Electronic Colloquium on Computational Complexity, Report No. 220 (2026)

# Derandomized Sunflowers and Radical Lower Bounds

Bruno Cavalar * Théo Borém Fabris† Partha Mukhopadhyay‡
Srikanth Srinivasan§ Amir Yehudayoff¶

September 28, 2026

**Abstract**

Robust Sunflower lemmas imply that any large enough monotone DNF of width $w$ contains a sunflower, i.e., a DNF equivalent to the conjunction of a common core with a DNF that is heavily biased towards 1. While these lemmas are typically proved in the context of the uniform distribution or i.i.d. distributions, they also hold for $O(w^2)$-wise independent distributions by Bazzi's theorem (Bazzi (SICOMP 2009); Tal (CCC 2017)), which states that width-$w$ DNFs cannot distinguish between such distributions and the uniform distribution.

We prove a derandomization of robust sunflower lemmas for $O(w)$-wise independent distributions, which recovers the derandomization above with slightly weaker parameters. Notably, our result also holds for distributions whose marginals are "locally independent" and "approximately identically" distributed. It is not known whether such distributions fool general DNFs, which makes the derandomization via DNF-fooling techniques unavailable. Our proof of this derandomization is via the method of moments, which might be of independent interest.

We apply this result to obtain improved separations between non-monotone arithmetic circuits and the radical of monotone circuits. Specifically, we construct an *explicit* family of multilinear polynomials $P_n$ that have small non-monotone arithmetic circuits such that any power of $P_n$ cannot be computed by monotone arithmetic circuits of *sub-exponential* size. This improves on a recent result of Cavalar, Fabris, Mukhopadhyay, Srinivasan and Yehudayoff (STOC 2026), who proved a non-explicit separation that was quasipolynomial. Our construction uses Nisan-Wigderson designs with an additional linear-algebraic expansion property.

*Department of Computer Science, University of Oxford, United Kingdom. Supported by EPSRC project EP/Z534158/1 on "Integrated Approach to Computational Complexity: Structure, Self-Reference and Lower Bounds". Email: bruno.cavalar@cs.ox.ac.uk

†Department of Computer Science, University of Copenhagen, Denmark. Supported by the European Research Council (ERC) under grant agreement no. 101125652 (ALBA). The author thanks BARC (VILLUM grant no. 54451) for the supportive research environment. Email: thfa@di.ku.dk

‡Chennai Mathematical Institute, India. Email: partham@cmi.ac.in

§Department of Computer Science, University of Copenhagen, Denmark. Supported by the European Research Council (ERC) under grant agreement no. 101125652 (ALBA). Email: srsr@di.ku.dk

¶Department of Computer Science, The University of Copenhagen, and The Technion-IIT. Supported by DNRF Chair grant no. 20231101-28697. Email: amir.yehudayoff@gmail.com

ISSN 1433-8092

# Contents

# 1 Introduction

## 1.1 Background and Results

The sunflower lemma of Erdős and Rado [ER60] states that every large enough family of sets must contain a *sunflower*: a family of sets whose pairwise intersections are identical. Along the decades, this elegant definition has found applications in several areas of theoretical computer science, including circuit complexity [Raz85, HJP95], data structure lower bounds [FMS93, RR18], matrix multiplication algorithms [ASU13], parametrized complexity [FG06], and much more [Rao25].

An "approximate" version of sunflowers was defined by [Ros14] in the context of average-case monotone circuit complexity. This variant, nowadays called *robust sunflowers*, has since become a central key in several results and breakthroughs, including progress in the sunflower conjecture [ALWZ21], improved monotone circuit lower bounds [CKR22, dRV25, CGR$^+$26, BM25, CFM$^+$26], communication complexity [LMM$^+$22], DNF sparsification [GMR13], sampling lower bounds [FLRS23], top-down circuit lower bounds [GRSS23], etc.

A robust sunflower can be defined as a monotone DNF which accepts inputs randomly sampled from a product distribution with very high probability, provided that the literals present in all terms, i.e., the core of the sunflower, are set to 1. Rossman [Ros14] proved the first bounds on how large a DNF must be to contain a robust sunflower as a sub-DNF, and later optimal bounds were discovered by [ALWZ21, Rao20, BCW21].

There is nothing special about product distributions, and one could also define robust sunflowers with respect to other distributions, particularly distributions with significantly smaller entropy, which we call derandomized sunflowers. Proving a robust sunflower lemma over such distributions was the key behind the recent exponential monotone circuit lower bound for Perfect-Matching [CGR$^+$26], as well as an improved monotone circuit lower bound for **NC** [CFM$^+$26]. It has also been speculated that such "derandomized sunflowers" may provide a path towards improved lifting theorems in communication complexity [Kel21].

**Robust sunflower bounds for almost-independent distributions.** In [CGR$^+$26], a derandomized sunflower lemma was obtained by an ad-hoc reduction to fully random robust sunflowers. The reduction works only for DNFs whose terms form a partial matching and to a specific distribution, being thus more tailored to their specific application. In [CFM$^+$26], a derandomized sunflower lemma was instead obtained by employing Bazzi's theorem [Baz09, Tal17] to argue that small DNFs cannot distinguish between $k$-wise independent and fully random distributions. This argument works for all small DNFs and $k$-wise independent distributions.

Unfortunately, a significant downside of employing pseudorandom generators (PRGs) for DNFs, such as Bazzi's theorem, as a blackbox is that such reductions are potentially

suboptimal. A standard structure-versus-randomness argument implies that to obtain robust sunflower bounds it suffices to show that spread DNFs are robust sunflowers, where we say that a DNF is *spread* if no set of literals appears in disproportionally too many terms. Bazzi's theorem, however, applies to *all* DNFs of sufficiently small size, not merely the spread ones. This generality comes with a cost: the resulting sunflower lemma has significantly worse bounds than the fully random case. In particular, the authors of [CFM+26] only manage to obtain exponential lower bounds with exponent $n^{1/3}$ on the monotone complexity of **NC** functions, whereas exponential lower bounds with exponent $n^{1/2}$ are the state-of-the-art for **NP** functions [CKR22]. More fundamentally, such arguments cannot capture distributions that do not fool DNFs. As an example, almost-independent distributions cannot even fool DNFs of polylogarithmic width [AGG+25].

Our first contribution is to show robust sunflower bounds for "local" convex combinations of product distributions via a high-order Markov's inequality, which avoids the more sophisticated machinery from PRGs for DNFs. We say that a distribution $\mathcal{D}$ with support $\{0,1\}^n$ is $(k,\varepsilon)$-*pseudo-independent with marginal probability* $q$ if, for every set $S \subseteq [n]$ of size at most $k$, the marginal distribution $\mathcal{D}_S$ of $\mathcal{D}$ on $\{0,1\}^S$ is a convex combination of product distributions, in each of which every bit is 1 with probability $q' \in [(1-\varepsilon)q, (1+\varepsilon)q]$. A monotone DNF $\mathcal{F}$ is a $(\mathcal{D},\delta)$-*sunflower* if $\mathbb{E}_{x\sim\mathcal{D}}[\mathcal{F}_\Delta(x)] > 1-\delta$, where $\mathcal{F}_\Delta$ is the DNF obtained from $\mathcal{F}$ by setting all literals that appear in *all the terms* of $\mathcal{F}$ to 1. We prove the following:

**Theorem 1.1.** For every $w \in \mathbb{N}$ and $0 < q, \delta < 1$, let $\mathcal{F}$ be a width-$w$ monotone DNF of size at least $(\frac{w}{q}\log(1/\delta))^w$. There exist parameters $k = O(w\log(1/\delta))$ and $\varepsilon = \Omega(1/w)$ such that if $\mathcal{D}$ is $(k,\varepsilon)$-pseudo-independent with marginal distribution $q$, then $\mathcal{F}$ contains a $(\mathcal{D},\delta)$-sunflower.

Let us compare the above result with the sunflower lemma of [CFM+26]. Their arguments roughly show a sunflower bound of $(\log(1/\delta)/q)^w$ for parameters $k \approx w^2 + w\log(1/\delta)$ and $\varepsilon = 0$, using the best known bounds for $k$-wise independence needed to fool DNFs [Tal17]. Whereas their size bound is better for this regime of parameters, our result achieves a derandomization of sunflowers with smaller $k$ even in the $\varepsilon = 0$ regime, as we only need $k = O(w\log(1/\delta))$. Moreover, it is easy to check that $(k,\varepsilon)$-pseudo-independent distributions with sufficiently small $\varepsilon$ are also "*almost independent*"[1]; whereas some "*almost independent*" distributions cannot fool DNFs [AGG+25]. Our result thus suggests that derandomizing sunflower lemmas may be strictly easier than building PRGs for DNFs.

Given the wide applicability and consequences of robust sunflower bounds, we expect our derandomized sunflower bounds to be useful in other contexts, and our techniques also seem sufficiently flexible to be adaptable to different distributions, as we discuss in Section 1.2. We now describe a particular application we derive from our derandomized

[1] A distribution $\mathcal{D}$ is $(k,\varepsilon)$-*wise almost independent* if $(1-\varepsilon)2^{-k} \le \Pr_{x\sim\mathcal{D}}[x_A = \alpha] \le (1+\varepsilon)2^{-k}$ for every $\alpha \in \{0,1\}^A$ and every $A$ of size at most $k$.

sunflower lemma, solving an open problem in circuit complexity [CFM+26]. The *pseudo-independence* condition (and not just $k$-wise independence) allowed by Theorem 1.1 is needed for this application.

**Monotone radical lower bounds.** Monotone arithmetic complexity studies arithmetic circuits over the nonnegative reals that disallow subtraction. The study of monotone polynomials is natural for counting problems, since many counting questions about combinatorial structures are naturally characterized as evaluating polynomials with non-negative coefficients on Boolean inputs. A classical example is the problem of counting the number of perfect matchings in bipartite graphs and its characterization via evaluations the permanent polynomial. Furthermore, many natural combinatorial strategies for solving these problems (e.g., pure dynamic programming algorithms) can be phrased as monotone arithmetic circuits [JS20], and algorithms that avoid subtractions and cancellations are inherently more robust to numerical noise, e.g. from rounding errors [DK06, FGK16].

This led researchers to the question of understanding the gap in computational power between monotone and non-monotone computations and by now, many results in this direction are known [SS77, Val80, JS82, GS91, RY11, CDM21, CDGM22, CFM+26]. The seminal work of Valiant [Val80] showed that a nonmonotone circuit computing a monotone polynomial using only one negation gate can be exponentially more powerful than any monotone computation. Continuing this line of work, the current state-of-the-art results establish strongly exponential separations between depth-three non-monotone circuits and general monotone circuits [CFM+26], showing the best possible exponential separation between nonmonotone and monotone classes. These results show that monotone counting algorithms are inherently weaker than their non-monotone counterparts.

However, it may be possible to get around this weakness of monotone computation with a trick: first perform an efficient monotone computation $M$ that produces a function $g(f)$ of the answer $f$ and then invert the function $g$ using a simple non-monotone computation $C$ to produce $f$ itself. In other words, $f$ can be computed by the composition $C \circ M$ of $C$ after $M$, which can be interpreted as way of computing $f$ via a non-monotone circuit with restricted non-monotone computation $C$.

A natural option for the non-monotone computation $C$ is taking the $k$-th root of $M$, since there are fast and numerically robust algorithms for computing $k$-th roots as long as $k$ itself is not too large [Kal87]. The resulting question can then be naturally stated in the language of *radicals*. Radicals appear, for example, in geometry (via the Pythagorean theorem) and in solving quadratic equations. More abstractly, a radical of an ideal is the set of elements whose powers belong to the ideal. There are many examples of radicals that are larger than their ideals, such as the radical of the ideal generated by 2 in the ring of algebraic integers and the radical of the ideal generated by $x^2$ in the ring of polynomials. Another important example is Hilbert's Nullstellensatz, which characterizes the geometric consequences of a set of polynomial equations in terms of its (algebraically defined) radical. We define the *radical* $\sqrt{\mathcal{C}}$ *of a circuit class* $\mathcal{C}$ as the set of polynomials $P$ such that some

power of $P$ is in $\mathcal{C}$. For non-monotone classes $\mathcal{C}$, there are questions about $\sqrt{\mathcal{C}}$ that are relevant to the study of Hardness vs. Randomness in arithmetic circuits [And20].

It is then natural to investigate potential computational gaps between non-monotone computation and monotone radical computations. This question can be formalized as follows: is there a polynomial $P(x_1, \ldots, x_n)$ that has non-monotone circuits of size poly$(n)$, but is not in the radical $\sqrt{\mathcal{C}}$,[2] where $\mathcal{C}$ is the class of *monotone* arithmetic circuits of some bounded size $s(n)$? Most existing proof techniques in monotone arithmetic complexity — either support-based methods [SS77, Val80, JS82, GS91] or approaches based on communication complexity and related techniques [RY11, Yeh19, Sri20, CDM21] — appear to fall short of resolving the question about the relative power of nonmonotone classes and the radical of monotone circuits.

Very recently, the work of [CFM+26] made progress on this problem, by showing the first separation between **VP** and the radical of monotone circuits with $s(n)$ being a superpolynomial function of $n$. Their result was obtained via a connection to monotone *Boolean* circuit lower bounds, suggested by Hrubeš and Yehudayoff [HY21] in the context of proving lower bounds for monotone circuits with division gates. For every $n$-variate monotone polynomial $P$ over $\mathbb{R}$, define a monotone Boolean function $f_P : \{0,1\}^n \to \{0,1\}$ via $f_P(x) = 1$ iff $P(x) > 0$. The key observation is that a monotone arithmetic circuit for $P$ naturally yields a monotone Boolean circuit for $f_P$ by replacing $+$ gates with $\vee$ gates, and $\times$ gates with $\wedge$ gates, and positive $\mathbb{R}$-constant with the bit 1. Importantly, the function $f_P$ depends only on the set of points where $P$ evaluates to a non-zero value and is therefore invariant under taking powers of $P$. Consequently, a monotone Boolean lower bound for $f_P$ implies monotone arithmetic lower bounds for all powers of $P$.

However, the polynomials constructed in [CFM+26] are not explicit, as their definitions rely on a base matrix chosen probabilistically, so their circuit upper bound (in **VP**) is not known to be described by a Turing machine running in polynomial time. Moreover, their monotone lower bound is only quasi-polynomial, whereas previous monotone vs. non-monotone separations (which do not imply lower bounds for the radical) yield exponential bounds.

We remove both these shortcomings. Using ideas from pseudorandomness — more precisely, by understanding linear-algebraic expansion properties of Nisan-Wigderson designs [NW94] based on univariate polynomials — we explicitly construct polynomials $(P_m)_m$ computed by arithmetic circuits described by Turing machine running in deterministic polynomial time and having the properties needed to obtain an exponential radical monotone lower bound via our derandomized sunflower lemma (Theorem 1.1). Our lower bound is obtained via a criterion of [CFM+26] that reduces monotone Boolean circuit lower bounds to sunflower bounds over carefully chosen pseudo-independent distributions.

[2] We could also bound the order of the resulting root to a polynomial function of $n$. But we keep this stronger definition as our results apply even in this setting.

**Theorem 1.2.** There is an infinite sequence $(P_m(x_1, \ldots, x_m))_{m \in \mathbb{N}}$ of polynomials such that the following hold:

1. (Explicit Upper bound) $P_m$ is a monotone multilinear polynomial with an arithmetic circuit $C_m$ of size $m^{O(1)}$. Further, given $m$, the circuit $C_m$ can be computed in deterministic time $m^{O(1)}$.

2. (Radical Lower bound) Any monotone arithmetic circuit computing a power of $P_m$ must have size at least $\exp(m^{\Omega(1)})$.

Employing arithmetic depth-reduction results [AV08, Koi12, Tav15, GKKS16], we also obtain the first super-polynomial separation between non-monotone constant-depth circuits and the radical of monotone circuits.

