On the Rational Degree of Boolean Functions and Applications

Vishnu Iyer
UT Austin

Siddhartha Jain
UT Austin

Matt Kovacs-Deak
University of Maryland

Vinayak M. Kumar
UT Austin

Luke Schaeffer
University of Maryland

Daochen Wang
University of Maryland

Michael Whitmeyer
University of Washington

Abstract

We study a natural complexity measure of Boolean functions known as the (exact) rational degree. For total functions f, it is conjectured that $\mathrm{rdeg}(f)$ is polynomially related to $\deg(f)$, where $\deg(f)$ is the Fourier degree. Towards this conjecture, we show that symmetric functions have rational degree at least $\deg(f)/2$ and monotone functions have rational degree at least $\sqrt{\deg(f)}$. We observe that both of these lower bounds are tight. In addition, we show that all read-once depth-d Boolean formulae have rational degree at least $\Omega(\deg(f)^{1/d})$. Furthermore, we show that almost every Boolean function on n variables has rational degree at least $n/2 - \mathcal{O}(\sqrt{n})$.

In contrast to total functions, we exhibit partial functions that witness unbounded separations between rational and approximate degree, in both directions. As a consequence, we show that for quantum computers, post-selection and bounded-error are incomparable resources in the black-box model.

1 Introduction

Starting with the seminal work of Minsky and Papert [MP69], a long line of research has sought to relate various measures of Boolean function complexity. In [NS92], Nisan and Szegedy proved that the deterministic decision tree complexity $\mathrm{D}(f)$ of a Boolean function f is polynomially related to its degree $\deg(f)$ as a multilinear polynomial. The same paper posed two open questions. One of them conjectures that the sensitivity and block sensitivity of a Boolean function are polynomially related. This conjecture was recently proven in a breakthrough by Huang [Hua19]. Huang's result brought sensitivity into a "happy flock" of complexity measures on total Boolean functions that are all polynomially related: sensitivity, degree, approximate degree, and notions of query complexity.

Another natural measure of Boolean function complexity is the minimal degree of a rational polynomial which represents the function exactly, called the *rational degree* (denoted rdeg). However, rdeg is *not* known to be either polynomially related to or separated from the complexity measures mentioned above. In fact, this was the other open question posed over 30 years ago in the paper of Nisan and Szegedy (via personal communication with Fortnow) [NS92]. This question was reiterated by Aaronson *et al.* [ABDK+21] yet very little progress has been made toward its resolution.

Question 1 (Fortnow [NS92])**.** Does there exist $c > 1$ such that for all total Boolean functions f, $\deg(f) \leq \mathcal{O}(\mathrm{rdeg}(f)^c)$?

One of the motivations for Fortnow's question was complexity-theoretic: is the intersection of $\mathsf{C_{=}P}$ and $\mathsf{coC_{=}P}$ strictly contained in PP with respect to a generic oracle [For03]? $\mathsf{C_{=}P}$ and $\mathsf{coC_{=}P}$ are "counting classes" [AK] which we define later, and rational degree corresponds to the black-box version of their intersection.

The rational degree is also related to quantum query complexity. In particular, de Wolf defined the *non-deterministic degree* $\mathrm{ndeg}(f)$ of a Boolean function f as the minimal degree of a polynomial whose zero set is precisely the set of inputs on which f evaluates to false [Wol00], and related it to the rational degree through the identity $\mathrm{rdeg}(f) = \max\{\mathrm{ndeg}(f), \mathrm{ndeg}(\bar{f})\}$. de Wolf also proved that the non-deterministic degree $\mathrm{ndeg}(f)$ equals the *non-deterministic quantum query complexity* up to a constant factor.

In the same manuscript, de Wolf stated the following conjecture which, together with the inequality $\deg(f) \leq \mathrm{D}(f)$, would resolve Fortnow's question in the affirmative with $c = 2$.

Conjecture 1 (de Wolf [Wol00])**.** *For all Boolean functions f, $\mathrm{D}(f) \leq \mathcal{O}(\mathrm{ndeg}(f)\,\mathrm{ndeg}(\bar{f}))$.*

Mahadev and de Wolf showed [MW15] an even tighter connection between the notion of rational degree and quantum query complexity: denoting by $\mathrm{rdeg}_\varepsilon(f)$ the minimum degree of a rational polynomial that ε-approximates f pointwise, they showed that $\mathrm{rdeg}_\varepsilon(f)$ equals (up to a constant factor) the query complexity of a quantum algorithm with *post-selection*[1] that computes f with error ε. For partial functions, it can be shown that the rational degree gives a lower bound on the query complexity of algorithms with post-selection, though the opposite direction is not known to be true. Furthermore, this result extends to the case of $\varepsilon = 0$, the so-called "zero-error" setting.

1.1 Our Results

We prove lower bounds on the rational degree for certain classes of total Boolean functions. We summarize our results according to section:

Sec 3.1 For symmetric functions we show that $\deg(f)/2 \leq \mathrm{rdeg}(f)$. This lower bound is tight, as witnessed by the PARITY_n function. Our technique for symmetric functions generalizes to classes of functions including ones which are constant on many Hamming weights.

Sec 3.2 We employ the lower bound on symmetric functions to show that for depth-d Boolean formulae, $\mathrm{rdeg}(f) \geq \Omega(\deg(f)^{1/d})$. For $d = 2$ this is tight, as witnessed by the $\mathsf{AND}_n \circ \mathsf{OR}_n$ function.

Sec 3.3 For monotone functions we prove that $\mathrm{rdeg}(f) = \mathrm{s}(f) \geq \sqrt{\deg(f)}$. This is also tight as witnessed by the $\mathsf{AND}_n \circ \mathsf{OR}_n$ function.

Sec 3.4 Our final lower bound on total functions is extremal: we prove that almost all Boolean functions on n bits have rational degree at least $n/2 - \mathcal{O}(\sqrt{n})$.

On the other hand, we show that for partial functions, the rational and approximate degrees can be unboundedly separated in both directions. These separations also resolve an open question of Fortnow [For03].

Sec 4.1 We give a partial function $\textsc{MajOrNone}_n$ on n bits with constant quantum query complexity yet rational degree $\Omega(n)$. As a result, $\textsc{MajOrNone}_n$ has constant approximate degree and $\Omega(n)$ zero-error post-selected quantum query complexity.

Sec 4.2 On the other hand, we give a partial function $\textsc{Imbalance}_n$ on n bits with approximate degree $\Omega(n)$ yet constant rational degree. As a result, $\textsc{Imbalance}_n$ has constant zero-error post-selected quantum query complexity and quantum query complexity $\Omega(n)$.

[1] Post-selection is an operation that allows for projection onto an efficiently computable set of basis states for free, even if this set accounts for an arbitrarily small fraction of the probability mass.

	Rational Degree Lower Bound	Attained By
Symmetric Functions	$\deg(f)/2$	PARITY_n
Monotone Functions	$\sqrt{\deg(f)}$	$\mathsf{AND}_n \circ \mathsf{OR}_n$
Read-once CNF/DNF Formulae	$\Omega(\sqrt{\deg(f)})$	$\mathsf{AND}_n \circ \mathsf{OR}_n$
Read-once Depth d Formulae	$\Omega(\deg(f)^{1/d})$	—
Almost all $f\colon \{0,1\}^n \to \{0,1\}$	$n/2 - \mathcal{O}(\sqrt{n})$	N/A

Figure 1: A table summarizing our lower bounds on rational degree for total functions. The third column gives an example of a function that demonstrates the tightness of our lower bound, where applicable.

