Hidden-State Proofs of Quantumness

Carl A. Miller

National Institute of Standards and Technology (NIST),
100 Bureau Dr., Gaithersburg, MD 20899

Joint Center for Quantum Information and Computer Science (QuICS),
3100 Atlantic Building, College Park, MD 20742

Abstract

An experimental cryptographic proof of quantumness — that is, a proof, based only on well-studied cryptographic assumptions, that a physical device is performing quantum computations — will be a vital milestone in the progress of quantum information science. However, error tolerance is a persistent challenge for implementing such tests: we need a test that not only can be passed by an efficient quantum prover, but one that can be passed by a prover that exhibits a certain amount of computational error.

(Brakerski *et al.* 2018) introduced a innovative two-round proof of quantumness based on the LWE (Learning With Errors) assumption. However, one of the steps in their protocol (the pre-image test) has low tolerance for error. In this work we present a proof of quantumness which maintains the same circuit structure as (Brakerski *et al.* 2018) but exhibits a large improvement in robustness for noise. Our protocol is based on cryptographically hiding an extended GHZ state within a sequence of classical bits. Asymptotically, our protocol allows the total probability of error within the circuit to be as high as $1 - \Omega(\lambda^{-C})$, where λ is the security parameter and C is a constant that be chosen arbitrarily large. As part of this result, we prove an uncertainty principle over finite abelian groups which may be of independent interest.

1 Introduction

As advances in quantum computing continue to accelerate, a central question is: how will we know when we have a quantum advantage in computing? Will we be able to prove that such an advantage has been achieved? The highest-profile target for quantum computing continues to be implementing Shor's algorithm [15], but that target remains a distant goal, in large part because of the need for quantum error-correction. Is it possible to prove the quantum behavior of a computer in the absence of full quantum error correction?

Google's breakthrough demonstration on a 53-qubit device [2] was based on random circuit sampling, and it had a high tolerance for error. However, Google's claim that [2] was a demonstration of quantum advantage was based on assumptions about the hardness of classically simulating quantum circuits, and those assumptions were (pretty drastically) disproved after the fact [6]. While advances in random quantum circuit demonstrations continue, it is useful to ask whether another direction can provide more stable claims of a computational quantum advantage.

In a breakthrough result in 2018, Brakerski *et al.* [3] established a theoretical interactive proof of quantumness based on the LWE (Learning With Errors) assumption. A benefit of using LWE a starting point is that it has a long history as a basis for classical cryptographic protocols [14], and thus there are well-established and stable metrics for the hardness of LWE problems. The protocol of [3] begins by having a classical verifier randomly construct a pair of linear injective functions

$$f_0, f_1 \colon \mathbb{Z}_q^n \to \mathbb{Z}_q^m \tag{1}$$

which have approximately the same image, in the sense that for any $\mathbf{s}_0 \in \mathbb{Z}_q^n$, there exists $\mathbf{s}_1 \in \mathbb{Z}_q^n$ such that the difference vector $f_0(\mathbf{s}_0) - f_1(\mathbf{s}_1)$ has entries close to 0. However, the LWE assumption implies that it is impossible for any outside party to reliably compute such a pair $(\mathbf{s}_0, \mathbf{s}_1)$.

In the first round of the protocol, the verifier has the quantum prover use f_0, f_1 to prepare a *claw-state*

$$\phi \quad = \quad \frac{1}{\sqrt{2}} \left(|\mathbf{s}_0, 0\rangle + |\mathbf{s}_1, 1\rangle \right). \tag{2}$$

Then, in the second round of the protocol, according to a random coin flip, the prover either asks the verifier to measure ϕ in the computational basis and report the result (the "pre-image test"), or to measure in the Hadamard basis and report the result (the "Hadamard" test). The prover (who knows the state ϕ) checks whether the result was valid; if so, the verifier passes. Otherwise, the verifier fails.

A quantum prover can (in theory) pass this test with probability 1. However, a classical prover cannot do better than $\frac{3}{4} + \text{negl}(\lambda)$, where λ denotes the security parameter. This fact is proved by a rewinding argument: if a classical prover can pass the pre-image and Hadamard tests with high probability, then the same prover could pass both tests simultaneously, and that would mean they could compute information information about $\mathbf{s}_0, \mathbf{s}_1$ beyond what the LWE assumption allows. Therefore, as long as the LWE problem cannot be solved in polynomial time, the protocol is sound against classical provers.

