Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 143 (2022)

Certificate Games and Consequences for the Classical Adversary Bound

Sourav Chakraborty* Anna Gál† Mika Göös‡ Sophie Laplante§ Rajat Mittal¶
Anupa Sunny‖

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 study four versions of certificate games, namely private coin, public coin, shared entanglement and non-signaling games. The public-coin variant of certificate games gives a new characterization of the classical adversary bound, a lower bound on randomized query complexity which was introduced as a classical version of the quantum (non-negative) quantum adversary bound.

We show that complexity in the public coin model (therefore also the classical adversary) is bounded above by certificate complexity, as well as by expectational certificate complexity (EC) and sabotage complexity (RS). On the other hand, it is bounded below by fractional and randomized certificate complexity. We provide new exponential separations between classical adversary and randomized query complexity for partial functions.

In contrast, the private coin model is bounded from below by zero-error randomized query complexity and above by EC^2.

The quantum measure reveals 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, fractional block sensitivity, as well as classical adversary. This implies the collapse of all models of certificate games, except private randomness, to the classical adversary bound.

We 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.

*Indian Statistical Institute, Kolkata
†University of Texas at Austin
‡EPFL
§Université Paris Cité, IRIF
¶IIT Kanpur
‖Université Paris Cité, IRIF

ISSN 1433-8092

Contents

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: 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 [26], 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 $\mathsf{D}(f) \leq O(\mathsf{s}(f)^6)$ [44, 38, 26], while the best separation is cubic [14]. 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 [56, 4].

With these questions in mind, we introduce new complexity measures based on the Karchmer-Wigderson relation of a Boolean function. This relation was introduced by Karchmer and Wigderson [29] 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 [29] 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 1.1 (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 the players 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 2.3. 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 ($\mathsf{CG}^{\mathrm{priv}}$ for the private coin model, $\mathsf{CG}^{\mathrm{pub}}$ for the public coin model, CG^{*} for the shared entanglement model and $\mathsf{CG}^{\mathrm{ns}}$ 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 total 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 $\mathsf{CG}^{\mathrm{priv}}(f) \leq \mathsf{C}^0(f) \cdot \mathsf{C}^1(f)$. This simple upper bound is tight for many functions including OR and Parity, but there are other examples where $\mathsf{CG}^{\mathrm{priv}}(f)$ 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 [17, 45], and on the interactions between communication complexity and nonlocality in reference [18].

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, 52]. 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) [53, 22]. 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 randomised query complexity $\mathsf{R}(f)$, zero-error randomized query complexity $\mathsf{R}_0(f)$, certificate complexity $\mathsf{C}(f)$, 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. If for a statement or theorem it is not explicitly written that it holds for a possibly partial function then we mean the statement or theorem is only known to hold for total functions.

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

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

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 exhibiting a strategy for the game. We provide some other techniques to prove lower bounds.

The classical adversary bound (CMM, Definition 4.2) which was defined in [35], as an analog of the quantum adversary method to study randomized query complexity (R), turns out to play a central role in our work. The CMM measure is well studied with a number of different formulations of it, already known [7]. We show that certificate games (with public randomness), gives another formulation of CMM. This characterization provides new insight that helps to obtain bounds and separations on CMM that were not known earlier.

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 side 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 6.2) that for any, possibly partial, Boolean function f,

$$\mathsf{CG}^{\mathrm{ns}}(f) \geq \mathsf{CMM}(f)$$

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, the marginal distribution of one of the players can be used to give a satisfying assignment for CMM bound.

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 CMM 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 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 5.7) that for any, possibly partial, Boolean function f,

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

In fact we can prove something much stronger. We prove (Theorem 7.1) that for any, possibly partial, Boolean function f,

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

Combining this with our lower bound result we have a new characterization of CMM.

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

This gives us a different way of understanding the classical adversary bound through the lens of two-player games. Slightly weaker results, namely $\mathsf{CG}^{\mathrm{pub}} = O(\mathsf{FC})$ (for total functions) and $\mathsf{CG}^{\mathrm{ns}} = O(\mathsf{CMM})$, were proved independently by [51] and [47].

Bounds on certificate games with private randomness: The private randomness model of certificate game complexity, $\mathsf{CG}^{\mathrm{priv}}$, 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 5.10). On the other hand $\mathsf{CG}^{\mathrm{priv}}$ is lower bounded by R_0. (This follows from [28].) Therefore, $\mathsf{R}_0(f) \leq O(\mathsf{CG}^{\mathrm{priv}}(f)) \leq O(\mathsf{C}^0(f)\mathsf{C}^1(f))$.

[1] OR_n is the OR of n variables. From Grover's algorithm [23, 16] we have $\mathsf{Q}(\mathsf{OR}_n) = \sqrt{n}$. On the other hand $\mathsf{FC}(\mathsf{OR}_n) = \Omega(\mathsf{s}(\mathsf{OR}_n)) = \Omega(n)$.

In fact, $\mathsf{CG}^{\mathrm{priv}}(f)$ can be larger than the arity of the function. This is because, we show (Theorem 5.10) that $\mathsf{CG}^{\mathrm{priv}}(f)$ 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 $\lambda(f)$.

Consequences on expectational certificate complexity and the classical adversary bound: The expectational certificate complexity [28] was introduced as a bound that is quadratically related to zero-error query complexity (R_0), that is, $\mathsf{EC}(f) \leq \mathsf{R}_0(f) \leq O(\mathsf{EC}(f)^2)$ for any total Boolean f.

We show that $\mathsf{CG}^{\mathrm{pub}}$ is bounded above by $\mathsf{EC}(f)$ up to constant factors (Theorem 5.5), so

$$\mathsf{CMM} \leq O(\mathsf{CG}^{\mathrm{pub}}) \leq O(\mathsf{EC}).$$

We also extend our result that $\mathsf{CG}^{\mathrm{pub}}$ is upper bounded by $\mathsf{R}(f)$ to prove that $\mathsf{CG}^{\mathrm{pub}}$ is also upper bounded by the sabotage complexity $\mathsf{RS}(f)$ (Theorem 5.8). This also proves that for any Boolean function (including partial functions)

$$\mathsf{CMM}(f) = O(\mathsf{RS}(f)).$$

This gives us upper bounds on $\mathsf{CMM}(f)$ that were not known before, answering a question asked by Ambainis et al [7], where they asked for a general limitation (that includes partial functions) on the power of the classical adversary method as a lower bound on randomized query complexity.

For total Boolean functions, CMM is known to be asymptotically equal to FC. Thus for total functions, the measures FC, CMM, $\mathsf{CG}^{\mathrm{ns}}$, CG^{*} and $\mathsf{CG}^{\mathrm{pub}}$ are all asymptotically equal. 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) [28]. We also give a direct proof that $\mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{C}(f))$ for total functions (Theorem 5.4) as a "warmup" to the stronger upper bound by EC.

Relating EC with $\mathsf{CG}^{\mathrm{priv}}$ and $\mathsf{CG}^{\mathrm{pub}}$ in turn gives us results about the certificate games themselves. To be precise, for total functions, $\mathsf{EC}(f) \leq O(\mathsf{FC}(f) \cdot \sqrt{\mathsf{s}(f)})$ [28]. Since $\mathsf{CG}^{\mathrm{priv}}(f) \leq O(\mathsf{EC}(f)^2)$ (Theorem 5.10), we have (in Corollary 10.1)

$$\mathsf{CG}^{\mathrm{priv}}(f) \leq O(\mathsf{CG}^{\mathrm{pub}}(f)^3) = O(\mathsf{CMM}(f)^3).$$

Composition: The $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ function is a composition of the $\mathsf{AND}_{\sqrt{n}}$ and $\mathsf{OR}_{\sqrt{n}}$ function. It is easy to show using certificate complexity that $\mathsf{FC}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = O(\sqrt{n})$, so CMM, $\mathsf{CG}^{\mathrm{pub}}$, CG^{*} and $\mathsf{CG}^{\mathrm{ns}}$ do not compose, 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. The question of whether $\mathsf{CG}^{\mathrm{priv}}$ composes is open.

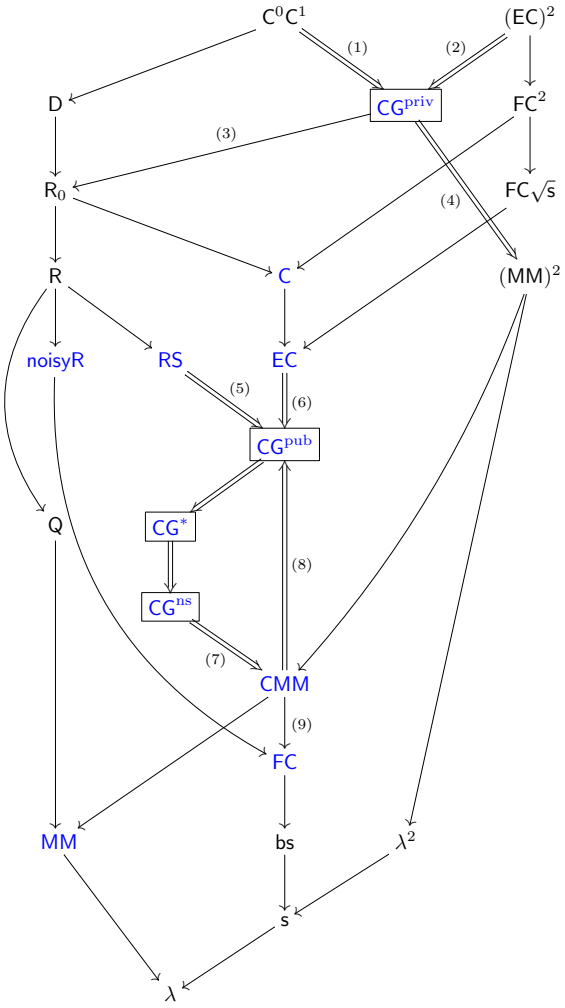
Certificate game complexity for partial functions: While $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ demonstrates a quadratic gap between R and $\mathsf{CG}^{\mathrm{pub}}$, we know the largest gap between R and $\mathsf{CG}^{\mathrm{pub}}$ for total functions is at most cubic (since $\mathsf{D} \leq (\mathsf{bs})^3$ [12, 43]). But for partial functions the situation is different. Ben-David and Blais [13] demonstrated a function, approximate index ApInd (Definition A.1), for which there is exponential separation between R and FC [2]. We improve this to show that $\mathsf{CG}^{\mathrm{pub}}$ of ApInd is at most $O(\log(\mathsf{R}))$ (Theorem A.2) and hence demonstrate an exponential separation between R and $\mathsf{CG}^{\mathrm{pub}}$ (CMM) for partial Boolean functions.

We also give a partial function f such that $\mathsf{R}(f) = \Omega(n)$ and $\mathsf{CG}^{\mathrm{pub}}(f) = O(1)$ (Lemma 9.1).

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 [30, 32]. 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.

[2] [13] 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.

We show that the single-bit version of private coin certificate game complexity is equal to λ^2 (Theorem 8.8). 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 8.4). 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 $\mathsf{CG}^{\mathrm{pub}}_{[1]}$.



1. Theorem 5.10. 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 5.10, Separation: OR, Tightness: $\oplus$.
3. Implicit in[28] (Theorem 5.10). Separation: $\oplus$, Tightness: OR.
4. Theorem 5.10 Separation: Pointer function in [6] and the cheat sheet version of the $k-$Forrelation function [10, 3]. Tightness: OR.
5. Theorem 5.8. Separation: Tribes (Theorem 5.2 and $\mathsf{RS}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(n)$ because RS composes [15]). Tightness: $\oplus$.
6. Theorem 5.5. Separation: OPEN, Tightness: $\oplus$.
7. Theorem 6.2.
8. Theorem 7.1.
9. The reverse direction is known to hold for total functions [7].

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 [56, 4] and we cite others in later sections. Known relations about EC are given in [28], and $\mathsf{FC} = O((\mathsf{MM})^2)$ is proven 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. $\mathsf{MM} = O(\mathsf{CMM})$ is proved in [33].

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 [20].)

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 2.1 (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 [21, 48, 31, 55]. A more recent proof is given in [46].

Proposition 2.2 (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 1.1.

2.1 Certificate games with 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 2.3 (Private coin certificate game complexity)**.** *For a (possibly partial) function f,*

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

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 $R_f(x, y, i)$.

2.2 Certificate games with public coins

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

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

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

2.3 Certificate games with quantum and non-signaling strategies

Similar to non-local games (see [20]), when the players can share a bipartite quantum state, a general strategy for a certificate game consists of a shared state $|\Psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ between the two players, and two families of projective measurements $M_A = \{M_A(x)\}_{x \in f^{-1}(0)}$ and $M_B = \{M_B(x)\}_{x \in f^{-1}(1)}$ made on their respective part of the shared state. Here $\mathcal{H}_A$ and $\mathcal{H}_B$ are the Hilbert spaces of respective players. For each measurement $M_*(x)$, we denote the family of orthogonal projections as $\{P_{*;x,i}\}_{i \in [n]}$ (see [42] for a definition of projective measurements).

We can now define the shared entanglement certificate game complexity of a Boolean function.

Definition 2.5 (Shared entanglement certificate game complexity)**.** *For a (possibly partial) function f,*

$$\mathsf{CG}^*(f) = \min_{|\Psi_{AB}\rangle, M_A, M_B} \quad \max_{x,y \in f^{-1}(0) \times f^{-1}(1)} \quad \frac{1}{\omega^\star((|\Psi_{AB}\rangle, M_A, M_B); x, y)},$$

where $\omega^\star((|\Psi_{AB}\rangle, M_A, M_B); x, y)$ is the winning probability of strategy $(|\Psi_{AB}\rangle, M_A, M_B)$ on x, y,

$$\omega^\star((|\Psi_{AB}\rangle, M_A, M_B); x, y) = \sum_{i : x_i \neq y_i} \langle \Psi_{AB} | P_{A;x,i} \otimes P_{B;y,i} | \Psi_{AB} \rangle.$$

Non-signaling strategies (Definition 2.1) 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 6.2).