**Corollary 1.3.** For every constant $k \geq 1$, there is an infinite sequence $(Q_M(x_1, \ldots, x_M))_{M \in \mathbb{N}}$ of polynomials such that the following hold:

1. $Q_M$ is a monotone multilinear polynomial with a depth $O(k)$ arithmetic circuit $C'_M$ of size $M^{O(1)}$. Further, given $M$, the circuit $C'_M$ can be computed in deterministic time $M^{O(1)}$.

2. Any monotone arithmetic circuit computing a power of $Q_M$ must have size at least $M^{\Omega((\log M)^k)}$.

## 1.2 Challenges and Proof Ideas

We now describe the main challenges and proof ideas in our results. First, we describe how to prove Theorem 1.1, our derandomized sunflower lemma. Then we show how the sunflower lemma can be employed to obtain the separation of Theorem 1.2 for polynomials with certain properties. We then describe how to construct such polynomials.

**Derandomization of sunflowers via the method of moments.** The first proof of a robust sunflower lemma was given by Rossman [Ros14] by means of an application of Janson's inequality [Jan90] (see also [AS16, Chapter 8]). Essentially, Janson's inequality helps us analyse the following type of event. Let $\mathcal{F}$ be a width-$w$ monotone DNF over $n$ bits with terms $F_1, \ldots, F_N$ where $N = r^w$ for some parameter $r$. We identify a term with its set of literals, thus frequently referring to $F_i$ both as a conjunction and as a set. Let $x$ be a uniformly random string of $n$ bits. Write $i \sim j$ if the events $\{F_i(x) = 1\}$ and $\{F_j(x) = 1\}$ are dependent (i.e., if $F_i \cap F_j \neq \varnothing$). For $\mu := \sum_{i \in [N]} \mathbb{E}_{x \sim \{0,1\}^n}[F_i(x)]$, Janson's inequality gives the following bound:

$$\Pr_{x \sim \{0,1\}^n}[\mathcal{F}(x) = 0] \leq \exp(-\mu^2/(2\Delta)),$$

where $\Delta := \sum_{i \sim j} \Pr_{x \sim \{0,1\}^n}[(F_i \wedge F_j)(x) = 1]$.

This bound is quite useful when $\mathcal{F}$ is $r$-*spread*, that is, when

$$|\{\, i \in [N] : A \subseteq F_i\}| \leq r^{w-|A|}$$

for every set $A \subseteq [n]$. One can then upper bound $\Delta$ simply by counting, for every $F \in \mathcal{F}$ and $A \subseteq F$, how many sets in $\mathcal{F}$ intersect $F$ at $A$; there will be at most $r^{w-|A|}$ such sets. From here, it follows that spread DNFs are robust sunflowers with an empty core.

When the DNF is not spread, it suffices to find a maximally spreadness violating set $A$; we can easily argue that $\mathcal{F}_A = \{F_i \setminus A : i \in [N], A \subseteq F_i\}$ is itself $r$-spread, and thus $\{F_i : i \in [N], A \subseteq F_i\}$ is a robust sunflower inside $\mathcal{F}$. Thus, the technical core of the proof is showing that spread DNFs are robust sunflowers with respect to the uniform distribution.

This simple argument, despite being suboptimal, still appears in some form in the optimal robust sunflower bounds obtained by [ALWZ21, Rao20], and thus generalising it can be the first step towards sunflowers bounds for other distributions. The problem is that Janson's inequality does not necessarily apply for arbitrary distributions.

Even if the distribution is $t$-wise independent and there are not many pairwise dependencies between terms (so $\Delta$ is small), arbitrary correlations can appear between larger collections of terms. However, existing proofs of Janson's inequality seem to require the fact that, if a random variable $Y_i := \{F_i(x) = 1\}$, for $i \in [N]$, is independent of each of the $p$ random variables $Y_{i_1}(x), \ldots, Y_{i_p}(x)$ individually, then $Y_i$ is independent of all of them. This holds for product distributions but not necessarily for a $(t, \varepsilon)$-pseudo-independent distribution $\mathcal{D}$. However, if $p \leq t/w$, the total amount of bits involved is at most $t$, and we can hope to control the dependencies in this case.

The approach taken by [CFM+26] is just to find an Erdős-Rado sunflower with $p \leq t/w$ petals. This works: it gives a robust sunflower bound, but the bound is too coarse and only yields quasi-polynomial circuit lower bounds.

Our approach is to apply the *method of moments*. Letting $\alpha := q^{-w}$ (assuming $\mathcal{D}$ has marginal probability $q$), we define $X_i := Y_i - \alpha$ and $X := \sum X_i$. We also let $\mu := N\alpha$. The method of moments is the following observation from Markov's inequality:

$$\Pr_{x \sim \mathcal{D}}[\mathcal{F}(x) = 0] = \Pr[X = -\mu] \leq \Pr[X^p \geq \mu^p] \leq \frac{\mathbb{E}[X^p]}{\mu^p},$$

where $p \leq t/w$ is an even number. The technical heart is then to bound $\mathbb{E}[X^p]$. We will obtain such an estimate in two steps.

1. For any $s \in [p]$, and $i \in [N]^s$, and $X_{i_1}, \ldots, X_{i_s}$ whose dependency graph forms a single connected component, we give a generic bound on $|\mathbb{E}[X_{i_1} \cdot \cdots \cdot X_{i_s}]|$ depending solely on the "intersection pattern" of the literals in the terms $F_{i_1}, \ldots, F_{i_s}$. Here we use the pseudo-independence of $\mathcal{D}$.

2. We partition the summands $\mathbb{E}[X_{i_1} \cdot \cdots \cdot X_{i_p}]$ using the partition of $[p]$ induced by the dependency graph corresponding to the terms $F_{i_1}, \ldots, F_{i_p}$. We use the $r$-spreadness

of $\mathcal{F}$ to bound the number of summands that respect a certain fixed intersection pattern, along with a careful analysis of the number of partitions that give rise to a specific dependency graph.

The first step avoids the difficulty of reproving Janson's inequality by focusing only on the expectation of random variables involving at most $t$ bits of $\mathcal{D}$. The second step applies a new "encoding-type" argument somewhat reminiscent of some encoding arguments employed in [ALWZ21, Rao20], albeit in a "higher-moment" fashion. Let $F_{i_1}, \ldots, F_{i_p}$ be terms of $\mathcal{F}$ and define $\mathrm{Vars}(F_{i_j})$ and $\mathrm{Vars}(F_{i_1,\ldots,i_{j-1}})$ as the literals involved in $F_{i_j}$ and $F_{i_1}, \ldots, F_{i_{j-1}}$, respectively. If we know that $|\mathrm{Vars}(F_{i_j}) \cap \mathrm{Vars}(F_{i_1,\ldots,i_{j-1}})| = \ell_j > 0$ for every $\ell \in \{2, \ldots, p\}$, we can "encode" $F_{i_j}$ by first choosing a set $V$ of size $\ell_j$ inside $\mathrm{Vars}(F_{i_1,\ldots,i_{j-1}})$ (there are $\binom{(j-1)w}{\ell_j}$ such sets) and then choosing $F_{i_j}$ among the $Nr^{-\ell_j}$ sets containing $V$.

This argument could form the basis for a more sophisticated proof giving optimal derandomized sunflower bounds. Moreover, our careful partitioning of tuples $(F_{i_1}, \ldots, F_{i_p})$ according to their dependencies (and the computation of the number of such partitionings) seems highly flexible and potentially adaptable to other families of distributions which are not pseudo-independent.

**Rank-based monotone polynomial.** Recall that we want to show a monotone Boolean circuit lower bound for a function of the form $f_P : \{0,1\}^m \to \{0,1\}$, where $P$ is a monotone polynomial and $f_P(x) = 1 \iff P(x) > 0$. Given an infinite sequence of matrices $(M_m)$ where $M_m \in \mathbb{R}^{n \times m}$ with $n \leq m$ (here $n$ is a parameter that grows with $m$), we define a sequence of multilinear polynomials with non-negative real coefficients as follows. For each $m$,

$$P_m(x_1, \ldots, x_m) := \sum_{S \in \binom{[m]}{n}} \det(M_m[S])^2 \cdot \prod_{i \in S} x_i$$

where $M_m[S]$ denotes the $n \times n$ submatrix obtained by keeping only the columns indexed by $S$ (in increasing order). Using Cauchy-Binet formula, it can be observed that the polynomial family can be computed by a uniform family of circuits if the matrix sequence is explicit [CFM+26].

Note that the function $f := f_{P_m}$ satisfies $f(1_S) = 1 \iff M_m[S]$ is full-rank, where $1_S$ is the indicating vector of a set columns $S \subseteq [m]$. For simplicity, henceforth we denote $M_m$ by $M$.

**Exponential monotone lower bounds via the approximation method.** To show a lower bound for $f$, we employ a monotone circuit lower bound criterion from [CFM+26] that reduces monotone circuit lower bounds to robust sunflower bounds. The criterion states that it suffices to define a no-distribution $\mathcal{D}_0$ and a yes-distribution $\mathcal{D}_1$ over the inputs $\{0,1\}^m$ with the following properties:

1. The distribution $\mathcal{D}_1$ must be $Q$-*spread*: $\Pr_{x\sim\mathcal{D}_1}[\bigwedge_{i\in A} x_i = 1] \leq Q^{-|A|}$, for every $A \subseteq [m]$;

2. Any monotone DNF with at least $r^\ell$ terms of width $\ell \in [t]$ must contain a $(\mathcal{D}_0, m^{-3t})$-sunflower; and

3. $\Pr_{b\sim\{0,1\},x\sim\mathcal{D}_b}[f(x) = b] = \Omega(1)$.

This results in a monotone circuit lower bound which is roughly $(Q/r)^{\Omega(t)}$.

In order to construct distributions $\mathcal{D}_1$ and $\mathcal{D}_0$ satisfying the above properties, we will need the columns of the matrix $M$ to have the following properties (informally described):

1. *Linear-algebraic expansion*: given any subspace $U$ spanned by a sub-collection of the columns, the chance that a uniformly chosen column vector will be outside of $U$ is high;

2. *Design property:* any pair of columns should intersect only at a few locations in their supports.

Property (1) allows us to show that a random set of $\approx n \log n$ columns from $M$ is very likely to be full-rank: indeed, if we imagine we are sampling those columns one-by-one, the expansion property makes it unlikely that the next column is spanned by the previous columns. We thus get a distribution $\mathcal{D}_1$ of accepting inputs which is roughly $(m/(n \log n))$-spread as it is the behaviour of the distribution obtained by uniformly choosing $n \log n$ columns of $M$.

Property (2) allows us to show a robust sunflower bound for the following distribution $\mathcal{D}_0$: sample $u \in \{-1, +1\}^n$ uniformly at random, and let $x_i := 1$ if the inner-product $M[i] \cdot u$ is equal to 0 (over $\mathbb{R}$), and otherwise $x_i := 0$. Since all the column vectors whose indices are in the support of $x \sim \mathcal{D}_0$ lie in a random linear space of dimension $n - 1$, the function $f$ must reject $\mathcal{D}_0$.

To obtain a sunflower bound for $\mathcal{D}_0$, we would like to show that $\mathcal{D}_0$ is $(t, \varepsilon)$-pseudo-independent and apply Theorem 1.1. Every column in our construction of $M$ will have a support of size $s = n^{\Omega(1)}$. We use the design property to show that, for any set $S = \{c_1, \ldots, c_t\} \subseteq [m]$ of at most $t = s^{0.1}$ columns of $M$, the set

$$R = \bigcup_{i\neq j} (\mathrm{supp}(M[c_i]) \cap \mathrm{supp}(M[c_j]))$$

has size at most $s^{0.2}$. Thus, for any $b \in \{-1, +1\}^R$, conditioning on the event $\{u_R = b\}$ gives us that that the random bits $x_{c_i}, \ldots, x_{c_t}$ are independent (where $x \sim \mathcal{D}_0$). This means that $(\mathcal{D}_0)_S$ is a convex combination of product distributions and thus $\mathcal{D}_0$ is pseudo-independent. It only remains to estimate the marginal probabilities, but this can be done using standard calculations about one-dimensional random walks (sums of Rademacher random variables).

In our actual constructions, we will only be able to show Properties (1) and (2) for a subset $C \subseteq [m]$ of the columns such that $C = \Omega(m)$. The arguments above can then be easily adapted to show a lower bound for a restriction $g$ of $f$ that is defined only on the columns of $C$.

**Explicit construction of $M$.** The main challenge in the explicit construction is to balance the design property as well as the linear-algebraic expansion properties. Informally, the columns of the matrix are indexed by low-degree univariate polynomials over a finite field $\mathbb{F}_q$, and the rows are essentially indexed by $[q] \times [s]$, where $s$ is the sparsity parameter. The $((i,j), f)$-th entry is equal to 1 if and only if $f(j) = i$. Thus, the columns essentially encode the graph of the univariate polynomials $f$. The limited intersection property of the columns follows immediately from the low degree of the polynomials. However, the main novelty lies in proving the linear-algebraic expansion property. To this end, the key technical lemma we prove states that the space spanned by matrices obtained from the graphs of all functions is equal to the space spanned by matrices obtained from the graphs of low-degree polynomials with affine shifts. For the full technical details, we refer to Section 4.

### 1.3 Conclusions and Open Problems

**Improved derandomized sunflowers.** One of our main results is a robust sunflower bound for pseudo-independent distributions, which also achieves better seed-length in the setting of bounded independence. Our results go beyond what is possible with the best known bounds for fooling DNFs using $k$-wise independent distributions [Tal17], and it is natural to ask whether they are tight:

**Question 1.** Is it possible to show better bounds on the size of width-$w$ monotone DNFs without $(\mathcal{D}, \delta)$-sunflowers, where $\mathcal{D}$ is $t$-wise independent with marginal probability $q$?

Inspired by the optimal robust sunflower bounds [ALWZ21, Rao20, BCW21], we conjecture that the right bound for width-$w$ DNFs is $O(\frac{1}{q} \cdot \log(w/\delta))^w$, for some $t = \widetilde{O}(w + \log(1/\delta))$. If this is true, then we can obtain $2^{\tilde{\Omega}(\sqrt{n})}$ monotone Boolean circuit lower bounds for a Boolean function in **P** (in fact, even in **NC**), matching the best known lower bounds for a function in **NP** [CKR22]. Hopefully some of our ideas can a provide a starting point for this direction.

**New applications of derandomized sunflowers.** As an application of our derandomization of sunflowers and our explicit construction via Nisan-Wigderson designs, we significantly improved known separations between general arithmetic circuits and the radical of monotone circuits. Our bounds are obtained via the framework of [CFM+26], which established a connection between sunflower bounds for weakly-independent distributions,

matrices with pseudorandom properties, and monotone Boolean lower bounds. Given the wide range of applications for sunflowers in theoretical computer science, we ask whether our new bounds can be used to improve other applications:

**Question 2.** Can derandomized sunflower bounds find applications in other contexts where robust sunflowers are typically applied? In particular, could they have impact on lifting theorems in communication complexity [LMM+22, Kel21]?

**Further radical lower bounds.** This paper introduced the notion of the radical $\sqrt{\mathcal{C}}$ of a complexity class $\mathcal{C}$, which was briefly mentioned in the work of Hrubeš and Yehudayoff [HY21]. This concept is also interesting from the (nonmonotone) point of view of white-box PIT algorithms, factoring, and algebraic hardness vs. randomness. For these settings, the most interesting regime is when the degree of the powers are bounded by a polynomially growing function on the number of variables, and many known closure of factoring results imply that the bounded-degree radical of a class $\mathcal{C}$ is equal to $\mathcal{C}$ [Kal87, BKR+26]. It is an open question is this area to understand whether the same closure results are true when the degree can be bounded by an exponentially growing function in the number of variables. For example, see Conjecture 8.3 in [Bür00] and the historical overview in [DSS18]. We believe it would be interesting to understand the relationship between $\sqrt{\mathcal{C}}$ and $\mathcal{C}$ for nonmonotone classes, specially with respect to the algorithmic prospects of the notion of radical mentioned in the introduction of this paper.