However, error-tolerance continues to be an issue. The pre-image test requires the prover to report correctly either the entire vector $\mathbf{s}_0$ or the entire vector $\mathbf{s}_1$. Naively, if the probability of an error occurring before or during the pre-image test is significantly more than $1/2$, then the prover's expected score will be below $(1/2)(1/2) + (1/2)(1) = (3/4)$, and the prover will fail too often to achieve a quantum advantage.

Our goal in this paper is to study how to improve the error tolerance of a protocol in the form of [3]. We begin by considering a parallel research topic (nonlocal games).

1.1 Interactive proofs of quantumness versus nonlocal games

A nonlocal game is different type of proof of quantumness with a much longer history, going back at least to the work of John Bell in the 1960s. In this setting, a classical verifier interacts with 2 or more provers. The verifier assigns a single score to the prover at the end of the interaction. If the average score of the provers (across multiple rounds) lies significantly outside the range achievable by classical provers, the verifiers conclude that the provers must be quantum.

A simple way to measure the error-tolerance of a nonlocal game is via the **bias ratio**. If G is a nonlocal game, the bias ratio is given by the expression

$$r(G) \quad = \quad \frac{\sup_C |\omega(G, C)|}{\sup_Q |\omega(G, Q)|}, \tag{3}$$

where C varies over all classical strategies for G and Q varies over all quantum strategies for G, and $\omega(G, S)$ denotes the expected score of a given strategy S. (The numerator above is the **classical bias**, and the denominator is the **quantum bias**.) If one accepts the heuristic that when an error occurs, the provers will perform no worse than the worst classical score (i.e., they do not accidentally achieve a Bell violation in the opposite direction), then we find that the provers can prove quantum behavior as long as their total error probability is less than $(1 - r(G))/(1 + r(G)) = 1 - \Omega(r(G))$. Thus, a small bias ratio is desirable.

The Brakerski *et al.* test, as given above, has bias ratio $3/4 = \text{negl}(\lambda)$. However, we can make a natural adjustment and say that if a prover fails at the Hadamard test, they receive a score of -1 (rather than a score of 0). In that case, the range of possible classical scores is between $-1/2 - \text{negl}(\lambda)$ and $1/2 + \text{negl}(\lambda)$, while the range of possible quantum scores is $[-1, 1]$, yielding a classical bias of approximately $1/2$, which is smaller, but still a positive constant. Subsequent work [9, 1] improved and optimized the test from [3], but the biases in those works were likewise positive constants.

In [10], a general compiler was given that can convert any multi-player nonlocal game into an interactive proof of quantumness based on LWE. This result suggests taking a known nonlocal game with very small bias ratio (such as one of the games from [5]) and compiling it with [10] to obtain an interactive proof

of quantumness with very small bias ratio. This approach is viable, but there is an important catch: [10] requires using the full machinery of quantum homomorphic encryption, which means substantially increasing the quantum circuits involved in the interactive test and thereby increasing the probability of an error. The motivating question behind the current work is the following: Can we, without changing the basic quantum circuit structure of [3], create a modified protocol in which the bias ratio tends to zero?

1.2 Main Result

One of the oldest known family of nonlocal games with vanishing bias ratio is the family of extended GHZ games. The GHZ_d game is played by k-players Alice$_1$, Alice$_2$, ..., Alice$_k$, with $k \geq 3$. A referee randomly chooses a bit string $\mathbf{x} = x_1, x_2, \ldots, x_k$ of even parity and sends x_j to Alice$_j$ for each j. Each Alice$_j$ then outputs a bit a_j. The players score $+1$ if the following equation holds:

$$x_1 + x_2 + \ldots + x_k + 2a_1 + 2a_2 + \ldots + 2a_k \quad \equiv \quad 0 \pmod 4. \tag{4}$$

and they score -1 if it does not hold. This game can be won perfectly if the players shared a GHZ state $\frac{1}{\sqrt{2}}\left(\left|0^k\right\rangle + \left|1^k\right\rangle\right)$ and Alice$_j$ applies a Pauli X-measurement on her qubit if $x_j = 0$ or a Pauli Y-measurement on her qubit if $x_j = 1$. However, a result by Mermin [11] implies that classical players will always have an average score between $-2^{-(k/2)+1}$ and $2^{-(k/2)+1}$, implying that bias ratio for the extended GHZ games is exponentially vanishing in k.

