Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 5 (2026)

Rational degree is polynomially related to degree

Robin Kothari* Matt Kovacs-Deak† Daochen Wang‡ Rain Zimin Yang§

Abstract

We prove that $\deg(f) \leq \widetilde{O}(\mathrm{rdeg}(f)^3)$ for every Boolean function f, where $\deg(f)$ is the degree of f and $\mathrm{rdeg}(f)$ is the rational degree of f. This resolves the second of the three open problems stated by Nisan and Szegedy, and attributed to Fortnow, in 1994 [NS94].

1 Introduction

The degree $\deg(f)$ of a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is the minimum value of $\deg(r)$ such that r is a real polynomial and $f = r$ on $\{0,1\}^n$. The rational degree $\mathrm{rdeg}(f)$ of f is the minimum value of $\max(\deg(p), \deg(q))$ such that p, q are real polynomials and $f = p/q$ on $\{0,1\}^n$. Clearly, $\mathrm{rdeg}(f) \leq \deg(f)$ as can be seen by taking the denominator q to be 1. On the other hand, it is unclear whether $\mathrm{rdeg}(f)$ could be much smaller than $\deg(f)$.

Degree is polynomially related to almost all Boolean complexity measures. Rational degree characterizes the exact postselected quantum query complexity [MdW15]. Whether rational degree is polynomially related to degree has remained an open problem since it was first stated by Nisan and Szegedy, and attributed to Fortnow, over three decades ago [NS94].

Since then, the problem has been reiterated in works such as [dW00; dW01; dW03; She13; MdW15; Cade20; ABK+21; IJK+25]. Rational degree can also be motivated from a variety of perspectives beyond quantum postselection:

1. The analogous randomized query measure, exact postselected randomized query complexity, equals the *certificate complexity* [Cade20, Theorem 16]. Therefore, rational degree can be viewed as a natural quantum notion of certificate complexity. (Note that rational degree is distinct from Aaronson's definition of quantum certificate complexity [Aar08].)
2. We have $\deg_\pm(f) \leq 2\,\mathrm{rdeg}(f)$ by squaring and shifting p, where $\deg_\pm(f)$ is the *sign degree* (or *threshold degree*) of f, that is, the minimum degree of a real polynomial that agrees in sign with $(-1)^{f(x)}$ for all $x \in \{0,1\}^n$. Therefore, $\deg_\pm(f)/2 \leq \mathrm{rdeg}(f) \leq \deg(f)$. Sign degree and degree are well-studied complexity measures [Saks93; NS94; O'D14]. As rational degree inherits structural properties of both, it helps us better understand their relationship.
3. It is not hard to see that $\mathrm{rdeg}(f) = \max(\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f))$, where $\neg$ denotes negation and $\mathrm{ndeg}(f)$ is the minimum degree of a real polynomial s such that, for all $x \in \{0,1\}^n$, $s(x) = 0$ if and only if $f(x) = 0$. (This is Fact 3, for which we give a proof for completeness.) In combinatorics, the Alon-Füredi theorem [AF93] is equivalent to $\mathrm{ndeg}(\mathrm{AND}_n) = n$, and the key lemma of [ABCO88] essentially shows $\mathrm{ndeg}(\mathrm{PARITY}_n) \geq n/2$. At a deeper level, the relation between rational degree and degree governs the *effectiveness* of a natural Nullstellensatz for the hypercube, in the sense of [Bro87; Kol88; Alon99; Jel05]. We give more details in Section 5.1.
4. In complexity theory, $\mathrm{ndeg}(f)$ equals the *degree of the set* $f^{-1}(0)$ as defined by Smolensky [Smo93], and equals the *one-sided* 0*-approximate degree* of f, up to a factor of 2, as defined by Sherstov [She18]. Polynomially relating rational degree to degree also implies $\mathbf{P} = (\mathrm{C}_=\mathbf{P} \cap \text{co-}\mathrm{C}_=\mathbf{P})$ with respect to generic oracles [FFKL03]. This originally motivated Fortnow to pose his open problem [For26], which he has described as one of his "favorite and most frustrating" [For03].

*Google †University of Maryland ‡University of British Columbia §University of British Columbia
‡Corresponding author: wdaochen@gmail.com

ISSN 1433-8092

In this work, we resolve the open problem by proving $\deg(f) \leq \widetilde{O}(\mathrm{rdeg}(f)^3)$ for every Boolean function f. In fact, we prove $\deg(f) \leq \widetilde{O}(\deg_{\pm}(f)^2 \,\mathrm{rdeg}(f))$, which is stronger.

Before presenting our strongest results in Section 4, we establish $\deg(f) \leq 16\,\mathrm{rdeg}(f)^4$ in Section 3. While weaker, this result already resolves Fortnow's open problem and serves as a gentle introduction to the techniques used later. We end by discussing a variety of implications and open problems in Section 5.

2 Preliminaries

This section presents the main definitions and tools used in our proof. For more context, we refer the reader to de Wolf's thesis [dW01] and the survey of Buhrman and de Wolf [BdW02].

For a positive integer n, we write $[n]$ for the set $\{1, \ldots, n\}$. We use the symbol $\bigsqcup$ for disjoint union of sets. We employ standard notation for polynomial rings and their fraction fields. For $p \in \mathbb{R}[X_1, \ldots, X_n]$, we write $\deg(p)$ for the degree of p. If p is of the form $\sum_{S \subseteq [n]} c_S \cdot \prod_{i \in S} X_i$, then we say it is multilinear. In this case, the degree of p is equal to $\max\{|S| : c_S \neq 0\}$. For $x \in \{0,1\}^n$, we write $|x|$ for Hamming weight of x, that is, the number of 1s in x.

2.1 Boolean functions

A Boolean function is a function of the form $f\colon \{0,1\}^n \to \{0,1\}$, where n is a positive integer. The degree of f is defined using the following well-known fact, see, e.g., [BdW02, Lemma 1].

Fact 1 (Multilinear representation)**.** *For every $f\colon \{0,1\}^n \to \mathbb{R}$, there exists a unique multilinear $p \in \mathbb{R}[X_1, \ldots, X_n]$ such that $p(x) = f(x)$ for all $x \in \{0,1\}^n$.*

Definition 1 (Degree)**.** The *degree* of $f\colon \{0,1\}^n \to \{0,1\}$, denoted $\deg(f)$, is defined to be the degree of the unique multilinear $p \in \mathbb{R}[X_1, \ldots, X_n]$ such that $p(x) = f(x)$ for all $x \in \{0,1\}^n$.

We now give the definitions of rational degree, sign degree and nondeterministic degree.

Definition 2 (Rational degree)**.** We say that $p/q \in \mathbb{R}(X_1, \ldots, X_n)$, where p, q are multilinear, is a *rational representation* of $f\colon \{0,1\}^n \to \{0,1\}$ if for all $x \in \{0,1\}^n$, $q(x) \neq 0$ and $p(x)/q(x) = f(x)$. The *rational degree* of f, denoted $\mathrm{rdeg}(f)$, is the minimum value of $\max(\deg(p), \deg(q))$ over all rational representations of f.

Definition 3 (Sign degree)**.** We say that $p \in \mathbb{R}[X_1, \ldots, X_n]$, where p is multilinear, is a *sign representation* of $f\colon \{0,1\}^n \to \{0,1\}$ if for all $x \in \{0,1\}^n$, $p(x) < 0$ if and only if $f(x) = 1$. The *sign degree* of f, denoted $\deg_{\pm}(f)$, is the minimum value of $\deg(p)$ over all sign representations of f.

Definition 4 (Nondeterministic degree)**.** We say that $p \in \mathbb{R}[X_1, \ldots, X_n]$, where p is multilinear, is a *nondeterministic representation* of $f\colon \{0,1\}^n \to \{0,1\}$ if for all $x \in \{0,1\}^n$, $p(x) \neq 0$ if and only if $f(x) = 1$. The *nondeterministic degree* of f, denoted $\mathrm{ndeg}(f)$, is the minimum value of $\deg(p)$ over all nondeterministic representations of f.

We record the following fact relating rational degree to sign degree mentioned in the introduction.

Fact 2. *For every Boolean function f, $\deg_{\pm}(f)/2 \leq \mathrm{rdeg}(f)$.*[1]

Our proof will use the following characterization of rational degree in terms of nondeterministic degrees. The result is folklore and we give a proof for completeness.

[1]The factor of 2 loss is unavoidable: for even n, $\deg_{\pm}(\mathrm{PARITY}_n) = n$ but $\mathrm{rdeg}(\mathrm{PARITY}_n) = n/2$.

Fact 3. *For every Boolean function f,* $\mathrm{rdeg}(f) = \max(\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f))$.

Proof. Let p/q be a rational representation of f with $\max(\deg(p), \deg(q)) = \mathrm{rdeg}(f)$. Then, p and $q - p$ are nondeterministic representations of f and $\neg f$ respectively. Thus,

$$\max(\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f)) \leq \max(\deg(p), \deg(q-p)) \leq \max(\deg(p), \max(\deg(p), \deg(q))) = \mathrm{rdeg}(f).$$

Conversely, let p and q be nondeterministic representations of f and $\neg f$ respectively, with $\deg(p) = \mathrm{ndeg}(f)$ and $\deg(q) = \mathrm{ndeg}(\neg f)$. Then $p/(p+q)$ is a rational representation of f. Thus,

$$\mathrm{rdeg}(f) \leq \max(\deg(p), \deg(p+q)) \leq \max(\deg(p), \max(\deg(p), \deg(q))) = \max(\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f)).$$

Taken together, we obtain $\mathrm{rdeg}(f) = \max(\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f))$, as required. □

We also record the fact that rational degree exactly equals the ϵ-approximate postselected quantum query complexity PostQ_ϵ with $\epsilon = 0$ as defined in [MdW15]. We will not use this fact later but it serves to underscore the tight connection between rational degree and quantum complexity, a connection first observed by Aaronson [Aar05].

Fact 4. *For every Boolean function f,* $\mathrm{rdeg}(f) = \mathrm{PostQ}_0(f)$.

Proof sketch. [MdW15] proves $\mathrm{PostQ}_\epsilon \leq \mathrm{rdeg}(f) \leq 2\,\mathrm{PostQ}_\epsilon(f)$ for all $\epsilon \in [0, 1/2)$. When $\epsilon = 0$, the factor of 2 can be removed by extending the argument in [MdW15]; see Appendix A for details. □

Our proof will relate rational degree to degree via the following three complexity measures.

Definition 5 (Block sensitivity)**.** Let $f\colon \{0,1\}^n \to \{0,1\}$. Let $x \in \{0,1\}^n$. We say that a subset $B \subseteq [n]$ is a *sensitive block* of f at x if $f(x) \neq f(x^B)$, where x^B denotes x with all bits in B flipped. The *block sensitivity* of f at x, denoted $\mathrm{bs}_x(f)$, is the maximum number of disjoint sensitive blocks of f at x.

Definition 6 (Hitting set)**.** For a multilinear polynomial $p := \sum_{S \subseteq [n]} c_S \cdot \prod_{i \in S} X_i \in \mathbb{R}[X_1, \ldots, X_n]$, its *set of maximal monomials* is the set $\mathcal{M}(p) := \{M \subseteq [n]\colon c_M \neq 0,\ c_{M'} = 0 \text{ for all } M' \supsetneq M\}$.[2] We say that $H \subseteq [n]$ is a *hitting set* of p if $H \cap M$ is nonempty for all $M \in \mathcal{M}(p)$.

Definition 7 (Decision tree complexity)**.** The *decision tree complexity* of $f\colon \{0,1\}^n \to \{0,1\}$, denoted $\mathrm{D}(f)$, is the minimum depth of a decision tree (deterministic query algorithm) that, for all $x \in \{0,1\}^n$, queries bits of x to exactly compute $f(x)$ at a leaf.

2.2 Technical tools

Our proof involves using polynomial symmetrization followed by Markov's inequality [Mar90]. The symmetrization we use is folklore, see, e.g., [AKKT20, Lemma 12] where it is attributed to [Shi02], and follows immediately from basic properties of expectation.

Fact 5. *Given multilinear $p \in \mathbb{R}[X_1, \ldots, X_n]$, define $P \in \mathbb{R}[Y]$ by replacing every monomial $\prod_{i \in S} X_i$ appearing in p by $Y^{|S|}$. For $y \in [0,1]$, let B_y^n denote the distribution over $\{0,1\}^n$ where each bit is sampled independently to be 1 with probability y. Then, for all $y \in [0,1]$,*

$$P(y) = \mathrm{E}_{x \sim \mathrm{B}_y^n}[\,p(x)\,]. \tag{1}$$

Furthermore, $\deg(P) \leq \deg(p)$.

[2] Note that this is not the same as $\mathcal{M}'(p) := \{M \subseteq [n]\colon c_M \neq 0 \text{ and } \deg(p) = |M|\}$. While $\mathcal{M}'(p)$ is always contained in $\mathcal{M}(p)$, the containment could be strict. This distinction matters for Section 4.