Definition 2.6 (Non-signaling certificate game complexity)**.** *For a (possibly partial) function f,*

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

where p ranges over all non-signaling strategies (Def. 2.1) and

$$\omega^{\mathrm{ns}}(p; x, y) = \sum_{i : x_i \neq y_i} p(i, i | x, y).$$

This can be expressed as a linear program by using the affine formulation of non-signaling distributions given in Proposition 2.2.

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

Proposition 2.7. *For any (possibly partial) Boolean function f,*

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

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.

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 use three general techniques for upper bounds on Certificate games. Given a decision tree, the players can pick queries by agreeing on a node of the decision tree in some way. We use this to show that $\mathsf{CG}^{\mathrm{pub}}$ is bounded by sabotage complexity. For certificate-based measures, we use shared randomness and hash functions to agree on an common index. We provide some details of this framework in Section 3.1.

Finally, our strongest general upper bound on public-coin certificate game complexity is $\mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{CMM}(f))$ (Theorem 7.1), which implies that all of $\mathsf{CG}^{\mathrm{pub}}$, CG^{*}, $\mathsf{CG}^{\mathrm{ns}}$ are equal (up to constant factors). The idea behind this upper bound is to apply the *correlated sampling* technique [25, 11]. In the correlated sampling game, Alice and Bob receive as input distributions p and q, respectively, and their goal is to output, using shared randomness and no communication, samples $X \sim p$ and $Y \sim q$ so as to maximize the agreement probability $\Pr[X = Y]$. The basic result about this game is that the players can achieve an agreement probability that depends only on the *total variation distance* between p and q. We apply this result in order to convert a non-signaling strategy (which is closely related to CMM)—where p and q roughly correspond to the marginal distributions of the strategy—into a public-coin strategy with only constant-factor loss in the winning probability. The details appear in Section 7.

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.

A more detailed overview of these techniques is given in the following sections.

3.1 Overview of upper bound techniques for $\mathsf{CG}^{\mathrm{pub}}$

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 constructing a $\mathsf{CG}^{\mathrm{pub}}$ strategy for the Tribes function.

Even though Tribes is a starting example for us, it already gives an example that separates R and $\mathsf{CG}^{\mathrm{pub}}$, and also implies that, under function composition, $\mathsf{CG}^{\mathrm{pub}}$ value is not the product of the $\mathsf{CG}^{\mathrm{pub}}$ value 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.

First, take the simple case when each entry of Alice's array is 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. 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 $\Omega(1/k)$.

A framework for upper bounds based on hashing: 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 the set of potential outputs of Alice on x that belong to the set T, and $B_y \subseteq T$ denote the 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 several different ways. We use it for proving that $\mathsf{CG}^{\mathrm{pub}}$ is upper bounded by C and even by EC. We also use it to get a strong upper bound for the approximate index function ApInd. Finally, we use the hashing framework to prove that the single-bit version of $\mathsf{CG}^{\mathrm{pub}}$ characterizes sensitivity up to constant factors. While each of these proofs fits into the framework we described above, their analysis is technically quite different.

$\mathsf{CG}^{\mathbf{pub}}$ strategy for ApInd: We can use the hashing framework to show an exponential separation between R and $\mathsf{CG}^{\mathrm{pub}}$ for Approximate Index, a partial function. The analysis of the strategy 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 $\Omega(\frac{1}{\sqrt{\log k}})$ 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 (Lemma A.10), 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 (Lemma A.11).

3.2 Overview of lower bound techniques for $\mathsf{CG}^{\mathbf{pub}}$, CG^* and $\mathsf{CG}^{\mathrm{ns}}$

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

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

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 $\mathsf{CG}^{\mathrm{ns}}$: if we only require the non-signaling property of quantum strategies, it suffices to prove a lower bound on $\mathsf{CG}^{\mathrm{ns}}$, which is a lower bound on CG^*. Using the characterization of non-signaling strategies in terms of an affine polytope (see Proposition 2.2), we obtain a convenient linear programming formulation for $\mathsf{CG}^{\mathrm{ns}}$.

Definition 2.6 shows that the value of $\omega^{\mathrm{ns}}(G)$ is a linear optimization problem. We compute its dual, a maximization problem, which allows us to prove lower bounds on $\mathsf{CG}^{\mathrm{ns}}$ and in turn CG^*.

Proposition 3.2 (Dual formulation of $\mathsf{CG}^{\mathrm{ns}}$)**.** *For a certificate game G corresponding to a (possibly partial) Boolean function f, $\mathsf{CG}^{\mathrm{ns}}(f) = 1/\omega^{ns}(G_f)$, where winning probability $\omega^{ns}(G_f)$ can be written as the following linear program.*

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

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

As a first step, we illustrate how the dual of the non-signaling variant can be used to prove a lower bound on $\mathsf{CG}^*(\text{Promise-}\mathsf{OR}_n)$ (Proposition 6.1). 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 $p = \frac{1}{\mathsf{CG}^*(\text{Promise-}\mathsf{OR})}$. 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.

The lower bound on the OR function generalizes to show that block sensitivity is a lower bound on the non-signaling value of the certificate games. We prove an even stronger result, by going back to the original definition of $\mathsf{CG}^{\mathrm{ns}}$ (Definition 2.6) and giving a very simple proof that $\mathsf{CG}^{\mathrm{ns}}$ is an upper bound on CMM (Theorem 6.2).

4 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. We include additional details and definitions with respect to partial functions for these measures in Section 4.4. 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 $i \in [n]$.

4.1 Query complexity and adversary bounds

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 $\mathsf{R}(f) \leq \mathsf{R}_0(f) \leq \mathsf{D}(f)$ 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 [52] that several formulations were equivalent, and we use the MinMax formulation MM here.

Definition 4.1 (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), $\sum_{i \in [n]} p_{x,i} = 1$*

The classical adversary bound was introduced in [1, 35] as a lower bound for randomized query complexity R. It was shown to be equal to fractional certificate complexity FC (Definition 4.4) for total functions (but can be larger for partial functions) and has many equivalent formulations, given in [7].

Definition 4.2 (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 $[n]$.*

4.2 Certificate complexity and its variants

Certificate complexity is a lower bound on query complexity [54], for total Boolean functions.

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 4.3. *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 $\mathsf{C}(f) = \max\{\mathsf{C}^0(f), \mathsf{C}^1(f)\}$, where $\mathsf{C}^b(f) = \max_{x \in f^{-1}(b)}\{\mathsf{C}(f; x)\}$.*

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 [53, 33, 22].

We use the fractional certificate complexity formulation.

Definition 4.4 (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 single player 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, 53, 22].

Expectational certificate complexity was introduced as a quadratically tight lower bound on R_0 [28].

Definition 4.5 (Expectational certificate complexity [28])**.** *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 such that* $0 \leq w_{z,i} \leq 1$ *satisfying* $\sum_{i:z_i \neq z'_i} w_{z,i} w_{z',i} \geq 1$ *for all z, z' s.t.* $f(z) = 1 - f(z')$*.*

Since the weights are between 0 and 1, we can associate with each i a Bernoulli variable. The players can sample from each of these variables independently and output the set of indices where the outcome was 1. The constraint says that the expected number of indices i in both sets that satisfy $z_i \neq z'_i$ should be bounded below by 1. The complexity measure is the expected size of the sets. For example, for the OR function, a strategy could be as follows. On input z, pick the smallest i for which $z_i = 1$, output the set $\{i\}$. If no such i exists, then output the set $[n]$. The (expected) size of the set is n and the (expected) size of the intersection is 1.

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

Proposition 4.6 ([28])**.** $\mathsf{FC} \leq \mathsf{EC} \leq \mathsf{C} \leq O(\mathsf{R}_0) \leq O(\mathsf{EC}^2)$.

4.3 Sensitivity and its variants

Sensitivity is a lower bound on most of the measures described above (except Q and MM). Given a Boolean function f, an input x is *sensitive at index i* if flipping the bit at index i (which we denote by $x^{(i)}$) changes the value of the function to $1-f(x)$.

Definition 4.7 (Sensitivity)**.** $\mathsf{s}(f;x)$ *is the number of sensitive indices of x.* $\mathsf{s}(f) = \max_x \mathsf{s}(f;x)$

If B is a subset of indices, an input x is *sensitive to block B* if simultaneously flipping all the bits in B (which we denote by x^B) changes the value of the function to $1-f(x)$.

Definition 4.8 (Block sensitivity)**.** $\mathsf{bs}(f;x)$ *is the maximum number of disjoint sensitive blocks of x.* $\mathsf{bs}(f) = \max_x \mathsf{bs}(f;x)$

Aaronson et al. [4] recently revived interest in a measure called λ. It was first introduced by Koutsoupias [32], and is a spectral relaxation of sensitivity.

Definition 4.9 (Spectral sensitivity, or λ)**.** *For a Boolean function f, let F be the $|f^{-1}| \times |f^{-1}|$ matrix defined by $F(x,y) = 1$ when $f(x) = 1 - f(y)$ and x, y differ in 1 bit. Then $\lambda(f) = \|F\|$, where $\|\cdot\|$ is the spectral norm.*

Note that F can also be taken to be a $|f^{-1}(0)| \times |f^{-1}(1)|$ matrix with rows indexed by elements of $f^{-1}(0)$ and columns by elements of $f^{-1}(1)$. It is easy to show that both ways of defining F give the same spectral norm.

Proposition 4.10 ([4, 53, 22, 34])**.** *For any (possibly partial) Boolean function f,*

$$\lambda(f) \leq \mathsf{s}(f) \leq \mathsf{bs}(f) \leq \mathsf{FC}(f) \text{ and } \lambda(f) \leq \mathsf{MM}(f)$$

4.4 Additional definitions for partial functions

Extending the definition of certificates to partial functions is slightly complex. For $f : \{0,1\}^n \to \{0,1,*\}$ it is natural to define the measures $\mathsf{C}^0(f)$, $\mathsf{C}^1(f)$, as well as $\mathsf{C}^{\{0,*\}}(f)$ and $\mathsf{C}^{\{1,*\}}(f)$ as follows:

Definition 4.11. *For $f : \{0,1\}^n \to \{0,1,*\}$ and $b \in \{0,1\}$ a partial assignment α is a b-certificate for $x \in f^{-1}(b)$ if α is consistent with x, and for any x' consistent with α $f(x') = b$.*

For $f : \{0,1\}^n \to \{0,1,*\}$ and $b \in \{0,1\}$ a partial assignment α is a $\{b,*\}$-certificate for $x \in f^{-1}(b)$ if α is consistent with x, and for any x' consistent with α $f(x') \in \{b,*\}$.

For $b \in \{0,1\}$ and $x \in f^{-1}(b)$, $\mathsf{C}^b(f;x)$ is the size of the smallest b-certificate for x and $\mathsf{C}^b(f) = \max_{x \in f^{-1}(b)}\{\mathsf{C}^b(f;x)\}$.

For $b \in \{0,1\}$ and $x \in f^{-1}(b)$, $\mathsf{C}^{\{b,*\}}(f;x)$ is the size of the smallest $\{b,*\}$-certificate for x and $\mathsf{C}^{\{b,*\}}(f) = \max_{x \in f^{-1}(b)}\{\mathsf{C}^{\{b,*\}}(f;x)\}$.

Note that for example, while one can think of 0-certificates for x certifying that $f(x) = 0$, a $\{0,*\}$-certificate for x certifies that $f(x) \neq 1$. We also note that in the definition of $\mathsf{C}^{\{b,*\}}(f)$ we take the maximum over $x \in f^{-1}(b)$, we do not include inputs x where the function is not defined (e.g. where $f(x) = *$).

The above definitions are fairly straightforward and natural, but it is not immediately clear how to define $\mathsf{C}(f)$ for partial functions. We use the following notation:

Definition 4.12. *For $f : \{0,1\}^n \to \{0,1,*\}$ we define $\mathsf{C}(f) = \max\{\mathsf{C}^{\{0,*\}}(f), \mathsf{C}^{\{1,*\}}(f)\}$ and $\mathsf{C}'(f) = \max\{\mathsf{C}^0(f), \mathsf{C}^1(f)\}$.*

Notice that $\mathsf{C}(f) \leq \mathsf{C}'(f)$ for any f, and for total functions $\mathsf{C}(f) = \mathsf{C}'(f)$. However, for partial functions $\mathsf{C}(f)$ can be much smaller than $\mathsf{C}'(f)$. The "Greater than Half" function (see section B) is an example of a partial function on n bits with $\mathsf{C}(f) = O(1)$ while $\mathsf{C}'(f) = \Theta(n)$.

It turns out that some results known for total functions remain valid for partial functions with respect to $\mathsf{C}(f)$ but not with respect to $\mathsf{C}'(f)$ and others remain valid for partial functions with respect to $\mathsf{C}'(f)$ but not with respect to $\mathsf{C}(f)$. Thus, it is important to distinguish between the two versions. We prefer to use this definition for $\mathsf{C}(f)$ since for example with this definition $\mathsf{C}(f)$ remains a lower bound on deterministic query complexity (and for R_0 as well) for partial functions. On the other hand, it is easy to construct partial functions with deterministic query complexity $O(1)$ but $\mathsf{C}'(f) = \Omega(n)$. Some of our results for total functions involving $\mathsf{C}(f)$ no longer hold for partial functions, even though they remain valid with respect to $\mathsf{C}'(f)$.

