Certificate Games

Sourav Chakraborty
Indian Statistical Institute, Kolkata, India

Anna Gál
University of Texas at Austin, TX, USA

Sophie Laplante
Université Paris Cité, IRIF, France

Rajat Mittal
IIT Kanpur, India

Anupa Sunny
Université Paris Cité, IRIF, France

Abstract

We introduce and study Certificate Game complexity, a measure of complexity based on the probability of winning a game where two players are given inputs with different function values and are asked to output some index i such that $x_i \neq y_i$, in a zero-communication setting.

We give upper and lower bounds for private coin, public coin, shared entanglement and non-signaling strategies, and give some separations. We show that complexity in the public coin model is upper bounded by Randomized query and Certificate complexity. On the other hand, it is lower bounded by fractional and randomized certificate complexity, making it a good candidate to prove strong lower bounds on randomized query complexity. Complexity in the private coin model is bounded from below by zero-error randomized query complexity. The quantum measure highlights an interesting and surprising difference between classical and quantum query models. Whereas the public coin certificate game complexity is bounded from above by randomized query complexity, the quantum certificate game complexity can be quadratically larger than quantum query complexity. We use non-signaling, a notion from quantum information, to give a lower bound of n on the quantum certificate game complexity of the OR function, whose quantum query complexity is $\Theta(\sqrt{n})$, then go on to show that this "non-signaling bottleneck" applies to all functions with high sensitivity, block sensitivity or fractional block sensitivity.

We also consider the single-bit version of certificate games, where the inputs of the two players are restricted to having Hamming distance 1. We prove that the single-bit version of certificate game complexity with shared randomness is equal to sensitivity up to constant factors, thus giving a new characterization of sensitivity. On the other hand, the single-bit version of certificate game complexity with private randomness is equal to λ^2, where λ is the spectral sensitivity.

2012 ACM Subject Classification Theory of computation → Computational complexity and cryptography; Theory of computation → Circuit complexity; Theory of computation → Quantum query complexity

Keywords and phrases block sensitivity, boolean function complexity, certificate complexity, query complexity, sensitivity, zero-communication two-player games

Digital Object Identifier 10.4230/LIPIcs.ITCS.2023.32

Related Version *Full Version*: https://eccc.weizmann.ac.il/report/2022/143/
Full Version: https://arxiv.org/abs/2211.03396

Funding AS has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement No 754362. Additional support comes from the French ANR projects ANR-18-CE47-0010 (QUDATA) and ANR-21-CE48-0023 (FLITTLA) and the QOPT project funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement no. 731473 and 101017733.

Acknowledgements We thank Jérémie Roland for helpful discussions, Chandrima Kayal for pointing out a function which separates C and Q, and the anonymous referees for helpful comments.

1 Introduction

There still remains much to be understood about the complexity of Boolean functions and the many complexity measures that are used to study various models of computation such as certificate complexity, degree, sensitivity, block sensitivity, their variants, to name a few. Some of the questions we ask about these measures are: How are these measures related, and what polynomial upper bounds can be given on these measures in terms of the smaller measures such as sensitivity? What separations can be shown between the measures? Do they have a natural computational interpretation? What properties do they have, for example, do they behave well under composition? How do they behave for symmetric functions? Since the sensitivity conjecture was resolved [23], one important new goal is to determine precisely how the larger measures, such as query complexity and certificate complexity, are bounded above by smaller measures such as sensitivity. The best known upper bound on deterministic query complexity is $\mathsf{D}(f) \leq O(\mathsf{s}(f)^6)$, [34, 31, 23] while the best separation is cubic [13]. For certificate complexity we know that $\mathsf{C}(f) \leq O(\mathsf{s}(f)^5)$, whereas the best known separation is cubic [9]. Many more of these upper bounds and separations are listed in the tables of known results in [42, 4].

With these questions in mind, we introduce a new complexity measure based on the Karchmer-Wigderson relation of a Boolean function. This relation was introduced by Karchmer and Wigderson [25] and it has been extensively studied in communication complexity. Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function. The relation $R_f \subseteq f^{-1}(0) \times f^{-1}(1) \times [n]$ is defined as $R_f = \{(x, y, i) : x_i \neq y_i\}$. (As a matter of convention, x denotes an input in $f^{-1}(0)$ and y denotes an input in $f^{-1}(1)$ unless otherwise stated.) Karchmer and Wigderson [25] showed that the communication complexity of R_f is equal to the circuit depth of f. We study the following 2-player *certificate game*, where the goal of the players is to solve the Karchmer-Wigderson relation in a zero-communication setting.

▶ **Definition 1** (Certificate game). *Let $f : \{0,1\}^n \to \{0,1\}$ be a (possibly partial) Boolean function. One player is given $x \in f^{-1}(0)$ and the other player is given $y \in f^{-1}(1)$. Their goal is to produce a common index i such that $x_i \neq y_i$, without any communication.*

We look at how well they can solve this task in several zero-communication settings. We consider four models: when they only have private coins, when they share a public random source, and when they share an entangled quantum state (also called quantum model) that does not depend upon their inputs. The fourth model allows any non-signaling strategy which we describe in Section 2.2. In all these models, we consider the probability of success that they can achieve, for the best strategy and worst case input pair. The multiplicative inverse of the winning probability is called the certificate game complexity of the function (CG for the private coin model, $\mathsf{CG}^{\mathrm{pub}}$ for the public coin model, CG^* for the shared entanglement model and $\mathsf{CG}^{\mathsf{ns}}$ for the non-signaling model).

To illustrate how to achieve such a task without communication, we consider the following simple strategy. Let f be a Boolean function whose 0-certificate complexity is c_0 and whose 1-certificate complexity is c_1. Then on input x such that $f(x) = 0$, Alice can output a random i in a minimal 0-certificate for x (similarly for Bob with a minimal 1-certificate for y). Then since the certificates intersect, the probability that they output the same index is at least $\frac{1}{c_0 \cdot c_1}$. This shows that $\mathsf{CG}(f) \leq \mathsf{C}^0(f) \cdot \mathsf{C}^1(f)$. This simple upper bound is tight

for many functions including OR and Parity, but there are other examples where $\mathsf{CG}(f)$ can be much smaller, and it is interesting to see what other upper and lower bounds can apply. We will also see that access to shared randomness can significantly reduce the complexity.

We show that the certificate game complexity measures in the four different models hold a pivotal position with respect to other measures, thus making them good candidates for proving strong lower and upper bounds on various measures. The operational interpretation in terms of winning probability of certificate games makes them convenient for proving upper bounds. Furthermore, the public coin and non-signaling versions are linear programs and therefore their dual formulation is convenient for proving lower bounds.

1.1 Motivation for certificate games

The two main ingredients in our certificate games are two-player zero-communication games, and the Karchmer-Wigderson relation. Two-player zero-communication games have been studied in many different contexts. They are called two-prover games in the context of parallel repetition theorems, central to the study of PCPs and the Unique Games Conjecture (we don't consider the case where there could be a quantum verifier, which has been studied in some papers). They also appear under the name of zero-communication protocols in the context of communication and information complexity. Finally, they are known as local or quantum games in the study of quantum nonlocality, an extensive field motivated by the study of quantum entanglement and the relative power of quantum over classical behaviors. Quantum behaviors are modeled by two parties making measurements on a shared bipartite quantum state, and in the classical setup, the two parties can share "hidden variables", or shared randomness. There has been extensive work, for instance, on simulating quantum behaviors with various resources, such as communication, post-selection, noise and more. There are also strong connections between finding separations between quantum and classical communication complexity, and between quantum and classical zero-communication games. A survey on quantum non-locality can be found in references [16, 35], and on the interactions between communication complexity and nonlocality in reference [17].

The Karchmer-Wigderson relation R_f appears in many contexts in the study of complexity measures, including the Adversary bound on quantum query complexity, and its variants [5, 38]. It is key in understanding how hard a function is and captures the intuition that if one is to distinguish the 0-instances from the 1-instances of a function, then some i in the relation has to play a key role in computing the function. Another measure where the Karchmer-Wigderson relation appears implicitly is Randomized certificate complexity (RC) defined by Aaronson [2]. It was further shown to be equivalent to fractional block sensitivity and fractional certificate complexity (FC) [39, 21]. The non-adaptive version can be viewed as a one-player game where the player is given an input x and should output an index i. The player wins against an input y (with $f(x) \neq f(y)$) if $x_i \neq y_i$.

1.2 Our results

We show that the certificate game complexity measures of a Boolean function f take pivotal roles in understanding the relationships between various other complexity measures like Randomized certificate complexity $\mathsf{RC}(f)$, Certificate complexity $\mathsf{C}(f)$, randomised query complexity $\mathsf{R}(f)$, zero-error randomized query complexity $\mathsf{R}_0(f)$ and other related measures. Our results also demonstrate the power of shared randomness over private randomness, even in a zero-communication setting. At the same time, our results also illustrate an interesting, and somewhat counter-intuitive, difference between the quantum world and the classical

world. Our main results for total functions are compiled in Figure 1. While most of our results also hold for partial functions, for simplicity we don't indicate that in the Figure. Instead we specify in each theorem whether our result holds for partial functions.

Shared entanglement can simulate shared randomness, and shared randomness gives more power to the players compared to private randomness so

$$\mathsf{CG}^*(f) \leq \mathsf{CG}^{\mathrm{pub}}(f) \leq \mathsf{CG}(f).$$

A natural question that arises is how separated are these measures. In other words, how much advantage does shared randomness give over private randomness and how much advantage does shared entanglement give over shared randomness? Because of the operational interpretation of certificate game complexity in terms of the winning probability of certificate games, proving upper bounds on certificate game complexity can be achieved by demonstrating a strategy for the game. We provide techniques to prove lower bounds.

Lower bounds on certificate games with shared entanglement. One surprising result of our work concerns the shared entanglement model. In order to prove lower bounds for this model, we introduce non-signaling certificate games. Non-signaling is a fundamental concept that comes from quantum non-locality; it states that when making a quantum measurement the outcome on one should not leak any information about the measurement made on the other side. This "non-signaling bottleneck" is shared by all of our certificate game complexity measures. Identifying it turned out to be the key insight which led to a very strong lower bound on all these measures, including the quantum model, with a single, simple proof, not involving any of the technical overhead inherent to the quantum setting. The simplicity of the proof comes from the fact that the non-signaling model has several equivalent formulations as linear programs, and the strength of the bounds comes from the fact that it captures precisely a fundamental computational bottleneck. It also neatly highlights one of the key differences between quantum and classical query models, since the quantum query model somehow averts this bottleneck.

Our main lower bound result is a simple and elegant proof (Theorem 23) that

$$\mathsf{CG}^{\mathsf{ns}} \geq \mathsf{FC}$$

which in turn lower bounds the other three variants of certificate game complexity. The idea is that when a strategy satisfies the non-signaling condition, the marginal distribution of one of the players' output does not depend on the other player's input. Therefore, playing according to the marginal distribution of one of the players is a successful strategy for the FC game. It follows from this lower bound that while the quantum query complexity of the OR_n function[1] is $\Theta(\sqrt{n})$, its quantum certificate game complexity is $\mathsf{CG}^*(\mathsf{OR}_n) = \Theta(n)$.

