Electronic Colloquium on Computational Complexity, Report No. 206 (2026)

Certification complexity of Boolean functions

Chandrima Kayal* Sophie Laplante† Émile Larroque‡ Krišjānis Prūsis§
Jevgēnijs Vihrovs¶

Abstract

Certificate complexity ($\mathsf{C}(f)$) is a fundamental measure of complexity of Boolean functions f which counts the number of bits of an input that need to be known in order for the value of the function to be determined. A certificate can be viewed as a partial assignment, or a boolean subcube where the function is constant. Certificate complexity is well understood for deterministic query (or decision tree) complexity (D) and other query models such as bounded-error randomized and quantum complexity (R, Q), but not as well for quantum zero-error (Q_0) and exact query complexity (Q_E), where there is no agreed-upon certificate "object" (even for Q).

Instead, we study an operational notion of certification and apply it to various query-based models, with a focus on zero-error and exact quantum query complexity, but also on polynomial degree measures. We give new characterizations of C, RC (randomized certificate complexity) and QC (quantum certificate complexity), in terms of various measures such as classical and quantum sabotage complexity, unambiguous certificate complexity, and variants of polynomial degree.

Certification complexity also gives rise to new lower bounds on Q_E and Q_0, the quantum analogues of D and R_0, complexity measures for which few lower bound techniques are known which are not already lower bounds for two-sided error quantum query complexity. We exhibit a total Boolean function for which our certification complexity measure gives a tight lower bound for Q_0, but rational degree and Q are asymptotically smaller.

Contents

*Université Paris-Cité, CNRS, IRIF kayal@irif.fr
†Université Paris-Cité, IRIF laplante@irif.fr
‡Université Paris-Cité, IRIF larroque@irif.fr
§University of Latvia, Faculty of Science and Technology krisjanis.prusis@lu.lv
¶University of Latvia, Faculty of Science and Technology jevgenijs.vihrovs@lu.lv

ISSN 1433-8092

1 Introduction

A certificate captures the amount of information about an input that is sufficient to ascertain the value of a function on a fixed input x. This notion appears naturally in several computational models. In the query model, a certificate for an input is a partial assignment of the input's variables such that every completion of this partial assignment yields the same function value. Thus, a certificate can be viewed as a set of queried variables whose values are sufficient to certify an output. A similar notion arises in communication complexity. Here, the input is distributed among two parties, and a certificate corresponds to a monochromatic rectangle: a product set of inputs on which the function has a fixed value. In both settings, the underlying idea is the same: rather than revealing the entire input, we seek a restricted region of the input space that is already sufficient to determine the output. The complexity of a certificate measures the amount of data required to identify such a monochromatic region.

In this paper, we systematically study an abstract notion of certification that applies to various complexity measures in the query complexity world. The main object of study are *decision problems*, that is, (possibly partial) functions $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ and we are interested in the complexity of the certification of f with respect to different complexity measures. In the classical deterministic setting, the minimum number of queries needed for any deterministic query algorithm to output $f(x)$ for the worst case input x is known as *deterministic query complexity* of f, denoted $\mathsf{D}(f)$. The notion of certificate is especially clear for $\mathsf{D}(f)$: A certificate is a *partial assignment* $\rho : [n] \to \{0,1,*\}$, that forces the value of the function to be constant. $\mathsf{C}(x,f)$ is the size of the smallest certificate that is consistent with x, and $\mathsf{C}(f) = \max_x\{\mathsf{C}(f,x)\}$. Equivalently, it corresponds to a monochromatic subcube containing the input.

In randomized and quantum computation, the notion becomes less immediate: what should constitute a certificate when the computation itself may involve randomness or querying in superposition? The quantum case is especially troublesome since a in a quantum query algorithm, we cannot assume that the queries that were made are known at the end of the computation. Hence, it is not clear what the corresponding certificate should be as a concrete combinatorial object. Although quantum certificate complexity is well understood for two-sided error, as a complexity measure, what would be the natural quantum equivalent to a classical certificate object is still a matter of debate [Jef26; KKW+26]. Several notions capture different aspects of classical certification, but no single quantum measure appears to play the canonical role of certificate complexity. An interesting perspective comes from postselection: the exact postselected randomized query complexity coincides with classical certificate complexity [Cad20, Theorem 16], whereas its quantum counterpart is characterized by rational degree. This suggests that rational degree can be viewed as a natural quantum analogue of certificate complexity. However, this notion is distinct from Aaronson's quantum certificate complexity [Aar08], which captures a different operational notion of quantum certification. The presence of these different, non-equivalent candidates highlights a more fundamental question: what is the appropriate notion of a certificate in the quantum query model, and which aspects of classical certification should such a notion preserve?

Rather than insisting on a model-specific notion of a certificate "object", we take a more operational viewpoint and focus on the certification *task*. Similar notions have appeared in various forms in previous works [Aar08; KT16; BK19]. Given a fixed, publicly known input z (so $f(z)$ is also known, as f is fixed), the certification task for z is as follows. On an arbitrary input x, output "accept" whenever $x = z$, and output "reject" whenever $f(x) \neq f(z)$.

What it means to compute this task will depend on the model of computation we are certifying for. Notice that since we are computing f on a restricted domain, this means that (up to negation) certification for a model M is an easier task than computing f in full, so certification complexity for M is usually a lower bound on M. In the case of deterministic query complexity, the certification task and the certificate objects are equivalent: making the queries to indices in the certificate suffices to achieve the certification task, and conversely, the queries made by an accepting execution of a certification algorithm form a certificate for this input. In this setting, certification is also equivalent to nondeterministic computation, or postselection, where it suffices to guess a certificate, and make those queries, to check for consistency with the given input.

Taking an operational perspective leads us to study certification across computational models without requiring *a priori* a common notion of what a certificate object should look like. We systematically investigate the certification task for various complexity measures in the query world, including quantum query complexity, polynomial degree, and several related measures.

1.1 Certification in operational terms

Let us define our object of study formally.

Definition 1 (input certification problem, or z-certification version of a function)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function and $z \in \mathcal{D}$. Then f_z^{cert} denotes the* z-certification version of f*, which is a partial function defined on the domain $\{z\} \cup \{y \in \mathcal{D} \mid f(y) \neq f(z)\}$ as*

$$f_z^{\mathsf{cert}}(x) := \begin{cases} 1 & \text{if } z = x \\ 0 & \text{if } f(z) \neq f(x) \end{cases}$$

Definition 2 (certification complexity $\mathsf{M}^{\mathsf{cert}}$)**.** *Consider a complexity measure M of Boolean (possibly partial) functions. Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. $\mathsf{M}^{\mathsf{cert}}(f)$ denotes the* certification complexity of f *obtained from M. $\mathsf{M}^{\mathsf{cert}}(f)$ is defined as the complexity of the (worst input z case) z-certification version of f, that is,*

$$\mathsf{M}^{\mathsf{cert}}(f) := \max_{z \in \mathcal{D}} \mathsf{M}\big(f_z^{\mathsf{cert}}\big).$$

As an example, consider the decision tree model D. Certification for z (which is fixed and known) can be achieved by making queries to an input x according to a decision tree for f, and outputting 1 if for all queries i that were made, $x_i = z_i$, and 0 otherwise. Clearly, this procedure will output 1 when $x = z$, and will output 0 whenever $f(x) \neq f(z)$. Running this procedure on z therefore certifies the value of $f(z)$. Since the domain of f_z^{cert} is a subset of $\mathcal{D}$, certifying is no harder than computing the function on the full domain, so we have that $\mathsf{D}^{\mathsf{cert}}(f) \leqslant \mathsf{D}(f)$.

To illustrate the difference between decision and certification, consider the Tribes function. Its input is composed of m blocks $X_1, \ldots, X_m$ where each X_i is an l-bit string, and $\mathsf{Tribes}_{l,m}(X_1, \ldots, X_m) := \bigwedge_{i=1}^m \mathsf{OR}(X_i)$. Certifying z reduces the domain to z and all inputs x where $f(x) \neq f(z)$. Whenever $\mathsf{Tribes}_{l,m}(z) = 0$, z contains an all-0 block, so to certify z, it suffices to output 1 on all inputs where this block is all-0, and zero everywhere else, essentially solving OR_l on this block. Similarly, if $\mathsf{Tribes}_{l,m}(z) = 1$, then z has at least some variable in each block that is set to 1 in z. To certify z, it suffices to output 1 whenever each of these variables is 1, and 0 on all other inputs. This amounts to deciding AND_m on these variables. Depending on the measure, this could be a substantially simpler task.

Operational definitions of certification have appeared in the literature in various forms [Aar08; BK19]. For example, Ben-David and Kothari [BK19, Definition 7] state that one can understand the certificate complexity C and its variants QC and RC through a unifying computational characterization.

1.2 Our contributions

Our main results fall into three categories: new characterizations of known complexity measures and the collapse of various certification measures, new lower bounds and a new framework to study quantum certificates, and some separations.

We apply the certification framework to a wide variety of complexity measures. We defer the formal definitions of these measures to Section 2.

1.2.1 Characterization of certificate complexity: classical and quantum

We start by showing that the input certification approach leads to several new characterizations of certificate complexity C and its variants QC and RC, an indication of the robustness of these notions.

Theorem 3 (characterizations of classical certificate complexities)**.** *For all Boolean (possibly partial) function f*

1. $\mathsf{C}(f) = \mathsf{D}^{\mathsf{cert}}(f) = \mathsf{R}_0^{\mathsf{cert}}(f) = \mathsf{UC}^{\mathsf{cert}}(f) = \Theta\big(\mathsf{CG}^{\mathsf{cert}}(f)\big)$
2. *up to $O(1)$ multiplicative factors,*

$$\mathsf{RC}(f) = \mathsf{R}^{\mathsf{cert}}(f) = \mathsf{RS}^{\mathsf{cert}}(f) = \mathsf{FC}(f) = \mathsf{EC}^{\mathsf{cert}}(f) = \mathsf{prt}^{\mathsf{cert}}(f) = \mathsf{fbs}(f) = \mathsf{cfbs}^{\mathsf{cert}}(f)$$

where UC is the unambiguous certificate complexity (Definition 23), RS is the sabotage complexity (Definition 30), CG is the private coin certificate game complexity (Definition 26), EC is the expectational certificate complexity (Definition 25), prt is the partition bound (Definition 29) and cfbs is the critical fractional block sensitivity (Definition 35).

For completeness, we included in the statement of Theorem 3 the previously known characterizations $\mathsf{FC}(f) = \mathsf{fbs}(f) = \Theta(\mathsf{RC}(f))$ (see Remark 39 for references).

Then we move to the quantum case, starting with characterizations of the bounded-error quantum query complexity Q.

Theorem 4 (computational characterizations of quantum certificate complexity)**.** *Up to $O(1)$ multiplicative factors, for all Boolean (possibly partial) functions f,*

$$\mathsf{QC}(f) = \mathsf{Q}^{\mathsf{cert}}(f) = \mathsf{QD}^{\mathsf{cert}}(f) = \mathsf{MM}^{\mathsf{cert}}(f) = \mathsf{QS}^{\mathsf{cert}}(f)$$

where QD is the quantum distinguishing complexity [BK19] (Definition 40), MM is the quantum adversary bound (minimax formulation, Definition 27), QS is the quantum sabotage complexity [CMP24] defined in Section 4.2.[1]

1.2.2 Exact and zero-error quantum certification complexity

A zero-error quantum algorithm (or a Las Vegas quantum algorithm) never produces an incorrect answer on an input, but is allowed to claim ignorance with probability at most $\frac{1}{2}$. The zero-error quantum query complexity of f, denoted $\mathsf{Q}_0(f)$, is the minimum number of queries needed for a zero-error quantum algorithm to compute f. On the other hand, Q_E denotes the minimum number of queries in a quantum algorithm that computes f exactly. It follows from the definitions that $\mathsf{Q}(f) \leqslant \mathsf{Q}_0(f) \leqslant \mathsf{Q}_\mathsf{E}(f)$ for any function f. For a formal definition, see Definition 17, Definition 18 and Definition 19. Our first contribution is a lower bound on both the complexity measures Q_0 and Q_E. It turns out the certification versions coincide while the certification for bounded error quantum query complexity Q remains different.

Theorem 5 (exact/zero-error collapse of Q_0 and Q_E through the $\cdot^{\mathsf{cert}}$ transform)**.** *Up to $O(1)$ multiplicative factors, for any Boolean (possibly partial) function f*

$$\mathsf{Q}_\mathsf{E}^{\mathsf{cert}}(f) = \mathsf{Q}_0^{\mathsf{cert}}(f) \leqslant \mathsf{Q}_0(f).$$

[1] The theorem holds for the four variants of quantum sabotage complexity, and details are provided in Section 4.2.

This result can be seen as the quantum version of the equality $\mathsf{C}(f) = \mathsf{D}^{\mathsf{cert}}(f) = \mathsf{R}_0^{\mathsf{cert}}(f)$, since Q_E is the quantum analogue of D, and Q_0 is the analogue of R_0, although the proof of Theorem 5 requires a more involved argument that uses exact quantum amplitude amplification (see Section 5 for details).

To the best of our knowledge, $\mathsf{Q}_\mathsf{E}^{\mathsf{cert}}$ is a new lower bound on quantum zero-error query complexity Q_0, a complexity measure that, aside from rational degree, lacks lower bound techniques that are not also lower bounds on Q. The fact that it has two equivalent formulations can also be viewed as an indication that this is a robust notion that merits further study.

1.2.3 Certification using polynomial degree

Perhaps the most intriguing aspect of our systematic study of certification is its application to non-querying complexity measures, including polynomial degree, sensitivity, and related measures. Applying certification to polynomials might seem at odds with the query based nature of certification, but it results in some interesting and often surprising connections with query based certification measures.

Polynomial lower bounds for quantum query complexity We start by giving two new characterizations of quantum certificates in terms of polynomials.

Theorem 6 (polynomial characterizations of quantum certificate complexity)**.** *Up to $O(1)$ multiplicative factors, for all Boolean (possibly partial) functions f,*

$$\mathsf{Q}^{\mathsf{cert}}(f) = \widetilde{\deg}^{\mathsf{cert}}(f) = \widetilde{\text{bm-deg}}^{\mathsf{cert}}(f).$$

Here $\widetilde{\text{bm-deg}}$ denotes block-multilinear approximate bounded-polynomial degree (Definition 38).

This is a good example of what we call the "Sandwich Lemma" (item (iv) from Theorem 13) which says that if $\mathsf{M}^{\mathsf{cert}} \leqslant \mathsf{N} \leqslant \mathsf{M}$, then $\mathsf{N}^{\mathsf{cert}}$ collapses to $\mathsf{M}^{\mathsf{cert}}$. The theorem follows because $\mathsf{Q}^{\mathsf{cert}} \leqslant \widetilde{\deg} \leqslant \widetilde{\text{bm-deg}} \leqslant \mathsf{Q}$ [BBC+01; AA15; AAI+16; ABK21].

Polynomial degree lower bound for zero-error quantum query complexity Next, we define one-sided-error approximate polynomials and the corresponding degree complexity measure $\widetilde{\text{osdeg}}$ (Definition 7), providing a new lower bound on zero-error quantum query complexity that is stronger than both approximate degree (a lower bound on Q), and rational degree (a lower bound on both exact polynomial degree and Q_0). We show that its certification version coincides with exact degree certification complexity $\deg^{\mathsf{cert}}$. This might seem surprising, but on the other hand, it can be seen as the polynomial degree equivalent of the collapses we have seen of $\mathsf{D}^{\mathsf{cert}}$ with $\mathsf{R}_0^{\mathsf{cert}}$, and of $\mathsf{Q}_\mathsf{E}^{\mathsf{cert}}$ with $\mathsf{Q}_0^{\mathsf{cert}}$.

Definition 7 (bounded-polynomial degree measures)**.** *Let $\varepsilon_0, \varepsilon_1 \geqslant 0$ be error parameters and let $\beta \geqslant 1$ be a bounding parameter. Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. The $(\varepsilon_0, \varepsilon_1)$-*approximate *$\beta$-*bounded-polynomial degree *of f, denoted $\Delta_{\varepsilon_0,\varepsilon_1,\beta}(f)$, is defined as*

$$\begin{aligned}
\Delta_{\varepsilon_0,\varepsilon_1,\beta}(f) \quad & \text{is the min of} \quad \deg(P) \\
& \text{over multilinear real polynomials } P \\
& \text{subject to error conditions} \quad \forall x \in f^{-1}(0), |P(x) - f(x)| \leqslant \varepsilon_0 \\
& \text{and} \quad \forall x \in f^{-1}(1), |P(x) - f(x)| \leqslant \varepsilon_1 \\
& \text{and to the bounding condition} \quad \forall x \in \{0,1\}^n, P(x) \in [0, \beta]
\end{aligned}$$

Define the (exact) bounded-polynomial degree *of f, denoted $\deg(f)$, the ε-*approximate bounded-polynomial degree *of f, denoted $\widetilde{\deg}_\varepsilon(f)$, and the* approximate bounded-polynomial degree *of f, denoted $\widetilde{\deg}(f)$, as*

$$\deg(f) := \Delta_{0,0,1}(f) \qquad \widetilde{\deg}_\varepsilon(f) := \Delta_{\varepsilon,\varepsilon,1}(f) \qquad \widetilde{\deg}(f) := \Delta_{\frac{1}{3},\frac{1}{3},1}(f).$$

For any function value $b \in \{0,1\}$*, and error parameter* $\varepsilon \geqslant 0$*, define the* b-sided-error ε-approximate bounded-polynomial degree of f*, denoted* $\widetilde{\mathrm{osdeg}}^b_\varepsilon(f)$*, and the* b-sided-error approximate bounded-polynomial degree of f*, denoted* $\widetilde{\mathrm{osdeg}}^b(f)$*, as*

$$\widetilde{\mathrm{osdeg}}^0_\varepsilon(f) := \Delta_{\varepsilon,0,1}(f) \qquad \widetilde{\mathrm{osdeg}}^1_\varepsilon(f) := \Delta_{0,\varepsilon,1}(f) \qquad \widetilde{\mathrm{osdeg}}^b(f) := \widetilde{\mathrm{osdeg}}^b_{\frac{1}{3}}(f)$$

and define the one-sided-error ε-approximate bounded-polynomial degree of f*, denoted* $\widetilde{\mathrm{osdeg}}_\varepsilon(f)$*, and the* one-sided-error approximate bounded-polynomial degree of f*, denoted* $\widetilde{\mathrm{osdeg}}(f)$*, as*

$$\widetilde{\mathrm{osdeg}}_\varepsilon(f) := \max\left(\widetilde{\mathrm{osdeg}}^0_\varepsilon(f), \widetilde{\mathrm{osdeg}}^1_\varepsilon(f)\right) \qquad \widetilde{\mathrm{osdeg}}(f) := \widetilde{\mathrm{osdeg}}_{\frac{1}{3}}(f).$$

Note that the choice to set the bounding parameter β to 1 is without loss of generality, as setting it to a different *constant* value leads to the same measures deg, $\widetilde{\mathrm{deg}}$, $\widetilde{\mathrm{osdeg}}^0_\varepsilon$, $\widetilde{\mathrm{osdeg}}^1_\varepsilon$ and $\widetilde{\mathrm{osdeg}}_\varepsilon$ up to a constant factor depending only on ε and β on the degree, and without any change in the error parameter. This fact corresponds to the lemmas proved in Appendix C.

We introduce one-sided-error approximate bounded-polynomial degree as a new lower bound on zero-error quantum query complexity.

Theorem 8. *For any* $0 < \varepsilon < 1$ *and any Boolean (possibly partial) function* $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$*,*

$$\mathsf{Q}_0(f) \geqslant \Omega\left(\widetilde{\mathrm{osdeg}}_\varepsilon(f)\right).$$

Although several variants of one-sided polynomials have appeared in the literature, to the best of our knowledge, this definition does not coincide with any of them. Since it is larger than both rational degree and bounded-polynomial approximate degree, it could lead to better lower bounds on Q_0. Moreover, proving lower bounds on one-sided-error approximate degree is comparatively easier than working with the completely bounded polynomial formulation of Arunachalam, Briët, and Palazuelos [ABP19], which characterizes quantum query complexity while also capturing the error parameter.