A property of certificates often exploited in proofs is that every 0-certificate must intersect (and contradict) every 1-certificate and this remains the case for partial functions. However, this property no longer holds for $\{0,*\}$ versus $\{1,*\}$-certificates. Proofs based on this property remain valid for partial functions with respect to $\mathsf{C}'(f)$, but may no longer hold for partial functions with respect to $\mathsf{C}(f)$. An important example where this happens is the result that $\mathsf{EC}(f) \leq \mathsf{C}(f)$ by [28]. This result does not hold for partial functions, as shown by the "Greater than Half" function which has $\mathsf{C}(f) = O(1)$ and $\mathsf{EC}(f) = \Theta(n)$ (see section B), but remains valid with respect to $\mathsf{C}'(f)$.

For sensitivity (block sensitivity) of partial functions, we consider an input x in the domain $f^{-1}(0) \cup f^{-1}(1)$ to be sensitive to an index (or to a block) if flipping it gives an input where f is defined and takes the complementary value $1 - f(x)$. We do not consider an input to be sensitive to an index (or block) if flipping it gives an input where f is undefined. Notice that with our definition, sensitivity can be 0 even for non-constant partial functions.

5 Public and private randomness in certificate games

As a starting point, we give an upper bound of C on CG^{pub} using a public coin protocol which illustrates how shared randomness can be used by the players to coordinate their outputs (Section 5.2). We then go on to show EC (Section 5.2), R and RS (Section 5.3) are upper bounds on CG^{pub}. Finally, we give several upper bounds on private coin variant, $\mathsf{CG}^{\text{priv}}$ (Section 5.4).

5.1 Public coin certificate game 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 5.1 (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. Thus $\mathsf{CG}^{\mathrm{pub}}$ of $\mathsf{OR}_{\sqrt{n}}$ and $\mathsf{AND}_{\sqrt{n}}$ is $\Theta(\sqrt{n})$. As a warmup to our general upper bounds on $\mathsf{CG}^{\mathrm{pub}}$, in Theorem 5.2 we give a direct proof that the $\mathsf{CG}^{\mathrm{pub}}$ of $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ is $O(\sqrt{n})$. (This also follows from Theorem 7.1, the fact that for total functions $\mathsf{CMM}(f) = O(\mathsf{C}(f))$, and the fact that $\mathsf{C}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \sqrt{n}$.) Thus the function $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ demonstrates a quadratic separation between $\mathsf{R}(f)$ and $\mathsf{CG}^{\mathrm{pub}}(f)$.

Theorem 5.2. $\mathsf{CG}^{\mathrm{pub}}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = O(\sqrt{n})$.

Proof. We give a public coin strategy for the Certificate game. Let x and y be the two strings given to Alice and Bob respectively, that is $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}(x) = 0$ and $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}(y) = 1$.

Since $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}(x) = 0$ for all $1 \le i \le \sqrt{n}$ there exists a_i such that $x_{i,a_i} = 0$ where x_{i,a_i} denotes the a_ith bit of the ith block of x. Note that the a_i is not necessarily unique. For each i, Alice arbitrarily picks a a_i such that $x_{i,a_i} = 0$ and then Alice considers a new string x' where for all i, $x_{(i,a_i)} = 0$ and for other bits of x' is 1.

Similarly, $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}(y) = 1$ implies there exists an b such that for all $1 \le j \le \sqrt{n}$, $y_{b,j} = 1$. Again, note that there might be multiple such b but Bob picks one such b and considers the input y' where $y_{b,j} = 1$ for all $1 \le j \le \sqrt{n}$ and all other bits of y' is set to 0.

Note that (b, a_b) is the unique index (i, j) such that $x'(i, j) = 0$ and $y'(i, j) = 1$. We will now present a protocol for Alice and Bob for outputting the index (b, a_b) with probability at least $1/\sqrt{n}$. Note that this would imply our theorem.

- Alice and Bob uses shared randomness to select the same list of $\sqrt{n}$ permutations $\sigma_1, \ldots, \sigma_{\sqrt{n}} : [\sqrt{n}] \to [\sqrt{n}]$, where the permutations are drawn (with replacement) uniformly and independently at random from the set of all possible permutations from $[\sqrt{n}]$ to $[\sqrt{n}]$.
- According to their pre-decided strategy both Alice and Bob picks the same index t between 1 and $\sqrt{n}$.
- Bob outputs $(b, \sigma_b^{-1}(t))$.
- Alice picks a number i such that $\sigma_i(a_i) = t$ and outputs (i, a_i). In case no i exists then Alice outputs any random index.

The probability of success of the protocol crucially depends on the fact that because Alice and Bob has shared randomness, they can pick the same set of permutations $\sigma_1, \ldots, \sigma_{\sqrt{n}}$ although the permutations are picked uniformly at random.

We will show that with constant probability there exists a unique i which satisfies $\sigma_i(a_i) = t$. Under the condition that this holds we will show that the probability of success of the above protocol is at least $1/\sqrt{n}$ which would prove the theorem. We start with the following claim that we will prove later.

Claim 5.3. *For any fixed number t, with probability at least $(1 - 1/\sqrt{n})^{\sqrt{n}-1} \approx e^{-1}$, there exists a unique i such that $\sigma_i(a_i) = t$.*

Note that the permutation σ_b is picked from the uniform distribution over all possible permutations from $[\sqrt{n}]$ to $[\sqrt{n}]$, i.e. σ_b is a random bijection from $[\sqrt{n}]$ to $[\sqrt{n}]$. So with probability $1/\sqrt{n}$, $t = \sigma_b(a_b)$. Assuming that $t = \sigma_b(a_b)$ and that there exists a unique i such that $\sigma_i(a_i) = t$, note that output of both Alice and Bob is indeed (b, a_b). Thus the probability of success of the protocol is $\Omega(1/\sqrt{n})$. □

Proof of Claim 5.3. Consider the event

$$\mathcal{E}_k := \sigma_k(a_k) = t \text{ and for all } i \neq k,\ \sigma_i(a_i) \neq t.$$

The probability that the event $\mathcal{E}_k$ occurs is $\frac{1}{\sqrt{n}} \cdot (1 - \frac{1}{\sqrt{n}})^{\sqrt{n}-1}$. The event that there exists a unique i such that $\sigma_i(a_i) = t$ is $\cup_{k=1}^{\sqrt{n}} \mathcal{E}_k$. The events $\mathcal{E}_k$ are disjoint and the claim follows. □

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

We will take advantage of having access to shared randomness by using the hashing based approach outlined in Section 3.1. 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.

Both players pick a certificate for their respective inputs. They permute the indices $\{1, \ldots, n\}$ with shared randomness and each player outputs the first index in this new order within their certificate. Since their certificates must intersect, the probability that they are correct is at least one over the size of the union which is at most $2\mathsf{C}(f)$, so for any total function $\mathsf{CG}^{\mathrm{pub}}(f) \leq 2\mathsf{C}(f)$).[3]

We now provide a different proof based on hashing as a warmup before we prove the stronger result $\mathsf{CG}^{\mathrm{pub}}(f) = O(\mathsf{EC}(f))$.

Theorem 5.4. *For a total Boolean function f, $\mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{C}(f))$.*

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 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 which does not hold for $\{0, *\}$- vs. $\{1, *\}$-certificates. The theorem fails to hold for the partial function "Greater than Half" (see Section B), for which it is the case that $\mathsf{C}(\mathsf{GTH}) = 1$ whereas $\mathsf{CG}^{\mathrm{pub}}(\mathsf{GTH})$ is $\Theta(n)$. However, the theorem and its proof remain valid for partial functions with respect to $\mathsf{C}'(f)$ (see Section 4.4). We obtain a stronger upper bound on $\mathsf{CG}^{\mathrm{pub}}$ by EC.

[3] We thank an anonymous referee for suggesting this simple and elegant proof.

Theorem 5.5. *For a (possibly partial) Boolean function f, $\mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{EC}(f))$.*

Proof. The proof will be similar but slightly more involved than the proof of the upper bound by C. We will rely on the "weights" $w_{x,i}$ from the definition of $\mathsf{EC}(f)$.

Let S be a finite set of cardinality $\lceil \mathsf{EC}(f) \rceil$. Using shared randomness, the players select a function $h : [n] \to S$ and an element $z \in S$ 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. In addition, z is selected uniformly from S and independently from the choices for h.

For all inputs $x \in \{0,1\}^n$ consider the weights $w_{x,i}$ achieving $\mathsf{EC}(f)$. Denote by EC_x the sum $\sum_{i\in[n]} w_{x,i}$ and recall that by the definition of EC, for each $x \in \{0,1\}^n$ we have $EC_x \leq \mathsf{EC}(f)$.

For a given $z \in S$, consider the preimage $h^{-1}(z)$. We use the notation

$$W_x(z) = \sum_{i \in h^{-1}(z)} w_{x,i} \ .$$

Notice that for any $z \in S$,

$$E[W_x(z)] = \sum_{i\in[n]} \frac{w_{x,i}}{|S|} = \frac{EC_x}{|S|}$$

where the expectation is over the choice of the hash function.

After selecting h and z using shared randomness, the players proceed as follows. On input $x \in f^{-1}(0)$ Alice selects an index i from $h^{-1}(z)$ such that each i is chosen with probability $\frac{w_{x,i}}{W_x(z)}$. Similarly, on input $y \in f^{-1}(1)$ Bob selects an index i from $h^{-1}(z)$ such that each i is chosen with probability $\frac{w_{y,i}}{W_y(z)}$. Note that these choices are made using Alice's and Bob's private randomness, so for fixed z and h Alice's choices are independent from Bob's choices. However, they both depend on z and h. In what follows, we will denote by Pr_z and Pr_h, respectively, the probabilities that are only over the choice of z and h, respectively.

Recall that $W_x(z)$ and $W_y(z)$ are measures of the preimage of z with respect to the weights for x and y respectively. Since $\frac{\mathsf{EC}_x}{|S|} \leq 1$ for any $x \in \{0,1\}^n$, the preimage of most elements in S will have small measure. Next we estimate the probability that a given element i is mapped to a value $h(i)$ whose preimage has small measures $W_x(h(i))$ and $W_y(h(i))$. Note that this only depends on the choice of h.

For a given i, consider first selecting the values $h(j)$ for all $j \neq i$ from $[n]$. Consider the measure of the preimages of elements in S at this point (without taking into account what happens to i). Since $\frac{\mathsf{EC}_x - w_{x,i}}{|S|} \leq 1$ for any $x \in \{0,1\}^n$, at most $\frac{1}{t-1}$ fraction of the elements in S can have measure more than $t-1$ at this point. Since $w_{x,i} \leq 1$, we get that for any $x \in \{0,1\}^n$ and $i \in S$, $Pr_h[W_x(h(i)) > t] \leq \frac{1}{t-1}$.

For $i \in [n]$, let $\mathbf{Small}_i$ denote the event that both $W_x(h(i))$ and $W_y(h(i))$ are at most t. Then $Pr_h[\mathbf{Small}_i] \geq 1 - \frac{2}{t-1}$.

For a given $i \in [n]$, let $\mathbf{Both}_i$ denote the event that both players select i. Let $I(x,y) = \{i | x_i \neq y_i\}$. Since $f(x) = 1 - f(y)$, $I(x,y) \neq \emptyset$.

Recall that the players goal is that they both output the same i from $I(x,y)$. Denote by $P(x,y)$ the probability that they both output the same i from $I(x,y)$. Note that $P(x,y)$ is at least as large as the probability that they both output the same i from $I(x,y)$, and both $W_x(h(i))$ and $W_y(h(i))$ are at most t.

Thus, using that the events $\mathbf{Both}_i$ are pairwise disjoint, we have

$$\begin{aligned} P(x,y) &\geq \sum_{i\in I(x,y)} Pr[\mathbf{Both}_i \cap (z{=}h(i)) \cap \mathbf{Small}_i] \\ &= \sum_{i\in I(x,y)} Pr[\mathbf{Both}_i | (z{=}h(i)) \cap \mathbf{Small}_i] Pr[(z{=}h(i)) \cap \mathbf{Small}_i] \ . \end{aligned}$$

Note that the events $z = h(i)$ and $\mathbf{Small}_i$ are independent, since the choice of z is independent of h. For any $i^* \in I(x,y)$, and $h : [n] \to S$, $Pr_z[z = h(i^*)] = \frac{1}{|S|}$, Thus, $Pr[z = h(i) \cap \mathbf{Small}_i] = Pr_z[z = h(i)] Pr_h[\mathbf{Small}_i] = \frac{1}{|S|} Pr_h[\mathbf{Small}_i] \geq \frac{1}{|S|}(1 - \frac{2}{t-1})$.

For any $i \in [n]$, we have

$$Pr[\mathbf{Both}_i | z = h(i)] = \frac{w_{x,i}}{W_x(z)} \frac{w_{y,i}}{W_y(z)} \text{ and } Pr[\mathbf{Both}_i | z = h(i) \cap \mathbf{Small}_i] \geq \frac{w_{x,i}}{t} \frac{w_{y,i}}{t} .$$

Thus, we get

$$P(x,y) \geq \frac{1}{t^2} \frac{1}{|S|} (1 - \frac{2}{t-1}) \sum_{i \in I(x,y)} w_{x,i} w_{y,i} \geq \frac{1}{t^2} \frac{1}{|S|} (1 - \frac{2}{t-1})$$

where the last inequality follows by the definition of $\mathsf{EC}(f)$.