Upper bounds on certificate games with shared randomness. The fact that CG^* is lower bounded by FC gives us examples (like the OR_n function) where the quantum query complexity Q, can be quadratically smaller than CG^*. In other words, a quantum query algorithm that computes the OR_n function using $\sqrt{n}$ queries, cannot reveal to players of a certificate game an index where their inputs differ, with probability better than $1/n$, because of the non-signaling constraint on quantum games. This, somewhat surprisingly, contrasts

[1] OR_n is the OR of n variables. From Grover's algorithm [22, 15] we have $\mathsf{Q}(\mathsf{OR}_n) = \sqrt{n}$. On the other hand $\mathsf{FC}(\mathsf{OR}_n) = \Omega(\mathsf{s}(\mathsf{OR}_n)) = \Omega(n)$.

with the randomized setting where the players can run their randomized query algorithm on their respective inputs using the same random bits and pick a common random query in order to find an index where the inputs differ, with probability $\frac{1}{\mathsf{R}(f)}$, for any f. Thus, we prove (Theorem 19) that for any Boolean function f,

$$\mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{R}(f)).$$

Whether the zero-error randomized query complexity, $\mathsf{R}_0(f)$ is upper bounded by the square of $\mathsf{FC}(f)$ is a long standing open problem. A natural step towards solving the open problem is to use a measure just above FC and show that R_0 is upper bounded by the square of that measure. In [24] the authors introduced such a measure, called expectational certificate complexity, EC, and showed that $\mathsf{R}_0(f) \leq O(\mathsf{EC}(f)^2)$. Showing that $\mathsf{EC} \leq O(\mathsf{FC})$ would solve the long-standing open problem. They made significant progress towards this by showing that $\mathsf{EC}(f) \leq O(\mathsf{FC}(f) \cdot \sqrt{\mathsf{s}(f)})$. Thus one of the main questions that remained unanswered in [24] was: "Is $\mathsf{EC}(f) = O(\mathsf{FC}(f))$?" and if the answer is negative, how to prove it? We show that $\mathsf{CG}^{\mathrm{pub}}$ is bounded above by $\mathsf{EC}(f)$ up to constant factors (Theorem 18). Combining with our results,

$$\mathsf{FC}(f) \leq \mathsf{CG}^{\mathsf{ns}}(f) \leq \mathsf{CG}^{*}(f) \leq \mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{EC}(f)).$$

Hence, certificate games may give us a handle on how to resolve the FC versus EC question: either prove that these measures are all equivalent, or give a separation between any of them.

A first step towards proving a separation could be to show a separation between the shared randomness and shared entanglement models. For Boolean predicates, it is known that the gap between the quantum and randomized winning probabilities can be at most constant (by Grothendieck's theorem, see for example Proposition 4.5 in [35]). But for games with non-Boolean outcomes, as is the case with certificate games, this limitation does not apply, and such a separation, or an impossibility result, in the special case of certificate games, could be of independent interest.

For total Boolean functions our upper bound on $\mathsf{CG}^{\mathrm{pub}}$ by EC implies that $\mathsf{CG}^{\mathrm{pub}}$ is also upper bounded by certificate complexity C (up to constant factors), since $\mathsf{EC}(f) \leq \mathsf{C}(f)$ for total functions [24]. We also give a direct proof that $\mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{C}(f))$ for total functions (Theorem 17) as a "warmup" to the stronger upper bound by EC (see the full version).

Bounds on certificate games with private randomness. The private randomness model of certificate game complexity, CG, is upper bounded by the product of 0-certificate complexity, C^0, and 1-certificate complexity, C^1, and also by the square of EC (Theorem 22). On the other hand the argument of [24] to show $\mathsf{R}_0(f) \leq O(\mathsf{EC}(f)^2)$ extends to show that CG is lower bounded by R_0. Therefore, $\mathsf{R}_0(f) \leq O(\mathsf{CG}(f)) \leq O(\mathsf{C}^0(f)\mathsf{C}^1(f))$.

In fact, $\mathsf{CG}(f)$ can be larger than the arity of the function. This is because, we show (in Theorem 22) that $\mathsf{CG}(f)$ is lower bounded by the square of the Minimax formulation of the positive adversary bound, $\mathsf{MM}(f)$, which sits between $\mathsf{Q}(f)$ and the spectral sensitivity $\lambda(f)$.

Relationships between the various models of certificate games. Combining our results with the fact that $\mathsf{EC}(f) \leq O(\mathsf{FC}(f) \cdot \sqrt{\mathsf{s}(f)})$, [24], we have (in Corollary 26)

$$\mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{EC}(f)) \leq O(\mathsf{CG}^{\mathsf{ns}}(f)^{3/2}) \leq O(\mathsf{CG}^{*}(f)^{3/2}).$$

Furthermore, since $\mathsf{CG}(f) \leq O(\mathsf{EC}(f)^2)$ we have (in Corollary 27)

$$\mathsf{CG}(f) \leq O(\mathsf{CG}^{\mathsf{ns}}(f)^3).$$

The $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}} = \mathsf{OR}_{\sqrt{n}} \circ \mathsf{AND}_{\sqrt{n}}$ (Definition 15) function demonstrates a quadratic separation between $\mathsf{CG}^{\mathrm{pub}}$ and R and hence between $\mathsf{CG}^{\mathrm{pub}}$ and CG. Since $\mathsf{CG}^{\mathrm{pub}} \leq \mathsf{C}$ for total functions, we see that $\mathsf{CG}^{\mathrm{pub}}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = O(\sqrt{n})$, while $\mathsf{R}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Omega(n)$. The fact that public coins can be used cleverly to design the strategy for $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ is not obvious at first glance. In fact, the strategy for the $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ function helps us to see the how public coins can be used effectively (via a hashing framework) for any function. Furthermore, since the $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ function is a composition of the $\mathsf{AND}_{\sqrt{n}}$ and $\mathsf{OR}_{\sqrt{n}}$ function, we also notice that the measures $\mathsf{CG}^{\mathrm{pub}}$, CG^{*} and $\mathsf{CG}^{\mathsf{ns}}$ do not compose (Corollary 28), that is, there are Boolean functions f and g such that the measures for the function $(f \circ g)$ is not asymptotically the same as the product of the measures for f and for g.

Certificate game complexity for partial functions. While $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ demonstrates a quadratic gap between R and $\mathsf{CG}^{\mathrm{pub}}$, we know the largest gap between R and $\mathsf{CG}^{\mathrm{pub}}$ for total functions is at most cubic (since $\mathsf{D} \leq (\mathsf{bs})^3$ [11, 33]). But for partial functions the situation is different. Ben David and Blais [12] demonstrated a function, approximate index ApInd (Definition 30), for which there is exponential separation between R and FC [2]. We show that $\mathsf{CG}^{\mathrm{pub}}$ of ApInd is at most $O(\log(\mathsf{R}))$ (Theorem 31) and hence demonstrate an exponential separation between R and $\mathsf{CG}^{\mathrm{pub}}$ for partial Boolean functions.

Single-bit versions of certificate games. Our final set of results is in the context of single-bit versions of certificate games. Single-bit versions of certain complexity measures were used in early circuit complexity bounds [26, 28]. More recently Aaronson et al. [4] defined single-bit versions of several formulations of the adversary method, and showed that they are all equal to the spectral sensitivity λ. Informally, single-bit versions of these measures are obtained by considering the requirements only with respect to pairs x, y such that $f(x) = 0$ and $f(y) = 1$ and x and y differ only in a single bit.

We show that the single-bit version of private coin certificate game complexity is equal to λ^2 (Theorem 38). One of our main results is that the single-bit version of public coin certificate game complexity, $\mathsf{CG}^{\mathrm{pub}}_{[1]}(f)$ is asymptotically equal to sensitivity $\mathsf{s}(f)$ (Theorem 38). This gives a new and very different interpretation of sensitivity, which is one of the central complexity measures in this area. This interpretation of sensitivity in the context of certificate games may give us a handle on resolving the sensitivity-block sensitivity conjecture (which asks if block sensitivity $\mathsf{bs}(f)$ is $O(\mathsf{s}(f)^2)$, and remains open in this stronger form), by trying to construct a strategy for $\mathsf{CG}^{\mathrm{pub}}$ using a strategy for $\mathsf{CG}^{\mathrm{pub}}_{[1]}$.

A note on partial functions. Our notion of certificate games naturally extends to partial functions, and many of our results hold for partial as well as total functions. The formal definitions are given in the full version of this paper [18]. We indicate here which results extend to partial functions.

1.3 Overview of our techniques

The main contribution of this paper is to give lower and upper bounds on certificate game complexity in different models: private coin, public coin and shared entanglement. The bounds on private coin certificate game complexity are obtained by manipulating previously known results and use standard techniques.

[2] [12] introduced a measure called noisyR in an attempt to answer the question of whether R composes, that is, whether $\mathsf{R}(f \circ g) = \Theta(\mathsf{R}(f) \cdot \mathsf{R}(g))$. They studied noisyR for the approximate index function ApInd and showed an exponential separation between noisyR and R for this partial function.

The principal contribution, in terms of techniques, is in giving upper and lower bounds on certificate game complexity of public coin and shared entanglement model ($\mathsf{CG}^{\mathrm{pub}}$ and CG^*). These techniques can naturally be divided into two parts.

Upper bounds. We prove strong (and arguably surprising) upper bounds on $\mathsf{CG}^{\mathrm{pub}}$ by constructing strategies using shared randomness. The challenge for giving a certificate game strategy is to get the two players to coordinate their strategies so that the index they output is the *same*. In public coin setting, we can take advantage of using shared randomness. We show multiple examples where using shared randomness to choose hash functions or permutations turns out to be helpful. We express the ideas behind our public coin strategies in a general framework based on using hash functions. However, the strategies that fall within this framework still require a separate analysis, which in some cases can be technically quite involved.

Lower bounds. Lower bounds on $\mathsf{CG}^{\mathrm{pub}}$ can be obtained by taking the dual of its linear programming formulation. For the shared entanglement model, which is not linear, we turn to more general non-signaling games. The resulting non-signaling certificate game complexity, $\mathsf{CG}^{\mathrm{ns}}$, is a lower bound on CG^*. It can be expressed as a linear program and lower bounds on CG^* can be obtained by taking the dual of this linear program and constructing feasible solutions for it.

2 Certificate game complexity

In this section, we give the formal definitions of our Certificate Game complexity measures.

A two-player game G is given by a relation $R(x, y, a, b) \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B}$, where $x \in \mathcal{X}$ is the first player's input, $y \in \mathcal{Y}$ is the second player's input. The players output a pair of values, $(a, b) \in \mathcal{A} \times \mathcal{B}$, and they win if $R(x, y, a, b)$ holds. A *deterministic strategy* is a pair of functions $A : \mathcal{X} \to \mathcal{A}$ and $B : \mathcal{Y} \to \mathcal{B}$. A *randomized strategy with private randomness* is the product of two mixed individual strategies. A *randomized strategy with shared randomness* is a mixture of pairs of deterministic strategies. A *quantum* or *shared entanglement strategy* is given by a shared bipartite state that does not depend on the input, and a family of projective measurements for Alice, indexed by her input, similarly for Bob. (More general measurements could be considered, but projective measurements suffice [19].)

