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

Rational degree is polynomially related to degree

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

Abstract

We prove that $\deg(f) \leq 2\,\mathrm{rdeg}(f)^4$ 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 degree.

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; 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 [Saks20; 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 4.1.
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].

*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 $\deg(f) \leq 2\,\mathrm{rdeg}(f)^4$ for every Boolean function f. In fact, we prove the stronger result that $\deg(f) \leq O(\deg_{\pm}(f)^2\,\mathrm{rdeg}(f)^2)$. We end by discussing a variety of implications and open problems.

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 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 $p(x) \neq 0$ for all $x \in \{0,1\}^n$, and $p(x) < 0$ 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.

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

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

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 maxonomials* is the set $\mathcal{M}(p) := \{M \subseteq [n]\colon |M| = \deg(p), c_M \neq 0\}$. 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 $D(f)$, is the minimum depth of a decision tree 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 $p \in \mathbb{R}[X_1, \ldots, X_n]$, 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, $\deg(P) \leq \deg(p)$.

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 $x \in [a_1, a_2]$,*

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

The next corollary of Fact 5 and Theorem 1 was shown to us by Robin Kothari, who kindly allowed us to reproduce his proof. (Our original approach used a variant of the next corollary, obtained from [BdW02, Lemma 2 and Theorem 3], which gave a somewhat worse bound: $\sqrt{n/3} \leq \deg(p)$.)

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 is analogous. 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 $y \in [0,1]$,

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

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 two theorems are used in Section 4. 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. 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. If $\deg(p) = 0$, then p must be a nonzero constant, so assume $\deg(p) > 0$. Fix a maxonomial M of 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.[2] The next two lemmas show how the measure can be used both as a lower bound and as (part of) an upper bound.

Lemma 1. *For every nonconstant Boolean function f,*

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

In particular, either

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

Proof. Let p be a sign representation of $f \colon \{0,1\}^n \to \{0,1\}$ 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 $B_1, \ldots, B_b$ be disjoint sensitive blocks of f at z.

Now consider the function $\tilde{r} \colon \{0,1\}^b \to \mathbb{R}$ defined by $\tilde{r}(t_1, \ldots, t_b) = p(x_1, \ldots, x_n)$, 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 $r \in \mathbb{R}[X_1, \ldots, X_b]$ of degree at most $\deg(p)$. Moreover, $|r(u)| \leq h$ for all $u \in \{0,1\}^b$, $\left|r(0^b)\right| = |p(z)| = h$, and $r(u) \cdot r(0^b) \leq 0$ for all $u \in \{0,1\}^b$ with $|u| = 1$. Therefore, Corollary 1 gives

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

[2] 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.

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 1 is false if the min in Eq. (9) is replaced by max. To see this, let n be even and consider $f\colon \{0,1\}^n \to \{0,1\}$ defined by $f(x) = 0$ if and only if $|x| = n/2$. We have $\deg_\pm(f) \le 2$ yet $\max_{x\in\{0,1\}^n} \mathrm{bs}_x(f) \ge \mathrm{bs}_{1^{n/2}0^{n/2}}(f) \ge n$.

The next lemma can be viewed as a tightened version of [BdW02, Lemmas 5 and 6], attributed to Nisan and Smolensky.[3] A key idea of its proof already appears in our proof of Theorem 3.

Lemma 2. *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 $H \coloneqq \{M_1, \dots, M_b\}$ be a maximal set of disjoint maxonomials of p. Then p must have a hitting set of size $\deg(p) \cdot b$. This is because $\bigsqcup_{i=1}^{b} M_i$ is a hitting set. Otherwise there is another maxonomial that we can add to H.

We now show that $b \le \mathrm{bs}_x(f)$. It suffices to show that each M_i contains a sensitive block of f at x. By fixing all variables of p with indices outside of M_i to their corresponding values in x, we obtain a multilinear polynomial r defined on $\deg(p)$ variables with $\deg(r) = \deg(p) > 0$. Then there must exist a $\deg(p)$-bit string z such that $r(z) \neq 0$. (Otherwise we have a contradiction as r must be the zero polynomial by uniqueness of multilinear representation.) Since p is a nondeterministic representation of f, this means M_i must contain a sensitive block of f at x.