Setting $t = 5$, we get that the players output the same element from $I(x,y)$ with probability at least $\frac{1}{50} \frac{1}{\lceil \mathsf{EC}(f) \rceil} = \Omega(\frac{1}{\mathsf{EC}(f)})$. □

5.3 Lower bound on sabotage complexity

Randomized sabotage complexity RS [15] is a measure of complexity introduced to study the behavior of randomized query complexity R under composition. It was shown that RS is a lower bound on R and that it behaves perfectly under composition.

Definition 5.6 (Sabotage Complexity [15])**.** *The sabotage complexity of a function f, denoted $\mathsf{RS}(f)$, is defined using a concept of* sabotaged *inputs $P_f \subseteq \{0,1,*\}^n$ which is the set of all partial assignments of a function f consistent with a $0-$input and a $1-$input. Let $P_f^\dagger$ is defined similarly with the symbol $*$ being replaced by $\dagger$. Given a (possibly partial) function f, a partial function $f_{sab} : P_f \cup P_f^\dagger \mapsto \{0,1\}$ is defined as $f_{sab}(x) = 1$ if $x \in P_f$ and $f_{sab}(x) = 0$ if $x \in P_f^\dagger$ (here we view $P_f, P_f^\dagger$ as subsets of $\{0,1,*,\dagger\}^n$). The sabotage complexity is defined as the randomized query complexity of computing f_{sab} i.e. $\mathsf{RS}(f) = \mathsf{R}(f_{sab})$.*

The classical adversary method CMM was introduced as a lower bound on R [35] but there were no limitations known on this quantity that hold for partial functions [7]. In this section we show that on sabotage complexity RS is an upper bound on CG^{pub} and therefore on CMM (see Theorem 7.1). As a warm-up, we give an easy proof that $\mathsf{CG}^{\text{pub}}(f) = O(\mathsf{R}(f))$.

Theorem 5.7. *For any Boolean (possibly partial) function f, $\mathsf{CG}^{\text{pub}}(f) \leq O(\mathsf{R}(f))$.*

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

Using the same idea we can show that the public coin certificate game complexity CG^{pub} is bounded above by randomized sabotage complexity.

Theorem 5.8. *The public coin certificate game complexity of a (possibly partial) function f is at most its sabotage complexity: $\mathsf{CG}^{\text{pub}}(f) \leq \frac{9}{2}\mathsf{RS}(f)$.*

Proof. We show this by using the sabotage complexity protocol to build a CG^{pub} protocol. Assuming that Alice has input x and Bob an input y such that $f(x) = 1 - f(y)$, we construct a sabotaged input $z_{x,y}$ that is consistent with x and y as follows:

$$z_{x,y}(i) = \begin{cases} x(i) & \text{if } x(i) = y(i) \\ * & \text{otherwise.} \end{cases}$$

On the input $z_{x,y}$, we know that a decision tree sampled from the distribution given by the RS protocol succeeds in finding a $*$ or $\dagger$ with probability $\geq 2/3$. The CG^{pub} protocol is as follows: using public randomness, Alice and Bob sample a decision tree from the RS protocol and follow the path on the decision tree according to their respective inputs for at most $\mathsf{RS}(f)$ steps. With probability at least $2/3$ the randomly chosen tree finds a $*$ on input $z_{x,y}$ in $\mathsf{RS}(f)$ steps. Since the sabotaged input $z_{x,y}$ is consistent with both Alice's and Bob's input, the path on x and y on the decision tree is the same as that on $z_{x,y}$ until they reach a place where they differ (or encounter a $*$ in $z_{x,y}$). Alice and Bob pick a random position t such that $1 \leq t \leq \mathsf{RS}(f)$ and output the t^{th} query made in the corresponding paths on the tree. With probability $\frac{1}{\mathsf{RS}(f)}$, it is place corresponding to a $* \in z_{x,y}$ and they succeed in finding a place where the inputs differ. This gives a success probability $\geq 2/3\frac{1}{\mathsf{RS}(f)}$ as the random decision tree sampled finds a $*$ on the sabotaged input $z_{x,y}$ with probability $\geq 2/3$. □

5.4 Upper and lower bounds for private coin certificate games

We first observe that the following formulation is equivalent to $\mathsf{CG}^{\text{priv}}$. The essential idea is rescaling, and the objective function gets squared because the constraints are quadratic.

Proposition 5.9 (Equivalent formulation for $\mathsf{CG}^{\text{priv}}$)**.** *For any (possibly partial) function f,*

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

Proof. We will first show that the value of the objective function in the formulation in terms of weights is at most $\mathsf{CG}^{\text{priv}}$. Let p be an optimal probability distribution that achieves $\mathsf{CG}^{\text{priv}}(f)$ and let

$$\Delta = \min_{x,y:f(x)=1-f(y)} \sum_{i:x_i \neq y_i} p_{x,i} p_{y,i} = \frac{1}{\mathsf{CG}^{\text{priv}}(f)}.$$

We construct the following weight scheme using p, $w_{x,i} = \frac{p_{x,i}}{\sqrt{\Delta}}$ and this is a feasible solution for the above formulation since $\forall x, y$ such that $f(x) = 1 - f(y)$,

$$\sum_{i:x_i \neq y_i} w_{x,i} w_{y,i} = \frac{1}{\Delta} \sum_{i:x_i \neq y_i} p_{x,i} p_{y,i} \geq \frac{\Delta}{\Delta} = 1$$

We now have

$$\min_{\{w'_{x,i}\}} \max_x \left\{ \sum_{i \in [n]} w'_{x,i} \right\}^2 \leq \max_x \left\{ \sum_{i \in [n]} w_{x,i} \right\}^2 = \max_x \left\{ \sum_{i \in [n]} \frac{p_{x,i}}{\sqrt{\Delta}} \right\}^2 = \frac{1}{\Delta} = \mathsf{CG}^{\text{priv}}(f)$$

For the other direction, let w be an optimal weight scheme w that minimises $\max_x \sum_i w_{x,i}$. We construct the following family of probability distributions: $p_{x,i} = \frac{w_{x,i}}{\sum_j w_{x,j}}$ This gives the following.

$$\begin{aligned}
\mathsf{CG}^{\text{priv}}(f) &\leq \max_{\substack{x,y \\ f(x)=1-f(y)}} \frac{1}{\sum_{i:x_i \neq y_i} p_{x,i} p_{y,i}} \\
&= \max_{\substack{x,y \\ f(x)=1-f(y)}} \frac{\sum_j w_{x,j} \sum_j w_{y,j}}{\sum_{i:x_i \neq y_i} w_{x,i} w_{y,i}} \\
&\leq \max_{\substack{x,y \\ f(x)=1-f(y)}} \sum_j w_{x,j} \sum_j w_{y,j}.
\end{aligned}$$

Thus we have $\mathsf{CG}^{\text{priv}}(f) \leq \max_x \left\{ \sum_j w_{x,j} \right\}^2$. □

We show that the following relations hold for $\mathsf{CG}^{\text{priv}}$.

Theorem 5.10. *For any total Boolean function f,*

1. $\mathsf{MM}(f)^2 \leq \mathsf{CG}^{\text{priv}}(f)$
2. $\mathsf{R}_0(f) \leq \mathsf{CG}^{\text{priv}}(f) \leq O(\mathsf{EC}(f)^2)$ *[28]*
3. $\mathsf{CG}^{\text{priv}}(f) \leq O(\mathsf{CG}^{\text{pub}}(f)^2 \mathsf{s}(f))$ *[28]*
4. $\mathsf{CG}^{\text{priv}}(f) \leq \mathsf{C}^0(f)\mathsf{C}^1(f)$

The first and last items also hold for partial functions. However, the "Greater than Half" function (see section B) is an example of a partial function that would violate item 4 using the alternate definitions $\mathsf{C}^{\{0,*\}}$ and $\mathsf{C}^{\{1,*\}}$.

Proof. **Item 1** Let p be an optimal solution for $\mathsf{CG}^{\text{priv}}(f)$ so that $\omega(p; x, y) \geq \frac{1}{\mathsf{CG}^{\text{priv}}(f)}$ for all x, y satisfying $f(x) = 1 - f(y)$. Using the same assignment for MM (Definition 4.1), it is the case that

$$\begin{aligned}
\frac{1}{\mathsf{MM}(f)^2} &\geq \min_{\substack{x \in f^{-1}(0) \\ y \in f^{-1}(1)}} \left(\sum_{i:x_i \neq y_i} \sqrt{p_{x,i} p_{y,i}} \right)^2 \\
&\geq \min_{\substack{x \in f^{-1}(0) \\ y \in f^{-1}(1)}} \sum_{i:x_i \neq y_i} p_{x,i} p_{y,i}
\end{aligned}$$

so $\mathsf{MM}(f)^2 \leq \mathsf{CG}^{\text{priv}}(f)$.

Item 2 From Proposition 5.9, the formulation of $\sqrt{CG}$ is a relaxation of the definition of EC, where the constraint $w_{x,i} \leq 1$ is dropped in $\sqrt{CG}$, giving the second inequality $\sqrt{CG}(f) \leq \mathsf{EC}(f)$.

For the first inequality, it was shown in [28] that $\mathsf{R}_0 \leq O(\mathsf{EC}^2)$. However, their proof does not make use of the constraints $w_{x,i} \leq 1$. Therefore, their proof already shows that $\mathsf{R}_0(f) \leq O(\mathsf{CG}^{\text{priv}}(f))$.

Item 3 Jain et al. [28] showed that $\mathsf{EC}(f)^2 \leq O(\mathsf{FC}(f)^2 \mathsf{s}(f))$. From the previous item $\mathsf{CG}^{\text{priv}}(f) \leq O(\mathsf{EC}(f)^2)$, and $\mathsf{FC}(f) = O(\mathsf{CMM}(f))$ [7], $\mathsf{CMM}(f) \leq \mathsf{CG}^{\text{ns}}(f) \leq \mathsf{CG}^{\text{pub}}(f)$ from Theorem 6.2 and Proposition 2.7. We get the desired result by combining these inequalities.

Item 4 It is easy to see that $\mathsf{CG}^{\text{priv}}(f) \leq \mathsf{C}^0(f) \cdot \mathsf{C}^1(f)$: on input x, each player outputs uniformly at random some index i in a minimal certificate for their input. The certificates must intersect in at least one index, otherwise we could simultaneously fix the value of f to 0 and to 1 by fixing both certificates. The strategy therefore succeeds when both players output the same index in the intersection, which occurs with probability at least $\frac{1}{\mathsf{C}^0(f)} \frac{1}{\mathsf{C}^1(f)}$. This argument remains valid for partial functions, however the "Greater than Half" function (see section B) is an example of a partial function that would violate item 4 using the alternate definitions $\mathsf{C}^{\{0,*\}}$ and $\mathsf{C}^{\{1,*\}}$. □

6 Lower bounds on quantum certificate game complexity

In this section, we give a very short and simple proof that the classical adversary (CMM) 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). By running this game several times, 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.

In order to give a formal proof, we show that $\mathsf{CG}^{\mathrm{ns}}(\text{Promise-}\mathsf{OR}) \geq n$. Since $\mathsf{CG}^{\mathrm{ns}}(f) \leq \mathsf{CG}^{*}(f)$ for every f, the following proposition implies that $\mathsf{CG}^{*}(\text{Promise-}\mathsf{OR}_n) \geq n$.

Proposition 6.1. $\mathsf{CG}^{\mathrm{ns}}(\textit{Promise-}\mathsf{OR}_n) \geq n$.

Proof of Proposition 6.1. We give a feasible solution to the dual, composed of a hard distribution μ and an assignment to the variables $\gamma_{i,j,x,y}$ that satisfy the constraints of the dual given in Proposition 3.2.

Let $\delta = \frac{1}{n}$, $x = 0^n$, and consider $\mu_{xy} = \frac{1}{n}$ when $y = x^{(i)}$ (x with the i^{th} bit flipped to 1), and 0 everywhere else. To satisfy the correctness constraint, we use γ to pick up weight $1/n$ whenever a strategy AB fails on some pair $x, x^{(i)}$. To do this, we define $\gamma_{i,j,x,x^{(i)}} = \frac{1}{n}$ for all $j \neq i$ (and 0 everywhere else). To see that this satisfies the constraints, consider any strategy AB and let $i = A(x)$ be A's output on x.

Case 1: If $B(x^{(i)}) = i$ then AB is correct on $x, x^{(i)}$, but cannot be correct on any other input pair with non-zero weight under μ. Therefore,

$$\sum_{x,y' : A(x)=B(y')=i \text{ and } x_i \neq y_i} \mu_{x,y} = \frac{1}{n} \quad \text{and} \quad \sum_{x,y'} \gamma_{A(x),B(y'),x,y'} = 0.$$

Case 2: If $B(x^{(i)}) = j \neq i$, then AB is incorrect on all non-zero weight input pairs, and we have

$$\sum_{x,y' : A(x)=B(y')=i \text{ and } x_i \neq y_i} \mu_{x,y} = 0 \quad \text{and} \quad \sum_{x,y'} \gamma_{A(x),B(y'),x,y'} = \frac{1}{n}.$$

Since $\delta = \frac{1}{n}$ this is satisfying assignment, which shows that

$$\mathsf{CG}^{\mathrm{ns}}(\text{Promise-}\mathsf{OR}) = \omega^{\mathrm{ns}}(R_{\text{Promise-}\mathsf{OR}})^{-1} \geq n.$$

□

Note that $\mathsf{Q}(\text{Promise-}\mathsf{OR})$ is $\Theta(\sqrt{n})$ [23, 12]. Thus, Promise-OR shows that there exist a function for which $\mathsf{CG}^{*}(f) = \omega(\mathsf{Q}(f))$ (as opposed to the randomized model where $\mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{R}(f))$. On the other hand, note that the function constructed by [3] demonstrates that there exists a total Boolean function f with $\mathsf{C}(f) = O(\sqrt{\mathsf{Q}(f)})$; this f also shows that $\mathsf{CG}^{\mathrm{pub}}(f)$ could be as small as $O(\sqrt{\mathsf{Q}(f)})$.