Our main result is based on a efficient way of compiling the extended GHZ game into an interactive proof of quantumness in the style of [3]. The proof of quantumness is called Game $\mathbf{R}$ in this paper, shown in Figure 5. The first round of the protocol is modified: the functions f_0, f_1 are chosen somewhat differently by the verifier, and some of the qubits of the claw-state (2) are measured immediately so that before the second round, the prover holds a state of the form

$$\phi' \quad = \quad \frac{1}{\sqrt{2}}\left(|\mathbf{c}, 0\rangle \pm |\mathbf{c}', 1\rangle\right). \tag{5}$$

where $\mathbf{c}, \mathbf{c}'$ are bit strings of length $d \leq n$. Crucially, the XOR string $\mathbf{c} \oplus \mathbf{c}'$ is cryptographically hidden from the prover.

In the second round, the verifier has the prover measure the first d qubits of ϕ' randomly in either the X- or Y-bases. The prover measures the $(d+1)$th qubit in the $(X-Y)/\sqrt{2}$-basis. All results are reported to the verifier, who checks a certain parity condition, and awards a score of $+1$ if the parity condition is satisfied and -1 if it is not.

Game $\mathbf{R}'$ (Figure 6) is the same as Game $\mathbf{R}$ except that the measurements of the qubits of the state ψ' are done sequentially by the prover, making Game $\mathbf{R}$ a $(d+2)$-round protocol instead of a 2-round protocol. We prove the following (see Propositions 8, 9 and Theorems 8, 9).

Theorem 1. *Games* $\mathbf{R}$ *and* $\mathbf{R}'$ *satisfy the following:*

1. *The quantum biases for Games* $\mathbf{R}$ *and* $\mathbf{R}'$ *are at least* $\sqrt{2}/2 - o(1)$.
2. *The classical bias for Game* $\mathbf{R}$ *is at most* $\exp(-\Omega(d)) + \mathrm{negl}(\lambda)$.
3. *The classical bias for Game* $\mathbf{R}'$ *is at most* $(0.75)^{d/4} + \mathrm{negl}(\lambda)$.

These results imply that the bias ratio for Game $\mathbf{R}$ vanishes exponentially in d. The same is true for Game $\mathbf{R}'$, which has the advantage of an explicit exponential base (namely, $\sqrt[4]{0.75}$).

In order for the proof method to work, the parameter d must be a polylogarithmic function of λ. This allows us, for example, to set $d = \lceil C \log \lambda \rceil$ for any chosen constant C, yielding a bias ratio for Game $\mathbf{R}$ that vanishes at a rate of $O(\lambda^{-C})$. Thus, any polynomial vanishing rate for the bias ratio is achievable.

1.3 Proof Techniques

The intuition behind Game **R** is that the verifier has hidden a GHZ in the state (5). The jth qubit is part of the GHZ state if $c_j \neq c'_j$, whereas if $c_j = c'_j$ the the jth qubit simply in a computational basis state (a decoy state). The prover is compelled to play a (modified version of) the extended GHZ game on the entangled qubits without knowing where they are. This cryptographic hiding mechanism is designed to foil coordinated classical cheating strategies by the prover. However, a method to prove that this cryptographic hiding actually works is not so obvious, and we take a somewhat indirect approach.

We design a two-player called Game $\mathbf{J}_d$ (Figure 1), which is essentially the GHZ game played with decoy states as described above. We characterize classical strategies and show that the expected score of a classical strategy can be conveniently expressed in terms of the discrete Fourier transform over $\mathbb{Z}_4^n$ (see Subsection 5.2).