Theorem 1 (Markov)**.** *Let $P \in \mathbb{R}[X]$. Let $a_1, a_2, b_1, b_2 \in \mathbb{R}$ be such that $a_1 < a_2$ and $b_1 < b_2$. Suppose $P(x) \in [b_1, b_2]$ for all $x \in [a_1, a_2]$. Then, for all $x \in [a_1, a_2]$,*

$$\left|P'(x)\right| \;\leq\; \frac{b_2 - b_1}{a_2 - a_1} \cdot \deg(P)^2. \tag{2}$$

Corollary 1. *Let $p \in \mathbb{R}[X_1, \ldots, X_n]$ and $h > 0$. Suppose that p has the following properties:*

(i) $|p(x)| \leq h$ *for all* $x \in \{0,1\}^n$,

(ii) $|p(0^n)| = h$,

(iii) $p(x) \cdot p(0^n) \leq 0$ *for all* $x \in \{0,1\}^n$ *with* $|x| = 1$.

Then,

$$\sqrt{n/2} \leq \deg(p). \tag{3}$$

Proof. There are two cases to consider: (1) $p(0^n) = h$ and $p(x) \leq 0$ for all $x \in \{0,1\}^n$ with $|x| = 1$; (2) $p(0^n) = -h$ and $p(x) \geq 0$ for all $x \in \{0,1\}^n$ with $|x| = 1$. We give the proof for the first case as the second case then follows from considering $(-p)$. We may assume that p is multilinear without loss of generality and write

$$p = a_0 + (a_1 X_1 + \cdots + a_n X_n) + (\text{higher degree terms}). \tag{4}$$

By assumption $a_0 = p(0^n) = h$. Evaluating p at bitstrings of Hamming weight 1, we see that $a_0 + a_i \leq 0$ for all $i \in [n]$. Hence, $a_i \leq -h$ for all $i \in [n]$. By Fact 5, we obtain $P \in \mathbb{R}[Y]$ with $\deg(P) \leq \deg(p)$, such that, for all $y \in [0,1]$,

$$|P(y)| \leq \mathrm{E}_{x \sim \mathrm{B}_y^n}[\,|p(x)|\,] \leq h. \tag{5}$$

Moreover, we can write

$$P = a_0 + (a_1 + \cdots + a_n)Y + (\text{higher degree terms}). \tag{6}$$

In particular, we see that $P'(0) = a_1 + \cdots + a_n \leq -n \cdot h$. Now Theorem 1 gives

$$n \cdot h \leq \left|P'(0)\right| \leq \frac{h - (-h)}{1 - 0} \cdot \deg(P)^2 = 2h \deg(P)^2. \tag{7}$$

Therefore, $\sqrt{n/2} \leq \deg(P) \leq \deg(p)$, as required. □

The next key lemma relates sensitive blocks of f at x with maximal monomials of a nondeterministic representation of f. It generalizes [BdW02, Lemma 5] (attributed to Nisan and Smolensky) to involve x, nondeterministic representation, and maximal monomials. The proof is the same.

Lemma 1 (Nisan-Smolensky)**.** *Let $f\colon \{0,1\}^n \to \{0,1\}$ be nonconstant and $x \in f^{-1}(0)$. Let p be a nondeterministic representation of f and M be a maximal monomial of p. Then there exists $B \subseteq M$ such that $f(x^B) = 1$.*

Proof. Let q be the restriction of p obtained by fixing all variables outside M according to x. Now M remains a maximal monomial of q. Therefore, q is nonconstant (as a formal polynomial). Therefore, there exists $y \in \{0,1\}^M$ with $q(y) \neq 0$ by uniqueness of multilinear representation. Let $x' \in \{0,1\}^n$ be equal to y on M and be equal to x outside M. Then $p(x') = q(y) \neq 0$, which implies $f(x') = 1$ as p is a nondeterministic representation of f. By definition, x' and x can only differ on M, so x' can be written as x^B for some $B \subseteq M$. □

The next two theorems are used in Section 5. The first, Minsky-Papert [MP69] symmetrization, is used to show the impossibility of generalizing our main result to all partial Boolean functions. The second, a lemma of Nisan and Szegedy from [NS94], which they attribute to Schwartz [Sch80], is used to show a lower bound on the rational degree of Boolean functions depending on n variables. For both theorems we give a concise proof for completeness.

Theorem 2 (Minsky-Papert)**.** *For every $p \in \mathbb{R}[X_1, \ldots, X_n]$, there exists $P \in \mathbb{R}[X]$ such that $\deg(P) \leq \deg(p)$ and, for all $i \in \{0, 1, \ldots, n\}$,*

$$P(i) = \binom{n}{i}^{-1} \sum_{x \in \{0,1\}^n \colon |x| = i} p(x). \tag{8}$$

Proof. Assume p is multilinear without loss of generality. For $i \in \{0, 1, \ldots, n\}$, and d distinct indices $j_1, \ldots, j_d \in [n]$, we have

$$\binom{n}{i}^{-1} \sum_{x \in \{0,1\}^n \colon |x| = i} x_{j_1} \cdots x_{j_d} = \binom{n}{i}^{-1} \binom{n-d}{i-d} = \frac{i(i-1)\cdots(i-d+1)}{n(n-1)\cdots(n-d+1)},$$

which is a polynomial in i of degree d. (Note that when $i < d$, it is the zero polynomial.) Since p is a linear combination of monomials, each of degree at most $\deg(p)$, the theorem follows. □

Theorem 3 ([NS94, Lemma 2.6])**.** *Let $p \in \mathbb{R}[X_1, \ldots, X_n]$ be a nonzero multilinear polynomial. Then, for x chosen uniformly at random from $\{0,1\}^n$, it holds that $\Pr[p(x) \neq 0] \geq 2^{-\deg(p)}$.*

Proof. We give an alternative proof of Theorem 3. If $\deg(p) = 0$, then p must be a nonzero constant, so assume $\deg(p) > 0$. Fix a monomial M of p with $|M| = \deg(p)$. For each of $2^{n-\deg(p)}$ partial assignments to variables outside M, the restricted polynomial has degree $\deg(p) > 0$. Therefore, by uniqueness of multilinear representation, this produces an $x \in \{0,1\}^n$ with $p(x) \neq 0$ that is consistent with each partial assignment. Therefore, $\Pr[p(x) \neq 0] \geq 2^{-n} \cdot 2^{n-\deg(p)} = 2^{-\deg(p)}$. □

3 Rational degree lower bound

Key to our proof is the use of *minimum* block sensitivity over elements of $f^{-1}(b)$ as an intermediary complexity measure. As far as we are aware, this measure has not been previously leveraged in the literature.[3] The next two lemmas show how the measure can be used both as a lower bound and as (part of) an upper bound.

Lemma 2. *For every nonconstant $f \colon \{0,1\}^n \to \{0,1\}$,*

$$\min_{x \in \{0,1\}^n} \mathrm{bs}_x(f) \leq 2 \deg_{\pm}(f)^2. \tag{9}$$

In particular, either

$$\min_{x \in f^{-1}(0)} \mathrm{bs}_x(f) \leq 2 \deg_{\pm}(f)^2 \quad \text{or} \quad \min_{x \in f^{-1}(1)} \mathrm{bs}_x(f) \leq 2 \deg_{\pm}(f)^2. \tag{10}$$

[3] The closest measure that has appeared in the literature may be the minimum certificate complexity, see, e.g., [Tal13; OWZ+14; ACK+21]. We thank Ronald de Wolf for bringing this measure to our attention. This measure will serve to motivate the approach in Section 4.

Proof. Let p be a sign representation of f of degree $\deg_\pm(f)$. Let h be the maximum value of $|p(x)|$ over $x \in \{0,1\}^n$, which is strictly positive. Let $z \in \{0,1\}^n$ be such that $|p(z)| = h$. Let $b \coloneqq \mathrm{bs}_z(f)$, and $B_1, \dots, B_b$ be disjoint sensitive blocks of f at z.

Now consider the function $\tilde{r}\colon \{0,1\}^b \to \mathbb{R}$ defined by $\tilde{r}(t_1, \dots, t_b) = p(x_1, \dots, x_n)$, where

$$x_j = \begin{cases} z_j & \text{if } j \notin \bigsqcup_i B_i, \\ t_i & \text{if } j \in B_i \text{ and } z_j = 0, \\ 1 - t_i & \text{if } j \in B_i \text{ and } z_j = 1. \end{cases} \tag{11}$$

By construction, $\tilde{r}$ can be represented on $\{0,1\}^b$ by a multilinear $r \in \mathbb{R}[X_1, \dots, X_b]$ of degree at most $\deg(p)$. Moreover, $|r(u)| \le h$ for all $u \in \{0,1\}^b$, $\left|r(0^b)\right| = |p(z)| = h$, and $r(u) \cdot r(0^b) \le 0$ for all $u \in \{0,1\}^b$ with $|u| = 1$. Therefore, Corollary 1 gives

$$\sqrt{b/2} \le \deg(r). \tag{12}$$

Therefore,

$$\min_{x \in \{0,1\}^n} \mathrm{bs}_x(f) \le b \le 2\deg(r)^2 \le 2\deg(p)^2 = 2\deg_\pm(f)^2, \tag{13}$$

as required. □

Remark 1. Lemma 2 is false if the min in Eq. (9) is replaced by max as witnessed by the majority function. Moreover, Lemma 2 is optimal up to a (square root) log factor as witnessed by the function $\mathrm{OR}_n \circ \mathrm{AND}_n$. First, $\deg_\pm(\mathrm{OR}_n \circ \mathrm{AND}_n) = O(\sqrt{n \log n})$. We know a polynomial of degree $O(\sqrt{n \log(1/\epsilon)})$ for AND_n that evaluates to 1 on 1-inputs and evaluates within $[0, \epsilon]$ for 0-inputs [KLS96; BCWZ99]. Summing this polynomial for each of the n AND_n gates that feed into the top OR_n gate with $\epsilon = 1/(2n)$, we get a polynomial that is ≥ 1 on 1-inputs and $\le 1/2$ on 0-inputs, which can be made into a sign-representing polynomial by subtracting $3/4$ and then multiplying by (-1). On the other hand, $\mathrm{bs}_x(\mathrm{OR}_n \circ \mathrm{AND}_n) = n$ for every input x, and hence $\min_x \mathrm{bs}_x(\mathrm{OR}_n \circ \mathrm{AND}_n) = n$.

The next lemma is a tightened version of [BdW02, Lemma 6], attributed to Nisan and Smolensky.

Lemma 3. *Let f be a nonconstant Boolean function. Let p, q be nondeterministic representations of f and $\neg f$, respectively. Then, both*

- *p has a hitting set H of size at most $|H| \le \deg(p) \cdot \min_{x \in f^{-1}(0)} \mathrm{bs}_x(f)$, and*
- *q has a hitting set K of size at most $|K| \le \deg(q) \cdot \min_{x \in f^{-1}(1)} \mathrm{bs}_x(f)$.*

Proof. We will prove the lemma for p as the proof is analogous for q.

Let $x \in f^{-1}(0)$. Let $\{M_1, \dots, M_b\}$ be a maximal set of disjoint maximal monomials of p. Then p must have a hitting set of size $\deg(p) \cdot b$. This is because $H \coloneqq \bigsqcup_{i=1}^b M_i$ is a hitting set. Otherwise there is another maximal monomial that we can add to $\{M_1, \dots, M_b\}$. But $b \le \mathrm{bs}_x(f)$ because each M_i contains a sensitive block of f at x by Lemma 1. Therefore, we deduce

$$|H| \le \deg(p) \cdot \mathrm{bs}_x(f). \tag{14}$$

Since x is an arbitrary element from $f^{-1}(0)$, the lemma for p follows. □

Combining Lemmas 2 and 3, we obtain

Corollary 2. *Let f be a nonconstant Boolean function. Let p, q be nondeterministic representations of f and $\neg f$, respectively. Then, either*

- *p has a hitting set of size at most $2\deg(p)\deg_{\pm}(f)^2$, or*
- *q has a hitting set of size at most $2\deg(q)\deg_{\pm}(f)^2$.*

From Corollary 2, we obtain our main theorem by explicitly constructing a decision tree for f using nondeterministic representations of f and $\neg f$.

Theorem 4. *For every Boolean function f,*

$$\mathrm{D}(f) \leq 4\deg_{\pm}(f)^2\,\mathrm{rdeg}(f)^2 \leq 16\,\mathrm{rdeg}(f)^4. \tag{15}$$

Proof. The second inequality follows from Fact 2 so it suffices to prove the first. Let p and q be nondeterministic representations of f and $\neg f$, respectively, such that $\deg(p) = \mathrm{ndeg}(f)$ and $\deg(q) = \mathrm{ndeg}(\neg f)$.

We claim that the following Algorithm 1 gives a deterministic query algorithm that computes f and uses at most $4\deg_{\pm}(f)^2\,\mathrm{rdeg}(f)^2$ queries.

Algorithm 1 Deterministic query algorithm for computing f

1: $i \leftarrow 1$; $(f^1, p^1, q^1) \leftarrow (f, p, q)$
2: **while** f^i is not constant **do**
3: Query a hitting set of p^i of size at most $2\deg(p^i)\deg_{\pm}(f^i)^2$ if it exists, else query a hitting set of q^i of size at most $2\deg(q^i)\deg_{\pm}(f^i)^2$.
4: Set f^{i+1}, p^{i+1}, q^{i+1} to be f^i, p^i, q^i, respectively, but with the variables just queried fixed to their queried values.
5: $i \leftarrow i + 1$
6: **return** constant value of f^i

Since restriction preserves nondeterministic representations, at every iteration of the while loop, p^i is a nondeterministic representation of f^i and q^i is a nondeterministic representation of $\neg f^i$. Therefore, Algorithm 1 is possible by Corollary 2.

