\}$, let $\mathcal{M}(f)$ denote the set of minterms of f, and let $\mathcal{M}_\ell(f) := \mathcal{M}(f) \cap \{0,1\}^n_{=\ell}$. Elements of $\mathcal{M}_\ell(f)$ are called ℓ-minterms of f.

This notation is valid only in Section 2 and will be slightly tweaked in Section 3 (Lower Bound for $\mathsf{Clique}_{k,n}$) for the sake of uniformity of exposition.

2.2 The function

We now describe the construction of the function $f_{\mathrm{HR}} : \{0,1\}^n \to \{0,1\}$ considered by Harnik and Raz [12]. First observe that, for every n-bit monotone Boolean function f, there exists a family $\mathcal{S} \subseteq 2^{[n]}$ such that

$$f(x_1, \ldots, x_n) = D_{\mathcal{S}}(x_1, \ldots, x_n) := \bigvee_{S \in \mathcal{S}} \bigwedge_{j \in S} x_j.$$

Indeed, $\mathcal{S}$ can be chosen to be the family of the coordinate-sets of minterms of f. Now, in order to construct the Harnik-Raz function, we will suppose n is a prime number and let $\mathbb{F}_n =$

$\{0, 1, \ldots, n-1\}$ be the field of n elements. Moreover, we fix two positive integers c and k with $c < k < n$. For a polynomial $P \in \mathbb{F}_n[x]$, we let S_P be the set of the valuations of P in each element of $\{1, 2, \ldots, k\}$ (in other words, $S_P = \{P(1), \ldots, P(k)\}$). Observe that it is not necessarily the case that $|S_P| = k$, since it may happen that $P(i) = P(j)$ for some i, j such that $i \neq j$. Finally, we consider the family $\mathcal{S}_{\mathrm{HR}}$ defined as

$$\mathcal{S}_{\mathrm{HR}} := \{S_P : P \in \mathbb{F}_n[x], P \text{ has degree at most } c-1 \text{ and } |S_P| \geqslant k/2\}.$$

We thus define f_{HR} as $f_{\mathrm{HR}} := D_{\mathcal{S}_{\mathrm{HR}}}$.

We now explain the choice of $\mathcal{S}_{\mathrm{HR}}$. First, the choice for valuations of polynomials with degree at most $c-1$ is explained by a fact observed in [2]. If a polynomial $\boldsymbol{P} \in \mathbb{F}_n[x]$ with degree $c-1$ is chosen uniformly at random, they observed that the random variables $\boldsymbol{P}(1), \ldots, \boldsymbol{P}(k)$ are c-wise independent, and are each uniform in $[n]$. This allows us to define a distribution on the inputs (the positive test distribution) that has high agreement with f_{HR} and is easy to analyze. Observe further that, since $|\mathcal{S}_{\mathrm{HR}}| \leqslant n^c$, the monotone complexity of f_{HR} is at most $2^{O(c \log n)}$. Later we will choose c to be roughly $n^{1/2}$, and prove that the monotone complexity of f_{HR} is $2^{\Omega(c)}$.

Finally, the restriction $|S_P| \geqslant k/2$ is a truncation made to ensure that no minterm of f_{HR} is very small. Otherwise, if f_{HR} had small minterms, it might have been a function that almost always outputs 1. Such functions have very few maxterms and are therefore computed by a small CNF. Since we desire f_{HR} to have high complexity, this is an undesirable property. The fact that f_{HR} doesn't have small minterms is important in the proof that f_{HR} almost surely outputs 0 in the negative test distribution (Lemma 2.4).

Remark 2.1 (Parameters are now fixed)**.** *Formally, the function f_{HR} depends on the choice of the parameters c and k. In other words, for every choice of positive integers c, k such that $c < k < n$, we obtain a different function $f_{\mathrm{HR}}^{(c,k)}$. For the rest of Section 2, we will let c and k be fixed parameters, and we will refer to f_{HR} unambiguously, always with respect to the fixed parameters c and k. We will make our choice of c and k explicit in Section 2.7, but before then we will make no assumptions about c and k other than $c < k < n$.*

2.3 Test distributions

We now define the positive and negative test distributions.

Definition 2.2 (Test distributions)**.** *Let $\boldsymbol{Y} \in \{0,1\}^n$ be the random variable which chooses a polynomial $\boldsymbol{P} \in \mathbb{F}_n[x]$ with degree at most $c-1$ uniformly at random, and maps it into the binary input $x_{S_{\boldsymbol{P}}} \in \{0,1\}^n$. Let also $\boldsymbol{N}$ be the $(1/2)$-biased distribution on $\{0,1\}^n$ (i.e., each bit is equal to 1 with probablity $1/2$, independently of all the others). Equivalently, $\boldsymbol{N}$ is the uniform distribution on $\{0,1\}^n$.*

Harnik and Raz proved that f_{HR} outputs 1 on $\boldsymbol{Y}$ with high probability. For completeness, we include their proof.

Lemma 2.3 (Claim 4.1 in [12])**.** *We have $\mathbb{P}[f_{\mathrm{HR}}(\boldsymbol{Y}) = 1] \geqslant 1 - (k-1)/n$.*

Proof. Let $\boldsymbol{P}$ be the polynomial randomly chosen by $\boldsymbol{Y}$. Call a pair $\{i, j\} \subseteq [k]$ with $i \neq j$ *coinciding* if $\boldsymbol{P}(i) = \boldsymbol{P}(j)$. Because the random variables $\boldsymbol{P}(i)$ and $\boldsymbol{P}(j)$ are uniformly distributed in $[n]$ and independent for $i \neq j$, we have that $\mathbb{P}[\boldsymbol{P}(i) = \boldsymbol{P}(j)] = 1/n$ for $i \neq j$. Therefore, the

expected number $\mathsf{Num}(\boldsymbol{P})$ of coiciding pairs is $\binom{k}{2}/n$. Observe now that $f_{\mathrm{HR}}(\boldsymbol{Y}) = 0$ if and only if $|\boldsymbol{P}(1), \ldots, \boldsymbol{P}(k)| < k/2$, which occurs only if there exists more than $k/2$ coinciding pairs. Therefore, by Markov's inequality, we have

$$\mathbb{P}\left[f_{\mathrm{HR}}(\boldsymbol{Y}) = 0\right] \leqslant \mathbb{P}\left[\mathsf{Num}(\boldsymbol{P}) > k/2\right] \leqslant \frac{\binom{k}{2}/n}{k/2} = \frac{k-1}{n}. \qquad \square$$

$\square$

We now claim that f_{HR} also outputs 0 on $\boldsymbol{N}$ with high probability.

Lemma 2.4. *We have* $\mathbb{P}[f_{\mathrm{HR}}(\boldsymbol{N}) = 0] \geqslant 1 - 2^{-(k/2 - c\cdot\log_2 n)}$.

Proof. Let $x_{\boldsymbol{A}}$ be an input sampled from $\boldsymbol{N}$. Observe that $f_{\mathrm{HR}}(x_{\boldsymbol{A}}) = 1$ only if there exists a minterm x of f_{HR} such that $x \leqslant x_{\boldsymbol{A}}$. Since all minterms of f_{HR} have Hamming weight at least $k/2$ and f_{HR} has at most n^c minterms, we have

$$\mathbb{P}[f_{\mathrm{HR}}(\boldsymbol{N}) = 1] \leqslant n^c \cdot 2^{-k/2} = 2^{-(k/2 - c\cdot\log_2 n)}.$$

$\square$

We will also need the following property about the positive test distribution.

Lemma 2.5. *For every* $\ell \leqslant c$ *and* $A \subseteq [n]$ *such that* $|A| = \ell$*, we have*

$$\mathbb{P}[x_A \leqslant \boldsymbol{Y}] \leqslant (k/n)^{\ell}.$$

Proof. Recall that the distribution $\boldsymbol{Y}$ takes a polynomial $\boldsymbol{P} \in \mathbb{F}_n[x]$ with degree at most $c-1$ uniformly at random and returns the binary vector $x_{\{\boldsymbol{P}(1), \boldsymbol{P}(2), \ldots, \boldsymbol{P}(k)\}} \in \{0,1\}^n$. Let $A \in \binom{[n]}{\ell}$ for $\ell \leqslant c$. Observe that $x_A \leqslant \boldsymbol{Y}$ if and only if $A \subseteq \{\boldsymbol{P}(1), \boldsymbol{P}(2), \ldots, \boldsymbol{P}(k)\}$. Therefore, if $x_A \leqslant \boldsymbol{Y}$, then there exists indices $\{j_1, \ldots, j_\ell\}$ such that $\{\boldsymbol{P}(j_1), \boldsymbol{P}(j_2), \ldots, \boldsymbol{P}(j_\ell)\} = A$. Since $\ell \leqslant c$, we get by the c-wise independence of $\boldsymbol{P}(1), \ldots, \boldsymbol{P}(k)$ that the random variables $\boldsymbol{P}(j_1), \boldsymbol{P}(j_2), \ldots, \boldsymbol{P}(j_\ell)$ are independent. It follows that

$$\mathbb{P}[\{\boldsymbol{P}(j_1), \boldsymbol{P}(j_2), \ldots, \boldsymbol{P}(j_\ell)\} = A] = \frac{\ell!}{n^\ell}.$$

Therefore, we have

$$\mathbb{P}[x_A \leqslant \boldsymbol{Y}] = \mathbb{P}[A \subseteq \{\boldsymbol{P}(1), \boldsymbol{P}(2), \ldots, \boldsymbol{P}(k)\}] \leqslant \binom{k}{\ell}\frac{\ell!}{n^\ell} \leqslant \left(\frac{k}{n}\right)^{\ell}. \qquad \square$$

2.4 A closure operator

In this section, we describe a closure operator in the lattice of monotone Boolean functions. We prove that the closure of a monotone Boolean function f is a good approximation for f on the negative test distribution (Lemma 2.10), and we give a bound on the size of the set of minterms of *closed* monotone functions. This bound makes use of the robust sunflower lemma (Theorem 1.3), and is crucial to bounding errors of approximation (Lemma 2.16). Finally, we observe that input functions are closed (Lemma 2.12). From now on, we let

$$\varepsilon := n^{-2c}. \tag{1}$$

Definition 2.6 (Closed function)**.** *We say that a monotone function* $f : \{0,1\}^n \to \{0,1\}$ *is* closed *if, for every* $A \in \binom{[n]}{\leqslant c}$*, we have*

$$\mathbb{P}[\ f(\boldsymbol{N} \vee x_A) = 1\ ] > 1 - \varepsilon \implies f(x_A) = 1.$$

This means that for, a closed function, we always have $\mathbb{P}[f(\boldsymbol{N} \vee x_A) = 1] \notin (1-\varepsilon, 1)$ when $|A| \leqslant c$.

Remark 2.7 (On the parametrization of closedness)**.** *We remark that the definition of a* closed *function depends on two parameters: the parameter* ε*, defined in (1), and the parameter* c*, used in the construction of* f_{HR} *(see Remark 2.1). Since both of these parameters are fixed throughout Section 2, it is safe to omit them without risk of confusion. Therefore, we will henceforth say that some function is* closed *without any further specification about the parameters. However, the reader must bear in mind that, whenever a function is said to be* closed*, the* fixed *parameters* c *and* ε *are in view.*

Definition 2.8 (Closure operator)**.** *Let* f *be a monotone Boolean function. We denote by* $\mathrm{cl}(f)$ *the unique minimal closed monotone Boolean function such that* $f \leqslant \mathrm{cl}(f)$*. In other words, the function* $\mathrm{cl}(f)$ *is the unique closed monotone function such that, whenever* $f \leqslant g$ *and* g *is monotone and closed, we have* $f \leqslant \mathrm{cl}(f) \leqslant g$*.*

Remark 2.9 (On closure)**.** *Note that* $\mathrm{cl}(f)$ *is well-defined, since the constant Boolean function that outputs* 1 *is closed and, if* f, g *are both closed monotone Boolean functions, then so is* $f \wedge g$*. Furthermore, just as with the definition of closed functions (see Remark 2.7), the closure operator* $\mathrm{cl}(\cdot)$ *depends crucially on the parameters* ε *and* c*, which are fixed throughout Section 2.*

We now give a bound on the error of approximating f by $\mathrm{cl}(f)$ under the distribution $\boldsymbol{N}$.