Along the way, we prove a strong uncertainty principle for the Fourier transform for finite abelian groups (Corollary 1). A long standing result by Donoho and Stark [7] asserts that if $h\colon G \to \mathbb{C}$ is a nonzero function on a finite abelian group G, and $\hat{h}$ is its Fourier transform, then

$$|\text{Supp } h| \cdot \left|\text{Supp } \hat{h}\right| \quad \geq \quad |G| \tag{6}$$

(Informally, this means that is is not possible for both h and $\hat{h}$ to have small support, in analogy to the Heisenberg uncertainty principle.) Corollary 1 takes this result a step further by characterizing cases in which inequality (6) is close to being an equality. Essentially, a near-equality is possible only if Supp h and Supp $\hat{h}$ are both close to being linear subsets of G.

As noted above, the expected score achieved by classical strategy at Game $\mathbf{J}_d$ can be expressed in terms of the discrete Fourier transform, and it turns out that the functions in this expression have very non-linear support. This fact is sufficient to prove that the classical bias of the Game $\mathbf{J}_d$ vanishes exponentially in d (see Section 5). Interestingly, proving this nonlinearity ultimately relies not on the properties of the d-player game GHZ_d, but on the parallel repeated 4-player game GHZ_4^d. We make use of a recent result [4] that asserts that the classical bias of the GHZ_4^d vanishes exponentially in d.

Finally, modifying reasoning from [10], we show in Section 6 that the upper bound on the classical bias of Game $\mathbf{J}_d$ implies a similar upper bound on the classical bias of Game **R**. The argument requires rewinding a classical algorithm exponentially many times in the parameter d. This rewinding must be done in polynomial time, and that is why there is a need to make d polylogarithmic in λ.

1.4 Future Work

A natural next step is to compute a concrete range of values for the parameters in Figure 6 which would achieve a proof of quantumness. Our soundness proof for Game **R** (Theorem 8) shows that any classical cheating strategy can be converted into an attack on LWE. Thus, we may consider a set of parameters to be appropriate for a proof of quantumness if the efficiency of this attack is far better than any known classical attacks on LWE. Optimizing the conversion procedure in the proof of Theorem 8 will be important in order to keep these parameters as small as possible.

2 Preliminaries

For any positive integer q, let $\mathbb{Z}_q$ denote the ring of integers modulo n. We denote elements of $\mathbb{Z}_q$ simply by $\{0, 1, 2, \ldots, q-1\}$. For any $x \in \mathbb{Z}_q$, let $|x| \in \mathbb{Z}$ denote the minimum absolute value among all integers congruent to x mod q (e.g., in the ring $\mathbb{Z}_5$, $|1| = |4| = 1$ and $|2| = |3| = 2$). For any vector $\mathbf{v} \in \mathbb{Z}_q^n$, let $\|\mathbf{v}\|_1 = \sum_{j=1}^n |v_j|$, and let $\|\mathbf{v}\|_\infty$ denote the maximum value of $|v_j|$ among all coordinates v_j of $\mathbf{v}$.

Remark 1. *We use the big-endian convention for binary representations. For any $x \in \mathbb{Z}_q$, let $[x] \in \{0,1\}^{\lceil \log z \rceil}$ denote the binary representation of x in big-endian order (for example, if $q = 11$ and $x = 5$, then $[x] = 0101$). If $\mathbf{x} \in \mathbb{Z}_q^n$, then $[\mathbf{x}]$ denotes the length-$(n\lceil \log z \rceil)$ binary sequence $[x_1][x_2]\ldots[x_n]$. For any*

$j \in \{1, 2, \ldots, \lceil \log z \rceil\}$, we denote by $[x]_j$ the jth bit of $[x]$. If $\mathbf{x} \in \mathbb{Z}_q^d$ is a vector over $\mathbb{Z}_q$, then $[\mathbf{x}]_j \in \{0,1\}^d$ denotes the bit string $[x_1]_j [x_2]_j \ldots [x_d]_j$.

A **register** is simply a finite set $\mathcal{Q}$ (the set of basic states). A quantum register also has an associated complex Hilbert space $Q = \{f \mid f \colon \mathcal{Q} \to \mathbb{C}\}$. A **qubit** is a quantum register $\mathcal{Q}$ with a fixed bijection $\mathcal{Q} \leftrightarrow \{0,1\}$.