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 1 and 2, 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,*

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

Proof. 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 build a deterministic decision tree for f as follows.

[3] We thank Ronald de Wolf for bringing this interpretation to our attention.

Set $i \leftarrow 1$. Set $f^1 \leftarrow f$, $p^1 \leftarrow p$, $q^1 \leftarrow q$. Then repeat the following.

1. If f^i is constant, output its constant value and stop. Else continue.
2. 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 $2\deg(q^i)\deg_\pm(f^i)^2$.
3. 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.
4. Set $i \leftarrow i+1$.

Observe that p^i is a nondeterministic representation of f^i; q^i is a nondeterministic representation of $\neg f^i$; and Step 2 is possible by Corollary 2.

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

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

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

Since $\deg_\pm(f) \le 2\,\mathrm{rdeg}(f)$ and $\deg(f) \le D(f)$, we immediately obtain

Corollary 3. *For every Boolean function f,*

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

By adapting the above proof, we could also obtain the following.

Corollary 4. *For every Boolean function f,*

$$\deg(f) \le D(f) \le 2\,\mathrm{ndeg}(f)^2\,\mathrm{ndeg}(\neg f)^2 \le 2\,\mathrm{rdeg}(f)^4. \tag{17}$$

Proof sketch. Adapt the proof of Lemma 1 to give $\min_{x\in f^{-1}(0)} \mathrm{bs}_x(f) \le 2\,\mathrm{ndeg}(\neg f)^2$, and adapt the proof of Theorem 4 so that only a hitting set of p^i is queried. □

Remark 2. The bound on D in terms of rdeg is technically stronger in Corollary 4 than in Corollary 3 when comparing constant factors.[4] However, by Fact 3, we have

$$\mathrm{ndeg}(f)^2\,\mathrm{ndeg}(\neg f)^2 = \min(\mathrm{ndeg}(f),\mathrm{ndeg}(\neg f))^2\cdot\mathrm{rdeg}(f)^2. \tag{18}$$

Since the left-hand side of the inequality $(\deg_\pm(f)/2)^2 \le \min(\mathrm{ndeg}(f),\mathrm{ndeg}(\neg f))^2$ can be much smaller than the right,[5] we generally prefer the bound in Corollary 3 involving sign degree.

[4] There is also an interesting sense in which $D(f) \le 2\,\mathrm{rdeg}(f)^4$ is stronger than $D(f) \le 16\,\mathrm{rdeg}(f)^4$: the former inequality is tight for the two-bit parity function, but we do not know of any function for which the latter is tight.

[5] The Majority function MAJ_n has $\deg_\pm(\mathrm{MAJ}_n) = 1$, but $\min(\mathrm{ndeg}(\mathrm{MAJ}_n), \mathrm{ndeg}(\neg\,\mathrm{MAJ}_n)) \ge n/2$. Threshold functions with threshold near $n/2$, as well as functions constructed in [She21], give similarly large separations.

4 Implications and open problems

4.1 Effective Hypercube Nullstellensatz

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

Theorem 5 (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*

$$h_1(x)g_1(x) + h_2(x)g_2(x) = 1 \quad \text{for all } x \in \{0,1\}^n, \tag{19}$$

and

$$\max(\deg(\overline{h_1 g_1}), \deg(\overline{h_2 g_2})) \leq 2\deg(g_1)^2 \deg(g_2)^2, \tag{20}$$

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. (19) 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 4. □

In view of existing Nullstellensatz results, we conjecture that a natural generalization of Theorem 5 to any number of polynomials holds.

Conjecture 1. *For all integers $m \geq 2$, the following holds. Let $g_1, \ldots, g_m \in \mathbb{R}[X_1, \ldots, X_n]$. 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*

$$h_1(x)g_1(x) + \cdots + h_m(x)g_m(x) = 1 \quad \text{for all } x \in \{0,1\}^n, \tag{21}$$

and

$$\max_{i \in [m]}(\deg(\overline{h_i g_i})) \leq \text{poly}(\deg(g_1), \ldots, \deg(g_m)). \tag{22}$$

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.[6]