For the monotone setting, we ask whether our separations can be improved:

**Question 3.** Can we improve our lower bounds for the radical of monotone arithmetic circuits? In particular, is there a technique for proving such bounds that does not rely on monotone Boolean lower bounds?

The main motivation for the second question is to avoid the long-standing problem of proving $2^{\Omega(n)}$ lower bounds for monotone Boolean circuits computing a function in **NP**, and the potential limitations of the known techniques for proving monotone Boolean circuit lower bounds [CKR22].

The motivation for the first question is to understand whether there is a radical analogue of the $2^{\Omega(n)}$-lower bound for monotone circuits computing a polynomial computed by depth-3 circuits obtained by [CFM+26]. This question is related to common hardness escalation phenomena in algebraic complexity: a priori, it could be the case that any depth-3 arithmetic circuit of size $n^{O(1)}$ computing an $n$-variate monotone polynomial $P$ has a power $k \in \mathbb{N}$ such that $P^k$ has a monotone circuit of size $2^{O(\sqrt{n})}$. This would be a quite surprising result, however many of the known lower bound techniques in algebraic complexity consist in lifting a lower bound for a restricted model of computation to a more general model via a nontrivial relationship between the complexity measures.

Note that our superpolynomial separation between constant-depth arithmetic circuits and the radical of monotone circuits rules out the existence of a polynomially-sized conversion of constant depth circuits into the radical of monotone circuits.

### 1.4 Organization of the Paper

The rest of the paper is organized as follows. Section 2 proves our derandomization of robust sunflower lemma via the method of moments. Section 3 uses our improved sunflower bounds to obtain better separation between nonmonotone arithmetic circuits and the radical of monotone circuits. Section 4 analyses a linear-algebraic expansion property of Nisan-Wigderson designs, which is used in Section 3 to obtain an explicit construction of our nonmonotone circuit upper bounds.

## 2 Robust Sunflower Bounds via the Method of Moments

The main goal of this section is to obtain sunflower bounds (Corollary 2.11) for pseudo-independent distributions. We start by recalling a few definitions.

**Definition 2.1.** For $r > 1$, we say that a DNF $\mathcal{F}$ with $N$ terms is *$r$-spread* if, for any subset $S$ of variables, the number of terms of $\mathcal{F}$ containing all the variables from $S$ is at most $N \cdot r^{-|S|}$. For a term $F$ of the DNF $\mathcal{F}$, we use $\mathrm{Vars}(F)$ to denote the set of variables appearing in $F$. We say $\mathcal{F}$ is *monotone* if every term only has positive literals. ◀

Note that throughout this paper we interpret set systems over $[n]$ as monotone DNFs over the variables $x_1, \ldots, x_n$, where each set $S$ in the system corresponds to a term $\bigwedge_{i \in S} x_i$ in the DNF.

**Definition 2.2.** We say that a distribution $\mathcal{D}$ on $\{0,1\}^n$ is *$(t, \varepsilon)$-pseudo-independent with marginal probability $q$* if, for any set $S \subseteq [n]$ of at most $t$ coordinates, the marginal distribution $\mathcal{D}_S$ on $\{0,1\}^S$ is a convex combination of distributions, each of which is a product distribution on $\{0,1\}^S$ with the marginal distribution on each coordinate $i \in S$ being a Boolean random variable that is set to 1 with probability $q'_i \in [q \cdot (1-\varepsilon), q \cdot (1+\varepsilon)]$. ◀

We now state the main combinatorial theorem of this paper.

**Theorem 2.3** (Spread lemma for pseudo-independent distributions)**.** The following holds for every $0 < q, \varepsilon < 1$ and $w, t \in \mathbb{N}$ and $r > 1$ as long as $w \leq t$ and $\varepsilon \leq \gamma / w$ for small enough constant $\gamma > 0$. Let $\mathcal{F}$ be an $r$-spread monotone $w$-DNF on $n$ variables with $N$ terms $F_1, \ldots, F_N$, each having width exactly $w$. If $\mathcal{D}$ is an $(t, \varepsilon)$-pseudo-independent distribution with marginal probability $q$, then

$$\Pr_{x \sim \mathcal{D}} [\mathcal{F}(x) = 0] \leq \exp(-\Omega(\min\{t/w, rq/w\})),$$

where $\Omega(\cdot)$ hides an absolute constant.

**Remark 2.4.** The only place we use monotonicity is where we argue that each term is satisfied on a random input with probability $q^w$. This also holds for *non-monotone* DNFs in the case $q = 1/2$. Thus our proof also works in that setting. We omit the details. Alternatively, a reduction can be found in [LMM+22, Claim 2.3].

We present a proof overview of Theorem 2.3 in Section 2.1, followed by its proof in Section 2.2. Then, in Section 2.3, we obtain sunflower bounds for pseudo-independent distributions as a corollary of Theorem 2.3.

## 2.1 Proof Idea

We want to upper bound

$$\Pr_x [\mathcal{F}(x) = 0]$$

for $x$ being a element of $\{0,1\}^n$ sampled according to $\mathcal{D}$. We will prove this by computing a high enough moment of an associated random variable.

Assume that $x$ is sampled according to distribution $\mathcal{D}$. For every $i \in [N]$, let

$$Y_i(x) := 1_{\{F_i(x)=1\}}, \text{ and } \alpha := q^w, \text{ and } X_i := Y_i - \alpha,$$

and let

$$X := \sum_{i\in[N]} X_i, \text{ and } Y := \sum_{i\in[N]} Y_i, \text{ and } \mu := N\alpha. \tag{1}$$

For every even $p \in \mathbb{N}$, we know that

$$\Pr_x [\mathcal{F}(x) = 0] = \Pr_x [X = -\mu] \leq \Pr_x [X^p \geq \mu^p] \leq \frac{\mathbb{E}[X^p]}{\mu^p},$$

so all we have to do is to obtain a good estimate for the $p$-th moment $\mathbb{E}[X^p]$ of $X$. We will obtain such an estimate in two steps.

1. For any $s \in \mathbb{N}$ and $i_1, \ldots, i_s \in [N]$, define

   $$S_{i_1,\ldots,i_s} := \left| \mathbb{E}\left[ \prod_{j=1}^{s} X_{i_j} \right] \right|.$$

   We will first obtain, for any $i_1, \ldots, i_p \in [N]$, an upper bound on $S_{i_1,\ldots,i_p}$ based on the dependency structure of the underlying terms. This requires the underlying distribution $\mathcal{D}$ to be $pw$-wise independent (eventually, we will fix $p \leq t/w$, so $(t,\varepsilon)$-pseudo-independence is enough).

2. Bound

   $$\mathbb{E}[X^p] = \sum_{i_1,\ldots,i_p\in[N]} \mathbb{E}\left[ \prod_{j=1}^{s} X_{i_j} \right]$$

   by a suitable covering argument applied to all the terms of the above form $S_{i_1,\ldots,i_p}$. In particular, we partition the terms $S_{i_1,\ldots,i_p}$ using the partition of $[p]$ induced by the dependency graph corresponding to the terms $F_{i_1}, \ldots, F_{i_p}$. This is where the $r$-spreadness of $\mathcal{F}$ will be used, along with a careful analysis of the number of such partitions with specified statistics.

## 2.2 Proof of Theorem 2.3

We now begin the formal argument with an execution of Step 1 in the above proof sketch. Let

$$p := ct/w$$

for a sufficiently small constant $c \in \mathbb{R}$ to be defined later.

**Definition 2.5.** For any $(i_1, \ldots, i_s) \in [N]^s$, let the *dependency graph* $G_{i_1,\ldots,i_s}$ of $(i_1, \ldots, i_s)$ be an undirected graph with vertex set $[s]$ and edges between distinct $a, b \in [s]$ if and only if $F_{i_a}$ and $F_{i_b}$ share a variable. ◀

**Lemma 2.6** (A basic bound for $S_{i_1,\ldots,i_s}$)**.** Assume $p \leq t/w$ and $s \in [p]$. Fix any $(i_1, \ldots, i_s) \in [N]^s$. The following hold:

- If $s = 1$, then $S_{i_1} \leq \alpha \cdot 2\varepsilon w$.
- If $1 < s \leq p$, then

$$S_{i_1,\ldots,i_s} \leq \alpha^s \cdot 4^s \cdot \prod_{j=1}^{s} \left(\frac{1}{q}\right)^{|\mathrm{Vars}(F_{i_j}) \cap \mathrm{Vars}(F_{i_1,\ldots,i_{j-1}})|},$$

  where $\mathrm{Vars}(F_{i_1,\ldots,i_{j-1}})$ denotes $\mathrm{Vars}(F_{i_1}) \cup \mathrm{Vars}(F_{i_2}) \cup \cdots \cup \mathrm{Vars}(F_{i_{j-1}})$ if $j > 1$, and $\varnothing$ otherwise.

*Proof of Lemma 2.6.* We start with the case $s = 1$. In this case

$$S_{i_1} = |\mathbb{E}[X_{i_1}]| = \left| \Pr_{x \sim \mathcal{D}} [Y_{i_1} = 1] - \alpha \right| \tag{2}$$

Since $t \geq w = |\mathrm{Vars}(F_{i_1})|$ and the distribution $\mathcal{D}$ is $(t, \varepsilon)$-pseudo-independent, it suffices to bound the above expression for each product distribution $\mathcal{D}'$ on $\{0,1\}^{\mathrm{Vars}(F_{i_1})}$ where each coordinate $a$ is set to 1 with probability $q_a \in [q(1-\varepsilon), q(1+\varepsilon)]$. For such a $\mathcal{D}'$, it follows that

$$\Pr_{x \sim \mathcal{D}'} [Y_{i_1} = 1] \leq q^w (1+\varepsilon)^w \leq \alpha \cdot (1 + 2\varepsilon w)$$

since $\varepsilon \leq \gamma/w$ and the constant $\gamma$ is small enough. Similarly, we also get

$$\Pr_{x \sim \mathcal{D}'} [Y_{i_1} = 1] \geq \alpha \cdot (1 - 2\varepsilon w).$$

By plugging these bounds into (2), we obtain that $S_{i_1} \leq \alpha \cdot 2\varepsilon w$.

From now on, we assume that $s \geq 2$. For notational simplicity, we assume $i_j = j$ for each $j \in [s]$. We note that

$$\begin{aligned} S_{1,\ldots,s} &= \left| \mathbb{E}\left[\prod_{j=1}^{s}(Y_j - \alpha)\right]\right| \leq \sum_{T\subseteq[s]} \alpha^{s-|T|} \cdot \left|\mathbb{E}\left[\prod_{j\in T} Y_j\right]\right| \\ &= \sum_{T\subseteq[s]} \alpha^{s-|T|} \cdot \Pr_{x\sim\mathcal{D}}\left[\bigwedge_{j\in T} F_j(x) = 1\right] \\ &\leq 2^s \cdot \max_{T\subseteq[s]} \left(\alpha^{s-|T|} \cdot \Pr_{x\sim\mathcal{D}}\left[\bigwedge_{j\in T} F_j(x) = 1\right]\right). \end{aligned}$$

Fix any $T := \{j_1, \ldots, j_t\} \subseteq [s]$. Since $\mathcal{D}$ is $(t,\varepsilon)$-pseudo-independent and

$$t \geq pw \geq sw \geq \left|\bigcup_{j\in T} \mathrm{Vars}(F_j)\right|,$$

it suffices to bound the above for a product distribution $\mathcal{D}'$ on $\{0,1\}^{\bigcup_{j\in T}\mathrm{Vars}(F_j)}$ where each coordinate $a$ is set to 1 with probability $q_a \in [q(1-\varepsilon), q(1+\varepsilon)]$. For such a distribution $\mathcal{D}'$, we have

$$\begin{aligned} \Pr_{x\sim\mathcal{D}'}\left[\bigwedge_{j\in T} F_j(x) = 1\right] &\leq (q(1+\varepsilon))^{|\bigcup_{j\in T}\mathrm{Vars}(F_j)|} && (3) \\ &\leq (1+\varepsilon)^{tw} \cdot q^{|\bigcup_{j\in T}\mathrm{Vars}(F_j)|} \\ &\leq 2^t \cdot q^{|\bigcup_{j\in T}\mathrm{Vars}(F_j)|} && (4) \\ &= 2^t \cdot q^{\sum_{k=1}^{t}|\mathrm{Vars}(F_{j_k})| - |\mathrm{Vars}(F_{j_k})\cap\mathrm{Vars}(F_{j_1,\ldots,j_{k-1}})|} \\ &= 2^t q^{tw} \cdot \prod_{k=1}^{t}\left(\frac{1}{q}\right)^{|\mathrm{Vars}(F_{j_k})\cap\mathrm{Vars}(F_{j_1,\ldots,j_{k-1}})|} \\ &\leq 2^t\alpha^t \cdot \prod_{j=1}^{s}\left(\frac{1}{q}\right)^{|\mathrm{Vars}(F_j)\cap\mathrm{Vars}(F_{1,\ldots,j-1})|} \\ &\leq 2^s\alpha^t \cdot \prod_{j=1}^{s}\left(\frac{1}{q}\right)^{|\mathrm{Vars}(F_j)\cap\mathrm{Vars}(F_{1,\ldots,j-1})|}, \end{aligned}$$

where (4) follows from $(1+\varepsilon)^w \leq (1+2\varepsilon w) \leq (1+2\gamma) \leq 2$ as above for $\gamma$ small enough. Since we bounded the above for any product distribution $\mathcal{D}'$ with the prescribed marginals, we have the same bound for the distribution $\mathcal{D}$. Plugging this bound into the upper bound for $S_{i_1,\ldots,i_s}$ above yields the lemma. ■

We now extend the bound from Lemma 2.6 to sum over all $(i_1, \ldots, i_s) \in [N]^s$ with a connected dependency graph. This is where we will use the spreadness of the DNF.

**Lemma 2.7** (The sum over connected $(i_1, \ldots, i_s)$)**.** Assume $p \leq \min\{t/w, qr/10w\}$. The following hold:

- If $s = 1$, then
$$\sum_{i_1 \in [N]^s} S_{i_1} \leq N\alpha \cdot 2 \cdot \varepsilon w.$$
- If $1 < s \leq p$, then
$$\sum_{\substack{(i_1,\ldots,i_s)\in[N]^s \\ G_{i_1,\ldots,i_s} \text{ connected}}} S_{i_1,\ldots,i_s} \leq (N\alpha)^s \cdot 2^{O(s)} \cdot \left(\frac{sw}{rq}\right)^{s-1}.$$

*Proof of Lemma 2.7.* The case $s = 1$ is immediate from Lemma 2.6 above since there are at most $N$ choices for $i_1$. For the rest of the lemma we assume that $s > 1$. For a given $(i_1, \ldots, i_s)$, define the *intersection pattern* $L_{i_1,\ldots,i_s}$ of $(i_1, \ldots, i_s)$ to be

$$L_{i_1,\ldots,i_s} := (\ell_2, \ldots, \ell_s),$$

where $\ell_j := |\mathrm{Vars}(F_{i_j}) \cap \mathrm{Vars}(F_{i_1,\ldots,i_{j-1}})|$.

We will partition the sum in the lemma statement based on the intersection patterns. For any fixed intersection pattern $L := (\ell_2, \ldots, \ell_s)$, we have by Lemma 2.6 above that

$$\sum_{\substack{(i_1,\ldots,i_s) \\ L_{i_1,\ldots,i_s}=L}} S_{i_1,\ldots,i_s} \leq \alpha^s \cdot 4^s \cdot \left(\frac{1}{q}\right)^{\ell_2+\cdots+\ell_s} \cdot N(L) \tag{5}$$

where $N(L)$ denotes the number of $(i_1, \ldots, i_s) \in [N]^s$ such that $L_{i_1,\ldots,i_s} = L$.