Let $\mathcal{V}$ be a quantum register and V its associated complex Hilbert space. We denote by $\mathbb{I}_V$ the identity operator on V. A **positive operator-valued measure** (POVM) on V is a finite set $\{M_y\}_{y \in Y}$ of positive semidefinite operators on V satisfying $\sum_y M_y = \mathbb{I}_V$. A **pure state** on V is a unit vector in V. A **mixed state** on V is a positive semi-definite linear operator on V of trace 1. A **subnormalized** mixed state is a positive semi-definite operator linear operator in V of trace less than or equal to 1.

If m is a positive integer and $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{C}^m$, then $\|\mathbf{w}\|_1$ denotes 1-norm of w:

$$\|\mathbf{w}\|_1 \quad = \quad \sum_{j=1}^{m} |w_j| \,. \tag{7}$$

The expression $\|\mathbf{w}\|$ denotes the Frobenius norm:

$$\|\mathbf{w}\| \quad = \quad \sqrt{\sum_{j=1}^{m} w_j^2}. \tag{8}$$

The **Cauchy-Schwarz inequality** is simply the obervation that if W is a complex Hilbert space and $\mathbf{w}, \mathbf{y} \in W$, then

$$|\langle \mathbf{x}, \mathbf{y} \rangle| \quad \leq \quad \|\mathbf{x}\| \, \|\mathbf{y}\| \,, \tag{9}$$

with equality if and only if $\mathbf{x}$ and $\mathbf{y}$ are parallel vectors.

If z is a complex number and $z = re^{i\theta}$ with $0 \leq \theta < 2\pi$, and if c is a real number, then we define z^c to mean the quantity

$$z^c \quad = \quad r^c e^{\theta c}. \tag{10}$$

If D is an $m \times m$ diagonal matrix with diagonal entries $d_1, d_2, \ldots, d_m \in \mathbb{C}^m$, then D^c denotes the diagonal matrix with entries $d_1^c, d_2^c, \ldots, d_m^c$.

We write $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ to denote, respectively, the following vectors on $\mathbb{C}^2$:

$$(1,0), (0,1), \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right), \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right). \tag{11}$$

(We may omit the Dirac brackets $|\cdot\rangle$ when it is convenient to do so.) The letters X, Y, Z denote the Pauli operators:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{12}$$

If W is a Hermitian operator on $\mathbb{C}^2$ with eigenvalues in $\{-1, +1\}$, then measuring "in the W-basis" means applying the POVM $\{(\mathbb{I} + W)/2, (\mathbb{I} - W)/2\}$ to obtain a bit w (where $(\mathbb{I} + W)/2$ corresponds to outcome $w = 0$ and $(\mathbb{I} - W)/2$ corresponds to outcome $w = 1$).

If S is a finite set and $p \colon S \to [0,1]$ is a probability distribution on S, then the **collision probability** of p is the quantity

$$\sum_{s \in S} p_s^2. \tag{13}$$

(This quantity is equal to the probability that two independent samples from p will agree.) We note the following proposition, which follows directly from the Cauchy-Schwartz inequality.

Proposition 1. *Let S be a finite set, let $p, p' \in S$ be probability distributions on S, and let $c = \sum_{s \in S} p_s^2$ and $c' = \sum_{s \in S} (p'_s)^2$. Then,*

$$\mathbf{P}\left[s = s' \mid s \leftarrow p, s' \leftarrow p'\right] \quad \leq \quad \sqrt{cc'}, \tag{14}$$

with equality if and only if $p = p'$. $\square$

2.1 Nonlocal Games

Definition 1. *A nonlocal m-player game (for $m \geq 2$) consists of the following data:*

- *Finite sets $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_m$ and $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m$.*
- *A probability distribution r on $\mathcal{X}_1 \times \cdots \times \mathcal{X}_m$.*
- *A scoring function*

$$F \colon \mathcal{X}_1 \times \cdots \times \mathcal{X}_m \times \mathcal{A}_1 \times \cdots \times \mathcal{A}_m \to \mathbb{R}. \tag{15}$$

Given the data above, a nonlocal m-player game proceeds as follows. We refer to the participants in the game as Referee and Alice$_1$, Alice$_2$, …, Alice$_m$.