Fact 6. *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*

$$h_1(x)g_1(x) + h_2(x)g_2(x) = 1 \quad \text{for all } x \in \{0,1\}^{2n}, \tag{23}$$

then

$$\max(\deg(\overline{h_1 g_1}), \deg(\overline{h_2 g_2})) \geq n. \tag{24}$$

[6] In computer science language, Fact 6 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

$$g_1 \coloneqq X_1 + \cdots + X_n \quad \text{and} \quad g_2 \coloneqq X_1 + \cdots + X_n + Y_1 + \cdots + Y_n - (n+1). \tag{25}$$

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

$$D_0 \coloneqq \{(x,y) \in \{0,1\}^n \times \{0,1\}^n \colon g_1(x,y) = 0\}, \tag{26}$$
$$D_1 \coloneqq \{(x,y) \in \{0,1\}^n \times \{0,1\}^n \colon g_2(x,y) = 0\}. \tag{27}$$

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. (23), 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

$$P(0,t) = 0, \qquad \text{for all } t \in \{0,1,\dots,n\}; \tag{28}$$
$$P(s,n+1-s) = 1, \qquad \text{for all } s \in \{1,\dots,n\}. \tag{29}$$

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. (28) 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. (29), 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

$$n \leq \deg(P(S,n+1-S)-1) \leq \deg(P) \leq \deg(p), \tag{30}$$

and the claim holds.

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

4.2 Gotsman-Linial conjecture

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 $\mathrm{Inf}[f] \coloneqq \sum_{i=1}^n \mathrm{Inf}_i[f]$.

The long-standing Gotsman-Linial conjecture [GL94] posits that $\mathrm{Inf}[f] \leq O(\sqrt{n}\deg_\pm(f))$. We make the following conjecture, which is weaker[7] 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; Kane20] 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 Corollary 3, since the corollary together with the aforementioned algebraic argument yields $\mathrm{rdeg}(f) \geq \Omega(\log n)$ more directly, as we show below. Note that this bound is tight for the address function [BdW02].

[7] Though the conjecture, if true, would still be tight, as witnessed by the function in Remark 1.

[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 6 — yields $\mathrm{rdeg}(f) \geq \Omega(\sqrt{\log n})$. (Also note that [DRST14] uses the notation "AS" for Inf.)

Theorem 6. *For every $f\colon \{0,1\}^n \to \{0,1\}$ that depends on all n variables,* $\operatorname{rdeg}(f) \geq \Omega(\log n)$.

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

$$g(x) \coloneqq f(x) - f(x^i) = \frac{p(x)}{q(x)} - \frac{p(x^i)}{q(x^i)} = \frac{p(x)q(x^i) - p(x^i)q(x)}{q(x)q(x^i)}, \tag{31}$$

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

From the numerator of g, we obtain $r \in \mathbb{R}[X_1, \ldots, X_n]$ such that $r(x) = p(x)q(x^i) - p(x^i)q(x)$ for all $x \in \{0,1\}^n$ and $\deg(r) \leq \deg(p) + \deg(q) \leq 2\operatorname{rdeg}(f)$. 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

$$\operatorname{Inf}_i[f] = \Pr[g(x) \neq 0] = \Pr[r(x) \neq 0] \geq 2^{-\deg(r)} \geq 2^{-2\operatorname{rdeg}(f)}. \tag{32}$$

We now unfix i and sum Eq. (32) over all $i \in [n]$. Combined with Corollary 3 and the fact that $\operatorname{Inf}[f] \leq \deg(f)$, this yields

$$\frac{n}{2^{2\operatorname{rdeg}(f)}} \leq \sum_{i=1}^{n} \operatorname{Inf}_i[f] = \operatorname{Inf}[f] \leq \deg(f) \leq O(\operatorname{rdeg}(f)^4). \tag{33}$$

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

Note that Eq. (33) in the proof of Theorem 6 shows that a Boolean function f with rational degree d can depend on at most $O(d^4 2^{2d})$ variables. It would be interesting to see whether this bound could be tightened along the lines of [CHS20; Wel22].