Lemma 2.10 (Approximation by closure)**.** *For every monotone* $f : \{0,1\}^n \to \{0,1\}$*, we have*

$$\mathbb{P}\left[f(\boldsymbol{N}) = 0 \text{ and } \mathrm{cl}(f)(\boldsymbol{N}) = 1\right] \leqslant n^{-c}.$$

Proof. We first prove that there exists a positive integer t and sets $A_1, \ldots, A_t$ and monotone functions $h_0, h_1, \ldots, h_t : \{0,1\}^n \to \{0,1\}$ such that

1. $h_0 = f$,
2. $h_i = h_{i-1} \vee \lceil A_i \rceil$,
3. $\mathbb{P}[h_{i-1}(\boldsymbol{N} \vee x_{A_i}) = 1] \geqslant 1 - \varepsilon$,
4. $h_t = \mathrm{cl}(f)$.

Indeed, if h_{i-1} is not closed, there exists $A_i \in \binom{[n]}{\leqslant c}$ such that $\mathbb{P}[h_{i-1}(\boldsymbol{N} \vee x_{A_i}) = 1] \geqslant 1 - \varepsilon$ but $h_{i-1}(x_{A_i}) = 0$. We let $h_i := h_{i-1} \vee \lceil A_i \rceil$. Clearly, we have that h_t is closed, and that the value of t is at most the number of subsets of $[n]$ of size at most c. Therefore, we get $t \leqslant \sum_{j=0}^{c} \binom{n}{j}$. Moreover, by induction we obtain that $h_i \leqslant \mathrm{cl}(f)$ for every $i \in [t]$. It follows that $h_t = \mathrm{cl}(f)$. Now, observe

that

$$\begin{aligned}\mathbb{P}\left[f(\boldsymbol{N})=0 \text{ and } \mathrm{cl}(f)(\boldsymbol{N})=1\right] &\leqslant \sum_{i=1}^{t} \mathbb{P}\left[h_{i-1}(\boldsymbol{N})=0 \text{ and } h_i(\boldsymbol{N})=1\right] \\ &= \sum_{i=1}^{t} \mathbb{P}\left[h_{i-1}(\boldsymbol{N})=0 \text{ and } x_{A_i} \leqslant \boldsymbol{N}\right] \\ &\leqslant \sum_{i=1}^{t} \mathbb{P}\left[h_{i-1}(\boldsymbol{N} \vee x_{A_i})=0\right] \\ &\leqslant \varepsilon \sum_{j=0}^{c} \binom{n}{j} \leqslant n^{-c}. \end{aligned}$$

□

We now bound the size of the set of ℓ-minterms of a closed function. This bound depends on the robust sunflower theorem (Theorem 1.3).

Lemma 2.11 (Closed functions have few minterms)**.** *Let $B > 0$ be as in Theorem 1.3. If a monotone function $f : \{0,1\}^n \to \{0,1\}$ is closed, then, for all $\ell \in [c]$, we have*

$$|\mathcal{M}_\ell(f)| \leqslant (6Bc \log n)^\ell$$

Proof. Fix $\ell \in [c]$. For convenience, let $p = 1/2$ and recall from (3) that $\varepsilon = n^{-2c}$. We will begin by proving that $|\mathcal{M}_\ell(f)| \leqslant (B \log(\ell/\varepsilon)/p)^\ell$.

For a contradiction, suppose we have $|\mathcal{M}_\ell(f)| > (B \log(\ell/\varepsilon)/p)^\ell$. Consider the family $\mathcal{F} := \left\{A \in \binom{[n]}{\ell} : x_A \in \mathcal{M}_\ell(f)\right\}$. Observe that $|\mathcal{F}| = |\mathcal{M}_\ell(f)|$. By Theorem 1.3, there exists a (p,ε)-robust sunflower $\mathcal{F}' \subseteq \mathcal{F}$. Let $Y := \bigcap \mathcal{F}'$ and let $\boldsymbol{W} \subseteq_p [n]$. We have

$$\begin{aligned}\mathbb{P}[f(\boldsymbol{N} \vee x_Y)=1] &\geqslant \mathbb{P}[\exists x \in \mathcal{M}_\ell(f) : x \leqslant \boldsymbol{N} \vee x_Y] \\ &= \mathbb{P}[\exists F \in \mathcal{F} : F \subseteq \boldsymbol{W} \cup Y] \\ &\geqslant \mathbb{P}[\exists F \in \mathcal{F}' : F \subseteq \boldsymbol{W} \cup Y] \\ &> 1-\varepsilon. \end{aligned}$$

Therefore, since f is closed, we get that $f(x_Y) = 1$. However, since $Y = \bigcap \mathcal{F}'$, there exists $F \in \mathcal{F}'$ such that $Y \subsetneq F$. This is a contradiction, because x_F is a minterm of f. We conclude that

$$|\mathcal{M}_\ell(f)| \leqslant (B \log(\ell/\varepsilon)/p)^\ell \leqslant (2B \log(cn^{2c}))^\ell \leqslant (6Bc \log n)^\ell.$$

□

Lemma 2.12 (Input functions are closed)**.** *For all $i \in [n]$ and large enough n, the Boolean functions $\lceil\{i\}\rceil$ are closed.*

Proof. Fix $i \in [n]$. Let $A \subseteq [n]$ be such that $|A| \leqslant c$ and suppose that $\lceil\{i\}\rceil(x_A) = 0$. Note that $\lceil\{i\}\rceil(x_A) = 0$ is equivalent to $(x_A)_i = 0$. We have

$$\mathbb{P}[\lceil\{i\}\rceil(\boldsymbol{N} \vee x_A)=1] = \mathbb{P}[(\boldsymbol{N} \vee x_A)_i = 1] = \mathbb{P}[\boldsymbol{N}_i = 1] = 1/2 \leqslant 1 - n^{-2c} = 1-\varepsilon,$$

since $\boldsymbol{N}$ is $(1/2)$-biased (Definition 2.2) and $\varepsilon = n^{-2c}$ (as fixed in (3)). Therefore, $\lceil\{i\}\rceil$ is closed. □

2.5 Trimmed monotone functions

In this section, we define a *trimming* operation for Boolean functions. We will bound the probability that a *trimmed* function gives the correct output on the distribution $\boldsymbol{Y}$, and we will give a bound on the error of approximating a Boolean function f by the trimming of f on that same distribution.

Definition 2.13 (Trimmed functions)**.** *We say that a monotone function $f \in \{0,1\}^n \to \{0,1\}$ is* trimmed *if all the minterms of f have size at most $c/2$. We define the trimming operation* $\mathrm{trim}(f)$ *as follows:*

$$\mathrm{trim}(f) := \bigvee_{\ell=0}^{c/2} \bigvee_{A \in \mathcal{M}_\ell(f)} \lceil A \rceil.$$

That is, the trim operation takes out from f all the minterms of size larger than $c/2$, yielding a trimmed function.

Remark 2.14 (Parametrization of $\mathrm{trim}(\cdot)$ and other remarks)**.** *We remark that the definition of trimmed functions depends on the choice of the parameter c. As this parameter is fixed (see Remark 2.1), the operator* $\mathrm{trim}(\cdot)$ *is well-defined. Moreover, if all minterms of f have Hamming weight larger than $c/2$ (i.e., if $\mathcal{M}_\ell(f) = \emptyset$ for all $\ell \in \{0, 1, \ldots, c/2\}$), then* $\mathrm{trim}(f)$ *is the constant function that outputs 0. Finally, if f is the constant function $\mathbb{1}$, then* $\mathrm{trim}(f) = \mathbb{1}$*, because $\mathbb{1}$ contains a minterm of Hamming weight equal to 0.*

We are now able to bound the probability that a trimmed Boolean function gives the correct output on distribution $\boldsymbol{Y}$ and give a bound on the approximation error of the trimming operation.

Lemma 2.15 (Trimmed functions are inaccurate in the positive distribution)**.** *If a monotone function $f \in \{0,1\}^n \to \{0,1\}$ is trimmed and $f \neq \mathbb{1}$ (i.e., f is not identically 1), then*

$$\mathbb{P}\left[f(\boldsymbol{Y}) = 1\right] \leqslant \sum_{\ell=1}^{c/2} \left(\frac{k}{n}\right)^\ell \left|\mathcal{M}_\ell(f)\right|.$$

Proof. It suffices to see that, since f is trimmed, if $f(\boldsymbol{Y}) = 1$ and $f \neq \mathbb{1}$ then there exists a minterm x of f with Hamming weight between 1 and $c/2$ such that $x \leqslant \boldsymbol{Y}$. The result follows from Lemma 2.5 and the union bound. □

Lemma 2.16 (Approximation by trimming)**.** *Let $f \in \{0,1\}^n \to \{0,1\}$ be a monotone function, all of whose minterms have Hamming weight at most c. We have*

$$\mathbb{P}\left[f(\boldsymbol{Y}) = 1 \text{ and } \mathrm{trim}(f)(\boldsymbol{Y}) = 0\right] \leqslant \sum_{\ell=c/2}^{c} \left(\frac{k}{n}\right)^\ell \left|\mathcal{M}_\ell(f)\right|.$$

Proof. If we have $f(\boldsymbol{Y}) = 1$ and $\mathrm{trim}(f)(\boldsymbol{Y}) = 0$, then there was a minterm x of f with Hamming weight larger than $c/2$ that was removed by the trimming process. Therefore, since $|x| \leqslant c$ by assumption, the result follows from Lemma 2.5 and the union bound. □

2.6 The approximators

Let $\mathcal{A} := \{\mathrm{trim}(\mathrm{cl}(f)) : f : \{0,1\}^n \to \{0,1\} \text{ is monotone}\}$. Functions in $\mathcal{A}$ will be called *approximators*. We define the *approximating* operations $\sqcup, \sqcap : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ as follows: for $f, g \in \mathcal{A}$, let

$$f \sqcup g := \mathrm{trim}(\mathrm{cl}(f \vee g)),$$
$$f \sqcap g := \mathrm{trim}(\mathrm{cl}(f \wedge g)).$$

We now observe that every input function is an approximator. Indeed, since every input $\lceil\{i\}\rceil$ is closed and trivially trimmed (Lemma 2.12), we have $\mathrm{trim}(\mathrm{cl}(\lceil\{i\}\rceil)) = \mathrm{trim}(\lceil\{i\}\rceil) = \lceil\{i\}\rceil$. Thus, $\lceil\{i\}\rceil \in \mathcal{A}$ for all $i \in [n]$. Therefore, we can replace each gate of a monotone $\{\vee, \wedge\}$-circuit C by its corresponding approximating gate, thus obtaining a $\{\sqcup, \sqcap\}$-circuit $C^{\mathcal{A}}$ computing an approximator.

The rationale for choosing this set of approximators is as follows. By letting approximators be the trimming of a closed function, we are able to plug the bound on the set of ℓ-minterms given by the robust sunflower lemma (Lemma 2.11) on Lemmas 2.15 and 2.16, since the trimming operation can only *reduce* the set of minterms. Moreover, since trimmings can only help to get a negative answer on the negative test distribution, we can safely apply Lemma 2.10 when bounding the errors of approximation.