We can bound $N(L)$ using the spreadness of the DNF $\mathcal{F}$. More precisely, given $L$, the number of ways of choosing an $(i_1, \ldots, i_s)$ such that $L_{i_1,\ldots,i_s} = L$ is at most

$$N \cdot \prod_{j=2}^{s} \left( \binom{(j-1)w}{\ell_j} \cdot N \cdot r^{-\ell_j} \right)$$

where:

- the first $N$ is the number of ways of choosing $i_1$, and
- for each $j > 1$, the $j$th term in the product is the number of ways of choosing $i_j$ given $i_1, \ldots, i_{j-1}$. Here, we use the spreadness of $\mathcal{F}$: to choose $i_j$, we can first fix some subset $V$ of size $\ell_j$ of $\mathrm{Vars}(F_{i_1}) \cup \cdots \cup \mathrm{Vars}(F_{i_{j-1}})$, which can be done in at most $\binom{(j-1)w}{\ell_j}$ ways; and then choosing a term that contains $V$, which can be done in at most $N \cdot r^{-\ell_j}$ ways using the spreadness property of $\mathcal{F}$.

Plugging the above bound into (5) we get

$$\begin{aligned}\sum_{\substack{(i_1,\dots,i_s)\in[N]^s:\\ L_{i_1,\dots,i_s}=L}} S_{i_1,\dots,i_s} &\le N^s\alpha^s\cdot 4^s\cdot\left(\frac{1}{q}\right)^{\ell_2+\cdots+\ell_s}\cdot\prod_{j=2}^{s}\left(\binom{(j-1)w}{\ell_j}\cdot r^{-\ell_j}\right)\\ &\le N^s\alpha^s\cdot 4^s\cdot\prod_{j=2}^{s}\left(\frac{1}{q^{\ell_j}}\cdot((j-1)w)^{\ell_j}\cdot r^{-\ell_j}\right)\\ &= N^s\alpha^s\cdot 4^s\cdot\prod_{j=2}^{s}\left(\frac{(j-1)w}{qr}\right)^{\ell_j}.\end{aligned}$$

Moreover, for $v := \sum_{i=2}^{s}\ell_i$, we have

$$\begin{aligned}\sum_{\substack{(i_1,\dots,i_s)\in[N]^s:\\ L\le L_{i_1,\dots,i_s}=:(v_2,\dots,v_s)}} S_{i_1,\dots,i_s} &\le N^s\alpha^s\cdot 4^s\cdot\sum_{L\le(v_2,\dots,v_s)\in\mathbb{N}^s}\prod_{j=2}^{s}\left(\frac{(j-1)w}{qr}\right)^{v_j}\\ &\le N^s\alpha^s\cdot 4^s\cdot\prod_{j=2}^{s}\sum_{v_j=\ell_j}^{\infty}\left(\frac{(j-1)w}{qr}\right)^{v_j}\\ &\le N^s\alpha^s\cdot 4^s\cdot\prod_{j=2}^{s}\left(\frac{2(j-1)w}{qr}\right)^{\ell_j}\\ &\le N^s\alpha^s\cdot 4^s\cdot\left(\frac{2sw}{qr}\right)^{\sum_{i=2}^{s}\ell_i}\\ &\le N^s\alpha^s\cdot 4^s\cdot\left(\frac{2sw}{qr}\right)^{v}.\end{aligned}$$

where the third inequality used the assumption that $s\le p\le qr/10w$ to deduce that each term of the product is a geometric progression with common ratio less than $1/2$.

Note that, for every $i\in[N]^s$ such that $G_i$ is connected, the intersection pattern $L_i\in\mathbb{N}^s$ of $i$ satisfies

$$L_i\ge L \text{ for some } L\in\left\{(\ell_2,\dots,\ell_s)\in\mathbb{N}^s\;\middle|\;\sum_{i=2}^{s}\ell_i=s-1\right\}=:\mathcal{L}_{\min},$$

since every connected graph contains a spanning tree as subgraph and the patterns in $\mathcal{L}_{\min}$ correspond to patterns of spanning trees. Furthermore,

$$|\mathcal{L}_{\min}|=\binom{s-1+s-1-1}{s-1}\le 2^{O(s)}.$$

Hence, we obtain

$$\begin{aligned}\sum_{\substack{(i_1,\ldots,i_s)\in[N]^s:\\ G_{i_1,\ldots,i_s}\text{ connected}}} S_{i_1,\ldots,i_s} &\le \sum_{(\ell_2,\ldots,\ell_s):=L\in\mathcal{L}_{\min}} \sum_{\substack{(i_1,\ldots,i_s)\in[N]^s:\\ L\le L_{i_1,\ldots,i_s}}} S_{i_1,\ldots,i_s} \\ &\le 2^{O(s)}\cdot\left(N^s\alpha^s\cdot 4^s\cdot\left(\frac{2sw}{qr}\right)^{s-1}\right) \\ &\le N^s\alpha^s\cdot 2^{O(s)}\cdot\left(\frac{sw}{qr}\right)^{s-1}\end{aligned}$$

■

**Definition 2.8.** Let $(i_1,\ldots,i_p)\in[N]^p$ be a tuple with a possibly disconnected dependency graph $G_{(i_1,\ldots,i_p)}$. For an unordered partition of $\pi := \{A_1,\ldots,A_m\}$ of the set $[p]$, we say that the tuple $(i_1,\ldots,i_p)$ is *$\pi$-consistent* if the connected components of $G_{(i_1,\ldots,i_p)}$ are $A_1,\ldots,A_m$. We use $\mathcal{C}_\pi$ to denote the set of $\pi$-consistent tuple $(i_1,\ldots,i_p)$. For a set $A := \{j_1,\ldots,j_s\}\subseteq[p]$ with $j_1<\cdots<j_s$, we use $i_A$ to denote the tuple $(i_{j_1},\ldots,i_{j_s})$. ◀

**Lemma 2.9** (Sum over $\pi$-consistent $(i_1,\ldots,i_p)$)**.** Assume $p\le\min\{t/w, qr/10w\}$. Fix any unordered partition $\pi := \{A_1,\ldots,A_m\}$ of $[p]$, and let $a_j := |A_j|$ for each $j\in[m]$. Let $c_1$ denote the number of singletons in $\pi$, that is, number of $j\in[m]$ such that $a_j=1$. Then, we have

$$\sum_{(i_1,\ldots,i_p)\in\mathcal{C}_\pi} S_{i_1,\ldots,i_p} \le \mu^p\cdot 2^{O(p)}\cdot(\varepsilon w)^{c_1}\cdot\left(\frac{pw}{rq}\right)^{p-m}$$

where $\mu = N\alpha$ (as in Equation 1).

*Proof of Lemma 2.9.* Without loss of generality, we may assume that $a_j=1$ for $j\le c_1$ and $a_j>1$ for $j>c_1$.

Fix any $(i_1,\ldots,i_p)\in\mathcal{C}_\pi$. Note that

$$S_{i_1,\ldots,i_p} = S_{i_{A_1}}\cdots S_{i_{A_m}}$$

by the independence of the variables $(X_{i_j} : j\in A_k)$ and $(X_{i_{j'}} : j'\in A_{k'})$ for any $k\ne k'$.

Using independence across $A_1, \ldots, A_m$ and using Lemma 2.7, we see that

$$\begin{aligned}
\sum_{(i_1,\ldots,i_p)\in\mathcal{C}_\pi} S_{i_1,\ldots,i_p} &= \sum_{\substack{(i_1,\ldots,i_p)\in[N]^p \\ G(i_{A_j}) \text{ connected } \forall j}} S_{i_{A_1}} \cdots S_{i_{A_m}} \\
&= \prod_{j=1}^{c_1} \left( \sum_{i_j \in [N]} S_{i_j} \right) \cdot \prod_{j=c_1+1}^{m} \left( \sum_{\substack{i_{A_j}\in[N]^{A_j} \\ G(i_{A_j}) \text{ connected}}} S_{i_{A_1}} \right) \\
&\leq (N\alpha)^{\sum_{j\in[m]} a_j} \cdot 2^{O(\sum_{j\in[m]} a_j)} \cdot (\varepsilon w)^{c_1} \left( \frac{a_j w}{rq} \right)^{\sum_{j>c_1}(a_j-1)} \\
&= (N\alpha)^p \cdot 2^{O(p)} \cdot (\varepsilon w)^{c_1} \cdot \left( \frac{pw}{rq} \right)^{p-m}.
\end{aligned}$$

Using the fact that $N\alpha = \mu$, we obtain the statement of the lemma. ■

Now we have all the auxiliary lemmas to prove Theorem 2.3.

*Proof of Theorem 2.3.* For any even integer $p$,

$$\Pr_x [\mathcal{F}(x) = 0] = \Pr_x [X = -\mu] \leq \Pr_x [X^p \geq \mu^p] \leq \frac{\mathbb{E}[X^p]}{\mu^p}. \tag{6}$$

We will set $p$ to be the largest even number such that

$$p \leq \min\{t/w, \eta(qr/w)\} \tag{7}$$

for a small enough constant $\eta > 0$.

To bound $\mathbb{E}[X^p]$, we proceed as follows:

$$\begin{aligned}
\mathbb{E}[X^p] = \mathbb{E}\left[ \sum_{(i_1,\ldots,i_p)\in[N]^p} X_{i_1} \cdots X_{i_p} \right] &\leq \sum_{(i_1,\ldots,i_p)\in[N]^p} S_{i_1,\ldots,i_p} \\
&= \sum_{m=1}^{p} \sum_{c_1=\max\{0,m-p/2\}}^{m} \sum_{\substack{\pi=\{A_1,\ldots,A_m\}: \\ \pi \text{ has } c_1 \text{ singletons}}} \sum_{(i_1,\ldots,i_p)\in\mathcal{C}_\pi} S_{i_1,\ldots,i_p},
\end{aligned}$$

where we are using above that for any partition with $m$ parts, there must be at least $m - p/2$ parts of size 1.

Applying Lemma 2.9 to bound each inner sum, we obtain

$$\mathbb{E}[X^p] \le \sum_{m=1}^{p} \sum_{c_1=\max\{0,m-p/2\}}^{m} \sum_{\substack{\pi=\{A_1,\dots,A_m\}:\\ \pi \text{ has } c_1 \text{ singletons}}} \mu^p \cdot 2^{O(p)} \cdot \left(\frac{pw}{rq}\right)^{p-m} \cdot (\varepsilon w)^{c_1}$$

$$\le \mu^p 2^{O(p)} \cdot \sum_{m=1}^{p} \left(\frac{pw}{rq}\right)^{p-m} \cdot \sum_{c_1=\max\{0,m-p/2\}}^{m} (\varepsilon w)^{c_1} \tag{8}$$

We bound the above quantities based on the value of $m$. First recall that $\varepsilon \le \gamma/w$ for a small enough constant $\gamma > 0$.

For $m \le p/2$, we note that the inner sum is bounded by an absolute constant, so we obtain

$$\sum_{m=1}^{p/2} \left(\frac{pw}{rq}\right)^{p-m} \cdot \sum_{c_1=\max\{0,m-p/2\}}^{m} (\varepsilon w)^{c_1} \le O\left(\sum_{m=1}^{p/2} \left(\frac{pw}{rq}\right)^{p-m}\right) \le O\left(\eta^{p/2}\right),$$

where the last inequality follows from Equation 7. For $m > p/2$, the inner sum is bounded by $O\left((\varepsilon w)^{m-p/2}\right)$, so we obtain

$$\sum_{m=p/2+1}^{p} \left(\frac{pw}{rq}\right)^{p-m} \cdot \sum_{c_1=\max\{0,m-p/2\}}^{m} (\varepsilon w)^{c_1} \le O\left(\sum_{m=p/2+1}^{p} \left(\frac{pw}{rq}\right)^{p-m} \cdot (\varepsilon w)^{m-p/2}\right)$$

$$\le O\left(p \cdot (\eta+\gamma)^{p/2}\right)$$

where we used the fact that $p \le \eta(rq/w)$ and $\varepsilon \le \gamma/w$ for the final inequality.

Using the above bounds in (8), we obtain

$$\mathbb{E}[X^p] \le \mu^p 2^{O(p)} \cdot (\eta+\gamma)^{p/2} = \mu^p \cdot \exp(-\Omega(p))$$

as long as $\eta, \gamma$ are small enough constants. Plugging the above bounds into (6), we obtain

$$\Pr_x[\mathcal{F}(x) = 0] \le \exp(-\Omega(p)) = \exp(-\Omega(\min\{t/w, rq/w\})).$$

■

### 2.3 Sunflower Bounds for Pseudo-Independent Distributions

Following [CFM+26], we have the following definition:

**Definition 2.10.** We define a DNF $\mathcal{F}$ to be a $(\mathcal{D}, \delta)$-*sunflower* if

$$\Pr_{x\sim\mathcal{D}}[\mathcal{F}_\Delta(x) = 1] > 1 - \delta$$

where $\mathcal{F}_\Delta$ denotes the DNF obtained from $\mathcal{F}$ by setting all literals that appear in *all the terms* of $\mathcal{F}$ to 1. ◀

Theorem 2.3 along with a standard argument now implies the following sunflower bound.

**Corollary 2.11** (Theorem 1.1)**.** There is an absolute constant $\theta_0$ so that the following holds. Let $r, q, w, \delta$ be such that $\delta \geq \exp(-\theta_0(rq/w))$. Then, there exist parameters $t = \Theta(w \log(1/\delta))$ and $\varepsilon = \Theta(1/w)$ such that the following holds. For any $(t, \varepsilon)$-pseudo-independent distribution $\mathcal{D}$ with marginals probability $q$, any monotone DNF with at least $r^w$ terms of width exactly $w$ contains a $(\mathcal{D}, \delta)$-sunflower.

*Proof.* Without loss of generality, assume the DNF $\mathcal{F}$ has exactly $N := r^w$ terms $F_1, \ldots, F_N$ of width $w$. Let $\theta_0$ be the absolute constant in the exponent of the concluding statement of Theorem 2.3. For $t := \frac{w \log(1/\delta)}{\theta_0}$, we obtain

$$\min\{t/w, rq/w\} \geq \frac{\log(1/\delta)}{\theta_0}, \tag{9}$$

as $\delta \geq \exp(-\theta_0(rq/w)))$.

If $\mathcal{F}$ is $r$-spread, the result follows immediately from Inequality (9) and Theorem 2.3. Suppose then $\mathcal{F}$ is not $r$-spread. Let $S$ be a maximal set witnessing a "spreadness violation", i.e., a set such that $\mathcal{F}_S := \{F_i \setminus S : S \subseteq F_i\}$ satisfies $|\mathcal{F}_S| \geq r^{w-|S|}$. Note that $\mathcal{F}_S$ is $r$-spread, otherwise $S$ would not be maximal. By Inequality (9) and Theorem 2.3, we get that $\mathcal{F}_S$ is a $(\mathcal{D}, \delta)$-sunflower, which implies that $\{F_i : S \subseteq F_i\}$ is a $(\mathcal{D}, \delta)$-sunflower in $\mathcal{F}$. ■

**Remark 2.12.** A near-identical argument also shows the same is true for non-monotone DNFs in the case $q = 1/2$. Again check [LMM+22, Claim 2.3] for details.

# 3 Improved Separations for the Radical of Monotone Circuits

The main theorem of this section is the following.

**Theorem 3.1** (Theorem 1.2)**.** There is an infinite sequence $(P_m(x_1, \ldots, x_m))_{m \in \mathbb{N}}$ of polynomials such that the following hold:

1. (Explicit Upper bound) $P_m$ is a monotone multilinear polynomial with an arithmetic circuit $C_m$ of size $m^{O(1)}$. Further, given $m$, the circuit $C_m$ can be computed in deterministic time $m^{O(1)}$.