Now, employing the framework of standard complexity results such as [FSS81], we can argue that post-selection and bounded error are incomparable resources in the black-box setting. To formalise this, we define $\mathsf{PostEQP}$ as the class of decision problems which can be decided deterministically in polynomial time by quantum computers with access to post-selection. In particular, there exists a bidirectional separation between $\mathsf{PostEQP}$ and BQP with respect to generic oracles. Formally, combining the results of Corollaries 18 and 22 we get the following statement.

Corollary 1. *There exist oracles O_1 and O_2 such that $\mathsf{BQP}^{O_1} \not\subseteq \mathsf{PostEQP}^{O_1}$ yet $\mathsf{PostEQP}^{O_2} \not\subseteq \mathsf{BQP}^{O_2}$.*

These complexity-theoretic consequences are summarized in Figure 2. As the figure illustrates, these are the strongest possible separations in the black-box model.

In addition to these consequences for $\mathsf{PostEQP}$, our lower bound also resolves Fortnow's complexity-theoretic question. We show that not only is $\mathsf{C_=P} \cap \mathsf{coC_=P}$ strictly contained in PP, even RP is not in this intersection with respect to a generic oracle. The class $\mathsf{C_=P}$ is the set of languages decidable by an NP machine such that if the string is in the language, the number of accepting paths is *exactly* equal to the number of rejecting paths. Finally, to contextualize the power of $\mathsf{PostEQP}$, we provide strong evidence that zero-error post-selection can offer advantage over efficient classical computation, even in the non-relativized setting.

Sec 4.3 We show that $\mathsf{PostEQP}$ contains $\mathsf{NP} \cap \mathsf{coNP}$. We remark that $\mathsf{NP} \cap \mathsf{coNP}$ is not even believed to be contained in BPP.

2 Preliminaries

In this section we review some of the notation and definitions used in our paper. For a more comprehensive introduction to the analysis of Boolean functions see [Sak93, O'D14]. We denote by $[n]$ the set $\{1, 2, ..., n\}$. Given a function $f\colon S \to \mathbb{R}$ we denote by $\|f\|_1$ its l_1 norm, $\|f\|_1 = \sum_{x \in S} |f(x)|$. For a bitstring $x \in \{0,1\}^n$, we denote by $|x|$ the Hamming weight of x: the number of indices equal to 1. If $x \in \{-1,1\}^n$ the Hamming weight is the number of bits that equal -1.

2.1 Boolean Functions

A (total) Boolean function is any function $f\colon \Sigma^n \to \Sigma$ where Σ is some two-element set. We will refer to the set Σ^n as the Boolean hypercube. We will primarily work over the sets $\Sigma = \{0,1\}$ and

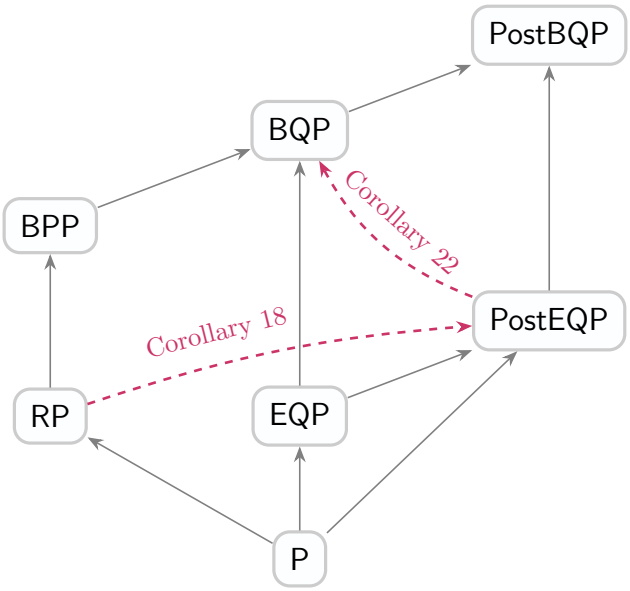

Figure 2: Relevant complexity classes. We are able to obtain the strongest possible oracle separations in this picture. An arrow $\mathsf{A} \to \mathsf{B}$ means $\mathsf{A} \subseteq \mathsf{B}$ relative to all oracles. A dashed arrow $\mathsf{A} \dashrightarrow \mathsf{B}$ means $\mathsf{A} \not\subseteq \mathsf{B}$ relative to some oracle.

$\Sigma = \{-1, 1\}$. The mapping $t \mapsto (t+1)/2$ maps $\{-1, 1\}$ onto $\{0, 1\}$. While not all Boolean complexity measures are left invariant by this change of representation, all of the measures considered in this paper are preserved.

We also consider restrictions of Boolean functions to proper subsets of the Boolean cube $D \subset \Sigma^n$. We refer to such functions $f\colon D \to \Sigma$ as *partial* Boolean functions. Given a Boolean function f, we denote its negation by $\bar{f}$. We can define an inner product on the space of functions $f\colon \{-1, 1\}^n \to \mathbb{R}$:

$$\langle f, g \rangle = 2^{-n} \sum_{x \in \{-1,1\}^n} f(x)g(x).$$

For each $S \subseteq [n]$ we define the *character function* χ_S *on* S as $\chi_S(x) = \prod_{i \in S} x_i$. The character functions χ_S form an orthonormal basis under the above inner product. Thus each function over $\{-1, 1\}^n$ can be uniquely expressed via its *Fourier representation*:

$$f = \sum_{S \subseteq [n]} \widehat{f}(S) \cdot \chi_S,$$

where we refer to $\widehat{f}(S) = \langle f, \chi_S \rangle$ as the *Fourier coefficient of* f *at* S. We say an input $i \in [n]$ is *relevant* for f if x_i appears in the Fourier expansion for f. In other words, f depends on x_i in a nontrivial manner.

2.2 Polynomials

As described above, each Boolean function can be represented uniquely as a formal multilinear polynomial through its Fourier representation. We define the Fourier *degree* (or simply degree)

of f as $\deg(f) = \max\{|S| : \widehat{f}(S) \neq 0\}$. We can extend this notion to polynomials that pointwise approximate f:

Definition 2. Let $D \subseteq \{-1,1\}^n$ and $f\colon D \to \{-1,1\}$. A polynomial $p : \{-1,1\}^n \to \mathbb{R}$ is said to ε-approximate f if for all $x \in D$, $|p(x) - f(x)| \leq \varepsilon$ and for all $x \in \{-1,1\}^n$, $|p(x)| \leq 1$. The *ε-approximate degree* of f, denoted $\widetilde{\deg}_\varepsilon(f)$, is defined as the minimum degree of any polynomial that ε-approximates f. The *degree* of f, denoted $\deg(f)$, is defined as $\widetilde{\deg}_0(f)$. The *approximate degree* of f, denoted $\widetilde{\deg}(f)$, is defined as $\widetilde{\deg}_{1/3}(f)$.

In this paper, we are primarily concerned with representations of f via rational polynomials. This gives rise to a measure known as *rational degree*, which is formally defined as follows.

Definition 3. Let $D \subseteq \{-1,1\}^n$ and $f\colon D \to \{-1,1\}$. If $p\colon D \to \mathbb{R}$ and $q\colon D \to \mathbb{R}$ are polynomials such that $|f(x) - p(x)/q(x)| \leq \varepsilon$ for all $x \in D$, we say that p/q is an ε-approximate rational representation of f. The *ε-approximate rational degree* of f, denoted $\mathrm{rdeg}_\varepsilon(f)$, is defined as the minimum value of $\max\{\deg(p), \deg(q)\}$ such that p/q is an ε-approximate rational representation of f. The *rational degree* of f, denoted $\mathrm{rdeg}(f)$, is defined as $\mathrm{rdeg}_0(f)$.