First note that the value the algorithm returns on Algorithm 1 must be the value of f on the input. Indeed, f^i is a restriction of f to values queried from the input, and the condition of the while loop ensures that f^i is a constant upon termination.

Next we bound the number of queries the algorithm uses. By the definition of a hitting set, if a hitting set of p^i is queried, then the degree of p^{i+1} must be strictly less than that of p^i. On the other hand, if a hitting set of q^i is queried, then the degree of q^{i+1} must be strictly less than that of q^i. If either p^i or q^i is constant, f^i is constant since p^i, q^i are nondeterministic representations of f^i and $\neg f^i$, respectively. Therefore, the number of iterations that make queries is at most $\deg(p) + \deg(q)$, which is at most $2\,\mathrm{rdeg}(f)$.

Moreover, the number of queries at the ith iteration is at most

$$\begin{aligned}
&2\max(\deg(p^i), \deg(q^i)) \cdot \deg_{\pm}(f^i)^2 && \\
&\leq 2\max(\deg(p), \deg(q)) \cdot \deg_{\pm}(f^i)^2 && (p^i, q^i \text{ are restrictions of } p, q) \\
&= 2\,\mathrm{rdeg}(f)\deg_{\pm}(f^i)^2 && (\text{Fact 3}) \\
&\leq 2\,\mathrm{rdeg}(f)\deg_{\pm}(f)^2 && (f^i \text{ is a restriction of } f).
\end{aligned}$$

Therefore, the total number of queries is at most $4\deg_{\pm}(f)^2\,\mathrm{rdeg}(f)^2$, as required. □

4 Improved lower bound

To understand how the previous proof can be improved, let us recap it in a more modular way. For this we need the notion of certificate complexity. Given $f\colon \{0,1\}^n \to \{0,1\}$ and $x \in \{0,1\}^n$, the certificate complexity of f at x, denoted $\mathrm{C}_x(f)$, is the minimum number of bits of x such that fixing them determines $f(x)$.

Step 1. We start with the argument that upper bounds $\mathrm{D}(f)$ in the proof of Theorem 4. The idea there is that if p is a nondeterministic polynomial for f and we query a hitting set for p, then restricting p to the queried variables produces a polynomial that nondeterministically represents the restricted function, and its degree has dropped by 1 (or more). One simple hitting set for any nondeterministic polynomial for f is any 0-certificate for f. To see this, note that a 0-certificate must intersect with every maximal monomial of a nondeterministic polynomial p. If it did not, then by restricting to those variables we get a function that cannot be identically zero (since it has at least one monomial), so there is some setting of those bits that makes it evaluate to 1. (This is the argument proving Lemma 1.) But then this 1-input is consistent with the 0-certificate, which is a contradiction. This argument shows that querying any 0-certificate reduces the degree of our nondeterministic polynomial by 1. More generally, if we pick the input x with minimum certificate complexity, $\mathrm{C}_{\min}(f) = \min_x \mathrm{C}_x(f)$, this reduces the degree of either the nondeterministic polynomial for f or $\neg f$ by 1, as in the current argument.

It is tempting to now conclude (incorrectly) that $\mathrm{D}(f) \le (\mathrm{ndeg}(f) + \mathrm{ndeg}(\neg f))\,\mathrm{C}_{\min}(f)$ because each query of size $\mathrm{C}_{\min}(f)$ drops the degree of one of these polynomials by at least 1, and hence after $\mathrm{ndeg}(f) + \mathrm{ndeg}(\neg f)$ rounds, we arrive at a trivial polynomial. The flaw in this argument is that after the first step, we have a restriction g of f, and it is not always true that $\mathrm{C}_{\min}(f) \ge \mathrm{C}_{\min}(g)$. This generally happens with all "best-case" complexity measures (i.e., ones where we minimize over inputs instead of maximizing over inputs as done in traditional worst-case measures), because a restriction might kill the best input making the complexity measure larger. The standard solution for such best-case measures is to explicitly define a "downward-closed" version of the measure that maximizes over all restrictions. More formally, we define $\mathrm{C}^{\downarrow}_{\min}(f) = \max_g \mathrm{C}_{\min}(g)$, where g ranges over all restrictions of f. We can now (correctly) conclude that

$$\mathrm{D}(f) \le \big(\mathrm{ndeg}(f) + \mathrm{ndeg}(\neg f)\big)\,\mathrm{C}^{\downarrow}_{\min}(f) \le 2\,\mathrm{rdeg}(f)\,\mathrm{C}^{\downarrow}_{\min}(f). \tag{16}$$

Step 2. We now turn to the argument in Lemma 3 that gives us an upper bound on $\mathrm{C}^{\downarrow}_{\min}(f)$. The standard argument (due to Nisan [Nis91]) that relates $\mathrm{C}(f)$ and $\mathrm{bs}(f)$ says that for every input x, if we take a set of maximal disjoint sensitive blocks, their union is a certificate for x. We know that every input x can have at most $\mathrm{bs}_x(f)$ disjoint sensitive blocks, and each of them can be taken to be a minimal sensitive block, so all we need to do is upper bound the size of the largest minimal sensitive block. A minimal sensitive block of size k on a 0-input is just a copy of the OR function of size k hiding inside our function up to negating the input variables. For example, on the 0^n input, a minimal sensitive block of size k has the property that it evaluates to 0 when at most $k-1$ of its bits are set to 1 and evaluates to 1 when all k bits are set to 1, which is exactly the AND_k function. Similarly for a 1-input we get the $\neg\,\mathrm{AND}_k$ function. In Nisan's standard argument, we upper bound the size of the largest minimal block by $\mathrm{s}(f)$, the sensitivity of f, since the AND and $\neg$ AND functions of size k have sensitivity k. But we can also upper bound it by $\mathrm{rdeg}(f)$, since the AND and $\neg$ AND functions of size k have rational degree k [IJK+25]. This gives us $\mathrm{C}_x(f) \le \mathrm{bs}_x(f)\,\mathrm{rdeg}(f)$. By minimizing over all inputs, we get

$$\mathrm{C}_{\min}(f) \le \mathrm{bs}_{\min}(f)\,\mathrm{rdeg}(f). \tag{17}$$

Step 3. Finally, Lemma 2 already gives us the last part of the argument:

$$\mathrm{bs}_{\min}(f) \leq 2\deg_{\pm}(f)^2. \tag{18}$$

Combining steps 2 and 3 gives us $\mathrm{C}_{\min}(f) \leq 2\deg_{\pm}(f)^2 \operatorname{rdeg}(f)$. To use Step 1, we need to upper bound $\mathrm{C}^{\downarrow}_{\min}(f)$, not $\mathrm{C}_{\min}(f)$. But degree measures do not increase under downward closure, so we immediately get

$$\mathrm{C}^{\downarrow}_{\min}(f) \leq 2\deg_{\pm}(f)^2 \operatorname{rdeg}(f). \tag{19}$$

Combining this with Eq. (16) gives us $\mathrm{D}(f) \leq 4\deg_{\pm}(f)^2 \operatorname{rdeg}(f)^2$.

Slack in the proof. So how can this proof be tightened? Step 1 upper bounds $\mathrm{D}(f)$ using minimum certificate complexity and Step 3 lower bounds sign degree (squared) using minimum block sensitivity, and we know that $\mathrm{C}_{\min}(f)$ and $\mathrm{bs}_{\min}(f)$ can genuinely be different, just like $\mathrm{C}(f)$ and $\mathrm{bs}(f)$ can be different. Can we find a complexity measure that is in between certificate complexity and block sensitivity as a compromise?

In previous work [Tal13; GSS16], it was observed that for every input x, $\mathrm{C}_x(f)$ and $\mathrm{bs}_x(f)$ admit integer-program formulations whose linear-programming (LP) relaxations are dual to each other. Consequently, the optimum values of these relaxations are equal by strong duality. The LP relaxation of $\mathrm{bs}_x(f)$ is called fractional block sensitivity and is denoted $\mathrm{fbs}_x(f)$. The LP relaxation of $\mathrm{C}_x(f)$ is called fractional certificate complexity, but we will instead use an algorithmic interpretation of it called randomized certificate complexity, denoted $\mathrm{RC}_x(f)$, which was first defined in [Aar08].

A clear strategy emerges that replaces the previous three-step strategy:

Step 1. Upgrade $\mathrm{D}(f) \leq 2\operatorname{rdeg}(f)\,\mathrm{C}^{\downarrow}_{\min}(f)$ to have $\mathrm{RC}^{\downarrow}_{\min}(f)$ instead of $\mathrm{C}^{\downarrow}_{\min}(f)$.

Step 2. Use linear programming duality to conclude that $\mathrm{RC}^{\downarrow}_{\min}(f) = O(\mathrm{fbs}^{\downarrow}_{\min}(f))$.

Step 3. Upgrade $\mathrm{bs}_{\min}(f) \leq 2\deg_{\pm}(f)^2$ to have $\mathrm{fbs}_{\min}(f)$ instead of $\mathrm{bs}_{\min}(f)$.

This strategy conceptually mirrors the previous proof. In Step 1, we upper bound $\mathrm{D}(f)$ using RC, which is morally quite similar to C. Informally, both are algorithmic measures, in the sense that it is easy to upper bound them by exhibiting a (deterministic or randomized) certificate. In Step 3, we replace bs with fbs, which are also morally similar, since they are both lower bound measures: it is easy to lower bound them by exhibiting an (integer or fractional) set of sensitive blocks. The old Step 2 used Nisan's argument to relate an algorithmic measure (C) to a lower bound measure (bs). In the new Step 2, we use linear programming duality to relate the algorithmic measure (RC) to the lower bound measure (fbs).

We execute this strategy for the remainder of this section. Our upper bound on $\mathrm{D}(f)$ contains an extra $\log n$ factor, which is why the overall result we obtain is $\mathrm{D}(f) \leq O(\operatorname{rdeg}(f)^3 \log n)$.

4.1 Randomized certificate complexity and fractional block sensitivity

The definition of randomized certificate complexity was first introduced in [Aar08]. The definition uses the notion of randomized decision tree, which is a probability distribution over decision trees.

Definition 8 (Randomized certificate complexity)**.** Let $f\colon \{0,1\}^n \to \{0,1\}$. Let $x \in \{0,1\}^n$. We say that a randomized decision tree τ is an RC-verifier for x (with respect to f) if (i) given input x, τ accepts with probability 1; and (ii) given input $y \in \{0,1\}^n$ such that $f(y) \neq f(x)$, τ rejects with probability $\geq 1/2$. The randomized certificate complexity of f at x, denoted $\mathrm{RC}_x(f)$, is defined to be the minimum expected number of queries made by an RC-verifier for x.

We observe that there always exists an RC-verifier for x that works by nonadaptively querying at most $O(\mathrm{RC}_x(f))$ bits of the input. This will be important for bounding $\mathrm{D}(f)$.

Lemma 4. *Let $f\colon \{0,1\}^n \to \{0,1\}$. Let $x \in \{0,1\}^n$. There exists an* RC*-verifier τ for x that works by sampling a random subset $Q \subseteq [n]$ of size $O(\mathrm{RC}_x(f))$, querying the input on Q, and accepting if and only if the returned values are consistent with x.*

Proof. Let σ be an RC-verifier for x whose expected number of queries is equal to $\mathrm{RC}_x(f)$. By definition, σ is a randomized decision tree, meaning it is a probability distribution $(p_T)_T$ over decision trees T. For each decision tree T with $p_T > 0$, let Q_T denote the set of indices that T queries given input x. Since σ accepts x with probability 1, T must accept x.

Consider the following randomized decision tree τ'': sample Q_T with probability p_T, query the input on Q_T, and accept if and only if the returned values are consistent with x. Given input x, it is clear that τ'' always accepts. Given input $y \in \{0,1\}^n$ such that $f(y) \neq f(x)$,

$$\Pr[\tau'' \text{ accepts } y] = \Pr_T[y \text{ agrees with } x \text{ on } Q_T] \leq \Pr_T[T \text{ accepts } y] < 1/2. \tag{20}$$

Since $\mathrm{E}_T[|Q_T|] \leq \mathrm{RC}_x(f)$, Markov's inequality gives $\Pr_T[|Q_T| \geq 10\,\mathrm{RC}_x(f)] \leq 1/10$. Let τ' be the variant of τ'' such that if Q_T with $|Q_T| \geq 10\,\mathrm{RC}_x(f)$ is sampled, then τ' immediately accepts without making any queries. Given input x, it is clear that τ' always accepts. Given input $y \in \{0,1\}^n$ such that $f(y) \neq f(x)$,

$$\Pr[\tau' \text{ accepts } y] < 1/2 + 1/10. \tag{21}$$

Let τ be defined by repeating τ' twice and accepting if and only if τ' accepts both times. Given input x, it is clear that τ always accepts. Given input $y \in \{0,1\}^n$ such that $f(y) \neq f(x)$,

$$\Pr[\tau \text{ accepts } y] < (1/2 + 1/10)^2 = 0.36 < 1/2. \tag{22}$$

Therefore, τ is an RC-verifier for x that samples a random subset $Q \subseteq [n]$ with $|Q| < 20\,\mathrm{RC}_x(f)$, queries the input on Q, and accepts if and only if the returned values are consistent with x. □

The definition of fractional block sensitivity was first introduced in [Tal13; GSS16].