2. (Radical Lower bound) Any monotone arithmetic circuit computing a power of $P_m$ must have size at least $\exp(m^{\Omega(1)})$.

This improves the result of [CFM+26] in two ways: it makes the upper bound uniform, and improves the separation from quasipolynomial to exponential. Furthermore, it allows us to obtain the first superpolynomial separation between nonmonotone constant-depth circuit and the radical of monotone circuits, via a subexponential depth-reduction for our upper bound.

**Corollary 3.2** (Corollary 1.3)**.** For every constant $k \geq 1$, there is an infinite sequence $(Q_M(x_1, \ldots, x_M))_{M \in \mathbb{N}}$ of polynomials such that the following hold:

1. $Q_M$ is a monotone multilinear polynomial with a depth $O(k)$ arithmetic circuit $C'_M$ of size $M^{O(1)}$. Further, given $M$, the circuit $C'_M$ can be computed in deterministic time $M^{O(1)}$.

2. Any monotone arithmetic circuit computing a power of $Q_M$ must have size at least $M^{\Omega((\log M)^k)}$.

*Proof.* By known depth reduction techniques [AV08, Koi12, Tav15, GKKS16], for any constant $\Delta \geq 3$, we can convert a circuit of size $m^{O(1)}$ computing a polynomial $P$ of degree $d$ into a depth-$\Delta$ circuit computing $P$ with size

$$2^{O(d^{1/(\Delta-1)} \cdot \log m)}.$$

Hence, the polynomial $P_m$ from Theorem 3.1 can be computed by a depth $\Delta$ circuit of size

$$s' \leq 2^{O(m^{2/\Delta})} = M_\Delta^{O(1)},$$

for $M_\Delta := 2^{m^{2/\Delta}}$. Moreover, by the radical lower bound in Theorem 3.1, there is a constant $c > 0$ such that any power of $P_m$ can only be computed by monotone circuits of size

$$2^{\Omega(m^c)}.$$

Let $\Delta := \lceil 4k/c \rceil$ and $M := M_\Delta$. We define $Q_M(x_1, \ldots, x_M)$ the padded version of $P_n$, that is,

$$Q_M(x_1, \ldots, x_M) := P_n(x_1, \ldots, x_n).$$

Then $Q_M$ can be computed by a constant depth circuit of size $M^{O(1)}$, and any power of $Q_M$ can only be computed by monotone circuits of size

$$2^{\Omega(m^c)} = M^{\Omega(\log M)^k}$$

implying the desired lower bound. ∎

**Organization.** Our proof of Theorem 3.1 is organized as follows. In Section 3.1, we recall the basic framework of [CFM+26]. We will use the same kind of 'matrix-rank' polynomial sequences based on a sequences of matrices $(M_m)$ as in [CFM+26] and thus our upper bounds will follow similarly. The separation is proved by a monotone *Boolean* circuit lower for an associated sequence of monotone Boolean functions $(f_m)$ and the proof of this is based on an abstract framework of [CFM+26] for proving such lower bounds.

In Section 3.2, we identify sufficient properties of the matrix sequence $M_m$ that allow us to use the [CFM+26] lower bound framework to prove an exponential monotone Boolean circuit lower bound. We improve upon the quasipolynomial lower bound of [CFM+26] because we are able to use our strong robust sunflower bounds (Corollary 2.11) for pseudo-independent distributions while the lower bound of [CFM+26] was based on the classical sunflower lemma for set-systems [ER60] which has worse parameters.

In Section 3.3, we state our results about constructing a sequence of matrices $(M_m)$ with the required properties from Section 3.2 in deterministic time $\mathrm{poly}(m)$. We use this construction to finish the proof of Theorem 3.1. The details of the construction are given in Section 4. Stated combinatorially, the columns of the matrices are a uniform family of sets that satisfy a combinatorial design property and furthermore satisfy a simple "linear-algebraic expansion" condition. We start with a well-known (see e.g. [Nis91, NW94]) construction of such set-systems based on graphs of low-degree polynomials and show that they have the required linear-algebraic properties. This latter fact may be independently interesting.

### 3.1 The Framework of [CFM+26]

**Matrix-rank polynomials.** Given an infinite sequence of matrices $(M_m)$ where $M_m \in \mathbb{R}^{n \times m}$ with $n \leq m$ (here $n$ is a parameter that grows with $m$), we define a sequence of multilinear polynomials with non-negative real coefficients as follows. For each $m$,

$$P_m(x_1, \ldots, x_m) := \sum_{S \in \binom{[m]}{n}} \det(M_m[S])^2 \cdot \prod_{i \in S} x_i$$

where $M_m[S]$ denotes the $n \times n$ submatrix obtained by keeping only the columns indexed by $S$ (in increasing order).

The following lemma was observed in [CFM+26] using known constructions of arithmetic circuits computing the determinant [Ber84, Mul87]. While it is not explicitly stated, it is easy to see that the construction yields a uniform family of circuits as long as the matrix sequence is explicit.

**Lemma 3.3** (Upper bound from [CFM+26])**.** For any matrix $M_m$, the polynomial $P_m(x_1, \ldots, x_m)$ can be computed by an arithmetic circuit $C_m$ of size $\mathrm{poly}(m)$ and depth $O((\log m)^2)$. Furthermore, there is a deterministic algorithm that, given as input the matrix $M_m$, produces the circuit $C_m$ in time $\mathrm{poly}(m)$.

**Radical lower bounds via Boolean circuit lower bounds.** For a monotone polynomial $P \in \mathbb{R}[x_1, \ldots, x_m]$, we define a corresponding Boolean function $f_P : \{0,1\}^m \to \{0,1\}$ by

$$f_P(x) = 1 \Leftrightarrow P(x) > 0.$$

For the monotone polynomial $P_m$ defined above, the corresponding Boolean function $f_m := f_{P_m}$ can be equivalently defined as

$$f_m(1_S) = 1 \Leftrightarrow \operatorname{rank}(M[S]) = n$$

where $1_S \in \{0,1\}^m$ denotes the indicator vector of $S \subseteq [m]$.

It is shown in [CFM+26] that there is a sequence of matrices $(M_m)$ such that the monotone arithmetic complexity of any power of $P_m$ is superpolynomial. To do this, they use the following observation (see also Remark 6.5 from [HY21]).

**Remark 3.4** ([CFM+26])**.** If $P^k$ has a monotone arithmetic circuit of size $s$, then $f_P$ has a monotone Boolean circuit of size $s$.

In particular, this observation reduces the problem of proving lower bounds on the monotone arithmetic circuit complexity of powers of $P_m^k$ to proving a lower bound on the monotone Boolean circuit complexity of the corresponding Boolean function $f_m$.

We will follow this strategy, and we prove our monotone Boolean circuit lower bound via an abstract framework for proving such lower bounds also from [CFM+26]. The framework is based on Razborov's approximation method [Raz85] and followup works based on robust sunflowers [Ros14, CKR22, CGR+26].

**Theorem 3.5** (Framework for monotone Boolean circuit lower bounds [CFM+26])**.** Let $m \in \mathbb{N}$ and let $f : \{0,1\}^m \to \{0,1\}$ be a monotone function. Fix parameters $t, Q, r \in \mathbb{N}$.

Assume that there exist probability distributions $\mathcal{D}_0, \mathcal{D}_1$ over $\{0,1\}^m$ such that

1. For any $T \subseteq [m]$ of size at most $t$,

$$\Pr_{x \sim \mathcal{D}_1}\left[\bigwedge_{i \in T} x_i = 1\right] \leq Q^{-|T|},$$

2. For some $w \leq t/2$ and any $\ell \in [2w]$, any monotone DNF with more than $r^\ell$ terms of width exactly $\ell$ contains a $(\mathcal{D}_0, \alpha m^{-3w})$-sunflower (Definition 2.10), where

$$\alpha := \min\left\{\Pr_{x \sim \mathcal{D}_0}[f(x) = 0], \Pr_{x \sim \mathcal{D}_1}[f(x) = 1]\right\}.$$

If $8r \leq Q \leq rm$, then any Boolean monotone circuit computing $f$ has size at least

$$\left(\frac{c\alpha Q}{r}\right)^w$$

where $c$ is a universal positive constant.

### 3.2 Monotone Lower Bounds from Properties of $(M_m)$

Fix a growing parameter $m$. For brevity we will use $M, P, f$ to denote the matrix $M_m$, the corresponding polynomial $P_m$ and the Boolean function $f_m$ respectively (as defined in Section 3.1).

In this section, we will show that if $M \in \mathbb{R}^{n\times m}$ has some suitable combinatorial and algebraic properties, then the corresponding Boolean function $f$ has high monotone Boolean circuit complexity. These properties are related to the definition of well-behaved matrix used by [CFM+26] to obtain their superpolynomial separation.

**Well-behaved matrices.** The following definition generalizes the notion of well-behaved matrix introduced by [CFM+26].

**Definition 3.6.** Fix a subset $C \subseteq [m]$ and define $V \subseteq \mathbb{R}^n$ to be the subspace spanned by the columns of $M$ indexed by $C$. For integer parameters $s, k$, we say that a rank-$n$ matrix $M \in \mathbb{R}^{n\times m}$ is $(C, s, k)$-*well-behaved* if the following conditions hold.

1. (Design property) Each column $v \in \{0,1\}^n$ indexed by $C$ is a $\{0,1\}$-vector with support $\mathrm{supp}(v) := \{\, i \in [n] \mid v_i \neq 0\}$ of cardinality $s$. Furthermore, for any distinct $i, j \in C$, there are at most $k$ indices where the corresponding columns $M[i]$ and $M[j]$ are both 1.

2. (Linear-algebraic expansion inside $V$) The subspace $V$ is non-zero and, given any vector subspace $U$ of $V$, we have

$$\Pr_{i\sim C}[M[i] \in U] \leq \frac{\dim(U)}{\dim(V)}.$$

◀

The main theorem of this section is the following.

**Lemma 3.7** (Lower bounds from well-behaved matrices)**.** Assume that $M$ is a $(C, s, k)$-well-behaved $n \times m$ matrix of rank $n$ with $s$ even, and that

$$\frac{s}{k^5} \geq m^{\Omega(1)}, \text{ and } s \leq \frac{|C|}{n \cdot m^{\Omega(1)}}.$$

Then, any monotone Boolean circuit computing $f$ has size at least $\exp(m^{\Omega(1)})$.

We will prove this theorem by applying the [CFM+26] framework (Theorem 3.5) to a restriction $g$ of $f$ and suitable distributions $\mathcal{D}_0$ and $\mathcal{D}_1$. The proof follows the ideas set forth in [CFM+26]. The technical part of the section will be to show that the distribution $\mathcal{D}_0$ is an $(t, \varepsilon)$- pseudo-independent distribution for suitable parameters $r$ and $\varepsilon$ so that we can apply Corollary 2.11 (which is necessary to obtain the sunflower bound in the hypothesis of Theorem 3.5).

**Restriction of $f$.** We start by defining the restriction $g$ of $f$ that we will consider. Fix $C, s, k$ as in the hypothesis of Lemma 3.7. Note that $|C| \geq nm^{\Omega(1)}$. As $M$ is rank $n$, there is a subset $C'$ of the columns of $M$ such that $C' \cap C = \varnothing$ and the columns $C'$ and $C$ together span the entire space $\mathbb{R}^n$. We fix the coordinates of the sampled point indexed by $[m] \setminus C$ as follows: $x_i = 1$ if $i \in C'$ and $x_i = 0$ if $i \in [m] \setminus (C \cup C')$. Under this setting, the function $f$ restricts to a monotone function $g$ on $m_1 := |C| = m^{\Omega(1)}$ variables. W.l.o.g. assume that $C = [m_1]$.

Clearly, the monotone Boolean circuit complexity of $g$ is at most that of $f$ and hence, it suffices to prove a lower bound for $g$.

Note also the following basic property of $g$, that follows directly from its definition and the fact that the columns of $M$ indexed by $C$ span the subspace $V$ of $\mathbb{R}^n$.

**Remark 3.8.** For any subset $S \subseteq [m_1]$,

$$g(1_S) = 1 \Leftrightarrow \operatorname{rank}(M[S \cup C']) = n \Leftrightarrow \text{the columns of } M \text{ indexed by } S \text{ span } V.$$

**Hard distributions.** We now define the distributions $\mathcal{D}_0$ and $\mathcal{D}_1$, which are defined similarly to the corresponding distributions in [CFM+26].

**Definition 3.9.** For the distribution $x \sim \mathcal{D}_1$: let $\lambda := 100n \log n$, and sample a set $I$ of $\lambda$ indices from $[m_1]$ independently and uniformly at random (i.e. $\lambda$ samples from $[m_1]$ with replacement); and define $x \in \{0,1\}^{m_1}$ as $x_i := 1$ for every $i \in I$, and $x_i := 0$ for every $i \in [m_1] \setminus I$.

For the distribution $x \sim \mathcal{D}_0$: we sample a uniformly random $u \in \{-1,1\}^n$, and define $x := x(u) \in \{0,1\}^{m_1}$ as, for each $i \in [m_1]$, we set $x(u)_i = 1$ if and only if the inner-product $M[i] \cdot u$ is zero over the reals. ◀

We now prove that these distributions have the required properties to apply Theorem 3.5.

### 3.2.1 Properties of $\mathcal{D}_1$

Our proofs of Lemmas 3.10 and 3.11 use essentially the same ideas from the corresponding lemmas in [CFM+26]. We postponed them to Appendix A.

**Lemma 3.10.** $\Pr_{x \sim \mathcal{D}_1}[g(x) = 1] \geq 1/2$.

**Lemma 3.11.** For any subset $T \subseteq [m_1]$, $\Pr_{x \sim \mathcal{D}_1}\left[\bigwedge_{i \in T} x_i = 1\right] \leq \left(\frac{m_1}{\lambda}\right)^{-|T|}$.

### 3.2.2 Properties of $\mathcal{D}_0$

**Lemma 3.12.** $\Pr_{x \sim \mathcal{D}_0}[g(x) = 0] \geq 1/2$.

*Proof.* First recall that, for every $i \in [m_1]$, we have that $M[i]$ is a Boolean vector of Hamming weight $s$, and, for every $S \subseteq [m_1]$,

$$g(1_S) = 1 \iff \text{span}\{\, M[i] \mid i \in [m_1]\} = V \subseteq \text{span}\{\, M[i] \mid i \in S\}.$$

Thus,

$$\begin{aligned}\Pr_{x\sim\mathcal{D}_0}[g(x)=1] &= \Pr_{x\sim\mathcal{D}_0}[\text{span}\{\, M[i] \mid i \in [m_1]\} \subseteq \text{span}\{\, M[i] \mid i \in [m_1], M[i]\cdot u = 0\}] \\ &\leq \Pr_{x\sim\mathcal{D}_0}[\forall i \in [m_1], M[i]\cdot u = 0] \leq \Pr_{x\sim\mathcal{D}_0}[M[1]\cdot u = 0]\,,\end{aligned}$$

and this lemma follows from the fact that, for every $i \in [m_1]$,

$$\begin{aligned}\Pr_{x\sim\mathcal{D}_0}[M[i]\cdot u = 0] &= \frac{|\{\, u \in \{-1,1\}^n \mid M[i]\cdot u = 0\}|}{2^n} \\ &= 2^{-s}\left|\left\{\, u \in \{-1,1\}^s \;\middle|\; \sum_{i=1}^{s} u_i = 0\right\}\right| \\ &\leq \Theta(1/\sqrt{s}) \leq 1/2.\end{aligned}$$

■

**Lemma 3.13.** For any $t \in \mathbb{N}$ such that $(t^2k)^3 \leq s$, the distribution $\mathcal{D}_0$ is $(t, \Theta(1/s^{1/3}))$-pseudo-independent with marginal probability $q := \Theta(1/\sqrt{s})$.