Unlike in the definition of approximate degree, there is no requirement for an approximate rational representation to be bounded outside of D. Whether or not such a boundedness condition is imposed matters significantly for the degree (see [BKT20]) but not for the rational degree (see Appendix A).

2.3 Sensitivity and Certificate Complexity

We now define some useful combinatorial measures of Boolean function complexity. Let f be a Boolean function, $x \in \{-1,1\}^n$, and $B \subseteq [n]$. We say that B is a sensitive block of f at x if $f(x) \neq f(x^B)$ where x^B denotes the bitstring obtained by flipping all bits of x indexed by B. We define, and denote by $\mathrm{bs}_f(x)$, the *block sensitivity of f at x* as the maximum number of disjoint blocks that are all sensitive at x. By restricting our attention to sensitive blocks that are singletons we obtain the analogous notion of the *sensitivity of f at x*, denoted $\mathrm{s}_f(x)$. The block sensitivity of f is defined as $\mathrm{bs}(f) = \max_x \mathrm{bs}_f(x)$. Similarly the *sensitivity of f* is defined as $\mathrm{s}(f) = \max_x \mathrm{s}_f(x)$. For $b \in \{0,1\}$, we also write $\mathrm{s}^{(b)}(f) = \max_{x \in f^{-1}(b)} \mathrm{s}_f(x)$.

A partial assignment is some function $\rho : [n] \to \{-1,1,\star\}$. We define, and denote by $|\rho|$, the size of the partial assignment ρ as cardinality of the set $\{i \in [n] : \rho(i) \neq \star\}$. We say that a partial assignment ρ is *consistent* with some $x \in \{-1,1\}^n$ if $x_i = \rho(i)$ for all i with $\rho(i) \neq \star$. Given a Boolean function f we denote by $f|_\rho$ the restriction of f to the set of inputs $x \in \{-1,1\}^n$ that are consistent with ρ. Given $b \in \{-1,1\}$, we say that a partial assignment ρ is a *b-certificate for f* if $f|_\rho(x) = b$ for all $x \in \mathrm{Dom}(f|_\rho)$. The *$b$-certificate complexity* of f is defined as

$$\mathrm{C}_b(f) = \max_{x \in f^{-1}(b)} \min\{|\rho| : \rho \text{ is a } b\text{-certificate for } f \text{ consistent with } x\}.$$

The *certificate complexity of f* is defined as $\mathrm{C}(f) = \max_{b \in \{-1,1\}} \mathrm{C}_b(f)$.

2.4 Sign and Non-Deterministic Degree

For a Boolean function f we say that a polynomial $p : \{-1,1\}^n \to \mathbb{R}$ is a *(strong) sign representation* if $\mathrm{sgn}(p(x)) = f(x)$ for all $x \in \{-1,1\}^n$ and $p(x) \neq 0$ on the entire hypercube. The *(strong) sign degree* of f is defined as the minimum degree of any polynomial that strongly sign represents f. Alon [Alo93] and Anthony [Ant95] have shown that all but a negligible fraction of n-bit Boolean

functions have sign degree at least $n/2$. Later, O'Donnell and Servedio proved [OS08] that almost every Boolean function has sign degree at most $n/2 + \mathcal{O}(\sqrt{n \log n})$.

A less common but somewhat similar notion is that of a *non-deterministic polynomial* introduced by de Wolf [Wol00]. In this context, it is customary to consider Boolean functions using the $\{0,1\}^n \to \{0,1\}$ representation.

We say that $p : \{0,1\}^n \to \mathbb{R}$ is a non-deterministic polynomial for $f : \{0,1\}^n \to \{0,1\}$ if $p(x) = 0$ if and only if $f(x) = 0$. An easy calculation establishes the following relationship between the rational and non-deterministic degrees

$$\mathrm{rdeg}(f) = \max\{\mathrm{ndeg}(f), \mathrm{ndeg}(\bar{f})\}.$$

As mentioned in the introduction de Wolf conjectured that $\mathrm{D}(f) \leq \mathcal{O}(\mathrm{ndeg}(f)\,\mathrm{ndeg}(\bar{f}))$ for all total Boolean functions. By showing that $\mathrm{ndeg}(f) \leq \mathrm{C}_1(f)$, de Wolf also established the inequality $\mathrm{rdeg}(f) \leq \mathrm{C}(f)$ [Wol00].

2.5 Quantum Query Complexity and Post-selection

We assume basic familiarity with concepts in quantum information. While we review some of these, we direct the reader to, e.g. [NC11], for background.

Consider a Boolean function f over a domain D. We say an ε-error quantum algorithm computes f if it outputs a bit $a(x)$ such that for all $x \in D$, $\Pr[a(x) = f(x)] \geq 1 - \varepsilon$. BQP is the class of problems that have efficient (polynomial-time) quantum algorithms with error $1/3$ and EQP is the analogous class of zero-error algorithms. We can also define complexity classes corresponding to quantum algorithms augmented with the power of *post-selection*.

Definition 4. $\mathsf{PostBQP}$ is the set of languages decidable by a polynomial time quantum algorithm that outputs two bits a, b such that for all inputs $x \in \{0,1\}^n$

(i) $\Pr[a(x) = 1] > 0$.

(ii) If $x \in L$, then $\Pr[b(x) = 1 | a(x) = 1] \geq 2/3$.

(iii) If $x \notin L$, then $\Pr[b(x) = 1 | a(x) = 1] \leq 1/3$.

$\mathsf{PostEQP}$ is the corresponding class of *zero-error* algorithms with post-selection.

Each of these computational complexity classes has an associated query measure. Formally, we say a function has query access to a string w if it has black-box access to a unitary s.t. $U|i\rangle|b\rangle = |i\rangle|b \oplus w_i\rangle$. When the input w encodes the truth table of a Boolean function f, we will often write this as $U|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle$, where $x \in \{0,1\}^n$. The number of calls an algorithm makes to the unitary U is its *query complexity*. By $\mathsf{Q}_\varepsilon(f)$ and $\mathsf{Q}_E(f)$ we denote the query complexities of ε-error and zero-error quantum algorithms, respectively. $\mathsf{PostQ}_\varepsilon(f)$ and $\mathsf{PostQ}_E(f)$ are defined analogously for quantum algorithms with post-selection. For simplicity of notation, $\mathsf{Q}(f)$ and $\mathsf{PostQ}(f)$ are understood to correspond to $\varepsilon = 1/3$.

A seminal result by Beals *et al.* gives a lower bound quantum query complexity using polynomials [BBC+01]. Formally, we have $\mathsf{Q}_\varepsilon(f) \geq \widetilde{\deg}_\varepsilon(f)/2$ for all (possibly partial) Boolean functions f. As a special case, $\mathsf{Q}_E(f) \geq \deg(f)/2$. This result gave rise to the so-called *polynomial method* for quantum query lower bounds. Similarly, it was shown by Mahadev and de Wolf that $\mathsf{PostQ}_\varepsilon(f) = \Theta(\mathrm{rdeg}_\varepsilon(f))$ and $\mathsf{PostQ}_E(f) = \Theta(\mathrm{rdeg}_0(f))$ for total functions f [MW15]. It is not difficult to extend this result for partial functions, see Appendix A. Nonetheless, it is surprising that the result does still hold for partial functions since the analogous result for quantum query complexity and approximate degree was recently shown to be false in [AB23].

3 Rational Degree Lower Bounds

In this section, we present rational degree lower bounds for certain classes of Boolean functions. Our results constitute progress towards showing that rational degree is polynomially related to Fourier degree for total functions.