Definition 9 (Fractional block sensitivity)**.** Let $f\colon \{0,1\}^n \to \{0,1\}$. Let $x \in \{0,1\}^n$. Write $\mathcal{B}$ for the set of sensitive blocks of f at x. The fractional block sensitivity of f at x, denoted $\mathrm{fbs}_x(f)$, is defined to be the optimal value of the following linear program:

$$\begin{aligned} \max \quad & \sum_{B \in \mathcal{B}} w_B \\ \text{s.t.} \quad & \forall B \in \mathcal{B}\colon \ w_B \geq 0 \\ & \forall i \in [n]\colon \sum_{B \in \mathcal{B}\colon i \in B} w_B \leq 1 \end{aligned}$$

(If the w_Bs are restricted to take values in $\{0,1\}$, then the value of the program equals $\mathrm{bs}_x(f)$.)

The following tight relation between $\mathrm{fbs}_x(f)$ and $\mathrm{RC}_x(f)$ was first shown in [Tal13; GSS16].

Theorem 5. *For every $f\colon \{0,1\}^n \to \{0,1\}$ and $x \in \{0,1\}^n$, $\mathrm{fbs}_x(f) = \Theta(\mathrm{RC}_x(f))$.*

Proof. [Tal13, Theorem 2] shows $\mathrm{fbs}_x(f) = \mathrm{FC}_x(f)$ by linear programming duality, where $\mathrm{FC}_x(f)$ is the fractional certificate complexity of f at x. But $\mathrm{FC}_x(f) = \Theta(\mathrm{RC}_x(f))$ by [Tal13, Claim 5.5]. □

To effectively use $\mathrm{RC}_x(f)$ in our proof, it is crucial to consider its minimum, or "best-case" value, over all $x \in \{0,1\}^n$. This is similar to how the use of $\min_{x\in\{0,1\}^n} \mathrm{bs}_x(f)$ is crucial in Section 3. We define this notion generally below.

Definition 10 (Best-case measures)**.** Let $f\colon \{0,1\}^n \to \{0,1\}$ and $x \in \{0,1\}^n$. Let $M_x(f)$ be a local measure of the complexity of f at x. Then we define $M_{\min}(f) \coloneqq \min_{x\in\{0,1\}^n} M_x(f)$.

We will also use downward closure, a notion which has appeared in works such as [LZ17; CG21].

Definition 11 (Downward closure)**.** Let M be a complexity measure of Boolean functions. The downward closure of M, denoted $M^{\downarrow}$, is the complexity measure of Boolean functions defined by $M^{\downarrow}(f) \coloneqq \max_\rho M(f|_\rho)$, where the maximum is taken over all restrictions ρ.

With the above definitions in place, we can state the following corollary of Theorem 5.

Corollary 3. *For every Boolean function f, $\mathrm{RC}^{\downarrow}_{\min}(f) \le O(\mathrm{fbs}^{\downarrow}_{\min}(f))$.*

Proof. Let ρ be a restriction of f and x be an input of $f|_\rho$. Theorem 5 shows $\mathrm{RC}_x(f|_\rho) \le O(\mathrm{fbs}_x(f|_\rho))$. Taking the minimum over x gives $\mathrm{RC}_{\min}(f|_\rho) \le O(\mathrm{fbs}_{\min}(f|_\rho))$. Taking the maximum over ρ gives $\mathrm{RC}^{\downarrow}_{\min}(f) \le O(\mathrm{fbs}^{\downarrow}_{\min}(f))$, as required. □

4.2 Randomized certificate complexity upper bounds decision tree complexity

We establish the following result in this section, which strengthens [Aar08, Theorem 10][4] to involve $\mathrm{RC}^{\downarrow}_{\min}$ and D. In order to involve $\mathrm{RC}^{\downarrow}_{\min}$, we exploit the freedom to choose which RC-verifier to run in the zero-error randomized algorithm used to prove the original theorem. To involve D, we further derandomize that algorithm.

Theorem 6. *For every $f\colon \{0,1\}^n \to \{0,1\}$,*

$$\mathrm{D}(f) \le O\big(\mathrm{rdeg}(f)\ \mathrm{RC}^{\downarrow}_{\min}(f)\ \log n\big). \tag{23}$$

We will use the following two lemmas in the proof. For an RC-verifier τ of the type in Lemma 4, we will identify τ with the distribution from which it samples the subset it queries.

Lemma 5. *Let g be a nonconstant Boolean function and $x \in g^{-1}(0)$. Let p be a nondeterministic representation of g and M be a maximal monomial of p. Suppose τ is an* RC*-verifier for x of the type in Lemma 4, then $\Pr_{Q\sim\tau}[Q \cap M \neq \varnothing] \ge 1/2$.*

Proof. By Lemma 1, there exists $B \subseteq M$ such that $g(x^B) = 1$. By definition, τ accepts x with probability 1. Therefore, if τ rejects x^B, then it must query some of the variables in B. Therefore,

$$\Pr_{Q\sim\tau}[Q \cap M \neq \varnothing] \ge \Pr_{Q\sim\tau}[Q \cap B \neq \varnothing] \ge \Pr[\tau \text{ rejects } x^B] \ge \frac{1}{2}, \tag{24}$$

as required. □

For the next lemma, we need the following definition of a potential function, which is inspired by a similar function used to prove [Aar08, Lemma 9]. This function will serve to track the progress made by the deterministic query algorithm we construct to prove Theorem 6. For a multilinear polynomial r, recall that $\mathcal{M}(r)$ denotes the set of maximal monomials of r.

[4] The original theorem shows $\mathrm{R}_0(f) \le O\big(\mathrm{ndeg}(f) \cdot \max_{x\in\{0,1\}^n} \mathrm{RC}_x(f) \cdot \log n\big)$ for every $f\colon \{0,1\}^n \to \{0,1\}$, where $\mathrm{R}_0(f)$ is the zero-error randomized query complexity of f.

Definition 12 (Potential function)**.** For multilinear $r \in \mathbb{R}[X_1, \ldots, X_m]$, define

$$\Phi(r) \coloneqq \sum_{\varnothing \neq M \in \mathcal{M}(r)} 3^{|M|}|M|! \tag{25}$$

Lemma 6. *Let $g\colon \{0,1\}^m \to \{0,1\}$ be nonconstant. Let r be a nondeterministic representation of g. Then for every $Q \subseteq [m]$ and every restriction r' of r obtained by fixing the variables in Q to arbitrary values, $\Phi(r') \leq \Phi(r)$. Furthermore, for every $x \in g^{-1}(0)$, there exists $Q^* \subseteq [m]$ with $|Q^*| \leq O(\mathrm{RC}_x(g))$ such that, for every restriction r' of r obtained by fixing the variables in Q^* to arbitrary values, $\Phi(r') \leq (3/4)\Phi(r)$.*

Proof. Let $Q \subseteq [m]$ and r' be the restriction of r obtained by fixing the variables in Q to arbitrary values in $\{0,1\}$. It will be convenient to write

$$\Phi^Q_{\mathrm{hit}}(r) \coloneqq \sum_{\substack{\varnothing \neq M \in \mathcal{M}(r)\colon \\ M \cap Q \neq \varnothing}} 3^{|M|}|M|! \quad \text{and} \quad \Phi^Q_{\mathrm{unhit}}(r) \coloneqq \sum_{\substack{\varnothing \neq M \in \mathcal{M}(r)\colon \\ M \cap Q = \varnothing}} 3^{|M|}|M|! \tag{26}$$

These definitions imply $\Phi(r) = \Phi^Q_{\mathrm{hit}}(r) + \Phi^Q_{\mathrm{unhit}}(r)$.

Consider a maximal monomial M of r. If M does not intersect Q, then M remains a maximal monomial of r'. On the other hand, if M does intersect Q, then M cannot be present in r' but it is possible for some submonomials of M to become maximal monomials of r'.[5] Writing $k \coloneqq |M|$, the contribution of such submonomials to $\Phi(r')$ is upper bounded by

$$\sum_{l=1}^{k-1} \binom{k}{l} 3^l l! = 3^k k! \sum_{r=1}^{k-1} \frac{1}{3^r r!} \leq 3^k k! \sum_{r=1}^{\infty} \frac{1}{3^r} = \frac{1}{2} \cdot 3^k k! \tag{27}$$

Since $3^k k!$ is the contribution of M to $\Phi^Q_{\mathrm{hit}}(r)$, we can sum over all maximal monomials M of r that intersect Q to deduce

$$\Phi(r') \leq \Phi^Q_{\mathrm{unhit}}(r) + \frac{1}{2}\Phi^Q_{\mathrm{hit}}(r) = \Phi(r) - \frac{1}{2}\Phi^Q_{\mathrm{hit}}(r). \tag{28}$$

In particular, $\Phi(r') \leq \Phi(r)$.

We now proceed to prove the "furthermore" part. By Lemma 4, there exists an RC-verifier τ for x that works by sampling a random subset $Q \subseteq [m]$ of size $O(\mathrm{RC}_x(g))$ and querying the input on Q. By Lemma 5, $\Pr_{Q\sim\tau}[M \cap Q \neq \varnothing] \geq 1/2$ for every maximal monomial M of r. Therefore,

$$\mathrm{E}_{Q\sim\tau}[\Phi^Q_{\mathrm{hit}}(r)] \geq \frac{1}{2}\Phi(r). \tag{29}$$

In particular, there exists $Q^* \in \mathrm{supp}(\tau)$ such that $\Phi^{Q^*}_{\mathrm{hit}}(r) \geq \Phi(r)/2$. As $Q^* \in \mathrm{supp}(\tau)$, we have $|Q^*| \leq O(\mathrm{RC}_x(g))$. Moreover, Eq. (28) shows that for every restriction r' of r obtained by fixing variables in Q^*, we have $\Phi(r') \leq \Phi(r) - \Phi^{Q^*}_{\mathrm{hit}}(r)/2 \leq (3/4)\Phi(r)$, as required. □

We are now ready to prove Theorem 6.

Proof of Theorem 6. Let p and q be nondeterministic representations of f and $\neg f$, respectively, such that $\deg(p) = \mathrm{ndeg}(f)$ and $\deg(q) = \mathrm{ndeg}(\neg f)$. For a nonconstant Boolean function g, an

[5] For example, consider $r = X_1 + X_1X_2$ and fix X_2 to 0 to obtain $r' = X_1$.

input $x \in g^{-1}(0)$, and a nondeterministic representation r of g, denote by RC-Sets(g, x, r) the sets Q^* satisfying the conditions of Lemma 6 with respect to (g, x, r).

We claim that the following Algorithm 2 gives a deterministic query algorithm that computes f and uses at most $O(\mathrm{rdeg}(f)\ \mathrm{RC}^{\downarrow}_{\min}(f) \log n)$ queries.

Algorithm 2 Deterministic query algorithm for computing f

$\rho \leftarrow \varnothing$ (empty restriction)
while $f|_\rho$ is not constant **do**
  let $x \in \operatorname{argmin}_y \mathrm{RC}_y(f|_\rho)$
  if $f|_\rho(x) = 0$ **then**
    let $Q^* \in$ RC-Sets$(f|_\rho, x, p|_\rho)$
  else
    let $Q^* \in$ RC-Sets$(\neg f|_\rho, x, q|_\rho)$
  Query Q^* and extend ρ according to the queried values
return constant value of $f|_\rho$

Since restriction preserves nondeterministic representations, at every iteration of the while loop, $p|_\rho$ and $q|_\rho$ are nondeterministic representations of $f|_\rho$ and $\neg f|_\rho$, respectively. Therefore, Lemma 6 guarantees that RC-Sets$(f|_\rho, x, p|_\rho)$ and RC-Sets$(\neg f|_\rho, x, q|_\rho)$ are nonempty.

First note that the value the algorithm returns on Algorithm 2 must be the value of f on the input. Indeed, $f|_\rho$ is a restriction of f to values queried from the input, and the condition of the while loop ensures that $f|_\rho$ is a constant upon termination.

Next we bound the number of queries the algorithm uses. Lemma 6 shows that each iteration makes at most $O(\mathrm{RC}^{\downarrow}_{\min}(f))$ queries. Therefore, it suffices to bound the number of iterations by $O(\mathrm{rdeg}(f) \log n)$. We do so by tracking the following potential measure

$$\Phi_\rho \coloneqq \Phi(p|_\rho) \cdot \Phi(q|_\rho), \tag{30}$$

which satisfies the following three properties:

1. Initially, we have $\Phi_\varnothing \le n^{O(\mathrm{rdeg}(f))}$. This is because we can bound the potential of p by the total potential of all possible monomials that could appear in a polynomial of degree $\deg(p) = \mathrm{ndeg}(f)$:

$$\Phi(p) \le \sum_{k=1}^{\mathrm{ndeg}(f)} \binom{n}{k} 3^k k! \le \sum_{k=1}^{\mathrm{ndeg}(f)} (3n)^k \le n^{O(\mathrm{ndeg}(f))}, \tag{31}$$

   and, similarly,

$$\Phi(q) \le n^{O(\mathrm{ndeg}(\neg f))}. \tag{32}$$

   Therefore,

$$\Phi_\varnothing = \Phi(p) \cdot \Phi(q) \le n^{O(\mathrm{ndeg}(f) + \mathrm{ndeg}(\neg f))} \le n^{O(\mathrm{rdeg}(f))}. \tag{33}$$

2. If $\Phi_\rho < 1$, then $f|_\rho$ is constant. This is because $\Phi_\rho < 1$ implies $\Phi(p|_\rho) < 1$ or $\Phi(q|_\rho) < 1$. If $\Phi(p|_\rho) < 1$, then $p|_\rho$ cannot have any nonempty maximal monomials as can be seen from the definition of Φ. Therefore, $p|_\rho$ is constant and so $f|_\rho$ is constant. Similarly, if $\Phi(q|_\rho) < 1$, then $f|_\rho$ is constant.
3. Φ_ρ decreases by a factor of at least $3/4$ at every iteration. This is because Lemma 6 shows that one of $\Phi(p|_\rho)$ or $\Phi(q|_\rho)$ decreases by a factor of at least $3/4$, and the other cannot increase.