2.7 The lower bound

In this section, we prove that the function f_{HR} requires monotone circuits of size $2^{\Omega(c)}$. By properly choosing c and k, this will imply the promised $\exp(\Omega(n^{1/2-o(1)}))$ lower bound for the Harnik-Raz function. First, we fix some parameters. Choose B as in Lemma 2.11. Let $T := 18B$. We also let

$$k := n^{1/2}, \qquad c := \frac{1}{T} \cdot (k/\log n) = \frac{k}{18B \cdot \log n}.$$

For simplicity, we assume these values are integers. Note that $c = \Theta(k/\log n) \ll k$.

Lemma 2.17 (Approximators make many errors)**.** *For every approximator $f \in \mathcal{A}$, we have*

$$\mathbb{P}[f(\boldsymbol{Y}) = 1] + \mathbb{P}[f(\boldsymbol{N}) = 0] \leqslant 3/2.$$

Proof. Let $f \in \mathcal{A}$. By definition, there exists a closed function h such that $f = \mathrm{trim}(h)$. Observe that $\mathcal{M}_\ell(f) \subseteq \mathcal{M}_\ell(h)$ for every $\ell \in [c]$. From Lemma 2.11, we get

$$|\mathcal{M}_\ell(h)| \leqslant (6Bc \log n)^\ell = (n/3k)^\ell.$$

Hence, applying Lemma 2.15, we obtain that, if $f \neq \mathbb{1}$, we have

$$\mathbb{P}[f(\boldsymbol{Y}) = 1] \leqslant \sum_{\ell=1}^{c/2} \left(\frac{k}{n}\right)^\ell |\mathcal{M}_\ell(h)| \leqslant \sum_{\ell=1}^{c/2} 3^{-\ell} \leqslant 1/2.$$

Therefore, for every $f \in \mathcal{A}$ we have $\mathbb{P}[f(\boldsymbol{Y}) = 1] + \mathbb{P}[f(\boldsymbol{N}) = 0] \leqslant 1 + 1/2 \leqslant 3/2$. □

Lemma 2.18 (C is well-approximated by $C^{\mathcal{A}}$)**.** *Let C be a monotone circuit. We have*

$$\mathbb{P}[C(\boldsymbol{Y}) = 1 \text{ and } C^{\mathcal{A}}(\boldsymbol{Y}) = 0] + \mathbb{P}[C(\boldsymbol{N}) = 0 \text{ and } C^{\mathcal{A}}(\boldsymbol{N}) = 1] \leqslant \mathrm{size}(C) \cdot 2^{-\Omega(c)}.$$

Proof. We begin by bounding the approximation errors under the distribution $\boldsymbol{Y}$. We will show that, for two approximators $f, g \in \mathcal{A}$, if $f \vee g$ accepts an input from $\boldsymbol{Y}$, then $f \sqcup g$ rejects that input with probability at most $2^{-\Omega(c)}$, and that the same holds for the approximation $f \sqcap g$.

First note that, if $f, g \in \mathcal{A}$, then all the minterms of both $f \vee g$ and $f \wedge g$ have Hamming weight at most c, since f and g are trimmed. Let now $h = \mathrm{cl}(f \vee g)$. We have $(f \sqcup g)(x) < (f \vee g)(x)$ only if $\mathrm{trim}(h)(x) < h(x)$. Since h is closed, we get from Lemma 2.11 that, for all $\ell \in [c]$, we have

$$|\mathcal{M}_\ell(h)| \leqslant (6Bc \log n)^\ell = (n/3k)^\ell.$$

We then obtain the following inequality by Lemma 2.16:

$$\mathbb{P}\left[(f \vee g)(\boldsymbol{Y}) = 1 \text{ and } (f \sqcup g)(\boldsymbol{Y}) = 0\right] \leqslant \sum_{\ell=c/2}^{c} \left(\frac{k}{n}\right)^\ell |\mathcal{M}_\ell(h)| \leqslant \sum_{\ell=c/2}^{c} 3^{-\ell} = 2^{-\Omega(c)}.$$

The same argument shows $\mathbb{P}\left[(f \wedge g)(\boldsymbol{Y}) = 1 \text{ and } (f \sqcap g)(\boldsymbol{Y}) = 0\right] = 2^{-\Omega(c)}$. Since there are $\mathrm{size}(C)$ gates in C, this implies that $\mathbb{P}[C(\boldsymbol{Y}) = 1 \text{ and } C^{\mathcal{A}}(\boldsymbol{Y}) = 0] \leqslant \mathrm{size}(C) \cdot 2^{-\Omega(c)}$.

To bound the approximation errors under $\boldsymbol{N}$, note that $(f \vee g)(x) = 0$ and $(f \sqcup g)(x) = 1$ only if $\mathrm{cl}(f \vee g)(x) \neq (f \vee g)(x)$, since trimming a Boolean function cannot decrease the probability that it rejects an input. Therefore, by Lemma 2.10 we obtain

$$\mathbb{P}\left[(f \vee g)(\boldsymbol{N}) = 0 \text{ and } (f \sqcup g)(\boldsymbol{N}) = 1\right] \leqslant n^{-c} = 2^{-\Omega(c)}.$$

The same argument shows $\mathbb{P}\left[(f \wedge g)(\boldsymbol{N}) = 0 \text{ and } (f \sqcap g)(\boldsymbol{N}) = 1\right] = 2^{-\Omega(c)}$. Once again, doing this approximation for every gate in C allows us to conclude $\mathbb{P}[C(\boldsymbol{N}) = 0 \text{ and } C^{\mathcal{A}}(\boldsymbol{N}) = 1] \leqslant \mathrm{size}(C) \cdot 2^{-\Omega(c)}$. This finishes the proof. □

Theorem 2.19. *Any monotone circuit computing f_{HR} has size $2^{\Omega(c)} = 2^{\Omega(n^{1/2}/\log n)}$.*

Proof. Let C be a monotone circuit computing f_{HR}. Since $k/2 - c\log_2 n = \Omega(k)$ and $k \ll n$, for large enough n we obtain from Lemmas 2.3 and 2.4 that

$$\mathbb{P}[f_{\mathrm{HR}}(\boldsymbol{Y}) = 1] + \mathbb{P}[f_{\mathrm{HR}}(\boldsymbol{N}) = 0] \geqslant 2 - (k-1)/n - 2^{-(k/2 - c\log_2 n)} \geqslant 9/5.$$

We then obtain from Lemmas 2.17 and 2.18:

$$\begin{aligned} 9/5 &\leqslant \mathbb{P}[f_{\mathrm{HR}}(\boldsymbol{Y}) = 1] + \mathbb{P}[f_{\mathrm{HR}}(\boldsymbol{N}) = 0] \\ &\leqslant \mathbb{P}[C(\boldsymbol{Y}) = 1 \text{ and } C^{\mathcal{A}}(\boldsymbol{Y}) = 0] + \mathbb{P}[C^{\mathcal{A}}(\boldsymbol{Y}) = 1] \\ &+ \mathbb{P}[C(\boldsymbol{N}) = 0 \text{ and } C^{\mathcal{A}}(\boldsymbol{N}) = 1] + \mathbb{P}[C^{\mathcal{A}}(\boldsymbol{N}) = 0] \\ &\leqslant 3/2 + \mathrm{size}(C) 2^{-\Omega(c)}. \end{aligned}$$

This implies $\mathrm{size}(C) = 2^{\Omega(c)}$. □

2.8 Are better lower bounds possible with robust sunflowers?

In this section, we allow some degree of imprecision for the sake of brevity and clarity, in order to highlight the main technical ideas of the proof.

A rough outline of how we just proved Theorem 2.19 is as follows. First, we noted that the minterms of f_{HR} are "well-spread". This is Lemma 2.5, which states that the probability that a fixed set $A \subseteq [n]$ is contained in a random minterm[4] of f_{HR} is at most $r^{|A|}$, where $r = k/n$. Moreover, we observed that f_{HR} outputs 0 with high probability in a p-biased distribution (Lemma 2.4), where $p = 1/2$.

In the rest of the proof, we roughly showed how this implies that DNFs of size approximately $s = c^{c/2}$ and width $w = c/2$ *cannot* approximate f_{HR} (Lemma 2.17).[5] We also observed that we can approximate the $\vee$ and $\wedge$ of width-w, size-s DNFs by another width-w, size-s DNF, bounding the error of approximation by $r^{c/2} \cdot c^{c/2}$. This was proved by noting that conjunctions of width $c/2$ accept a positive input with probability at most $r^{c/2}$, and there are at most $c^{c/2}$ of them. When $c \approx k \approx \sqrt{n}$, we have $(rc)^{c/2} = 2^{-\Omega(c)}$, and thus *we can* approximate circuits of size $2^{o(c)}$ with width-w, size-s DNFs (Lemma 2.18). This yields the lower bound.

There are two essential numerical components in the proof. First, the "spreadness rate" of the function f_{HR}. A simple counting argument can show that the upper bound of $(k/n)^{|A|}$ to the probability $\mathbb{P}[x_A \leqslant \boldsymbol{Y}]$ is nearly best possible when the support of $\boldsymbol{Y}$ is contained in $\{0,1\}^n_{=k}$ and $k = o(n)$. So this can hardly be improved with the choice of another Boolean function. Secondly, the bounds for the size and width of the DNF approximators come from the robust sunflower lemma (Theorem 1.3), which was used to employ the approximation method on p-biased distributions. Since the bound of Theorem 1.3 is essentially best possible as well, as observed in [3], we cannot hope to get better approximation bounds on a p-biased distribution from sunflowers. Therefore, there does not seem to be much room for getting better lower bounds for monotone circuits using the classical approximation method with sunflowers, if we use p-biased distributions. To get beyond $2^{\Omega(\sqrt{n})}$, another approach seems to be required.

3 Lower Bound for $\mathsf{Clique}_{k,n}$

Recall that the Boolean function $\mathsf{Clique}_{k,n} : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ receives a graph on n vertices as an input and outputs a 1 if this graph contains a clique on k vertices. In this section, we prove an $n^{\Omega(\delta^2 k)}$ lower bound on the monotone circuit size of $\mathsf{Clique}_{k,n}$ for $k \leqslant n^{(1/3)-\delta}$.

We note that the first superpolynomial lower bound for the monotone circuit complexity of $\mathsf{Clique}_{k,n}$ was given by Razborov [23], who proved a $n^{\Omega(k)}$ lower bound for $k \leqslant \log n$. Soon after, Alon and Boppana [1] proved a $n^{\Omega(\sqrt{k})}$ for $\mathsf{Clique}_{k,n}$ when $k \leqslant n^{2/3-o(1)}$. This exponential lower bound was better than Razborov's, as it could be applied to a larger range of k, but it was short of the obvious upper bound of $n^{O(k)}$. Our result finally closes that gap, by proving that the monotone complexity of $\mathsf{Clique}_{k,n}$ is $n^{\Theta(k)}$ even for large k.

As in Section 2, we will follow the approximation method. However, instead of using sunflowers as in [1, 23] or robust sunflowers as in [24], we introduce a notion of *clique-sunflowers* and employ it to bound the errors of approximation.

[4] Here, "random minterm" means an input from the distribution $\boldsymbol{Y}$, which correlates highly with the minterms of f_{HR}.

[5] Formally, our approximators have at most $O(c \log n)^\ell$ terms of width ℓ (Lemma 2.11), and no terms of width larger than $c/2$ (by trimming).