Theorem 9 (certification equivalence between deg and $\widetilde{\mathrm{osdeg}}$)**.** *For any* $0 < \varepsilon < 1$*, up to* $O(1)$ *multiplicative factors, for any Boolean (possibly partial) function* f

$$\mathrm{deg}^{\mathsf{cert}}(f) = \widetilde{\mathrm{osdeg}}_\varepsilon^{\,\mathsf{cert}}(f) \leqslant \mathsf{Q}_0^{\mathsf{cert}}(f).$$

Certification for degree is not rational degree Each one of Theorem 5 and Theorem 9 independently implies that $\mathrm{deg}^{\mathsf{cert}}$ is a polynomial degree lower bound method on Q_0. In Section 6.4.2, we exhibit a total Boolean function f_m for which $\mathsf{Q}_0(f_m) = \widetilde{\Theta}\big(\mathrm{deg}^{\mathsf{cert}}(f_m)\big) = \widetilde{\Theta}(\mathsf{Q}_{\mathsf{E}}^{\mathsf{cert}}(f_m))$, and both $\mathsf{Q}(f_m), \mathrm{rdeg}(f_m)$ are asymptotically smaller than $\mathrm{deg}^{\mathsf{cert}}(f_m)$.

Theorem 10. *There exists a total function* f_m *on* m^2 *bits such that*

1. $\mathrm{rdeg}(f_m) = m$
2. $\mathrm{deg}^{\mathsf{cert}}(f_m) \geqslant \widetilde{\Omega}\big(m^{3/2}\big)$

This shows that the degree certification measure and the quantum exact certification complexity are new lower bound methods on Q_0. We show that for this function, the bound is tight for Q_0, and that Q is asymptotically smaller that Q_0 (Lemma 55).

1.2.4 Polynomial relations between measures

Spectral sensitivity (Definition 32) is a lower bound on sensitivity, and was shown by Huang [Hua19; ABK+21] to be polynomially related to known query complexity measures for total functions.

Our first result is that certification for spectral sensitivity equals the square root of sensitivity, which establishes that it is also polynomially related to the other known bounds.

We also show that rational degree (Definition 37), a lower bound on Q_0, in equal to its certification measure. Rational degree was recently shown to be polynomially related to query complexity and other known measures, so these two results can be interpreted to mean that certification produces nontrivial measures for the purposes of proving lower bounds.

Theorem 11 (polynomial relationship for certification measures)**.** *For any Boolean (possibly partial) function f*

1. $\lambda^{\mathsf{cert}}(f) = \sqrt{\mathsf{s}(f)} \geqslant \sqrt{\lambda(f)}$ *(Theorem 42)*
2. $\mathrm{rdeg}^{\mathsf{cert}}(f) = \mathrm{rdeg}(f)$ *(Lemma 50)*

To conclude, we provide a quadratic relationship between block sensitivity and $\deg^{\mathsf{cert}}$, and a cubic relationship between certificate complexity and $\deg^{\mathsf{cert}}$ for total functions.

Theorem 12. *Up to $O(1)$ multiplicative factors,*

1. *for any Boolean (possibly partial) function f, $\mathsf{bs}(f) \leqslant \deg^{\mathsf{cert}}(f)^2$*
2. *for any Boolean total function $\mathsf{C}(f) \leqslant \deg^{\mathsf{cert}}(f)^3$.*

We give a proof sketch to illustrate some of our proof techniques. For item 1, Nisan and Szegedy showed [NS94]

$$\mathsf{bs}(f) \leqslant 2\deg(f)^2$$

and their result holds for partial functions. Therefore we can apply one of our Toolbox results described in the next section (item (i) from Theorem 13) and get

$$\mathsf{bs}^{\mathsf{cert}}(f) \leqslant 2\deg^{\mathsf{cert}}(f)^2.$$

Combining this with the fact that $\mathsf{bs}^{\mathsf{cert}}(f) = \mathsf{bs}(f)$ (Remark 39) concludes the proof.

For item 2, Midrijanis showed [Mid04, Theorem 4] that for total functions f,

$$\mathsf{D}(f) \leqslant \deg(f) \cdot \mathsf{bs}(f).$$

Although there are partial functions for which this theorem fails to hold, it holds for any certification function f_z^{cert}, provided that f is total: Lemma 3 in [Mid04] shows that for a total f, every maxonomial of a polynomial representing f contains a sensitive block for z. This block remains sensitive on z when we restrict the function to f_z^{cert}, since $f^{-1}(1-f(z))$ is still included in the domain of f_z^{cert}. Then, for Theorem 4 from that paper, if the queried bits of the input have not fixed the value of the function, they have to be consistent with z. Therefore the queried monomials have to contain a sensitive block for z, and the rest of the proof goes through. Thus, we get

$$\mathsf{D}\big(f^{\mathsf{cert}}\big) \leqslant \deg\big(f_z^{\mathsf{cert}}\big) \cdot \mathsf{bs}\big(f_z^{\mathsf{cert}}\big)$$

which is the same as

$$\mathsf{D}^{\mathsf{cert}}(f) \leqslant \deg^{\mathsf{cert}}(f) \cdot \mathsf{bs}^{\mathsf{cert}}(f).$$

Combining this with item 1 and the fact that $\mathsf{bs}^{\mathsf{cert}}(f) = \mathsf{bs}(f)$ (Remark 39) and $\mathsf{D}^{\mathsf{cert}}(f) = \mathsf{C}(f)$ (Theorem 3), we get the claimed bound on C.

Notice that item 1 is subsumed by the result of de Wolf that $\mathsf{C}(f) \leqslant \max\{\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f)\} \cdot \mathsf{bs}(f)$ [dW03, Lemma 2.6] together with the relations $\mathrm{rdeg}(f) = \max\{\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f)\}$ [KKW+26, Fact 3] and $\mathrm{rdeg} \leqslant \widetilde{\mathrm{osdeg}}^{\mathsf{cert}} = \deg^{\mathsf{cert}}$ (Corollary 51 and Theorem 9). See Section 2.5 for the definitions of rdeg and ndeg.

Nevertheless, the proof highlights an interesting property of the class of partial functions f_z^{cert} where f is a total: it is an example of partial functions where the upper bound of Midrijanis still holds. This class of partial functions might have other interesting properties. For example, Huang's resolution of the sensitivity conjecture holds for total functions, and there are partial functions for which it fails. Therefore, one might ask: does it hold for this family of partial functions? If so, it would imply $\mathsf{FC}(f) \leqslant \deg^{\mathsf{cert}}(f)^2 \leqslant \lambda^{\mathsf{cert}}(f)^4 = \mathsf{s}(f)^2$ for all Boolean total functions f, which would be tight [Rub95], whereas the best upper bound known to hold for total functions is $\mathsf{FC}(f) \leqslant \mathsf{s}(f)^4$.

1.3 Key properties of certification measures

We make use of the following general properties of certification measures $\mathsf{M}^{\mathsf{cert}}$ as a central toolbox to prove many of our results (Theorem 13, Figure 2).

We say that a measure M is *stable* if the following two properties hold for any (possibly partial) function f :

1. $\mathsf{M}(f) = \mathsf{M}(\neg f)$
2. for any g that is a restriction of f to a domain $\mathcal{D}' \subseteq \mathcal{D}$, $\mathsf{M}(g) \leqslant \mathsf{M}(f)$.

Theorem 13 (certification complexity toolbox)**.** *Let* M *and* N *be complexity measures defined on all Boolean (possibly partial) function* $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$*. Then the following holds.*

(i) (the certification transform is monotone) If $\mathsf{M}(g) \leqslant \mathsf{N}(g)$ *for every Boolean (possibly partial) function* g*, then*

$$\mathsf{M}^{\mathsf{cert}}(f) \leqslant \mathsf{N}^{\mathsf{cert}}(f).$$

Furthermore, if M *is stable, then the following properties also hold.*

(ii) (certification is easier than decision) $\mathsf{M}^{\mathsf{cert}}(f) \leqslant \mathsf{M}(f)$

(iii) (the certification transform is idempotent) $(\mathsf{M}^{\mathsf{cert}})^{\mathsf{cert}}(f) = \mathsf{M}^{\mathsf{cert}}(f)$

(iv) (Sandwich Lemma) If for all Boolean (possibly partial) functions g*,* $\mathsf{M}^{\mathsf{cert}}(g) \leqslant \mathsf{N}(g) \leqslant \mathsf{M}(g)$*, then*

$$\mathsf{M}^{\mathsf{cert}}(f) = \mathsf{N}^{\mathsf{cert}}(f).$$

There are a few non-stable measures that also verify items (ii)–(iv) trivially because they collapse to a constant. The only measures in this paper (i.e. among all the measures defined in Section 2) for which items (ii)–(iv) fail to hold are C_1*,* FC_1*,* UC_1 *and* ndeg*.*

The Sandwich Lemma is key to proving the collapse of various certification measures. In addition to LP duality, it provides further explanation to the surprising fact that there are so many equivalent definitions of certification measures such as RC [AKP+21].

Figure 1 summarizes the main relations and separations between some complexity measures and their certification measures.

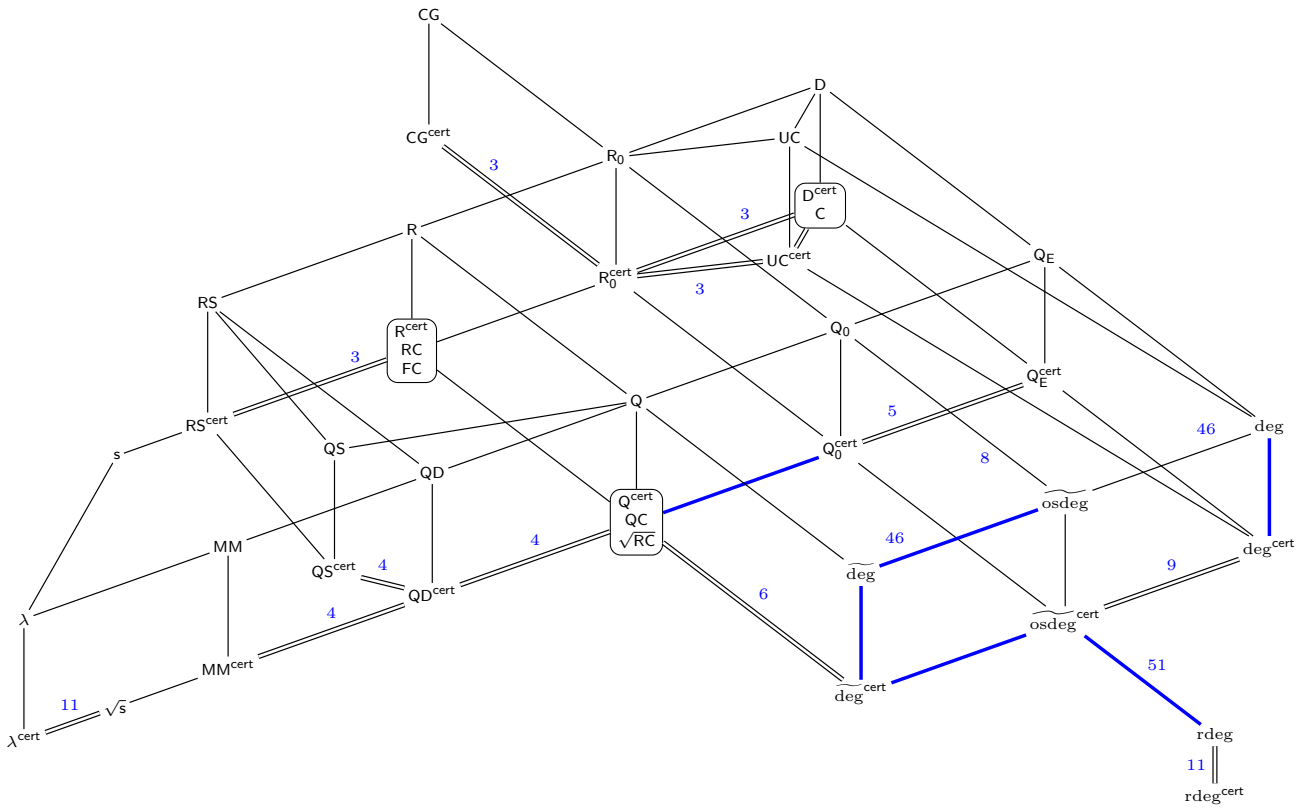

Figure 1: Relations between the complexity measures for all Boolean (possibly partial) functions f. A single line from N to M from down to up means $\mathsf{N}(f) \leqslant O(\mathsf{M}(f))$. Double lines, as well as measures being in the same box, denote equality up to $O(1)$ multiplicative factors, i.e. $\mathsf{N}(f) = \Theta(\mathsf{M}(f))$. Numbers indicate the corresponding theorems in which such relations are shown in this work. In addition, when the line is **thick and blue**, it furthermore indicates a polynomial separation by total function in presented in this article, i.e. there exist a constant power $k > 1$ and a family of Boolean total functions $f_n : \{0,1\}^n \to \{0,1\}$ such that $\mathsf{N}(f_n)^k \leqslant O(\mathsf{M}(f_n))$. These separations witnessing that some complexity measures are not equivalent follow from Theorem 10, Lemma 55 and Proposition 52. The definitions of the complexity measures can be found in Section 2.

1.4 Related work

Certificate complexity was defined by Nisan [Nis89], and has been widely studied since. Randomized and quantum analogues (RC and QC) were proposed by Aaronson [Aar08]. Aaronson used a similar operational definition of certificates that we study in this paper. Tal [Tal13] defined an equivalent measure RC for the randomized setting, formulated as a linear program. In later work, [BK19] gave equivalent formulations as the complexity of the partial function f_z^{cert}. The present work studies this formulation systematically, applying it in a variety of contexts.

A witness in a nondeterministic algorithm could be considered to be a natural candidate for a certificate object. The exact postselected randomized query complexity indeed coincides with classical certificate complexity [Cad20, Theorem 16]. However, in the quantum setting, it is characterized by rational degree (which is equivalent to the maximum between the nondeterministic degree of f and of $\neg f$). This suggests that rational degree can be viewed as another natural quantum analogue of certificate complexity. However, this notion is distinct from Aaronson's quantum certificate complexity [Aar08].

Taking a different approach, Jeffery [Jef26] proposes a notion of quantum witnesses, which can be viewed as witnesses for span programs, known to provide a characterization of quantum query complexity. The corresponding complexity measure coincides with Q, suggesting that certificate objects and certification complexity do not coincide for quantum query complexity.

The presence of these different, non-equivalent candidates highlights a more fundamental question: what is the appropriate notion of a certificate in the quantum query model, and which aspects of classical

certification should such a notion preserve?

Returning to the classical setting, expectational certificate complexity (EC, Definition 25) [JKK+20] defines an expectational version of randomized certificates. EC certificates can be used to give a certification algorithm, however, it is not known to be equivalent to RC.

2 Preliminaries

We provide all the necessary definitions in this section. We refer the reader to [BdW02] and [ABB+17] for more formal definitions of the deterministic query model of computation, the randomized query model of computation and the quantum query model of computation for Boolean functions.

2.1 Query measures

Definition 14 (deterministic query complexity)**.** *The deterministic query complexity of a Boolean (possibly partial) function f, denoted by $\mathsf{D}(f)$, is the worst-case cost of the best deterministic query algorithm computing f.*

Definition 15 (randomized query complexity)**.** *The randomized query complexity of a Boolean (possibly partial) function f, denoted by $\mathsf{R}(f)$, is the worst-case cost of the best randomized query algorithm computing f with two-sided error at most $1/3$.*

Definition 16 (zero-error randomized query complexity)**.** *The zero-error randomized query complexity of a Boolean (possibly partial) function $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$, denoted by $\mathsf{R}_0(f)$, is the minimum worst-case expected cost of a randomized query algorithm that computes f with zero-error, i.e. on every input $x \in \mathcal{D}$ the algorithm should give the correct answer $f(x)$ with probability 1.*

Definition 17 (quantum query complexity)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. The* bounded-error quantum query complexity *of f, denoted by $\mathsf{Q}(f)$, is the minimum number of queries made by a quantum query algorithm A that, for every input $x \in \mathcal{D}$, outputs $f(x)$ with probability at least $\frac{2}{3}$, i.e.*

$$\mathbb{P}[A^x = f(x)] \geqslant \frac{2}{3}$$

where A^x denotes A having query access to input x.

The constant $2/3$ in the definition is arbitrary: it can be replaced by any constant strictly larger than $1/2$, with only a constant-factor change in the query complexity, by standard amplification.

Definition 18 (zero-error quantum query complexity)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. The* zero-error quantum query complexity *of f, denoted by $\mathsf{Q}_0(f)$, is the number of queries made by a quantum query algorithm that on any input $x \in \mathcal{D}$ is allowed to output $\perp$ with probability at most $1/2$. When it outputs a Boolean value b, $f(x) = b$ with probability 1.*

Definition 19 (exact quantum query complexity)**.** *The exact quantum query complexity of a Boolean (possibly partial) function $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$, denoted by $\mathsf{Q}_\mathsf{E}(f)$, is the minimum number of queries made by a quantum algorithm that outputs $f(x)$ on every input $x \in \mathcal{D}$ with probability 1.*

2.2 Certificates and related measures

Definition 20 (partial assignment)**.** *A word $\rho \in \{0,1,*\}^n$ is said to be a* partial assignment over $\{0,1\}^n$ *(where $*$ stands for "not assigned"). If ρ and τ are partial assignments over $\{0,1\}^n$, then τ is said to be* consistent *with ρ, denoted $\rho \prec \tau$, if*

$$\forall i \in [n], \rho(i) \neq * \Rightarrow \rho(i) = \tau(i).$$

The number of assigned positions in ρ *is*

$$|\rho| := |\rho^{-1}(\{0,1\})|.$$

Partial assignments ρ and τ are said to conflict *if there exists an index $i \in [n]$ where $* \neq \rho(i) \neq \tau(i) \neq *$.*

Definition 21 (certificate)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. For all inputs $x \in \mathcal{D}$, a partial assignment $c \in \{0,1,*\}^n$ is said to be a* certificate for x *if $c \prec x$ and for all $z \in \mathcal{D}$ such that $c \prec z$ we have $f(x) = f(z)$.*

Note that partial functions admit two extensions of the definition of certificate for total functions. We use the weak version, where a certificate for x should only conflict with inputs $y \in \mathcal{D} \setminus f^{-1}(f(x))$, whereas in the strong version it should conflict with all elements of $y \in \{0,1\}^n \setminus f^{-1}(f(x))$ which includes the elements outside of the domain.

Definition 22 (certificate complexity)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. For all input $x \in \mathcal{D}$ the* certificate complexity of f at x*, denoted by $\mathsf{C}(f,x)$, is defined as*

$$\mathsf{C}(f,x) := \min_{c \text{ certificate for } x} |c|.$$

For $b \in \{0,1\}$ the b-certificate complexity of f *is defined as*

$$\mathsf{C}_b(f) := \max_{x \in f^{-1}(b)} \mathsf{C}(f,x).$$

Then the certificate complexity of f*, denoted $\mathsf{C}(f)$, is defined as*

$$\mathsf{C}(f) := \max_{x \in \mathcal{D}} \mathsf{C}(f,x) = \max\{\mathsf{C}_0(f), \mathsf{C}_1(f)\}.$$

Definition 23 (unambiguous certificate complexity)**.** *Let $b \in \{0,1\}$. Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. Let a family of partial assignments $(c_x)_{x \in \mathcal{D}}$. The family $\mathcal{C} = (c_x)$ is said to be an* unambiguous family of certificates w.r.t. *f if for all $x, y \in \{0,1\}^n$*

- *certificate condition: c_x is a certificate for x,*
- *unambiguity condition: either $c_x = c_y$, or c_x and c_y conflict.*

For $b \in \{0,1\}$ the unambiguous b-certificate complexity of f *is defined as*

$$\mathsf{UC}_b(f) := \min_{\substack{(c_x) \text{ unambiguous family} \\ \text{of certificates w.r.t. } f}} \max_{x \in f^{-1}(b)} |c_x|.$$

The unambiguous certificate complexity of f*, denoted $\mathsf{UC}(f)$, is defined as*

$$\mathsf{UC}(f) := \max\{\mathsf{UC}_0(f), \mathsf{UC}_1(f)\}.$$

Note that removing the unambiguity condition gives C_0, C_1 and C.