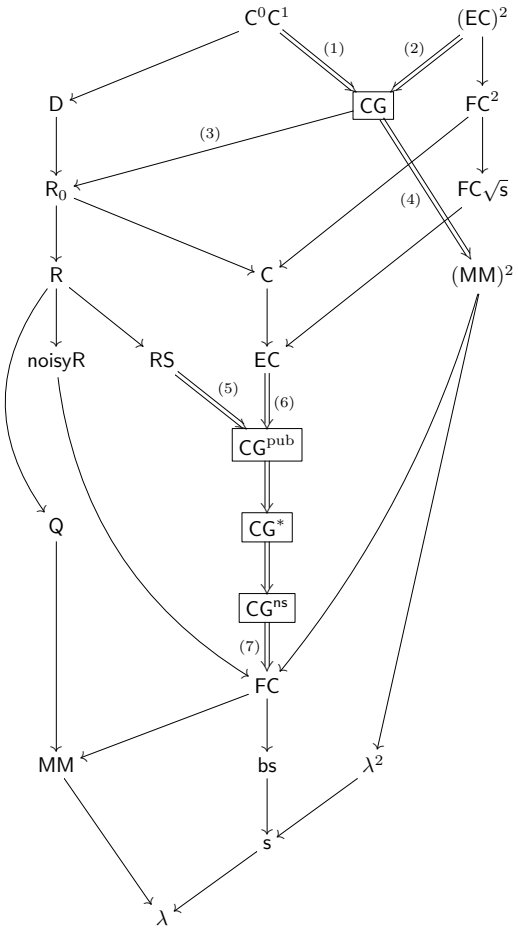
For any strategy, we will write $p(a, b|x, y)$ to mean the probability that the players output (a, b) when their inputs are x, y. The marginal distribution of Alice's output is $p(a|x, y) = \sum_b p(a, b|x, y)$, and similarly, $p(b|x, y) = \sum_a p(a, b|x, y)$ is Bob's marginal distribution.

Non-signaling is a notion that comes from quantum games, which says that if players are spatially separated, then they cannot convey information to each other instantaneously. All the types of strategies described above verify the non-signaling condition.

▶ **Definition 2** (Non-signaling strategy). *Let $p(a, b|x, y)$ be the probability that players, on input x, y output a, b. Then p is non-signaling if $p(a|x, y) = p(a|x, y')$ and $p(b|x, y) = p(b|x', y)$ for all inputs x, x', y, y' and all outcomes a, b.*

Since nonsignaling means that Alice's output does not depend on Bob's input, we can write $p(a|x)$ for Alice's marginal distribution, similarly, we will write $p(b|y)$ for Bob.

Surprisingly, non-signaling strategies are characterized by the *affine combinations* of local deterministic strategies that lie in the positive orthant. This has been known since the 1980s [20, 37, 27, 41]. A more recent proof is given in [36].



1. Theorem 22. Separation: GSS_1 (follows from the fact that $\mathsf{C}^1(\mathsf{GSS}_1) = \Theta(n)$ and $\mathsf{C}^0(\mathsf{GSS}_1) = \Theta(n^2)$). Tightness: $\oplus$.
2. Theorem 22, Separation: OR, Tightness: $\oplus$.
3. Implicit in[24] (Theorem 22). Separation: $\oplus$, Tightness: OR.
4. Theorem 22 Separation: Pointer function in [6] and the cheat sheet version of the $k-$Forrelation function [10, 3]. Tightness: OR.
5. Theorem 19 and Proposition 20. Separation: Tribes (Theorem 16 and $\mathsf{RS}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(n)$ because RS composes [14]). Tightness: $\oplus$.
6. Theorem 18. Separation: OPEN, Tightness: $\oplus$.
7. Theorem 23. Separation: OPEN, Tightness: $\oplus$.

Figure 1 Some known relations among complexity measures for total functions. An arrow from A to B indicates that for every total Boolean function f, $B(f) = O(A(f))$. Double arrows indicate results in this paper, and boxes indicate new complexity measures. Single arrows indicate known results and references are omitted from the diagram for space considerations. Most references can be found in the tables in [42, 4] and we cite others in later sections. Known relations about EC are given in [24], and $\mathsf{FC} = O((\mathsf{MM})^2)$ is implicit in [8]. Fractional certificate complexity FC is equal to fractional block sensitivity and to randomized certificate complexity RC (up to multiplicative constants). MM is the minimax formulation of the positive adversary method. $\mathsf{MM} = O(\mathsf{FC})$ is proved in [29].

▶ **Proposition 3** (Characterization of non-signaling strategies). *A strategy p is non-signaling if and only if it is given by a family of coefficients $\lambda = \{\lambda_{AB}\}_{AB}$ (not necessarily nonnegative), AB ranging over pairs (A, B) of deterministic strategies, such that $p(a, b|x, y) = \sum_{AB:A(x)=a,B(y)=b} \lambda_{AB}$, and λ verifies $\sum_{AB} \lambda_{AB} = 1$, and $\sum_{AB:A(x)=a,B(y)=b} \lambda_{AB} \geq 0$ for all a, b, x, y.*

Given a Boolean function f on n variables, define a two-player game such that $\mathcal{X} = f^{-1}(0)$, $\mathcal{Y} = f^{-1}(1)$, $\mathcal{A} = \mathcal{B} = [n]$ and $R(x, y, a, b) = 1$ if and only if $a = b$ and $x_a \neq y_a$. Notice that this setting gives rise to a certificate game according to Definition 1.

2.1 Certificate games with public and private coins

In case of private coins, a randomized strategy for each player amounts to assigning, for every input $x \in \{0, 1\}^n$, a probability $p_{x,i}$ of producing i as its outcome, for each $i \in [n]$.

▶ **Definition 4** (Private coin certificate game complexity). *For a (possibly partial) function f,*

$$\mathsf{CG}(f) = \min_{p} \max_{x,y \in f^{-1}(0) \times f^{-1}(1)} \frac{1}{\omega(p; x, y)},$$

with p a collection of nonnegative variables $\{p_{x,i}\}_{x,i}$ satisfying, $\sum_{i \in [n]} p_{x,i} = 1$, $\forall x \in f^{-1}(0) \cup f^{-1}(1)$, and $\omega(p; x, y) = \sum_{i:x_i \neq y_i} p_{x,i} p_{y,i}$ is the probability that both players output a common index i that satisfies $R_f(x, y, i)$.

When the players share randomness, a *public-coin randomized strategy* is a distribution over pairs (A, B) of deterministic strategies. We assign a nonnegative variable $p_{A,B}$ to each strategy and require that they sum to 1. We say that *a pair of strategies (A, B) is correct on x, y* if $A(x) = B(y) = i$ and $x_i \neq y_i$.

▶ **Definition 5** (Public coin certificate game complexity). *For a (possibly partial) function f,*

$$\mathsf{CG}^{pub}(f) = \min_{p} \max_{x,y \in f^{-1}(0) \times f^{-1}(1)} \frac{1}{\omega^{pub}(p; x, y)},$$

where p is a collection of nonnegative variables $\{p_{A,B}\}_{A,B}$ satisfying $\sum_{(A,B)} p_{A,B} = 1$ and $\omega^{pub}(p; x, y) = \sum_{(A,B) \text{ correct on } x,y} p_{A,B}$.

2.2 Certificate games with quantum and non-signaling strategies

Similar to non-local games (see [19]), when the players can share a bipartite quantum state, a general quantum strategy for a certificate game consists of a shared state between the two players, and projective measurements made on their respective part of the shared state that depend on their input. CG^* is the multiplicative inverse of the winning probability (in the worst case) for the best quantum strategy. The formal definition is given in the full version of this paper [18]. Non-signaling strategies (Definition 2) are a generalization of quantum strategies and are useful to give lower bounds on quantum games. They are particularly well-suited when in a given problem, the bottleneck is that shared entanglement cannot allow players to learn any information about each others' inputs. This is the case for the OR function (Theorem 23).

▶ **Definition 6** (Non-signaling certificate game complexity). *For a (possibly partial) function f,*

$$\mathsf{CG}^{\mathsf{ns}}(f) = \min_{\lambda} \max_{x,y \in f^{-1}(0)\times f^{-1}(1)} \frac{1}{\omega^{\mathsf{ns}}(\lambda; x, y)},$$

where λ is a collection of (possibly negative) variables $\{\lambda_{A,B}\}_{A,B}$ with A, B ranging over all pairs of deterministic strategies satisfying $\sum_{(A,B)} \lambda_{A,B} = 1$ and

$$\omega^{\mathsf{ns}}(\lambda; x, y) = \sum_{\substack{A,B: A(x)=B(y)=i \\ \text{and } x_i \neq y_i}} \lambda_{AB}.$$

2.3 Dual formulation of $\mathsf{CG}^{\mathsf{pub}}$ and $\mathsf{CG}^{\mathsf{ns}}$

In the public coin setting, maximizing the winning probability in the worst case can be written as a linear program. This allows us to write a dual formulation, so (since it becomes a minimization problem, and we are considering its multiplicative inverse) this form will be more convenient when proving lower bounds. The dual variables $\mu_{x,y}$ can be thought of as a hard distribution on pairs of inputs, and the objective function is the μ-size of the largest set of input pairs where any deterministic strategy is correct. The next two propositions follow by standard LP duality.

▶ **Proposition 7** (Dual formulation of $\mathsf{CG}^{\mathsf{pub}}$). *For a two-player certificate game G_f corresponding to a (possibly partial) Boolean function f, $\mathsf{CG}^{pub}(f) = 1/\omega^{pub}(G_f)$, where the winning probability $\omega^{pub}(G_f)$ is given by the following linear program.*

$$\begin{aligned} \omega^{pub}(G_f) = \quad & \min_{\delta,\mu} \quad \delta \\ \text{such that} \quad & \sum_{x,y:\ A,B \text{ correct on } x,y} \mu_{x,y} \leq \delta \quad \text{for every deterministic strategy } A, B \\ & \sum_{x,y} \mu_{xy} = 1, \quad \mu_{x,y} \geq 0, \end{aligned}$$

where $\mu = \{\mu_{x,y}\}_{x\in f^{-1}(0),\, y\in f^{-1}(1)}$. A, B correct on x, y implies $A(x) = B(x) = i$ and $x_i \neq y_i$.

To prove lower bounds on CG^*, we cannot proceed in the same way since the value of CG^* cannot be written as a linear program. However, a key observation is that in many cases (and in all the cases we have considered in this paper), the fundamental bottleneck for proving lower bounds on quantum strategies is the non-signaling property, which says that in two-player games with shared entanglement, the outcome of one of the player's measurements cannot reveal the other player's input. This was the original motivation for defining $\mathsf{CG}^{\mathsf{ns}}$: if we only require the non-signaling property of quantum strategies, it suffices to prove a lower bound on $\mathsf{CG}^{\mathsf{ns}}$, which is a lower bound on CG^*. Using the characterization of non-signaling strategies in terms of an affine polytope (see Proposition 3), we obtain a convenient linear programming formulation for $\mathsf{CG}^{\mathsf{ns}}$.

Definition 6 shows that the value of $\omega^{\mathsf{ns}}(G)$ is a linear optimization problem. Its dual, a maximization problem, allows us to prove lower bounds on $\mathsf{CG}^{\mathsf{ns}}$ and in turn CG^*.

▶ **Proposition 8** (Dual formulation of $\mathsf{CG}^{\mathsf{ns}}$). *For a certificate game G corresponding to a (possibly partial) Boolean function f, $\mathsf{CG}^{\mathsf{ns}}(f) = 1/\omega^{ns}(G_f)$, where winning probability $\omega^{ns}(G_f)$ can be written as the following linear program.*

$$\begin{aligned}\omega^{\mathsf{ns}}(G_f) = \quad & \min_{\mu,\gamma,\delta} \quad \delta \\ \textit{such that} \quad & \sum_{x,y:\ A,B \textit{ correct on } x,y} \mu_{x,y} + \sum_{x,y} \gamma_{A(x),B(y),x,y} = \delta \textit{ for every deterministic strategy } A,B \\ & \sum_{x,y} \mu_{xy} = 1, \quad \mu_{x,y} \geq 0, \quad \gamma_{a,b,x,y} \geq 0,\end{aligned}$$

where $\mu = \{\mu_{x,y}\}_{x\in f^{-1}(0),\, y\in f^{-1}(1)}$ *and* $\gamma = \{\gamma_{i,j,x,y}\}_{i,j\in[n],x\in f^{-1}(0),\, y\in f^{-1}(1)}$.