First, we establish the tight lower bound $\deg(f)/2 \leq \mathrm{rdeg}(f)$ for symmetric functions. This result then becomes key in proving a rational degree lower bound for read-once Boolean formulae, which is tight for formulae of depth 2. Next, we prove that the rational degree equals the sensitivity for monotone functions, which implies that $\sqrt{\deg(f)} \leq \mathrm{rdeg}(f)$ for monotone functions. This lower bound is also tight. Finally, we show that almost all Boolean functions $f\colon \{-1,1\}^n \to \{-1,1\}$ have rational degree at least $n/2 - \mathcal{O}(\sqrt{n})$.

3.1 Symmetric Functions

Our first lower bounds are for (possibly partial) functions which are constant on a large number of Hamming slices. Of course, this subsumes the class of symmetric functions. This lemma will later be useful in obtaining an unbounded separation of rational degree from quantum query complexity (and thus approximate degree) in the case of partial functions.

Lemma 5. *Let f be a (possibly partial) nonconstant Boolean function over input domain $D \subseteq \{0,1\}^n$ and define $S_0 = \{k \in [n]\colon |x| = k \implies f(x) = 0\}$, $S_1 = \{k \in [n]\colon |x| = k \implies f(x) = 1\}$. Then* $\mathrm{rdeg}(f) \geq \max(|S_0|, |S_1|)$.

We use the Minsky-Papert symmetrization technique, which converts a multivariate polynomial over $\{0,1\}^n$ to a univariate polynomial over $\mathbb{R}$ [MP69]. Formally, given $p : \{0,1\}^n \to \mathbb{R}$ we define $P(k) \coloneqq \mathbb{E}_{|x|=k}[p(x)]$.

Proof. Since $\mathrm{rdeg}(f) = \mathrm{rdeg}(\bar{f})$, we can assume without loss of generality that $|S_0| \geq |S_1|$. It suffices to show that $\mathrm{rdeg}(f) \geq |S_0|$. Indeed, let $f = p/q$ be a rational representation of f. Applying the Minsky-Papert symmetrization technique to $p(x)$ we obtain a univariate polynomial $P(k)$ such that $\deg(p) \geq \deg(P)$ and $P(k) = 0$ for any $k \in S_0$. On the other hand, there exists at least one $k \in [n]$ such that $P(k) \neq 0$, since f is nonconstant. Thus $\deg(p) \geq \deg(P) \geq |S_0|$. Since this holds for every rational representation of f, the result follows. □

Of course, a special case of this result is a strong lower bound for symmetric total functions.

Corollary 6. *If $f\colon \{0,1\}^n \to \{0,1\}$ is symmetric then* $\mathrm{rdeg}(f) \geq \deg(f)/2$.

3.2 Read-Once Formulae

We now turn our attention to a generalized version of read-once Boolean formulae, where each gate is an arbitrary nonconstant symmetric gate. The key observations behind the lower bound are that these formulae can be written as compositions of symmetric gates, and that any depth d tree must contain a node with branching factor $\geq n^{1/d}$.

Lemma 7. *Let $f\colon \{0,1\}^n \to \{0,1\}$ and $g_i\colon \{0,1\}^{n_i} \to \{0,1\}$ be Boolean functions where every variable in each function is relevant. Defining $h : \{0,1\}^{\sum n_i} \to \{0,1\}$ to be $h(x^1, \ldots, x^n) = f(g_1(x^1), \ldots, g_n(x^n))$, we have that*

$$\mathrm{rdeg}(h) \geq \max\{\mathrm{rdeg}(f), \mathrm{rdeg}(g_1), \ldots, \mathrm{rdeg}(g_n)\}.$$

Proof. Since every variable is relevant for each g_i, we know there exists restrictions ρ^i to all but 1 variable in each x^i such that $g_i|_{\rho^i}(x^i) = x^i_{k_i}$ or $(1 - x^i_{k_i})$ for some $1 \le k_i \le n_i$. Considering the restriction $\rho = \rho^1 \cup \cdots \cup \rho^n$, it is evident that $h|_\rho(x) = f(x^1_{k_1}, \ldots, x^n_{k_n})$ up to negations. Therefore,

$$\mathrm{rdeg}(h) \ge \mathrm{rdeg}(h|_\rho) \ge \mathrm{rdeg}(f). \tag{1}$$

Now pick an arbitrary i. Since, by assumption, every variable of f is relevant, there exists an assignment $x_j = z_j$ for all $j \ne i$ such that $f(z_1, \ldots z_{i-1}, x_i, z_{i+1}, \ldots, z_n) = x_i$ or $\overline{x_i}$. Since g_i is nonconstant, it follows that there exists an assignment to the variables $(x^j)_{j \ne i}$ such that each $g_j(x^j)$ is fixed to z_j.

Let τ be the restriction induced by this partial assignment. Then

$$h|_\tau(x) = f(z_1, \ldots z_{i-1}, g_i(x^i), z_{i+1}, \ldots z_n) = g_i(x^i) \text{ or } \overline{g_i(x^i)}.$$

Consequently,

$$\mathrm{rdeg}(h) \ge \mathrm{rdeg}(h|_\tau) \ge \mathrm{rdeg}(g_i). \tag{2}$$

Combining Equations (1) and (2) gives the desired result. □

Lemma 8. *Let f be written as a read-once formula with symmetric gates where the maximum branching factor of any node is w. Then* $\mathrm{rdeg}(f) = \Omega(w)$.

Proof. Let p/q be a rational representation of f. We can assume without loss of generality that f is monotone (i.e. only the literals x_i, and not $\overline{x_i}$ appear in the formula).

Now consider the node G with branching factor w. Let F be the subformula with top gate G and let $F_1, \ldots, F_w$ be the read-once subformulas below G. Each F_i is nonconstant, which implies the existence of a restriction ρ_i of all but 1 variable in each V_i such that toggling the sole live variable (say x_{k_i}) toggles the value of F_i (i.e. $F_i|_{\rho_i} = x_j$ or $\overline{x_k}$ for some k). As the V_i are disjoint (as f is read-once), these restrictions together define a unified restriction ρ such that $F|_\rho(x) = G(x_{k_1}, \ldots, x_{k_w})$ up to negations. Inductively using Lemma 7 on the formula $f|_\rho$ by starting at the top node and going down the path to G, it follows that

$$\mathrm{rdeg}(f) \ge \mathrm{rdeg}(f|_\rho) \ge \mathrm{rdeg}(F|_\rho) = \mathrm{rdeg}(G) \ge w/2, \tag{3}$$

where the last inequality follows from Lemma 5. □

Now we can prove polynomial rational degree lower bounds on read-once formulae.

Corollary 9. *Let f be written as a depth-d read-once formula with symmetric gates. Then* $\mathrm{rdeg}(f) = \Omega(\deg(f)^{1/d})$.

Proof. The result follows from Lemma 8 and a simple contradiction argument: if all nodes have branching factor strictly less than $n^{1/d}$ then there must be strictly fewer than n literals. Note that $n \ge \deg(f)$ so the lower bound $\Omega(n^{1/d})$ is stronger. □

This lower bound is tight for $d = 2$, as witnessed by the AND-of-ORs function $f = \mathsf{AND}_{\sqrt{n}} \circ \mathsf{OR}_{\sqrt{n}}$. Indeed, $\mathrm{rdeg}(f) \le \mathrm{C}(f) = n^{1/2} = \sqrt{\deg(f)}$. However, for larger depth $d > 2$, it is unclear whether a depth-d read-once AC^0 formula with rational degree $O(n^{1/d})$ exists or if the lower bound can be improved. It can be shown that there exist arbitrary-depth read-once formulae with rational degree at most $\sqrt{n}$ (see Figure 3. We leave as an open question whether the bound $\Omega(\deg(f)^{1/d})$ is tight.