3.1 Notation for this section

In this section, we will often refer to graphs on n vertices and Boolean strings in $\{0,1\}^{\binom{n}{2}}$ interchangeably. For $A \subseteq [n]$, let K_A be the graph on n vertices with a clique on A and no other edges. When $|A| \leqslant 1$, the graph K_A is the empty graph with n vertices and 0 edges (corresponding to the Boolean string all of which $\binom{n}{2}$ entries are equal to 0.) The *size* of K_A is $|A|$. Let also $\lceil A \rceil : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ denote the indicator function of containing K_A, which satisfies

$$\lceil A \rceil(G) = 1 \iff K_A \subseteq G.$$

Functions of the forms $\lceil A \rceil$ are called *clique-indicators.* Moreover, if $|A| = \ell$, we say that $\lceil A \rceil$ is a clique-indicator of *size* equal to ℓ. When $|A| \leqslant 1$, the function $\lceil A \rceil$ is the constant function $\mathbb{1}$.

For $p \in (0,1)$, we denote by $\boldsymbol{G}_{n,p}$ the Erdős-Rényi random graph, a random graph on n vertices in which each edge appears independently with probability p.

Let $f : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ be monotone and suppose $\ell \in \{1, \dots, \delta k\}$. We define

$$\mathcal{M}_\ell(f) := \{A \in \tbinom{[n]}{\ell} : f(K_A) = 1 \text{ and } f(K_{A \setminus \{a\}}) = 0 \text{ for all } a \in A\}.$$

Elements of $\mathcal{M}_\ell(f)$ are called *ℓ-clique-minterms* of f.

3.2 Clique-sunflowers

Here we introduce the notion of *clique-sunflowers*, which is analogous to that of robust sunflowers for "clique-shaped" set systems.

Definition 3.1 (Clique-sunflowers)**.** *Let $\varepsilon, p \in (0,1)$. Let $\mathcal{S}$ be a family of subsets of $[n]$ and let $Y := \bigcap \mathcal{S}$. The family $\mathcal{S}$ is called a* (p,ε)-clique-sunflower *if*

$$\mathbb{P}\left[\exists A \in S : K_A \subseteq \boldsymbol{G}_{n,p} \cup K_Y\right] > 1 - \varepsilon.$$

Equivalently, the family $\mathcal{S}$ is a clique-sunflower if the family $\{K_A : A \in \mathcal{S}\} \subseteq \binom{[n]}{2}$ is a (p,ε)-robust sunflower, since $K_A \cap K_B = K_{A \cap B}$.

Though clique-sunflowers may seem similar to regular sunflowers, the importance of this definition is that it allows us to explore the "clique-shaped" structure of the sets of the family, and thus obtain an asymptotically better upper bound on the size of sets that do not contain a clique-sunflower.

Lemma 3.2 (Clique-sunflower lemma)**.** *Let $\varepsilon < e^{-1/2}$ and let $\mathcal{S} \subseteq \binom{[n]}{\ell}$. If the family $\mathcal{S}$ satisfies $|\mathcal{S}| > \ell!(2\ln(1/\varepsilon))^\ell (1/p)^{\binom{\ell}{2}}$, then $\mathcal{S}$ contains a (p,ε)-clique-sunflower.*

Observe that, whereas the bounds for "standard" robust sunflowers (Theorems 1.2 and 1.3) would give us an exponent of $\binom{\ell}{2}$ on the $\log(1/\varepsilon)$ factor, Lemma 3.2 give us only an ℓ at the exponent. As we shall see, this is asymptotically better for our choice of parameters.

We defer the proof of Lemma 3.2 to Section 3.8. The proof is based on an application of Janson's inequality [13], as in the original robust sunflower lemma of [24] (Theorem 1.2).

3.3 Test distributions

We now define the positive and negative test distributions. First, we fix some parameters that will be used throughout the proof. Fix $\delta \in (0, 1/3)$. Let

$$k = n^{1/3-\delta} \quad \text{and} \quad p := n^{-2/(k-1)}. \tag{2}$$

For simplicity, we will assume from now on that δk and $\delta k/2$ are integers.

Remark 3.3 (Parameters are now fixed)**.** *From now on until the end of Section 3.7, the symbols p, δ and k refer to fixed parameters, and will always unambiguously refer to the values just fixed. This will only change in Section 3.8, which is independent of the proof of the lower bound for $\mathsf{Clique}_{k,n}$, and in which we will permit ourselves to reuse some of these symbols for other purposes. This means that, whenever p, δ and k appear in the following discussion, the reader must bear in mind that $p = n^{-2/(k-1)}$, δ is a fixed number inside $(0, 1/3)$ and k is fixed to be $k = n^{1/3-\delta}$.*

We observe that the probability that $\boldsymbol{G}_{n,p}$ has a k-clique is bounded away from 1.

Lemma 3.4. *We have $\mathbb{P}[\, \boldsymbol{G}_{n,p}$ contains a k-clique $] \leqslant 3/4$.*

Proof. There are $\binom{n}{k} \leqslant (en/k)^k$ potential k-cliques, each present in $\boldsymbol{G}_{n,p}$ with probability $p^{\binom{k}{2}} = n^{-k}$. By a union bound, we have $\mathbb{P}[\, \boldsymbol{G}_{n,p}$ contains a k-clique $] \leqslant (e/k)^k \leqslant (e/3)^3 \leqslant 3/4$. □

Definition 3.5. *Let $\boldsymbol{Y}$ be the uniform random graph chosen from all possible K_A, where $|A| = k$. In other words, the distribution $\boldsymbol{Y}$ samples a random minterm of $\mathsf{Clique}_{k,n}$. We call $\boldsymbol{Y}$ the* positive test distribution*. Let also $\boldsymbol{N} := \boldsymbol{G}_{n,p}$. We call $\boldsymbol{N}$ the* negative test distribution*.*

From Lemma 3.4, we easily obtain the following corollary.

Corollary 3.6. *We have $\mathbb{P}[\mathsf{Clique}_{k,n}(\boldsymbol{Y}) = 1] + \mathbb{P}[\mathsf{Clique}_{k,n}(\boldsymbol{N}) = 0] \geqslant 5/4$.*

We now prove an analogous result to that of Lemma 2.5, which shows that the positive distribution $\boldsymbol{Y}$ is unlikely to contain a large fixed clique.

Lemma 3.7. *For every $\ell \leqslant k$ and $A \subseteq [n]$ such that $|A| = \ell$, we have*

$$\mathbb{P}[K_A \leqslant \boldsymbol{Y}] \leqslant (k/n)^\ell .$$

Proof. The distribution $\boldsymbol{Y}$ samples a set $\boldsymbol{B}$ uniformly at random from $\binom{[n]}{k}$ and returns the graph $K_{\boldsymbol{B}}$. Note that $K_A \subseteq K_{\boldsymbol{B}}$ if and only if $A \subseteq \boldsymbol{B}$. We have

$$\mathbb{P}[K_A \leqslant \boldsymbol{Y}] = \mathbb{P}[A \subseteq \boldsymbol{B}] = \frac{\binom{n-k}{k-\ell}}{\binom{n}{k}} \leqslant \left(\frac{k}{n}\right)^\ell .$$ □

3.4 A closure operator

As in Section 2.4, we define here a closure operator in the lattice of monotone Boolean functions. We will again prove that the closure of a function will be a good approximation for it on the negative test distribution. However, unlike Section 2.4, instead of bounding the set of minterms, we will bound the set of "clique-shaped" minterms, as we shall see. Finally, we will observe that input functions are also closed. Henceforth, we fix the error parameter

$$\varepsilon := n^{-k}. \tag{3}$$

Definition 3.8 (Closed functions)**.** *We say that* $f \in \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ *is* closed *if, for every* $A \subseteq [n]$ *such that* $|A| \in \{2, \ldots, \delta k\}$*, we have*

$$\mathbb{P}[\ f(\boldsymbol{N} \vee K_A) = 1\ ] > 1 - \varepsilon \implies f(K_A) = 1.$$

Remark 3.9 (On the parametrization of closedness)**.** *Similarly to the Harnik-Raz case (see Remark 2.7), the definition of a* closed *function depends on three parameters: the probability* p*, which controls the distribution* $\boldsymbol{N}$ *(as discussed in Definition 3.5), the parameter* ε*, defined in (3), and the parameter* k*. Since all of these three parameters are fixed until the end of Section 3.7 (see Remark 3.3), and no other reference to closed functions will be made after that, it is safe to omit them without risk of confusion. Therefore, we will henceforth say that some function is* closed *without any further specification about the parameters. However, the reader must bear in mind that, whenever a function is said to be* closed*, the* fixed *parameters* p, ε *and* k *are in view.*

Remark 3.10 (Definitions of closedness compared)**.** *Definition 3.11 bears great resemblance to Definition 2.8, which also talks about a notion of* closed monotone functions *in the context of lower bounds for the function of Harnik and Raz. Apart from the different parametrizations, the main difference between those two definitions is that, whereas Definition 2.8 looks into* all *inputs of Hamming weight at most* c*, here we only care about* clique-shaped *inputs of size at most* δk*.*

As before, we can define the closure of a monotone Boolean function f.

Definition 3.11 (Closure operator)**.** *Let* f *be a monotone Boolean function. We denote by* $\mathrm{cl}(f)$ *the unique minimal closed monotone Boolean function such that* $f \leqslant \mathrm{cl}(f)$*.*

Remark 3.12 (On closure)**.** *We note again that* $\mathrm{cl}(f)$ *is well-defined (the same arguments of Remark 2.9 apply here) and remark that its definition also depends on the parameters* p, ε *and* k *(see Remark 3.9), which are fixed throughout the proof, and therefore can be safely omitted.*

Lemma 3.13 (Approximation by closure)**.** *For every monotone* $f : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$*, we have*

$$\mathbb{P}\left[f(\boldsymbol{N}) = 0 \text{ and } \mathrm{cl}(f)(\boldsymbol{N}) = 1\right] \leqslant n^{-(2/3)k}.$$

Proof. We repeat the same argument as that of Lemma 2.10. Since there are at most $n^{\delta k}$ graphs K_A such that $|A| \leqslant \delta k$ and $\varepsilon = n^{-k}$, the final bound then becomes $n^{-k} \cdot n^{\delta k} \leqslant n^{-(2/3)k}$. □

By employing the clique-sunflower lemma (Lemma 3.2), we are able to bound the set of ℓ-clique-minterms of closed monotone functions.

Lemma 3.14 (Closed functions have few minterms)**.** *If a monotone function* $f : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ *is closed, then, for all* $\ell \in \{2, \ldots, \delta k\}$*, we have*

$$|\mathcal{M}_\ell(f)| \leqslant n^{2\ell/3}.$$

Proof. Recall that $p = n^{-2/(k-1)}$ and $\varepsilon = n^{-k}$ (see (2) and (3)). Applying the same strategy of Lemma 2.11, replacing the application of Theorem 1.3 (robust sunflower theorem) by Lemma 3.2 (clique-sunflower lemma), we obtain

$$\begin{aligned} |\mathcal{M}_\ell(f)| &\leqslant \ell!(2\log(1/\varepsilon))^\ell (1/p)^{\binom{\ell}{2}} \leqslant (2\ell k \log n)^\ell \cdot p^{-\binom{\ell}{2}} \\ &\leqslant (2\delta k^2 \log n)^\ell \cdot n^{2\binom{\ell}{2}/(k-1)} \leqslant (n^{2/3-2\delta} \log n)^\ell \cdot n^{\delta\ell} \leqslant n^{2\ell/3}. \end{aligned}$$

□

Lemma 3.15 (Input functions are closed)**.** *Let $i, j \in [n]$ be such that $i \neq j$. For large enough n, the Boolean function $\lceil\{i,j\}\rceil$ is closed.*

Proof. Fix $i, j \in [n]$ such that $i \neq j$. Let $A \subseteq [n]$ be such that $|A| \leqslant \delta k$ and suppose that $\lceil\{i,j\}\rceil(K_A) = 0$. Note that $\lceil\{i,j\}\rceil(K_A) = 0$ is equivalent to $\{i,j\} \not\subseteq A$. This implies that $\{i,j\}$ is an edge of $\boldsymbol{N} \cup K_A$ if and only if $\{i,j\}$ is an edge of $\boldsymbol{N}$. Therefore, we have

$$\begin{aligned}\mathbb{P}[\lceil\{i,j\}\rceil(\boldsymbol{N} \vee K_A) = 1] &= \mathbb{P}[\lceil\{i,j\}\rceil(\boldsymbol{N}) = 1] \\ &= \mathbb{P}[\{i,j\} \text{ is an edge of } \boldsymbol{G}_{n,p}] \\ &= n^{-2/(k-1)},\end{aligned}$$

since $\boldsymbol{N} = \boldsymbol{G}_{n,p}$ and $p = n^{-2/(k-1)}$ (see (2), Remark 3.3 and Definiton 3.5). It now suffices to show that, for large enough n, we have $p \leqslant 1 - \varepsilon = 1 - n^{-k}$ (recall from (3) that $\varepsilon = n^{-k}$).