The dual of the non-signaling variant can be used to bound on $\mathsf{CG}^*(\text{Promise-OR}_n)$ from below. The intuition comes from the fact that any quantum strategy for the certificate game for OR has to be non-signaling. Let one of the player have input $x = 0^n$, and the other player have one of n strings $x^{(i)}$ (x with the i-th bit flipped). At the end of the game, they output i with probability $p = \frac{1}{\mathsf{CG}^*(\text{Promise-OR})}$. If this probability were bigger than $\frac{1}{n}$, then the player with input x would learn some information about the other player's input.

Since we have considered progressively stronger models, the following holds trivially.

▶ **Proposition 9.** *For any (possibly partial) Boolean function f,*

$$\mathsf{CG}^{\mathsf{ns}}(f) \leq \mathsf{CG}^*(f) \leq \mathsf{CG}^{pub}(f) \leq \mathsf{CG}(f).$$

3 Preliminaries

We define many known complexity measures in this section. Almost all definitions are given for arbitrary Boolean functions, including partial functions. A few notable exceptions are certificate complexity, sensitivity and block sensitivity. Additional details for these measures in case of partial functions are given in the full version [18]. We use the following notation. A total Boolean function f is $f : \{0,1\}^n \to \{0,1\}$. Except when noted otherwise, inputs $x \in \{0,1\}^n$ are in $f^{-1}(0)$ and inputs $y \in f^{-1}(1)$, and sums over x range over $x \in f^{-1}(0)$, similarly for y. For partial functions we use f^{-1} for $f^{-1}(0) \cup f^{-1}(1)$.

Indices i range from 1 to n and x_i denotes the ith bit of x. We write $x^{(i)}$ to mean the string x with the ith bit flipped. When not specified, sums over i range over $i \in [n]$.

3.1 Query complexity

We recall briefly the standard notations and definitions of query complexity for Boolean functions $f : \{0,1\}^n \to \{0,1\}$. The deterministic query complexity (or decision tree complexity) $\mathsf{D}(f)$ is the minimum number of queries to bits of an input x required to compute $f(x)$, in the worst case. Randomized query complexity, denoted $\mathsf{R}(f)$, is the number of queries needed to compute f, in the worst case, with probability at least $2/3$ for all inputs. Zero-error randomized query complexity, denoted by $\mathsf{R}_0(f)$, is the expected number of queries needed to compute f correctly on all inputs. The relation $\mathsf{R}(f) \leq \mathsf{R}_0(f) \leq D(f)$ holds for all Boolean functions f. It will be useful to think of a randomized decision tree as a probability distribution over deterministic decision trees. When computing the probability of success, the randomness is over the choice of a deterministic tree.

Quantum query complexity, written $\mathsf{Q}(f)$, is the number of quantum queries needed to compute f correctly on all inputs with probability at least $2/3$.

In this paper we will consider the positive adversary method, a lower bound on quantum query complexity. It was shown by Spalek and Szegedy [38] that several formulations were equivalent, and we use the MinMax formulation MM here.

▶ **Definition 10** (Positive adversary method, Minimax formulation). *For any (possibly partial) Boolean function f, $\mathsf{MM}(f) = \min_p \max_{x\in f^{-1}(0), y\in f^{-1}(1)} \frac{1}{\sum_{i:x_i\neq y_i}\sqrt{p_{x,i}p_{y,i}}}$, where p is taken over all families of nonnegative $p_{x,i} \in \mathbb{R}$ such that for all $x \in f^{-1}$ (where f is defined), $\sum_{i\in[n]} p_{x,i} = 1$*

3.2 Sensitivity, certificate complexity and their variants

The sensitivity of a function is the number of bits that can be flipped, for the worst case input, so that the value of the function changes. Similarly, block sensitivity is the number of disjoint blocks that can be flipped.

For a total Boolean function f, a *certificate* is a partial assignment of the bits of an input to f that forces the value of the function to be constant, regardless of the value of the other bits. A *certificate for input x* is a partial assignment consistent with x that is a certificate for f.

▶ **Definition 11** ([40]). *For any total Boolean function f and input x, $\mathsf{C}(f;x)$ is the size of the smallest certificate for x. The certificate complexity of the function is $\mathsf{C}(f) = \max_{0,1}\{\mathsf{C}^0(f), \mathsf{C}^1(f)\}$, where $\mathsf{C}^b(f) = \max_{x\in f^{-1}(b)}\{\mathsf{C}(f;x)\}$.*

Certificate complexity is a lower bound on query complexity, for total Boolean functions.

Randomized certificate complexity was introduced by Aaronson as a randomized version of certificate complexity [2], and subsequently shown to be equivalent (up to constant factors) to fractional block sensitivity and fractional certificate complexity [39, 29, 21]. We use the fractional certificate complexity formulation.

▶ **Definition 12** (Fractional certificate complexity). *For any (possibly partial) Boolean function f $\mathsf{FC}(f) = \max_{z\in f^{-1}} \mathsf{FC}(f,z)$, where $\mathsf{FC}(f,z) = \min_v \sum_i v_{z,i}$, subject to $\sum_{i:z_i\neq z'_i} v_{z,i} \geq 1$ for all $z' \in f^{-1}$ such that $f(z) = 1 - f(z')$, with v a collection of variables $v_{z,i} \geq 0$.*

Another equivalent formulation is, $\mathsf{FC}(f) = \min_w \max_{\substack{z,z'\in f^{-1}\\ f(z)=1-f(z')}} \frac{\sum_i w_{z,i}}{\sum_{i:z_i\neq z'_i} w_{z,i}}$, where w is a collection of non-negative variables $w_{z,i}$.

Randomized certificate complexity (in its non-adaptive formulation) can be viewed as a game where a player is given an input z and should output an index i (say with probability $p_{z,i} = \frac{w_{z,i}}{\sum_j w_{z,j}}$). The player wins against an input z' (with $f(z) = 1 - f(z')$) if $z_i \neq z'_i$. Then, $\mathsf{FC}(f)$, for total functions, is (up to constant factors) the multiplicative inverse of the probability of winning the game in the worst case [2, 39, 21]. Expectational certificate complexity was introduced as a quadratically tight lower bound on R_0 [24].

▶ **Definition 13** (Expectational certificate complexity [24]). *For any (possibly partial) Boolean function f, $\mathsf{EC}(f) = \min_w \max_{z\in f^{-1}} \sum_{i\in[n]} w_{z,i}$ with w a collection of variables $0 \leq w_{z,i} \leq 1$ satisfying $\sum_{i:z_i\neq y_i} w_{z,i}w_{z',i} \geq 1$ for all z, z' s.t. $f(z) = 1 - f(z')$.*

The following relations are known to hold for any total Boolean function f.

▶ **Proposition 14** ([24]). $\mathsf{FC} \leq \mathsf{EC} \leq \mathsf{C} \leq O(\mathsf{R}_0) \leq O(\mathsf{EC}^2)$.

4 Public and private randomness in certificate games

As a starting point, we give an upper bound of C on $\mathsf{CG}^{\mathrm{pub}}$ using a public coin protocol which illustrates how shared randomness can be used by the players to coordinate their outputs (Section 4.3). We then go on to show EC (Section 4.3), R and RS (Section 4.4) are upper bounds on $\mathsf{CG}^{\mathrm{pub}}$. Finally, we give several upper bounds on private coin variant, CG (Section 4.5).

4.1 Public coin certificate game for the Tribes function

To construct a strategy for a certificate game, the main challenge is to *match* the index of the other side. In public coin setting, we can take advantage of having access to shared randomness to achieve this task. We illustrate this idea by giving a $\mathsf{CG}^{\mathrm{pub}}$ strategy for the Tribes function. The $\mathsf{Tribes}_{s,t}$ function is a composition of two functions, $\mathsf{Tribes}_{s,t} = \mathsf{OR}_s \circ \mathsf{AND}_t$.

▶ **Definition 15** (Tribes). $\mathsf{Tribes}_{s,t} : \{0,1\}^{st} \to \{0,1\}$ *is defined using the DNF formula*

$$\mathsf{Tribes}_{s,t}(x) = \bigvee_{i=1}^{s} \bigwedge_{j=1}^{t} x_{i,j}.$$

The Tribes function is a very well studied problem in complexity theory. It has full randomized query complexity, in particular, $\mathsf{R}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(n)$. On the other hand, the functions OR_s and AND_t have full sensitivity, and by Theorem 23, $\mathsf{CG}^{\mathrm{pub}}$ of $\mathsf{OR}_{\sqrt{n}}$ and $\mathsf{AND}_{\sqrt{n}}$ are $\Theta(\sqrt{n})$. In Theorem 16 we prove that the $\mathsf{CG}^{\mathrm{pub}}$ of $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ is $O(\sqrt{n})$. Thus the function $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ demonstrates a quadratic separation between $\mathsf{R}(f)$ and $\mathsf{CG}^{\mathrm{pub}}(f)$, and also implies that, under function composition, $\mathsf{CG}^{\mathrm{pub}}$ is not the product of the $\mathsf{CG}^{\mathrm{pub}}$ of the individual functions. We describe the main idea behind the strategy here.

For the $\mathsf{Tribes}_{k,k}$ function, we want a strategy that wins the certificate game with probability $\Omega(1/k)$ (instead of the obvious $\Omega(1/k^2)$). The input of $\mathsf{Tribes}_{k,k}$ consists of k blocks of k bits each. We will reduce the general problem to the case when all blocks of Alice's input have a single 0, and Bob has exactly one block with all 1's and Alice and Bob wins when they both can output the unique index i where Alice's bit is 0 and Bob's bit is 1.

Here we discuss this special case. Let us view Alice's input as an array A of k values, specifying the position of the 0 in each block (each entry is in $\{1, 2, \cdots, k\}$). On the other hand, Bob's input can be thought of as an index, say j, between 1 and k, identifying his all-1 block. Alice wants to find j and Bob wants to find $A[j]$, so both can output a position where their inputs differ.

Consider the case where all of the entries of Alice's array are distinct. Bob simply picks a random number r and outputs the r-th index of the j-th block. Alice can use the same r (due to shared randomness), and find the unique j such that $A[j] = r$. Whenever Bob picks r such that $A[j] = r$, they win the game. The probability that a random r matches $A[j]$ is $1/k$.

For the harder case when some of the entries of A coincide, we use the shared randomness to permute entries of each block. This ensures that, with constant probability, we have a unique j such that $A[j] = r$. This gives the required success probability $\Omega(1/k)$.

▶ **Theorem 16.** $\mathsf{CG}^{pub}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = O(\sqrt{n})$.

4.2 A framework for upper bounds based on hashing

We give the following general framework for $\mathsf{CG}^{\mathrm{pub}}$ protocols, building on the idea of using hash functions and permutations. Let $f : \{0,1\}^n \to \{0,1\}$ be a (possibly partial) Boolean function. Alice is given $x \in f^{-1}(0)$ and Bob is given $y \in f^{-1}(1)$. Their goal is to produce a common index $i \in [n]$ such that $x_i \neq y_i$.