4.3 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 $\operatorname{ndeg}_\epsilon(f)$, to be the minimum degree of a real polynomial p such that, for all $x \in \{0,1\}^n$,

$$\begin{cases} |p(x)| \leq \epsilon & \text{if } f(x) = 0, \\ |p(x)| \geq 1 & \text{if } f(x) = 1. \end{cases} \tag{34}$$

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

For constant ϵ, it is easy to adapt the analytic side of our proof, namely Lemma 1, to prove

Theorem 7. *For every Boolean function f, and constant $\epsilon \in [0,1)$,*

$$D(f) \leq O(\operatorname{ndeg}_\epsilon(f)^2 \operatorname{ndeg}(\neg f)^2) \quad \text{and} \quad D(f) \leq O(\operatorname{ndeg}(f)^2 \operatorname{ndeg}_\epsilon(\neg f)^2). \tag{35}$$

If we could similarly adapt the combinatorial side of our proof, namely Lemma 2, then we would prove the following conjecture.

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

$$D(f) \leq O(\operatorname{ndeg}_\epsilon(f)^2 \operatorname{ndeg}_\epsilon(\neg f)^2). \tag{36}$$

4.4 Improving polynomial relations

Since degree is polynomially related to almost all other Boolean complexity measures, Corollary 3 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, this work turns all question marks in [IJK+25, Table 1] into the number 4, but can we obtain matching numbers?

We conjecture that Corollary 3 is optimal with respect to D versus rdeg.

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

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] $D(f) \leq O(\mathrm{ndeg}(f) \cdot \mathrm{ndeg}(\neg f))$ 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:

$$Q_E(f) \overset{?}{\leq} O(\mathrm{ndeg}(f) \cdot \mathrm{ndeg}(\neg f)), \tag{37}$$

where Q_E denotes the exact quantum query complexity of f. If Eq. (37) held, it would be a quantum counterpart to the classical fact $D(f) \leq C_0(f) \cdot C_1(f)$, where C_b denotes the b-certificate complexity.

Acknowledgments

We thank Lance Fortnow, Joel Friedman, Zbigniew Jelonek, Robin Kothari, and Ronald de Wolf for helpful discussions, comments, and suggestions. In particular, we thank Robin for observing that our original proof of $\deg(f) \leq O(\mathrm{rdeg}(f)^4)$ could be adapted to give $\deg(f) \leq O(\deg_\pm(f)^2 \,\mathrm{rdeg}(f)^2)$.

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 3 ([IJK+25, Lemma 26])**.** *Let N be a positive integer. Let D be a finite set. Let $a_1, \ldots, a_N \colon D \to \mathbb{R}$. Suppose that for all $x \in D$, there exists $i \in [N]$ such that $a_i(x) \neq 0$. Then there exist $c_1, \ldots, c_N > 0$ 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 3. 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 $i = 2, \ldots, N$, define $c_i > 0$ by

$$c_i b_i \coloneqq 1 + \sum_{j=1}^{i-1} c_j B_j > \sum_{j=1}^{i-1} c_j B_j. \tag{38}$$

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. □

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

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

We will use Lemma 3 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 integer $m \geq 2$ and complex multilinear polynomials $\alpha_s \in \mathbb{C}[X_1, \ldots, X_n]$ 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

$$|\psi(x)\rangle \coloneqq \sum_{s \in \{0,1\}^m} \alpha_s(x)|s\rangle; \tag{39}$$

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

$$r(x) \coloneqq \frac{\sum_{s \in \{0,1\}^m \colon s_1=1, s_2=1} |\alpha_s(x)|^2}{\sum_{s \in \{0,1\}^m \colon s_1=1, s_2=1} |\alpha_s(x)|^2 + \sum_{t \in \{0,1\}^m \colon t_1=1, t_2=0} |\alpha_t(x)|^2} = f(x). \tag{40}$$

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

For convenience of notation, we will henceforth write

$$S \coloneqq \{s \in \{0,1\}^m \colon s_1 = 1, s_2 = 1\} \quad \text{and} \quad T \coloneqq \{t \in \{0,1\}^m \colon t_1 = 1, t_2 = 0\}. \tag{41}$$

Then, Eq. (40) can be written as

$$r(x) \coloneqq \frac{\sum_{s \in S} |\alpha_s(x)|^2}{\sum_{s \in S} |\alpha_s(x)|^2 + \sum_{t \in T} |\alpha_t(x)|^2} = f(x), \tag{42}$$

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:

$$\alpha_s = a_{s,0} + i a_{s,1}, \tag{43}$$

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:

[11] [IJK+25] uses Lemma 3 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 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 3 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

$$R \coloneqq \frac{\sum_{s \in S \times \{0,1\}} c_s \cdot a_s}{\sum_{s \in S \times \{0,1\}} c_s \cdot a_s + \sum_{t \in T \times \{0,1\}} c_t \cdot a_t} \tag{44}$$

is a rational representation of f, and the degree 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] S. 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] S. 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.