For convenience, let $\alpha = 1/3 - \delta$. Note that $k = n^{\alpha}$. For large enough n, we have

$$\frac{2 \cdot \log n}{n^{\alpha} - 1} \geqslant n^{-n^{\alpha}} + n^{-2n^{\alpha}}.$$

Using the inequality $\log(1 - x) \geqslant -x - x^2$ for $x \in [0, 1/2]$, we get

$$\frac{2 \cdot \log n}{k - 1} = \frac{2 \cdot \log n}{n^{\alpha} - 1} \geqslant n^{-n^{\alpha}} + n^{-2n^{\alpha}} \geqslant -\log(1 - n^{-n^{\alpha}}) = -\log(1 - n^{-k}).$$

Therefore, we have

$$n^{-2/(k-1)} \leqslant 1 - n^{-k},$$

and we conclude that $\lceil\{i,j\}\rceil$ is closed. □

3.5 Trimmed monotone functions

In this section, we define again a trimming operation for Boolean functions and prove analogous bounds to that of Section 2.5.

Definition 3.16 (Clique-shaped and trimmed functions)**.** *We say that a function $f : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ is* clique-shaped *if, for every minterm x of f, there exists $A \subseteq [n]$ such that $x = K_A$. Moreover, we say that f is* trimmed *if f is clique-shaped and all the clique-minterms of f have size at most $\delta k/2$. For a clique-shaped function f, we define the trimming operation* $\mathrm{trim}(f)$ *as follows:*

$$\mathrm{trim}(f) := \bigvee_{\ell=1}^{\delta k/2} \bigvee_{A \in \mathcal{M}_\ell(f)} \lceil A \rceil.$$

That is, the trim *operation takes out from f all the clique-indicators of size larger than $\delta k/2$, yielding a trimmed function.*

Remark 3.17 (Parametrization of $\mathrm{trim}(\cdot)$ and other remarks)**.** *Analogously to the Harnik-Raz case (see Remark 2.14), the definition of trimmed functions depends on the choice of the parameters δ and k. As these parameters are fixed (see Remark 3.3), the operator* $\mathrm{trim}(\cdot)$ *is well-defined. Moreover, if all clique-minterms of f have size larger than $\delta k/2$ (i.e., if $\mathcal{M}_\ell(f) = \emptyset$ for all $\ell \in [\delta k/2]$), then* $\mathrm{trim}(f)$ *is the constant function that outputs 0. Finally, if f is the constant function $\mathbb{1}$, then* $\mathrm{trim}(f) = \mathbb{1}$*, because $\mathbb{1}$ contains a clique-minterm of size equal to 1 (a clique containing one vertex and no edges).*

Imitating the proofs of Lemmas 2.15 and 2.16, replacing Lemma 2.5 by Lemma 3.7, we may now obtain the following lemmas.

Lemma 3.18 (Trimmed functions are inaccurate in the positive distribution)**.** *If a monotone function $f : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ is a trimmed clique-shaped function such that $f \neq \mathbb{1}$, then*

$$\mathbb{P}\left[f(\boldsymbol{Y}) = 1\right] \leqslant \sum_{\ell=2}^{\delta k/2} \left(\frac{k}{n}\right)^{\ell} \left|\mathcal{M}_\ell(f)\right|.$$

Lemma 3.19 (Approximation by trimming)**.** *Let $f : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ be a clique-shaped monotone function, all of whose clique-minterms have size at most δk. We have*

$$\mathbb{P}\left[f(\boldsymbol{Y}) = 1 \text{ and } \operatorname{trim}(f)(\boldsymbol{Y}) = 0\right] \leqslant \sum_{\ell=\delta k/2}^{\delta k} \left(\frac{k}{n}\right)^{\ell} \left|\mathcal{M}_\ell(f)\right|.$$

3.6 Approximators

Similarly as in Section 2.6, we will consider a set of *approximators* $\mathcal{A}$. Let

$$\mathcal{A} := \{\operatorname{trim}(\operatorname{cl}(f)) : f \in \{0,1\}^{\binom{n}{2}} \to \{0,1\} \text{ is monotone and clique-shaped}\}.$$

Functions in $\mathcal{A}$ are called *approximators*. Note that every function in $\mathcal{A}$ is clique-shaped and is the trimming of a closed function. Moreover, observe that every edge-indicator $\lceil\{u,v\}\rceil$ belongs to $\mathcal{A}$, since every edge-indicator is closed by Lemma 3.15.

Let $f, g \in \mathcal{A}$ such that $f = \bigvee_{i=1}^{t} \lceil A_i \rceil$ and $g = \bigvee_{j=1}^{s} \lceil B_j \rceil$. We define $\bigwedge(f,g) := \bigvee_{i=1}^{t} \bigvee_{j=1}^{s} \lceil A_i \cup B_j \rceil$. We also define operations $\sqcup, \sqcap : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ as follows:

$$f \sqcup g := \operatorname{trim}(\operatorname{cl}(f \vee g)),$$
$$f \sqcap g := \operatorname{trim}\left(\operatorname{cl}\left(\bigwedge(f,g)\right)\right).$$

It's easy to see that, if $f, g \in \mathcal{A}$, then $f \sqcup g \in \mathcal{A}$. To see that $f \sqcap g \in \mathcal{A}$, note that $\bigwedge(f,g)$ is also a monotone clique-shaped function.

Remark 3.20 (Reason for definition of $\sqcap$)**.** *The reason for defining $\sqcap$ in that way is as follows. First observe that $f \wedge g = \bigvee_{i=1}^{t} \bigvee_{j=1}^{s} (\lceil A_i \rceil \wedge \lceil B_j \rceil)$. We simply replace each $\lceil A_i \rceil \cap \lceil B_j \rceil$ with $\lceil A_i \cup B_j \rceil$, thus obtaining $f \sqcap g$. In general, since $\lceil A_i \cup B_j \rceil$ is a larger conjunction than $\lceil A_i \rceil \wedge \lceil B_j \rceil$, we have $\bigwedge(f,g) \leqslant f \wedge g$. However, note that, for every $A \subseteq [n]$, we have $\bigwedge(f,g)(K_A) = (f \wedge g)(K_A)$. Thus, the transformation from $f \wedge g$ to $\bigwedge(f,g)$ incurs no mistakes in the positive distribution $\boldsymbol{Y}$.*

If C is a monotone $\{\vee, \wedge\}$-circuit, let $C^{\mathcal{A}}$ be the corresponding $\{\sqcup, \sqcap\}$-circuit, obtained by replacing each $\vee$-gate by a $\sqcup$-gate, and each $\wedge$-gate by an $\sqcap$-gate. Note that $C^{\mathcal{A}}$ computes an approximator.

3.7 The lower bound

In this section we obtain the lower bound for the clique function. Recall that $k = n^{1/3-\delta}$. We will prove that the monotone complexity of $\mathsf{Clique}_{k,n}$ is $n^{\Omega(\delta^2 k)}$.

Repeating the same arguments of Lemmas 2.17 and 2.18, we obtain the following analogous lemmas.

Lemma 3.21 (Approximators make many errors)**.** *For every $f \in \mathcal{A}$, we have*

$$\mathbb{P}[f(\boldsymbol{Y}) = 1] + \mathbb{P}[f(\boldsymbol{N}) = 0] \leqslant 1 + o(1).$$

Proof. Let $f \in \mathcal{A}$. By definition, there exists a closed function h such that $f = \mathrm{trim}(h)$. Observe that $\mathcal{M}_\ell(f) \subseteq \mathcal{M}_\ell(h)$ for every $\ell \in \{2, \ldots, \delta k/2\}$. By Lemmas 3.14 and 3.18, if $f \in \mathcal{A}$ is such that $f \neq \mathbb{1}$, then

$$\mathbb{P}[f(\boldsymbol{Y}) = 1] \leqslant \sum_{\ell=2}^{\delta k/2} \left(\frac{k}{n}\right)^\ell |\mathcal{M}_\ell(h)| \leqslant \sum_{\ell=2}^{\delta k/2} \left(\frac{k}{n^{1/3}}\right)^\ell \leqslant \sum_{\ell=2}^{\delta k/2} n^{-\delta\ell} = o(1).$$

Therefore, for every $f \in \mathcal{A}$ we have $\mathbb{P}[f(\boldsymbol{Y}) = 1] + \mathbb{P}[f(\boldsymbol{N}) = 0] \leqslant 1 + o(1)$. □

Lemma 3.22 (C is well-approximated by $C^{\mathcal{A}}$)**.** *Let C be a monotone circuit. We have*

$$\mathbb{P}[C(\boldsymbol{Y}) = 1 \text{ and } C^{\mathcal{A}}(\boldsymbol{Y}) = 0] + \mathbb{P}[C(\boldsymbol{N}) = 0 \text{ and } C^{\mathcal{A}}(\boldsymbol{N}) = 1] \leqslant \mathrm{size}(C) \cdot O(n^{-\delta^2 k/2}).$$

Proof. To bound the approximation errors under the distribution $\boldsymbol{Y}$, first note that, if $f, g \in \mathcal{A}$, then all the clique-minterms of both $f \vee g$ and $f \wedge g$ have size at most δk. Moreover, if $(f \vee g)(x) = 1$ but $(f \sqcup g)(x) = 0$, then $\mathrm{trim}(\mathrm{cl}(f \vee g)(x)) \neq \mathrm{cl}(f \vee g)(x)$. Therefore, we obtain by Lemmas 3.14 and 3.19 that, for $f, g \in \mathcal{A}$, we have

$$\begin{aligned}\mathbb{P}\left[(f \vee g)(\boldsymbol{Y}) = 1 \text{ and } (f \sqcup g)(\boldsymbol{Y}) = 0\right] &\leqslant \sum_{\ell=\delta k/2}^{\delta k} \left(\frac{k}{n}\right)^\ell |\mathcal{M}_\ell(\mathrm{cl}(f \vee g))| \\ &\leqslant \sum_{\ell=\delta k/2}^{\delta k} n^{-\delta\ell} = O(n^{-\delta^2 k/2}).\end{aligned}$$

As observed in Remark 3.20, we have $\bigwedge(f, g)(\boldsymbol{Y}) = (f \wedge g)(\boldsymbol{Y})$. Thus, once again, the only approximation mistakes incurred by changing a $\wedge$-gate for a $\sqcap$-gate comes from the trimming operation. Again, we conclude

$$\mathbb{P}\left[(f \wedge g)(\boldsymbol{Y}) = 1 \text{ and } (f \sqcap g)(\boldsymbol{Y}) = 0\right] = O(n^{-\delta^2 k/2}),$$

which implies

$$\mathbb{P}[C(\boldsymbol{Y}) = 1 \text{ and } C^{\mathcal{A}}(\boldsymbol{Y}) = 0] \leqslant \mathrm{size}(C) \cdot O(n^{-\delta^2 k/2}).$$