Definition 24 (fractional certificate complexity FC)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. For $b \in \{0,1\}$, the* fractional b-certificate complexity of f*, denoted $\mathsf{FC}_b(f)$, is the value of the following linear program.*

$$\begin{aligned}
\mathsf{FC}_b(f) \qquad & \text{is the min of} \quad \max_{x \in f^{-1}(b)} \sum_{i \in [n]} w_x(i) \\
& \text{over} \quad (w_x)_{x \in \mathcal{D}} \\
& \text{subject to} \quad \forall x \in \mathcal{D}, \forall i \in [n], 0 \leqslant w_x(i) \\
& \text{and the weak conflict condition} \\
& \forall x \in \mathcal{D}, \forall y \in \mathcal{D}, \\
& f(x) \neq f(y) \Rightarrow \sum_{i \in [n] : x_i \neq y_i} w_x(i) \geqslant 1
\end{aligned}$$

Weights $(w_x)_{x \in \mathcal{D}}$ subject to such conditions are said to be a family of fractional b-certificates w.r.t. f.

The fractional certificate complexity of f*, denoted $\mathsf{FC}(f)$, is defined to be* $\max\{\mathsf{FC}_0(f), \mathsf{FC}_1(f)\}$.

Because each fractional certificate of a family of fractional certificates satisfies the conditions independently of the rest of the family, and similarly for the fractional b-certificates, then $\mathsf{FC}(f) = \max\{\mathsf{FC}_0(f), \mathsf{FC}_1(f)\}$.

Definition 25 (expectational certificate complexity EC [JKK+20, Definition 9])**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. The* expectational certificate complexity of f*, denoted $\mathsf{EC}(f)$, is the value of the following linear program.*

$$\begin{aligned}
\mathsf{EC}(f) \quad & \text{is the min of} \quad \max_{x\in\mathcal{D}} \sum_{i\in[n]} w_x(i) \\
& \text{over} \quad (w_x)_{x\in\mathcal{D}} \\
& \text{subject to} \quad \forall x \in \mathcal{D}, \forall i \in [n], 0 \leqslant w_x(i) \leqslant 1 \\
& \text{and the strong conflict condition} \\
& \forall x \in \mathcal{D}, \forall y \in \mathcal{D}, \\
& f(x) \neq f(y) \Rightarrow \sum_{i\in[n]:x_i\neq y_i} w_x(i) w_y(i) \geqslant 1
\end{aligned}$$

Weights $(w_x)_{x\in\mathcal{D}}$ subject to such conditions are said to be a family of expectational certificates w.r.t. f.

Definition 26 (certificate game complexity with private randomness CG [CGL+23])**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. The* certificate game complexity with private randomness of f*, denoted $\mathsf{CG}(f)$, is given by the following linear program.*

$$\begin{aligned}
\sqrt{\mathsf{CG}(f)} \quad & \text{is the min of} \quad \max_{x\in\mathcal{D}} \sum_{i\in[n]} w_x(i) \\
& \text{over} \quad (w_x)_{x\in\mathcal{D}} \\
& \text{subject to} \quad \forall x \in \mathcal{D}, \forall i \in [n], 0 \leqslant w_x(i) \\
& \text{and the strong conflict condition} \\
& \forall x \in \mathcal{D}, \forall y \in \mathcal{D}, \\
& f(x) \neq f(y) \Rightarrow \sum_{i\in[n]:x_i\neq y_i} w_x(i) w_y(i) \geqslant 1
\end{aligned}$$

2.3 Adversary bounds and other measures

Definition 27 (min max adversary bound MM)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. The* min max adversary bound of f*, denoted $\mathsf{MM}(f)$, is the value of the following program.*

$$\begin{aligned}
\mathsf{MM}(f) \quad & \text{is the min of} \quad \max_{x\in\mathcal{D}} \sum_{i\in[n]} w_x(i) \\
& \text{over} \quad (w_x(i))_{x\in\mathcal{D},i\in[n]} \\
& \text{subject to} \quad \forall x \in \mathcal{D}, \forall i \in [n], w_x(i) \geqslant 0 \\
& \text{and} \\
& \forall x \in \mathcal{D}, \forall y \in \mathcal{D}, \\
& f(x) \neq f(y) \Rightarrow \sum_{i\in[n]:x_i\neq y_i} \sqrt{w_x(i) w_y(i)} \geqslant 1
\end{aligned}$$

Definition 28 (classical adversary bound CAdv [AKP+21, where CAdv is denoted CMM, see Lemma 7 for the equivalence with this definition; ABK21, Section 2.2.2])**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a*

Boolean (possibly partial) function. The classical adversary bound of f, *denoted* $\mathsf{CAdv}(f)$, *is the value of the following program.*

$$\begin{aligned}
\mathsf{CAdv}(f) \quad & \text{is the min of} \quad \max_{x\in\mathcal{D}} \sum_{i\in[n]} w_x(i) \\
& \text{over} \quad (w_x(i))_{x\in\mathcal{D},i\in[n]} \\
& \text{subject to} \quad \forall x\in\mathcal{D}, \forall i\in[n], w_x(i)\geqslant 0 \\
& \text{and} \\
& \forall x\in\mathcal{D}, \forall y\in\mathcal{D}, \\
& f(x)\neq f(y) \Rightarrow \sum_{i\in[n]:x_i\neq y_i} \min\{w_x(i), w_y(i)\} \geqslant 1
\end{aligned}$$

We give the primal definition of the partition bound for query complexity.

Definition 29 (partition bound [JK10, Definition 13])**.** *Let $f:\mathcal{D}\subseteq\{0,1\}^n\to\{0,1\}$ be a Boolean (possibly partial) function. Let $\mathcal{A}$ denote the set of all partial assignments $A:S\to\{0,1\}$, where $S\subseteq[n]$. We write $x\in A$ if $x_i=A(i)$ for every $i\in S$, and define $|A|:=|S|$.*

For $\varepsilon\geqslant 0$, the ε-partition bound of f, denoted by $\mathsf{Prt}_\varepsilon(f)$, is the optimal value of the following linear program:

$$\begin{aligned}
\mathsf{Prt}_\varepsilon(f) \quad & \text{is the min of} \quad \sum_{b\in\{0,1\}}\sum_{A\in\mathcal{A}} w_{b,A}\, 2^{|A|} & & \\
& \text{over weights} \quad (w_{b,A})_{b\in\{0,1\},A\in\mathcal{A}} & & \\
& \text{subject to} \quad \sum_{\substack{A\in\mathcal{A}\\ x\in A}} w_{f(x),A} \geqslant 1-\varepsilon & & \forall x\in\mathcal{D}, \\
& \text{and} \quad \sum_{\substack{A\in\mathcal{A}\\ x\in A}}\sum_{b\in\{0,1\}} w_{b,A} = 1 & & \forall x\in\{0,1\}^n, \\
& \text{and} \quad w_{b,A}\geqslant 0 & & \forall b\in\{0,1\}, \forall A\in\mathcal{A},
\end{aligned}$$

The partition bound is scaled exponentially compared to other query lower bounds, so we define $\mathsf{prt}_\varepsilon(f):=\log_2(\mathsf{Prt}_\varepsilon(f))$. Also define $\mathsf{prt}(f):=\mathsf{prt}_{\frac{1}{3}}(f)$.

Definition 30 (sabotage complexity)**.** *Let $f:\mathcal{D}\subseteq\{0,1\}^n\to\{0,1\}$ be a Boolean (possibly partial) function. For $b\in\{*,\dagger\}$, define*

$$P_f^b := \left\{\rho\in\{0,1,b\}^n \;\middle|\; \text{there exist } x\in f^{-1}(0) \text{ and } y\in f^{-1}(1) \text{ such that } \rho\prec x \text{ and } \rho\prec y\right\}.$$

The sabotage function *associated to f is $f_{\mathsf{sab}}:P_f^*\cup P_f^\dagger\to\{0,1\}$, defined by*

$$f_{\mathsf{sab}}(z) := \begin{cases} 0 & \text{if } z\in P_f^*, \\ 1 & \text{if } z\in P_f^\dagger \end{cases}$$

The randomized sabotage complexity of f *is defined as*

$$\mathsf{RS}(f) := \mathsf{R}_0(f_{\mathsf{sab}})$$

where R_0 denotes zero-error randomized query complexity.

2.4 Sensitivity and related measures

Definition 31 (sensitivity)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. For all input $x \in \mathcal{D}$ the i^{th} bit is said to be* sensitive for x w.r.t. f *if $f(x^i) \neq f(x)$ where x^i denotes the input equal to x on every bit except on bit i, which is flipped. The* sensitivity of x w.r.t f *is defined as*

$$\mathsf{s}(f,x) := \left|\left\{i \in [n] \,\middle|\, f(x^i) \neq f(x), x^i \in \mathcal{D}\right\}\right|,$$

while the sensitivity of f *is defined as*

$$\mathsf{s}(f) := \max_{x \in \mathcal{D}} \mathsf{s}(f,x).$$

Spectral sensitivity was first introduced by [Kou93] to prove formula size lower bounds. It is a spectral relaxation of sensitivity.

Definition 32. *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. We define M_f as the $\mathcal{D} \times \mathcal{D}$ sensitivity matrix of f as $M_f(x,y) = 1$ whenever $f(x) \neq f(y)$ and $d_H(x,y) = 1$, and 0 otherwise. Its spectral sensitivity is defined as*

$$\lambda(f) = \|M_f\|$$

where $\|\cdot\|$ is the spectral norm.

Definition 33 (block sensitivity)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. For all input $x \in \mathcal{D}$ a block $B \subseteq [n]$ is said to be a* sensitive block for x w.r.t f *if $x^B \in \mathcal{D}$ and $f(x^B) \neq f(x)$, where x^B denotes the input equal to x on every bit except on bits $i \in B$, which are flipped. The* block sensitivity of f at x*, denoted by $\mathsf{bs}(f,x)$, is defined as*

$$\mathsf{bs}(f,x) := \max\left\{k \,\middle|\, \exists B_1, \ldots, B_k \text{ with } B_i \cap B_j = \emptyset \text{ for } i \neq j \text{ and } f(x^{B_i}) \neq f(x) \text{ and } x^{B_i} \in \mathcal{D}\right\}.$$

The block sensitivity of f *is defined as*

$$\mathsf{bs}(f) := \max_{x \in \mathcal{D}} \mathsf{bs}(f,x).$$

Fractional block sensitivity (fbs) is obtained by allowing fractional weights on sensitive blocks.

Definition 34 (fractional block sensitivity)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. For all input $x \in \mathcal{D}$ let $\mathcal{B}(f,x) := \left\{B \subseteq [n] \,\middle|\, f(x^B) \neq f(x), x^B \in \mathcal{D}\right\}$ denote the set of all its sensitive blocks. The* fractional block sensitivity of f at x*, denoted by $\mathsf{fbs}(f,x)$, is the value of the following linear program.*

$$\begin{aligned} \mathsf{fbs}(f,x) \quad & \text{is the max of} \quad \sum_{B \in \mathcal{B}(f,x)} w(B) \\ & \text{over} \quad (w(B))_{B \in \mathcal{B}(f,x)} \\ & \text{subject to} \quad \forall i \in [n], \sum_{B \in \mathcal{B}(f,x) : i \in B} w(B) \leqslant 1 \\ & \text{and} \quad \forall B \in \mathcal{B}(f,x), w(B) \in [0,1] \end{aligned}$$

The fractional block sensitivity of f *is defined as:*

$$\mathsf{fbs}(f) := \max_{x \in \mathcal{D}} \mathsf{fbs}(f,x).$$

Note that restricting the linear program for $\mathsf{fbs}(f,x)$ to integral values gives $\mathsf{bs}(f,x)$.

The fractional measures fbs and FC were introduced in [Tal13], where it was shown that for all $x \in \{0,1\}^n$ they verify $\mathsf{fbs}(f,x) = \mathsf{FC}(f,x)$ since the linear program for fractional certificate complexity and fractional block sensitivity are the primal-dual of each other and are also feasible.

Next we define critical fractional block sensitivity from fractional block sensitivity.

Definition 35 (critical fractional block sensitivity [ABK21, Section 2.2.1])**.** *Let $f : \mathcal{D}(f) \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. A Boolean total function $g : \{0,1\}^n \to \{0,1\}$ is called a* completion of f *if for all inputs $x \in \mathcal{D}$ they coincide, i.e. $g(x) = f(x)$. The* critical fractional block sensitivity of f*, denoted* $\mathsf{cfbs}(f)$*, is defined as*

$$\mathsf{cfbs}(f) := \min_{g \text{ completion of } f} \max_{x \in \mathcal{D}(f)} \mathsf{fbs}(x, g).$$

2.5 Polynomial degree measures

Degree and approximate degree are defined in Section 1.2.3. We give the definitions of a few more polynomial degree-based measures in this section.

We start with the two only degree measures where we do not require the polynomials to be bounded on the whole Boolean hypercube $\{0,1\}^n$.

Definition 36 (nondeterministic polynomial degree)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. The* nondeterministic polynomial degree of f*, denoted* $\mathrm{ndeg}(f)$*, is defined as*

$$\begin{aligned} \mathrm{ndeg}(f) \quad & \text{is the min of} \quad \deg(P) \\ & \text{over real polynomial } P \\ & \text{subject to} \quad \forall x \in f^{-1}(0), P(x) = 0 \\ & \text{and} \quad \forall x \in f^{-1}(1), P(x) \neq 0 \end{aligned}$$

Definition 37 (rational degree)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. The* rational polynomial degree of f*, denoted* $\mathrm{rdeg}(f)$*, is defined as*

$$\begin{aligned} \mathrm{rdeg}(f) \quad & \text{is the min of} \quad \max\{\deg(P), \deg(Q)\} \\ & \text{over real polynomials } P, Q \\ & \text{subject to} \quad \forall x \in \mathcal{D}, \frac{P(x)}{Q(x)} = f(x) \end{aligned}$$

For all Boolean (possibly partial) functions f, $\mathrm{rdeg}(f) = \max\{\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f)\}$. We use this characterization from [KKW+26, Fact 3] when working with rdeg.

Definition 38 (block-multilinear bounded-polynomial degree [AA15; AAI+16, Definition 2.3])**.** *Let $f : \mathcal{D} \subseteq \{-1,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. Let $\epsilon \geqslant 0$. A polynomial P of degree d is called* block-multilinear *if its variables can be partitioned into d blocks such that every monomial of P contains exactly one variable from each block.*

For $x = (x_1, \ldots, x_n) \in \{-1,1\}^n$, let

$$\widetilde{x} := (1, x_1, \ldots, x_n).$$

The block-multilinear ϵ-approximate bounded-polynomial degree of f*, denoted by* $\widetilde{\text{bm-deg}}_\epsilon(f)$*, is defined as the value of the following program.*

$$\begin{aligned} \widetilde{\text{bm-deg}}_\epsilon(f) \quad & \text{is the min of} \quad d \\ & \text{over} \quad d \in \mathbb{N} \\ & \text{and block-multilinear real polynomial } P : \mathbb{R}^{d(n+1)} \to \mathbb{R} \text{ of degree } d \\ & \text{subject to} \quad \forall x \in \mathcal{D}, 0 \leqslant P(\widetilde{x}, \ldots, \widetilde{x}) \leqslant 1 \\ & \text{and the error condition} \quad \forall x \in \mathcal{D}, |P(\widetilde{x}, \ldots, \widetilde{x}) - f(x)| \leqslant \epsilon \\ & \text{and the bounding condition} \quad \forall z \in \{-1,1\}^{k(n+1)}, |P(z)| \leqslant 1 \end{aligned}$$

Then define the block-multilinear approximate bounded-polynomial degree of f*, denoted* $\widetilde{\text{bm-deg}}(f)$*, and the* block-multilinear bounded-polynomial degree of f*, denoted* $\text{bm-deg}(f)$*, as*

$$\widetilde{\text{bm-deg}}(f) := \widetilde{\text{bm-deg}}_{\frac{1}{3}}(f) \qquad \text{bm-deg}(f) := \widetilde{\text{bm-deg}}_0(f).$$

Given a block-multilinear polynomial P approximating $g : \mathcal{D} \subseteq \{-1,1\}^n \to \{0,1\}$ in the $\{-1,1\}$ basis, the polynomial $P \circ \frac{1+x}{2}$ is now in the $\{0,1\}$ basis with the same degree and same values. Similarly for $f : \mathcal{D}' \subseteq \{0,1\}^n \to \{0,1\}$ in the $\{0,1\}$ basis, the reverse transformation $f \circ (2x-1)$ brings it to the $\{-1,1\}$ basis. That's this relabeling that we have in mind when applying $\widetilde{\text{bm-deg}}_\epsilon$ to a function f in the $\{0,1\}$ basis [AAI+16, Section 2.2]: first we go to $g := f \circ (2x-1)$ and then apply $\widetilde{\text{bm-deg}}_\epsilon$ to g.

3 Certification complexity

Informally, an algorithm that certifies the value $f(z)$ of z should output 1 on z and 0 whenever it is given an input x such that $f(x) \neq f(z)$. The formal definition is given in Definition 1 and Definition 2, where we have used the notation

$$\mathsf{M}^{\mathsf{cert}}(f) := \max_{z \in \mathcal{D}} \mathsf{M}\big(f_z^{\mathsf{cert}}\big),$$

for M a complexity measure of Boolean functions.

3.1 General properties of certification measures

We prove several properties of certification complexity that will be essential tools in proving the main results of the paper. We show that certification is non-increasing, idempotent, and monotone with respect to the underlying query complexity measure. We also give a general condition under which two measures have the same certification complexity. These properties will be used throughout the paper.

Theorem 13 (certification complexity toolbox)**.** *Let* M *and* N *be complexity measures defined on all Boolean (possibly partial) function* $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$*. Then the following holds.*

(i) (the certification transform is monotone) If $\mathsf{M}(g) \leqslant \mathsf{N}(g)$ *for every Boolean (possibly partial) function* g*, then*

$$\mathsf{M}^{\mathsf{cert}}(f) \leqslant \mathsf{N}^{\mathsf{cert}}(f).$$

Furthermore, if M *is stable, then the following properties also hold.*

(ii) (certification is easier than decision) $\mathsf{M}^{\mathsf{cert}}(f) \leqslant \mathsf{M}(f)$

(iii) (the certification transform is idempotent) $(\mathsf{M}^{\mathsf{cert}})^{\mathsf{cert}}(f) = \mathsf{M}^{\mathsf{cert}}(f)$

(iv) (Sandwich Lemma) If for all Boolean (possibly partial) functions g*,* $\mathsf{M}^{\mathsf{cert}}(g) \leqslant \mathsf{N}(g) \leqslant \mathsf{M}(g)$*, then*

$$\mathsf{M}^{\mathsf{cert}}(f) = \mathsf{N}^{\mathsf{cert}}(f).$$

There are a few non-stable measures that also verify items (ii)–(iv) trivially because they collapse to a constant. The only measures in this paper (i.e. among all the measures defined in Section 2) for which items (ii)–(iv) fail to hold are C_1*,* FC_1*,* UC_1 *and* ndeg*.*

Figure 2 summarizes the properties in Theorem 13.

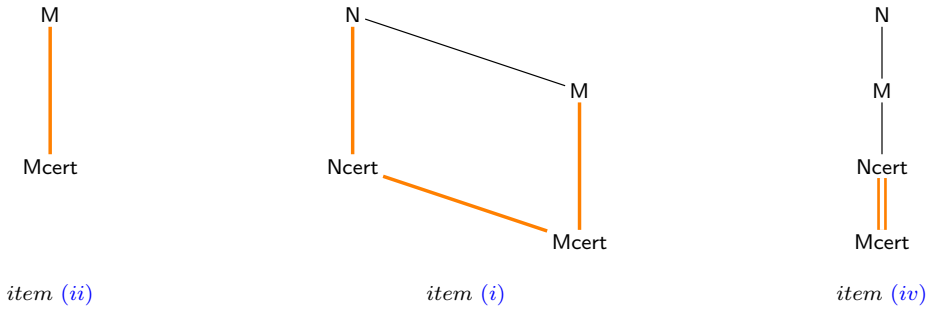

Figure 2: Three items from the Toolbox (Theorem 13). Double lines denote equality up to $O(1)$ multiplicative factor. A single line from N to M from down to up means $\mathsf{N}(f) \leqslant O(\mathsf{M}(f))$. Double lines denote equality up to $O(1)$ multiplicative factors, i.e. $\mathsf{N}(f) = \Theta(\mathsf{M}(f))$. **Orange lines** are the lines implied by black lines. The case of stable complexity measures is depicted.