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. However, using a different technique, we can prove an even stronger result. We do this by going back to the original definition of $\mathsf{CG}^{\mathrm{ns}}$ (Definition 2.6) and giving a very simple proof that $\mathsf{CG}^{\mathrm{ns}}$ is an upper bound on CMM.

Theorem 6.2. *For any (possibly partial) Boolean function f, $\mathsf{CMM}(f) \leq \mathsf{CG}^{\mathrm{ns}}(f)$.*

Proof. Let $p(i,j|x,y)$ be the distribution over outcomes in an optimal nonsignaling strategy for $\mathsf{CG}^{\mathrm{ns}}(f)$. 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, so $\min\{p(i|x), p(i|y)\} \geq p(i,i|x,y)$.

$$\begin{aligned}\mathsf{CMM}(f) &= \min_p \max_{\substack{x,y\in S \\ f(x)=1-f(y)}} \frac{1}{\sum_{i:x_i\neq y_i} \min\{p(i|x), p(i|y)\}} \\ &\leq \min_p \max_{\substack{x,y\in S \\ f(x)=1-f(y)}} \frac{1}{\sum_{i:x_i\neq y_i} p(i,i|x,y)}\end{aligned}$$

Since we have that $\sum_{i:x_i\neq y_i} p(i,i|x,y) \geq \frac{1}{\mathsf{CG}^{\mathrm{ns}}(f)}$ for all x,y such that $f(x) = 1-f(y)$, $\mathsf{CMM}(f) \leq \mathsf{CG}^{\mathrm{ns}}(f)$. □

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.

7 Closing the loop

In this section we will show that all of $\mathsf{CG}^{\mathrm{pub}}$, CG^*, $\mathsf{CG}^{\mathrm{ns}}$, and CMM are actually asymptotically equal.

Theorem 7.1. *For any (possibly partial) Boolean function f,*

$$\mathsf{CG}^{\mathrm{pub}}(f) = \Theta(\mathsf{CG}^*(f)) = \Theta(\mathsf{CG}^{\mathrm{ns}}(f)) = \Theta(\mathsf{CMM}(f)).$$

The key idea is to apply the *correlated sampling* technique of Holenstein [25]. We use the following formulation from the Rao–Yehudayoff textbook [49, Lemma 7.5]. Here, *total variation distance* between distributions p and q is defined by $\mathrm{TV}(p,q) := \frac{1}{2}\sum_i |p(i) - q(i)|$.

Lemma 7.2 (Correlated sampling [25, 49])**.** *Suppose Alice is given as input a distribution p over a set $\mathcal{U}$, and Bob is given as input a distribution q over $\mathcal{U}$. There is a protocol using public randomness and no communication with the following guarantees.*

- *Alice outputs a value X which is distributed according to p.*
- *Bob outputs a value Y which is distributed according to q.*
- *We have*[4] $\Pr[X = Y] \geq \frac{1}{2}(1 - \mathrm{TV}(p,q))$.

Proof of Theorem 7.1. Given Theorem 6.2, it remains to prove the inequality $\mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{CMM}(f))$ by designing a protocol for f that wins with probability $\Omega(1/\mathsf{CMM}(f))$. Recall from Definition 4.2 that

$$\mathsf{CMM}(f) = \min_p \max_{\substack{x\in f^{-1}(1) \\ y\in f^{-1}(0)}} \frac{1}{\sum_{i:x_i\neq y_i} \min\{p_x(i), p_y(i)\}}. \tag{1}$$

Starting with a distribution p_x over $[n]$, we define distributions p'_x and p''_x over $[n]\times\{0,1\}$ as follows. To define p'_x, first sample $i \sim p_x$ and then output $(i, x_i) \sim p'_x$. To define p''_x, first sample $i \sim p_x$ and then

[4] The original formulation from [49, Lemma 7.5] states the incomparable bound $\Pr[X \neq Y] \leq 2\,\mathrm{TV}(p,q)$ (which is useful when TV is small). However, it is straightforward to inspect the protocol and see that it also satisfies our lower bound (which is useful when TV is close to 1).

output $(i, 1-x_i) \sim p''_x$. (Note how p'_x and p''_x are the same except for the flipped bit.) We can now write the denominator in (1) as

$$\begin{aligned}\sum_{i:x_i \neq y_i} \min\{p_x(i), p_y(i)\} &= \sum_{\alpha \in [n]\times\{0,1\}} \min\{p'_x(\alpha), p''_y(\alpha)\} \\ &= \sum_{\alpha} \left(\tfrac{1}{2}(p'_x(\alpha) + p''_y(\alpha)) - \tfrac{1}{2}|p'_x(\alpha) - p''_y(\alpha)| \right) \\ &= 1 - \mathrm{TV}(p'_x, p''_y).\end{aligned}$$

The $\mathsf{CG}^{\mathrm{pub}}$ protocol for f is now defined from the optimal p in (1) as follows. On input (x, y) the players use the protocol from Lemma 7.2 to compute correlated samples $X := (i_X, b_X) \sim p'_x$ and $Y := (i_Y, b_Y) \sim p''_y$, respectively, and then they output (i_X, i_Y). The players win the game with probability

$$\Pr[X = Y] \geq \tfrac{1}{2}(1 - \mathrm{TV}(p'_x, p''_y)) \geq \Omega(1/\mathsf{CMM}(f)).$$

□

Combining the above theorem with the result of [7], which states that $\mathsf{FC}(f) = \Theta(\mathsf{CMM}(f))$ for total f, we get the following immediate corollary.

Corollary 7.3. *For any total Boolean function f, $\mathsf{CG}^{\mathrm{pub}}(f) = \Theta(\mathsf{FC}(f))$.*

8 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.

$$\mathsf{MM}_{[1]}(f) = \min_{\{w_{x,i}\}} \max_{x} \sum_{i} w_{x,i} \text{ such that } w_{x,i} w_{x^{(i)},i} \geq 1 \quad \forall x, i \text{ with } f(x) = 1 - f(x^{(i)}) \tag{2}$$

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

Similarly to the proof of Proposition 5.9 it can be shown that this is equal to the following formulation, which we include for comparison with some of our other definitions.

$$\mathsf{MM}_{[1]}(f) := \min_{p} \max_{\substack{x,y \in f^{-1}(0)\times f^{-1}(1) \\ d(x,y)=1}} \frac{1}{\sum_{i:x_i \neq y_i} \sqrt{p_{x,i} p_{y,i}}} = \min_{p} \max_{x,i:f(x)=1-f(x^{(i)})} \frac{1}{\sqrt{p_{x,i} p_{x^{(i)},i}}} \tag{3}$$

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 8.1. *(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 $\mathsf{CG}^{\mathrm{priv}}$ and show that they characterize sensitivity and λ^2, respectively, up to constant factors.

Definition 8.2 (Single-bit private coin certificate game complexity)**.** *For any (possibly partial) Boolean function f with $\mathsf{s}(f) \neq 0$*

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

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

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

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

Theorem 8.4. *For any (possibly partial) Boolean function $f : \{0,1\}^n \to \{0,1\}$ with $\mathsf{s}(f) \neq 0$ $\mathsf{CG}^{\mathrm{pub}}_{[1]}(f) = \Theta(\mathsf{s}(f))$.*

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 5.2).

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 3.1. 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. □

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

Definition 8.5. *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 8.6. *For any (possibly partial) Boolean function $f : \{0,1\}^n \to \{0,1\}$ with $\mathsf{s}(f) \neq 0$, $\mathsf{s}(f) = \mathsf{FC}_{[1]}(f) = \mathsf{EC}_{[1]}(f)$.*

Proof. We can think of the values $v_{x,i}$ and $w_{x,i}$ as weights assigned to the edges of the Boolean hypercube. We say that an edge $(x, x^{(i)})$ is sensitive (with respect to the function f) if $f(x) = 1 - f(x^{(i)})$. First notice, that both definitions require to place weight at least 1 on each sensitive edge, thus both $\mathsf{FC}_{[1]}(f)$ and $\mathsf{EC}_{[1]}(f)$ are at least $s(f)$. On the other hand, placing weight 1 on each sensitive edge and weight 0 on every other edge satisfies the constraints of both definitions, thus both $\mathsf{FC}_{[1]}(f)$ and $\mathsf{EC}_{[1]}(f)$ are at most $s(f)$. □

Thus we get the following.

Corollary 8.7. *For any (possibly partial) Boolean function $f : \{0,1\}^n \to \{0,1\}$ with $\mathsf{s}(f) \neq 0$, $\mathsf{s}(f) = \mathsf{FC}_{[1]}(f) = \mathsf{EC}_{[1]}(f) = \Theta(\mathsf{CG}^{\mathrm{pub}}_{[1]}(f))$.*

In case of the single-bit version of private coin certificate game complexity we have:

Theorem 8.8. *For any (possibly partial) Boolean function $f : \{0,1\}^n \to \{0,1\}$ with $\mathsf{s}(f) \neq 0$, $\mathsf{CG}^{\mathrm{priv}}_{[1]}(f) = \lambda^2$.*

Proof. Comparing the definitions of $\mathsf{MM}_{[1]}$ and $\mathsf{CG}^{\mathrm{priv}}_{[1]}$ (e.g. the formulation of $MM_{[1]}$ in Equation (3) with Definition 8.2) notice that $\sqrt{\mathsf{CG}^{\mathrm{priv}}_{[1]}} = \mathsf{MM}_{[1]}$. (One can also restate Definition 8.2 with weights as in Proposition 5.9 and compare that version with the formulation of $\mathsf{MM}_{[1]}$ in Equation (2).) The statement then follows from Theorem 8.1. □

9 Separations between classical adversary and randomized query complexity for partial functions

For a partial function f, it is even possible to have an exponential separation between $\mathsf{R}(f)$ and $\mathsf{CG}^{\mathrm{pub}}(f)$.

Lemma 9.1. *There is a partial Boolean function $f\colon \{0,1\}^n \to \{0,1,*\}$ such that*

$$\mathsf{R}(f) \geq \Omega(n) \qquad \textit{but} \qquad \mathsf{CG}^{\mathrm{pub}}(f) \leq O(1).$$

Proof. Fix any error-correcting code $C \subseteq \{0,1\}^n$ of constant rate and constant relative distance, that is, $|C| \geq 2^{\Omega(n)}$ and for every distinct $x, y \in C$ we have that x and y differ in $\Omega(n)$ coordinates. (For example, we can use a Justesen code or a random code.) Note that any partial function $f\colon \{0,1\}^n \to \{0,1,*\}$ with domain $f^{-1}(\{0,1\}) = C$ has $\mathsf{CG}^{\mathrm{pub}}(f) = O(1)$. Indeed, both players simply output a uniform random coordinate.

Finally, we show that if $f\colon C \to \{0,1\}$ is chosen uniformly at random, then $\mathsf{R}(f) \geq \Omega(n)$ with high probability. Indeed, let $\mathcal{T}$ be a randomized decision tree of depth d computing f. That is, $\mathcal{T}$ is a probability

distribution over deterministic depth-d decision trees. By standard randomness sparsification techniques (e.g., Newman's theorem [41]) we may assume that $\mathcal{T}$ is a uniform distribution over $n^{O(1)}$ many deterministic trees. Each tree $T \in \mathrm{supp}(\mathcal{T})$ can be encoded as a $O(\binom{n}{d})$-bit string (for each leaf of T, encode the root-to-leaf path). Hence $\mathcal{T}$ can be encoded as a string of length $n^{O(1)} \cdot O(\binom{n}{d})$. However, a random function f needs $\Omega(|C|) = 2^{\Omega(n)}$ bits to describe it, with high probability. It follows that $d \geq \Omega(n)$. □

An example of an explicit function to separate R and $\mathsf{CG}^{\mathrm{pub}}$ is the approximate index function constructed by Ben-David and Blais [13]. The proof of this exponential separation is given in Appendix A.

We know that $\mathsf{CG}^{\mathrm{pub}}$ and FC cannot be asymptotically different for a total function. Though, there is a partial function, GTH (defined by Ambainis et al. [7], for definition see Appendix B), for which FC is constant [7] but $\mathsf{CG}^{\mathrm{pub}}$ is $\Theta(n)$ (follows from Theorem 6.2 and $\mathsf{CMM}(\mathsf{GTH}) = \Theta(n)$ [7]).

10 Relations and separations between measures

Understanding the relationships between the various models of certificate game complexity would 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 first natural separation to consider is the relation between $\mathsf{CG}^{\mathrm{priv}}$ and $\mathsf{CG}^{\mathrm{pub}}$.

Corollary 10.1. *For any total Boolean function f, $\mathsf{CG}^{\mathrm{pub}}(f) \leq \mathsf{CG}^{\mathrm{priv}}(f) \leq O(\mathsf{CG}^{\mathrm{pub}}(f)^3)$.*

Proof. The first inequality follows from the definitions and the second inequality follows from

$$\mathsf{CG}^{\mathrm{priv}} \leq O(\mathsf{EC}(f)^2) \leq O(\mathsf{FC}^2(f) \cdot \mathsf{s}(f)) \leq O(\mathsf{CG}^{\mathrm{ns}}(f)^2 \cdot \mathsf{s}(f)) \leq O(\mathsf{CG}^{\mathrm{ns}}(f)^3),$$

where the first inequality follows from Theorem 5.10, the second was proved in [28] and the last two inequality follows from Theorem 6.2. □

Note that the above corollary follows from $\mathsf{CG}^{\mathrm{priv}} \leq O(\mathsf{CG}^{\mathrm{pub}}(f)^2 \cdot \mathsf{s}(f))$ (Theorem 5.10)

Open Problem 1 : Is there a $c < 3$ such that $\mathsf{CG}^{\mathrm{priv}}(f) \leq O(\mathsf{CG}^{\mathrm{pub}}(f)^c)$?