Taken together, these three properties imply that the total number of iterations can be bounded by $\log_{4/3}(n^{O(\mathrm{rdeg}(f))}) \le O(\mathrm{rdeg}(f) \log n)$, as required. □

4.3 Fractional block sensitivity lower bounds sign degree

In this subsection, we upgrade Lemma 2 to a lower bound on sign degree by minimum fractional block sensitivity. We implement the upgrade by adapting the proof of [ABK21, Lemma 28].

Lemma 7 (Bounded polynomial for partial-OR)**.** *For every positive integer k, there exists a $q \in \mathbb{R}[X_1, \dots, X_k]$ of degree $\lceil (\pi/2) \cdot \sqrt{k} \rceil$ such that $q(0^k) = 0$ and $q(e_j) = 1$ for all $j \in [k]$ and $q(x) \in [0,1]$ for all $x \in \{0,1\}^k$.*

Proof. Let $d \coloneqq \lceil (\pi/2) \cdot \sqrt{k} \rceil$. Let T_d be the degree-d Chebyshev polynomial of the first kind. Then, define $r \in \mathbb{R}[Z]$ and $q \in \mathbb{R}[X_1, \dots, X_k]$ by

$$r \coloneqq \frac{1 - T_d(1 - (1 - \cos(\pi/d))Z)}{2} \quad \text{and} \quad q \coloneqq r(X_1 + \cdots + X_k). \tag{34}$$

By definition, $T_d(\cos\theta) = \cos(d\theta)$ for all real θ. Therefore, $r(0) = 0$ and $r(1) = 1$, so $q(0^k) = 0$ and $q(e_j) = 1$ for all $j \in [k]$. Moreover, $|T_d(x)| \le 1$ for all $x \in [-1, 1]$, so $r(z) \in [0,1]$ for all $z \in [0, 2/(1 - \cos(\pi/d))]$. Using $1 - \cos(\theta) \le \theta^2/2$ for all real θ, we deduce

$$\frac{2}{1 - \cos(\pi/d)} \ge \frac{4d^2}{\pi^2} \ge k. \tag{35}$$

Hence $r(z) \in [0,1]$ for all $z \in [0, k]$ and therefore $q(x) \in [0,1]$ for all $x \in \{0,1\}^k$. □

We will also need the following fact about multilinear polynomials.

Fact 6 (Multilinear maximum principle)**.** *Let $p \in \mathbb{R}[X_1, \dots, X_n]$. Suppose p is multilinear, then*

$$\max_{x \in \{0,1\}^n} |p(x)| = \max_{\mu \in [0,1]^n} |p(\mu)|. \tag{36}$$

Proof. It suffices to prove $\max_{\mu \in [0,1]^n} |p(\mu)| \le \max_{x \in \{0,1\}^n} |p(x)|$ as the reverse inequality is clear. Fix $\mu \in [0,1]^n$. Let B_μ denote the distribution on $\{0,1\}^n$ where the ith bit is sampled to be 1 with probability μ_i independently. Since p is multilinear, we have $p(\mu) = \mathrm{E}_{x \sim \mathrm{B}_\mu}[p(x)]$. Therefore,

$$|p(\mu)| = \left|\mathrm{E}_{x \sim \mathrm{B}_\mu}[p(x)]\right| \le \mathrm{E}_{x \sim \mathrm{B}_\mu}[|p(x)|] \le \max_{x \in \{0,1\}^n} |p(x)|. \tag{37}$$

Since this holds for all $\mu \in [0,1]^n$, we obtain $\max_{\mu \in [0,1]^n} |p(\mu)| \le \max_{x \in \{0,1\}^n} |p(x)|$, as required. □

Theorem 7. *For every nonconstant Boolean function f,*

$$\mathrm{fbs}^{\downarrow}_{\min}(f) \le \frac{\pi^2}{2} \deg_{\pm}(f)^2. \tag{38}$$

Proof. Let $f \colon \{0,1\}^n \to \{0,1\}$. Let p be a sign representation of f with $\deg(p) = \deg_{\pm}(f)$. Let $z \in \{0,1\}^n$ be such that $|p(z)|$ is maximized.

Fix an arbitrary positive integer k. Let $q \in \mathbb{R}[X_1, \dots, X_k]$ be the polynomial from Lemma 7. Write $q^{(0)}$ for q and $q^{(1)}$ for $1 - q$.

Then define an (nk)-variate polynomial $r \in \mathbb{R}[X_{1,1}, \dots, X_{1,k}, \dots, X_{n,1}, \dots, X_{n,k}]$ by

$$r \coloneqq p\big(\, q^{(z_1)}(X_{1,1}, \dots, X_{1,k}), \dots, q^{(z_n)}(X_{n,1}, \dots, X_{n,k}) \,\big), \tag{39}$$

and define $g \colon \{0,1\}^{nk} \to \{0,1\}$ by $g(x) = 1$ if and only if $r(x) < 0$. For convenience, write $\mathbf{0} \coloneqq 0^{nk}$.

From these definitions, it is clear that $r(\mathbf{0}) = p(z)$ and that

$$\deg(r) \leq \deg(p) \cdot \deg(q) = \deg_{\pm}(f) \cdot \left\lceil \frac{\pi}{2}\sqrt{k} \right\rceil. \tag{40}$$

Since p is multilinear, and $q(x) \in [0,1]$ and $1 - q(x) \in [0,1]$ for all $x \in \{0,1\}^k$, Fact 6 implies $\max_{v \in \{0,1\}^{nk}} |r(v)| \leq |p(z)|$ and equality holds at $v = \mathbf{0}$. Therefore, by the same argument used in the proof of Lemma 2, we have

$$\mathrm{bs}_{\mathbf{0}}(g) \leq 2\deg(r)^2. \tag{41}$$

We now show that

$$k \cdot \mathrm{fbs}_z(f) - 2^n \leq \mathrm{bs}_{\mathbf{0}}(g). \tag{42}$$

Let $\mathcal{B}$ be the collection of sensitive blocks of f at z. Let $\{w_B\}_{B \in \mathcal{B}}$ be an optimal solution to the linear program defining $\mathrm{fbs}_z(f)$. Define integer $W_B \coloneqq \lfloor k \cdot w_B \rfloor$ for each $B \in \mathcal{B}$. Then,

$$\sum_{B \in \mathcal{B}} W_B \geq \sum_{B \in \mathcal{B}} (k \cdot w_B - 1) = k \cdot \mathrm{fbs}_z(f) - |\mathcal{B}| \geq k \cdot \mathrm{fbs}_z(f) - 2^n. \tag{43}$$

For each $B \in \mathcal{B}$, we can associate one or more sensitive blocks of g at $\mathbf{0}$ as follows. Write $B = \{i_1, \ldots, i_m\}$. Then associate the block $B_{\mathrm{lift}} \coloneqq \{(i_1, j_1), \ldots, (i_m, j_m)\}$ for any choice of $j_1, \ldots, j_m \in [k]$. Using the definition of q, we see that $r(\mathbf{0}^{B_{\mathrm{lift}}}) = p(z^B)$. Since p sign-represents f, and r sign-represents g, the block B_{lift} is a sensitive block of g at $\mathbf{0}$. In fact, for each $B \in \mathcal{B}$, we can associate W_B sensitive blocks of g at $\mathbf{0}$, forming a collection $\mathrm{lifts}(B)$, such that all blocks in $\cup_{B \in \mathcal{B}} \mathrm{lifts}(B)$ are pairwise disjoint. This is because, for all $i \in [n]$, we have

$$\sum_{B \ni i} W_B \leq \sum_{B \ni i} k \cdot w_B \leq k. \tag{44}$$

Therefore,

$$\sum_{B \in \mathcal{B}} W_B \leq \mathrm{bs}_{\mathbf{0}}(g). \tag{45}$$

Combining Eqs. (43) and (45) gives Eq. (42) as claimed. By further combining Eq. (42) with Eqs. (40) and (41), we obtain

$$k \cdot \mathrm{fbs}_z(f) - 2^n \leq 2\left(\deg_{\pm}(f) \cdot \left\lceil \frac{\pi}{2}\sqrt{k} \right\rceil\right)^2. \tag{46}$$

Since k is arbitrary, we can divide the preceding equation by k and take the $k \to \infty$ limit to obtain

$$\mathrm{fbs}_z(f) \leq \frac{\pi^2}{2} \deg_{\pm}(f)^2. \tag{47}$$

Since $\mathrm{fbs}_{\min}(f) \leq \mathrm{fbs}_z(f)$, we have

$$\mathrm{fbs}_{\min}(f) \leq \frac{\pi^2}{2} \deg_{\pm}(f)^2. \tag{48}$$

The theorem follows upon noting that the preceding equation holds for all Boolean functions f and that $\deg_{\pm}(f|_\rho) \leq \deg_{\pm}(f)$ for all restrictions ρ. □

4.4 Putting everything together

By combining Corollary 3, Theorem 6, and Theorem 7, we obtain

Theorem 8. *For every* $f\colon \{0,1\}^n \to \{0,1\}$,

$$\mathrm{D}(f) \le O\big(\mathrm{rdeg}(f)\ \deg_{\pm}(f)^2\ \log n\big) \le O\big(\mathrm{rdeg}(f)^3\ \log n\big). \tag{49}$$

Remark 2. The first inequality in Eq. (49) can be tight up to a $\log n$ factor as witnessed by the majority function. It may also be difficult to significantly improve $\mathrm{D}(f) \le O(\mathrm{rdeg}(f)^3 \log n)$ since the best-known upper bound on $\mathrm{D}(f)$ by even $\deg(f)$ is $\mathrm{D}(f) \le O(\deg(f)^3)$ [Mid04].

Theorem 8 is asymptotically stronger than Theorem 4 because of the next theorem. To prove the theorem, we need the notion of influence. For $f\colon \{0,1\}^n \to \{0,1\}$ and $i \in [n]$, the ith *influence* of f is defined by $\mathrm{Inf}_i[f] \coloneqq \Pr[f(x) \neq f(x^i)]$, where x^i is x with the ith bit flipped, and the probability is over uniformly random $x \in \{0,1\}^n$. The *total influence* of f is defined by $\mathrm{Inf}[f] \coloneqq \sum_{i=1}^n \mathrm{Inf}_i[f]$.

Theorem 9. *For every* $f\colon \{0,1\}^n \to \{0,1\}$ *that depends on all* n *variables,* $\mathrm{rdeg}(f) \ge \Omega(\log n)$.

Proof. Let $p/q \in \mathbb{R}(X_1, \dots, X_n)$ be a rational representation of f such that $\max(\deg(p), \deg(q)) = \mathrm{rdeg}(f)$. Fix an arbitrary $i \in [n]$ and define $g\colon \{0,1\}^n \to \{-1,0,1\}$ by

$$g(x) \coloneqq f(x) - f(x^i) = \frac{p(x)}{q(x)} - \frac{p(x^i)}{q(x^i)} = \frac{p(x)q(x^i) - p(x^i)q(x)}{q(x)q(x^i)}, \tag{50}$$

where x^i denotes x with the ith bit flipped.

From the numerator of g, we obtain $r \in \mathbb{R}[X_1, \dots, X_n]$ such that $r(x) = p(x)q(x^i) - p(x^i)q(x)$ for all $x \in \{0,1\}^n$ and $\deg(r) \le \deg(p) + \deg(q) \le 2\,\mathrm{rdeg}(f)$. Observe that $g(x) \neq 0$ if and only if $r(x) \neq 0$. Moreover, observe that g is not constantly zero since f depends on variable i by assumption. Therefore, Theorem 3 gives

$$\mathrm{Inf}_i[f] = \Pr[g(x) \neq 0] = \Pr[r(x) \neq 0] \ge 2^{-\deg(r)} \ge 2^{-2\,\mathrm{rdeg}(f)}. \tag{51}$$

We now sum Eq. (51) over all $i \in [n]$. Combined with Theorem 8 and the fact that $\mathrm{Inf}[f] \le \deg(f)$, this yields

$$\frac{n}{2^{2\,\mathrm{rdeg}(f)}} \le \sum_{i=1}^n \mathrm{Inf}_i[f] = \mathrm{Inf}[f] \le \deg(f) \le O(\mathrm{rdeg}(f)^3 \log n). \tag{52}$$

Rearranging gives $\mathrm{rdeg}(f) \ge \Omega(\log n)$ as required. □

Remark 3. The bound in Theorem 9 is tight for the address function [BdW02]. Eq. (52) in the proof shows that a Boolean function f with rational degree d can depend on at most $O(d^4 2^{2d})$ variables. It may be possible to improve this bound along the lines of [CHS20; Wel22].