Proof of item (i) from Theorem 13. Let two complexity measures M and N such that $\mathsf{M}(g) \leqslant \mathsf{N}(g)$ for all Boolean (possibly partial) function g. Applying the inequality to the z-certification versions of f, one gets

$$\mathsf{M}^{\mathsf{cert}}(f) = \max_{z \in \mathcal{D}} \mathsf{M}\big(f_z^{\mathsf{cert}}\big) \leqslant \max_{z \in \mathcal{D}} \mathsf{N}\big(f_z^{\mathsf{cert}}\big) = \mathsf{N}^{\mathsf{cert}}(f). \qquad \square$$

Proof of item (ii) of Theorem 13. We prove that all complexity measures considered in this work, except C_1, FC_1, UC_1, and ndeg, verify item (ii) of Theorem 13. (See definitions in Section 2 for the list of these measures.) Let M be any of these measures. Then M is monotone under restriction of the domain (item 2 of the definition of stability).

Let first consider measures M that are stable (i.e. that also verify item 1 of the definition). For all $z \in f^{-1}(1)$,

$$\mathsf{M}\big(f_z^{\mathsf{cert}}\big) = \mathsf{M}\left(f_{\big|\{z\} \cup \{y \in \mathcal{D} \,|\, f(z) \neq f(y)\}}\right) \leqslant \mathsf{M}(f)$$

and for all $z \in f^{-1}(0)$,

$$\mathsf{M}\big(f_z^{\mathsf{cert}}\big) = \mathsf{M}\left(\neg f_{\big|\{z\} \cup \{y \in \mathcal{D} \,|\, f(z) \neq f(y)\}}\right) \leqslant \mathsf{M}(f).$$

So $\mathsf{M}^{\mathsf{cert}}(f) = \max\limits_{z \in \mathcal{D}}(f_z^{\mathsf{cert}}) \leqslant \mathsf{M}$.

Now consider $\mathsf{M}(f)$ being one of $\mathrm{ndeg}(\neg f)$, $\mathsf{C}_0(f)$ or $\mathsf{FC}_0(f)$ – for which item 1 of the definition fails. The result will still hold as these measures vanish through the cert transform, as follows.

For any constant function $f : \mathcal{D} \subseteq \{0,1\} \to \{0,1\}$ we have $\mathsf{M}(f) = 0$, so

$$\mathsf{M}^{\mathsf{cert}}(f) = \max_{z \in \mathcal{D}} \mathsf{M}\big(f_z^{\mathsf{cert}}\big) = 0 = \mathsf{M}(f)$$

where the second equality follows from f_z^{cert} being constant. Now, for any non constant f and any input $z \in \mathcal{D}$, we have $\mathsf{M}(f) \leqslant 1$ and $\mathsf{M}(f_z^{\mathsf{cert}}) = 1$ so

$$\mathsf{M}^{\mathsf{cert}}(f) = \max_{z \in \mathcal{D}} \mathsf{M}\big(f_z^{\mathsf{cert}}\big) = 1 \leqslant \mathsf{M}(f).$$

$\square$

Proof of item (iii) from Theorem 13. For all $z \in \mathcal{D}$ we have that $(f_z^{\mathsf{cert}})_z^{\mathsf{cert}} = f_z^{\mathsf{cert}}$. Then on the one hand,

$$\begin{aligned}
\big(\mathsf{M}^{\mathsf{cert}}\big)^{\mathsf{cert}}(f) &= \max_{z \in \mathcal{D}} \mathsf{M}^{\mathsf{cert}}\big(f_z^{\mathsf{cert}}\big) \\
&= \max_{z \in \mathcal{D}} \max_{y \in \mathcal{D}} \mathsf{M}\Big(\big(f_z^{\mathsf{cert}}\big)_y^{\mathsf{cert}}\Big) \\
&\geqslant \max_{z \in \mathcal{D}} \mathsf{M}\Big(\big(f_z^{\mathsf{cert}}\big)_z^{\mathsf{cert}}\Big) \\
&= \max_{z \in \mathcal{D}} \mathsf{M}\big(f_z^{\mathsf{cert}}\big) \\
&= \mathsf{M}^{\mathsf{cert}}(f)
\end{aligned}$$

On the other hand,

$$\big(\mathsf{M}^{\mathsf{cert}}\big)^{\mathsf{cert}}(f) = \max_{z \in \mathcal{D}} \mathsf{M}^{\mathsf{cert}}\big(f_z^{\mathsf{cert}}\big) \leqslant \max_{z \in \mathcal{D}} \mathsf{M}\big(f_z^{\mathsf{cert}}\big) = \mathsf{M}^{\mathsf{cert}}(f)$$

where the inequality follows from the assumption item (ii) from Theorem 13. $\square$

Proof of item (iv) from Theorem 13. Suppose that $\mathsf{M} \geqslant \mathsf{N} \geqslant \mathsf{M}^{\mathsf{cert}}$, i.e.

$$\mathsf{M}(g) \geqslant \mathsf{N}(g) \geqslant \mathsf{M}^{\mathsf{cert}}(g)$$

for every Boolean (possibly partial) function g. Applying item (i) from Theorem 13 on the hypothesis for the first inequality, applying the hypothesis for the second inequality, and applying item (iii) from Theorem 13 for the last equality, we have

$$\mathsf{M}^{\mathsf{cert}}(f) \geqslant \mathsf{N}^{\mathsf{cert}}(f) = \max_{z \in \mathcal{D}} \mathsf{N}\big(f_z^{\mathsf{cert}}\big) \geqslant \max_{z \in \mathcal{D}} \mathsf{M}^{\mathsf{cert}}\big(f_z^{\mathsf{cert}}\big) = \big(\mathsf{M}^{\mathsf{cert}}\big)^{\mathsf{cert}}(f) = \mathsf{M}^{\mathsf{cert}}(f)$$

so $\mathsf{M}^{\mathsf{cert}}(f) = \mathsf{N}^{\mathsf{cert}}(f)$.

□

We (informally) say a complexity measure M is *local* if it is defined as the worst case, over inputs x, of the complexity at x, usually written as $\mathsf{M}(f;x)$.

Remark 39 (Certification of local complexity measures)**.** *If a complexity measure* M *is* local*, and for any Boolean (possibly partial) function* $g : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ *and any* $z \in \mathcal{D}$ *it verifies* $\mathsf{M}(g,z) = \mathsf{M}(g_z^{\mathsf{cert}})$*, then for any Boolean (possibly partial) function* f *we have* $\mathsf{M}^{\mathsf{cert}}(f) = \max_{z \in \mathcal{D}} \mathsf{M}(g_z^{\mathsf{cert}}) = \mathsf{M}(f)$*.*

Of course this is exactly Definition 2 (so it is trivial). The remark is actually about noticing that s*,* bs*,* FC*,* fbs*,* RC *and* C *are usually defined in this local way, e.g.* $\mathsf{s}(f) := \max_{z \in \mathcal{D}} \mathsf{s}(f,z)$ *where* $\mathsf{s}(f,z) = \mathsf{s}(f_z^{\mathsf{cert}})$*. So for any Boolean (possibly partial) function* f

- $\mathsf{s}^{\mathsf{cert}}(f) = \mathsf{s}(f)$
- $\mathsf{bs}^{\mathsf{cert}}(f) = \mathsf{bs}(f)$
- $\mathsf{FC}^{\mathsf{cert}}(f) = \mathsf{FC}(f) = \mathsf{fbs}(f) = \mathsf{fbs}^{\mathsf{cert}}(f)$*, where the second equality follows from [Tal13, Theorem 2; GSS16, Section 2.6]*
- $\mathsf{RC}^{\mathsf{cert}}(f) = \mathsf{RC}(f)$
- $\mathsf{C}^{\mathsf{cert}}(f) = \mathsf{C}(f)$.

Also recall that any Boolean (possibly partial) function f *verifies* $\mathsf{FC}(f) = \Theta(\mathsf{RC}(f))$ *[Tal13, Claim 5.5; GSS16, Claim 38] (even though the claims are not explicitly stated to hold for partial functions, their proofs are done for partial functions).*

3.2 Certification, witnesses and postselection

There are a few other candidates to consider if we wish to capture what certificate complexity should mean over various models of computation, or more broadly, for complexity measures M. We have proposed an operational definition, but one might also like to define a certificate "object" : given an input x, a purported value for $f(x)$, and given this certificate "object" for x, we would like to use it to verify that $f(x)$ is as claimed. For D, this is a partial assignment. For R, it can be a weighted set of queries. One certificate may be used to certify several instances of f. The associated certificate complexity would then be the computational cost in model M to carry out the certification algorithm. One can also think of it as a nondeterministic task: given a certificate and an input, accept if the certificate is valid for this input, otherwise reject. Similarly, in a query-based model, one might also phrase it in terms of postselection: guess a certificate, and if the certification procedure accepts, accept; else abort.

For classical query model these three notions coincide. In Section A we make this claim more formal.

But in the quantum case, we show that they do not coincide. On the postselection side, Cade showed that exact postselected randomized query complexity is equal to certificate complexity [Cad20, Theorem 16], whereas Mahadev and de Wolf showed that exact postselected quantum query complexity is characterized by rational degree [MdW15, Theorem 1, Theorem 2]. On the certification side, we recover that deterministic certification complexity is equal to certificate complexity, whereas our approach allows us to find a distinction between the certification task and postselection in the quantum case. We show that exact quantum query certification complexity $\mathsf{Q}_{\mathsf{E}}^{\mathsf{cert}}$ and exact postselected quantum query complexity are two distinct notions, thanks to our lower bound on $\mathsf{Q}_{\mathsf{E}}^{\mathsf{cert}}$ by $\deg^{\mathsf{cert}}$ for which we provide an asymptotic separation with rdeg in Theorem 10.

4 Characterizations of certificate complexity

In this section, we give the proofs of the new characterizations of C and RC.

4.1 Certification for classical complexity measures

We start by reproducing the known characterization for the classical certificate complexity. Note that most of the characterizations are already known in the literature (some of them implicitly, some of them explicitly). Our certification framework is abstract enough to capture the different variant of the same complexity measure.

Theorem 3 (characterizations of classical certificate complexities)**.** *For all Boolean (possibly partial) function f*

1. $\mathsf{C}(f) = \mathsf{D}^{\mathsf{cert}}(f) = \mathsf{R}_0^{\mathsf{cert}}(f) = \mathsf{UC}^{\mathsf{cert}}(f) = \Theta\big(\mathsf{CG}^{\mathsf{cert}}(f)\big)$
2. *up to $O(1)$ multiplicative factors,*

$$\mathsf{RC}(f) = \mathsf{R}^{\mathsf{cert}}(f) = \mathsf{RS}^{\mathsf{cert}}(f) = \mathsf{FC}(f) = \mathsf{EC}^{\mathsf{cert}}(f) = \mathsf{prt}^{\mathsf{cert}}(f) = \mathsf{fbs}(f) = \mathsf{cfbs}^{\mathsf{cert}}(f)$$

where UC is the unambiguous certificate complexity (Definition 23), RS is the sabotage complexity (Definition 30), CG is the private coin certificate game complexity (Definition 26), EC is the expectational certificate complexity (Definition 25), prt is the partition bound (Definition 29) and cfbs is the critical fractional block sensitivity (Definition 35).

Proof of item 1 of Theorem 3. We break the proof into three parts.

(i) $\mathsf{D}^{\mathsf{cert}} = \mathsf{R}_0^{\mathsf{cert}} = \mathsf{C}$: It is known that $\mathsf{D} \geqslant \mathsf{R}_0 \geqslant \mathsf{C}$ (follows from the definitions). Applying item (i) from Theorem 13 (certification monotonicity) to the known relation $\mathsf{D} \geqslant \mathsf{R}_0 \geqslant \mathsf{C}$ one gets $\mathsf{D}^{\mathsf{cert}}(f) \geqslant \mathsf{R}_0^{\mathsf{cert}} \geqslant \mathsf{C}^{\mathsf{cert}}(f) = \mathsf{C}(f)$ where the equality follows from Remark 39.

To prove the converse inequality $\mathsf{D}^{\mathsf{cert}}(f) \leqslant \mathsf{C}(f)$, let $z \in \mathcal{D}$ and consider the certificate given by $\mathsf{C}(f, z)$. The following deterministic algorithm computes f_z^{cert} in $\mathsf{C}(f_z^{\mathsf{cert}})$ queries: query the defined positions of the certificate, then output 1 iff the queried values all match the certificate. Then $\mathsf{D}(f_z^{\mathsf{cert}}) \leqslant \mathsf{C}(f, z)$. So

$$\mathsf{D}^{\mathsf{cert}}(f) = \max_{z \in \mathcal{D}} \mathsf{D}\big(f_z^{\mathsf{cert}}\big) \leqslant \max_{z \in \mathcal{D}} \mathsf{C}(f, z) = \mathsf{C}(f).$$

(ii) $\mathsf{UC}^{\mathsf{cert}}(f) = \mathsf{D}^{\mathsf{cert}}(f)$: Apply item (iv) from Theorem 13 (Sandwich Lemma) to $\mathsf{D} \geqslant \mathsf{UC} \geqslant \mathsf{C} = \mathsf{D}^{\mathsf{cert}}$ where the inequalities follow from the definitions and the equality follows from the previous item.

(iii) Lemma 59 states that $(\mathsf{C}_0 \cdot \mathsf{C}_1)^{\mathsf{cert}} = \mathsf{C}$ on Boolean (possibly partial) functions, and is proved in Section B. So one can conclude by applying item (iv) from Theorem 13 (Sandwich Lemma) to $\mathsf{C} \leqslant \mathsf{R}_0 \leqslant O(\mathsf{CG}) \leqslant O(\mathsf{C}_0 \cdot \mathsf{C}_1)$ where the second inequality follows from [JKK+20, Theorem 1; CGL+23, Theorem 22.2] (the proof of which indeed holds for partial functions, even though not explicitly stated as such in the theorems) and the last inequality follows from [CGL+23, Theorem 22.4]. □

Proof of item 2 of Theorem 3. Equalities and inequalities between complexity measures are up to $O(1)$ multiplicative factor. We proceed in four steps:

(i) $\mathsf{RC}(f) = \mathsf{R}^{\mathsf{cert}}(f)$ is shown in [Aar08, Proposition 4; BK19, Definition 7].

(ii) $\mathsf{R}^{\mathsf{cert}}(f) = \mathsf{RS}^{\mathsf{cert}}(f) = \mathsf{FC}^{\mathsf{cert}}$: Apply item (iv) from Theorem 13 (Sandwich Lemma) to $\mathsf{R} \geqslant \mathsf{RS} \geqslant \mathsf{FC} = \mathsf{RC} = \mathsf{R}^{\mathsf{cert}}$ where the first equality follows from the end of Remark 39 and the last equality follows from the previous item.

(iii) $\mathsf{prt}^{\mathsf{cert}}(f) = \mathsf{CAdv}^{\mathsf{cert}}(f) = \mathsf{cfbs}^{\mathsf{cert}}(f) = \mathsf{FC}(f)$: Apply item (iv) from Theorem 13 to $\mathsf{R} \geqslant \mathsf{prt} \geqslant \mathsf{CAdv} \geqslant \mathsf{cfbs} \geqslant \mathsf{fbs} = \mathsf{RC} = \mathsf{R}^{\mathsf{cert}}$ where the first inequality follows from [JK10, Theorem 3.1], the second inequality follows from [JK10, Theorem 3.5, Definition 19; AKP+21, where CAdv is denoted CMM, see Lemma 7 for the equivalence with our Definition 28 of CAdv], the third inequality follows from [ABK21, Lemma 26], the fourth inequality follows from definitions [ABK21, beginning of Section 2.3.2], the first equality follows from Remark 39 and the last equality follows from previous items.

(iv) $\mathsf{EC}^{\mathsf{cert}}(f) = \mathsf{FC}(f)$: Let $(v_z(i))_{z\in\mathcal{D},i\in[n]}$ be optimal weights for the $\mathsf{FC}(f)$ program. Then, for $z \in \mathcal{D}$ and $x \in \{z\} \cup \{y \in \mathcal{D} \,|\, f(y) \neq f(z)\}$, if $f(x) \neq f(z)$ let $B_x^z \subseteq \{i \in [n] \,|\, x_i \neq z_i\}$ be a minimal sensitive bloc of z, and for $i \in [n]$ let

$$w_x^z(i) := \begin{cases} v_x(i) & \text{if } x = z \\ \mathbb{1}_{i\in B_x^z} & \text{if } f(x) \neq f(z) \end{cases}$$

Then for all $z \in \mathcal{D}$, weights $(w_x^z(i))$ satisfy the $\mathsf{EC}(f_z^{\mathsf{cert}})$ program. So

$$\begin{aligned}
\mathsf{EC}^{\mathsf{cert}}(f) &= \max_{z\in\mathcal{D}} \mathsf{EC}\big(f_z^{\mathsf{cert}}\big) \\
&\leqslant \max_{z\in\mathcal{D}} \max_{x\in\{z\}\cup\{y\in\mathcal{D}\,|\,f(y)\neq f(z)\}} \sum_{i\in[n]} w_x^z(i) \\
&\leqslant \max_{z\in\mathcal{D}} \max\left\{ \sum_{i\in[n]} v_z(i), \max_{\substack{x\in\mathcal{D}: \\ f(x)\neq f(z)}} |B_x^z| \right\} \\
&\leqslant \max_{z\in\mathcal{D}} \max\{\mathsf{FC}(f), \mathsf{s}(f)\} \\
&\leqslant \mathsf{FC}(f) \\
&\leqslant \mathsf{EC}(f)
\end{aligned}$$

where the third inequality follows from the fact that each bit in B_x^z is sensitive for the input $z^{B_x^z}$ as B_x^z is a minimal sensitive bloc of z, and the last inequality follows from [JKK+20, Theorem 1].

Applying item (iv) from Theorem 13 (Sandwich Lemma) and Remark 39, conclude that $\mathsf{EC}^{\mathsf{cert}} = \mathsf{FC}$. □

4.2 Quantum certification complexity measures

In this subsection we provide the proofs for the characterizations of quantum certificate complexity. Before going into the theorem we will first describe some of the definitions of complexity measures that we will be using.

Definition 40 (quantum distinguishing complexity [BK19])**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. The* quantum distinguishing complexity of f*, denoted $\mathsf{QD}(f)$, is the smallest integer k for which there exists a k-query quantum algorithm that, on every input $x \in D$, outputs a quantum state ρ_x such that*

$$|\rho_x - \rho_y|_{\mathrm{tr}} \geqslant \frac{1}{6}$$

for every $x, y \in \mathcal{D}$ satisfying $f(x) \neq f(y)$.