Let $T \subseteq [n]$ be a set of potential outputs, known to both players, and let S be a finite set. T and S are fixed in advance as part of the specification of the strategy (they do not depend on the input, only on the function f). Let $A_x \subseteq T$ denote a set of potential outputs of Alice on x that belong to the set T, and $B_y \subseteq T$ denote a set of potential outputs of Bob on y that belong to the set T. The players proceed as follows:

1. Using shared randomness, they select a random mapping $h : T \to S$.
2. Using shared randomness, they select a random element $z \in S$.
3. Alice outputs a (possibly random) element of $h^{-1}(z) \cap A_x$ (if this set is empty, she outputs an arbitrary element). Similarly, Bob outputs a (possibly random) element of $h^{-1}(z) \cap B_y$ (if this set is empty, he outputs an arbitrary element).

This general strategy will be correct with good enough probability, if the following two conditions can be ensured:

(i) $h^{-1}(z) \cap W$ is not empty, where $W \subseteq A_x \cap B_y$ denotes the set of correct outputs from $A_x \cap B_y$, that is, for any $i \in W$, $x_i \neq y_i$.

(ii) $h^{-1}(z) \cap A_x$ and $h^{-1}(z) \cap B_y$ are "small enough".

Note, Condition (i) implies that both sets, $h^{-1}(z) \cap A_x$ and $h^{-1}(z) \cap B_y$, are not empty.

We will apply this general framework in various ways. We use it for proving that $\mathsf{CG}^{\mathrm{pub}}$ is bounded above by C and even by EC. We also use it to get a strong upper bound for the approximate index function ApInd in Section 6.2. Finally, we use the hashing framework to prove that the single-bit version of $\mathsf{CG}^{\mathrm{pub}}$ characterizes sensitivity up to constant factors in the proof of Theorem 38. While each of these proofs fits into the framework we described above, their analyses are technically quite different.

4.3 Upper bounds on $\mathsf{CG}^{\mathsf{pub}}$ by C and EC

We will take advantage of having access to shared randomness by using the hashing based approach outlined above. To illustrate the ideas of the proof, we start with a simple argument to show that $\mathsf{CG}^{\mathrm{pub}}$ is always upper bounded by certificate complexity. A slightly more involved argument will show a stronger upper bound by EC.

▶ **Theorem 17.** *For a total Boolean function f, $\mathsf{CG}^{pub}(f) \leq O(\mathsf{C}(f))$.*

Proof. Let S be a finite set of cardinality $\mathsf{C}(f)$. An element $z \in S$ is fixed as part of the specification of the protocol (z does not depend on the input).

Using shared randomness, the players select a function $h : [n] \to S$ as follows. Let $h : [n] \to S$ be a random hash function such that for each $i \in [n]$, $h(i)$ is selected independently and uniformly from S.

For $x \in f^{-1}(0)$ we fix an optimal 0-certificate C_x, and denote by $A_x \subseteq [n]$ the set of indices fixed by C_x. Similarly, for $y \in f^{-1}(1)$ we fix an optimal 1-certificate C_y, and denote by $B_y \subseteq [n]$ the set of indices fixed by C_y.

After selecting h using shared randomness, the players proceed as follows. On input x, Alice outputs an index $i \in A_x$ such that $h(i) = z$, and on input y, Bob outputs an index $j \in B_y$ such that $h(j) = z$. If they have several valid choices, they select randomly, and if they have no valid choices they output arbitrary indices.

Let $i^* \in A_x \cap B_y$, such that $x_{i^*} \neq y_{i^*}$. By the definition of certificates, such an element i^* exists for any $x \in f^{-1}(0)$ and $y \in f^{-1}(1)$, and i^* is a correct answer on input (x, y) if both players output i^*. Next, we estimate what is the probability that both players output i^*.

First recall that by the definition of h, the probability that $h(i^*) = z$ is $\frac{1}{|S|} = \frac{1}{\mathsf{C}(f)}$. Next, notice that for any $i \in A_x \cup B_y$ the number of elements different from i in $A_x \cup B_y$ is $\ell = |A_x \cup B_y| - 1 \leq |A_x| + |B_y| - 2$. Thus for any $z \in S$ and any $i \in A_x \cup B_y$ the probability (over the choice of h) that no element other than i in $A_x \cup B_y$ is mapped to z by h is $(1 - \frac{1}{|S|})^\ell \geq \frac{1}{e^2}$, since $\max\{|A_x|, |B_y|\} \leq \mathsf{C}(f) = |S|$ and thus $\ell \leq 2(|S| - 1)$.

Thus, the players output a correct answer with probability at least $\frac{1}{e^2}\frac{1}{\mathsf{C}(f)}$. ◀

The previous theorem is stated for total functions and its proof critically depends on the intersection property of 0- and 1-certificates. The theorem fails to hold for the partial function "Greater than Half" [7] (see full version for more details [18]), for which it is the case that $\mathsf{C}(\mathsf{GTH}) = 1$ whereas $\mathsf{CG}^{\text{pub}}(\mathsf{GTH})$ is $\Theta(n)$. We obtain a stronger upper bound on CG^{pub} by EC, the proof of which can be found in the full version [18].

▶ **Theorem 18.** *For a (possibly partial) Boolean function f , $\mathsf{CG}^{pub}(f) \leq O(\mathsf{EC}(f))$.*

4.4 Upper bound on public coin certificate game complexity by R

▶ **Theorem 19.** *For any Boolean (possibly partial) function f, $\mathsf{CG}^{pub}(f) \leq O(\mathsf{R}(f))$.*

Proof. From the definition of $\mathsf{R}(f)$ there is a randomized decision tree $\mathcal{R}$ that on any input x outputs $f(x)$ correctly with probability at least $2/3$, and $\mathcal{R}$ only reads at most $\mathsf{R}(f)$ number of bits of x. To prove $\mathsf{CG}^{\text{pub}}(f) \leq \mathsf{R}(f)$ let us consider the following strategies used by the two players:

Both the players run the algorithm $\mathcal{R}$ on their respective inputs using the same random coins (using the shared randomness). Both the player also use shared randomness to pick a number t uniformly at random between 1 and $\mathsf{R}(f)$. Both the players output the t-th index that is queried by $\mathcal{R}$.

Let x and y be the inputs to the players respectively. Since $f(x) = 1 - f(y)$, with probability at least $4/9$ the algorithm $\mathcal{R}$ will output different answers when the players run the algorithm on their respective inputs. Also since the algorithm $\mathcal{R}$ is run using the same internal coins, the initial sequence of indices queried by both the runs of the algorithm is the same until the algorithm queries an index k such that $x_k \neq y_k$. Note that with probability $1/\mathsf{R}(f)$, the random number t picked by t is the same as k. So with probability $\frac{4}{9} \cdot \frac{1}{\mathsf{R}(f)}$, the players correctly output the same index t such that $x_t \neq y_t$. Hence $\mathsf{CG}^{\text{pub}}(f) \leq O(\mathsf{R}(f))$. ◀

A proof that sabotage complexity RS [14] is bounded below by CG^{pub} is in the full version [18].

▶ **Proposition 20.** *The public coin certificate game complexity of a (possibly partial) function f is at most its sabotage complexity: $\mathsf{CG}^{pub}(f) \leq \frac{9}{2}\mathsf{RS}(f)$.*

4.5 Upper and lower bounds for private coin certificate games

We first observe that the following formulation is equivalent to CG. The essential idea is rescaling, and the objective function gets squared because the constraints are quadratic.

▶ **Proposition 21** (Equivalent formulation for CG). *For any (possibly partial) function f,*

$$\mathsf{CG}(f) = \min_{\{w_{x,i}\}} \max_{x} \left\{ \sum_i w_{x,i} \right\}^2$$
$$\text{such that} \sum_{i:x_i \neq y_i} w_{x,i} w_{y,i} \geq 1 \quad \forall x \in f^{-1}(0), y \in f^{-1}(1)$$
$$w_{x,i} \geq 0 \quad \forall x, i$$

We show that the following relations hold for CG. In the full version, we also make the distinction on which of these relations hold for partial functions [18].

▶ **Theorem 22.** *For any total Boolean function f,*

1. $\mathsf{MM}(f)^2 \leq \mathsf{CG}(f)$
2. $\mathsf{R}_0(f) \leq \mathsf{CG}(f) \leq O(\mathsf{EC}(f)^2)$ *[24]*
3. $\mathsf{CG}(f) \leq O(\mathsf{CG}^{pub}(f)^2 \mathsf{s}(f))$ *[24]*
4. $\mathsf{CG}(f) \leq \mathsf{C}^0(f)\mathsf{C}^1(f)$

5 Lower bounds on quantum certificate game complexity

In this section, we give a very short and simple proof that fractional certificate complexity (FC) is a lower bound on all of our certificate game models.

To illustrate the idea behind the proof and the technique we use, we start with a quantum lower bound on the OR function. Consider a hypothetical strategy with shared entanglement that would allow two players to win the certificate game with probability more than $1/n$. Then the players could use this strategy for the certificate game as a black box, to convey information (without using communication) in the following way. Assume Alice wants to send an integer $i \in \{1, \ldots, n\}$ to Bob. Bob uses input $y = 0^n$ and Alice uses input $x = y^{(i)}$ (all 0s with the i-th bit 1). Bob could learn i by taking the majority output of several runs of this game, which would violate the non-signaling principle of quantum information. To make this formal, we give a satisfying assignment to the dual formulation of $\mathsf{CG}^{\mathsf{ns}}$.

The previous lower bound on the OR function can be generalized, with a slightly more complicated weight assignment, to show that block sensitivity is a lower bound on the non-signaling value of the certificate games. We can prove a stronger result by using the primal formulation of $\mathsf{CG}^{\mathsf{ns}}$ (Definitions 2 and 6) to prove that $\mathsf{CG}^{\mathsf{ns}}$ is an upper bound on FC.

▶ **Theorem 23.** *For any (possibly partial) Boolean function f, $\mathsf{FC}(f) \leq \mathsf{CG}^{\mathsf{ns}}(f)$.*

Proof. Let $p(i, j|x, y)$ be the distribution over outcomes in an optimal nonsignaling strategy for $\mathsf{CG}^{\mathsf{ns}}(f)$. Then p verifies the nonsignaling condition, $\sum_j p(i, j|x, y) = \sum_j p(i, j|x, y')$ for all x, y, y', i, so we can write the marginal distribution for x as $p(i|x) = \sum_j p(i, j|x, y)$, since it does not depend on y. Notice that $p(i|x) = \sum_j p(i, j|x, y) \geq p(i, i|x, y)$ for all x, y, i.

With $\delta = \frac{1}{\mathsf{CG}^{\mathsf{ns}}(f)}$, we have that $\sum_{i:x_i \neq y_i} p(i, i|x, y) \geq \delta$ for all x, y such that $f(x) = 1 - f(y)$. Let $v_{x,i} = p(i|x)/\delta$ for some arbitrary y. Then $\sum_i v_{x,i} = \frac{1}{\delta}$ for all x (since p is a distribution) and $\sum_{i:x_i \neq y_i} v_{x,i} = \sum_{i:x_i \neq y_i} p(i|x)/\delta \geq \sum_{i:x_i \neq y_i} p(i, i, x, y)/\delta \geq 1$. Since this is a feasible solution to FC, we have that $\mathsf{FC}(f) \leq \mathsf{CG}^{\mathsf{ns}}(f)$. ◀

The lower bound can further be improved by slightly modifying the proof to hold for the Classical Adversary bound, denoted CMM. This measure was introduced in [1, 30] as a lower bound for randomized query complexity R and was shown to equal fractional certificate complexity FC for total functions (but can be larger for partial functions) [7].