[ABB+17] A. Ambainis, K. Balodis, A. Belovs, T. Lee, M. Santha, and J. Smotrovs. "Separations in Query Complexity Based on Pointer Functions". In: *J. ACM* 64.5 (2017). doi:10.1145/3106234. arXiv:1506.04719.

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

[ABK+21] S. Aaronson, S. Ben-David, R. Kothari, S. Rao, and A. 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.

[ABK16] S. Aaronson, S. Ben-David, and R. 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.

[ACK+21] S. Arunachalam, S. Chakraborty, M. Koucký, N. Saurabh, and R. 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.

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

[AKKT20] S. Aaronson, R. Kothari, W. Kretschmer, and J. Thaler. "Quantum lower bounds for approximate counting via Laurent polynomials". In: *Proceedings of the 35th Computational Complexity Conference (CCC)*. 2020. doi:10.4230/LIPIcs.CCC.2020.7. arXiv:1904.08914.

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

[BBC+01] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. "Quantum lower bounds by polynomials". In: *J. ACM* 48.4 (2001), pp. 778–797. doi:10.1145/502090.502097.

[BdW02] H. Buhrman and R. 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.

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

[BT22] M. Bun and J. 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] C. W. Cade. "Quantum Algorithms and Complexity in Non-standard Models". Doctor of Philosophy (PhD) Thesis. University of Bristol, 2020.

[CHS20] J. Chiarelli, P. Hatami, and M. 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] I. Diakonikolas, P. Raghavendra, R. A. Servedio, and L.-Y. 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.

[dW00] R. 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] R. de Wolf. "Quantum Computing and Communication Complexity". Doctor of Philosophy (PhD) Thesis. Universiteit van Amsterdam, 2001.

[dW03] R. 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.

[FFKL03] S. Fenner, L. Fortnow, S. A. Kurtz, and L. 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] L. Fortnow. Computational Complexity Blog, https://blog.computationalcomplexity.org/2003/11/rational-functions-and-decision-tree.html. 2003.

[For26] L. Fortnow. Personal communication. 2026.

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

[HKM14] P. Harsha, A. Klivans, and R. 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] V. Iyer, S. Jain, R. Kothari, M. Kovacs-Deak, V. M. Kumar, L. Schaeffer, D. Wang, and M. Whitmeyer. *On the Rational Degree of Boolean Functions and Applications*. 2025. arXiv:2310.08004.

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

[Kane20] D. 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] J. Kollár. "Sharp Effective Nullstellensatz". In: *Journal of the American Mathematical Society* 1.4 (1988), pp. 963–975. doi:10.2307/1990996.

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

[MdW15] U. Mahadev and R. 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.

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

[NS94] N. Nisan and M. 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] R. O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014. arXiv:2105.10386.

[OWZ+14] R. O'Donnell, J. Wright, Y. Zhao, X. Sun, and L.-Y. Tan. "A Composition Theorem for Parity Kill Number". In: *Proceeding of the 29th Computational Complexity Conference (CCC)*. 2014, pp. 144–154. doi:10.1109/CCC.2014.22.

[Saks20] M. E. Saks. "Slicing the hypercube". In: *Surveys in Combinatorics, 1993*. Cambridge University Press, 1993, pp. 211–255. doi:10.5555/164558.164579.

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

[She18] A. 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.

[She21] A. A. Sherstov. "The hardest halfspace". In: *computational complexity* 30.2 (2021), p. 11. doi:10.1007/s00037-021-00211-4. arXiv:1902.01765.

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

[Smo93] R. 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] A. 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] J. Wellens. "Relationships between the number of inputs and other complexity measures of Boolean functions". In: *Discrete Analysis* (2022). arXiv:2005.00566.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il