Definition 41 (quantum sabotage complexity [CMP24])**.** *For inputs $x, y \in \{0,1\}^n$ and $b \in \{*, \dagger\}$, define $[x, y, b] \in \{0, 1, b\}^n$ coordinate wise by*

$$[x,y,b]_i := \begin{cases} x_i & \text{if } x_i = y_i \\ b & \text{if } x_i \neq y_i \end{cases}$$

Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ *be a Boolean (possibly partial) function, and let*

$$\mathcal{D}_0 := f^{-1}(0) \qquad \text{and} \qquad \mathcal{D}_1 := f^{-1}(1).$$

For $b \in \{*, \dagger\}$*, define the set of* b-sabotaged inputs *as*

$$S_b := \{[x, y, b] \,|\, x \in \mathcal{D}_0,\ y \in D_1\}$$

and let

$$\mathcal{D}_{\mathsf{sab}} := S_* \cup S_\dagger.$$

The sabotage function *associated with* f *is the partial function*

$$f_{\mathsf{sab}} : \mathcal{D}_{\mathsf{sab}} \to \{0,1\}$$

defined by

$$f_{\mathsf{sab}}(z) := \begin{cases} 0 & \text{if } z \in S_* \\ 1 & \text{if } z \in S_\dagger \end{cases}$$

The quantum sabotage complexity *of* f *in the weak input model is*

$$\mathsf{QS}_{\mathsf{weak}}(f) := \mathsf{Q}(f_{\mathsf{sab}})$$

where $\mathsf{Q}(\cdot)$ *denotes bounded-error quantum query complexity.*

The paper defines several variants

$$\mathsf{QS}_{\mathsf{weak}}(f) := \mathsf{Q}(f_{\mathsf{sab}}) \qquad \mathsf{QS}^{\mathsf{ind}}_{\mathsf{weak}}(f) := \mathsf{Q}(f^{\mathsf{ind}}_{\mathsf{sab}})$$

and, in the strong input model,

$$\mathsf{QS}_{\mathsf{str}}(f) := \mathsf{Q}\big(f^{\mathsf{str}}_{\mathsf{sab}}\big) \qquad \mathsf{QS}^{\mathsf{ind}}_{\mathsf{str}}(f) := \mathsf{Q}\Big(f^{\mathsf{str},\mathsf{ind}}_{\mathsf{sab}}\Big).$$

See [CMP24] for more details.

Theorem 4 (computational characterizations of quantum certificate complexity)**.** *Up to* $O(1)$ *multiplicative factors, for all Boolean (possibly partial) functions* f*,*

$$\mathsf{QC}(f) = \mathsf{Q}^{\mathsf{cert}}(f) = \mathsf{QD}^{\mathsf{cert}}(f) = \mathsf{MM}^{\mathsf{cert}}(f) = \mathsf{QS}^{\mathsf{cert}}(f)$$

where QD *is the quantum distinguishing complexity [BK19] (Definition 40),* MM *is the quantum adversary bound (minimax formulation, Definition 27),* QS *is the quantum sabotage complexity [CMP24] defined in Section 4.2.*[2]

Proof. Equalities and inequalities between complexity measures are up to $O(1)$ multiplicative factor. The proof is divided into six parts.

(i) [Aar08, Proposition 4; BK19, Definition 7] proved that any Boolean (possibly partial) function f verifies

$$\mathsf{QC}(f) = \mathsf{Q}^{\mathsf{cert}}(f).$$

(ii) $\mathsf{Q}^{\mathsf{cert}}(f) = \mathsf{QD}^{\mathsf{cert}}(f) = \mathsf{MM}^{\mathsf{cert}}(f)$: Apply item (iv) from Theorem 13 to $\mathsf{Q} \geqslant \mathsf{QD} \geqslant \mathsf{MM} \geqslant \sqrt{\mathsf{CAdv}} \geqslant \sqrt{\mathsf{cfbs}} \geqslant \sqrt{\mathsf{fbs}} = \sqrt{\mathsf{RC}} = \mathsf{QC} = \mathsf{Q}^{\mathsf{cert}}$, where the first and second inequalities follow from [BK19], the third inequality follows from [ABK21, Theorem 30], the fourth inequality follows from [ABK21, Lemma 26], the fifth inequality follows from definitions [ABK21, beginning of Section 2.3.2], the first equality follows from Remark 39, the second equality follows from [Aar08, Theorem 7], and the last equality follows from the previous item (i).

[2]The theorem holds for the four variants of quantum sabotage complexity, and details are provided in Section 4.2.

(iii) As a bonus, we give an elementary proof of

$$\mathsf{Q}^{\mathsf{cert}}(f) = \mathsf{QD}^{\mathsf{cert}}(f).$$

For any $z \in \mathcal{D}$ let algorithm $A(z)$ be optimal for $\mathsf{QD}(f_z^{\mathsf{cert}})$. Measuring the output of algorithm $A(z)$ on basis $\left(A(z)\left|z\right\rangle, (A(z)\left|z\right\rangle)^{\perp}\right)$ gives an algorithm computing f_z^{cert} in the query model of computation Q with the same quantum query complexity. So $\mathsf{QD}(f_z^{\mathsf{cert}}) \geqslant \mathsf{Q}(f_z^{\mathsf{cert}})$. Thus

$$\mathsf{QD}^{\mathsf{cert}}(f) = \max_{z\in\mathcal{D}} \mathsf{QD}\big(f_z^{\mathsf{cert}}\big) \geqslant \max_{z\in\mathcal{D}} \mathsf{Q}\big(f_z^{\mathsf{cert}}\big) = \mathsf{Q}^{\mathsf{cert}}(f).$$

The converse $\mathsf{QD}^{\mathsf{cert}}(f) \leqslant \mathsf{Q}^{\mathsf{cert}}(f)$ follows from $\mathsf{QD} \leqslant \mathsf{Q}$ by item (i) from Theorem 13.

(iv) We give two proofs of the fact that $\left(\mathsf{QS}^{\mathsf{ind}}_{\mathsf{weak}}\right)^{\mathsf{cert}}(f) \leqslant \mathsf{QD}^{\mathsf{cert}}(f)$.

- Let z be the input for which the maximum of $\mathsf{QS}^{\mathsf{ind}}_{\mathsf{weak}}(f_z)$ is achieved and let $c = f(z)$. Let $a = *$ and $b = \dagger$. Modify the query oracle so that if the result of the query on the i-th bit is a or b, then the modified result is z_i and $1 - z_i$, respectively. In this way, the inputs in S_a are all mapped to z, and the inputs in S_b are all mapped to the inputs $f^{-1}(c)$. By [Aar08], there exists a bounded-error quantum algorithm that uses at most $O(\mathsf{QC}(f))$ queries such that:
  - it "accepts" z;
  - it "rejects" any input $y \in f^{-1}(c)$ and returns a position i such that $z_i \neq y_i$.

  The output of this algorithm can be used to solve the sabotaged function. If the algorithm rejected, return 1; also return the index found by the algorithm. If the algorithm accepted, try the same strategy with $a = \dagger$ and $b = *$. Since in one of the two cases the sabotaged input will be mapped to an input y such that $f(y) \neq f(z)$, the algorithm will reject in that case and thus solve the sabotaged function. The required follows as $\mathsf{QD}^{\mathsf{cert}}(f) = \mathsf{QC}(f)$ by points above.
- Proof by amplitude amplification: Let $z \in \mathcal{D}$. Let A be an optimal algorithm for $\mathsf{QD}(f_z^{\mathsf{cert}})$, hence running in $T = \mathsf{QD}(f_z^{\mathsf{cert}})$ queries.

  Consider the following algorithm B, which runs on a b-sabotaged input $[y, z, b]$ (where $b \in \{*, \dagger\}$ and $f(y) \neq f(z)$) of f_z^{cert} as follows. Pick $t \in [0, T]$ uniformly at random and run A^z (which does not require any query to y) until right before the tth query. Measure the query index register – it gives an index $i \in [n]$.

  According to [BK19, Lemma 12], the probability that $y_i \neq z_i$ (i.e. $[y, z, b]_i \in \{*, \dagger\}$) is $\Omega\left(\frac{1}{T^2}\right)$, which can be tested in one query to $[y, z, b]$. Hence, using quantum amplitude amplification, one can find a b-index in $[y, z, b]$ with $O(T)$ repetitions of algorithm B and so $O(T)$ queries to $[y, z, b]$. Thus, $\mathsf{QS}^{\mathsf{ind}}_{\mathsf{weak}}(f_z^{\mathsf{cert}}) \leqslant \mathsf{QD}(f_z^{\mathsf{cert}})$. So $\left(\mathsf{QS}^{\mathsf{ind}}_{\mathsf{weak}}\right)^{\mathsf{cert}}(f) \leqslant \mathsf{QD}^{\mathsf{cert}}(f)$.

(v) $\mathsf{QC} \leqslant \mathsf{QS}_{\mathsf{str}}(f)$: [CMP24, Theorem 5] states that $\sqrt{\mathsf{fbs}} \leqslant \mathsf{QS}_{\mathsf{str}}$ and its proof indeed holds for partial functions (see [CMP24, Lemma 18 and beginning of Section 5.1]), even though it is not explicitly stated as such in the theorem. Conclude with $\mathsf{QC} = \sqrt{\mathsf{FC}} = \sqrt{\mathsf{fbs}}$ where the first equality follows from [Aar08, Theorem 7] and the last equality from Remark 39.

(vi) item (i), item (ii), item (iv) and item (v) from Theorem 4 imply that $\left(\mathsf{QS}^{\mathsf{ind}}_{\mathsf{weak}}\right)^{\mathsf{cert}} \leqslant \mathsf{QD}^{\mathsf{cert}} = \mathsf{Q}^{\mathsf{cert}} = \mathsf{QC} \leqslant \mathsf{QS}_{\mathsf{str}} \leqslant \mathsf{QS}^{\mathsf{ind}}_{\mathsf{str}} \leqslant \mathsf{QS}^{\mathsf{ind}}_{\mathsf{weak}}$ and $\left(\mathsf{QS}^{\mathsf{ind}}_{\mathsf{weak}}\right)^{\mathsf{cert}} \leqslant \mathsf{QD}^{\mathsf{cert}} = \mathsf{Q}^{\mathsf{cert}} = \mathsf{QC} \leqslant \mathsf{QS}_{\mathsf{str}} \leqslant \mathsf{QS}_{\mathsf{weak}} \leqslant \mathsf{QS}^{\mathsf{ind}}_{\mathsf{weak}}$. Then, applying item (iv) from Theorem 13 (Sandwich Lemma) one gets

$$(\mathsf{QS}_{\mathsf{weak}})^{\mathsf{cert}} = (\mathsf{QS}_{\mathsf{str}})^{\mathsf{cert}} = \left(\mathsf{QS}^{\mathsf{ind}}_{\mathsf{weak}}\right)^{\mathsf{cert}} = \left(\mathsf{QS}^{\mathsf{ind}}_{\mathsf{str}}\right)^{\mathsf{cert}} = \left(\mathsf{Q}^{\mathsf{cert}}\right)^{\mathsf{cert}} = \mathsf{Q}^{\mathsf{cert}}$$

where the last equality follows from item (iii) from Theorem 13.

□

4.3 Certification for sensitivity

Since sensitivity is a local measure, certification applied to sensitivity. However when applied to spectral sensitivity, we show that λ^{cert} equals $\sqrt{\mathsf{s}}$:

Theorem 42. *For any boolean (possibly partial) function $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$*

$$\lambda^{\mathsf{cert}}(f) = \sqrt{\mathsf{s}(f)}.$$

Proof. Let $z \in \mathcal{D}$ and $b := 1 - f(z)$. For $x, y \in \{z\} \cup f^{-1}(b)$ let

$$M_{f_z^{\mathsf{cert}}}(x,y) := \begin{cases} 1 & \text{if } f(x) \neq f(y) \text{ and there exists } i \in [n] \text{ such that } x^i = y \\ 0 & \text{otherwise} \end{cases}$$

Notice that the sensitivity matrix contains only $\mathsf{s}(f;z)$ 1's in the row and column indexed by z, and is 0 everywhere else. Therefore, $\lambda(f_z^{\mathsf{cert}}) = \left\|M_{f_z^{\mathsf{cert}}}\right\| = \sqrt{\mathsf{s}(f,z)}$, which implies that $\lambda^{\mathsf{cert}}(f) = \sqrt{\mathsf{s}(f)}$. □

5 Certification complexity for Q_0 and Q_E

In this section, we will prove the equivalence between $\mathsf{Q}_\mathsf{E}^{\mathsf{cert}}$ and $\mathsf{Q}_0^{\mathsf{cert}}$. Let us restate our theorem.

Theorem 5 (exact/zero-error collapse of Q_0 and Q_E through the $\cdot^{\mathsf{cert}}$ transform)**.** *Up to $O(1)$ multiplicative factors, for any Boolean (possibly partial) function f*

$$\mathsf{Q}_\mathsf{E}^{\mathsf{cert}}(f) = \mathsf{Q}_0^{\mathsf{cert}}(f) \leqslant \mathsf{Q}_0(f).$$

The proof uses *exact* amplitude amplification, [BHM+02, Theorem 4, second method].

Recall that amplitude amplification is a quantum algorithm that amplifies the correctness of an algorithm that succeeds with probability at least p to a constant success probability, using $O(\sqrt{\frac{1}{p}})$ iterations [BHM+02].

Stated informally, [BHM+02] also show that *exact* quantum amplitude amplification can be achieved when the probability of success on an input z is known exactly (not just a lower bound). In the certification setting, the certification input z is known, and we are provided with a quantum algorithm for f_z^{cert} which is zero-error, but not exact, which means it can fail (output $\perp$) with constant probability, but never errs otherwise. The key is to observe that since z is known, and the algorithm is known, the error probability on z is known exactly, so zero error can be incurred on input z by using exact error amplification. In addition, for inputs y such that $f(z) \neq f(y)$, the zero-error quantum algorithm always outputs either 0 or $\perp$. After running exact amplitude amplification parameterized for the error on z, the state of the algorithm on any of the remaining inputs y such that $f(z) \neq f(y)$, will remain in the subspace corresponding to the 0 or $\perp$ outputs, which is orthogonal to the subspace corresponding to the 1 output.

The more formal statement of exact amplitude amplification follows.

Theorem 43 (exact quantum amplitude amplification [BHM+02, Theorem 4, second method])**.** *Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean total function. Let $\mathcal{H} = \mathcal{H}_0 \otimes \mathcal{H}_1$ be an Hilbert space of dimension at least 2^n and π_0 (resp. π_1) be the projector onto $\mathcal{H}_0$ (resp. $\mathcal{H}_1$). Let $(|x\rangle)_{x\in\{0,1\}^n}$ be a family of orthonormal states in $\mathcal{H}$ (that are not necessarily in $\mathcal{H}_0$ or $\mathcal{H}_1$). Let $|init\rangle$ be a state in $\mathcal{H}$. Let G be a unitary. Let the success probability of G be $p := \|\pi_1 G |init\rangle\|_2^2$. Let S_0 be a unitary such that for all $|\chi\rangle \in \mathcal{H}_0$*

$$S_0(\phi)|\chi\rangle = e^{i\phi}|\chi\rangle$$

and for all $|\chi\rangle \in \mathcal{H}_1$

$$S_0(\phi)|\chi\rangle = |\chi\rangle.$$

Let $S_f(\varphi)$ be a unitary such that for all $x \in \{0,1\}^n$

$$S_f(\varphi)|x\rangle = e^{i\varphi f(x)}|x\rangle.$$

We will refer to $S_0(\phi)$ *and* $S_f(\varphi)$ *as* pseudo-reflections. *Let* $Q(\phi,\varphi) := GS_0(\phi)G^\dagger S_f(\varphi)$.

If $p \neq 0$, *then there exists phases* ϕ *and* φ *and a number of iterations* k *such that*

$$Q(\phi,\varphi)Q(\pi,\pi)^k G\,|init\rangle \in \mathcal{H}_1$$

and

$$k \leqslant O\left(\frac{1}{\sqrt{p}}\right)$$

i.e. it is an algorithm that achieves exact success, with $O\left(\frac{1}{\sqrt{p}}\right)$ *queries to* G *and* $G^\dagger$, *and relies on the knowledge of* p.

Lemma 44 (exact quantum certification algorithm from zero-error quantum certification algorithm)**.** *Let* $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ *be a Boolean (possibly partial) function. Let* $\mathcal{H} = \widehat{\mathcal{H}}_0 \otimes \widehat{\mathcal{H}}_1 \otimes \widehat{\mathcal{H}}_\perp$ *be an Hilbert space of dimension* 2^n *and* $\widehat{\pi}_0$ *(resp.* $\widehat{\pi}_1$ *and* $\widehat{\pi}_{0,\perp}$*) be the projector onto* $\widehat{\mathcal{H}}_0$ *(resp.* $\widehat{\mathcal{H}}_1$ *and* $\widehat{\mathcal{H}}_0 \oplus \widehat{\mathcal{H}}_\perp$*). Let* $(|x\rangle)_{x\in\{0,1\}^n}$ *be a family of orthonormal states in* $\mathcal{H}$ *(that are not necessarily in* $\widehat{\mathcal{H}}_0$, $\widehat{\mathcal{H}}_1$ *or* $\widehat{\mathcal{H}}_\perp$*). Let* $|init\rangle$ *be a state in* $\mathcal{H}$.

Let $0 < \varepsilon < 1$. *Let* $z \in \mathcal{D}$. *Let* A *be a* Q_0 *algorithm computing* f_z^{cert} *in* $\mathsf{Q}_0(f_z^{\mathsf{cert}})$ *queries, i.e. for any input* $x \in \{z\} \cup \{y \in \mathcal{D} \,|\, f(y) \neq f(z)\}$ *the algorithm* A, *when given query access to input* x *(which we denote* A^x*), has measurement probabilities satisfying* $\left\|\widehat{\pi}_{1-f(x)}A^x\,|init\rangle\right\|_2^2 = 1$ *and* $\left\|\widehat{\pi}_{f(x)}A^x\,|init\rangle\right\|_2^2 \leqslant \frac{1}{2}$.

Let $S_{0,\perp}$ *be a unitary such that for all* $|\chi\rangle \in \mathcal{H}_0 \otimes \mathcal{H}_\perp$

$$S_{0,\perp}(\phi)\,|\chi\rangle = e^{i\phi}\,|\chi\rangle$$

and for all $|\chi\rangle \in \mathcal{H}_1$

$$S_{0,\perp}(\phi)\,|\chi\rangle = |\chi\rangle\,.$$

Let $S_f(\varphi)$ *be a unitary such that for all* $x \in \mathcal{D}$

$$S_f(\varphi)\,|x\rangle = e^{i\varphi f(x)}\,|x\rangle\,.$$

and acts as the identity on any other $|x\rangle$. *For phases* ϕ *and* φ, *define algorithm* $Q(\phi,\varphi)$, *when given query access to input* $x \in \{z\} \cup \{y \in \mathcal{D} \,|\, f(y) \neq f(z)\}$, *as*

$$Q^x(\phi,\varphi) := A^x S_{0,\perp}(\phi)(A^x)^\dagger S_f(\varphi)$$

where in order to compute $(A^x)^\dagger$, *the inverse of algorithm* A *is implemented with the same number of queries as* A, *which is always possible since the quantum query operator is its own inverse.*

Then, the theorem states that there exists phases ϕ *and* φ *and a number of iterations* k *such that*

$$Q^z(\phi,\varphi)Q^z(\pi,\pi)^k A^z\,|init\rangle \in \widehat{\mathcal{H}}_1$$

and for all $y \in D$ *such that* $f(y) \neq f(z)$

$$Q^y(\phi,\varphi)Q^y(\pi,\pi)^k A^y\,|init\rangle \in \widehat{\mathcal{H}}_0 \otimes \widehat{\mathcal{H}}_\perp$$

and

$$k \leqslant O(1)$$

i.e. it is an algorithm that achieves exactness w.r.t. measurement $(\widehat{\pi}_1, \widehat{\pi}_{0,\perp})$ *in* $O(\mathsf{Q}_0(f_z^{\mathsf{cert}}))$ *queries.*

Proof. Let us first consider the case of input z, which will fix phases ϕ and φ in order to have exactness, and then prove exactness for any other input under those parameters:

- For input z: Apply Theorem 43 with $\mathcal{H}_1 := \widehat{\mathcal{H}}_1$, $\mathcal{H}_0 := \widehat{\mathcal{H}}_0 \otimes \widehat{\mathcal{H}}_\perp$, $G := A^z$ and $p := \|\widehat{\pi}_1 A^z\,|init\rangle\|_2^2 \geqslant \frac{1}{2} > 0$. This gives exactness on input z and fixes phases ϕ and φ and the number of iterations $k \leqslant O\left(\frac{1}{\sqrt{p}}\right) \leqslant O(1)$, which corresponds to $O(\mathsf{Q}_0(f_z^{\mathsf{cert}}))$ queries (since G and $G^\dagger$ are computed using the same number of queries).
- For input $y \in \mathcal{D}$ such that $f(y) \neq f(z)$: Notice that for any phases ϕ' and φ', operator $Q^y(\phi',\varphi')$ only adds a global phase, i.e. there exists a phase γ such that $Q(\phi',\varphi')A^y\,|init\rangle = e^{i\gamma}A^y\,|init\rangle$. In particular with phases ϕ, φ and π it implies that $Q^y(\phi,\varphi)Q^y(\pi,\pi)^k G\,|init\rangle \in \widehat{\mathcal{H}}_0 \otimes \widehat{\mathcal{H}}_\perp$. Hence exactness on input y. □

Theorem 5 follows as a corollary.