1. Referee samples a sequence $(x_1, \ldots, x_m)$ according to r and sends x_i to Alice$_i$.
2. Alice$_i$ outputs an element $a_i \in \mathcal{A}_i$.
3. The Referee awards the score $F(x_1, \ldots, x_m, a_1, \ldots, a_m)$.

We will also need the definition of a sequential nonlocal two-player game. (See [8] for some related formalism.)

Definition 2. *A sequential nonlocal m-player game is a nonlocal game*

$$(\mathcal{X}_1, \ldots, \mathcal{X}_m, \mathcal{A}_1, \ldots, \mathcal{A}_m, r, F) \tag{16}$$

with additional positive integer parameters $d_1, d_2, \ldots, d_m$ such that for every $i \in \{1, 2, \ldots, m\}$,

$$\mathcal{X}_i \quad = \quad \mathcal{X}_{i,1} \times \mathcal{X}_{i,2} \times \cdots \times \mathcal{X}_{i,d_i} \tag{17}$$

$$\mathcal{A}_i \quad = \quad \mathcal{A}_{i,1} \times \mathcal{A}_{i,2} \times \cdots \times \mathcal{A}_{i,d_i}. \tag{18}$$

A sequential nonlocal two-player game proceeds as follows.

1. Referee samples a sequence $(x_1, \ldots, x_m)$ according to r and sends x_i to Alice$_i$.
2. For $j = 1, 2, \ldots d_1$, Referee sends the jth component of x_1 to Alice$_1$ and receives output $a_{1,i} \in \mathcal{A}_{i,1}$. She records the outputs as $a_1 := (a_{1,1}, a_{1,2}, \ldots, a_{1,d_1})$.
3. Referee repeats Step 2 for each of Alice$_2$, Alice$_3$, …, Alice$_m$ to obtain a sequence $(a_1, a_2, \ldots, a_m)$.
4. The Referee awards the score $F(x_1, \ldots, x_m, a_1, \ldots, a_m)$.

Crucially, in steps 2–3, Alice$_i$ must return her output $a_{i,j}$ before receiving the next input $x_{i,j+1}$.

Definition 3. *Let $H = (\mathcal{X}_1, \ldots, \mathcal{X}_m, \mathcal{A}_1, \ldots, \mathcal{A}_m, r, F)$ be m-player nonlocal game. A **quantum strategy** for H consists of the following data.*

- *Quantum registers $A_1, A_2, \ldots, A_m$*
- *A pure state $\psi \in A_1 \otimes \cdots \otimes A_m$,*

- *For every $i \in \{1, 2, \ldots, m\}$ and every $x \in \mathcal{X}_i$, a POVM $\left\{M_{i,x}^a \mid a \in \mathcal{A}_i\right\}$ on A_i.*

These data specify how Alice$_1$, ..., Alice$_m$ act when playing Game G:

1. Before receiving their inputs, Alice$_1$, ..., Alice$_m$ share state ψ (with Alice$_i$ possessing register A_i).
2. When Alice$_i$ receives her input x_i she applies the POVM $\{M_{i,x}^a\}$ and outputs the result.

We can compute probabilistic behavior of the players directly in terms of the mathematical objects defined above: for example, if $m = 2$, the probability that Alice and Bob will output (a_1, a_2) on input (x_1, x_2) is given by

$$\psi^*(M_{1,x_1}^{a_1} \otimes M_{2,x_2}^{a_2})\psi. \tag{19}$$

We refer to the subnormalized states

$$\mathrm{Tr}_{A_2}\left[\left(\mathbb{I}_{A_1} \otimes M_{2,x_2}^{a_2}\right)\psi\psi^*\right] \tag{20}$$

for $a_2 \in \mathcal{A}_2, x_2 \in \mathcal{X}_2$ as the **steered states** for the first player, and the subnormalized states

$$\mathrm{Tr}_{A_1}\left[\left(M_{1,x_1}^{a_1} \otimes \mathbb{I}_{A_2}\right)\psi\psi^*\right] \tag{21}$$

as the steered states for the second player.