There are total functions f, for which $\mathsf{CG}^{\mathrm{priv}}(f) = \Theta(\mathsf{CG}^{\mathrm{pub}}(f)^2)$. One such example is the Tribes function. For $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}} := \mathsf{OR}_{\sqrt{n}} \circ \mathsf{AND}_{\sqrt{n}}$, we have $\mathsf{CG}^{\mathrm{pub}}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(\sqrt{n})$, and $\mathsf{CG}^{\mathrm{priv}}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(n)$.

Proof. Firstly, note that since the functions OR and AND has full sensitivity, from Theorem 6.2 we have $\mathsf{CG}^{\mathrm{pub}}(\mathsf{OR}_{\sqrt{n}}) = \mathsf{CG}^{\mathrm{ns}}(\mathsf{OR}_{\sqrt{n}}) = \Theta(\sqrt{n})$.

Also, the sensitivity of $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ is $\Theta(\sqrt{n})$ and hence from Theorem 6.2 we have that the $\mathsf{CG}^{\mathrm{pub}}$ and $\mathsf{CG}^{\mathrm{ns}}$ of $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ is $\Omega(\sqrt{n}$. The upper bound follows Theorem 5.5 and the fact that the certificate complexity of $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$ is at most $\sqrt{n}$. But we have also provided a separate proof (Theorem 5.2) for the upper bound of the $\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$. Thus we have $\mathsf{CG}^{\mathrm{ns}}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \mathsf{CG}^{\mathrm{pub}}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(\sqrt{n})$.

Now for the certificate game complexity with shared randomness, from Theorem 5.10 we know that $\mathsf{CG}^{\mathrm{priv}}$ is bounded below by R_0 and we know that $\mathsf{R}_0(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(n)$. On the other, Theorem 5.10 also helps us to upper bound $\mathsf{CG}^{\mathrm{priv}}$ by $(\mathsf{EC})^2$, and since $\mathsf{EC}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) \leq \mathsf{C}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) \leq \sqrt{n}$, so we have that $\mathsf{CG}^{\mathrm{priv}}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(n)$. □

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 $\mathsf{CG}^{\mathrm{priv}}$ and $\mathsf{CG}^{\mathrm{pub}}$. This is because $\mathsf{CG}^{\mathrm{priv}}(f) = \Omega((\mathsf{MM}(f))^2)$, from Theorem 5.10, and $\mathsf{MM}(f) = \Omega(\lambda(f))$. Thus for any such functions $\mathsf{CG}^{\mathrm{priv}}$ is $\Theta(n^2)$ while $\mathsf{CG}^{\mathrm{pub}}$ is $\Theta(n)$.

One possible attempt to tighten the relation between $\mathsf{CG}^{\mathrm{priv}}$ and $\mathsf{CG}^{\mathrm{pub}}$ is to modify the inequality $\mathsf{CG}^{\mathrm{priv}} = O(\mathsf{EC}^2)$. We observe that the bound $\mathsf{CG}^{\mathrm{priv}}(f) \leq O(\mathsf{EC}(f)^2)$ is indeed tight (Parity function). Though, we could possibly find a better relation between EC and $\mathsf{CG}^{\mathrm{pub}}$. Since $\mathsf{EC}(f) \leq C(f)$, we know that $\mathsf{EC}(F) = O(\mathsf{CG}^{\mathrm{pub}}(f)^2)$.

Open Problem 2 : What is the minimum c such that $\mathsf{EC}(f) \leq O(\mathsf{CG}^{\text{pub}}(f)^c)$?

Note that if $\mathsf{CG}^{\text{pub}} = \Theta(\mathsf{EC})$ we have $R_0 \leq O((\mathsf{CG}^{\text{pub}})^2) = O(\mathsf{FC}^2)$, which is a well-known open problem [28]. Theorem 5.10 shows that $\mathsf{R}_0(f) \leq O(\mathsf{CG}^{\text{priv}}(f))$ (though parity shows that these two measures need not be equal). A quadratic bound on $\mathsf{CG}^{\text{priv}}$ with respect to CG^{pub} will also settle the well-known open problem mentioned above.

Another possible direction to tighten the relation between $\mathsf{CG}^{\text{priv}}$ and CG^{pub} is to improve the inequality $\mathsf{CG}^{\text{priv}} = \Omega(\mathsf{MM}^2)$.

Open Problem 3 : What is the biggest separation between $\mathsf{CG}^{\text{priv}}(f)$ and $\mathsf{MM}(f)$?

To the best of our knowledge, the best upper bound on $\mathsf{CG}^{\text{priv}}$ for total functions in terms of MM is

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

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 $\mathsf{CG}^{\text{priv}}$ and MM in this direction is cubic: there is a total Boolean function f for which $\mathsf{CG}^{\text{priv}}(f) \leq \Omega(\mathsf{EC}(f)^{3/2})$. 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,

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

where the first inequality follows from Theorem 5.10 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 5.10) for any total Boolean function f, $(\mathsf{MM}(f))^2 \leq O(\mathsf{CG}^{\text{priv}}(f))$ and this inequality is in fact tight (for any total function with full spectral sensitivity, such as parity). In fact, the two quantities, $\mathsf{CG}^{\text{priv}}$ and $(\mathsf{MM})^2$, are asymptotically identical for symmetric functions [39].

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

Corollary 10.2 ([28, 22])**.** *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 $C^0(f) \cdot C^1(f) = \Omega(\mathsf{CG}^{\text{priv}}(f)^{3/2})$.*

Proof. In [28, Theorem 11] they constructed a total function $f : \{0,1\}^N \to \{0,1\}$ such that $\mathsf{C}^0(f) = \Theta(N)$ and $\mathsf{C}^1(f) = \Theta(\sqrt{N})$ and $\mathsf{EC}(f) = \Theta(\sqrt{N})$. Thus, from Theorem 5.10 we have $\mathsf{CG}^{\text{priv}}(f) = \Theta(\mathsf{EC}(f))^2 \leq \Theta(N)$. Thus we have the corollary. □

The separations between single bit version and general version of certificate games is pretty interesting too. 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 [26] 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 8.4, designing a strategy for CG^{pub} using $\mathsf{CG}^{\text{pub}}_{[1]}$ may help us solve the sensitivity-block sensitivity conjecture.

Open Problem 4 : What is the smallest c such that, for any Boolean function f, $\mathsf{CG}^{\text{pub}}(f) = O(\mathsf{CG}^{\text{pub}}_{[1]}(f)^c)$?

Note that $\mathsf{CG}^{\text{pub}}(f) = O(\mathsf{CG}^{\text{pub}}_{[1]}(f)^2)$ is equivalent to $\mathsf{bs}(f) \leq O(\mathsf{s}(f)^2)$ (the separation between FC and s is same as bs and s by [33]). 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 [26], we already know that $\mathsf{CG}^{\mathrm{pub}}(f) = O(\mathsf{CG}^{\mathrm{pub}}_{[1]}(f)^4)$ for any total Boolean function f.

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. RM would like to thank IRIF, Paris for hosting him where part of the work was done. 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. MG is supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number MB22.00026.

References

[1] Scott Aaronson. Lower bounds for local search by quantum arguments. *SIAM Journal on Computing*, 35(4):804–824, 2006.

[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, page 863–876, 2016.

[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.

[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), Sep 2017.

[7] Andris Ambainis, Martins Kokainis, Krisjanis Prusis, and Jevgenijs Vihrovs. All Classical Adversary Methods are Equivalent for Total Functions. In *35th Symposium on Theoretical Aspects of Computer Science (STACS 2018)*, volume 96, pages 8:1–8:14, 2018.

[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.

[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*, page 1303–1316, 2021.

[11] Mohammad Bavarian, Badih Ghazi, Elad Haramaty, Pritish Kamath, Ronald L. Rivest, and Madhu Sudan. Optimality of correlated sampling strategies. *Theory of Computing*, 16(12):1–18, 2020.

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

[13] 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.

[14] 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.

[15] Shalev Ben-David and Robin Kothari. Randomized query complexity of sabotaged and composed functions. *Theory of Computing*, 14(5):1–27, 2018.

[16] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik*, 46(4-5):493–505, 1998.

[17] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014.

[18] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald de Wolf. Nonlocality and communication complexity. *Rev. Mod. Phys.*, 82:665–698, Mar 2010.

[19] Sourav Chakraborty. On the sensitivity of cyclically-invariant boolean functions. In *Proceedings of the Annual IEEE Conference on Computational Complexity*, volume 13, pages 163 – 167, 07 2005.

[20] 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.

[21] 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.

[22] Justin Gilmer, Michael Saks, and Srikanth Srinivasan. Composition limits and separating examples for some boolean function complexity measures. *Combinatorica*, 36(3):265–311, 2016.

[23] 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.

[24] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963.

[25] Thomas Holenstein. Parallel repetition: Simplification and the no-signaling case. *Theory of Computing*, 5(8):141–172, 2009.

[26] Hao Huang. Induced subgraphs of hypercubes and a proof of the sensitivity conjecture. *Annals of Mathematics*, 190(3):949–955, 2019.

[27] Rahul Jain and Hartmut Klauck. The partition bound for classical communication complexity and query complexity. In *Proceedings of the Annual IEEE Conference on Computational Complexity*, 10 2009.

[28] 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, jan 2020.

[29] Mauricio Karchmer and Avi Wigderson. Monotone circuits for connectivity require super-logarithmic depth. *SIAM J. Discrete Math.*, 3:255–265, 01 1990.

[30] 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.

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

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

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

[34] Sophie Laplante, Troy Lee, and Mario Szegedy. The quantum adversary method and classical formula size lower bounds. *Comput. Complex.*, 15(2):163–196, 2006.

[35] 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.

[36] Troy Lee, Rajat Mittal, Ben Reichardt, Robert Spalek, and Mario Szegedy. Quantum query complexity of state conversion. In *Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS*, pages 344 – 353, 11 2011.

[37] Jiří Matoušek and Jan Vondrák. The probabilistic method lecture notes, March 2008.

[38] Gatis Midrijanis. Exact quantum query complexity for total Boolean functions. Technical Report quant-ph/0403168, arXiv, 2004.

[39] Rajat Mittal, Sanjay S Nair, and Sunayana Patro. Lower bounds on quantum query complexity for symmetric functions. Technical Report quant-ph/2110.12616, arXiv, 2021.

[40] Michael Mitzenmacher and Eli Upfal. *Probability and Computing*. Cambridge University Press, 2005.

[41] Ilan Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39(2):67–71, July 1991.

[42] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[43] Noam Nisan. CREW PRAMS and decision trees. In *Symposium on Theory of Computing*, STOC '89, page 327–335, 1989.

[44] Noam Nisan and Mario Szegedy. On the degree of boolean functions as real polynomials. *Computational Complexity*, 4:301–313, 1994.

[45] Carlos Palazuelos and Thomas Vidick. Survey on nonlocal games and operator space theory. *Journal of Mathematical Physics*, 57, 12 2015.

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

[47] K. Prūsis. Personal communication, 2022.

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

[49] Anup Rao and Amir Yehudayoff. *Communication Complexity: And Applications*. Cambridge University Press, 2020.

[50] David Rubinstein. Sensitivity vs. block sensitivity of boolean functions. *Combinatorica*, 15(2):297–299, 1995.

[51] S. Sanyal. Personal communication, 2022.

[52] Robert Špalek and Mario Szegedy. All quantum adversary methods are equivalent. *Theory of Computing*, 2(1):1–18, 2006.

[53] 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.

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

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

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

A Approximate Index: Exponential gap between R and $\mathsf{CG}^{\mathrm{pub}}$ 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 [13] (please refer to [13] 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 is interesting to see whether $\mathsf{CG}^{\mathrm{pub}}$ is also a lower bound on noisyR.

Open Problem 5 : Is it the case that for all f, $\mathsf{CG}^{\mathrm{pub}}(f) \leq O(\mathsf{noisyR}(f))$?

Ben-David and Blais [13] constructed the approximate index function, which is the only function known where noisyR and R are different. But the approximate index function that they construct is not a total Boolean function but a partial 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 A.1. $\mathsf{ApInd}_k : \{0,1\}^k \times \{0,1,2\}^{2^k} \to \{0,1,*\}$ *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 $\mathsf{CG}^{\mathrm{pub}}$ could be a lower bound on noisyR, we show the following theorem.

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

Sketch of Proof of Theorem A.2. We can use the hashing framework to show an exponential separation between R and $\mathsf{CG}^{\mathrm{pub}}$ for Approximate Index, a partial function.

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 3.1 (we state it in a more general form).

Lemma A.3. *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 $\mathsf{CG}^{\text{pub}}(f) \leq O(t^2)$.*

Proof. Let A_x and B_y be sets of size L guaranteed by the statement of the lemma. We can assume that for t in the statement of the lemma $20 \leq t \leq 0.1L$ holds, since $O(L^2)$ is a trivial upper bound on $\mathsf{CG}^{\text{pub}}(f)$. Let S be a finite set with $|S| = \lfloor \frac{L}{2t} \rfloor > 1$. Let z be a fixed element of S (e.g. the first element of S) given as part of the specification of the protocol. (Note that z could also be selected using shared randomness, but this is not necessary.)