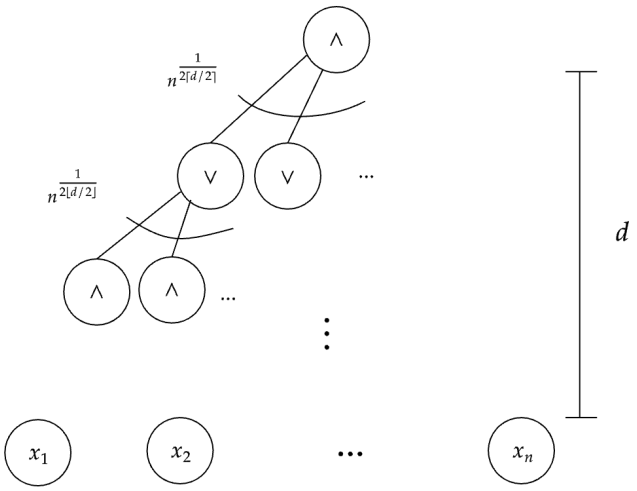

Figure 3: A depth-d AND-OR tree with certificate complexity $\sqrt{n}$, and thus rational degree at most $\sqrt{n}$. Indeed, setting all input wires to 1 for AND functions and a single input wire to 1 for OR functions along a single path to root gives a 1 certificate, and setting all input wires to 0 for OR functions and a single input wire to 0 for AND functions gives a 0-certificate. One can easily verify that both of these certificates are of size $\sqrt{n}$.

3.3 Monotone Functions

A Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is said to be monotone if $\forall x, y \in \{0,1\}^n$, $x \leq y$ implies $f(x) \leq f(y)$ where $x \leq y$ is taken pointwise. In this subsection we prove that $\mathrm{rdeg}(f) = \mathrm{s}(f)$ for monotone Boolean function f. We note that it suffices to prove that $\mathrm{s}(f) \leq \mathrm{rdeg}(f)$. This is because the certificate complexity of a monotone Boolean functions f equals its sensitivity $\mathrm{C}(f) = \mathrm{s}(f)$ [Nis91]. Combining this with the fact that $\mathrm{rdeg}(f) \leq C(f)$ we can already conclude the other inequality.

Claim 10. *For monotone Boolean functions $f\colon \{0,1\}^n \to \{0,1\}$, $s(f) \leq \mathrm{rdeg}(f)$.*

Our proof is similar to the proof that for all monotone Boolean functions $s(f) \leq \deg(f)$ as presented in [BW02, Proposition 4].

Proof. Suppose without loss of generality that f is monotone increasing. We prove the claim by showing that

$$\mathrm{s}_0(f) \leq \mathrm{ndeg}(\bar{f}) \quad \text{and} \quad \mathrm{s}_1(f) \leq \mathrm{ndeg}(f). \tag{4}$$

We only prove the first inequality as the second can be proven analogously. Let x be such that $\mathrm{s}_0(f) = s_f(x)$. All sensitive variables must be 0 in x since f is monotone increasing. Moreover, setting any sensitive variable to 1 changes the value of f from 0 to 1. Therefore, fixing all variables in x except for the $\mathrm{s}_0(f)$ many sensitive variables yields the OR_m function on $m := \mathrm{s}_0(f)$ variables. Since $\mathrm{ndeg}(\overline{\mathsf{OR}}_m) \geq m$, $\mathrm{ndeg}(\bar{f}) \geq s_0(f)$. □

Since $\mathrm{s}(f) = \mathrm{C}(f)$ and $\sqrt{\deg(f)} \leq \mathrm{s}(f)$ for monotone functions, we have the following corollary.

Corollary 11. *For monotone Boolean functions f, $\mathrm{rdeg}(f) = \mathrm{s}(f)$. In particular, $\sqrt{\deg(f)} \leq \mathrm{rdeg}(f)$.*

Note that this bound is tight, as witnessed by the AND-of-ORs function, $f = \mathsf{AND}_n \circ \mathsf{OR}_n$, on n^2 bits, which has $\operatorname{rdeg}(f) \leq \mathrm{C}(f) = n = \sqrt{\deg(f)}$. We remark that Claim 10 cannot be extended to all Boolean functions, as evidenced by the Kushilevitz function $K_m \colon \{0,1\}^{6^m} \to \{0,1\}$ [NW95]. Indeed, K_m has full sensitivity, but its degree is 3^m.

3.4 Random Functions

As our final piece of evidence that rational degree is polynomially related to degree, we prove that all but a negligible fraction of Boolean functions $f \colon \{-1,1\}^n \to \{-1,1\}$ have rational degree at least $n/2 - \mathcal{O}(\sqrt{n})$.

As mentioned in the introduction Alon [Alo93] and Anthony [Ant95] used counting arguments to show that all but a negligible fraction of n-bit Boolean functions have sign degree at least $n/2$. Below we restate a variant of the function counting theorem used by Athony.

Given a finite set X and a mapping $\phi \colon X \to \mathbb{R}^d$, we say that a ϕ-separable dichotomy of X is a partition of X into subsets $X^+ \cup X^-$ such that there exists some $w \in \mathbb{R}^d$ for which $w \cdot \phi(x) > 0$ for all $x \in X^+$ and $w \cdot \phi(x) < 0$ for all $x \in X^-$.

Theorem 12 (Function counting theorem, [Cov65])**.** *Let $\phi \colon S \to \mathbb{R}^d$. Let $X = \{x_1, \ldots, x_N\} \subseteq S$. If a ϕ-surface (i.e., a set of the form $\{x \in S : w \cdot \phi(x) = 0\}$ for some $w \in \mathbb{R}^d$) contains a set of points $Y = \{y_1, y_2, \ldots, y_k\} \subseteq S$, where $\phi(y_i)$ are linearly independent for all i, and where the projection of $\phi(x_1), \ldots, \phi(x_N)$ onto the orthogonal subspace to the space spanned by the $\phi(y_i)$'s is in general position, then there are $C(N, d-k)$ many ϕ-separable dichotomies of X, where*

$$C(N,d) = 2\sum_{i=0}^{d-1} \binom{N-1}{i}.$$

We consider the following adaptation of the above theorem. Consider a set of N points $S = \{v_1, \ldots, v_n\}$ in $\mathbb{R}^D$. Given a 2-coloring of the points $f \colon [N] \to \{-1,1\}$, we say that the coloring f is separable by two hyperplanes if there exist hyperplanes $H_j = \{v : \ \alpha_j \cdot v = 0\}$ for $j = 1, 2$ such that

$$\forall i \in [N] \colon \ f(i) = \operatorname{sgn}((\alpha_1 \cdot v_i)(\alpha_2 \cdot v_i)).$$

Corollary 13. *Given N points in $\mathbb{R}^M$, the number of two colorings $f \colon [N] \to \{-1,1\}$ that are separable by two hyperplanes is at most $C(N,M)^2$.*

Proof. Let $S \subset \mathbb{R}^M$ be given and suppose that f is a coloring that is separated by the hyperplanes H_1 and H_2. Then there exist colorings f_1, f_2 that are separated by the hyperplanes H_1 and H_2 respectively. Since there are at most $C(N,M)$ choices for each of f_1 and f_2, the number of such colorings f is bounded by $C(N,M)^2$. □

Lemma 14. *Let $m \leq n$ be two positive integers. The number of Boolean functions $f \colon \{-1,1\}^n \to \{-1,1\}$ with rational degree at most m is at most $C(2^n, \binom{n}{\leq m})^2$.*

Proof. Let $M = \binom{n}{\leq m}$. For each $x \in \{-1,1\}^n$ define $v_x \in \mathbb{C}^M$ by letting $(v_x)_S = \chi_S(x)$ for $S \subseteq [n]$, $|S| \leq m$. Suppose p/q is a rational representation of f of degree at most m. Then

$$f(x) = \operatorname{sgn}(p(x)/q(x)) = \operatorname{sgn}(p(x)q(x)) = \operatorname{sgn}((\widehat{p} \cdot v_x)(\widehat{q} \cdot v_x)).$$

Thus the coloring given by f is separated by the hyperplanes defined by $\widehat{p}$ and $\widehat{q}$. The result follows by Corollary 13. □

We can now state and prove our extremal lower bound on rational degree.