Definition 4. *Let H be a nonlocal m-player game (with notation as in Definition 1) . A **deterministic strategy** for H is an m-tuple $(S_1, S_2, \ldots, S_m)$ of functions $S_i \colon \mathcal{X}_i \to \mathcal{A}_i$. A **randomized strategy** for H is a probability distribution on the set of all deterministic strategies for H.*

Definition 5. *Let d be a positive integer and let $Y_1, Y_2, \ldots, Y_d, Z_1, Z_2, \ldots, Z_d$ be finite sets. Then a function*

$$f \colon Y_1 \times \cdots \times Y_d \to Z_1 \times \cdots \times Z_d \tag{22}$$

*is **time-ordered** if for all $i \in \{1, 2, \ldots, d-1\}$, the ith component of $f(y_1, y_2, \ldots, y_d)$ is independent of the values $y_{i+1}, y_{i+2}, \ldots y_d$.*

Let G be a sequential nonlocal m-player game (with notation as in Definition 2). Then, a deterministic strategy for G is an m-tuple $(S_1, S_2, \ldots, S_m)$ of functions $S_i \colon \mathcal{X}_i \to \mathcal{A}_i$ such that for all $i \in \{1, 2, \ldots, m\}$, S_i is time-ordered with respect to equations (17) and (18).

If H is a game and S is a strategy, then we will write $\omega(H, S)$ for the expected score of S. (For convenience, we will use this same notation regardless of whether H is sequential or whether S is a deterministic or quantum strategy.)

Definition 6. *Let H be an m-player nonlocal game. Then,*

- *The **classical value** of G, denoted $\omega^c(H)$, is the supremum of $\omega(H, S)$ over all deterministic strategies S. The **classical bias** of H, denoted $\beta^c(H)$, is the supremum of $|\omega(H, S)|$ over all deterministic strategies S.*
- *The **entangled value** of H, denoted $\omega^q(H)$, is the supremum of $\omega(H, T)$ over all quantum strategies T. The **quantum bias** of H, denoted $\beta^q(H)$, is the supremum of $|\omega(H, T)|$ over all quantum strategies T.*

Definition 7. *Let H be an m-player nonlocal game. The **classical-quantum ratio** of G is the quantity*

$$\frac{\beta_c(H)}{\beta_q(H)}. \tag{23}$$

Let H be an m-player nonlocal game whose scoring function has range $\{0,1\}$, and let k be a positive integer. Then H^d denotes n-fold parallel repeated game in which Alice$_1$, ..., Alice$_m$ play d instances of game H simultaneously. The score in H^d is 1 if Alice$_1$, ..., Alice$_m$ win all d of the games, and 0 if any of the n games is lost. Let $H^{[d]}$ denote the sequential nonlocal game that arises from having the players play d-rounds of game H in sequence. While it is easy to show that

$$\omega^c(H^{[d]}) \quad = \quad \omega^c(H)^d. \tag{24}$$

the same inequality does not necessarily hold when $H^{[d]}$ is replaced by H^d [13].

2.2 The Fourier Transform for Finite Abelian Groups

If G is a finite abelian group, then $\hat{G}$ (the dual group of G) denotes the set of all functions

$$h\colon G \to \mathbb{C} \setminus \{0\} \tag{25}$$

satisfying $h(x+y) = h(x)h(y)$ for all $x, y \in G$.

Definition 8. *Let G be a finite abelian group and let $f\colon G \to \mathbb{C}$ be a function. Then, the Fourier transform of f, denoted $\hat{f}$, is the function from $\hat{G}$ to $\mathbb{C}$ given by*

$$\hat{f}(h) \quad = \quad |G|^{-1/2} \sum_{x \in G} f(x)\overline{h(x)} \tag{26}$$