6 Polynomial certification complexity

In this section, we give the proofs of our results pertaining to the certification of polynomial degree comlexity measures.

6.1 Exact polynomials

In order to give a flavor of certifying polynomials, we start by giving a direct proof that $\deg^{\mathsf{cert}}(f) \leqslant \mathsf{C}(f)$. (Notice that since $\deg(f) \leqslant \mathsf{D}(f)$, we can also immediately get $\deg^{\mathsf{cert}}(f) \leqslant \mathsf{C}^{\mathsf{cert}}(f) = \mathsf{C}(f)$ by applying Theorem 13 item (i).)

Remark 45 (elementary proof of $\deg^{\mathsf{cert}}(f) \leqslant \mathsf{C}(f)$)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. Then*

$$\deg^{\mathsf{cert}}(f) = \max_{z \in \mathcal{D}} \deg\left(f_z^{\mathsf{cert}}\right) \leqslant \max_{z \in \mathcal{D}} \mathsf{C}(f, z) = \mathsf{C}(f)$$

where the inequality follows from the fact that $P(x) := \prod_{i \in c} x_i - z_i$ is an exact polynomial for $f_z^{\mathsf{cert}}(x)$ whenever c is an f-certificate of z.

By construction, the degree certification measure $\deg^{\mathsf{cert}}$ is a lower bound on $\mathsf{Q}_{\mathsf{E}}^{\mathsf{cert}}$ – as one can prove by applying item (i) from Theorem 13 to $\deg \leqslant 2\mathsf{Q}_{\mathsf{E}}$ [BBC+01, Theorem 4.3]. Hence, it is a lower bound on Q_0, by the collapse $\mathsf{Q}_{\mathsf{E}}^{\mathsf{cert}} = \mathsf{Q}_0^{\mathsf{cert}}$ (Theorem 5). In Section 6.3 we will show another way to prove that degree certification gives a lower bound on Q_0 by proving that it collapses with its one-sided-error counterpart.

Finally, for completeness, we restate here the upper bounds in terms of $\deg^{\mathsf{cert}}$ proved in the introduction (Section 1.2.4).

Theorem 12. *Up to $O(1)$ multiplicative factors,*

1. *for any Boolean (possibly partial) function f, $\mathsf{bs}(f) \leqslant \deg^{\mathsf{cert}}(f)^2$*
2. *for any Boolean total function $\mathsf{C}(f) \leqslant \deg^{\mathsf{cert}}(f)^3$.*

6.2 Approximate polynomials with two-sided error

We prove a new characterization of QC in terms of certification complexity for approximate polynomials.

Theorem 6 (polynomial characterizations of quantum certificate complexity)**.** *Up to $O(1)$ multiplicative factors, for all Boolean (possibly partial) functions f,*

$$\mathsf{Q}^{\mathsf{cert}}(f) = \widetilde{\deg}^{\mathsf{cert}}(f) = \widetilde{\text{bm-deg}}^{\mathsf{cert}}(f).$$

Proof. Equalities and inequalities between complexity measures are up to $O(1)$ multiplicative factor. Apply item (iv) from Theorem 13 to $\mathsf{Q}^{\mathsf{cert}} = \mathsf{QC} = \sqrt{\mathsf{RC}} = \sqrt{\mathsf{fbs}} \leqslant \widetilde{\deg} \leqslant \widetilde{\text{bm-deg}} \leqslant \mathsf{Q}$ where the first equality follows from Theorem 4, the second equality follows from [Aar08, Theorem 7], the third equality follows from Remark 39, the first inequality follows from [ABK21, Theorem 28], the second inequality follows from definitions, and the last inequality follows from [AA15, Lemma 10; AAI+16, Lemma 2.2]. □

6.3 Approximate polynomials with one-sided error

We introduce one-sided-error approximate degree as the zero-error counterpart of degree and approximate degree, hence a new lower bound on zero-error quantum query complexity (see Definition 7).

Fact 46. *For any Boolean (possibly partial) function f*

$$\widetilde{\deg}(f) \leqslant \widetilde{\text{osdeg}}(f) \leqslant \deg(f).$$

Proof. This follows directly from their definitions. □

Theorem 8. *For any $0 < \varepsilon < 1$ and any Boolean (possibly partial) function $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$,*

$$\mathsf{Q}_0(f) \geqslant \Omega\Big(\widetilde{\mathrm{osdeg}}_\varepsilon(f)\Big).$$

Proof. Let A be a T-query zero-error quantum query algorithm for f. Then according to [BBC+01, Lemma 4.2] there exist multilinear real polynomials P^0 and P^1 of degree at most $2T$ such that for all $x \in \mathcal{D}$

$$P^0(x) = \mathbb{P}[A \text{ outputs } 0 \text{ on } x] \qquad \text{and} \qquad P^1(x) = \mathbb{P}[A \text{ outputs } 1 \text{ on } x].$$

Then, not only each P^b is a $\frac{1}{2}$-approximating bounded polynomial for f, but also, since A is zero-error, it is moreover b-sided-error. So

$$\widetilde{\mathrm{osdeg}}^0_{\frac{1}{2}}(f) \leqslant \deg\big(P^0\big) \leqslant 2T \qquad \text{and} \qquad \widetilde{\mathrm{osdeg}}^1_{\frac{1}{2}}(f) \leqslant \deg\big(P^1\big) \leqslant 2T.$$

Thus $\widetilde{\mathrm{osdeg}}_{\frac{1}{2}}(f) \leqslant 2T \leqslant 2\mathsf{Q}_0(f)$ and more generally for any $0 < \varepsilon \leqslant \frac{1}{2}$. Similarly, using standard error reduction of a Q_0 algorithm by iterating it a constant number of time, one gets $\mathsf{Q}_0(f) \geqslant \Omega\Big(\widetilde{\mathrm{osdeg}}_\varepsilon(f)\Big)$. □

We can easily derive the following relation on the corresponding certification measures.

Corollary 47. *For any $0 < \varepsilon < 1$ and any Boolean (possibly partial) function f,*

$$\mathsf{Q}_0^{\mathsf{cert}}(f) \geqslant \Omega\left(\widetilde{\mathrm{osdeg}}_\varepsilon^{\ \mathsf{cert}}(f)\right).$$

Proof. Apply item (i) from Theorem 13 to Theorem 8. □

Before we prove that the one-sided-error approximate degree and exact degree certification measures collapse, we need the following lemma.

Lemma 48. *For any $0 < \varepsilon < 1$ and any Boolean (possibly partial) function $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$*

$$\deg^{\mathsf{cert}}(f) \leqslant O\Big(\widetilde{\mathrm{osdeg}}_\varepsilon(f)\Big).$$

Proof. Recall $\widetilde{\mathrm{osdeg}}_\varepsilon(f) = \max\Big(\widetilde{\mathrm{osdeg}}^0_\varepsilon(f), \widetilde{\mathrm{osdeg}}^1_\varepsilon(f)\Big)$. Let P^0 and P^1 be the corresponding bounded polynomials that approximate f_z^{cert} with one-sided error ε, i.e. for all $x \in f^{-1}(0)$ they satisfy $P^0(x) = 0$ and $\big|P^1(x)\big| \leqslant \varepsilon$, and for all $y \in f^{-1}(1)$ they satisfy $\big|P^0(y) - 1\big| \leqslant \varepsilon$, and $P^1(y) = 1$.

Let $z \in \mathcal{D}$ and $b := 1 - f(z)$. Define polynomial P_z as

$$P_z(x) := \frac{P^b(x) - b}{P^b(z) - b}.$$

Then P_z is equal to f_z^{cert} on its domain, and is bounded by $\frac{1}{1-\varepsilon}$ since P^b is bounded by 1 and the denominator satisfies $1 - \varepsilon \leqslant \big|P^b(z) - b\big|$. Thus,

$$\begin{aligned}
\widetilde{\mathrm{osdeg}}_\varepsilon^{\ \mathsf{cert}}(f) &= \max_{z \in \mathcal{D}} \widetilde{\mathrm{osdeg}}_\varepsilon\big(f_z^{\mathsf{cert}}\big) \\
&= \max_{z \in \mathcal{D}} \deg(P_z) \\
&\geqslant \max_{z \in \mathcal{D}} \Delta_{0,0,\frac{1}{1-\varepsilon}}\big(f_z^{\mathsf{cert}}\big) \\
&\geqslant \Omega\left(\max_{z \in \mathcal{D}} \deg\big(f_z^{\mathsf{cert}}\big)\right) \\
&\geqslant \Omega\big(\deg^{\mathsf{cert}}(f)\big)
\end{aligned}$$

where the second inequality follows from Lemma 60. □

We now state and prove the collapse of exact and one-sided-error approximate degree certification complexities. This result can be viewed as the degree analogue of the collapse of $\mathsf{D}^{\mathsf{cert}}$ and $\mathsf{R}_0^{\mathsf{cert}}$, as well as $\mathsf{Q}_E^{\mathsf{cert}}$ with $\mathsf{Q}_0^{\mathsf{cert}}$.

Theorem 9 (certification equivalence between deg and $\widetilde{\mathrm{osdeg}}$)**.** *For any $0 < \varepsilon < 1$, up to $O(1)$ multiplicative factors, for any Boolean (possibly partial) function f*

$$\deg^{\mathsf{cert}}(f) = \widetilde{\mathrm{osdeg}}_{\varepsilon}^{\mathsf{cert}}(f) \leqslant \mathsf{Q}_0^{\mathsf{cert}}(f).$$

Proof. Apply item (iv) from Theorem 13 to $\deg \geqslant \widetilde{\mathrm{osdeg}}_{\varepsilon} \geqslant \Omega\big(\deg^{\mathsf{cert}}\big)$ where the last inequality follows from Lemma 48. The lower bound on $\mathsf{Q}_0^{\mathsf{cert}}$ is simply Corollary 47. □

Thus, both the exact/zero-error quantum query complexity collapses and the exact/one-sided-error degree collapse are individually sufficient to prove that the degree certification measure is a novel lower bound on Q_0.

Note 49. *Note that* OR *provides a separation showing that* $\deg^{\mathsf{cert}} \neq \widetilde{\deg}^{\mathsf{cert}}$.

Our final result in this section is that rational degree is a lower bound on one-sided-error approximate degree certification complexity. First, we prove the following lemma.

Lemma 50. *For any Boolean (possibly partial) function $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$,*

$$\mathrm{rdeg}^{\mathsf{cert}}(f) = \mathrm{rdeg}(f).$$

Proof. We use the characterization $\mathrm{rdeg}(f) = \max\{\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f)\}$ [KKW+26, Fact 3]. For $z \in \mathcal{D}$ let P_z be a polynomial such that $\deg(P_z) = \mathrm{ndeg}(f_z^{\mathsf{cert}})$ and $P_z(z) \neq 0$ and for any $y \in \mathcal{D}$ such that $f(y) \neq f(z)$ it satisfies $P_z(y) = 0$.

Let $b \in \{0,1\}$ and $z \in f^{-1}(b)$. Enumerate $f^{-1}(b) =: \{z_1, \ldots, z_k\}$ where $z_1 = z$. Let us prove by recurrence on $j \in [k]$ the property (R_j) defined as: There exists real numbers $(\alpha_i)_{i\in[j]}$ such that polynomial $P_j := \sum_{i\in[j]} \alpha_i \cdot P_{z_i}$ is non zero on inputs $\{z_1, \ldots, z_j\}$. For the base case (R_1), let $\alpha_1 := 1$.

Suppose (R_j), which gives real numbers $(\alpha_i)_{i\in[j]}$. Let A be a set of $k+1$ distinct non-zero real numbers. Since $P_{z_{j+1}}(z_{j+1}) = 1 \neq 0$ and P_j is non zero on inputs $\{z_1, \ldots, z_j\}$, then there exists some $\alpha_{j+1} \in A$ such that $P_j + \alpha_{j+1} \cdot P_{z_{j+1}} = P_{j+1}$ is non-zero on $\{z_1, \ldots, z_{j+1}\}$, hence proving (R_{j+1}).

Thus (R_k) is proved, giving $P^b := P_k$ which is a b-nondeterministic polynomial for f, i.e. for all $x \in f^{-1}(b)$ it satisfies $P^b(x) \neq 0$ and for all $x \in f^{-1}(1-b)$ it satisfies $P^b(x) = 0$.

Thus, having done this for each value of b, one gets

$$\begin{aligned}
\mathrm{rdeg}(f) &\leqslant \max_{b\in\{0,1\}} \deg\Big(P^b\Big) \\
&\leqslant \max_{b\in\{0,1\}} \max_{z\in f^{-1}(b)} \deg(P_z) \\
&\leqslant \max_{z\in\mathcal{D}} \mathrm{rdeg}\big(f_z^{\mathsf{cert}}\big) \\
&= \mathrm{rdeg}^{\mathsf{cert}}(f) \\
&= \max_{z\in\mathcal{D}} \mathrm{rdeg}\big(f_z^{\mathsf{cert}}\big) \\
&= \max\left\{ \max_{z\in f^{-1}(0)} \max\big\{\mathrm{ndeg}\big(f_z^{\mathsf{cert}}\big), \mathrm{ndeg}\big(\neg f_z^{\mathsf{cert}}\big)\big\}, \max_{z\in f^{-1}(1)} \max\big\{\mathrm{ndeg}\big(f_z^{\mathsf{cert}}\big), \mathrm{ndeg}\big(\neg f_z^{\mathsf{cert}}\big)\big\} \right\} \\
&\leqslant \max\left\{ \max_{z\in f^{-1}(0)} \max\{\mathrm{ndeg}(\neg f), \mathrm{ndeg}(f)\}, \max_{z\in f^{-1}(1)} \max\{\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f)\} \right\} \\
&= \max\{\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f)\} \\
&= \mathrm{rdeg}(f)
\end{aligned}$$

Hence $\mathrm{rdeg}(f) = \mathrm{rdeg}^{\mathsf{cert}}(f)$. □

Corollary 51. *For any $0 < \varepsilon < 1$ and any Boolean (possibly partial) function f*

$$\mathrm{rdeg}(f) \leqslant \widetilde{\mathrm{osdeg}}_{\varepsilon}^{\mathsf{cert}}(f).$$

Proof. One gets $\mathrm{rdeg}^{\mathsf{cert}} \leqslant \widetilde{\mathrm{osdeg}}_{\varepsilon}^{\mathsf{cert}}$ by applying item (i) from Theorem 13 to

$$\mathrm{rdeg}(f) = \max\{\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f)\} \leqslant \max\left\{\widetilde{\mathrm{osdeg}}_{\varepsilon}^{1}(f), \widetilde{\mathrm{osdeg}}_{\varepsilon}^{0}(f)\right\} = \widetilde{\mathrm{osdeg}}_{\varepsilon}(f)$$

where the first equality follows from [KKW+26, Fact 3]. Then conclude with Lemma 50. □

6.4 Separations

6.4.1 Separations between degree certification and degree measures

The Tribes function is a natural candidate to separate measures from their certification measure, since $\mathsf{Tribes}_x^{\mathsf{cert}}$ reduces to solving an OR function on a block (for 0-instances) or on one variable per block (for 1-instances). This holds for any measure that is stable. For degree and approximate degree we get the following separations.

Proposition 52 (quadratic separation between deg and $\mathrm{deg}^{\mathsf{cert}}$ and between $\widetilde{\mathrm{deg}}$ and $\widetilde{\mathrm{deg}}^{\mathsf{cert}}$ by a total function)**.**

1. $\mathrm{deg}\left(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}\right) = n$ *and* $\mathrm{deg}^{\mathsf{cert}}\left(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}\right) = \mathrm{deg}\left(\mathsf{OR}_{\sqrt{n}}\right) = \sqrt{n}$.
2. $\widetilde{\mathrm{deg}}\left(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}\right) = \sqrt{n}$ *and* $\widetilde{\mathrm{deg}}^{\mathsf{cert}}\left(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}\right) = \widetilde{\mathrm{deg}}\left(\mathsf{OR}_{\sqrt{n}}\right) = n^{\frac{1}{4}}$.

6.4.2 Separation between $\mathrm{deg}^{\mathsf{cert}}$ and rdeg

The proofs in this section were obtained using significant assistance from GPT-5.6 Sol.

Finally, we show that exact degree certification complexity is asymptotically different from rational degree. This is exhibited by the following family of functions. Define

$$f_m := \mathsf{AND}_m \circ (\neg\mathsf{Exact}_{1,m})$$

with variables $x_{i,1}, \ldots, x_{i,m}$ in the i-th block. Here, $\mathsf{Exact}_{1,m}(z_1, \ldots, z_m) = 1$ iff $|z| = 1$, where $|z|$ is the Hamming weight of z.

Theorem 10. *There exists a total function f_m on m^2 bits such that*

1. $\mathrm{rdeg}(f_m) = m$
2. $\mathrm{deg}^{\mathsf{cert}}(f_m) \geqslant \widetilde{\Omega}\left(m^{3/2}\right)$

Proof. First we deal with the rational degree and then proceed with the degree certification lower bound.

Rational degree. We prove that $\mathrm{rdeg}(f_m) = m$ via the non-deterministic degree characterization $\mathrm{rdeg}(f_m) = \max\{\mathrm{ndeg}(f_m), \mathrm{ndeg}(\neg f_m)\}$ [KKW+26, Fact 3]. For $\mathrm{ndeg}(f_m)$, we have a non-deterministic polynomial $\prod_{i=1}^{m}(1 - |x_i|)$. For $\mathrm{ndeg}(\neg f_m)$, first define $Q(w) := w\prod_{i=2}^{m}(w - i)$. Then the polynomial $\sum_{i=1}^{m} Q(|x_i|)$ is a non-deterministic polynomial for $\neg f_m$. The degree of each polynomial is at most m, so $\mathrm{rdeg}(f) \leqslant m$.

For the other direction, fix all the variables except one in each block to 0. This restricted function is then $\neg\mathsf{OR}_m$. Since $\mathrm{rdeg}(f) = \max\{\mathrm{ndeg}(f), \mathrm{ndeg}(\neg f)\}$ [KKW+26, Fact 3], and the non-deterministic degree is non-increasing under restrictions, and $\mathrm{rdeg}(\mathsf{OR}_m) = m$ (see e.g. [dW03, Section 2.1]), then we have $\mathrm{rdeg}(f) \geqslant m$.

Degree lower bound. For the $\deg^{\mathsf{cert}}$ lower bound, we use the notion of selective families [CMS01]. An (n,k)-selective family of sets is a collection of subsets $S_1,\dots,S_\ell \subseteq [n]$ such that for any subset $T \subseteq [n]$ with $1 \leqslant |T| \leqslant k$, we have $|S_i \cap T| = 1$ for at least one $i \in [\ell]$. A s-light selective family is such that $|S_i| \leqslant s$ for all $i \in [\ell]$.

Lemma 53. *There exists an s-light (n,k)-selective family of sets with size $\ell \leqslant O\Big(\big(k+\frac{n}{s}\big)\cdot \log(n)^2\Big)$.*

Proof. In [Hra21], an s-light (n,ω)-selector is a collection of subsets $S_1,\dots,S_\ell \subseteq [n]$ such that for any subset $T \subseteq [n]$ with $\frac{\omega}{2} \leqslant |T| \leqslant \omega$, we have $|S_i \cap T| = 1$ for at least $\frac{\omega}{4}$ elements $i \in [\ell]$, and $|S_i| \leqslant s$ for all $i \in \ell$. This is stronger than selective families, but is sufficient for our needs. Note the difference here that $|T| \geqslant \frac{\omega}{2}$. Theorem 4 of the same work shows the existence of an s-light (n,ω)-selector of size $O((\omega + n/s)\log n)$. By taking the union of such selectors for $\omega = k, \frac{k}{2}, \frac{k}{4}, \dots, 2$, we obtain an s-light (n,k)-selective family of size $\ell \leqslant O\Big(\big(k+\frac{n}{s}\big)\log(n)^2\Big) \leqslant \widetilde{O}\big(k+\frac{n}{s}\big)$. □

Now take $s = m$, $n \leqslant O\Big(\frac{m^2}{\log(m)^2}\Big)$, $k \leqslant O\Big(\frac{m}{\log(m)^2}\Big)$. Then by Lemma 53, there exists an m-light $\Big(O\Big(\frac{m^2}{\log(m)^2}\Big), O\Big(\frac{m}{\log(m)^2}\Big)\Big)$-selective family of size $\ell \leqslant O\Big(m + \frac{m^2}{m}\Big) \leqslant O(m)$. By picking appropriate constants, we can assume that $\ell \leqslant m$.