▶ **Definition 24** (Classical Adversary Bound). *For any (possibly partial) Boolean function f, the minimax formulation of the Classical Adversary Bound is as:* $\mathsf{CMM}(f) = \min_p \max_{\substack{x,y\in S \\ f(x)=1-f(y)}} \frac{1}{\sum_{i:x_i\neq y_i} \min\{p_x(i),p_y(i)\}}$, *where p_x is a probability distribution over $[n]$.*

▶ **Theorem 25.** *For any (possibly partial) Boolean function f,* $\mathsf{CMM}(f) \leq \mathsf{CG}^{\mathsf{ns}}(f)$.

To summarize the key idea of this section, introducing the non-signaling model of Certificate games provides a very clean and simple way to give lower bounds on all of our previous models, including the shared entanglement model. It has several linear formulations, making it very easy to give upper and lower bounds. Finally, it captures an essential feature of zero-communication games, which we think of as the "non-signaling bottleneck". As an added bonus, it allows us to give proofs on the shared entanglement model without having to get into the technicalities of what characterizes quantum games.

6 Relations and separations between measures

6.1 Relationship between the various models of certificate games

Understanding the relationships between the various models of certificate game complexity can help us understand the power of shared randomness over private randomness and the power of quantum shared entanglement over shared randomness in the context of certificate games. The following results follow from results in the previous sections together with the fact that $\mathsf{EC}(f) \leq O(\mathsf{FC}(f)\cdot\sqrt{\mathsf{s}(f)})$ [24]. We start with relating $\mathsf{CG}^{\mathrm{pub}}$ and $\mathsf{CG}^{\mathsf{ns}}$.

▶ **Corollary 26.** *For any total Boolean function f,* $\mathsf{CG}^{\mathsf{ns}}(f) \leq \mathsf{CG}^{pub}(f) \leq O(\mathsf{CG}^{\mathsf{ns}}(f)^{3/2})$.

Since $\mathsf{CG}^{\mathsf{ns}}(\mathsf{GTH}) = \Theta(n)$ and $\mathsf{FC}(\mathsf{GTH}) = O(1)$, the partial function GTH separates $\mathsf{CG}^{\mathsf{ns}}$ and FC (see [18]). We don't know of a total Boolean function for which FC is significantly lower than $\mathsf{CG}^{\mathrm{pub}}$. In fact we have following set of open problems:

▶ **Open Problem 1.** Are any two complexity measures in the following chain of inequalities asymptotically separated by a total function?

$$\mathsf{FC}(f) \leq \mathsf{CG}^{\mathsf{ns}}(f) \leq \mathsf{CG}^{*}(f) \leq \mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{EC}(f))$$

Note that if $\mathsf{FC} = \Theta(\mathsf{EC})$, it would follow that $R_0 \leq O(\mathsf{FC}^2)$, a well-known open problem.

We now present the best known relation between CG and $\mathsf{CG}^{\mathsf{ns}}$.

▶ **Corollary 27.** *For any total Boolean function f,* $\mathsf{CG}^{\mathsf{ns}}(f) \leq \mathsf{CG}(f) \leq O(\mathsf{CG}^{\mathsf{ns}}(f)^3)$.

The above corollary implies that $\mathsf{CG} \leq O(\mathsf{CG}^{\mathsf{ns}})^3$. Hence,

▶ **Open Problem 2.** Is there a $c < 3$ such that $\mathsf{CG}(f) \leq O(\mathsf{CG}^{\mathsf{ns}}(f)^c)$?

For the case of CG versus $\mathsf{CG}^{\mathrm{pub}}$, the best known exponent is also 3. There are total functions f, for which $\mathsf{CG}(f) = \Theta(\mathsf{CG}^{\mathrm{pub}}(f)^2)$. One such example is the Tribes function.

▶ **Corollary 28.** *While* $\mathsf{CG}^{pub}(\mathsf{OR}_{\sqrt{n}}) = \mathsf{CG}^{\mathsf{ns}}(\mathsf{OR}_{\sqrt{n}}) = \Theta(\sqrt{n})$, *for* $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}} := \mathsf{OR}_{\sqrt{n}} \circ \mathsf{AND}_{\sqrt{n}}$, $\mathsf{CG}^{\mathsf{ns}}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \mathsf{CG}^{pub}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(\sqrt{n})$, *and* $\mathsf{CG}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(n)$.

The Tribes function also demonstrates a quadratic separation between $\mathsf{CG}^{\mathrm{pub}}$ and R while showing that the $\mathsf{CG}^{\mathrm{pub}}$ measure does not compose. Also note that any function with $\lambda(f) = n$, like the parity function, demonstrates a quadratic gap between CG and $\mathsf{CG}^{\mathrm{pub}}$. This is because $\mathsf{CG}(f) = \Omega((\mathsf{MM}(f))^2)$, from Theorem 22, and $\mathsf{MM}(f) = \Omega(\lambda(f))$. Thus for any such functions, CG is $\Theta(n^2)$ while $\mathsf{CG}^{\mathrm{pub}}$ is $\Theta(n)$. Hence,

▶ **Open Problem 3.** Is $\mathsf{CG}(f) \leq O(\mathsf{CG}^{\mathrm{pub}}(f)^2)$ for all functions f?

Note that Open Problem 3 and Open Problem 2 are related (for total functions). Also, we already know that for any total function $\mathsf{CG}(f) \leq O(\mathsf{CG}^{\mathrm{pub}}(f)^2 \cdot \mathsf{s}(f))$.

The two inequalities that we used in the corollaries and discussion above are $\mathsf{CG} = O(\mathsf{EC}^2)$ and $\mathsf{CG} = \Omega(\mathsf{MM}^2)$. Obtaining tighter versions of these inequalities may help us obtain tighter bounds between CG and $\mathsf{CG}^{\mathrm{pub}}$ (or $\mathsf{CG}^{\mathsf{ns}}$).

We observe that the bound $\mathsf{CG}(f) \leq O(\mathsf{EC}(f)^2)$ is indeed tight for the parity function $\oplus$. On the other hand, there is a quadratic gap between CG and EC^2 for the function OR_n. From Theorem 22, we have $\mathsf{CG} \leq \mathsf{C}^0 \cdot \mathsf{C}^1$, and hence $\mathsf{CG}(\mathsf{OR}_n) = \Theta(n)$ but $\mathsf{EC}(\mathsf{OR}_n) \geq \mathsf{FC}(\mathsf{OR}_n) = \Omega(n)$.

Another question is: what is the biggest separation between $\mathsf{CG}(f)$ and $\mathsf{MM}(f)$? To the best of our knowledge, the best upper bound on CG for total functions in terms of MM is

$$\mathsf{CG} \leq O(\mathsf{FC}^2\mathsf{s}) \leq O(\mathsf{MM}^6),$$

where the final inequality follows from the fact that $\mathsf{FC} \leq \mathsf{MM}^2$[8] and $\mathsf{s} \leq \lambda^2 \leq \mathsf{MM}^2$. The biggest separation between CG and MM in this direction is cubic: there is a total Boolean function f for which $\mathsf{CG}(f) \leq \Omega(\mathsf{EC}(f)^{3/2})$. In [6] they constructed a "pointer function" g, for which $\mathsf{R}_0(g) = \Omega(\mathsf{Q}(g)^3)$. We observe that, for the pointer function,

$$\mathsf{CG}(g) \geq \Omega(\mathsf{R}_0(g)) \geq \Omega(\mathsf{Q}(g)^3) \geq \Omega(\mathsf{MM}(g)^3),$$

where the first inequality follows from Theorem 22 and the other inequalities follows from earlier known results. This separation can also be achieved by the cheat sheet version of $k-$Forrelation function that gives a cubic separation between Q and R [10, 3].

However (from Theorem 22) for any total Boolean function f, $(\mathsf{MM}(f))^2 \leq O(\mathsf{CG}(f))$ and this inequality is in fact tight (for any total function with full spectral sensitivity, such as parity). In fact, the two quantities, CG and $(\mathsf{MM})^2$, are asymptotically identical for symmetric functions [32].

We also note that inequality that $\mathsf{CG}(f) \geq \Omega(\mathsf{R}_0(f))$ (from Theorem 22) is not tight: that is, there are functions like the parity function which separates CG from R_0 (see [18]).

Another upper bound on CG that we observe is $\mathsf{CG} \leq \mathsf{C}^0 \cdot \mathsf{C}^1$. While for some functions (like the Tribes function) the two quantities CG and $\mathsf{C}^0 \cdot \mathsf{C}^1$ are asymptotically equal we note that there are functions for which CG is significantly less than $\mathsf{C}^0 \cdot \mathsf{C}^1$.

▶ **Corollary 29** ([24, 21]). *There exists a total function $f : \{0,1\}^N \to \{0,1\}$ for which, $\mathsf{C}^0(f) = \Theta(N)$, $\mathsf{C}^1(f) = \Theta(\sqrt{N})$ and $\mathsf{EC}(f) = \Theta(\sqrt{N})$. Thus $C^0(f) \cdot C^1(f) = \Omega(\mathsf{CG}(f)^{3/2})$.*

6.2 Approximate Index: Exponential gap between R and $\mathsf{CG}^{\mathsf{pub}}$ for a *partial Boolean* function

We saw that $\mathsf{CG}^{\mathrm{pub}}$ of a Boolean function lies between its randomized query complexity and randomized certificate complexity; the same is true for noisyR. The measure noisyR was introduced in [12] (please refer to [12] for the formal definition) to study how randomised query complexity R behaves under composition and it was shown that $\mathsf{R}(f \circ g) = \Omega(\mathsf{noisyR}(f)\mathsf{R}(g))$. As it was also shown that almost all lower bounds (except Q) on R are also lower bounds on noisyR, it would be interesting to see whether $\mathsf{CG}^{\mathrm{pub}}$ is also a lower bound on noisyR.

▶ **Open Problem 4.** Is it the case that for all f, $\mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{noisyR}(f))$?

Ben-David and Blais [12] constructed the approximate index function, which is the only function known where noisyR and R are different. However, this is partial Boolean function, not a total Boolean function.

Let ApInd_k be the approximate index function where the input has an address part, say a, of k bits and a table with 2^k bits. The function is defined on inputs where all positions of the table labelled by strings within $\frac{k}{2} - \sqrt{k \log k}$ Hamming distance from a have the same value (either 0 or 1), and all positions that are farther away from a have 2 in them, i.e.

▶ **Definition 30.** $\mathsf{ApInd}_k : \{0,1\}^k \times \{0,1,2\}^{2^k} \to \{0,1,*\}$ *is defined as*

$$\mathsf{ApInd}_k(a,x) = \begin{cases} x_a & \text{if } x_b = x_a \in \{0,1\} \text{ for all } b \text{ that satisfy } |b-a| \leq \frac{k}{2} - \sqrt{k \log k} \\ & \text{and } x_b = 2 \text{ for all other } b, \\ * & \text{otherwise.} \end{cases}$$

Note that, even though the range of ApInd_k (as defined above) is non-Boolean, it can be converted into a Boolean function by encoding the input appropriately. This will only affect the lower/upper bounds by a factor of at most two.

Ben-David and Blais showed that $\mathsf{noisyR}(\mathsf{ApInd}_k) = O(\log k)$, and $\mathsf{R}(\mathsf{ApInd}) = \Theta(\sqrt{k \log k})$. As an indication that CG^{pub} could be a lower bound on noisyR, we show the following theorem.