*Proof.* Let

$$q := \sqrt{\frac{2}{\pi s}} \text{ and } \varepsilon := cs^{-1/3}$$

for a constant $c$ to be defined at the end of this proof. Let $S \subseteq [m]$ with $|S| = t$. Our goal is to show that the marginal distribution

$$\mathcal{D} := (\mathcal{D}_0)_S$$

of $\mathcal{D}_0$ is a convex combination of distributions, where each one of them is a product distribution on $x \in \{0,1\}^S$ with each coordinate $x_i$ being a Bernoulli random variable with success probability in the interval $[q(1-\varepsilon), q(1+\varepsilon)]$.

Let

$$R := \cup_{i,j\in S, i\neq j} \text{supp}(M_i) \cap \text{supp}(M_j),$$

where, by the design property of $M$ (Definition 3.6),

$$|R| \leq t^2k.$$

For every $b \in \{-1,1\}^R$, let $\mathcal{D}_b$ be the distribution obtained by conditioning $\mathcal{D}$ to the event $\{u\restriction_R = b\}$.

Note that, for every event $A$, we have that

$$\begin{aligned}\Pr_{x(u)\in\mathcal{D}}[x(u)\in A] &= \sum_{b\in\{-1,1\}^R} \Pr_{x(u)\in\mathcal{D}}[u\restriction_R = b] \Pr_{x(u)\in\mathcal{D}}[x(u)\in A | u\restriction_R = b] \\ &= \sum_{b\in\{-1,1\}^R} \Pr_{x(u)\in\mathcal{D}}[u\restriction_R = b] \Pr_{x(u)\in\mathcal{D}_b}[x(u)\in A],\end{aligned}$$

thus, $\mathcal{D} = (\mathcal{D}_0)_S$ is a convex combination of the distributions $\{\mathcal{D}_b \mid b\in\{-1,1\}^R\}$.

Let us now prove that, for every $b\in\{-1,1\}^R$, the distribution $\mathcal{D}_b$ is a product distribution on $x\in\{0,1\}^S$. Note that, for every $i\in S$, we have that

$$\begin{aligned}x_i = 1 &\iff M[i]\cdot u = 0 \\ &\iff M[i]\restriction_{\mathrm{supp}(M[i])\setminus R}\cdot u\restriction_{\mathrm{supp}(M[i])\setminus R} = -M[i]\restriction_R \cdot u\restriction_R \\ &\iff \sum_{j\in\mathrm{supp}(M[i])\setminus R} u_j = -\sum_{j\in\mathrm{supp}(M[i])\cap R} b_j =: c_{b,i},\end{aligned}$$

where $c_{b,i}$ has value in the interval $[-t^2k, t^2k]$. Let

$$S_i := \mathrm{supp}(M[i])\setminus R.$$

Thus, for every $i,i'\in S$ with $i\neq i'$, the variables $x_i$ and $x_{i'}$ of $\mathcal{D}_b$ have disjoint sources of randomness $\{u_j\}_{j\in S_i}$ and $\{u_j\}_{j\in S_{i'}}$. Hence, the facts above imply that $\mathcal{D}_b$ is a product distribution with each variable $x_i$ for $i\in S$ being a Bernoulli random variable with success probability

$$q_i := \Pr_u\left[\sum_{j\in S_i} u_j = c_{b,i}\right].$$

Therefore, the final step of the proof is to prove upper and lower bounds for $q_i$. These bounds follow from standard calculations about the distribution of the height of a 1-dimensional random walk with $|S_i|$ steps. For completeness, we prove the following lemma in the appendix.

**Lemma 3.14.** If the hypothesis of Lemma 3.13 holds, then there is a universal constant $c>0$ such that

$$\sqrt{\frac{2}{\pi s}}(1-cs^{-1/3}) \le q_i \le \sqrt{\frac{2}{\pi s}}(1+cs^{-1/3}).$$

*Proof.* See Appendix B. ■

This finishes the proof of Lemma 3.13. ■

The following lemma follows from Lemma 3.13 and Corollary 2.11.

**Corollary 3.15.** Assume that $(s/k^5) \geq m^{\Omega(1)}$. Fix any $w \in \mathbb{N}$ such that $w \leq (s/k^5)^{1/6}$. For any $r \geq s$, the distribution $\mathcal{D}_0$ satisfies the following property. For any $\ell \in [2w]$, any monotone DNF $\mathcal{F}$ with at least $r^\ell$ terms of width $\ell$ contains a $(\mathcal{D}_0, m^{-3w})$-sunflower.

*Proof.* Let

$$\delta := m^{-3w} \text{ and } t := s^{1/3}/k^{3/2} \text{ and } q := \Theta(1/\sqrt{s}).$$

By Lemma 3.13 and the choice of $t$, the distribution $\mathcal{D}_0$ is $(t, 1/t)$-pseudo-independent with marginal probability $q$. Note that $w$ satisfies $w \leq \sqrt{\frac{t}{(\log m)^2}}$ and

$$w \log(1/\delta) \leq 3w^2 \log m \leq o(t),$$

so $\mathcal{D}_0$ is $(t, \Omega(1/w))$-pseudo-independent and satisfies the hypothesis of Corollary 2.11. By Corollary 2.11 (using $r' := \Theta(w \log(1/\delta)/q)$ as the $r$ in the statement of this corollary and width $\ell \leq 2w$), we obtain the result above since $r \geq s \geq r'$. ■

### 3.2.3 The Monotone Boolean Circuit Lower Bound

We now prove Lemma 3.7, the main lemma of this subsection.

*Proof of Lemma 3.7.* It suffices to prove a lower bound for the monotone function $g$ on $m_1$ variables which is a restriction of $f$.

We apply Theorem 3.5 with the distributions $\mathcal{D}_0, \mathcal{D}_1$ defined above. By Lemma 3.12 and Lemma 3.10, we have

$$\min\left\{\Pr_{x\sim\mathcal{D}_0}[f(x)=0], \Pr_{x\sim\mathcal{D}_1}[f(x)=1]\right\} \geq \frac{1}{2}.$$

By Lemma 3.11 and Corollary 3.15, we see that Theorem 3.5 is applicable with parameters

$$Q := \frac{m_1}{100n \log n} \text{ and } r := s.$$

Note also that

$$8r = 8s \leq O\left(\frac{m_1}{n \cdot m^{\Omega(1)}}\right) \leq Q \leq rm_1.$$

where we used the hypothesis $s \leq m_1/(n \cdot m^{\Omega(1)})$ of the lemma to get the second equality.

Applying Theorem 3.5 now proves the claim. ■

## 3.3 Uniform Arithmetic Circuits for $(P_m)$

In order to finish the proof of Theorem 3.1, we will need the following construction, whose proof we defer to the next section.

**Lemma 3.16** (Explicit construction of $(M_m)$)**.** There is a deterministic poly$(m)$ time algorithm, which on input $1^m$, produces a matrix $M_m \in \{0,1\}^{n \times m}$ with the following properties.

1. $m = \Theta(n^{3/2})$.
2. $M_m$ is $(C, s, k)$-well-behaved for a set $C$ of size $\Theta(m)$, $s = \Theta(\sqrt{n})$ and $k = O(1)$.

Now we have all the ingredients to prove the main result of this section (Theorem 3.1).

*Proof of Theorem 3.1.* We use the above sequence of matrices to define the polynomial sequence $(P_m)$ as in Section 3.1. The upper bound follows from Lemma 3.3. The lower bound follows from Remark 3.4 and Lemma 3.7. ■

# 4 Construction of Designs with Linear-Algebraic Expansion

The goal of this section is to prove the following theorem.

**Theorem 4.1.** There is a deterministic poly$(q, s, t, d)$ time algorithm, which on input $(1^q, 1^s, 1^d, 1^t)$ for any $s, t, d \in \mathbb{N}$ and prime number $q \in \mathbb{N}$ such that $s \leq q$ and $d < q$ and $t \leq q^{d-1}$, outputs a matrix $G \in \{0,1\}^{n \times m}$ for

$$n := sq \text{ and } m := m_1 + s \text{ and } m_1 := t((q-1)s + 1)$$

such that $G$ is $(C, s, d)$-well-behaved matrix (Definition 3.6) for a set $C$ of size $m_1$.

Let us first see how the theorem yields Lemma 3.16 from the previous section.

*Proof of Lemma 3.16.* This lemma is a special case of the construction Theorem 4.1 using parameters $k := 2$ and

$$q := cn^{1/2} \text{ prime for } c > 2, \text{ and } s := 2\lfloor n^{1/2} \rfloor, \text{ and } t := \frac{m - s}{(q-1)s + 1} \leq q = q^{k-1},$$

and $n := qs$. ■

We now prove Theorem 4.1. Let $q, s, d, t \in \mathbb{N}$ as in the statement of this theorem. Consider the following notation.

**Definition 4.2.** For every $a \in [q], b \in [s]$:

- let $e_a \in \mathbb{R}^q$ be the vector defined by $(e_a)_i := 1_{\{i=a\}}$ for every $i \in [q]$;
- let $e_b \in \mathbb{R}^s$ be the vector defined by $(e_b)_i := 1_{\{i=b\}}$ for every $i \in [s]$;
- let $\delta_{a,b} \in \mathbb{R}^{q \times s}$ be the matrix $\delta_{a,b} := e_a e_b^\top$;

- let $1_q \in \mathbb{R}^q$ be the vector $1_q := \sum_{i \in [q]} e_i$;
- let $1_s \in \mathbb{R}^s$ be the vector $1_s := \sum_{i \in [s]} e_i$;
- let $C_b := 1_q e_b^\top \in \mathbb{R}^{q \times s}$, which is a matrix consisting of the $b$-th column being the all-ones vector; ◀

Let us start by defining a collection of matrices in $\{0,1\}^{q \times s}$ that we will use to define the columns (vectors in $\{0,1\}^{qs}$) of the matrix $G \in \mathbb{R}^{n \times m}$ outputted by our algorithm. For any function $f \colon [s] \to \mathbb{F}_q$, let

$$M_f := \sum_{i \in [s]} e_{f(i)} e_i^\top \in \mathbb{R}^{q \times s}$$

be the matrix representing the graph of the polynomial $f$. Let $V \subseteq \mathbb{R}^{q \times s}$ be the following vector space

$$V := \operatorname{span}\{ M_f \mid f \colon [s] \to \mathbb{F}_q \},$$

and let $\mathcal{C} \subseteq \mathbb{R}^{q \times s}$ be the following collection of matrices

$$\mathcal{C} := \{ M_f \mid f \colon [s] \to \mathbb{F}_q \text{ is a univariate polynomial of degree at most } d \}.$$

Let us first prove that $\mathcal{C}$ satisfies a version of the design property of Definition 3.6.

**Lemma 4.3.** For every $A, B \in \mathcal{C}$, if $A \neq B$, then

$$|\operatorname{supp}(A) \cap \operatorname{supp}(B)| \leq d$$

*Proof.* Let $f, g \in \mathbb{F}_q[x]$ be univariate polynomials of degree at most $d$ such that

$$A = M_f \text{ and } B = M_g.$$

Note that if $(a, b) \in \operatorname{supp}(A) \cap \operatorname{supp}(B) \subseteq [q] \times [s]$, then

$$f(b) = a = g(b).$$

As $f$ and $g$ are distinct polynomials of degree at most $d$, they can intersect in at most $d$ points, which implies the conclusion of this lemma. ■

Now our goal will be to develop tools that will help us to analyse the "linear-algebraic expansion" for the matrices in the collection $\mathcal{C}$. For every $a \in [q]$, $b \in [s]$ and $r \in \mathbb{F}_q$, let $l_{a,b,r} \colon [s] \to \mathbb{F}_q$ be the linear function defined by

$$l_{a,b,r}(i) := (i - b)r + a$$

for every $i \in [s]$. Let

$$M_{a,b,r} := M_{l_{a,b,r}}.$$

Let us now define

$$\mathcal{A} := \{ M_l \mid l \colon [s] \to \mathbb{F}_q \text{ is a polynomial of degree at most } 1\} \text{ and } \mathcal{B} := \{ C_b \mid b \in [s]\}.$$

Consider the following technical lemmas:

**Lemma 4.4.** The vector space $V$ has dimension $d_V := \dim(V) = (q-1)s + 1$.

*Proof.* We first claim that

$$V = \{ M \in \mathbb{R}^{q \times s} \mid \exists c \in \mathbb{R} \text{ s.t. } 1_q^\top M e_i = c \; \forall i \in [s]\} =: W, \tag{10}$$

that is, $V$ is the set of all matrices whose the sums of the entries of each of its columns are the same. As $V$ is the span of matrices $M_f$ and the sum of all the entries of each column of a matrix $M_f$ is 1, we obtain that $V \subseteq W$. In order to prove that $W \subseteq V$, one can argue that every matrix $M \in W$ can be written as a linear combination of matrices $M_f$ via the following arguments (induction on the number of nonzero entries of $M$):

1. If $M = 0$, then $M \in V$.
2. Otherwise, if the column sum of $M$ is zero, then there is a column $i$ with two different entries $u, v$ with opposite nonzero value $a$. Define

   $$M' := M - aM_f + M_g,$$

   where $f, g$ are the functions with $f(i) := u$ and $g(i) := v$ and with $f(j) = g(j)$ for a fixed value. Note that $M' \in W$ and has two less nonzero entries than $M$.
3. If the column sum of $M$ is nonzero, then choose a nonzero element $j_i$ for every column $i$ of $M$ and then let

   $$M' := M - aM_f$$

   where $a := M_{j_1,1}$ and $f(i) := j_i$.

Now we come back to the proof of the lemma. Let $\phi \colon \mathbb{R}^{q \times s} \to \mathbb{R}^s$ be the following linear map:

$$\phi(M) := \sum_{i \in [s]} (1_q^\top M e_i) e_i.$$

By the characterization in Equation 10, we obtain

$$\ker(\phi) = \{ M \in \mathbb{R}^{q \times s} \mid 1_q^\top M e_i = 0 \; \forall i \in [s]\} \subseteq V,$$

and $\phi(V) \cong \mathbb{R}$. By the rank-nullity theorem,

$$qs = \dim(\mathbb{R}^{q\times s}) = \dim(\ker(\phi)) + \dim(\mathrm{Im}(\phi)) = \dim(\ker(\phi)) + s,$$

so $\dim(\ker(\phi)) = (q-1)s$. Let $\psi := \phi\restriction_V : V \to \mathbb{R}^s$. Thus, $\ker(\psi) = \ker(\phi)$ and $\mathrm{Im}(\psi) = \phi(V) \cong \mathbb{R}$, and, by the rank-nullity theorem,

$$\dim(V) = \dim(\ker(\psi)) + \dim(\mathrm{Im}(\psi)) = (q-1)s + 1.$$

■

**Lemma 4.5.** The set $\mathcal{A} \cup \mathcal{B}$ spans $\mathbb{R}^{q\times s}$.

*Proof.* Let us prove that the set $\mathcal{D} := \mathcal{A} \cup \mathcal{B}$ is a spanning set of $\mathbb{R}^{q\times s}$. For every $a \in [q], b \in [s]$, note that

$$C_b + \sum_{r\in\mathbb{F}_q} M_{a,b,r} = q\delta_{a,b} + \sum_{b'\in[s]} C_{b'},$$

since the support of the matrices $C_b$ and $\{M_{a,b,r}\}_{r\in[q]}$ only pairwise intersect entry $(a,b)$, and every other entry in $[q]\times[s]$ is in the support of exactly one of these matrices. Hence, $\delta_{a,b}$ is in $\mathrm{span}(\mathcal{D})$, which implies that $\mathcal{D}$ is a spanning set of $\mathbb{R}^{q\times s}$. ■

**Lemma 4.6.** The set $\mathcal{A}$ spans $V$.

*Proof.* Let us prove that $\mathcal{A}$ is a spanning set of $V$. First note that if $M \in V$, then there is $c \in \mathbb{R}$ such that the sum of the entries in any column of $M$ is equal to $c$ (as this is true for any matrix $M_f$ in the definition of $V$; see the proof of (10) above). Thus, for every $M \in V \cap \mathrm{span}(\mathcal{B})$, there is $\alpha \in \mathbb{R}^s$ such that

$$M = \sum_{i\in[s]} \alpha_i C_i,$$

and there is $c \in \mathbb{R}$ such that $1_q^\top (Me_i) = c$ for every $i \in [s]$. As the matrices $C_i$'s are column matrices with disjoint support, we get that, for every $i \in [s]$,

$$c = 1_q^\top (Me_i) = \alpha_i 1_q^\top (C_i e_i) = \alpha_i q,$$

which implies that

$$\begin{aligned} M &= \sum_{i\in[s]} \alpha_i C_i \\ &= \frac{c}{q} \sum_{i\in[s]} C_i \\ &= \frac{c}{q} \sum_{a\in[q]} M_{a,1,0} \in \mathrm{span}(\mathcal{A}). \end{aligned}$$

Therefore, $V \cap \mathrm{span}(\mathcal{B}) \subseteq \mathrm{span}(\mathcal{A})$, which implies that $\mathcal{A}$ spans $V$, since $\mathcal{A} \subseteq V$ and Lemma 4.5. ■

**Lemma 4.7.** For every function $f\colon [s] \to \mathbb{F}_q$, the set

$$\mathcal{A}_f := \{\, M_{f+l} \mid l\colon [s] \to \mathbb{F}_q \text{ affine polynomial}\}$$

spans $V$.