Corollary 15. *All but a negligible fraction of Boolean functions on n variables have rational degree at least $n/2 - \mathcal{O}(\sqrt{n})$.*

Proof. Write $m = n/2 - \sqrt{cn}$ for some constant c, and let $N = 2^n$. Then by Corollary 13 there are at most $C\big(N, \binom{n}{\leq m}\big)^2$ Boolean functions on n variables of rational degree less than m. By the Chernoff bound $\binom{n}{\leq n/2-\lambda} < 2^n e^{-2\lambda^2/n}$ and the Hamming bound, we have that the proportion of Boolean functions with rational degree strictly less m is bounded above by

$$\frac{C\big(N, \binom{n}{\leq m}\big)^2}{2^N} \leq \frac{C(N, Ne^{-2c})^2}{2^N} \leq O\big(2^{N(2h_2(e^{-2c})-1)}\big),$$

where $h_2(\cdot)$ denotes the binary entropy function. Solving the inequality $h_2(e^{-2c}) < 1/2$ numerically we find that for $c \geq 1.104$, the above bound tends to 0. □

4 Applications in Complexity Theory

In this section, we give two functions: one whose rational degree is unboundedly higher than its approximate degree and one which has approximate degree unboundedly higher than its rational degree. These examples in turn give bidirectional separations between BQP and PostEQP with respect to generic oracles. We conclude the section by giving evidence that zero-error quantum computation with post-selection gives advantage over bounded-error randomized algorithms, providing context to our results.

4.1 Post-Selection can be a Weak Resource

In this subsection, we give an oracle which witnesses that BQP $\not\subseteq$ PostEQP (in fact, even RP $\not\subseteq$ PostEQP). This is accomplished by constructing a partial function which has constant 1-sided error randomized query complexity but maximal PostQ_E. In fact, this problem also demonstrates that the rational degree can be arbitrarily higher than the approximate degree for partial functions.

Problem 16 (Majority or None)**.** *The* MajOrNone$_n$ *function is defined as a partial Boolean function on the set of bitstrings $x \in \{0,1\}^n$ that have Hamming weight either 0 or at least $n/2$. The function* MajOrNone$_n$ *takes value 0 in the former case, and takes value 1 otherwise.*

Theorem 17. *The* MajOrNone$_n$ *function can be decided by a quantum algorithm using constantly many queries, yet its rational degree is at least $\Omega(n)$. Consequently,* MajOrNone$_n$ *witnesses the following separations:*

$$\widetilde{\deg}(\textsc{MajOrNone}_n) \leq \mathcal{O}(1) \quad \textit{yet} \quad \mathrm{rdeg}(\textsc{MajOrNone}_n) \geq \Omega(n),$$
$$\mathsf{Q}(\textsc{MajOrNone}_n) \leq \mathcal{O}(1) \quad \textit{yet} \quad \mathsf{PostQ}_E(\textsc{MajOrNone}_n) \geq \Omega(n).$$

Proof. The MajOrNone$_n$ function even has constant RP query complexity. Indeed, we may simply query a constant number of random bits and output 1 if any of them are 1. Therefore, MajOrNone$_n$ has constant quantum query complexity, which in turn implies a constant approximate degree. We show via a rational degree lower bound that $\mathsf{PostQ}_E(\textsc{MajOrNone}_n) = \Omega(n)$. In particular, we show that $\mathrm{rdeg}(\textsc{MajOrNone}_n) = \Omega(n)$. Using the notation of Lemma 5, for MajOrNone$_n$ we have $|S_1| \geq n/2$, giving us

$$\mathsf{PostQ}_E(\textsc{MajOrNone}_n) \geq \mathrm{rdeg}(\textsc{MajOrNone}_n) = \Omega(n).$$ □

The complexity classes Q and PostQ_E are the query complexity equivalents of BQP and $\mathsf{PostEQP}$, respectively. As such, our unbounded separation between these complexity measures gives a separation of BQP and $\mathsf{PostEQP}$ with respect to a generic oracle.

Corollary 18. *There exists an oracle O such that $\mathsf{RP}^O \not\subseteq \mathsf{PostEQP}^O$.* □

4.2 Post-Selection can be a Strong Resource

On the other hand, we can give an oracle which witnesses $\mathsf{PostEQP} \not\subseteq \mathsf{BQP}$. We do this by constructing a promise problem f for which $\mathsf{PostQ}_E(f) = \mathcal{O}(1)$ but $\mathsf{Q}_\varepsilon(f) \geq \Omega(n)$. This problem also witnesses the fact that approximate degree can be unboundedly larger than rational degree.

Problem 19 (Imbalance)**.** *Let $n = 4m + 2$ for some positive integer m. Define the functions $L, R : \{-1,1\}^n \to \mathbb{R}$ as $L(x) = x_1 + x_2 + \ldots + x_{2m+1}$ and $R(x) = x_{2m+2} + \ldots + x_{4m+2}$. Then the* Imbalance$\colon \{-1,1\}^n \to \mathbb{R}$ *function is defined as* Imbalance$(x) = \frac{L(x)}{R(x)}$.

Note that we assumed $4 \nmid n$ to ensure that the denominator $R(x)$ cannot be 0.

Problem 20 (Boolean Imbalance)**.** *Let m and n be as in the above problem. We define the Boolean Imbalance* BI_n *function as the restriction of* Imbalance *to the union $S_- \cup S_+$ where we let*

$$S_+ = \{(x_L, x_R) \colon |x_L| = |x_R| = m\},$$
$$S_- = \{(x_L, x_R) \colon |x_L| + |x_R| = 2m + 1 \text{ and } |x_L|, |x_R| \geq m\}.$$

Note that $\mathrm{BI}_n(x) = 1$ for any $x \in S_+$ since the numerator and denominator evaluate to the same quantity. On the other hand, for any $x \in S_-$ we have that $\mathrm{BI}_n(x) = -1$ since both $L(x)$ and $R(x)$ must be ± 1 but they must be different.

By a generalisation of the equivalence of Mahadev and de Wolf (Lemma 25) we have an upper bound of 2 on $\mathsf{PostQ}_E(\mathrm{BI}_n)$. We now show that it has a linear lower bound on the approximate degree.

Lemma 21. *The BI_n function can be decided by a postselected quantum algorithm using only 2 queries, yet its rational degree is at least $\Omega(n)$. Consequently, BI_n witnesses the following separations:*

$$\begin{aligned} \mathrm{rdeg}(\mathrm{BI}_n) &\leq \mathcal{O}(1) \quad \textit{yet} \quad \widetilde{\deg}(\mathrm{BI}_n) \geq \Omega(n), \\ \mathsf{PostQ}_E(\mathrm{BI}_n) &\leq \mathcal{O}(1) \quad \textit{yet} \quad \mathsf{Q}(\mathrm{BI}_n) \geq \Omega(n). \end{aligned}$$

Proof. Note that BI_n is defined on inputs of Hamming weight $2m$ and $2m+1$. By a result of Nayak and Wu any function which is constant on Hamming slices $l, l+1$ and flips its value has approximate degree $\Omega(\max\{l, n-l\})$ [NW99]. In this case, since the function value flips on Hamming weights $2m, 2m+1$ we get a lower bound of $\Omega(\max\{2m+1, 2m\}) = \Omega(n)$. □

Finally, just like in the previous section, this separation between complexity measures allows us to construct an oracle relative to which $\mathsf{PostEQP}$ is not contained in BQP.