▶ **Theorem 31.** *The public coin certificate game complexity of* ApInd *on* $n = k + 2^k$ *bits is* $\mathsf{CG}^{pub}(\mathsf{ApInd}_k) = O(\log k)$.

Sketch of Proof of Theorem 31. A central ingredient to the proof of this theorem is the following lemma that captures yet another application of the hashing based framework introduced in Section 4.2 (we state it in a more general form).

▶ **Lemma 32.** *Let* L *be an integer. Assume that for every* $x \in f^{-1}(0)$ *and* $y \in f^{-1}(1)$ *there are sets* A_x *depending only on* x*, and* B_y *depending only on* y*, of size* L*, such that any element of* $A_x \cap B_y$ *is a correct output on the input pair* (x,y)*, i.e. for any* $i \in A_x \cap B_y$*, we have* $x_i \neq y_i$*. If for any* $x \in f^{-1}(0)$ *and* $y \in f^{-1}(1)$*,* $L = |A_x| = |B_y| \leq t|A_x \cap B_y|$ *, then* $\mathsf{CG}^{pub}(f) \leq O(t^2)$.

Before we see how the hashing lemma helps prove Theorem 31, we define the following notation. The Hamming Sphere of radius r centred at a k-bit string a, denoted as $\mathcal{S}_a(r)$, contains all strings $z \in \{0,1\}^k$ that are at distance exactly r from a. Similarly the Hamming Ball of radius r centred at a, denoted as $\mathcal{B}_a(r)$, contains all strings $z \in \{0,1\}^k$ such that $d(a,z) \leq r$. For the ApInd_k function, a valid input has the function value in all positions in the table indexed by strings in $\mathcal{B}_a\left(\frac{k}{2} - \sqrt{k \log k}\right)$ where a is the address part.

Our analysis reduces to a very natural question: what is the intersection size of two Hamming balls of radius $\frac{k}{2} - \sqrt{k \log k}$ whose centers are at a distance $\frac{k}{\log k}$? We are able to show that the intersection is at least an $\Omega(\frac{1}{\sqrt{logk}})$ fraction of the total volume of the Hamming ball. This result and the techniques used could be of independent interest.

To bound the intersection size, we focus on the outermost $\sqrt{k}$ layers of the Hamming ball (since they contain a constant fraction of the total volume), and show that for each such layer the intersection contains an $\Omega(\frac{1}{\sqrt{\log k}})$ fraction of the elements in that layer.

For a single layer, the intersection can be expressed as the summation of the latter half of a hypergeometric distribution $P_{k,m,r}$ from $\frac{m}{2}$ to m ($m = \frac{k}{\log k}$ is the distance between the Hamming Balls and r is the radius of the layer). By using the "symmetric" nature of the hypergeometric distribution around $\frac{m}{2}$ for a sufficient range of values, this reduces to showing a concentration result around the expectation with width $\sqrt{m}$ (as the expectation for our choice of parameters is $\frac{m}{2} - O(\sqrt{m})$).

We use the standard concentration bound on hypergeometric distribution with width $\sqrt{r}$ and reduce it to the required width $\sqrt{m}$ by noticing a monotonicity property of the hypergeometric distribution. The strategies of Alice and Bob and how the above ideas help in proving Theorem 31 can be found in the full version [18]. ◀

Although we have proven an upper bound on $\mathsf{CG}^{\mathrm{pub}}(\mathsf{AplnD})$, a lower bound has not been shown and we leave it as an open problem.

▶ **Open Problem 5.** Give a lower bound on $\mathsf{CG}^{\mathrm{pub}}(\mathsf{AplnD})$.

7 Single bit versions

Aaronson et al. [4] defined single-bit versions of several formulations of the adversary method, and showed that they are all equal to the spectral sensitivity λ. Informally, single-bit versions of these measures are obtained by considering the requirements only with respect to pairs x, y such that $x, y \in f^{-1}(0) \times f^{-1}(1)$ and x and y differ only in a single bit.

We denote by $d(x, y)$ the Hamming distance of x and y, and by $x^{(i)}$ the string obtained from x by flipping the value of the i-th bit x_i to its negation. The single-bit version of $\mathsf{MM}(f)$ was defined in [4] as follows.

$$\mathsf{MM}_{[1]}(f) = \min_{\{w_{x,i}\}} \max_{x} \sum_{i} w_{x,i} \text{ such that } w_{x,i} w_{x^{(i)},i} \geq 1 \quad \forall x, i \text{ with } f(x) = 1 - f(x^{(i)}) \quad (1)$$

where $x \in \{0,1\}^n$ and $i \in [n]$.

Similarly to the proof of Proposition 21 it can be shown that this is equal to the following formulation, which we include for comparison with some of our other definitions.

$$\mathsf{MM}_{[1]}(f) := \min_{p} \max_{\substack{x,y \in f^{-1}(0) \times f^{-1}(1) \\ d(x,y)=1}} \frac{1}{\sum_{i: x_i \neq y_i} \sqrt{p_{x,i} p_{y,i}}} = \min_{p} \max_{x,i: f(x)=1-f(x^{(i)})} \frac{1}{\sqrt{p_{x,i} p_{x^{(i)},i}}} \quad (2)$$

where p is taken over all families of nonnegative $p_{x,i} \in \mathbb{R}$ such that for all x, $\sum_{i \in [n]} p_{x,i} = 1$.

Note that the definition of $\mathsf{MM}_{[1]}(f)$ is well defined for partial functions provided that there exist $x, y \in f^{-1}(0) \times f^{-1}(1)$ such that x and y differ in exactly one bit. This is equivalent to sensitivity, $\mathsf{s}(f)$, being non-zero. Aaronson et al. [4] proved the following theorem which also hold for these partial functions.

▶ **Theorem 33** (Thm. 28 in [4]). *For any Boolean function f, $\lambda(f) = \mathsf{MM}_{[1]}(f)$.*

Here we consider single-bit versions of $\mathsf{CG}^{\mathrm{pub}}$ and CG and show that they characterize sensitivity and λ^2, respectively, up to constant factors.

▶ **Definition 34** (Single-bit private coin certificate game complexity). *For any (possibly partial) Boolean function f with $\mathsf{s}(f) \neq 0$*

$$\mathsf{CG}_{[1]}(f) := \min_{p} \max_{\substack{x,y \in f^{-1}(0) \times f^{-1}(1) \\ d(x,y)=1}} \frac{1}{\omega(p; x, y)} = \min_{p} \max_{x,i: f(x)=1-f(x^{(i)})} \frac{1}{p_{x,i} p_{x^{(i)},i}},$$

where p is a collection of nonnegative variables $\{p_{x,i}\}_{x,i}$ that satisfies, for each $x \in \{0,1\}^n$, $\sum_{i \in [n]} p_{x,i} = 1$, and $\omega(p; x, x^{(i)})$ is the probability that both players output the unique index i where x and $x^{(i)}$ differ. (Note that $\omega(p; x, x^{(i)}) = p_{x,i} p_{x^{(i)},i}$.)

Recall that when the players share randomness, a public-coin randomized strategy is a distribution over pairs (A, B) of deterministic strategies. We assign a nonnegative variable $p_{A,B}$ to each strategy and require that they sum to 1. We say that a pair of strategies (A, B) is correct on x, y if $A(x) = B(y) = i$ and $x_i \neq y_i$.

▶ **Definition 35** (Single-bit public coin certificate game complexity). *For any (possibly partial) Boolean function f with $\mathsf{s}(f) \neq 0$*

$$\mathsf{CG}^{pub}_{[1]}(f) := \min_{p} \max_{\substack{x,y \in f^{-1}(0)\times f^{-1}(1) \\ d(x,y)=1}} \frac{1}{\omega^{pub}(p;x,y)} = \min_{p} \max_{x,i:x\in f^{-1}(0),x^{(i)}\in f^{-1}(1)} \frac{1}{\omega^{pub}(p;x,x^{(i)})},$$

where p is a collection of nonnegative variables $\{p_{A,B}\}_{A,B}$ satisfying $\sum_{(A,B)} p_{A,B} = 1$ and $\omega^{pub}(p;x,y) = \sum_{(A,B)\ correct\ on\ x,y} p_{A,B}$.

We define single-bit versions of FC and EC, and show that both are equal to sensitivity.

▶ **Definition 36.** *For any (possibly partial) Boolean function f with $\mathsf{s}(f) \neq 0$,*

- $\mathsf{FC}_{[1]}(f) = \max_{x\in\{0,1\}^n} \mathsf{FC}_{[1]}(f,x)$, *where* $\mathsf{FC}_{[1]}(f,x) = \min_v \sum_i v_{x,i}$, *subject to* $v_{x,i} \geq 1$ *for all i such that $f(x) = 1 - f(x^{(i)})$, with v a collection of variables $v_{x,i} \geq 0$.*
- $\mathsf{EC}_{[1]}(f) = \min_w \max_x \sum_{i\in[n]} w_{x,i}$, *with w a collection of variables $0 \leq w_{x,i} \leq 1$ satisfying $w_{x,i}w_{x^{(i)},i} \geq 1$ for all x, i s.t. $f(x) = 1 - f(x^{(i)})$.*

▶ **Proposition 37.** *For any (possibly partial) Boolean function $f : \{0,1\}^n \to \{0,1\}$ with $\mathsf{s}(f) \neq 0$, $\mathsf{s}(f) = \mathsf{FC}_{[1]}(f) = \mathsf{EC}_{[1]}(f)$.*

We prove the following about the single bit versions of the certificate games. We only include the proof of the first part here and proof of the second part can be found in the full version [18].

▶ **Theorem 38.** *For any (possibly partial) Boolean function f with $\mathsf{s}(f) \neq 0$,*

1. $\mathsf{s}(f) = \mathsf{FC}_{[1]}(f) = \mathsf{EC}_{[1]}(f) = \Theta(\mathsf{CG}^{pub}_{[1]}(f))$.
2. $\mathsf{CG}_{[1]}(f) = \lambda^2$.

Proof.

Upper bound by sensitivity. We use the hashing based approach, similarly to the upper bounds on $\mathsf{CG}^{\mathrm{pub}}$ by C and EC (Section 4.3).

Let S be a finite set of cardinality $\mathsf{s}(f)$. An element $z \in S$ is fixed as part of the specification of the protocol (z does not depend on the input). Using shared randomness, the players select a function $h : [n] \to S$ as follows. Let $h : [n] \to S$ be a random hash function such that for each $i \in [n]$, $h(i)$ is selected independently and uniformly from S. For $x \in f^{-1}(0)$ let A_x be the set of indices of the sensitive bits of x, that is $A_x = \{i \in [n] | f(x) = 1 - f(x^{(i)}\}$. Similarly, for $y \in f^{-1}(1)$ let $B_y = \{i \in [n] | f(y) = 1 - f(y^{(i)}\}$.

After selecting h using shared randomness, the players proceed as follows. On input x, Alice outputs an index $i \in A_x$ such that $h(i) = z$, and on input y, Bob outputs an index $j \in B_y$ such that $h(j) = z$. If they have several valid choices, or if they have no valid choices they output arbitrary indices.

Let $i^* \in A_x \cap B_y$, such that $x_{i^*} \neq y_{i^*}$. Notice that for $x \in f^{-1}(0)$ and $y \in f^{-1}(1)$ such that $d(x, y) = 1$ there is exactly one such index i^*.