Let $T \subseteq [n]$ be a set of possible outputs that contains the sets A_x and B_y for every $x \in f^{-1}(0)$ and $y \in f^{-1}(1)$. Let $h : T \to S$ be a random hash function such that for each $i \in T$, $h(i)$ is selected independently and uniformly from S. The players select such h using shared randomness. Then, on input x, Alice outputs a uniformly random element from $h^{-1}(z) \cap A_x$(if this set is empty, she outputs an arbitrary element). On input y, Bob outputs a uniformly random element of $h^{-1}(z) \cap B_y$ (if this set is empty, he outputs an arbitrary element).

Claim A.4. *For any $x \in f^{-1}(0)$ and $y \in f^{-1}(1)$,*

$$Pr[h^{-1}(z) \cap A_x \cap B_y = \emptyset] \leq \frac{1}{e^2}$$

where the probability is over the choice of the hash function h.

Proof. Notice that our setting implies that for any $x \in f^{-1}(0)$ and $y \in f^{-1}(1)$, $|A_x \cap B_y| \geq \frac{L}{t} \geq 2|S|$. Thus, $Pr[h^{-1}(z) \cap A_x \cap B_y = \emptyset] = (1 - \frac{1}{|S|})^{|A_x \cap B_y|} \leq (1 - \frac{1}{|S|})^{2|S|} \leq \frac{1}{e^2}$. □

Claim A.5. *For any $x \in f^{-1}(0)$ and $y \in f^{-1}(1)$, $Pr[|h^{-1}(z) \cap A_x| > 3t] \leq \epsilon$ and $Pr[|h^{-1}(z) \cap B_y| > 3t] \leq \epsilon$, where $\epsilon = e^{-0.1t}$.*

Proof. Notice that the expected size (over the choice of the hash function h) of the intersection of the pre-image of z with the set A_x is $E[|h^{-1}(z) \cap A_x|] = \frac{|A_x|}{|S|} \leq 2.1t$. The claim follows by using the following form of the Chernoff bound [40]:

$$Pr[X \geq (1 + \delta)\mu] \leq e^{-\frac{\delta^2 \mu}{2+\delta}}$$

where X is a sum of independent random variables with values from $\{0, 1\}$ and $\mu = E[X]$. The proof with respect to B_y is identical. □

Using the above two claims, we obtain that with probability at least $1 - e^{-2} - 2e^{-0.1t} > \frac{1}{2}$ the following conditions hold:

(i) $h^{-1}(z) \cap A_x \cap B_y \neq \emptyset$ and

(ii) $h^{-1}(z) \cap A_x$ and $h^{-1}(z) \cap B_y$ are both nonempty and have size at most $3t$.

Let $i^* \in h^{-1}(z) \cap A_x \cap B_y$. Then i^* is a correct output, and the probability that both Alice and Bob select i^* as their output is at least $\frac{1}{9t^2}$. Thus on any input $x \in f^{-1}(0)$ and $y \in f^{-1}(1)$, the players output a correct answer with probability at least $\frac{1}{18t^2}$.

□

Before we see how the hashing lemma helps prove Theorem A.2, 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 AplnD_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.

Proof of Theorem A. We consider two different strategies for different kinds of inputs: the first for when the Hamming distance between the address parts a, b of the inputs is large, i.e. $d(a,b) \geq k/\log k$ and the second when the distance is smaller. For the first case, Alice and Bob use public randomness to sample an index $i \in [k]$ and this bit differentiates a from b with probability $\geq 1/\log k$. In the other case, we first show that $\Omega(1/\sqrt{\log k})$ fraction of the Hamming Ball $\mathcal{B}_a\left(\frac{k}{2} - \sqrt{k \log k}\right)$ around a (or b) intersects that around b (or a). We then use the hashing lemma (Lemma A.3) for Alice and Bob to pick an index in the intersection with probability $\Omega(1/\log k)$.

Public coin strategy for ApInd**:** Let us suppose that Alice has an input $(a, x) \in f^{-1}(1)$ and Bob has $(b, y) \in f^{-1}(0)$. We will consider two separate strategies for Alice and Bob to win the public coin Certificate Game with probability $\Omega(\frac{1}{\log k})$. They choose to play either strategy with probability 1/2.

- **Strategy 1:**

  > Alice and Bob sample a random element $z \in [k]$ using public coins and output the element z.

  This strategy works for inputs for which the Hamming distance between the address parts a and b is large, i.e. $d(a,b) \geq \frac{k}{\log k}$. The probability that this strategy succeeds, $\Pr[a_z \neq b_z] \geq \frac{1}{\log k}$.

- **Strategy 2:** We use the strategy described in Lemma A.3 where $A_{(a,x)}$ and $B_{(b,y)}$ are Hamming Balls of radius $\frac{k}{2} - \sqrt{k \log k}$ centred at a and b respectively. Let S be a set of size $\left\lfloor \frac{|A_x|}{2\sqrt{\log k}} \right\rfloor$

  > - Alice and Bob agree on a $z \in S$ in advance.
  > - They sample a random hash function $h : \{0,1\}^k \mapsto S$ using public randomness.
  > - Alice outputs a uniformly random element from $h^{-1}(z) \cap A_{(a,x)}$ (if this set is empty, she outputs an arbitrary element). Similarly, Bob outputs a uniformly random element of $h^{-1}(z) \cap B_{(b,y)}$, and if empty, an arbitrary element.

  The proof that this strategy works for inputs where the Hamming distance between the address parts a and b is small, i.e. $d(a,b) \leq \frac{k}{\log k}$ essentially relies on the following lemma.

Lemma A.6. *(Intersection Lemma): For two $k-$bit strings a and b at Hamming distance $\frac{k}{\log k}$, a Hamming sphere of radius r centred at a has $\frac{c}{\sqrt{\log k}}$ fraction of it lying in the Hamming ball of the same radius centred at b*

$$\frac{|\mathcal{S}_a(r) \cap \mathcal{B}_b(r)|}{|\mathcal{S}_a(r)|} \geq \frac{c}{\sqrt{\log k}}$$

where $\frac{k}{2} - 100\sqrt{k \log k} \leq r \leq \frac{k}{2} - \sqrt{k \log k}$ and c is a constant.

The proof of Lemma A.6 is given in Appendix A.1. The basic outline of the proof is as follows: the fraction $\frac{|\mathcal{S}_a(r) \cap \mathcal{B}_b(r)|}{|\mathcal{S}_a(r)|}$ is at least the sum of probabilities from a hypergeometric distribution $P_{k,m,r}$ from $\frac{m}{2}$ to m where $m = \frac{k}{\log k}$ is the distance between the Hamming Ball and the Sphere. We show in Lemma A.10 that the hypergeometric distribution $P_{k,m,r}$ is symmetric about $\frac{m}{2}$ for a range up to $200\sqrt{m}$. The expected value E of $P_{k,m,r}$ for our choice of m and r lies between $\frac{m}{2} - 100\sqrt{m}$ and $\frac{m}{2} - \sqrt{m}$. We have a concentration bound for hypergeometric distribution $P_{k,m,r}$ by Hoeffding [24] stated in Lemma A.9 that the sum of the probabilities around the expected value of width $\sqrt{r}$ is at least 0.7. Using the property of hypergeometric distributions that it is monotone increasing up to the expected value E and monotone decreasing beyond it shown in Lemma A.11, we derive a concentration bound of width $\sqrt{m}$ around E that the probabilities in

this range sum to at least $0.7 \times \frac{\sqrt{m}}{\sqrt{r}}$, which for our choice of m and r is at least $\frac{1}{\sqrt{\log k}}$. This gives us that the $\frac{|\mathcal{S}_a(r) \cap \mathcal{B}_b(r)|}{|\mathcal{S}_a(r)|} \geq \frac{c'}{\sqrt{\log k}}$ for a constant c'.

Since we can show most of the weight of the Hamming ball is concentrated on outer layers (proof of which is given in the Appendix A.12) and since the size of the intersection of the Hamming Balls increases as the distance between them decreases, we easily get the following corollary from Lemma A.6.

Corollary A.7. *For two $k-$bit strings a and b at Hamming distance at most $\frac{k}{\log k}$, the ratio of $k-$bit strings in the intersection between the Hamming balls of radius $\frac{k}{2} - \sqrt{k \log k}$ centred at a and b to the total size of each Hamming Ball is at least $\frac{c_1}{\sqrt{\log k}}$.*

$$\frac{|\mathcal{B}_a\left(\frac{k}{2} - \sqrt{k \log k}\right) \cap \mathcal{B}_b\left(\frac{k}{2} - \sqrt{k \log k}\right)|}{|\mathcal{B}_a\left(\frac{k}{2} - \sqrt{k \log k}\right)|} \geq \frac{c_1}{\sqrt{\log k}}$$

where c_1 is a constant.

Using the hashing-based framework described in Lemma A.3 with $A_x = \mathcal{B}_a\left(\frac{k}{2} - \sqrt{k \log k}\right)$ and $B_y = \mathcal{B}_b\left(\frac{k}{2} - \sqrt{k \log k}\right)$, we get that $\mathsf{CG}^{\text{pub}}(\mathsf{ApInd}) = O(\log k)$ as $t = \sqrt{\log k}/c$ where c is a constant. □

The analysis of the strategy 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 $\Omega(\frac{1}{\sqrt{\log k}})$ 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. □

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

Open Problem 6 : Give a lower bound on $\mathsf{CG}^{\text{pub}}(\mathsf{ApInd})$.

A.1 Proof of the Intersection Lemma A.6

The Hamming sphere $\mathcal{S}_a(r)$ centred at the $k-$bit string a of radius r contains $\binom{k}{r}$ $k-$ bit strings, i.e. $|\mathcal{S}_a(r)| = \binom{k}{r}$.

Suppose we denote the Hamming distance between a and b as m. For our purposes, we choose $m = \frac{k}{\log k}$. A $k-$bit string z at a distance r from a lies in $\mathcal{B}_b(r)$ if on the m indices that a differs from b, z is closer to b than a. The number of $k-$bit strings at a distance r from a that lie in $\mathcal{B}_b(r)$,

$$|\mathcal{S}_a(r) \cap \mathcal{B}_b(r)| = \left|\left\{z \in \{0,1\}^k \mid d_H(a,z) = r \wedge d_H(b,z) \leq r\right\}\right| \geq \sum_{j=m/2}^{m} \binom{m}{j}\binom{k-m}{r-j}$$

The hypergeometric distribution on parameters k, m and r, for $0 \leq j \leq m$ is given by,

$$P_{k,m,r}(j) = \frac{\binom{m}{j}\binom{k-m}{r-j}}{\binom{k}{r}}$$

Proposition A.8. *The fraction of the size of the intersection to the size of the Hamming Ball can be expressed as a sum of probabilities from a hypergeometric distribution,*

$$\frac{|\mathcal{S}_a(r) \cap \mathcal{B}_b(r)|}{|\mathcal{S}_a(r)|} \geq \sum_{j=m/2}^{m} P_{k,m,r}(j)$$

The proof relies on following three lemmas about hypergeometric distribution.

Lemma A.9 (Concentration Lemma [24])**.** *For a hypergeometric distribution P with parameters k, m and r,*

$$\sum_{i=0}^{E-\sqrt{r}} P_{k,m,r}(i) \leq e^{-2}$$
$$\sum_{i=E+\sqrt{r}}^{r} P_{k,m,r}(i) \leq e^{-2}$$

where $E = \frac{mr}{k}$ is the expected value of the distribution P.

Lemma A.10 (Symmetric Property)**.** *For the hypergeometric distribution with parameters $m = \frac{k}{\log k}$ and $k/2 - c\sqrt{k \log k} \leq r \leq k/2 - \sqrt{k \log k}$*

$$\frac{P_{k,m,r}(m/2+j)}{P_{k,m,r}(m/2-j)} \geq c'$$

where $0 \leq j \leq 2c\sqrt{m}$ and c, c' are constants.