Corollary 22. *There exists an oracle O such that $\mathsf{PostEQP}^O \not\subseteq \mathsf{BQP}^O$.* □

Our unbounded separation of rational degree and approximate degree gives a generic oracle separation of $\mathsf{PostEQP}$ and BQP. Combined with Corollary 18, this tells us that zero-error post-selection and bounded error are "incomparable" resources in the black-box model: one is not stronger than the other.

4.3 Post-Selection and Non-Determinism

To conclude the section, we provide more context to our results by giving evidence that zero-error quantum computation with post-selection gives advantage over efficient classical computation.

Claim 23. $\mathsf{NP} \cap \mathsf{coNP} \subseteq \mathsf{PostEQP}$.

Proof. Let $L \in \mathsf{NP} \cap \mathsf{coNP}$. Since $L \in \mathsf{NP}$, there is an efficient algorithm M_1 and a polynomial p_1 such that for every $x \in L$, there exists $u_1 \in \{0,1\}^{p_1(|x|)}$ such that $M_1(x, u_1) = 1$ and for every $x \notin L$ and $u \in \{0,1\}^{p_1(|x|)}$ we have $M_1(x, u) = 0$. Similarly since $L \in \mathsf{coNP}$ there is an efficient algorithm M_2 and polynomial p_2 such that for every $x \notin L$, there exists $u_2 \in \{0,1\}^{p_2(|x|)}$ such that $M_2(x, u_2) = 1$ and for every $x \in L$ and $u_2 \in \{0,1\}^{p_2(|x|)}$ we have $M_2(x, u_2) = 0$.

Now, given x, our quantum computer can generate a uniform superposition over all the possible certificates for both M_1 and M_2 (concatenated together), and post-select on the event that either $M(x, u_1) = 1$ or $M_2(x, u_2) = 1$. Then, the quantum algorithm can measure all registers and simulate both $M_1(x, u_1)$ and $M_2(x, u_2)$ and see which one is 1. By definition, only one of M_1 and M_2 will accept, and whichever one accepts tells us if $x \in L$ or not. □

It is widely believed that $\mathsf{NP} \cap \mathsf{coNP}$ is not contained in P or even BPP. As such, there is reason to believe that zero-error quantum algorithms with post-selection can offer advantage over efficient classical computation.

5 Open Questions

In this paper, we considered the problem of lower bounding the rational degree of Boolean functions in terms of their Fourier degree. While we could not answer this question in its full generality, we showed that the square root of the degree lower bounds the rational degree for both monotone and symmetric Boolean functions. We conjecture that this lower bound extends to all total Boolean functions.

Conjecture 2. *For all Boolean functions* $f\colon \{-1,1\}^n \to \{-1,1\}$, $\sqrt{\deg(f)} \leq \mathrm{rdeg}(f)$.

Answering this conjecture in the affirmative would place rational degree within a plethora of Boolean function complexity measures all of which are polynomially related. Recall that for partial functions, we have unbounded separations between the rational and approximate degrees in both directions.

In this work, we showed that a hypothetical total function that witnesses any such separation must lack a certain level of structure: in particular, it cannot be symmetric, monotone, or expressible by a low-depth read-once Boolean formula. In this direction, an easier question is whether there are other classes of functions for which rational degree cannot be separated from Fourier degree. Some candidates that may be amenable to current techniques include unate and transitive-symmetric functions. In particular, showing that unate functions have polynomial rational degree would, in turn, imply polynomial rational degree lower bounds for read-once TC_0 circuits by adapting our result for read-once Boolean formulae with symmetric gates.

We also proved that almost all Boolean functions $f\colon \{-1,1\}^n \to \{-1,1\}$ have rational degree at least $n/2 - \mathcal{O}(\sqrt{n})$. As mentioned in the preliminaries O'Donnell and Servedio proved [OS08] that almost all Boolean functions $f\colon \{-1,1\}^n \to \{-1,1\}$ have sign degree at most $n/2 + \mathcal{O}(\sqrt{n \log n})$. It would be interesting to know if an analogous result can be established for the rational degree.

Conjecture 3. *All but a negligible fraction of Boolean functions* $f\colon \{-1,1\}^n \to \{-1,1\}$ *have rational degree at most* $n/2 + o(n)$.

Acknowledgements

The authors thank Scott Aaronson, Yuval Filmus, Lance Fortnow, Sabee Grewal, Robin Kothari, Geoffrey Mon, Rocco Servedio, Avishay Tal, Ronald de Wolf, and David Zuckerman for helpful conversations.

VI and SJ are supported by Scott Aaronson's Vannevar Bush Fellowship from the US Department of Defense, the Berkeley NSF-QLCI CIQC Center, a Simons Investigator Award, and the Simons "It from Qubit" collaboration. VI is supported by a National Science Foundation Graduate Research Fellowship. MKD and DW acknowledge support from the Army Research Office (grant W911NF-20-1-0015) and the Department of Energy, Office of Science, Office of Advanced Scientific Computing Research, Accelerated Research in Quantum Computing program. VMK acknowledges support from NSF Grant CCF-2008076 and a Simons Investigator Award (#409864, David Zuckerman). MW was supported by NSF grant CCF-2006359.

References

[AB23] Andris Ambainis and Aleksandrs Belovs. An exponential separation between quantum query complexity and the polynomial degree. In *Proceedings of the 38th Annual Conference on Computational Complexity (CCC)*, 2023. arXiv:2301.09218, doi:10.4230/LIPIcs.CCC.2023.24. [p. 6]

[ABDK+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 SIGACT Symposium on Theory of Computing*, page 1330–1342, 2021. arXiv:2010.12629, doi:10.1145/3406325.3451047. [p. 1]

[AK] Scott Aaronson and Greg Kuperberg. Complexity zoo. https://complexityzoo.net/Complexity_Zoo. [p. 1]

[Alo93] Noga Alon. Personal communication to M. Saks. Reported in M. Saks, Slicing the Hypercube, 1993. [pp. 5, 10]

[Ant95] Martin Anthony. Classification by polynomial surfaces. *Discrete Applied Mathematics*, 61(2):91–103, 1995. doi:10.1016/0166-218X(94)00008-2. [pp. 5, 10]

[BBC+01] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001. arXiv:quant-ph/9802049. [pp. 6, 16]

[BKT20] Mark Bun, Robin Kothari, and Justin Thaler. The polynomial method strikes back: Tight quantum query bounds via dual polynomials. *Theory of Computing*, 16(10):1–71, 2020. doi:10.4086/toc.2020.v016a010. [p. 5]

[BW02] Harry Buhrman and Ronald de Wolf. Complexity measures and decision tree complexity: a survey. *Theoretical Computer Science*, 288(1):21–43, 2002. doi:10.1016/S0304-3975(01)00144-X. [p. 9]

[Cov65] Thomas M. Cover. Geometrical and statistical properties of systems of linear inequalities with applications in pattern recognition. *IEEE Transactions on Electronic Computers*, EC-14(3):326–334, 1965. doi:10.1109/PGEC.1965.264137. [p. 10]

[For03] Lance Fortnow. Computational complexity - rational functions and decision-tree complexity. https://blog.computationalcomplexity.org/2003/11/rational-functions-and-decision-tree.html, 2003. [pp. 1, 2]

[FSS81] Merrick Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. In *22nd Annual Symposium on Foundations of Computer Science*, pages 260–270, 1981. doi:10.1109/SFCS.1981.35. [p. 3]