*Proof.* Let

$$f\colon [s] \to \mathbb{F}_q \text{ be a function and } g := -f.$$

Let $\pi_f\colon V \to \mathbb{R}^{q\times s}$ be the following map: for every $M \in V$ and every $i \in [s]$, let $M_i$ be the $i$-th column of $M$ and define the $i$-th column $P_i$ of $\pi_f(M)$ to be

$$P_i := \sum_{j\in[q]} (M_i)_{j-f(i)} e_j.$$

You can interpret $P_i$ as a cyclic shift of the column $M_i$ using the value of $f(i)$. Note that $\pi_f$ is a bijective linear map with inverse $\pi_g$, and, for any linear function $l$,

$$\pi_f(M_l) = M_{f+l}.$$

Hence,

$$V = \pi_f(V), \text{ and } \mathcal{A}_f = \pi_f(\mathcal{A}),$$

which implies that $\mathcal{A}_f$ spans $V$, since, by Lemma 4.6, $\mathcal{A}$ spans $V$. ∎

We use the lemma above to construct the matrix $G \in \{0,1\}^{n\times m}$ and analyse its linear-algebraic expansion.

For every $\alpha \in \mathbb{F}_q^{d-1}$, let

$$F_\alpha(x) := \sum_{i=1}^{d-1} \alpha_i x^{i+1}.$$

Using Lemma 4.7, fix a basis $\mathcal{B}_\alpha \subseteq \mathcal{A}_{F_\alpha}$ for $V$. By Lemma 4.4, we have that

$$|\mathcal{B}_\alpha| = \dim(V) = (q-1)s + 1 = d_V.$$

As $d < q$, two polynomials of degree at most $d$ do not correspond to the same function; thus, for every $\alpha, \beta \in \mathbb{F}_q^{d-1}$ distinct, we have

$$\mathcal{A}_{F_\alpha} \cap \mathcal{A}_{F_\beta} = \varnothing \text{ and } \mathcal{B}_\alpha \cap \mathcal{B}_\beta = \varnothing,$$

since $\mathsf{deg}(F_\alpha), \mathsf{def}(F_\beta) \geq 2$.

Let $\mathcal{S}_t \subseteq \mathbb{F}_q^{d-1}$ be an arbitrary fixed set of $t$ elements of $\mathbb{F}_q^{d-1}$ (e.g., the first $t$ elements according to the lexicographic order). Define

$$\mathcal{C}' := \cup_{\alpha\in\mathcal{S}_t} \mathcal{B}_\alpha.$$

Hence, $|\mathcal{C}'| = t d_V$ and, as $\mathcal{C}' \subseteq \mathcal{C}$, Lemma 4.3 implies that $\mathcal{C}'$ also satisfies a design property. Now we show that $\mathcal{C}'$ satisfies a linear-algebraic expansion.

**Lemma 4.8.** For every subspace $U \subseteq V$, the probability that a uniformly random matrix of $\mathcal{C}'$ lie in $U$ is at most $\dim(U)/\dim(V)$.

*Proof.* Consider the following random process to generate a uniform random matrix $M$ of $\mathcal{C}'$:

1. Choose $\alpha \in \mathcal{S}_t$ uniformly at random;
2. Let $M$ be a uniformly random matrix in $\mathcal{B}_\alpha$.

It is not hard to prove that $M$ is a uniform random matrix of $\mathcal{C}'$ (as $\mathcal{B}_\alpha$'s are disjoint), and, if we condition on $\alpha \in \mathcal{S}_t$, then $M$ is a uniform random matrix of $\mathcal{B}_\alpha$. For every $a \in \mathcal{S}_t$, we have that

$$|\mathcal{B}_a \setminus U| \geq \dim(V) - \dim(U)$$

as $\mathcal{B}_a$ is a basis of $V$. Hence,

$$\Pr_{M,\alpha}[M \notin U | \alpha = a] \geq \frac{\dim(V) - \dim(U)}{|\mathcal{B}_a|} = 1 - \frac{\dim(U)}{\dim(V)}.$$

Therefore, by a conditioning argument over the component $\alpha$ of the random process generating $M$, we get that

$$\Pr_{M,\alpha}[M \notin U] \geq 1 - \frac{\dim(U)}{\dim(V)},$$

which proves the lemma. ∎

Therefore, we can construct the matrix $G \in \{0,1\}^{n \times m}$ as follows. Recall that

$$n = qs \text{ and } m = m_1 + s \text{ and } m_1 = td_V.$$

Fix total orders for the elements of $\mathcal{S}_t$ and the elements of each $\mathcal{B}_\alpha$. For every $i \in [t]$ and $j \in [d_V]$, let $\alpha \in \mathcal{S}_t$ be the $i$-th element of $\mathcal{S}_t$ and $M \in \mathcal{B}_\alpha$ be the $j$-th element of $\mathcal{B}_\alpha$. We define the $((i-1)t + j)$-th column $G_{i,j}$ of $G$ to be

$$G_{i,j} := \texttt{vect}(M) \in \{0,1\}^{qs},$$

where $\texttt{vect}\colon \mathbb{R}^{q \times s} \to \mathbb{R}^{qs}$ is a fixed isomorphism between matrices $M \in \{0,1\}^{q \times s}$ and a vector $v \in \{0,1\}^{qs}$ obtained by rearranging the $qs$ entries of $M$ as entries of $v$ in a fixed arbitrary way. For every $j \in [s]$, we define the $(m_1 + i)$-th column $G_{0,j}$ of $G$ to be

$$G_{0,j} := \texttt{vect}(C_j),$$

where $C_j$ as defined by Definition 4.2. It is not hard to show that $G$ can be constructed in time $\text{poly}(q, s, t, d)$ by a deterministic algorithm, as the sets $B_\alpha$ can be obtained by findinig a basis of the set $\mathcal{A}_\alpha$.

For

$$C := \{\, (i-1)t + j \mid i \in [t], j \in [d_V] \,\} \subseteq [m],$$

let us prove that the matrix $G \in \{0,1\}^{n \times m}$ defined above is $(C, s, d)$-well behaved:

- The vector space $V' := \mathrm{span}\{\, G_{i,j} \mid i \in [t], j \in [d_V]\}$ of column of $G$ indexed by $C$ is isomorphic to the vector space $V$ spanned by the matrices in $\mathcal{C}'$ using the isomorphism `vect` above.
- All the matrices $M \in \mathcal{C}'$ and $C_j$'s have support of size $s$, and the columns of $G$ are rearrangements of the entries of these matrices in vector form. Thus, all columns of $G$ have support size $s$.
- By Lemma 4.3, all pairs of distinct matrices $M, N$ in $\mathcal{C}'$ have

$$|\operatorname{supp}(M) \cap \operatorname{supp}(N)| \leq d.$$

  This also holds for all pairs of columns of $G$ in $C$ as they are vector corresponding to matrices in $\mathcal{C}'$.
- For any subspace $U' \subseteq V'$, the probability of a column of $G$, chosen uniformly at random from the columns indexed by $C$, be inside $U'$ is the same as the probability of an element of $\mathcal{C}'$, chosen uniformly at random, be inside a subspace $U$ of $V$ isomorphic to $U'$. By Lemma 4.8, the latter probability is at most $\dim(U')/\dim(V')$.

## References


[AGG+25] Yaroslav Alekseev, Mika Göös, Ziyi Guan, Gilbert Maystre, Artur Riazanov, Dmitry Sokolov, and Weiqiang Yuan. Generalised Linial-Nisan conjecture is false for DNFs. In Srikanth Srinivasan, editor, *40th Computational Complexity Conference, CCC 2025, Toronto, Canada, August 5-8, 2025*, LIPIcs, pages 29:1–29:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025. URL: https://doi.org/10.4230/LIPIcs.CCC.2025.29, doi:10.4230/LIPICS.CCC.2025.29.

[ALWZ21] Ryan Alweiss, Shachar Lovett, Kewen Wu, and Jiapeng Zhang. Improved bounds for the sunflower lemma. *Ann. of Math.*, 2(194(3)):795–815, 2021. doi:10.4007/annals.2021.194.3.5.

[And20] Robert Andrews. Algebraic hardness versus randomness in low characteristic. In Shubhangi Saraf, editor, *35th Computational Complexity Conference, CCC 2020, Saarbrücken, Germany (Virtual Conference), July 28-31, 2020*, LIPIcs, pages 37:1–37:32. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. URL: https://doi.org/10.4230/LIPIcs.CCC.2020.37, doi:10.4230/LIPICS.CCC.2020.37.

[AS16] Noga Alon and Joel H. Spencer. *The probabilistic method*. Wiley Series in Discrete Mathematics and Optimization. John Wiley & Sons, Inc., Hoboken, NJ, fourth edition, 2016.

[ASU13] Noga Alon, Amir Shpilka, and Christopher Umans. On sunflowers and matrix multiplication. *Comput. Complex.*, 22(2):219–243, 2013. URL: https://doi.org/10.1007/s00037-013-0060-1, doi:10.1007/S00037-013-0060-1.

[AV08] Manindra Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, Philadelphia, PA, USA, October 25-28, 2008*, pages 67–75. IEEE Computer Society, 2008. doi:10.1109/FOCS.2008.32.

[Baz09] Louay M. J. Bazzi. Polylogarithmic independence can fool DNF formulas. *SIAM J. Comput.*, 38(6):2220–2272, 2009. doi:10.1137/070691954.

[BCW21] Tolson Bell, Suchakree Chueluecha, and Lutz Warnke. Note on Sunflowers. *Discrete Mathematics*, 344(8):112328, 2021. Preprint: https://arxiv.org/abs/2009.09327. arXiv:arXiv:2009.09327, doi:10.1016/j.disc.2021.112328.

[Ber84] Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Inf. Process. Lett.*, 18(3):147–150, 1984. doi:10.1016/0020-0190(84)90018-8.

[BKR+26] Somnath Bhattacharjee, Mrinal Kumar, Shanthanu S. Rai, Varun Ramanathan, Ramprasad Saptharishi, and Shubhangi Saraf. Closure under factorization from a result of Furstenberg. In Aditya Bhaskara and Artur Czumaj, editors, *Proceedings of the 58th Annual ACM Symposium on Theory of Computing, STOC 2026, Salt Lake City, UT, USA, June 22-26, 2026*, pages 174–185. ACM, 2026. doi:10.1145/3798129.3800738.

[BM25] Jaroslaw Blasiok and Linus Meierhöfer. Hardness of clique approximation for monotone circuits. In Srikanth Srinivasan, editor, *40th Computational Complexity Conference, CCC 2025, August 5-8, 2025, Toronto, Canada*, volume 339 of *LIPIcs*, pages 4:1–4:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025. URL: https://doi.org/10.4230/LIPIcs.CCC.2025.4, doi:10.4230/LIPICS.CCC.2025.4.

[Bür00] Peter Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*, volume 7 of *Algorithms and computation in mathematics*. Springer, 2000.

[CDGM22] Arkadev Chattopadhyay, Rajit Datta, Utsab Ghosal, and Partha Mukhopadhyay. Monotone complexity of spanning tree polynomial re-visited. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPIcs*, pages 39:1–39:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. URL: https://doi.org/10.4230/LIPIcs.ITCS.2022.39, doi:10.4230/LIPICS.ITCS.2022.39.

[CDM21] Arkadev Chattopadhyay, Rajit Datta, and Partha Mukhopadhyay. Lower bounds for monotone arithmetic circuits via communication complexity. In Samir Khuller and Virginia Vassilevska Williams, editors, *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 786–799. ACM, 2021. doi:10.1145/3406325.3451069.

[CFM+26] Bruno Cavalar, Théo Borém Fabris, Partha Mukhopadhyay, Srikanth Srinivasan, and Amir Yehudayoff. Negations are powerful even in small depth. In Aditya Bhaskara and Artur Czumaj, editors, *Proceedings of the 58th Annual ACM Symposium on Theory of Computing, STOC 2026, Salt Lake City, UT, USA, June 22-26, 2026*, pages 2071–2082. ACM, 2026. doi:10.1145/3798129.3800911.

[CGR+26] Bruno Cavalar, Mika Göös, Artur Riazanov, Anastasia Sofronova, and Dmitry Sokolov. Monotone circuit complexity of matching. In Aditya Bhaskara and Artur Czumaj, editors, *Proceedings of the 58th Annual ACM Symposium on Theory of Computing, STOC 2026, Salt Lake City, UT, USA, June 22-26, 2026*, pages 1128–1132. ACM, 2026. doi:10.1145/3798129.3800824.

[CKR22] Bruno Pasqualotto Cavalar, Mrinal Kumar, and Benjamin Rossman. Monotone circuit lower bounds from robust sunflowers. *Algorithmica*, 84(12):3655–3685, 2022. URL: https://doi.org/10.1007/s00453-022-01000-3, doi:10.1007/S00453-022-01000-3.

[DK06] James Demmel and Plamen Koev. Accurate and efficient evaluation of Schur and Jack functions. *Mathematics of computation*, 75(253):223–239, 2006.

[dRV25] Susanna F. de Rezende and Marc Vinyals. Lifting with colourful sunflowers. In Rahul Santhanam, editor, *40th Computational Complexity Conference (CCC 2025)*, volume 339 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 36:1–36:19, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.CCC.2025.36.

[DSS18] Pranjal Dutta, Nitin Saxena, and Amit Sinhababu. Discovering the roots: uniform closure results for algebraic classes under factoring. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 1152–1165. ACM, 2018. doi:10.1145/3188745.3188760.

[ER60] P. Erdös and R. Rado. Intersection theorems for systems of sets. *J. Lond. Math. Soc.*, 35(1):85–90, 1960.

[FG06] Jörg Flum and Martin Grohe. *Parameterized Complexity Theory*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2006. doi:10.1007/3-540-29953-X.

[FGK16] Sergey Fomin, Dima Grigoriev, and Gleb Koshevoy. Subtraction-free complexity, cluster transformations, and spanning trees. *Foundations of Computational Mathematics*, 16(1):1–31, 2016.