Similarly, to bound the approximation errors under $\boldsymbol{N}$, note that $(f \vee g)(x) = 0$ and $(f \sqcup g)(x) = 1$ only if $\mathrm{cl}(f \vee g)(x) \neq (f \vee g)(x)$. Therefore, we obtain by Lemma 3.13 that, for $f, g \in \mathcal{A}$, we have

$$\mathbb{P}\left[(f \vee g)(\boldsymbol{N}) = 0 \text{ and } (f \sqcup g)(\boldsymbol{N}) = 1\right] \leqslant n^{-(2/3)k}.$$

Moreover, note that $\bigwedge(f,g) \leqslant f \wedge g$. As $f \sqcap g = \mathrm{trim}(\mathrm{cl}(\bigwedge(f,g)))$, we obtain that $(f \wedge g)(x) = 0$ and $(f \sqcap g)(x) = 1$ only if $\mathrm{cl}(\bigwedge(f,g))(x) > \bigwedge(f,g)(x)$. Therefore, we also have

$$\mathbb{P}\left[(f \wedge g)(\boldsymbol{N}) = 0 \text{ and } (f \sqcap g)(\boldsymbol{N}) = 1\right] \leqslant n^{-(2/3)k}.$$

By the union bound, we conclude:

$$\mathbb{P}[C(\boldsymbol{N}) = 0 \text{ and } C^{\mathcal{A}}(\boldsymbol{N}) = 1] \leqslant \mathrm{size}(C) \cdot n^{-(2/3)k}.$$

This finishes the proof. □

We now prove the lower bound for the clique function.

Theorem 3.23. *Let $\delta \in (0, 1/3)$ and $k = n^{1/3-\delta}$. The monotone circuit complexity of $\mathsf{Clique}_{k,n}$ is $\Omega(n^{\delta^2 k/2})$.*

Proof. Let C be a monotone circuit computing $\mathsf{Clique}_{k,n}$. For large n, we obtain from Corollary 3.6 and Lemmas 3.21 and 3.22

$$\begin{aligned} 5/4 &\leqslant \mathbb{P}[\mathsf{Clique}_{k,n}(\boldsymbol{Y})] + \mathbb{P}[\mathsf{Clique}_{k,n}(\boldsymbol{N})] \\ &\leqslant \mathbb{P}[C(\boldsymbol{Y}) = 1 \text{ and } C^{\mathcal{A}}(\boldsymbol{Y}) = 0] + \mathbb{P}[C^{\mathcal{A}}(\boldsymbol{Y}) = 1] \\ &\quad + \mathbb{P}[C(\boldsymbol{N}) = 0 \text{ and } C^{\mathcal{A}}(\boldsymbol{N}) = 1] + \mathbb{P}[C^{\mathcal{A}}(\boldsymbol{N}) = 1] \\ &\leqslant 1 + o(1) + \mathrm{size}(C) \cdot O(n^{-\delta^2 k/2}). \end{aligned}$$

This implies $\mathrm{size}(C) = \Omega(n^{\delta^2 k/2})$. □

3.8 Proof of Lemma 3.2 (Clique-sunflowers)

In this section, we give the proof of Lemma 3.2. The proof is essentially the same as the one given by Rossman for Theorem 1.2 in [24]. We will rely on an inequality due to Janson [13] (see also Theorem 2.18 in [14]).

Lemma 3.24 (Janson's inequality [13])**.** *Let $\mathcal{F}$ be a nonempty hypergraph on $[n]$ and let $\boldsymbol{W} \subseteq_p [n]$. Define μ and Δ in the following way:*

$$\begin{aligned} \mu &:= \sum_{F \in \mathcal{F}} \mathbb{P}[F \subseteq \boldsymbol{W}], \\ \Delta &:= \sum_{\substack{F,H \in \mathcal{F} \\ F \cap H \neq \emptyset}} \mathbb{P}[F \cup H \subseteq \boldsymbol{W}]. \end{aligned}$$

Then we have

$$\mathbb{P}[\forall F \in \mathcal{F} : F \not\subseteq \boldsymbol{W}] \leqslant \exp\{-\mu^2/\Delta\}.$$

The following estimates appear in an unpublished note due to Rossman [25], and a slightly weaker form appears implicitly in [24]. We reproduce the proof for completeness.

Lemma 3.25 (Lemma 8 of [25]). *Let $s_0(t), s_1(t), \dots$ be the sequence of polynomials defined by*

$$s_0(t) := 1 \quad \text{and} \quad s_\ell(t) := t \sum_{j=0}^{\ell-1} \binom{\ell}{j} s_j(t).$$

For all $t > 0$, we have $s_\ell(t) \leqslant \ell!(t + 1/2)^\ell$.

Proof. We first prove by induction on ℓ that $s_\ell(t) \leqslant \ell!(\log(1/t + 1))^{-\ell}$, as follows:

$$\begin{aligned}
s_\ell(t) = t \sum_{j=0}^{\ell-1} \binom{\ell}{j} s_j(t) &\leqslant t \sum_{j=0}^{\ell-1} \binom{\ell}{j} j!(\log(1/t+1))^{-j} \\
&= t\ell!(\log(1/t+1))^{-\ell} \sum_{j=0}^{\ell-1} \frac{(\log(1/t+1))^{\ell-j}}{(\ell-j)!} \\
&\leqslant t\ell!(\log(1/t+1))^{-\ell} \left(-1 + \sum_{j=0}^{\infty} \frac{(\log(1/t+1))^j}{j!} \right) \\
&= t\ell!(\log(1/t+1))^{-\ell}(-1 + \exp(\log(1/t+1))) \\
&= \ell!(\log(1/t+1))^{-\ell}.
\end{aligned}$$

To conclude the proof, we apply the inequality $1/\log(1/t + 1) < t + 1/2$ for all $t > 0$. □

We will also need the following auxiliary definition.

Definition 3.26. *Let $\varepsilon, p, q \in (0, 1)$. Let $\boldsymbol{U}_{n,q} \subseteq [n]$ be a q-random subset of $[n]$ independent of $\boldsymbol{G}_{n,p}$. Let $\mathcal{S}$ be a family of subsets of $[n]$ and let $B := \bigcap \mathcal{S}$. The family $\mathcal{S}$ is called a* (p, q, ε)-clique-sunflower *if*

$$\mathbb{P}\left[\exists A \in \mathcal{S} : K_A \subseteq \boldsymbol{G}_{n,p} \cup K_B \text{ and } A \subseteq \boldsymbol{U}_{n,q} \cup B\right] > 1 - \varepsilon.$$

The set B is called core.

Clearly, a $(p, 1, \varepsilon)$-clique sunflower is a (p, ε)-clique sunflower. By taking $q = 1$ in the following lemma, and observing that $s_\ell(\log(1/\varepsilon)) \leqslant \log(1/\varepsilon) + 1/2 \leqslant 2\log(1/\varepsilon)$ for $\varepsilon \leqslant e^{-1/2}$, we obtain Lemma 3.2.

Lemma 3.27. *For all $\ell \in \{1, \dots, n\}$ and $S \subseteq \binom{[n]}{\ell}$, if $|\mathcal{S}| > s_\ell(\log(1/\varepsilon)) \cdot (1/q)^\ell (1/p)^{\binom{\ell}{2}}$, then $\mathcal{S}$ contains a (p, q, ε)-clique sunflower.*

Proof. By induction on ℓ. In the base case $\ell = 1$, we have by independence that

$$\begin{aligned}
\mathbb{P}[\forall A \in \mathcal{S} : K_A \nsubseteq \boldsymbol{G}_{n,p} \text{ or } A \nsubseteq \boldsymbol{U}_{n,q}] &= \mathbb{P}[\forall A \in \mathcal{S} : A \nsubseteq \boldsymbol{U}_{n,q}] \\
&= \prod_{A \in S} \mathbb{P}[A \nsubseteq \boldsymbol{U}_{n,q}] \\
&= (1-q)^{|S|} < (1-q)^{\ln(1/\varepsilon)/q} \leqslant e^{-\ln(1/\varepsilon)} = \varepsilon.
\end{aligned}$$

Thus $\mathcal{S}$ is itself a (p, q, ε)-clique sunflower.

Let now $\ell \geqslant 2$ and assume that the claim holds for $t \in \{1, \dots, \ell - 1\}$. For convenience, let

$$c_j := s_j(\log(1/\varepsilon)),$$

for every $j \in \{0, 1, \dots, \ell - 1\}$.

Case 1. There exists $j \in \{1, \dots, \ell - 1\}$ and $B \in \binom{[n]}{j}$ such that

$$|\{A \in \mathcal{S} : B \subseteq A\}| \geqslant c_{\ell-j}(1/qp^j)^{\ell-j}(1/p)^{\binom{\ell-j}{2}}.$$

Let $\mathcal{T} = \{A \setminus B : A \in \mathcal{S} \text{ such that } B \subseteq A\} \subseteq \binom{[n]}{\ell-j}$. By the induction hypothesis, there exists a (p, qp^j, ε)-clique sunflower $\mathcal{T}' \subseteq \mathcal{T}$ with core a D satisfying $D \in \binom{[n]\setminus B}{<\ell-j}$. We will now show that $\mathcal{S}' := \{B \cup C : C \in \mathcal{T}'\} \subseteq \mathcal{S}$ is a (p, q, ε)-clique sunflower contained in $\mathcal{S}$ with core $B \cup D$. We have

$$\begin{aligned}
&\mathbb{P}[\forall A \in \mathcal{S}' : K_A \nsubseteq \boldsymbol{G}_{n,p} \cup K_{B\cup D} \text{ or } A \nsubseteq \boldsymbol{U}_{n,q} \cup B \cup D] \\
&\quad = \mathbb{P}[\forall C \in \mathcal{T}' : K_{B\cup C} \nsubseteq \boldsymbol{G}_{n,p} \cup K_{B\cup D} \text{ or } B \cup C \nsubseteq \boldsymbol{U}_{n,q} \cup B \cup D] \\
&\quad = \mathbb{P}[\forall C \in \mathcal{T}' : K_{B\cup C} \nsubseteq \boldsymbol{G}_{n,p} \cup K_{B\cup D} \text{ or } C \nsubseteq \boldsymbol{U}_{n,q} \cup D] \\
&\quad = \mathbb{P}[\forall C \in \mathcal{T}' : K_C \nsubseteq \boldsymbol{G}_{n,p} \cup K_D \text{ or } \\
&\qquad\qquad C \nsubseteq \big\{v \in \boldsymbol{U}_{n,q} : \{v, w\} \in E(\boldsymbol{G}_{n,p}) \text{ for all } w \in B\big\} \cup D] \\
&\quad \leqslant \mathbb{P}[\forall C \in \mathcal{T}' : K_C \nsubseteq \boldsymbol{G}_{n,p} \cup K_D \text{ or } C \nsubseteq \boldsymbol{U}_{n,qp^j} \cup D] \\
&\quad < \varepsilon.
\end{aligned}$$

Therefore, $\mathcal{S}'$ is a (p, q, ε)-clique sunflower contained in $\mathcal{S}$.