We now present some direct corollaries of Theorem 8 that we find most interesting. The first shows that the $\log n$ factor in Eq. (49) can be replaced by $\log \mathrm{rdeg}(f)$ if the left-hand side is relaxed to $\deg(f)$ or $\mathrm{s}(f)$. Here $\mathrm{s}(f)$ denotes the sensitivity of f which is defined as follows. For $f\colon \{0,1\}^n \to \{0,1\}$ and $x \in \{0,1\}^n$, write $\mathrm{s}_x(f)$ for the size of the set $\{i \in [n]\colon f(x) \neq f(x^i)\}$, where x^i denotes x with the ith bit flipped, then $\mathrm{s}(f) \coloneqq \max_{x \in \{0,1\}^n} \mathrm{s}_x(f)$.

Corollary 4. *For every Boolean function* f,

$$\deg(f) \le O\big(\mathrm{rdeg}(f)\ \deg_{\pm}(f)^2\ \log \mathrm{rdeg}(f)\big) \le \widetilde{O}\big(\mathrm{rdeg}(f)^3\big), \tag{53}$$

$$\mathrm{s}(f) \le O\big(\mathrm{rdeg}(f)\ \deg_{\pm}(f)^2\ \log \mathrm{rdeg}(f)\big) \le \widetilde{O}\big(\mathrm{rdeg}(f)^3\big). \tag{54}$$

Proof. Consider Eq. (53) first. As $\mathrm{rdeg}(f)\deg_{\pm}(f)^2\log\mathrm{rdeg}(f) \le \widetilde{O}(\mathrm{rdeg}(f)^3)$, it suffices to prove the first inequality. Let p be the polynomial representation of f and let M be a monomial of p with $|M| = \deg(f)$. Let $f|_M$ denote an arbitrary restriction of f to M. Note that $f|_M$ is defined on $\deg(f)$ variables. Applying Theorem 8 to $f|_M$ gives

$$\deg(f) = \deg(f|_M) \le \mathrm{D}(f|_M) \le O\big(\mathrm{rdeg}(f|_M)\cdot\deg_{\pm}(f|_M)^2\cdot\log\deg(f)\big). \tag{55}$$

Eq. (53) follows from the facts that $\mathrm{rdeg}(f|_M) \le \mathrm{rdeg}(f)$ and $\deg_{\pm}(f|_M) \le \deg_{\pm}(f)$.[6]

Now consider Eq. (54). Let $f\colon \{0,1\}^n \to \{0,1\}$ and $x \in \{0,1\}^n$ be such that $\mathrm{s}(f) = \mathrm{s}_x(f)$. Let $S \coloneqq \{i \in [n]\colon f(x) \ne f(x^i)\}$. Let $f|_S$ denote the restriction of f to S by fixing variables outside S according to x. Since $|S| = \mathrm{s}_x(f) = \mathrm{s}(f)$, $f|_S$ is defined on $\mathrm{s}(f)$ variables. Applying Theorem 8 to $f|_S$ gives

$$\mathrm{s}(f) = \mathrm{s}(f|_S) \le \mathrm{D}(f|_S) \le O\big(\mathrm{rdeg}(f|_S)\cdot\deg_{\pm}(f|_S)^2\cdot\log\mathrm{s}(f)\big). \tag{56}$$

Eq. (54) follows from the facts that $\mathrm{rdeg}(f|_S) \le \mathrm{rdeg}(f)$ and $\deg_{\pm}(f|_S) \le \deg_{\pm}(f)$. □

Remark 4. One may attempt a similar proof strategy to show $\mathrm{D}(f) \le \widetilde{O}(\mathrm{rdeg}(f)^3)$. For this to work, it suffices to show that $\mathrm{D}(f)$ satisfies the following *hardness-condensation* property: for every Boolean function f, there exists a restriction f' of f to $\mathrm{poly}(\mathrm{D}(f))$ variables such that $\mathrm{D}(f) \le O(\mathrm{D}(f'))$. Hardness condensation has been studied previously in [GNRS24] for example.

By adapting the proof of Theorem 8, we can obtain the following corollary.

Corollary 5. *For every Boolean function f,*

$$\deg(f) \le \widetilde{O}\big(\deg_{\mathbb{F}_2}(f)\ \deg_{\pm}(f)^2\big), \tag{57}$$

where $\deg_{\mathbb{F}_2}(f)$ is the minimum degree of $p \in \mathbb{F}_2[X_1,\dots,X_n]$ such that $\forall x \in \{0,1\}^n$, $p(x) = f(x)$.

Proof sketch. Theorem 6 still holds with $\mathrm{rdeg}(f)$ replaced by $\deg_{\mathbb{F}_2}(f)$, as Lemma 1 holds when p is a polynomial representation of f over $\mathbb{F}_2$. □

Remark 5. We find Corollary 5 surprising because both $\deg_{\mathbb{F}_2}(f)$ and $\deg_{\pm}(f)$ are not polynomially related to $\deg(f)$, as witnessed by the parity and majority functions, respectively. This is reminiscent of how neither $\mathrm{C}_0(f)$ nor $\mathrm{C}_1(f)$ are polynomially related to $\deg(f)$ yet $\deg(f) \le \mathrm{C}_0(f)\ \mathrm{C}_1(f)$, where $\mathrm{C}_b(f) \coloneqq \max_{x\in f^{-1}(b)}\mathrm{C}_x(f)$ denotes the b-certificate complexity. But unlike $\mathrm{C}_0(f)$ and $\mathrm{C}_1(f)$, both $\deg_{\mathbb{F}_2}(f)$ and $\deg_{\pm}(f)$ stay invariant under negating f.

The next two corollaries concern $\mathrm{ndeg}(f)$ and $\mathrm{ndeg}(\neg f)$.

Corollary 6. *For every $f\colon \{0,1\}^n \to \{0,1\}$,*

$$\mathrm{D}(f) \le O\big(\mathrm{ndeg}(f)^{1.5}\ \mathrm{ndeg}(\neg f)^{1.5}\ \log n\big) \quad \textit{and} \quad \mathrm{D}(f) \le O\big(\mathrm{ndeg}(f)^2\ \mathrm{ndeg}(\neg f)^2\big). \tag{58}$$

Proof. The first inequality follows from Theorem 8 since $\deg_{\pm}(f) \le O(\min(\mathrm{ndeg}(f),\mathrm{ndeg}(\neg f)))$ and $\mathrm{rdeg}(f) = \max(\mathrm{ndeg}(f),\mathrm{ndeg}(\neg f))$. The second inequality additionally uses Theorem 9. □

Corollary 7. *For every Boolean function f,*

$$\deg(f) \le O\big(\mathrm{ndeg}(f)^{1.5}\ \mathrm{ndeg}(\neg f)^{1.5}\ \log\mathrm{rdeg}(f)\big) \le \widetilde{O}\big(\mathrm{ndeg}(f)^{1.5}\ \mathrm{ndeg}(\neg f)^{1.5}\big). \tag{59}$$

Proof. The corollary follows from Corollary 6 by the same argument as in the proof of Corollary 4. □

[6] If $a/\log a \le O(b)$, there is a constant C such that $a \le Cb\log a$ for all large a. Taking logarithms gives $\log a \le \log b + \log\log a + O(1)$, hence $\log a \le O(\log b)$; substituting back gives $a \le Cb\log a \le O(b\log b)$.

5 Implications and open problems

5.1 Effective Hypercube Nullstellensatz

The main result of this work can be framed as an effective Hypercube Nullstellensatz.

Theorem 10 (Effective Hypercube Nullstellensatz)**.** *Let $g_1, g_2 \in \mathbb{R}[X_1, \ldots, X_n]$. Suppose g_1 and g_2 do not share any common zeros on the hypercube $\{0,1\}^n$. Further suppose $g_1(x) \cdot g_2(x) = 0$ for all $x \in \{0,1\}^n$. Then there exist $h_1, h_2 \in \mathbb{R}[X_1, \ldots, X_n]$ such that*

$$h_1(x)g_1(x) + h_2(x)g_2(x) = 1 \quad \text{for all } x \in \{0,1\}^n, \tag{60}$$

and

$$\max\big(\deg(\overline{h_1 g_1}), \deg(\overline{h_2 g_2})\big) \leq \widetilde{O}\big(\deg(g_1)^{1.5} \deg(g_2)^{1.5}\big), \tag{61}$$

where the overline denotes multilinearization using the relations $X_1^2 = X_1, \ldots, X_n^2 = X_n$.

Proof. Construct polynomials h_1, h_2 satisfying Eq. (60) by interpolation. We proceed to bound $\max(\deg(\overline{h_1 g_1}), \deg(\overline{h_2 g_2}))$. Define $f\colon \{0,1\}^n \to \{0,1\}$ by $f(x) = 0$ if and only if $g_1(x) = 0$. Then by the hypotheses of the theorem, g_1, g_2 are nondeterministic representations of f and $\neg f$, respectively. For every $x \in \{0,1\}^n$, we have $h_1(x)g_1(x) = f(x)$ and $h_2(x)g_2(x) = \neg f(x)$. Therefore by uniqueness of multilinear representation, we deduce $\max(\deg(\overline{h_1 g_1}), \deg(\overline{h_2 g_2})) = \max(\deg(f), \deg(\neg f))$, and the theorem follows from Corollary 7. □

In view of existing Nullstellensatz results, in particular [Jel05], we conjecture that a natural generalization of Theorem 10 to any number of polynomials holds.

Conjecture 1. *For all integers $m \geq 2$, the following holds. Let $0 \neq g_1, \ldots, g_m \in \mathbb{R}[X_1, \ldots, X_n]$. Suppose $g_1, \ldots, g_m$ do not share any common zeros on the hypercube $\{0,1\}^n$. Further suppose $g_1(x) \cdots g_m(x) = 0$ for all $x \in \{0,1\}^n$. Then there exist $h_1, \ldots, h_m \in \mathbb{R}[X_1, \ldots, X_n]$ such that*

$$h_1(x)g_1(x) + \cdots + h_m(x)g_m(x) = 1 \quad \text{for all } x \in \{0,1\}^n, \tag{62}$$

and

$$\max_{i \in [m]}(\deg(\overline{h_i g_i})) \leq \mathrm{poly}(\deg(g_1), \ldots, \deg(g_m)). \tag{63}$$

Again in view of existing Nullstellensatz results, a possible strengthening of the conjecture would have the condition "$g_1(x) \cdots g_m(x) = 0$ for all $x \in \{0,1\}^n$" removed. Such a conjecture would mean that an effective Nullstellensatz holds for all subsets of the hypercube. However, this conjecture is false, even when $m = 2$, as we demonstrate below.[7]

Fact 7. *There exist $g_1, g_2 \in \mathbb{R}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ each of degree 1 that do not share any common zeros on $\{0,1\}^{2n}$ such that: if $h_1, h_2 \in \mathbb{R}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ satisfy*

$$h_1(x)g_1(x) + h_2(x)g_2(x) = 1 \quad \text{for all } x \in \{0,1\}^{2n}, \tag{64}$$

then

$$\max\big(\deg(\overline{h_1 g_1}), \deg(\overline{h_2 g_2})\big) \geq n. \tag{65}$$

[7] In computer science language, Fact 7 shows that rational degree could be much smaller than degree for partial Boolean functions f, even when the (rational) polynomial representation is not required to be bounded outside the domain of f. Such separation cannot be shown by the "Boolean Imbalance" function of [IJK+25], or others like it.

Proof. We give an explicit construction. Let $g_1, g_2 \in \mathbb{R}[X_1, \dots, X_n, Y_1, \dots, Y_n]$ be defined by

$$g_1 \coloneqq X_1 + \cdots + X_n \quad \text{and} \quad g_2 \coloneqq X_1 + \cdots + X_n + Y_1 + \cdots + Y_n - (n+1). \tag{66}$$

Clearly, $\deg(g_1) = \deg(g_2) = 1$, and g_1, g_2 do not share any common zeros on $\{0,1\}^{2n}$.

Let disjoint sets $D_0, D_1 \subseteq \{0,1\}^n \times \{0,1\}^n$ be defined by

$$D_0 \coloneqq \{(x,y) \in \{0,1\}^n \times \{0,1\}^n \colon g_1(x,y) = 0\}, \tag{67}$$
$$D_1 \coloneqq \{(x,y) \in \{0,1\}^n \times \{0,1\}^n \colon g_2(x,y) = 0\}. \tag{68}$$

Let $D \coloneqq D_0 \sqcup D_1$ and define $f \colon D \to \{0,1\}$ by $f(x,y) = 0$ if and only if $(x,y) \in D_0$.

We claim that if $p \in \mathbb{R}[X_1, \dots, X_n, Y_1, \dots, Y_n]$ satisfies $p(x,y) = f(x,y)$ for all $(x,y) \in D$, then $\deg(p) \geq n$. This directly implies that, if h_1, h_2 satisfy Eq. (64), then $\deg(\overline{h_1 g_1}) \geq n$.