Proof. From the definition

$$\begin{aligned}
\frac{P_{k,m,r}(m/2+j)}{P_{k,m,r}(m/2-j)} &= \frac{\binom{m}{m/2+j}\binom{k-m}{r-m/2-j}}{\binom{m}{m/2-j}\binom{k-m}{r-m/2+j}} \\
&= \frac{(r-m/2-j+1)\cdots(r-m/2+j)}{(k-m/2-r-j+1)\cdots(k-m/2-r+j)} \\
&\geq \left(\frac{r-m/2-j}{k-m/2-r+j}\right)^{2j} = \left(1 - \frac{k-2r+2j}{k-m/2-r+j}\right)^{2j}
\end{aligned}$$

where in the last line we have approximated all the terms in the numerator by a factor smaller than the smallest factor and in the denominator by the largest factor. On substituting the values for m and r, we have

$$\begin{aligned}
\frac{P_{k,m,r}(m/2+j)}{P_{k,m,r}(m/2-j)} &\geq \left(1 - \frac{1}{2j}\left(\frac{2j\left(2c\sqrt{k\log k}+2j\right)}{k/2 - \frac{k}{2\log k} + \sqrt{k\log k}+j}\right)\right)^{2j} \\
&\approx e^{-\left(\frac{2j\left(2c\sqrt{k\log k}+2j\right)}{k/2-\frac{k}{2\log k}+\sqrt{k\log k}+j}\right)} \geq e^{-16c^2}
\end{aligned}$$

We get the last inequality after replacing j by the largest possible value that we consider which is $2c\sqrt{m}$ and we get $c' \approx e^{-16c^2}$. □

Lemma A.11 (Monotonicity Property)**.** *For the hypergeometric distribution where k is large and $m = \frac{k}{\log k}$ and $k/2 - c\sqrt{k \log k} \leq r \leq k/2 - \sqrt{k \log k}$, $P_{k,m,r}(j+1) \geq P_{k,m,r}(j)$ for $j \leq E - 1/2$ and $P_{k,m,r}(j+1) \leq P_{k,m,r}(j)$ otherwise. Here, $E = \frac{mr}{k}$ is the expected value of the distribution P.*

Proof. From the definition of hypergeometric distribution, we have

$$\frac{P_{k,m,r}(j+1)}{P_{k,m,r}(j)} = \frac{\binom{m}{j+1}\binom{k-m}{r-j-1}}{\binom{m}{j}\binom{k-m}{r-j}} = \frac{(m-j)(r-j)}{(j+1)(k-m-r+j+1)}$$

If $P_{k,m,r}(j+1) \geq P_{k,m,r}(j)$, we have $\frac{(m-j)(r-j)}{(j+1)(k-m-r+j+1)} \geq 1$. On simplifying this expression, we get $j \leq \frac{mr+m-k+r-1}{(k+2)}$. Similarly we have $P_{k,m,r}(j+1) \leq P_{k,m,r}(j)$ when $j \geq \frac{mr+m-k+r-1}{(k+2)}$. When k is large, $k+2 \approx k$ and $\frac{mr+m-k+r-1}{(k+2)} \approx E - (1 - \frac{m+r}{k})$. On substituting for m and r, we get $\frac{m+r}{k} \approx 1/2 + \epsilon$ where $\epsilon \ll 0$. Thus we can conclude that when k is large enough, $P_{k,m,r}(j+1) \geq P_{k,m,r}(j)$ when $j \leq E - 1/2$ and $P_{k,m,r}(j+1) \leq P_{k,m,r}(j)$ otherwise. □

We can now prove the main result of this section.

Proof of Lemma A.6. To prove this theorem, from Proposition A.8 it is enough to show that

$$\sum_{j=m/2}^{m} P_{k,m,r}(j) \geq \frac{c'}{\sqrt{\log k}}$$

when $m = \frac{k}{\log k}$ and $k/2 - c\sqrt{k \log k} \leq r \leq k/2 - \sqrt{k \log k}$. From the monotonicity property in Lemma A.11, we have that

$$\sum_{j=E-\sqrt{m}}^{j=E+\sqrt{m}} P_{k,m,r}(j) \geq \frac{\sqrt{m}}{\sqrt{r}} \sum_{j=E-\sqrt{r}}^{j=E+\sqrt{r}} P_{k,m,r}(j) > \sqrt{\frac{2}{\log k}} \sum_{j=E-\sqrt{r}}^{j=E+\sqrt{r}} P_{k,m,r}(j)$$

From Lemma A.9, we have

$$\sum_{j=E-\sqrt{r}}^{j=E+\sqrt{r}} P_{k,m,r}(j) \geq 0.72$$

This gives,

$$\sum_{j=E-\sqrt{m}}^{j=E+\sqrt{m}} P_{k,m,r}(j) > \sqrt{\frac{2}{\log k}} \times 0.72 > \frac{1}{\sqrt{\log k}}$$

For our choice of m and r, we have the expected value $m/2 - c\sqrt{m} \leq E \leq m/2 - \sqrt{m}$. Using Lemma A.10, by the symmetric property of the hypergeometric distribution for our choice of m and r, on reflecting about $m/2$ we have

$$\sum_{j=m/2}^{m} P_{k,m,r}(j) \geq c' \sum_{j=E-\sqrt{m}}^{j=E+\sqrt{m}} P_{k,m,r}(j) \geq \frac{c'}{\sqrt{\log k}}.$$

where $c' \approx e^{-16c^2}$. □

A.2 Most of the weight is concentrated on outer surfaces of the Hamming ball

Lemma A.12. *For a Hamming Ball of radius $r = k/2 - \sqrt{k \log k}$, the weight contributed by Hamming Spheres of radius $\leq k/2 - 100\sqrt{k \log k}$ is small.*

$$\frac{\sum_{i=0}^{\frac{k}{2}-100\sqrt{k\log k}} |\mathcal{S}_a(i)|}{|\mathcal{B}_a\left(\frac{k}{2} - \sqrt{k \log k}\right)|} \leq c_1$$

where c_1 is a constant.

Proof. We would like to show

$$\frac{\sum_{j=0}^{\frac{k}{2}-100\sqrt{k\log k}}\binom{k}{j}}{\sum_{j=0}^{\frac{k}{2}-\sqrt{k\log k}}\binom{k}{j}} \leq c_1$$

We use the following form of Chernoff Bound [40],

$$\Pr\left[X \leq (1-\delta)\mu\right] \leq e^{\frac{\delta^2\mu}{2}}$$

for $0 \leq \delta \leq 1$ and apply it to the binomial distribution with $p = 1/2$ to get $\sum_{j=0}^{\frac{k}{2}-100\sqrt{k\log k}}\binom{k}{j} \leq 2^k k^{-10^4}$. We now use the following lower bound for the tail of the binomial distribution when $p = 1/2$ (which is restated slightly from its original form in [37]).

$$\Pr\left[X \leq k/2 - \delta\right] \geq \frac{1}{15}e^{-16\delta^2/k}$$

for $\delta \geq 3k/8$. This gives $\sum_{j=0}^{\frac{k}{2}-\sqrt{k\log k}}\binom{k}{j} \geq 2^k\frac{1}{15}k^{-16}$. Thus we have

$$\frac{\sum_{j=0}^{\frac{k}{2}-100\sqrt{k\log k}}\binom{k}{j}}{\sum_{j=0}^{\frac{k}{2}-\sqrt{k\log k}}\binom{k}{j}} \leq \frac{15k^{-10^4}}{k^{-16}} \ll c_1$$

□

B Examples of functions

Interesting examples of total and partial Boolean functions are very important to understand the relations between various complexity measures. In fact constructing interesting functions is one of the commonly used techniques to prove separation between pairs of measures. A number of interesting functions has been constructed for this purpose (for example [22, 3, 10, 19, 50]). In this paper we use some of them to understand the relation between the certificate games measures and others. The various complexity measures for the functions we consider is compiled in Table 1.

OR and Parity ($\oplus$) are one of the simplest functions, probably the first ones to be studied for any complexity measures. The bounds on $\oplus_n$ follow from the observation that $\lambda(\oplus_n) = \Theta(n)$ ($\mathsf{CG}^{\text{priv}}(\oplus_n) = \Theta(n^2)$ follows from Theorem 5.10); the bounds on OR_n follow from $\lambda(f) = \Theta(\sqrt{n})$ [4], $\mathsf{Q}(\mathsf{OR}_n) = O(\sqrt{n})$ [23] and the observation that $\mathsf{s}(\mathsf{OR}_n) = \Theta(n)$ (please refer to Figure 1).

$\mathsf{Tribes}_{m,n} = \mathsf{OR}_m \circ \mathsf{AND}_n$ is a non-symmetric function, made by composing OR and AND. We use it as an example of a total function where R and CG^{pub} are asymptotically different. It can be verified that $\mathsf{C}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(\sqrt{n})$, and $\lambda(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \mathsf{Q}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(\sqrt{n})$ follows from composition [4, 36]. $\mathsf{R}(\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}) = \Theta(n)$ is from Jain and Klauck [27], other measures follow from these observations.

The function GSS_1 is a function defined in [22]. It is defined on $\{0,1\}^{n^2}$. The complexity measures of GSS_1 was computed in [22] and [28]. The blank spaces indicates that the tight bounds are not known.

Function	λ	s	bs	FC	MM	Q	CG^{pub}	R	EC	C	$\mathsf{CG}^{\text{priv}}$
OR_n	$\Theta(\sqrt{n})$	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$
$\oplus_n$	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$	$\Theta(n^2)$
$\mathsf{Tribes}_{\sqrt{n},\sqrt{n}}$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$	$\Theta(n)$	$\Theta(\sqrt{n})$	$\Theta(\sqrt{n})$	$\Theta(n)$
GSS_1		$\Theta(n)$	$\Theta(n)$	$\Theta(n)$			$\Theta(n)$		$\Theta(n)$	$\Theta(n^2)$	$O(n^2)$

Table 1: Some of the commonly referred total functions and their complexity measures

Regarding partial functions we would like to discuss a couple of them that are used in multiple places in the paper to show separations between measures for partial functions - namely the "approximate indexing" function and the "greater than half" function. The know measures for these functions are compiled in the Table 2.

ApInd is the approximate indexing function defined by Ben-David and Blais [13], we show that R and CG^{pub} are exponentially separated for this partial function (we know $\mathsf{R}(\mathsf{ApInd}) = \Theta(\sqrt{k \log k})$ [13] and $\mathsf{CG}^{\text{pub}}(\mathsf{ApInd}) = O(\log k)$, from Section A). Rest of the measures mentioned in the table can be observed easily.

There is a partial function, GTH (defined by Ambainis et al. [7], see Definition B.1), for which FC is constant [7] but CG^{pub} is $\Theta(n)$ (follows from Theorem 6.2 and $\mathsf{CMM}(\mathsf{GTH}) = \Theta(n)$ [7]).

Definition B.1 (GTH [7])**.** *The "greater than half" function is a partial function defined only on n bit strings that have Hamming weight 1. The function evaluates to 1 on an input x if the position i where the input bit is 1 is in the second half of the string, i.e.* $\mathsf{GTH} : \{0,1\}^n \to \{0,1\}$ *is defined as* $\mathsf{GTH}(x) = 1$ *if* $x_i = 1$ *where* $i > n/2$.

To show that $\mathsf{CG}^{\text{priv}}(\mathsf{GTH}) = \Theta(n)$, we use the version in Proposition 5.9. For a 1-input y, we only put a non-zero weight of $\sqrt{n}$ on index i where $y_i = 1$. For a 0-input, we put a non-zero weight of $\frac{1}{\sqrt{n}}$ only on indices i such that $i > n/2$. It can be verified that this is a feasible solution of the equivalent formulation of $\mathsf{CG}^{\text{priv}}$ (from Proposition 5.9) with objective value n.

Function	λ	s	bs	FC	MM	Q	CMM	CG^{pub}	R	EC	C	$\mathsf{CG}^{\text{priv}}$
ApInd		0	$O(1)$	$O(1)$				$O(\log k)$	$\Theta(\sqrt{k \log k})$		$O(1)$	
GTH_n		0	$O(1)$	$O(1)$			$\Theta(n)$	$\Theta(n)$		$\Theta(n)$	$O(1)$	$\Theta(n)$

Table 2: The known complexity measures for ApInd and GTH_n

C FC as a local version of CG^{pub}

In this section we will show that $\mathsf{FC}(x)$ can be viewed as a certificate game where Alice's input is fixed. We start with the dual of the CG^{pub} optimization problem.

For a two-player certificate game G_f corresponding to a (possibly partial) Boolean function f, $\mathsf{CG}^{\text{pub}}(f) = 1/\omega^{pub}(G_f)$ (Proposition 3.1), where the winning probability $\omega^{pub}(G_f)$ is given by the following linear program.

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

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 $x_i \neq y_i$.

Re-normalizing, we get the linear program for $\mathsf{CG}^{\text{pub}}(f)$,

$$\begin{aligned}
\mathsf{CG}^{\text{pub}}(f) = \quad & \sum_{x,y} \mu_{x,y} \\
\text{such that} \quad & \sum_{x,y:\ A,B \text{ correct on } x,y} \mu_{x,y} \le 1 \quad \text{for every deterministic strategy } A, B \\
& \mu_{x,y} \ge 0,
\end{aligned}$$

Let us define the local version of CG^{pub} in two stages: Let $\mathsf{CG}^{\text{pub}}_L(f,x)$ be the value of the CG^{pub} game when one of the party's input is fixed to x (say Alice), then $\mathsf{CG}^{\text{pub}}_L(f) = \max_x \mathsf{CG}^{\text{pub}}_L(x)$. We will show that $\mathsf{CG}^{\text{pub}}_L$ is same as fbs; given that $\mathsf{CG}^{\text{pub}}(f) = \Theta(\text{fbs}(f))$, we see that local and global version of CG^{pub} are same.

The linear program for the local version can be written as:

$$\begin{aligned}\mathsf{CG}^{\text{pub}}_L(f,x) = \quad & \sum_y \mu_y \\ \text{such that} \quad & \sum_{y:B \text{ outputs } i \text{ on } y \text{ and } x_i \neq y_i} \mu_y \leq 1 \quad \forall \text{ deterministic strategies } B, \text{ index } i \\ & \mu_y \geq 0,\end{aligned}$$

Where it is understood that the deterministic strategy for Alice, A, answers i. Notice that fixing an i, the *strictest* constraint is obtained by B which answers i whenever $y_i \neq x_i$. This means we can keep just one constraint for every i.

$$\begin{aligned}\mathsf{CG}^{\text{pub}}_L(f,x) = \quad & \sum_y \mu_y \\ \text{such that} \quad & \sum_{y:x_i \neq y_i} \mu_y \leq 1 \quad \text{for all } i \\ & \mu_y \geq 0,\end{aligned}$$

Every y (such that $f(x) \neq f(y)$) has a one to one correspondence with a sensitive block B such that $y = x^{\oplus B}$. The linear program can be simplified to the linear program for $\text{fbs}(f,x)$.

$$\begin{aligned}\mathsf{CG}^{\text{pub}}_L(f,x) = & \sum_B \mu_B \\ \text{such that} \quad & \sum_{B:i \in B} \mu_B \leq 1 \quad \text{for all } i \\ & \mu_B \geq 0,\end{aligned}$$

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il