Case 2. For all $j \in \{1, \dots, \ell - 1\}$ and $B \in \binom{[n]}{j}$, we have

$$|\{A \in \mathcal{S} : B \subseteq A\}| \leqslant c_{\ell-j}(1/qp^j)^{\ell-j}(1/p)^{\binom{\ell-j}{2}}.$$

In this case, we show that the bound of the lemma holds with $B = \emptyset$. Let

$$\begin{aligned}
\mu &:= |\mathcal{S}|\, q^\ell p^{\binom{\ell}{2}} > c_\ell, \\
\overline{\Delta} &:= \sum_{j=1}^{\ell-1} \sum_{(A,A') \in \mathcal{S}^2 \,:\, |A\cap A'| = j} q^{2\ell-j} p^{2\binom{\ell}{2} - \binom{j}{2}}.
\end{aligned}$$

Note that $\overline{\Delta}$ excludes $j = \ell$ from the sum, which corresponds to pairs (A, A') such that $A = A'$, in which case the summand becomes μ. In other words, the number Δ of Janson's inequality (Lemma 3.24) satisfies $\Delta = \mu + \overline{\Delta}$. Janson's Inequality now gives the following bound:

$$\mathbb{P}[\forall A \in \mathcal{S} : K_A \nsubseteq \boldsymbol{G}_{n,p} \text{ or } A \nsubseteq \boldsymbol{U}_{n,q}] \leqslant \exp\left(-\frac{\mu^2}{\mu + \overline{\Delta}}\right). \tag{4}$$

We bound $\overline{\Delta}$ as follows:

$$\begin{aligned}
\overline{\Delta} &\leqslant \sum_{j=1}^{\ell-1} q^{2\ell-j} p^{2\binom{\ell}{2}-\binom{j}{2}} \sum_{B\in\binom{[n]}{j}} |\{A \in S : B \subseteq A\}|^2 \\
&\leqslant \sum_{j=1}^{\ell-1} q^{2\ell-j} p^{2\binom{\ell}{2}-\binom{j}{2}} \sum_{B\in\binom{[n]}{j}} |\{A \in S : B \subseteq A\}| \cdot c_{\ell-j}(1/q)^{\ell-j}(1/p)^{\binom{\ell-j}{2}} \\
&\leqslant q^{\ell} p^{\binom{\ell}{2}} \sum_{j=1}^{\ell-1} c_{\ell-j} \sum_{B\in\binom{[n]}{j}} |\{A \in S : B \subseteq A\}| \\
&= q^{\ell} p^{\binom{\ell}{2}} \sum_{j=1}^{\ell-1} c_{\ell-j} \sum_{A\in S} \sum_{B\in\binom{A}{j}} 1 \\
&= |S| q^{\ell} p^{\binom{\ell}{2}} \sum_{j=1}^{\ell-1} \binom{\ell}{j} c_{\ell-j} \\
&= \mu \sum_{j=1}^{\ell-1} \binom{\ell}{j} c_j = \mu \sum_{j=0}^{\ell-1} \binom{\ell}{j} c_j - \mu.
\end{aligned}$$

Therefore,

$$\frac{\mu^2}{\mu + \overline{\Delta}} \geqslant \frac{\mu}{\sum_{j=0}^{\ell-1} \binom{\ell}{j} c_j} = \frac{\mu}{c_\ell/(\log(1/\varepsilon))} > \log(1/\varepsilon).$$

Finally, from (4) we get

$$\mathbb{P}[\forall A \in \mathcal{S} : K_A \nsubseteq \boldsymbol{G}_{n,p} \text{ or } A \nsubseteq \boldsymbol{U}_{n,q}] \leqslant \exp\left(-\frac{\mu^2}{\mu + \overline{\Delta}}\right) < \varepsilon.$$

Therefore, the family $\mathcal{S}$ is a (p, q, ε)-clique sunflower with an empty core. □

4 Monotone arithmetic circuits

In this section, we give a short and simple proof of a truly exponential ($\exp(\Omega(n))$) lower bound for real monotone arithmetic circuits computing a multilinear n variate polynomial. Real monotone arithmetic circuits are arithmetic circuits over the reals that use only positive numbers as coefficients. As we shall see, the lower bound argument holds for a general family of multilinear polynomials constructed in a very natural way from error correcting codes, and the similarities to the hard function used by Harnik and Raz in the Boolean setting is quite evident (see Section 2.2). In particular, our lower bound just depends on the rate and relative distance of the underlying code. We note that exponential lower bounds for monotone arithmetic circuits are not new, and have been known since the 80's with various quantitative bounds. More precisely, Jerrum and Snir proved an $\exp(\Omega(\sqrt{n}))$ lower bound for an n variate polynomial in [15]. This bound was subsequently improved to a lower bound of $\exp(\Omega(n))$ by Raz and Yehudayoff in [22], via an extremely

clever argument, which relied on deep and beautiful results on character sums over finite fields. A similar lower bound of $\exp(\Omega(n))$ was shown by Srinivasan [26] using more elementary techniques building on a work of Yehudayoff [30]. In a recent personal communication Igor Sergeev pointed out to us that truly exponential lower bounds for monotone arithmetic circuits had also been proved in the 1980's in the erstwhile Soviet Union by several authors, including the works of Kasim-Zade, Kuznetsov and Gashkov. We refer the reader to [10] for a detailed discussion on this line of work.

We show a similar lower bound of $\exp(\Omega(n))$ via a simple and short argument, which holds in a somewhat general setting. Our contribution is just the simplicity, the (lack of) length of the argument and the observation that it holds for families of polynomials that can be constructed from any sufficiently *good* error correcting codes.

Definition 4.1 (Monotone, multilinear, homogeneous)**.** *A real polynomial is said to* monotone *if all of its coefficients are positive. A real arithmetic circuit is said to be* monotone *if it uses only positive numbers as coefficients. A polynomial P is said to be* multilinear *if the degree of each variable of P is at most 1 in all of the monomials of P. A polynomial P is said to be* homogeneous *if all the monomials of P have the same degree. An arithmetic circuit C is said to be to* homogeneous *(*multilinear*) if the polynomial computed in each of the gates of C is homogeneous (multilinear).*

Definition 4.2 (From sets of vectors to polynomials)**.** *Let $C \subseteq \mathbb{F}_q^n$ be an arbitrary subset of $\mathbb{F}_q^n$. Then, the polynomial P_C is a multilinear homogeneous polynomialof degree n on qn variables $\{x_{i,j} : i \in [q], j \in [n]\}$ and is defined as follows:*

$$P_C = \sum_{c \in C} \prod_{j \in [n]} x_{c(j),j} \,.$$

Here, $c(j)$ is the j^{th} coordinate of c which is an element of $\mathbb{F}_q$, which we bijectively identify with the set $[q]$.

Here, we will be interested in the polynomial P_C when the set C is a *good* code, i.e it has high rate and high relative distance. The following observation summarizes the properties of P_C and relations between the properties of C and P_C.

Observation 4.3 (Codes vs Polynomials)**.** *Let C be any subset of $\mathbb{F}_q^n$ and let P_C be the polynomial as defined in Definition 4.2. Then, the following statements are true:*

- *P_C is a multilinear homogeneous polynomial of degree equal to n with every coefficient being either 0 or 1.*
- *The number of monomials with non-zero coefficients in P_C is equal to the cardinality of C.*
- *If any two distinct vectors in C agree on at most k coordinates (i.e. C is a code of distance $n - k$), then the intersection of the support of any two monomials with non-zero coefficients in P_C has size at most k.*

The observation immediately follows from Definition 4.2. We note that we will work with monotone arithmetic circuits here, and hence will interpret the polynomial P_C as a polynomial over the field of real numbers.

We now prove the following theorem, which essentially shows that for every code C with sufficiently good distance, any monotone arithmetic circuit computing P_C must essentially compute it by computing each of its monomials separately, and taking their sum.

Theorem 4.4. *If any two distinct vectors in C agree on at most $n/3 - 1$ locations, then any monotone arithmetic circuit for P_C has size at least $|C|$.*

The proof of this theorem crucially uses the following well known structural lemma about arithmetic circuits. This lemma also plays a crucial role in the other proofs of exponential lower bounds for monotone arithmetic circuits (e.g. [15, 22, 26, 30]).

Lemma 4.5 (See Lemma 3.3 in [22])**.** *Let Q be a homogeneous multilinear polynomial of degree d computable by a homogeneous arithmetic circuit of size s. Then, there are homogeneous polynomials $g_0, g_1, g_2, \ldots, g_s, h_0, h_1, h_2, \ldots, h_s$ of degree at least $d/3$ and at most $2d/3 - 1$ such that*

$$Q = \sum_{i=0}^{s} g_i \cdot h_i \,.$$

Moreover, if the circuit for Q is monotone, then each g_i and h_i is multilinear, variable disjoint and each one their non-zero coefficients is a positive real number.

We now use this lemma to prove Theorem 4.4.

Proof of Theorem 4.4. Let B be a monotone arithmetic circuit for P_C of size s. We know from Observation 4.3 that P_C is a multilinear homogeneous polynomial of degree equal to n. This along with the monotonicity of B implies that B must be homogeneous and multilinear since there can be no cancellations in B. Thus, from (the moreover part of) Lemma 4.5 we know that P_C has a monotone decomposition of the form

$$P_C = \sum_{i=0}^{s} g_i \cdot h_i \,,$$

where, each g_i and h_i is multilinear, homogeneous with degree between $n/3$ and $2n/3 - 1$, g_i and h_i are variable disjoint. We now make the following claim.

Claim 4.6. *Each g_i and h_i has at most one non-zero monomial.*

We first observe that the claim immediately implies theorem 4.4: since every g_i and h_i has at most one non-zero monomial, their product $g_i h_i$ is just a monomial. Thus, the number of summands s needed in the decomposition above must be equal to the number of monomials in P_C, which is equal to $|C|$ from the second item in Observation 4.3. □

We now prove the Claim.

Proof of Claim. The proof of the claim will be via contradiction. To this end, let us assume that there is an $i \in \{0, 1, 2, \ldots, s\}$ such that g_i has at least two distinct monomials with non-zero coefficients and let α and β be two of these monomials. Let γ be a monomial with non-zero coefficient in h_i . Since h_i is homogeneous with degree between $n/3$ and $2n/3 - 1$, we know that the degree of γ is at least $n/3$. Since we are in the monotone setting, we also know that each non-zero coefficient in any of the g_j and h_j is a positive real number. Thus, the monomials $\alpha \cdot \gamma$ and $\beta \cdot \gamma$ which have non-zero coefficients in the product $g_i \cdot h_i$ must have non-zero coefficient in P_C as well (since a monomial once computed cannot be cancelled out). But, the supports of $\alpha\gamma$ and $\beta\gamma$ overlap on γ which has degree at least $n/3$. This contradicts the fact that no two distinct monomials with non-zero coefficients in P_C share a sub-monomial of degree at least $n/3$ from the distance of C and the third item in Observation 4.3. □

Theorem 4.4 when instantiated with an appropriate choice of the code C, immediately implies an exponential lower bound on the size of monotone arithmetic circuits computing the polynomial P_C. Observe that the total number of variables in P_C is $N = qn$ and therefore, for the lower bound for P_C to be of the form $\exp(\Omega(N))$, we would require q, the underlying field size to be a constant. In other words, for any code of relative distance at least $2/3$ over a constant size alphabet which has exponentially many code words, we have a truly exponential lower bound.

The following theorem of Garcia and Stichtenoth [9] implies an explicit construction of such codes. The statement below is a restatement of their result by Cohen et al.[7].

Theorem 4.7 ([9] and [27])**.** *Let p be a prime number and let $m \in \mathbb{N}$ be even. Then, for every $0 < \rho < 1$ and a large enough integer n, there exists an explicit rate ρ linear error correcting block code $C : \mathbb{F}_{p^m}^n \to \mathbb{F}_{p^m}^{n/\rho}$ with distance*

$$\delta \geqslant 1 - \rho - \frac{1}{p^{m/2} - 1}\,.$$

The theorem has the following immediate corollary.