[FLRS23] Yuval Filmus, Itai Leigh, Artur Riazanov, and Dmitry Sokolov. Sampling and certifying symmetric functions. In Nicole Megow and Adam D. Smith, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2023, Atlanta, Georgia, USA, September 11-13, 2023*, LIPIcs, pages 36:1–36:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023. URL: https://doi.org/10.4230/LIPIcs.APPROX/RANDOM.2023.36, doi:10.4230/LIPICS.APPROX/RANDOM.2023.36.

[FMS93] Gudmund Skovbjerg Frandsen, Peter Bro Miltersen, and Sven Skyum. Dynamic word problems. In *34th Annual Symposium on Foundations of Computer Science, Palo Alto, California, USA, November 3-5, 1993*, pages 470–479. IEEE Computer Society, 1993. doi:10.1109/SFCS.1993.366840.

[GKKS16] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth 3. *SIAM J. Comput.*, 45(3):1064–1079, 2016. doi:10.1137/140957123.

[GMR13] Parikshit Gopalan, Raghu Meka, and Omer Reingold. DNF sparsification and a faster deterministic counting algorithm. *Comput. Complex.*, 22(2):275–310, 2013. URL: https://doi.org/10.1007/s00037-013-0068-6, doi:10.1007/S00037-013-0068-6.

[GRSS23] Mika Göös, Artur Riazanov, Anastasia Sofronova, and Dmitry Sokolov. Top-down lower bounds for depth-four circuits. In *64th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2023, Santa Cruz, CA, USA, November 6-9, 2023*, pages 1048–1055. IEEE, 2023. doi:10.1109/FOCS57990.2023.00063.

[GS91] S. B. Gashkov and I. S. Sergeev. A method for deriving lower bounds for the complexity of monotone arithmetic circuits computing real polynomials. *Mathematical Notes*, 50(1–2):863–873, 1991. doi:10.1007/BF01158240.

[HJP95] Johan Håstad, Stasys Jukna, and Pavel Pudlák. Top-down lower bounds for depth-three circuits. *Comput. Complex.*, 5(2):99–112, 1995. doi:10.1007/BF01268140.

[HY21] Pavel Hrubeš and Amir Yehudayoff. Shadows of Newton Polytopes. In Valentine Kabanets, editor, *36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference)*, volume 200 of *LIPIcs*, pages 9:1–9:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. URL: https://doi.org/10.4230/LIPIcs.CCC.2021.9, doi:10.4230/LIPICS.CCC.2021.9.

[Jan90] Svante Janson. Poisson approximation for large deviations. *Random Structures & Algorithms*, 1(2):221–229, 1990. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/rsa.3240010209, arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/rsa.3240010209, doi:10.1002/rsa.3240010209.

[JS82] Mark Jerrum and Marc Snir. Some exact complexity results for straight-line computations over semirings. *Journal of the ACM*, 29(3):874–897, 1982. doi:10.1145/322326.322341.

[JS20] Stasys Jukna and Hannes Seiwert. Approximation limitations of pure dynamic programming. *SIAM J. Comput.*, 49(1):170–205, 2020. doi:10.1137/18M1196339.

[Kal87] Erich L. Kaltofen. Single-factor hensel lifting and its application to the straight-line complexity of certain polynomials. In Alfred V. Aho, editor, *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 443–452. ACM, 1987. doi:10.1145/28395.28443.

[Kel21] Zander Kelley. An improved derandomization of the switching lemma. In Samir Khuller and Virginia Vassilevska Williams, editors, *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 272–282. ACM, 2021. doi:10.1145/3406325.3451054.

[Koi12] Pascal Koiran. Arithmetic circuits: The chasm at depth four gets wider. *Theor. Comput. Sci.*, 448:56–65, 2012. URL: https://doi.org/10.1016/j.tcs.2012.03.041, doi:10.1016/J.TCS.2012.03.041.

[LMM+22] 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*, LIPIcs, pages 104:1–104:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. URL: https://doi.org/10.4230/LIPIcs.ITCS.2022.104, doi:10.4230/LIPICS.ITCS.2022.104.

[Mul87] Ketan Mulmuley. A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. *Comb.*, 7(1):101–104, 1987. doi:10.1007/BF02579205.

[Nis91] Noam Nisan. Pseudorandom bits for constant depth circuits. *Comb.*, 11(1):63–70, 1991. doi:10.1007/BF01375474.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs. randomness. *Journal of Computer and System Sciences*, 49(2):149–167, 1994. doi:10.1016/S0022-0000(05)80043-1.

[Rao20] Anup Rao. Coding for sunflowers. *Discrete Analysis*, 2020(2), 2020. doi:DOI:10.19086/da.11887.

[Rao25] Anup Rao. The story of sunflowers, 2025. URL: https://arxiv.org/abs/2509.14790, arXiv:2509.14790.

[Raz85] Alexander Razborov. Lower bounds on the monotone complexity of some Boolean functions. *Dokl. Akad. Nauk SSSR*, 281(4):798–801, 1985.

[Ros14] Benjamin Rossman. The monotone complexity of $k$-clique on random graphs. *SIAM Journal on Computing*, 43(1):256–279, 2014. doi:10.1137/110839059.

[RR18] Sivaramakrishnan Natarajan Ramamoorthy and Anup Rao. Lower bounds on non-adaptive data structures maintaining sets of numbers, from sunflowers. In Rocco A. Servedio, editor, *33rd Computational Complexity Conference, CCC 2018, San Diego, CA, USA, June 22-24, 2018*, LIPIcs, pages 27:1–27:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. URL: https://doi.org/10.4230/LIPIcs.CCC.2018.27, doi:10.4230/LIPICS.CCC.2018.27.

[RY11] Ran Raz and Amir Yehudayoff. Multilinear formulas, maximal-partition discrepancy and mixed-sources extractors. *J. Comput. Syst. Sci.*, 77(1):167–190, 2011. doi:10.1016/j.jcss.2010.06.013.

[Sri20] Srikanth Srinivasan. Strongly exponential separation between monotone VP and monotone VNP. *ACM Trans. Comput. Theory*, 12(4):12, 2020. Id/No 23. doi:10.1145/3417758.

[SS77] Eli Shamir and Marc Snir. Lower bounds on the number of multiplications and additions in monotone computations. Technical Report RC 6757, IBM Thomas J. Watson Research Center, 1977.

[Tal17] Avishay Tal. Tight bounds on the fourier spectrum of AC0. In Ryan O'Donnell, editor, *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, volume 79 of *LIPIcs*, pages 15:1–15:31. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017. URL: https://doi.org/10.4230/LIPIcs.CCC.2017.15, doi:10.4230/LIPICS.CCC.2017.15.

[Tav15] Sébastien Tavenas. Improved bounds for reduction to depth 4 and depth 3. *Inf. Comput.*, 240:2–11, 2015. URL: https://doi.org/10.1016/j.ic.2014.09.004, doi:10.1016/J.IC.2014.09.004.

[Val80] Leslie G. Valiant. Negation can be exponentially powerful. *Theor. Comput. Sci.*, 12:303–314, 1980. doi:10.1016/0304-3975(80)90060-2.

[Yeh19] Amir Yehudayoff. Separating monotone VP and VNP. In Moses Charikar and Edith Cohen, editors, *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23-26, 2019*, pages 425–429. ACM, 2019. doi:10.1145/3313276.3316311.

# A Properties of $\mathcal{D}_1$

*Proof of Lemma 3.11.* Let $T := \{u_1, \ldots, u_t\} \subseteq [m_1]$. By Definition 3.9, $x \sim \mathcal{D}_1$ is the indicator vector of a random set $I$ obtained from sampling $\lambda$ elements $v_1, \ldots, v_\lambda$ of $[m_1]$ with replacement. Thus

$$\Pr_{x\sim\mathcal{D}_1}[\wedge_{i\in T} x_i = 1] \leq \sum_{S\in\binom{[\lambda]}{t}} \Pr_I[\cap_{i\in S}\{v_i = u_i\}] = \sum_{S\in\binom{[\lambda]}{t}} m^{-t} \leq \lambda^t m^{-t} = (m/\lambda)^{-t}.$$

■

Our proof of Lemma 3.10 is essentially the same proof as for a similar lemma in [CFM+26], but using the linear-algebraic expansion property of the matrix.

*Proof of Lemma 3.10.* By the definition of $g$, we have that, for every $S \subseteq [m_1]$,

$$g(1_S) = 1 \iff V = \text{span}\{\, M[i] \mid i \in S\}.$$

By Definition 3.9, $x \sim \mathcal{D}_1$ is the indicator vector of a random set $I$ obtained from sampling $\lambda$ elements $v_1, \ldots, v_\lambda$ of $[m_1]$ with replacement. For every $i \in [\lambda]$, let

$$C_i := M[v_i].$$

Let $N := \dim(V)$. For each $d \leq N$, let $X_d$ denote the smallest $r \in [\lambda]$ such that $C_1, \ldots, C_r$ span a subspace of dimension $d$ (if such an $r$ exists). For $X_0 := 0$, we have that

$$X_N = \sum_{d=0}^{N-1} X_{d+1} - X_d,$$

which implies that

$$\mathbb{E}[X_N] = \sum_{d=0}^{N-1} \mathbb{E}[X_{d+1} - X_d].$$

For every $d \in [N]$ and $r \in [\lambda]$, if $X_d = r$, then

$$U := \operatorname{span}\{C_1, \ldots, C_r\}$$

has dimension $d$. Thus, by the linear-algebraic expansion property for $(C, s, k)$-well-behaved matrices (Definition 3.6), we have that, for every $i > r$,

$$\Pr_x [C_i \in U] \leq \frac{\dim(U)}{\dim(V)} = \frac{d}{N} =: p_d.$$

It follows that $X_{d+1} - X_d$ (conditioned on $v_1, \ldots, v_r$ spanning a space of dimension $d$) has a geometric distribution with success probability at least $1 - p_d = (N-d)/N$ and thus has expectation at most $N/(N-d)$. Hence,

$$\mathbb{E}[X_N] \leq \sum_{d=0}^{N-1} \frac{N}{N-d} \leq 2N \log N.$$

By Markov's inequality,

$$\Pr_x [X_N > \lambda] \leq \Pr_x [X_N > 100n \log n] \leq \Pr_x [X_N > 100N \log N] \leq \Pr_x [X_N > 50\mathbb{E}[X_N]] \leq 1/50.$$

This concludes the proof of the lemma, as

$$g(x) = 1 \iff X_N \leq \lambda.$$

■

# B Proof of Lemma 3.14

Let $v \in [0, |R|]$ and $N \geq v$ such that $N + v$ is even. Let $R_N \sim \text{Rademacher}(N)$ be a sum of $N$ independent Rademacher random variables. A simple counting argument shows that

$$\Pr [R_N = v] = \binom{N}{(N+v)/2} 2^{-N}.$$

Furthermore, for $N = 2l + b$ for $l \in \mathbb{N}$ and $b \in \{0, 1\}$ and $w := (v + b)/2$, we obtain

$$\begin{aligned} \frac{\binom{N}{(N+v)/2}}{\binom{N}{\lceil N/2 \rceil}} &= \frac{\lceil N/2 \rceil! \lfloor N/2 \rfloor!}{((N+v)/2)!((N-v)/2)!} = \frac{(l+b)!l!}{(l+(b+v)/2)!(l+b-(v+b)/2)!} \\ &= \frac{\prod_{i=0}^{w-1} l + b - i}{\prod_{i=1}^{w} l + i} = \prod_{i=1}^{w} \left(1 - \frac{2i - b - 1}{l + i}\right). \end{aligned}$$

Using that $\exp(-x/(1-x)) \leq 1-x \leq \exp(-x)$ for every $x \leq 1$, we obtain that

$$\begin{aligned}\prod_{i=1}^{w}\left(1-\frac{2i-b-1}{l+i}\right) &\leq \exp\left(-\sum_{i=1}^{w}\frac{2i-b-1}{l+i}\right)\\ &\leq \exp\left(-\frac{1}{l+w}(1-b+2w-b-1)w/2\right)\\ &= \exp\left(-\frac{(w-b)w}{l+w}\right),\end{aligned}$$

and

$$\begin{aligned}\prod_{i=1}^{w}\left(1-\frac{2i-b-1}{l+i}\right) &\geq \exp\left(-\sum_{i=1}^{w}\frac{2i-b-1}{l-i+b+1}\right)\\ &\geq \exp\left(-\frac{1}{l-w}(1-b+2w-b-1)w/2\right) = \exp\left(-\frac{(w-b)w}{l-w}\right)\\ &= \exp\left(-\frac{(w-b)w}{l+w}\left(1+\frac{2w}{l-w}\right)\right)\\ &= \exp\left(-\frac{(w-b)w}{l+w}\right)\exp\left(-\frac{2(w-b)w^2}{(l+w)(l-w)}\right).\end{aligned}$$

Hence,

$$\binom{N}{(N+v)/2} \in \binom{N}{\lfloor N/2\rfloor}\cdot\exp\left(-\frac{(w-b)w}{l+w}\right)\cdot\left[\exp\left(-\frac{2(w-b)w^2}{(l+w)(l-w)}\right),1\right].$$

In the following, consider

$$c_1,\ldots,c_{10} \in \mathbb{R}_{\geq 0}$$

to be positive constants implicitly defined during our calculations. It is well known that

$$n! \in \sqrt{2\pi n}(n/e)^n\cdot[1-c_1/n, 1+c_1/n]$$

for sufficiently large $n$. So, we can prove that

$$\binom{N}{\lfloor N/2\rfloor} \in \sqrt{\frac{2}{\pi N}}\cdot 2^N\cdot e^{c_2/N}\cdot[e^{-c_3/N},1].$$

Recall that, for

$$N := |S_i| = |\operatorname{supp}(M[i])\setminus R| \in [s-t^2k, s], \text{ and } v := |c_{b,i}| \in [0, t^2k],$$

we have

$$q_i = \Pr\left[R_N = v\right].$$

By our assumption, we have $v^3 \le |R|^3 \le (t^2k)^3 \le s$, so

$$N \in s \cdot \left[1 - \frac{|R|}{s}, 1\right] \subseteq s \cdot \left[1 - \frac{1}{s^{2/3}}, 1\right] \subseteq s \cdot [e^{-2s^{-2/3}}, 1],$$

and $1/\sqrt{N} \in (1/\sqrt{s})e^{2s^{-2/3}} \cdot [e^{-2s^{-2/3}}, 1]$ and

$$\begin{aligned}
\Pr[R_N = v] = &\quad \binom{N}{(N+v)/2} \cdot 2^{-N} \\
\in &\quad \sqrt{\frac{2}{\pi N}} \cdot e^{c_2/N} \cdot e^{-(w-b)w/(l+w)} \cdot [e^{-c_3/N} e^{-2w^3/((l+w)(l-w))}, 1] \\
\subseteq &\quad \sqrt{\frac{2}{\pi s}} e^{2s^{-2/3}} \cdot e^{c_4(1+v^2)/s} \cdot \left[e^{-2s^{-2/3}} e^{-(c_5/s)(1+v^3/s)}, 1\right].
\end{aligned}$$

Moreover, we have $v^2/s \le 1/s^{1/3}$, so

$$\begin{aligned}
\Pr[R_N = v] \in &\quad \sqrt{\frac{2}{\pi s}} e^{2s^{-2/3}} \cdot e^{c_6 s^{-1/3}} \cdot \left[e^{-2s^{-2/3}} e^{c_7 s^{-1/3}} e^{-c_8 s^{-1}}, 1\right]. \\
\subseteq &\quad \sqrt{\frac{2}{\pi s}} \cdot \left[e^{-c_9 s^{-1/3}}, e^{c_{10} s^{-1/3}}\right].
\end{aligned}$$

Therefore,

$$\sqrt{\frac{2}{\pi s}}(1 - c_9 s^{-1/3}) \le q_i \le \sqrt{\frac{2}{\pi s}}(1 + 2c_{10} s^{-1/3}),$$

and we define $c := \max\{c_9, 2c_{10}\}$.



ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il