We prove the claim using Minsky-Papert symmetrization (Theorem 2). By symmetrizing p, first with respect to the X_is and then the Y_is, we obtain $P \in \mathbb{R}[S,T]$ such that $\deg(P) \leq \deg(p)$ and

$$P(0,t) = 0, \qquad \text{for all } t \in \{0,1,\dots,n\}; \tag{69}$$
$$P(s, n+1-s) = 1, \qquad \text{for all } s \in \{1,\dots,n\}. \tag{70}$$

We then perform case analysis based on the degree of the univariate polynomial $P(0,T) \in \mathbb{R}[T]$:

1. Case $\deg(P(0,T)) \geq n$. Then $\deg(p) \geq \deg(P) \geq \deg(P(0,T)) \geq n$ and the claim holds.
2. Case $\deg(P(0,T)) < n$. Since $P(0,T)$ has at least $n+1$ roots by Eq. (69) and degree less than n, it must be the zero polynomial. Therefore, the polynomial $P(S, n+1-S) - 1$ is not identically zero, since $P(0, n+1) - 1 = -1$. Moreover, by Eq. (70), we see that $P(S, n+1-S) - 1$ has at least n roots. Therefore, $\deg(P(S, n+1-S) - 1) \geq n$. This shows that

$$n \leq \deg(P(S, n+1-S) - 1) \leq \deg(P) \leq \deg(p), \tag{71}$$

and the claim holds.

Since the claim holds in either case, the fact follows. □

5.2 Gotsman-Linial conjecture

The long-standing Gotsman-Linial conjecture [GL94] posits that for every $f \colon \{0,1\}^n \to \{0,1\}$, $\mathrm{Inf}[f] \leq O(\sqrt{n}\deg_{\pm}(f))$. We conjecture the following, which is weaker since $\deg_{\pm}(f)/2 \leq \mathrm{ndeg}(f)$.

Conjecture 2. *For every $f \colon \{0,1\}^n \to \{0,1\}$, $\mathrm{Inf}[f] \leq O(\sqrt{n}\,\mathrm{ndeg}(f))$.*

The motivation for this conjecture is rooted in the origins of this work, namely the observation that existing results on the Gotsman-Linial conjecture [DRST14; HKM14; Kane14] together with an algebraic argument imply $\mathrm{rdeg}(f) \geq \Omega(\sqrt{\log n})$ for every Boolean function f that depends on n variables.[8] Proving that $\mathrm{Inf}[f] \leq O(\sqrt{n}\,\mathrm{ndeg}(f))$ would yield $\mathrm{rdeg}(f) \geq \Omega(\log n)$. We deferred pursuing Conjecture 2 after obtaining Theorem 4, since that theorem yields $\mathrm{rdeg}(f) \geq \Omega(\log n)$ more directly, as the proof of Theorem 9 shows.

[8] For example, [DRST14, Theorem 1.1] shows $\mathrm{Inf}[f] \leq 2^{O(\deg_{\pm}(f))} \cdot \log n \cdot n^{1-1/(4\deg_{\pm}(f)+2)}$, which implies that the same inequality holds with $\deg_{\pm}(f)$ replaced by $2\,\mathrm{rdeg}(f)$. Combining this with $n/2^{2\,\mathrm{rdeg}(f)} \leq \mathrm{Inf}[f]$ — see proof of Theorem 9 — yields $\mathrm{rdeg}(f) \geq \Omega(\sqrt{\log n})$. (Also note that [DRST14] uses the notation "AS" for Inf.)

5.3 Approximate nondeterministic degree

For $f\colon \{0,1\}^n \to \{0,1\}$ and $\epsilon \in [0,1)$, define the ϵ-approximate nondeterministic degree of f, denoted $\mathrm{ndeg}_\epsilon(f)$, to be the minimum degree of a real polynomial p such that, for all $x \in \{0,1\}^n$,

$$\begin{cases} |p(x)| \le \epsilon & \text{if } f(x) = 0, \\ |p(x)| \ge 1 & \text{if } f(x) = 1. \end{cases} \tag{72}$$

It is easy to see that $\mathrm{ndeg}_0(f) = \mathrm{ndeg}(f)$ for all f. The value of ndeg_ϵ also coincides (up to constants) with "deg_ϵ^+" of [She18] and "$\widetilde{\mathrm{odeg}}_\epsilon$" of [BT22].

For constant ϵ, it is easy to adapt the analytic side of our proofs, say Lemma 2, to obtain

Theorem 11. *For every Boolean function f, and constant $\epsilon \in [0,1)$,*

$$\mathrm{D}(f) \le O(\mathrm{ndeg}_\epsilon(f)^2\, \mathrm{ndeg}(\neg f)^2) \quad \textit{and} \quad \mathrm{D}(f) \le O(\mathrm{ndeg}(f)^2\, \mathrm{ndeg}_\epsilon(\neg f)^2). \tag{73}$$

If we could similarly adapt the combinatorial side of our proofs, say Lemma 3, then we would prove the following conjecture.

Conjecture 3. *For every Boolean function f, and constant $\epsilon \in [0,1)$,*

$$\mathrm{D}(f) \le \mathrm{poly}(\max(\mathrm{ndeg}_\epsilon(f), \mathrm{ndeg}_\epsilon(\neg f))). \tag{74}$$

5.4 Improving polynomial relations

Since degree is polynomially related to almost all other Boolean complexity measures, Corollary 4 immediately yields polynomial relations between rational degree and those measures too. It would be interesting to see the extent to which these polynomial relations could be tightened. More specifically, the main results of this work turn all question marks in [IJK+25, Table 1] into either the number 3 or 4 (depending on whether a $\log n$ factor can be removed), but can we obtain matching numbers? In particular, we conjecture that Theorem 8 is optimal up to a $\log n$ factor.

Conjecture 4. *There exists a family of Boolean functions f such that* $\mathrm{D}(f) \ge \Omega(\mathrm{rdeg}(f)^3)$.

The currently best-known separation is quadratic. It can be witnessed by at least two different functions: the balanced AND-OR tree,[9] or the "pointer function" that quadratically separates D from exact quantum query complexity [ABB+17].

We note that [dW03, Section 4] conjectured[10] $\mathrm{D}(f) \le O(\mathrm{ndeg}(f)\ \mathrm{ndeg}(\neg f))$ for every Boolean function f. If true, this would falsify Conjecture 4. However, at the time [dW03] was published, contrived Boolean functions like those constructed in [ABK16; ABB+17] were unknown. More recently (in 2026), Ronald de Wolf informed us of a weaker conjecture:

$$Q_E(f) \overset{?}{\le} O(\mathrm{ndeg}(f)\ \mathrm{ndeg}(\neg f)), \tag{75}$$

where Q_E denotes the exact quantum query complexity of f. If Eq. (75) held, it would be a quantum counterpart to the classical fact $\mathrm{D}(f) \le \mathrm{C}_0(f)\ \mathrm{C}_1(f)$.

[9] The balanced AND-OR tree on m^2 variables also simultaneously separates sign degree, rational degree, and degree: $\mathrm{deg}_\pm = O(\sqrt{m \log m})$ [BT22] (also see Remark 1), $\mathrm{rdeg} = m$ [IJK+25], $\mathrm{deg} = m^2$.

[10] [dW03, Section 4] made this conjecture in the form $\mathrm{D}(f) \le O(\mathrm{NQ}(f)\ \mathrm{NQ}(\neg f))$, but the same paper also showed that $\mathrm{ndeg}(f) = \mathrm{NQ}(f)$. For comparison, Corollary 6 implies $\mathrm{D}(f) \le O(\mathrm{ndeg}(f)^2\, \mathrm{ndeg}(\neg f)^2)$.

Acknowledgments

We thank Lance Fortnow, Joel Friedman, Zbigniew Jelonek, and Ronald de Wolf for helpful discussions, comments, and suggestions. We acknowledge the use of ChatGPT, Claude, and Gemini to search the literature and brainstorm proof strategies for Section 4.

A Rational degree and quantum postselection

In this appendix, we show that rational degree exactly equals the zero-error postselected quantum query complexity. We will need the following technical lemma from [IJK+25].

Lemma 8 ([IJK+25, Lemma 26])**.** *Let N be a positive integer. Let D be a finite set. Let $a_1, \dots, a_N : D \to \mathbb{R}$. Suppose that for all $x \in D$, there exists $i \in [N]$ such that $a_i(x) \neq 0$. Then there exist $c_1, \dots, c_N > 0$ such that, for all $x \in D$, $(c_1 a_1 + \cdots + c_N a_N)(x) \coloneqq c_1 a_1(x) + \cdots + c_N a_N(x) \neq 0$.*

Since the proof is short, we reproduce it below for completeness.

Proof of Lemma 8. Since D is finite, for all $i \in [N]$, there exists $0 < b_i < B_i$ such that $a_i(D) \setminus \{0\}$ is a subset of $(-B_i, -b_i) \cup (b_i, B_i)$. Now define $c_1 = 1$ and for $i = 2, \dots, N$, define $c_i > 0$ by

$$c_i b_i \coloneqq 1 + \sum_{j=1}^{i-1} c_j B_j > \sum_{j=1}^{i-1} c_j B_j. \tag{76}$$

It is straightforward to verify that $(c_1 a_1 + \cdots + c_N a_N)(x) \neq 0$ for all $x \in D$, as required. □

We will use Lemma 8 to show[11]

Fact 4. *For every Boolean function f, $\mathrm{rdeg}(f) = \mathrm{PostQ}_0(f)$.*

Our proof assumes familiarity with the notation and definitions of [MdW15].

Proof. [MdW15, Theorem 2] gives $\mathrm{rdeg}(f) \geq \mathrm{PostQ}_0(f)$ so it suffices to prove $\mathrm{rdeg}(f) \leq \mathrm{PostQ}_0(f)$.

Write $Q \coloneqq \mathrm{PostQ}_0(f)$ for convenience. Suppose there exists a Q-query postselected quantum query algorithm $\mathcal{A}$ that computes f exactly with zero error. Then, using the polynomial method [BBC+01] following [MdW15, Proof of Theorem 1], we deduce that there exists an integer $m \geq 2$ and complex multilinear polynomials $\alpha_s \in \mathbb{C}[X_1, \dots, X_n]$ for all $s \in \{0,1\}^m$ such that:

1. For all $s \in \{0,1\}^m$, the degree of α_s is at most Q;
2. For all inputs $x \in \{0,1\}^n$, when $\mathcal{A}$ is run on x, its state just before postselection is

$$|\psi(x)\rangle \coloneqq \sum_{s \in \{0,1\}^m} \alpha_s(x) |s\rangle; \tag{77}$$

3. For all inputs $x \in \{0,1\}^n$, when $\mathcal{A}$ is run on x, its probability of outputting 1 is

$$r(x) \coloneqq \frac{\sum_{s \in \{0,1\}^m :\, s_1 = 1, s_2 = 1} |\alpha_s(x)|^2}{\sum_{s \in \{0,1\}^m :\, s_1 = 1, s_2 = 1} |\alpha_s(x)|^2 + \sum_{t \in \{0,1\}^m :\, t_1 = 1, t_2 = 0} |\alpha_t(x)|^2} = f(x). \tag{78}$$

(In particular, the denominator of $r(x)$ is strictly positive.)

[11] [IJK+25] uses Lemma 8 for two other purposes: proving an AND-composition lemma for nondeterministic degree, and proving an upper bound on the rational degree of their "Middle Third" function.

For convenience of notation, we will henceforth write

$$S \coloneqq \{s \in \{0,1\}^m \colon s_1 = 1, s_2 = 1\} \quad \text{and} \quad T \coloneqq \{t \in \{0,1\}^m \colon t_1 = 1, t_2 = 0\}. \tag{79}$$

Then, Eq. (78) can be written as

$$r(x) \coloneqq \frac{\sum_{s\in S} |\alpha_s(x)|^2}{\sum_{s\in S} |\alpha_s(x)|^2 + \sum_{t\in T} |\alpha_t(x)|^2} = f(x), \tag{80}$$

which implies:

- For all $x \in f^{-1}(0)$, we have $\sum_{s\in S} |\alpha_s(x)|^2 = 0$ and $\sum_{t\in T} |\alpha_t(x)|^2 \neq 0$. Therefore, $\alpha_s(x) = 0$ for all $s \in S$, and $\alpha_t(x) \neq 0$ for some $t \in T$.
- For all $x \in f^{-1}(1)$, we have $\sum_{s\in S} |\alpha_s(x)|^2 \neq 0$ and $\sum_{t\in T} |\alpha_t(x)|^2 = 0$. Therefore, $\alpha_s(x) \neq 0$ for some $s \in S$, and $\alpha_t(x) = 0$ for all $t \in T$.

For all $s \in \{0,1\}^m$, decompose $\alpha_s \in \mathbb{C}[X_1, \ldots, X_n]$ into its real and imaginary parts:

$$\alpha_s = a_{s,0} + i a_{s,1}, \tag{81}$$

where $a_{s,0}, a_{s,1} \in \mathbb{R}[X_1, \ldots, X_n]$ each have degree at most Q.

Since a complex number is zero if and only if its real and imaginary parts are both zero, we see:

- For all $x \in f^{-1}(0)$, we have $a_s(x) = 0$ for all $s \in S \times \{0,1\}$, and $a_t(x) \neq 0$ for some $t \in T \times \{0,1\}$.
- For all $x \in f^{-1}(1)$, we have $a_s(x) \neq 0$ for some $s \in S \times \{0,1\}$, and $a_t(x) = 0$ for all $t \in T \times \{0,1\}$.