Corollary 4.8. *For every large enough constant q which is an even power of a prime, and for all large enough n, there exist explicit construction of codes $C \subseteq \mathbb{F}_q^n$ which have relative distance at least $2/3$ and $|C| \geqslant \exp(\Omega(n))$.*

By an explicit construction here, we mean that given a vector v of length n over $\mathbb{F}_q$, we can decide in deterministic polynomial time if $v \in C$. In the arithmetic complexity literature, a polynomial P is said to be explicit, if given the exponent vector of a monomial, its coefficient in P can be computed in deterministic polynomial time. Thus, if a code C is explicit, then the corresponding polynomial P_C is also explicit in the sense described above. Therefore, we have the following corollary of Corollary 4.8 and Theorem 4.4.

Corollary 4.9. *There exists an explicit family $\{P_n\}$ of homogeneous multilinear polynomials such that for every large enough n, any monotone arithmetic circuit computing the n variate polynomial P_n has size at least $\exp(\Omega(n))$.*

5 Further directions

In this paper, we obtained the first monotone circuit lower bound of the form $\exp(\Omega(n^{1/2}/\log n))$ for an explicit n-bit monotone Boolean function. It's natural to ask if we can do better. Ideally, we would like to achieve a truly exponential bound for Boolean monotone circuits, like the one achieved for arithmetic monotone circuits in Section 4. However, as discussed in Section 2.8, the $\sqrt{n}$ exponent seems to be at the limit of what current techniques can achieve.

An important open-ended direction is to develop sharper techniques for proving monotone circuit lower bounds. Sticking to the approximation method, it is not yet known whether there exists another "sunflower-type" notion which still allows for good approximation bounds and yet admits significantly better bounds than what is possible for robust sunflowers.

One approach can be to try to weaken the requirement of the core, and ask only that the core of a "sunflower-type" set system $\mathcal{F}$ is properly contained in one of the elements of $\mathcal{F}$. A weaker notion of robust sunflowers with this weakened core could still be used succesfully in the proof of

the lower bound of Section 2, but it's not yet clear whether this weaker notion admits stronger bounds or not.

Moreover, perhaps developing specialised sunflowers for specific functions, such as done for $\mathsf{Clique}_{k,n}$ in Section 3, could help here. One could also consider distributions which are not p-biased, as perhaps better bounds are possible in different regimes.

Finally, as noted before, our proof of the clique-sunflower lemma follows the approach of Rossman in [24]. We expect that a proof along the lines of the work of Alweiss, Lovett, Wu and Zhang [3] and Rao [21] should give us an even better bound on the size of set systems without clique-sunflowers, removing the $\ell!$ factor. This would extend our $n^{\Omega(\delta^2 k)}$ lower bound to $k \leqslant n^{1/2-\delta}$.

Acknowledgements

We are grateful to Stasys Junka for bringing the lower bound of Andreev [5] to our attention and to the anonymous referees of LATIN 2020 for numerous helpful suggestions. We also thank Igor Sergeev for bringing [10] and the references therein to our attention which show that truly exponential lower bounds for monotone arithmetic circuits had already been proved in the 1980s. Finally, we thank the anonymous reviewers of Algorithmica for careful proofreading and many helpful suggestions and comments.

Bruno Pasqualotto Cavalar was supported by São Paulo Research Foundation (FAPESP), grants #2018/22257-7 and #2018/05557-7, and he acknowledges CAPES (PROEX) for partial support of this work. A part of this work was done during a research internship of Bruno Pasqualotto Cavalar and a postdoctoral stay of Mrinal Kumar at the University of Toronto. Benjamin Rossman was supported by NSERC and Sloan Research Fellowship.

This version of the article has been accepted for publication after peer review, but is not the Version of Record and does not reflect post-acceptance improvements, or any corrections. The Version of Record is available online at: https://doi.org/10.1007/s00453-022-01000-3.

References

[1] N. Alon and R. B. Boppana, *The monotone circuit complexity of Boolean functions*, Combinatorica **7** (1987), no. 1, 1–22. MR905147

[2] Noga Alon, László Babai, and Alon Itai, *A fast and simple randomized parallel algorithm for the maximal independent set problem*, J. Algorithms **7** (1986), no. 4, 567–583. MR866792

[3] Ryan Alweiss, Shachar Lovett, Kewen Wu, and Jiapeng Zhang, *Improved bounds for the sunflower lemma*, Proceedings of the 52nd annual acm sigact symposium on theory of computing, 2020, pp. 624–630.

[4] A. E. Andreev, *A method for obtaining lower bounds on the complexity of individual monotone functions*, Dokl. Akad. Nauk SSSR **282** (1985), no. 5, 1033–1037. MR796937

[5] AE Andreev, *A method for obtaining efficient lower bounds for monotone complexity*, Algebra and Logic **26** (1987), no. 1, 1–18.

[6] Tolson Bell, Suchakree Chueluecha, and Lutz Warnke, *Note on sunflowers*, Discrete Mathematics **344** (2021), no. 7, 112367.

[7] Gil Cohen, Bernhard Haeupler, and Leonard J. Schulman, *Explicit binary tree codes with polylogarithmic size alphabet*, Proceedings of the 50th annual acm sigact symposium on theory of computing, pp. 535–544.

[8] P. Erdős and R. Rado, *Intersection theorems for systems of sets*, J. London Math. Soc. **35** (1960), 85–90. MR0111692

[9] A Garcia and H Stichtenoth, *A tower of artin-schreier extensions of function fields attaining the drinfeld-vladut bound*, Inventiones Mathematicae **121** (1995), no. 1, 211–222.

[10] Sergey B. Gashkov and Igor'S. Sergeev, *A method for deriving lower bounds for the complexity of monotone arithmetic circuits computing real polynomials*, Sbornik: Mathematics **203** (October 2012), no. 10, A02.

[11] Parikshit Gopalan, Raghu Meka, and Omer Reingold, *DNF sparsification and a faster deterministic counting algorithm*, Computational Complexity **22** (2013), no. 2, 275–310.

[12] Danny Harnik and Ran Raz, *Higher lower bounds on monotone size*, Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, 2000, pp. 378–387. MR2114553

[13] Svante Janson, *Poisson approximation for large deviations*, Random Structures and Algorithms **1** (1990), no. 2, 221–229.

[14] Svante Janson, Tomasz Ł uczak, and Andrzej Ruciński, *Random graphs*, Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley-Interscience, New York, 2000. MR1782847

[15] Mark Jerrum and Marc Snir, *Some exact complexity results for straight-line computations over semirings*, J. ACM **29** (July 1982), no. 3, 874–897.

[16] Stasys Jukna, *Combinatorics of monotone computations*, Combinatorica **19** (1999), no. 1, 65–85.

[17] Xin Li, Shachar Lovett, and Jiapeng Zhang, *Sunflowers and quasi-sunflowers from randomness extractors*, Approx-random, 2018, pp. 51:1–13.

[18] Shachar Lovett, Noam Solomon, and Jiapeng Zhang, *From dnf compression to sunflower theorems via regularity*, arXiv preprint arXiv:1903.00580 (2019).

[19] Shachar Lovett and Jiapeng Zhang, *Dnf sparsification beyond sunflowers*, Proceedings of the 51st annual acm sigact symposium on theory of computing, 2019, pp. 454–460.

[20] Toniann Pitassi and Robert Robere, *Strongly exponential lower bounds for monotone computation*, Proceedings of the 49th annual acm sigact symposium on theory of computing, 2017, pp. 1246–1255.

[21] Anup Rao, *Coding for sunflowers*, Discrete Anal. (2020), Paper No. 2, 8. MR4072543

[22] Ran Raz and Amir Yehudayoff, *Multilinear formulas, maximal-partition discrepancy and mixed-sources extractors*, J. Comput. Syst. Sci. **77** (2011), no. 1, 167–190.

[23] A. A. Razborov, *Lower bounds on the monotone complexity of some Boolean functions*, Dokl. Akad. Nauk SSSR **281** (1985), no. 4, 798–801. MR785629

[24] Benjamin Rossman, *The monotone complexity of k-clique on random graphs*, SIAM J. Comput. **43** (2014), no. 1, 256–279. MR3166976

[25] ———, *Approximate sunflowers*, 2019. unpublished, available at http://www.math.toronto.edu/rossman/approx-sunflowers.pd

[26] Srikanth Srinivasan, *Strongly exponential separation between monotone VP and monotone VNP*, CoRR **abs/1903.01630** (2019), available at 1903.01630.

[27] H. Stichtenoth, *Algebraic function fields and codes*, Vol. 254, Springer Science & Business Media, 2009.

[28] Terence Tao, *The sunflower lemma via shannon entropy*, Blogpost (2020).

[29] J Tiekenheinrich, *A 4n-lower bound on the mononotone network complexity of a oneoutput boolean function*, Information Processing Letters **18** (1984), 201–201.

[30] Amir Yehudayoff, *Separating monotone VP and VNP*, Proceedings of the 51st annual ACM SIGACT symposium on theory of computing, STOC 2019, phoenix, az, usa, june 23-26, 2019., 2019, pp. 425–429.

A Proof of Theorem 1.3

We say that a family $\mathcal{F}$ of sets is *r-spread* if there are most $|\mathcal{F}|/r^{|T|}$ sets in $\mathcal{F}$ containing any given non-empty set T. The following theorem is a p-biased variant of the main technical lemma of Rao [21]. A full proof is given in the appendix of [6].

Theorem A.1 (Theorem 3 of [6]). *There exists a constant $B > 0$ such that the following holds for all $p, \varepsilon \in (0, 1/2]$ and all positive integers ℓ. Let $r = B \log(\ell/\varepsilon)/p$. Let $\mathcal{F}$ be a r-spread ℓ-uniform family of subsets of $[n]$ such that $|\mathcal{F}| \geqslant r^\ell$. Then $\mathbb{P}_{\boldsymbol{W} \subseteq_p [n]}[\exists F \in \mathcal{F} : F \subseteq \boldsymbol{W}] > 1 - \varepsilon$.*

We now combine Theorem A.1 with the main argument of the proof of Theorem 4.4 of [24] to finish the proof of Theorem 1.3.

Proof of Theorem 1.3. The proof is by induction on ℓ. When $\ell = 1$, we have

$$\mathbb{P}[\forall F \in \mathcal{F} : F \not\subseteq \boldsymbol{W}] = (1-p)^{|\mathcal{F}|} \leqslant e^{-p|\mathcal{F}|} < \varepsilon.$$

Therefore, $\mathcal{F}$ itself is a (p, ε)-robust sunflower. We now suppose $\ell > 1$ and that the result holds for every $t \in [\ell - 1]$. For a set $T \subseteq [n]$, let $\mathcal{F}_T = \{F \setminus T : F \in \mathcal{F}, T \subseteq F\}$. Let $r = B \log(\ell/\varepsilon)/p$, where B is the constant of Theorem A.1.

Case 1. The family $\mathcal{F}$ is not r-spread. By definition, there exists a nonempty set $T \subseteq [n]$ such that $|\mathcal{F}_T| > |\mathcal{F}| / r^{|T|} \geqslant r^{\ell - |T|}$. By induction, the family $\mathcal{F}_T$ contains a (p, ε)-robust sunflower $\mathcal{F}'$. It is easy to see that $\{F \cup T : F \in \mathcal{F}'\}$ is a (p, ε)-robust sunflower contained in $\mathcal{F}$.

Case 2. The family $\mathcal{F}$ is r-spread. Therefore, from Theorem A.1, it follows that $\mathcal{F}$ is itself a (p, ε)-robust sunflower. □

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il