Now define a partial function $g : \{0,1\}^n \to \{0,1\}$ on inputs $z_1,\dots,z_n$, which is 1 on the input $z = 0^n$ and 0 on the inputs with $|z| \leqslant k$. We have that $\deg(g) \geqslant \sqrt{nk}$ by Lemma 54 (below). Now we show that this function can be embedded in f_m.

For each $i \in [\ell]$, map the elements of S_i to $|S_i|$ variables in the i-th block x_i. Then for an input z, let $x(z)$ be defined as follows. Set all of the variables of $x(z)$ to which nothing has been mapped to 0. If $z_j = b$, then all of the variables of x to which z_j has been mapped are equal to b as well. By the selective family properties, if $|z| > 0$, there is at least one block in which there is a single 1. Hence, $f_m(x) = 0$. Finally, if $z = 0$, then $f_m(x) = 1$ because all variables are 0.

Now consider the polynomial representing the 0^{m^2}-certification function $f^{\mathsf{cert}}_{m,0^{m^2}}$. By replacing the mapped variables of x with the corresponding variables of z, and other variables to 0, we obtain a polynomial for g. Hence, $\deg(g) \leqslant \deg\Big(f^{\mathsf{cert}}_{m,0^{m^2}}\Big) \leqslant \deg^{\mathsf{cert}}(f_m)$, and therefore

$$\deg^{\mathsf{cert}}(f_m) \geqslant \Omega\left(\sqrt{\frac{m^3}{\log(m)^4}}\right) \geqslant \widetilde{\Omega}\Big(m^{3/2}\Big).$$ □

It remains to prove Lemma 54.

Lemma 54. *Let $P : \mathbb{R}^n \to \mathbb{R}$ be a polynomial satisfying*

$$\begin{aligned} P(0^n) &= 1 \\ P(z) &= 0 \qquad \text{if } 1 \leqslant |z| \leqslant k \\ 0 \leqslant P(z) &\leqslant 1 \qquad \text{for all inputs } z \in \{0,1\}^n. \end{aligned}$$

Then

$$\deg(P) = \Omega(\sqrt{nk}).$$

Proof. Symmetrizing P, we obtain a univariate polynomial Q with $\deg(Q) \leqslant \deg(P)$ such that

$$\begin{aligned} Q(0) &= 1 \\ Q(1) = \dots = Q(k) &= 0 \\ 0 \leqslant Q(j) &\leqslant 1 \qquad \text{for } j = 0,\dots,n. \end{aligned}$$

Let $d = \deg(Q)$. Since Q has k distinct roots, we have $d \geqslant k$.

Then we can factor this polynomial:

$$Q(x) = \prod_{i=1}^{k}\left(1 - \frac{x}{i}\right) R(x).$$

Then $R(0) = 1$ and $\deg(R) = d - k$.

Let A be a large integer constant to be defined later, and set $t = Ak$. If $t \geqslant n/2$, then $k = \Omega(n)$, and therefore $d \geqslant k = \Omega(\sqrt{nk})$. Thus, we may assume that $t < n/2$.

For every integer $j \geqslant t$,

$$\left|\prod_{i=1}^{k}\left(1 - \frac{j}{i}\right)\right| = \prod_{i=1}^{k}\frac{j-i}{i}.$$

Since $j \geqslant Ak$, for every $1 \leqslant i \leqslant k$ we have

$$\frac{j-i}{i} \geqslant \frac{Ak-k}{k} = A - 1.$$

Therefore

$$\left|\prod_{i=1}^{k}\left(1 - \frac{j}{i}\right)\right| \geqslant (A-1)^k.$$

Since $0 \leqslant Q(j) \leqslant 1$, it follows that for$j = t, \ldots, n$ we have $|R(j)| \leqslant (A-1)^{-k}$.

Define $S(x) = 1 - R(x)^2$ and $\varepsilon = (A-1)^{-2k}$. Then $S(0) = 0$ and for $j = t, \ldots, n$ we have

$$1 - \varepsilon \leqslant S(j) \leqslant 1.$$

Now let $D := \deg(S) = 2(d-k)$.

We now apply Theorem 17 of [BCdW+99]: there exist absolute constants $a, b > 0$ such that, whenever $D \leq n - t$,

$$\varepsilon \geq \frac{1}{a}\exp\left(-\frac{bD^2}{n-t} - \frac{4D\sqrt{tn}}{n-t}\right).$$

If $D > n - t$, then, since $t < n/2$,

$$d = k + \frac{D}{2} \geq \frac{D}{2} > \frac{n-t}{2} > \frac{n}{4}.$$

Since $k \leq n$, this implies $d = \Omega(n) = \Omega(\sqrt{nk})$, and we are done.

It remains to consider the case $D \leq n - t$. Substituting $t = Ak$ and $\varepsilon = (A-1)^{-2k}$ into the above inequality and taking logarithms gives

$$2k\log(A-1) \leqslant \log a + \frac{bD^2}{n-t} + \frac{4D\sqrt{Akn}}{n-t}.$$

Since $t < n/2$, we have $n - t \geqslant n/2$, and therefore

$$2k\log(A-1) \leqslant \log a + \frac{2bD^2}{n} + 8\sqrt{A}\,D\sqrt{\frac{k}{n}}.$$

Choosing A to be a sufficiently large, we obtain for some absolute constant $C > 0$,

$$k \leqslant C \cdot \left(\frac{D^2}{n} + D\sqrt{\frac{k}{n}}\right).$$

Now let $x := \frac{D}{\sqrt{nk}}$. Dividing the preceding inequality by k and replacing $D = x\sqrt{nk}$ gives

$$1 \leqslant C \cdot \big(x^2 + x\big).$$

Hence $x = \Omega(1)$, and therefore $D = \Omega(\sqrt{nk})$. Since $D = 2(d-k) \leqslant 2d$, we conclude that $d = \deg(Q) = \Omega(\sqrt{nk})$. Finally, since $\deg(Q) \leqslant \deg(P)$, we have

$$\deg(P) = \Omega\Big(\sqrt{nk}\Big).$$ □

6.5 Tight lower bound on Q_0

Given that $\deg^{\mathsf{cert}}$ is a lower bound on Q_0 (Theorem 8, Theorem 9 and item (ii) from Theorem 13), as an immediate corollary of Theorem 10 we obtain that

$$\mathsf{Q}_0(f_m) = \widetilde{\Omega}\Big(n^{3/2}\Big).$$

This lower bound is tight for this function.

Lemma 55.

1. $\mathsf{Q}_0(f_m) = O\big(m^{3/2}\big)$.
2. $\mathsf{Q}(f_m) = O(m)$.

Proof. For each $b \in \{0,1\}$, we show an algorithm that outputs b on b-inputs with constant probability, never outputs b on any $(1-b)$-input, and uses $O\big(m^{3/2}\big)$ queries. By running the two algorithms in alternation repeatedly, we obtain a zero-error quantum algorithm for f_m.

Positive inputs. First we show the case for the 1-inputs. For an input x to be positive, each of the $\mathsf{Exact}_{1,m}$ functions have to evaluate to 0. We build a one-sided procedure with $O\big(m^{3/2}\big)$ expected number of queries for the inputs of $\mathsf{Exact}_{1,m}$. By Markov's inequality, we can stop the algorithm after $O\big(m^{3/2}\big)$ queries to get a bounded-error one-sided algorithm.

Let $z_1, \ldots, z_m$ be the input to an instance of $\mathsf{Exact}_{1,m}$. For z to be a 0-input, we need to have either $|z| = 0$ or $|z| \geqslant 2$. First we run the exact Grover's search with a promise that there is a unique marked element [Høy00]. If that returns 0, then we know with certainty that $|z| \neq 1$, so in that case we return the correct answer. If we get 1, then $|z| \geqslant 1$. To determine whether $|z| \geqslant 2$, we search for two distinct positions i, j such that $z_i = z_j = 1$ using two applications of Grover's search. If this doesn't find the two ones, we repeat. If we find the two ones, we query the two positions to certify that $|z| \geqslant 2$ with certainty.

If $|z| \geqslant 2$, this procedure evaluates $\mathsf{Exact}_{1,m}(z)$ to 0 in $O(\sqrt{m})$ expected number of queries. If $|z| = 1$, we never output 0 as the certification of the two 1s will be unsuccessful. If $|z| = 0$, we evaluate $\mathsf{Exact}_{1,m}(z)$ correctly already after the exact Grover's search. By running this procedure for all m input blocks of f_m, we get the required algorithm.

Negative inputs. For an input x to be a 0-input, there must be at least one $\mathsf{Exact}_{1,m}$ that evaluates to 1. To determine that for a single copy of $\mathsf{Exact}_{1,m}$, with input $z_1, \ldots, z_m$, we can first run Grover's search to find a single 1, and then run another Grover's search to find whether there are any more 1s. If $|z| = 1$, this gives the correct answer to this $\mathsf{Exact}_{1,m}$ with constant probability.

To determine whether any copy of $\mathsf{Exact}_{1,m}$ evaluates to 1, we run another Grover's search with bounded-error inputs [HMdW03] over the blocks. That in total requires $O(\sqrt{m} \cdot \sqrt{m}) = O(m)$ queries. If the input x is a 0-input, this procedure will find the block i where $\mathsf{Exact}_{1,m}$ evaluates to 1 with constant success probability. To certify this, we then can classically query all variables in the i-th block to check whether there is a single 1. Thus, with $O(m)$ queries, we will output 0 on 0-inputs with constant probability, and never output 0 on 1-inputs.

Finally, this part immediately implies $\mathsf{Q}(f_m) = O(m)$. □

As immediate corollaries, we get that the same function separates QC from $\mathsf{Q}_0^{\mathsf{cert}}$, $\widetilde{\deg}$ from $\widetilde{\mathrm{osdeg}}$, and $\widetilde{\deg}^{\mathsf{cert}}$ from $\widetilde{\mathrm{osdeg}}^{\mathsf{cert}}$.

7 Conclusion and further work

Systematically studying certification for various measures has allowed us to identify new bounds and to uncover new relationships between these and previously studied bounds.

There are many avenues to continue exploring. We provided one separation, between degree certification complexity and rational degree. We would also like to see other separations, or collapses.

Many polynomial relations between known bounds are not known to be tight. Can using certification measures help provide tighter bounds or bigger separations?

Finally, many relations between measures behave differently for total and partial functions. They can hold for total functions, and be constant for some partial functions. What can be said about these relations for the class of certifying functions? We hope that studying this class of partial functions will help us to gain a better understanding of why this gap between total and partial functions can occur.

AI Disclosure

We used GPT-5.6 Terra, GPT-5.6 Sol and Claude Opus 5 to assist with developing the proofs of Theorem 10, Lemma 53, Lemma 54 and Lemma 55 in Section 6.4.2, as well as Lemma 60, Lemma 61 and Lemma 62 in Section C. The authors verified the correctness and originality of all content including references.

Acknowledgments

E.L. has received support under the program "Investissement d'Avenir" launched by the French Government and implemented by ANR, with the reference "ANR-22-CMAS-0001, QuanTEdu-France". C.K. and E.L. are supported by the French PEPR integrated project EPiQ (ANR-22-PETQ-0007) and partially supported by the ANR Grant FLITTLA (ANR-21-CE48-0023). J.V. is supported by the 1.1.1.9 Research application No 1.1.1.9/LZP/2/25/206 of the Activity "Post-doctoral Research" "Practical applications and limitations of quantum search".

References

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

[AA15] Scott Aaronson and Andris Ambainis. "Forrelation: A Problem that Optimally Separates Quantum from Classical Computing". In: *Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing*. STOC '15. Portland, Oregon, USA: Association for Computing Machinery, 2015, 307–316. ISBN: 978-1-45033-536-2. DOI: 10.1145/2746539.2746547. arXiv: 1411.5729 [quant-ph].

[AAI+16] Scott Aaronson, Andris Ambainis, Jānis Iraids, Martins Kokainis, and Juris Smotrovs. "Polynomials, quantum query complexity, and Grothendieck's inequality". In: *Proceedings of the 31st Conference on Computational Complexity*. Ed. by Ran Raz. Vol. 50. CCC '16. Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2016, 25:1–25:19. ISBN: 978-3-95977-008-8. DOI: 10.4230/LIPIcs.CCC.2016.25.

[ABK+21] Scott Aaronson, Shalev Ben-David, Robin Kothari, Shravas Rao, and Avishay Tal. "Degree vs. approximate degree and Quantum implications of Huang's sensitivity theorem". In: *STOC*. 2021, pp. 1330–1342. DOI: 10.1145/3406325.3451047.

[ABB+17] Andris Ambainis, Kaspars Balodis, Aleksandrs Belovs, Troy Lee, Miklos Santha, and Juris Smotrovs. "Separations in Query Complexity Based on Pointer Functions". In: *Journal of the ACM* 64.5 (2017), 32:1–32:24. DOI: 10.1145/3106234.

[AKP+21] Andris Ambainis, Martins Kokainis, Krišjānis Prūsis, Jevgēnijs Vihrovs, and Aleksejs Zajakins. "All Classical Adversary Methods Are Equivalent for Total Functions". In: *ACM Trans. Comput. Theory* 13.1 (Jan. 2021). ISSN: 1942-3454. DOI: 10.1145/3442357. URL: https://doi.org/10.1145/3442357.

[ABK21] Anurag Anshu, Shalev Ben-David, and Srijita Kundu. "On Query-To-Communication Lifting for Adversary Bounds". In: *36th Computational Complexity Conference (CCC 2021)*. Ed. by Valentine Kabanets. Vol. 200. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021, 30:1–30:39. ISBN: 978-3-95977-193-1. DOI: 10.4230/LIPIcs.CCC.2021.30. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.CCC.2021.30.

[ABP19] Srinivasan Arunachalam, Jop Briët, and Carlos Palazuelos. "Quantum Query Algorithms Are Completely Bounded Forms". In: *SIAM Journal on Computing* 48.3 (2019), pp. 903–925. DOI: 10.1137/18M117563X.

[BBC+01] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. "Quantum lower bounds by polynomials". In: *J. ACM* 48.4 (July 2001), 778–797. ISSN: 0004-5411. DOI: 10.1145/502090.502097. URL: https://doi.org/10.1145/502090.502097.

[BK19] Shalev Ben-David and Robin Kothari. "Quantum Distinguishing Complexity, Zero-Error Algorithms, and Statistical Zero Knowledge". In: *14th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2019)*. Ed. by Wim van Dam and Laura Mančinska. Vol. 135. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2019, 2:1–2:23. ISBN: 978-3-95977-112-2. DOI: 10.4230/LIPIcs.TQC.2019.2. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.TQC.2019.2.

[Ber12] Sergei Natanovich Bernstein. "Démonstration du théoréme de Weierstrass fondée sur le calcul des probabilités". In: *Communications of the Kharkov Mathematical Society* 2.13 (1912), p. 1.

[BHM+02] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. "Quantum amplitude amplification and estimation". eng. In: *Quantum Computation and Information*. Vol. 305. Contemporary Mathematics. Providence, Rhode Island: American Mathematical Society, 2002, pp. 53–74. ISBN: 978-0-82182-140-4.

[BCdW+99] Harry Buhrman, Richard Cleve, Ronald de Wolf, and Christof Zalka. "Bounds for small-error and zero-error quantum algorithms". In: *40th Annual Symposium on Foundations of Computer Science*. 1999, pp. 358–368. DOI: 10.1109/SFFCS.1999.814607. arXiv: cs/9904019 [cs.CC].

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

[Cad20] Chris Cade. "Postselection and Rational Functions in Quantum Complexity Theory". PhD thesis. University of Bristol, 2020.

[CGL+23] Sourav Chakraborty, Anna Gál, Sophie Laplante, Rajat Mittal, and Anupa Sunny. "Certificate Games". In: *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*. Ed. by Yael Tauman Kalai. Vol. 251. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023, 32:1–32:24. ISBN: 978-3-95977-263-1. DOI: 10.4230/LIPIcs.ITCS.2023.32. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2023.32.

[CMS01] Andrea E. F. Clementi, Angelo Monti, and Riccardo Silvestri. "Selective families, superimposed codes, and broadcasting on unknown radio networks". In: *Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms*. Society for Industrial and Applied Mathematics, 2001, 709–718. ISBN: 0898714907. DOI: 10.5555/365411.365756.

[CMP24] Arjan Cornelissen, Nikhil S. Mande, and Subhasree Patro. "Quantum Sabotage Complexity". In: *44th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2024)*. Ed. by Siddharth Barman and Sławomir Lasota. Vol. 323. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024, 19:1–19:20. ISBN: 978-3-95977-355-3. DOI: 10.4230/LIPIcs.FSTTCS.2024.19. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.FSTTCS.2024.19.

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

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

[Høy00] Peter Høyer. "Arbitrary phases in quantum amplitude amplification". In: *Phys. Rev. A* 62 (5 2000), p. 052304. DOI: 10.1103/PhysRevA.62.052304.

[HMdW03] Peter Høyer, Michele Mosca, and Ronald de Wolf. "Quantum Search on Bounded-Error Inputs". In: *Automata, Languages and Programming* (Eindhoven, The Netherlands). ICALP 2003. Berlin, Heidelberg: Springer-Verlag, 2003, 291–299. ISBN: 3540404937. DOI: 10.1007/3-540-45061-0_25.

[Hra21] Ilya Hradovich. "Efficient communication algorithms in shared channels with adversary". PhD Thesis. Institute of Computer Science, Polish Academy of Sciences, 2021. URL: https://ipipan.waw.pl/pliki/doktoraty/Hradovich/Hradovich_Doktorat.pdf.

[Hua19] Hao Huang. "Induced subgraphs of hypercubes and a proof of the sensitivity conjecture". In: *Annals of Mathematics* 190.3 (2019), pp. 949–955. DOI: 10.4007/annals.2019.190.3.6.

[JK10] Rahul Jain and Hartmut Klauck. "The Partition Bound for Classical Communication Complexity and Query Complexity". In: *Proceedings of the 2010 IEEE 25th Annual Conference on Computational Complexity*. CCC '10. USA: IEEE Computer Society, 2010, 247–258. ISBN: 978-0-76954-060-3. DOI: 10.1109/CCC.2010.31. URL: https://doi.org/10.1109/CCC.2010.31.

[JKK+20] Rahul Jain, Hartmut Klauck, Srijita Kundu, Troy Lee, Miklos Santha, Swagato Sanyal, and Jevgēnijs Vihrovs. "Quadratically Tight Relations for Randomized Query Complexity". In: *Theory of Computing Systems* 64.1 (2020), pp. 101–119. ISSN: 1433-0490. DOI: 10.1007/s00224-019-09935-x. URL: https://doi.org/10.1007/s00224-019-09935-x.

[Jef26] Stacey Jeffery. *Week 5: Quantum Query Complexity*. https://homepages.cwi.nl/~jeffery/notes/week5.pdf. Lecture notes. Mar. 2026.

[KKW+26] Robin Kothari, Matt Kovacs-Deak, Daochen Wang, and Rain Zimin Yang. "Rational degree is polynomially related to degree". In: *FOCS*. to appear. 2026.

[Kou93] Elias Koutsoupias. "Improvements on Khrapchenko's theorem". In: *Theoretical Computer Science* 116.2 (1993), pp. 399–403.

[KT16] Raghav Kulkarni and Avishay Tal. "On Fractional Block Sensitivity". In: *Chicago Journal of Theoritical Computer Science* 2016 (2016). URL: http://cjtcs.cs.uchicago.edu/articles/2016/8/contents.html.

[Lor86] George G. Lorentz. *Bernstein Polynomials*. AMS Chelsea Publishing Series. Chelsea Publishing Company, 1986. ISBN: 978-0-82840-323-8.