[Hua19] Hao Huang. Induced subgraphs of hypercubes and a proof of the sensitivity conjecture. *Ann. of Math. (2)*, 190(3):949–955, 2019. arXiv:1907.00847, doi:10.4007/annals.2019.190.3.6. [p. 1]

[MP69] Marvin Minsky and Seymour Papert. *Perceptrons*. MIT Press, Cambridge, MA, 1969. [pp. 1, 7]

[MW15] Urmila Mahadev and Ronald de Wolf. Rational approximations and quantum algorithms with postselection. *Quantum Info. Comput.*, 15(3–4):295–307, 2015. arXiv:1401.0912, doi:10.48550/ARXIV.1401.0912. [pp. 2, 6, 16]

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, USA, 10th edition, 2011. [p. 6]

[Nis91] Noam Nisan. Crew prams and decision trees. *SIAM Journal on Computing*, 20(6):999–1007, 1991. doi:10.1137/0220062. [p. 9]

[NS92] Noam Nisan and Mario Szegedy. On the degree of boolean functions as real polynomials. In *Proceedings of the 24th ACM Symposium on Theory of Computing (STOC)*, pages 462–467. ACM, 1992. doi:10.1145/129712.129757. [p. 1]

[NW95] Noam Nisan and Avi Wigderson. On rank vs. communication complexity. *Combinatorica*, 15(4):557–565, 1995. doi:10.1007/BF01192527. [p. 10]

[NW99] Ashwin Nayak and Felix Wu. The quantum query complexity of approximating the median and related statistics. In *Annual ACM Symposium on Theory of Computing (Atlanta, GA, 1999)*, pages 384–393. ACM, New York, 1999. doi:10.1145/301250.301349. [p. 12]

[O'D14] Ryan O'Donnell. *Analysis of Boolean functions*. Cambridge University Press, New York, 2014. arXiv:2105.10386, doi:10.1017/CBO9781139814782. [p. 3]

[OS08] Ryan O'Donnell and Rocco A. Servedio. Extremal properties of polynomial threshold functions. *Journal of Computer and System Sciences*, 74(3):298–312, 2008. Computational Complexity 2003. doi:10.1016/j.jcss.2007.06.021. [pp. 6, 13]

[Sak93] Michael E. Saks. *Slicing the hypercube*, page 211–256. London Mathematical Society Lecture Note Series. Cambridge University Press, 1993. doi:10.1017/CBO9780511662089.009. [p. 3]

[Wol00] Ronald de Wolf. Characterization of non-deterministic quantum query and quantum communication complexity. In *Proceedings of the 15th Annual Conference on Computational Complexity (CCC)*, pages 271–278. 2000. arXiv:cs/0001014, doi:10.1109/CCC.2000.856758. [pp. 2, 6]

A Rational Degree and Query Complexity with Post-Selection

In this appendix, we show that the main theorem of [MW15], stated for total Boolean functions, in fact also holds for partial ones. We do so simply by observing that the proof given in [MW15] also works for partial Boolean functions.

Theorem 24. *For any (possibly partial) Boolean function f on n variables and $\varepsilon \in [0, 1/2)$, $\mathrm{rdeg}_\varepsilon(f) = \Theta(\mathsf{PostQ}_\varepsilon(f))$.*

First we show that rational degree lower bounds quantum query complexity with post-selection.

Lemma 25. *Let $D \subseteq \{0,1\}^n$ and consider $f\colon D \to \{0,1\}$. Then $\mathrm{rdeg}_\varepsilon(f) \leq \mathsf{PostQ}_\varepsilon(f)$.*

Proof. Suppose there is a T-query post-selected ε-error algorithm for f. As in Definition 4 let $a(x)$ be the random variable corresponding to the measurement of the post-selected qubit and $b(x)$ the random variable corresponding to the measurement of the output qubit. We have that

$$|\Pr[b(x) = 1 | a(x) = 1] - f(x)| \leq \varepsilon.$$

Now, by [BBC+01], the amplitudes of a quantum algorithm after T oracle queries are polynomials in $x_1, \ldots, x_n$ of degree at most $2T$. It immediately follows that $\Pr[a(x) \wedge b(x) = 1]$ and $\Pr[a(x) = 1]$ are polynomials of degree at most $2T$: call them p and q respectively. Thus we have

$$\left| \frac{p(x)}{q(x)} - f(x) \right| = |\Pr[b(x) = 1 | a(x) = 1] - f(x)| \leq \varepsilon,$$

which gives us the desired rational approximation of f. □

Now, we show that, up to a constant factor, the rational degree upper bounds quantum query complexity with post-selection. The proof is Fourier analytic, and so we switch to the $\{-1, 1\}$ basis.

Lemma 26. *Let $D \subseteq \{-1,1\}^n$ and consider $f\colon D \to \{-1,1\}$. Then $\mathsf{PostQ}_\varepsilon(f) \leq 2\,\mathrm{rdeg}_\varepsilon(f)$.*

Proof. Suppose $f\colon D \to \{-1,1\}^n$ has an ε-approximate rational representation p/q such that $\max\{\deg(p), \deg(q)\} = d$. Considering the Fourier expansions of p, q, we can construct the state

$$\sum_{S \subseteq [n]} \widehat{p}(S) \left|0\right\rangle \left|S\right\rangle + \widehat{q}(S) \left|1\right\rangle \left|S\right\rangle,$$

where $\left|S\right\rangle$ is the basis state that corresponds to the indicator bitstring for the set S. For simplicity, we have left out normalizing constants. Then, using $\max\{\deg(p), \deg(q)\} = d$ queries to x, we can construct the state

$$\sum_{S \subseteq [n]} \widehat{p}(S)\chi_S(x) \left|0\right\rangle \left|S\right\rangle + \widehat{q}(S)\chi_S(x) \left|1\right\rangle \left|S\right\rangle.$$

Now we apply an n-qubit Hadamard to the second register, obtaining the state

$$\left|0\right\rangle \left(\sum_{S \subseteq [n]} \widehat{p}(S) \left|0^n\right\rangle + \ldots \right) + \left|1\right\rangle \left(\sum_{S \subseteq [n]} \widehat{q}(S) \left|0^n\right\rangle + \ldots \right)$$

after which we postselect on the second register being equal to 0^n. This gives us the (again, unnormalized) state

$$\left|0\right\rangle \left(\sum_{S \subseteq [n]} \widehat{p}(S) \left|0^n\right\rangle \right) + \left|1\right\rangle \left(\sum_{S \subseteq [n]} \widehat{q}(S) \left|0^n\right\rangle \right) = \left(p(x) \left|0\right\rangle + q(x) \left|1\right\rangle\right) \left|0^n\right\rangle.$$

After discarding the second register and normalizing, we are left with

$$\frac{p(x)}{p(x)^2+q(x)^2}\left|0\right\rangle+\frac{q(x)}{p(x)^2+q(x)^2}\left|1\right\rangle.$$

We measure this state in the Hadamard basis and interpret the result as having value in $\{-1,1\}$. If $f(x)=-1$, then $p(x)/q(x)\in[-1-\varepsilon,-1+\varepsilon]$. The probability of measuring $\left|-\right\rangle$ is

$$\frac{(q(x)-p(x))^2}{2(p(x)^2+q(x)^2)}=\frac{(1-p(x)/q(x))^2}{2((p(x)/q(x))^2+1}\leq\frac{\varepsilon^2}{2(1+(1-\varepsilon)^2)}\leq\varepsilon.$$

□

Note that in the proof of Lemma 25 we get a rational polynomial which is bounded outside of the promise. Therefore, as a consequence we have that imposing this boundedness condition only increases the ε-approximate rational degree by at most a factor of 2.