Next, we estimate what is the probability that both players output i^*. Recall that by the definition of h, the probability that $h(i^*) = z$ is $\frac{1}{|S|} = \frac{1}{\mathsf{s}(f)}$. Notice that for any $i \in A_x \cup B_y$ the number of elements different from i in $A_x \cup B_y$ is $\ell = |A_x \cup B_y| - 1 \leq 2(|S| - 1)$, since $\max\{|A_x|, |B_y|\} \leq \mathsf{s}(f) = |S|$. Thus for any $z \in S$ and any $i \in A_x \cup B_y$ the probability (over the choice of h) that no element other than i in $A_x \cup B_y$ is mapped to z by h is $(1 - \frac{1}{|S|})^\ell \geq \frac{1}{e^2}$.

Thus, the players output a correct answer with probability at least $\frac{1}{e^2}\frac{1}{\mathsf{s}(f)}$.

Lower bound by sensitivity. We will use the dual formulation of $\mathsf{CG}^{\mathrm{pub}}_{[1]}$ obtained similarly to Proposition 7. The only difference is that the distribution μ takes nonzero values only on pairs $x, x^{(i)}$ (on pairs with Hamming distance 1). Let x^* be an input such that $\mathsf{s}(f; x^*) = \mathsf{s}(f) =: s$, and assume without loss of generality that $f(x^*) = 0$. Consider the following distribution μ over input pairs at Hamming distance 1. $\mu_{x^*,y} = \frac{1}{s}$ for $y \in f^{-1}(1)$ such that $d(x^*, y) = 1$ and $\mu_{x^*,y} = 0$ for every other y. Furthermore, $\mu_{x',y} = 0$ for any y and $x' \neq x^*$. Thus, we only have s input pairs with nonzero measure.

Let A, B be any pair of deterministic strategies for Alice and Bob. Since A is a deterministic strategy, Alice will output the same index i for every pair x^*, y. This means that the probability over μ that the players win is at most $\frac{1}{s(f;x)} = \frac{1}{s} = \frac{1}{\mathsf{s}(f)}$ for any pair of deterministic strategies. ◀

One of the enticing open problems in this area of complexity theory is the sensitivity-block sensitivity conjecture. The best gap between $\mathsf{bs}(f)$ and $\mathsf{s}(f)$ is quadratic: that is there exists a function f such that $\mathsf{bs}(f) = \Theta(\mathsf{s}(f)^2)$. The conjecture is that this is indeed tight, that is, for any Boolean function f, $\mathsf{bs}(f) = O(\mathsf{s}(f)^2)$. In the seminal work of [23] the degree of a Boolean function was bounded by the square of sensitivity, and this is tight for Boolean functions. Since the degree of a Boolean function is quadratically related to the block sensitivity, we have $\mathsf{bs}(f) \leq O(\mathsf{s}(f)^4$. Unfortunately, this approach via degree will not be able to give any tighter bound on block sensitivity in terms of sensitivity.

Estimating certificate game complexity may be a possible way to prove a tighter bound on block sensitivity in terms of sensitivity. Given the result in Theorem 38, designing a strategy for $\mathsf{CG}^{\mathrm{pub}}$ using $\mathsf{CG}^{\mathrm{pub}}_{[1]}$ may help us solve the sensitivity-block sensitivity conjecture.

▶ **Open Problem 6.** What is the smallest c such that, for any Boolean function f, $\mathsf{CG}^{\mathrm{pub}}(f) = O(\mathsf{CG}^{\mathrm{pub}}_{[1]}(f)^c)$?

Note that proving $\mathsf{CG}^{\mathrm{pub}}(f) = O(\mathsf{CG}^{\mathrm{pub}}_{[1]}(f)^2)$ would prove that $\mathsf{bs}(f) \leq O(\mathsf{s}(f)^2)$. It may seem too much to expect that the single-bit version of the game can help get upper bounds on the general public coin setting, but thanks to Huang's breakthrough result [23], we already know that $\mathsf{CG}^{\mathrm{pub}}(f) = O(\mathsf{CG}^{\mathrm{pub}}_{[1]}(f)^5)$ for any total Boolean function f.

References

1. Scott Aaronson. Lower bounds for local search by quantum arguments. *SIAM Journal on Computing*, 35(4):804–824, 2006. doi:10.1137/S0097539704447237.
2. Scott Aaronson. Quantum certificate complexity. *J. Comput. Syst. Sci.*, 74:313–322, 2008.
3. Scott Aaronson, Shalev Ben-David, and Robin Kothari. Separations in query complexity using cheat sheets. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '16, pages 863–876, 2016. doi:10.1145/2897518.2897644.
4. 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 *Symposium on Theory of Computing (STOC)*, pages 1330–1342. ACM, 2021.
5. Andris Ambainis. Quantum lower bounds by quantum arguments. In *Symposium on Theory of Computing (STOC)*, pages 636–643, 2000. doi:10.1145/335305.335394.
6. Andris Ambainis, Kaspars Balodis, Aleksandrs Belovs, Troy Lee, Miklos Santha, and Juris Smotrovs. Separations in query complexity based on pointer functions. *J. ACM*, 64(5), September 2017. doi:10.1145/3106234.

7 Andris Ambainis, Martins Kokainis, Krisjanis Prusis, and Jevgenijs Vihrovs. All Classical Adversary Methods are Equivalent for Total Functions. In Rolf Niedermeier and Brigitte Vallée, editors, *35th Symposium on Theoretical Aspects of Computer Science (STACS 2018)*, volume 96 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 8:1–8:14, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.STACS.2018.8.

8 Anurag Anshu, Shalev Ben-David, and Srijita Kundu. On Query-To-Communication Lifting for Adversary Bounds. In *36th Computational Complexity Conference (CCC 2021)*, volume 200, pages 30:1–30:39, 2021. doi:10.4230/LIPIcs.CCC.2021.30.

9 Kaspars Balodis, Shalev Ben-David, Mika Göös, Siddhartha Jain, and Robin Kothari. Unambiguous DNFs and Alon-Saks-Seymour. In *Symposium on Foundations of Computer Science, FOCS*, 2021.

10 Nikhil Bansal and Makrand Sinha. K-forrelation optimally separates quantum and classical query complexity. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1303–1316, 2021.

11 Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001.

12 Shalev Ben-David and Eric Blais. A tight composition theorem for the randomized query complexity of partial functions: Extended abstract. In *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS*, pages 240–246, 2020. doi:10.1109/FOCS46700.2020.00031.

13 Shalev Ben-David, Pooya Hatami, and Avishay Tal. Low-Sensitivity Functions from Unambiguous Certificates. In *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, volume 67 of *LIPIcs*, pages 28:1–28:23, 2017. doi:10.4230/LIPIcs.ITCS.2017.28.

14 Shalev Ben-David and Robin Kothari. Randomized query complexity of sabotaged and composed functions. *Theory of Computing*, 14(5):1–27, 2018. doi:10.4086/toc.2018.v014a005.

15 Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik*, 46(4-5):493–505, 1998. doi:10.1002/(SICI)1521-3978(199806)46:4/5<493::AID-PROP493>3.0.CO;2-P.

16 Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, April 2014. doi:10.1103/RevModPhys.86.419.

17 Harry Buhrman, Richard Cleve, Serge Massar, and Ronald de Wolf. Nonlocality and communication complexity. *Rev. Mod. Phys.*, 82:665–698, March 2010. doi:10.1103/RevModPhys.82.665.

18 Sourav Chakraborty, Anna Gál, Sophie Laplante, Rajat Mittal, and Anupa Sunny. Certificate games. *CoRR*, 2022. ECCC report TR-143 (2022). arXiv:2211.03396.

19 R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proc. of the 19th Annual IEEE Conference on Computational Complexity*, pages 236–249, 2004.

20 D. J. Foulis and C. H. Randall. Empirical logic and tensor products. In *Interpretations and Foundations of Quantum Theory*, volume Interpretations and Foundations of Quantum Theory, pages 1–20, 1981.

21 Justin Gilmer, Michael Saks, and Srikanth Srinivasan. Composition limits and separating examples for some boolean function complexity measures. *Combinatorica*, 36(3):265–311, 2016. doi:10.1007/s00493-014-3189-x.

22 Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 212–219, 1996.

23 Hao Huang. Induced subgraphs of hypercubes and a proof of the sensitivity conjecture. *Annals of Mathematics*, 190(3):949–955, 2019. URL: https://www.jstor.org/stable/10.4007/annals.2019.190.3.6.

24 Rahul Jain, Hartmut Klauck, Srijita Kundu, Troy Lee, Miklos Santha, Swagato Sanyal, and Jevgundefinednijs Vihrovs. Quadratically tight relations for randomized query complexity. *Theor. Comp. Sys.*, 64(1):101–119, January 2020. doi:10.1007/s00224-019-09935-x.

25 Mauricio Karchmer and Avi Wigderson. Monotone circuits for connectivity require super-logarithmic depth. *SIAM J. Discrete Math.*, 3:255–265, January 1990.

26 V. M. Khrapchenko. Complexity of the realization of a linear function in the class of π-circuits. *Mathematical notes of the Academy of Sciences of the USSR*, 9:21–23, 1971.

27 M. Kläy, C. H. Randall, and D. J. Foulis. Tensor products and probability weights. *Int. J. Theor. Phys.*, 26(3):199–219, 1987.

28 Elias Koutsoupias. Improvements on Khrapchenko's theorem. *Theor. Comput. Sci.*, 116(2):399–403, 1993.

29 Raghav Kulkarni and Avishay Tal. On fractional block sensitivity. *Chicago Journal of Theoretical Computer Science*, 2016:1–16, 2016. Article 08.

30 Sophie Laplante and Frédéric Magniez. Lower bounds for randomized and quantum query complexity using Kolmogorov arguments. *SIAM Journal on Computing*, 38(1):46–62, 2008. doi:10.1137/050639090.

31 Gatis Midrijanis. Exact quantum query complexity for total Boolean functions. *CoRR*, 2004. arXiv:quant-ph/0403168.

32 Rajat Mittal, Sanjay S Nair, and Sunayana Patro. Lower bounds on quantum query complexity for symmetric functions. *CoRR*, 2021. arXiv:2110.12616.

33 Noam Nisan. CREW PRAMS and decision trees. In *Symposium on Theory of Computing*, STOC '89, pages 327–335, 1989. doi:10.1145/73007.73038.

34 Noam Nisan and Mario Szegedy. On the degree of boolean functions as real polynomials. *Computational Complexity*, 4:301–313, 1994. doi:10.1007/BF01263419.

35 Carlos Palazuelos and Thomas Vidick. Survey on nonlocal games and operator space theory. *Journal of Mathematical Physics*, 57, December 2015.

36 Stefano Pironio. Lifting Bell inequalities. *J. Math. Phys.*, 46:062112, 2005.

37 C. H. Randall and D. J. Foulis. Operational statistics and tensor products. In *Interpretations and Foundations of Quantum Theory*, pages 21–28, 1981.

38 Robert Špalek and Mario Szegedy. All quantum adversary methods are equivalent. *Theory of Computing*, 2(1):1–18, 2006. doi:10.4086/toc.2006.v002a001.

39 Avishay Tal. Properties and applications of boolean function composition. In *Innovations in Theoretical Computer Science*, ITCS '13, pages 441–454, New York, NY, USA, 2013. ACM. doi:10.1145/2422436.2422485.

40 Uzi Vishkin and Avi Wigderson. Trade-offs between depth and width in parallel computation. *SIAM J. Discrete Math.*, 14:303–314, 1985.

41 Alexander Wilce. Tensor products in generalized measure theory. *Int. J. Theor. Phys.*, 31(11):1915–1928, 1992.

42 Alex Yu. Boolean function complexity measures. https://funcplot.com/table/, 2019. Adapted from [ABK16].