[MdW15] Urmila Mahadev and Ronald de Wolf. "Rational approximations and quantum algorithms with postselection". In: *Quantum Information & Computation* 15.3–4 (Mar. 2015), 295–307. ISSN: 1533-7146. DOI: 10.26421/QIC15.3-4-5. URL: https://doi.org/10.26421/QIC15.3-4-5.

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

[Nis89] Noam Nisan. "CREW PRAMS and decision trees". In: *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*. STOC '89. Seattle, Washington, USA: Association for Computing Machinery, 1989, 327–335. ISBN: 0897913078. DOI: 10.1145/73007.73038. URL: https://doi.org/10.1145/73007.73038.

[NS94] Noam Nisan and Mario Szegedy. "On the Degree of Boolean Functions as Real Polynomials". In: *Computational Complexity* 4 (1994), pp. 301–313. DOI: 10.1007/BF01263419.

[Rub95] David Rubinstein. "Sensitivity vs. Block Sensitivity of Boolean Functions". In: *Combinatorica* 15.2 (1995), pp. 297–299. DOI: 10.1007/BF01200762.

[Tal13] Avishay Tal. "Properties and applications of Boolean function composition". In: *ITCS*. 2013, pp. 441–454. DOI: 10.1145/2422436.2422485.

A Nondeterminism vs certification

We now give the NP-like definition of certification complexity (Definition 57) – which is only defined on complexity measures that correspond to the query complexity of an algorithm, i.e. complexity measures coming from a model of computation (Definition 56). On such query complexity measures, this definition is equivalent to the general one above (Lemma 58).

Definition 56 (query model of computation)**.** *A* query model of computation M *specifies:*

- *what are the possible* algorithms *(their operations, possibly some constraints on their structure)*
- *what it means for an algorithm A to* compute *an output b when given query access to an input $x \in \{0,1\}^n$, i.e. $A^x = b$*
- *a corresponding* query complexity $\mathsf{M}(A,x)$ *of algorithm A on input x.*

Thus, for a Boolean (possibly partial) function $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$, it gives a query complexity measure *of the function:*

$$\mathsf{M}(f) := \max_{\substack{A \text{ algorithm in model } \mathsf{M}: \\ A \text{ computes } f}} \max_{x \in \mathcal{D}} \mathsf{M}(A,x)$$

where A computes *f iff for all $x \in \mathcal{D}$ computes $f(x)$ on input x.*

The the NP-like definition of certification complexity is one of the motivations of our systematic study of the general notion.

Definition 57 (query certification complexity $\mathsf{M}^{\mathsf{cert}}$ (witness version))**.** *Consider a query model of computation M. Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function. Let $\mathcal{C} = (w_x)_{x \in \mathcal{D}}$ be a family of* witnesses*. (Intuitively w_x will be chosen to be a proof of knowledge of the value of $f(x)$, i.e. the correct proof w_x should be accepted, and any wrong proof w_y such that $f(x) \neq f(y)$ should be rejected. Thus, $\mathcal{C}$ certifies f, and we are interested in the best achievable query complexity of such a certification procedure.)*

In the context of the query model of computation M, for any input $x \in \mathcal{D}$, we say that algorithm A certifies *f at x* w.r.t. *$\mathcal{C}$ with query complexity at most T if*

- *certification soundness: the computation of A with query access to input x and plain access (for free, and classical) to witness w_x accepts, i.e. $A^x(w_x) = 1$, and query complexity of $A(w_x)$ on x is at most T, i.e. $\mathsf{M}(A(w_x), x) \leqslant T$*
- *certification completeness: for any input $y \in \mathcal{D}$ such that $f(x) \neq f(y)$, the computation of A with query access to input x and plain access (for free, and classical) to witness w_y (a wrong witness) rejects, i.e. $A^x(w_y) = 0$, and query complexity of $A(w_y)$ on x is at most T, i.e. $\mathsf{M}(A(w_y), x) \leqslant T$.*

The query f-certification complexity of A w.r.t. $\mathcal{C}$ *is*

$$\mathsf{M}^{\mathsf{cert}}(A, \mathcal{C}, f) := \max_{x \in \mathcal{D}} \min_{\substack{T \in \mathbb{N}: \\ A \text{ certifies } f \text{ at } x \text{ w.r.t. } \mathcal{C} \\ \text{with query complexity at most } T}} T.$$

Thus, the query certification complexity of f *in model* M *is*

$$\mathsf{M}^{\mathsf{cert}}(f) := \min_{\mathcal{C}} \min_{\substack{A \text{ algorithm in model } \mathsf{M}: \\ \forall x \in \mathcal{D},\, A \text{ certifies } f \text{ at } x \text{ w.r.t. } \mathcal{C}}} \mathsf{M}^{\mathsf{cert}}(A, \mathcal{C}, f).$$

Saying that algorithm A certifies f at x w.r.t. $\mathcal{C}$ only specifies how A behaves with query access to an input in $\{z\} \cup \{y \in \mathcal{D} \,|\, f(x) \neq f(y)\}$ and nothing outside of this domain. Restrictions on the behavior of the algorithm outside of this domain fall within the specification of the query model of computation. More generally (Definition 2), one should be aware that the complexity measure M should be defined on partial functions for $\mathsf{M}^{\mathsf{cert}}$ to be defined (event on total functions).

Lemma 58 (equivalence of the definitions of query certification complexity)**.** *Definition 2 and Definition 57 define the same query certification complexity, i.e. for any query model of computation* M *and any Boolean (possibly partial) function* $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ *they define the same complexity measure* $\mathsf{M}^{\mathsf{cert}}(f)$*.*

Proof. We label by w objects and predicates defined by the witness version of query certification complexity (Definition 57) and by c those defined by the usual certification version (Definition 2). Consider a query model of computation M.

Fist we show $\mathsf{M}_c^{\mathsf{cert}}(f) \leqslant \mathsf{M}_w^{\mathsf{cert}}(f)$. Let the family of witnesses $\mathcal{C} = (w_z)_{z\in\mathcal{D}}$ and algorithm A be such that for all $x \in \mathcal{D}$ algorithm A certifies f at x w.r.t. $\mathcal{C}$, and $\mathsf{M}_w^{\mathsf{cert}}(f) = \mathsf{M}_w^{\mathsf{cert}}(A, \mathcal{C}, f)$ (i.e. they are optimal). So for any inputs $x, z \in \mathcal{D}$, if $z = x$ then $A^x(w_z) = 1$ with query complexity $\mathsf{M}(A(w_z), x) \leqslant \mathsf{M}_w^{\mathsf{cert}}(A, \mathcal{C}, f) = \mathsf{M}_w^{\mathsf{cert}}(f)$, and if $f(z) \neq f(x)$ then $A^x(w_z) = 0$ with query complexity $\mathsf{M}(A(w_z), x) \leqslant \mathsf{M}_w^{\mathsf{cert}}(A, \mathcal{C}, f) = \mathsf{M}_w^{\mathsf{cert}}(f)$. Let algorithm B be such that for any inputs $x, z \in \{0,1\}^n$, $B^x(z)$ first computes w_z (for free) and continues like $A^x(w_z)$. Then, for all inputs $z \in \mathcal{D}$ and $x \in \{z\} \cup \{y \in \mathcal{D} \mid f(y) \neq f(z)\}$, $B^x(z) = A^x(z) = f_z^{\mathsf{cert}}(x)$ with query complexity $\mathsf{M}(B(z), x) = \mathsf{M}(A(w_z), x) \leqslant \mathsf{M}_w^{\mathsf{cert}}(f)$. So

$$\mathsf{M}_c^{\mathsf{cert}}(f) = \max_{z\in\mathcal{D}} \mathsf{M}(f_z^{\mathsf{cert}}) \leqslant \max_{z\in\mathcal{D}} \max_{x\in\{z\}\cup\{y\in\mathcal{D}\,|\,f(y)\neq f(z)\}} \mathsf{M}(B(z), x) \leqslant \max_{z\in\mathcal{D}} \mathsf{M}_w^{\mathsf{cert}}(f) = \mathsf{M}_w^{\mathsf{cert}}(f).$$

Now we show the other way $\mathsf{M}_w^{\mathsf{cert}}(f) \leqslant \mathsf{M}_c^{\mathsf{cert}}(f)$. For all $z \in \mathcal{D}$, let $A(z)$ be an algorithm computing f_z^{cert} with optimal query complexity $\mathsf{M}(f_z^{\mathsf{cert}})$. So for all inputs $z \in \mathcal{D}$ and $x \in \{z\} \cup \{y \in \mathcal{D} \mid f(y) \neq f(z)\}$, $A^x(z) = f_z^{\mathsf{cert}}(x)$ with query complexity $\mathsf{M}(A(z), x) \leqslant \mathsf{M}(f_z^{\mathsf{cert}})$. Since $\mathcal{D}$ is finite, then $(A(z))_{z\in\mathcal{D}}$ is a uniform family of algorithms, so A itself is an algorithm. So A w-certifies f w.r.t. $\mathcal{C} := (z)_{z\in\mathcal{D}}$ with query complexity $\mathsf{M}_w^{\mathsf{cert}}(A, \mathcal{C}, f) \leqslant \max_{z\in\mathcal{D}} \mathsf{M}(f_z^{\mathsf{cert}}) = \mathsf{M}_c^{\mathsf{cert}}(f)$. Thus

$$\mathsf{M}_w^{\mathsf{cert}}(f) \leqslant \mathsf{M}_w^{\mathsf{cert}}(A, \mathcal{C}, f) \leqslant \mathsf{M}_c^{\mathsf{cert}}(f).$$

□

B Proof of Lemma 59

Lemma 59. *For any boolean (possibly partial) function* $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ *and any* $k > 0$*,*

$$(\mathsf{C}_0 \cdot \mathsf{C}_1)^{\mathsf{cert}}(f) = \mathsf{C}(f)$$

Proof. Suppose f is non-constant, as whenever f is constant $(\mathsf{C}_0 \cdot \mathsf{C}_1)^{\mathsf{cert}}(f) = 0 = \mathsf{C}(f)$ and the equality holds. Since for a 0-input y of f_z^{cert}, a single bit i where y_i differs from z_i is enough to certify y (and at least one bit is necessary to certify y as f is non-constant), then $\mathsf{C}_0(f_z^{\mathsf{cert}}) = 1$ holds for any input $z \in \mathcal{D}$. Hence

$$\begin{aligned}
(\mathsf{C}_0 \cdot \mathsf{C}_1)^{\mathsf{cert}}(f) &= \max_{z\in\mathcal{D}} \mathsf{C}_0\big(f_z^{\mathsf{cert}}\big) \cdot \mathsf{C}_1\big(f_z^{\mathsf{cert}}\big) \\
&= \max_{z\in\mathcal{D}} 1 \cdot \max\big(1, \mathsf{C}_1\big(f_z^{\mathsf{cert}}\big)\big) \\
&= \max_{z\in\mathcal{D}} \max\big(\mathsf{C}_0\big(f_z^{\mathsf{cert}}\big), \mathsf{C}_1\big(f_z^{\mathsf{cert}}\big)\big) \\
&= \mathsf{C}^{\mathsf{cert}}(f) \\
&= \mathsf{C}(f)
\end{aligned}$$

where the second equality follows from $\mathsf{C}_0(f_z^{\mathsf{cert}}) = 1$ and $\mathsf{C}_1(f_z^{\mathsf{cert}}) \geqslant 1$ as f is non constant, the third equality follows from $\mathsf{C}_0(f_z^{\mathsf{cert}}) = 1$, and the last equality follows from Remark 39. □

C Independence of bounded-polynomial degree measures from the boundedness parameter

The proofs in Appendix C were obtained using significant assistance from GPT-5.6 Terra and Claude Opus 5.

The following three lemmas allow us to show that up to constant factors in the degree, the bounding parameter for bounded polynomials can be taken to be 1. Rescaling the polynomials does not increase the error.

Lemma 60 (range reduction)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function and let P be a degree d exact polynomial for f, with values bounded to the range $[-C, C]$ for all points on the Boolean hypercube, where $C > 1$, i.e.*

$$\begin{aligned} P(x) &= f(x) && \forall x \in \mathcal{D}, \\ P(x) &\in [-C, C] && \forall x \in \{0,1\}^n, \\ \deg(P) &= d. \end{aligned}$$

Then there exists a polynomial Q that exactly computes f with range $[0,1]$ on the hypercube and degree $m_C \cdot d$, where m_C is a constant depending only on C, i.e.

$$\begin{aligned} Q(x) &= f(x) && \forall x \in \mathcal{D}, \\ Q(x) &\in [0,1] && \forall x \in \{0,1\}^n, \\ \deg(Q) &\leqslant m_C \cdot d. \end{aligned}$$

Proof. We will construct a univariate polynomial A with

$$A([-C, C]) \subseteq [0,1], \qquad A(0) = 0, \qquad A(1) = 1.$$

Choose $m \equiv 2 \pmod 4$ such that $\pi C \leqslant m \leqslant \pi C + 4$. Then

$$A(t) = \frac{1 + T_m\big(\sin\big(\frac{\pi}{m}\big)t\big)}{2}$$

where T_m is the degree-m Chebyshev polynomial of the first kind, i.e. defined by the property that $T_m(\cos\theta) = \cos(m\theta)$. Denote $u(t) := \sin\big(\frac{\pi}{m}\big)t$.

Since $\sin\big(\frac{\pi}{m}\big) \leqslant \frac{\pi}{m} \leqslant \frac{1}{C}$, we have for every $t \in [-C, C]$

$$|t| \sin\Big(\frac{\pi}{m}\Big) \leqslant C \sin\Big(\frac{\pi}{m}\Big) \leqslant 1,$$

so $u(t) \in [-1, 1]$. As $|T_m| \leqslant 1$ on $[-1, 1]$, it follows that $A(t) \in [0, 1]$ for all $t \in [-C, C]$.

Since $m \equiv 2 \pmod 4$, then $\frac{m}{2}$ is an odd integer and $T_m(u(0)) = T_m(0) = \cos\big(\frac{m\pi}{2}\big) = -1$, therefore

$$A(0) = \frac{1 + (-1)}{2} = 0.$$

On the other hand, $u(1) = \sin\big(\frac{\pi}{m}\big) = \cos\big(\frac{\pi}{2} - \frac{\pi}{m}\big) = \cos\left(\frac{\left(\frac{m}{2} - 1\right)\pi}{m}\right)$, and $\frac{m}{2} - 1$ is even, so $T_m(u(1)) = \cos\big(\big(\frac{m}{2} - 1\big)\pi\big) = 1$. Therefore

$$A(1) = \frac{1 + 1}{2} = 1.$$

Finally, define polynomial Q as $Q(x) := A(P(x))$. This satisfies all the conditions, and has degree $\deg(Q) \leqslant m \cdot d$, where m depends only on C. □

Lemma 61 (approximate range reduction)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function and let P be an ε-approximating polynomial for f with $0 < \varepsilon < \frac{1}{2}$ and degree d, with values bounded to the range $[-C, C]$ for all points on the Boolean hypercube:*

$$\begin{aligned} |P(x) - f(x)| &\leqslant \varepsilon && \forall x \in \mathcal{D}, \\ P(x) &\in [-C, C] && \forall x \in \{0,1\}^n, \\ \deg(P) &= d. \end{aligned}$$

Then there exists a polynomial Q that ε-approximates f with range $[0,1]$ on the hypercube and degree at most $m_{C,\varepsilon} \cdot d$, where $m_{C,\varepsilon}$ is a constant depending only on C and ε:

$$\begin{aligned} |Q(x) - f(x)| &\leqslant \varepsilon \qquad \forall x \in \mathcal{D}, \\ Q(x) &\in [0,1] \qquad \forall x \in \{0,1\}^n, \\ \deg(Q) &\leqslant m_{C,\varepsilon} \cdot d. \end{aligned}$$

Proof. Define the continuous function $g : [-C, C] \to [0,1]$:

$$g(t) = \begin{cases} 0 & \text{if } t \leqslant \varepsilon, \\ \dfrac{t-\varepsilon}{1-2\varepsilon} & \text{if } \varepsilon < t < 1-\varepsilon, \\ 1 & \text{if } t \geqslant 1-\varepsilon. \end{cases}$$

Then we can rescale $[-C, C]$ to $[0,1]$ and examine the m-th Bernstein approximation polynomial of this function:

$$A_m(t) := \sum_{k=0}^{m} g\left(-C + \frac{2Ck}{m}\right) \binom{m}{k} \left(\frac{t+C}{2C}\right)^k \left(1 - \frac{t+C}{2C}\right)^{m-k}.$$

Then, by the Bernstein approximation theorem [Ber12], there exists some $m_{C,\varepsilon}$ such that $\left|A_{m_{C,\varepsilon}}(t) - g(t)\right| \leqslant \varepsilon$ on $t \in [-C, C]$.

Furthermore, by the properties of Bernstein polynomials [Lor86], for $t \in [-C, C]$, the quantities multiplying the values of g are nonnegative and sum to 1. Since $g(t) \in [0,1]$, it follows that $A_{m_{C,\varepsilon}}(t) \in [0,1]$ for all $t \in [-C, C]$.

Now let $Q(x) = A_{m_{C,\varepsilon}}(P(x))$. Since $P(x) \in [-C, C]$ for every $x \in \{0,1\}^n$, we have $Q(x) \in [0,1]$ for all $x \in \{0,1\}^n$.

On the other hand, if $x \in \mathcal{D}$, we have that either $P(x) \in [-\varepsilon, \varepsilon]$ or $P(x) \in [1-\varepsilon, 1+\varepsilon]$ and hence $g(P(x)) = 0$ or $g(P(x)) = 1$ exactly. Therefore

$$|Q(x) - f(x)| = \left|A_{m_{C,\varepsilon}}(P(x)) - g(P(x))\right| \leqslant \varepsilon.$$

Finally, $\deg(Q) \leqslant \deg(A) \cdot \deg(P) \leqslant m_{C,\varepsilon} \cdot d$. □

Lemma 62 (one-sided range reduction)**.** *Let $f : \mathcal{D} \subseteq \{0,1\}^n \to \{0,1\}$ be a Boolean (possibly partial) function and let P be a one-sided-error ε-approximating polynomial for f with $0 < \varepsilon < \frac{1}{2}$ and degree d, with values bounded to the range $[-C, C]$ for all points on the Boolean hypercube.*

Then there exists a polynomial Q that is a one-sided ε-approximation of f with range $[0,1]$ on the hypercube and degree at most $m_{C,\varepsilon} \cdot d$, where $m_{C,\varepsilon}$ is a constant depending only on C and ε.

Proof. W.l.o.g. assume that $P(x) = 0$ on $f^{-1}(0)$ and $P(x) \in [1-\varepsilon, 1+\varepsilon]$ on $f^{-1}(1)$.

The proof extends the construction of Lemma 61, define the function $g(t)$ and polynomial $A_m(t)$ as in that proof. However, we will now pick $m_{C,\varepsilon'}$ so that $\left|A_{m_{C,\varepsilon'}}(t) - g(t)\right| \leqslant \varepsilon'$, for $\varepsilon' < \varepsilon$ to be chosen later.

Let $\delta := A_{m_{C,\varepsilon'}}(0)$, by construction $\delta \leqslant \varepsilon'$. Then define the polynomial

$$B(t) = \left(\frac{A_{m_{C,\varepsilon'}}(t) - \delta}{1-\delta}\right)^2.$$

For $t \in [-C, C]$ we have $\frac{A_{m_{C,\varepsilon'}}(t)-\delta}{1-\delta} \in \left[-\frac{\delta}{1-\delta}, 1\right]$, therefore $B(t) \in [0,1]$.

For $t = 0$ we have $B(t) = 0$.

Finally, for $t \in [1-\varepsilon, 1+\varepsilon]$ we have that $A_{m_{C,\varepsilon'}}(t) \in [1-\varepsilon', 1]$, therefore

$$B(t) \geqslant \left(\frac{1-\varepsilon'-\delta}{1-\delta}\right)^2 \geqslant (1-2\varepsilon')^2.$$

Then we can pick ε' so that this value is at least $1-\varepsilon$.

Finally, take $Q(x) = B(P(x))$, obtaining a polynomial with degree $2d \cdot m_{C,\varepsilon'}$. □

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il