Then, Lemma 8 gives $c_t > 0$ for all $t \in T \times \{0,1\}$ and $c_s > 0$ for all $s \in S \times \{0,1\}$ such that:

- For all $x \in f^{-1}(0)$, we have $\sum_{t\in T\times\{0,1\}} c_t \cdot a_t(x) \neq 0$.
- For all $x \in f^{-1}(1)$, we have $\sum_{s\in S\times\{0,1\}} c_s \cdot a_s(x) \neq 0$.

Therefore, it is clear that $R \in \mathbb{R}(X_1, \ldots, X_n)$ defined by

$$R \coloneqq \frac{\sum_{s\in S\times\{0,1\}} c_s \cdot a_s}{\sum_{s\in S\times\{0,1\}} c_s \cdot a_s + \sum_{t\in T\times\{0,1\}} c_t \cdot a_t} \tag{82}$$

is a rational representation of f, and the degrees of R's numerator and denominator are each at most Q. Therefore, $\mathrm{rdeg}(f) \leq Q = \mathrm{PostQ}_0(f)$, as required. □

References

[Aar05] Scott Aaronson. "Quantum computing, postselection, and probabilistic polynomial-time". In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 461.2063 (2005), pp. 3473–3482. doi:10.1098/rspa.2005.1546. arXiv:quant-ph/0412187.

[Aar08] Scott Aaronson. "Quantum certificate complexity". In: *Journal of Computer and System Sciences* 74.3 (2008), pp. 313–322. doi:10.1016/j.jcss.2007.06.020. arXiv:quant-ph/0210020.

[ABK16] Scott Aaronson, Shalev Ben-David, and Robin Kothari. "Separations in query complexity using cheat sheets". In: *Proceedings of the 48th Annual ACM Symposium on Theory of Computing (STOC)*. 2016, pp. 863–876. doi:10.1145/2897518.2897644. arXiv:1511.01937.

[ABK+21] Scott Aaronson, Shalev Ben-David, Robin Kothari, Shravas Rao, and Avishay Tal. "Degree vs. approximate degree and quantum implications of Huang's sensitivity theorem". In: *Proceedings of the 53rd Annual ACM Symposium on Theory of Computing (STOC)*. 2021, pp. 1330–1342. doi:10.1145/3406325.3451047. arXiv:2010.12629.

[AKKT20] Scott Aaronson, Robin Kothari, William Kretschmer, and Justin Thaler. "Quantum Lower Bounds for Approximate Counting via Laurent Polynomials". In: *Proceedings of the 35th Computational Complexity Conference (CCC)*. Vol. 169. 2020, 7:1–7:47. doi:10.4230/LIPIcs.CCC.2020.7. arXiv:1904.08914.

[Alon99] Noga Alon. "Combinatorial Nullstellensatz". In: *Combinatorics, Probability and Computing* 8.1–2 (1999), pp. 7–29. doi:10.1017/S0963548398003411.

[ABCO88] Noga Alon, Ernest E. Bergmann, Don Coppersmith, and Andrew M. Odlyzko. "Balancing sets of vectors". In: *IEEE Trans. Inf. Theor.* 34.1 (1988), pp. 128–130. doi:10.1109/18.2610.

[AF93] Noga Alon and Zoltán Füredi. "Covering the Cube by Affine Hyperplanes". In: *European Journal of Combinatorics* 14.2 (1993), pp. 79–83. doi:10.1006/eujc.1993.1011.

[ABB+17] Andris Ambainis, Kaspars Balodis, Aleksandrs Belovs, Troy Lee, Miklos Santha, and Juris Smotrovs. "Separations in Query Complexity Based on Pointer Functions". In: *Journal of the ACM* 64.5 (2017). doi:10.1145/3106234. arXiv:1506.04719.

[ABK21] Anurag Anshu, Shalev Ben-David, and Srijita Kundu. "On Query-To-Communication Lifting for Adversary Bounds". In: *Proceedings of the 36th Computational Complexity Conference (CCC)*. Vol. 200. 2021, 30:1–30:39. doi:10.4230/LIPIcs.CCC.2021.30. arXiv:2012.03415.

[ACK+21] Srinivasan Arunachalam, Sourav Chakraborty, Michal Koucký, Nitin Saurabh, and Ronald de Wolf. "Improved Bounds on Fourier Entropy and Min-entropy". In: *ACM Trans. Comput. Theory* 13.4 (2021). doi:10.1145/3470860. arXiv:1809.09819.

[BBC+01] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. "Quantum lower bounds by polynomials". In: *Journal of the ACM* 48.4 (2001), pp. 778–797. doi:10.1145/502090.502097. arXiv:quant-ph/9802049.

[Bro87] W. Dale Brownawell. "Bounds for the Degrees in the Nullstellensatz". In: *Annals of Mathematics* 126.3 (1987), pp. 577–591. doi:10.2307/1971361.

[BdW02] Harry Buhrman and Ronald de Wolf. "Complexity measures and decision tree complexity: a survey". In: *Theoretical Computer Science* 288.1 (2002). Complexity and Logic, pp. 21–43. doi:10.1016/S0304-3975(01)00144-X.

[BCWZ99] Harry Buhrman, Richard Cleve, Ronald de Wolf, and Christof Zalka. "Bounds for Small-Error and Zero-Error Quantum Algorithms". In: *Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*. 1999, pp. 358–368. doi:10.1109/SFFCS.1999.814607. arXiv:cs/9904019.

[BT22] Mark Bun and Justin Thaler. "Approximate Degree in Classical and Quantum Computing". In: *Foundations and Trends in Theoretical Computer Science* 15.3–4 (2022), pp. 229–423. doi:10.1561/0400000107.

[Cade20] Chris W. Cade. "Quantum Algorithms and Complexity in Non-standard Models". Doctor of Philosophy (PhD) Thesis. University of Bristol, 2020.

[CG21] Siddhesh Chaubal and Anna Gál. "Diameter Versus Certificate Complexity of Boolean Functions". In: *46th International Symposium on Mathematical Foundations of Computer Science (MFCS)*. Vol. 202. 2021, 31:1–31:22. doi:10.4230/LIPIcs.MFCS.2021.31.

[CHS20] John Chiarelli, Pooya Hatami, and Michael Saks. "An Asymptotically Tight Bound on the Number of Relevant Variables in a Bounded Degree Boolean function". In: *Combinatorica* 40.2 (2020), pp. 237–244. doi:10.1007/s00493-019-4136-7. arXiv:1801.08564.

[DRST14] Ilias Diakonikolas, Prasad Raghavendra, Rocco A. Servedio, and Li-Yang Tan. "Average Sensitivity and Noise Sensitivity of Polynomial Threshold Functions". In: *SIAM Journal on Computing* 43.1 (2014), pp. 231–253. doi:10.1137/110855223. arXiv:0909.5011.

[FFKL03] Stephen Fenner, Lance Fortnow, Stuart A. Kurtz, and Lide Li. "An oracle builder's toolkit". In: *Information and Computation* 182.2 (2003), pp. 95–136. doi:10.1016/S0890-5401(03)00018-X.

[For03] Lance Fortnow. Computational Complexity Blog, https://blog.computationalcomplexity.org/2003/11/rational-functions-and-decision-tree.html. 2003.

[For26] Lance Fortnow. Personal communication. 2026.

[GSS16] Justin Gilmer, Michael Saks, and Srikanth Srinivasan. "Composition limits and separating examples for some boolean function complexity measures". In: *Combinatorica* 36.3 (2016), pp. 265–311. doi:10.1007/s00493-014-3189-x. arXiv:1306.0630.

[GNRS24] Mika Göös, Ilan Newman, Artur Riazanov, and Dmitry Sokolov. "Hardness condensation by restriction". In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC)*. 2024, pp. 2016–2027. doi:10.1145/3618260.3649711. ECCC:2023/181.

[GL94] Craig Gotsman and Nathan Linial. "Spectral properties of threshold functions". In: *Combinatorica* 14.1 (1994), pp. 35–50. doi:10.1007/BF01305949.

[HKM14] Prahladh Harsha, Adam Klivans, and Raghu Meka. "Bounding the Sensitivity of Polynomial Threshold Functions". In: *Theory of Computing* 10.1 (2014), pp. 1–26. doi:10.4086/toc.2014.v010a001. arXiv:0909.5175.

[IJK+25] Vishnu Iyer, Siddhartha Jain, Robin Kothari, Matt Kovacs-Deak, Vinayak M. Kumar, Luke Schaeffer, Daochen Wang, and Michael Whitmeyer. *On the Rational Degree of Boolean Functions and Applications*. 2025. arXiv:2310.08004.

[Jel05] Zbigniew Jelonek. "On the effective Nullstellensatz". In: *Inventiones mathematicae* 162.1 (2005), pp. 1–17. doi:10.1007/s00222-004-0434-8.

[KLS96] Jeff Kahn, Nathan Linial, and Alex Samorodnitsky. "Inclusion-Exclusion: Exact and Approximate". In: *Combinatorica* 16.4 (1996), pp. 465–477. doi:10.1007/BF01271266.

[Kane14] Daniel M. Kane. "The correct exponent for the Gotsman–Linial Conjecture". In: *computational complexity* 23.2 (2014), pp. 151–175. doi:10.1007/s00037-014-0086-z. arXiv:1210.1283.

[Kol88] János Kollár. "Sharp Effective Nullstellensatz". In: *Journal of the American Mathematical Society* 1.4 (1988), pp. 963–975. doi:10.2307/1990996.

[LZ17] Chengyu Lin and Shengyu Zhang. "Sensitivity Conjecture and Log-Rank Conjecture for Functions with Small Alternating Numbers". In: *Proceedings of the 44th International Colloquium on Automata, Languages, and Programming (ICALP)*. Vol. 80. 2017, 51:1–51:15. doi:10.4230/LIPIcs.ICALP.2017.51. arXiv:1602.06627.

[MdW15] Urmila Mahadev and Ronald de Wolf. "Rational approximations and quantum algorithms with postselection". In: *Quantum Info. Comput.* 15.3–4 (2015), pp. 295–307. doi:10.5555/2871393.2871398. arXiv:1401.0912.

[Mar90] Andrei Andreyevich Markov. "On a question by D. I. Mendeleev". In: *Zapiski Imperatorskoi Akademii Nauk* 62 (1890), pp. 1–24.

[Mid04] Gatis Midrijanis. *Exact quantum query complexity for total Boolean functions*. 2004. arXiv:quant-ph/0403168.

[MP69] Marvin Minsky and Seymour A. Papert. *Perceptrons: An Introduction to Computational Geometry*. The MIT Press, 1969. doi:10.7551/mitpress/11301.001.0001.

[Nis91] Noam Nisan. "CREW PRAMs and Decision Trees". In: *SIAM Journal on Computing* 20.6 (1991), pp. 999–1007. doi:10.1137/0220062.

[NS94] Noam Nisan and Mario Szegedy. "On the degree of Boolean functions as real polynomials". In: *computational complexity* 4.4 (1994), pp. 301–313. doi:10.1007/BF01263419.

[O'D14] Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014. arXiv:2105.10386.

[OWZ+14] Ryan O'Donnell, John Wright, Yu Zhao, Xiaorui Sun, and Li-Yang Tan. "A Composition Theorem for Parity Kill Number". In: *Proceedings of the 29th Computational Complexity Conference (CCC)*. 2014, pp. 144–154. doi:10.1109/CCC.2014.22. arXiv:1312.2143.

[Saks93] Michael E. Saks. "Slicing the hypercube". In: *Surveys in Combinatorics, 1993*. Cambridge University Press, 1993, pp. 211–255. doi:10.5555/164558.164579.

[Sch80] Jacob T. Schwartz. "Fast Probabilistic Algorithms for Verification of Polynomial Identities". In: *Journal of the ACM* 27.4 (1980), pp. 701–717. doi:10.1145/322217.322225.

[She13] Alexander A. Sherstov. TCS+ talk, https://www.youtube.com/live/fp5mIceFED4?si=RF_Gbywn8Rr4QMj1&t=3904. 2013.

[She18] Alexander A. Sherstov. "Breaking the Minsky–Papert Barrier for Constant-Depth Circuits". In: *SIAM Journal on Computing* 47.5 (2018), pp. 1809–1857. doi:10.1137/15M1015704.

[Shi02] Yaoyun Shi. *Approximating linear restrictions of Boolean functions*. Manuscript. 2002.

[Smo93] Roman Smolensky. "On representations by low-degree polynomials". In: *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*. 1993, pp. 130–138. doi:10.1109/SFCS.1993.366874.

[Tal13] Avishay Tal. "Properties and applications of Boolean function composition". In: *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science (ITCS)*. 2013, pp. 441–454. doi:10.1145/2422436.2422485. ECCC: 2012/163.

[Wel22] Jake Wellens. "Relationships between the number of inputs and other complexity measures of Boolean functions". In: *Discrete Analysis* (2022). arXiv:2005.00566.

[dW00] Ronald de Wolf. "Characterization of non-deterministic quantum query and quantum communication complexity". In: *Proceedings of the 15th Computational Complexity Conference (CCC)*. 2000, pp. 271–278. doi:10.1109/CCC.2000.856758.

[dW01] Ronald de Wolf. "Quantum Computing and Communication Complexity". Doctor of Philosophy (PhD) Thesis. Universiteit van Amsterdam, 2001.

[dW03] Ronald de Wolf. "Nondeterministic Quantum Query and Communication Complexities". In: *SIAM Journal on Computing* 32.3 (2003), pp. 681–699. doi:10.1137/S0097539702407345. arXiv:cs/0001014.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il