Note that in the case where $G = \mathbb{Z}_q^m$ where $q \geq 2$ and m are positive integers, then there is a natural isomorphism $i\colon G \to \hat{G}$ given by

$$i(g)(g') \quad = \quad \zeta^{-g \cdot g'} \tag{27}$$

for all $g, g' \in G$, where $\zeta = \exp(2\pi i/q)$. In this case, we can consider the Fourier transformed function $\hat{f}$ from Definition 8 as a function on G itself given by

$$\hat{f}(g) \quad = \quad |G|^{-1/2} \sum_{x \in G} f(x)\zeta^{x \cdot g}. \tag{28}$$

Definition 9. *Let G be a finite abelian group. If $f, g \in \hat{G}$, then the **convolution** of f and g, denoted by $f * g \in \mathbf{G}$, is defined as*

$$(f * g)(x) \quad = \quad |G|^{-1/2} \sum_{y \in G} f(x-y)g(y). \tag{29}$$

The following are commonly used facts:

- If $f\colon G \to \mathbb{C}$ is a function, then

$$f(x) \quad = \quad |G|^{-1/2} \sum_{h \in \hat{G}} \hat{f}(h)h(x) \tag{30}$$

- If $f\colon G \to \mathbb{C}$ is a function, then

$$\|f\|_2 \quad = \quad \left\|\hat{f}\right\|_2. \tag{31}$$

- If $f, g\colon G \to \mathbb{C}$ are functions, then

$$\hat{f} * \hat{g} \quad = \quad \widehat{(f \cdot g)}, \tag{32}$$

  where $f \cdot g$ denotes the pointwise product of f and g.

3 An Uncertainty Principle for Functions on Finite Abelian Groups

Let $r, s \colon \mathbb{R} \to \mathbb{C}$ be an infinitely differentiable function such that the Frobenius norm

$$\|r\|_2 \quad = \quad \sqrt{\int_{-\infty}^{\infty} |r(t)|^2 \, dt} \tag{33}$$

is equal to 1. Let $\hat{r} \colon \mathbb{R} \to \mathbb{C}$ denote the Fourier transform

$$\hat{r}(x) \quad = \quad \int_{-\infty}^{\infty} r(t) e^{-2\pi i x t} \tag{34}$$

Then, the Heisenberg uncertainty principle, interpreted mathematically (see Theorem 4.9 in [17]), asserts that the product of the variances

$$Var(r) \quad = \quad \left(\int_{-\infty}^{\infty} t^2 \, |r(t)|^2 \, dt \right) - \left(\int_{-\infty}^{\infty} t \, |r(t)|^2 \, dt \right)^2 \tag{35}$$

$$Var(\hat{r}) \quad = \quad \left(\int_{-\infty}^{\infty} t^2 \, |\hat{r}(t)|^2 \, dt \right) - \left(\int_{-\infty}^{\infty} t \, |\hat{r}(t)|^2 \, dt \right)^2 \tag{36}$$

is bounded below by a constant.

It is natural to ask whether a similar assertion exists for the Fourier transform over finite abelian groups. A commonly used uncertainty principle in the finite abelian case, attributed to Donoho and Stark [7], is the following. Rather than measuring the uncertainty of a function in terms of its variance, one measures it in terms of the size of the support of the function. A simple proof can be found in [17] (see subsection 3.1).

Theorem 2 ([7])**.** *Let G be an abelian group, and let $f \colon G \to \mathbb{C}$ be a function. Then,*

$$|\text{Supp } f| \left| \text{Supp } \hat{f} \right| \quad \geq \quad |G| \, . \quad \square \tag{37}$$

A number of variants of Theorem 2 are stated in section 3 of [17]. For the purpose of this work, we wish to understand the shape of the supports of f and $\hat{f}$ in the case where equality for the bound (37) is nearly achieved. This topic is touched on in papers such as [7, 16], but I have not yet found an uncertainty principle that suits our particular purposes. We therefore prove directly a strengthened version of Theorem 2.

We begin with two definitions.

Definition 10. *Let G be a finite abelian group, and let $f \colon G \to \mathbb{C}$ be a nonzero function. Let p be the probability distribution defined by $p = |f| \, / \, \|f\|_1$. Then, the* ***uniformity coefficient*** *of f is the quantity*

$$\nu(f) \quad = \quad \frac{\mathbf{P}[x = y \mid x, y \leftarrow \text{Supp } p]}{\mathbf{P}[x = y \mid a, b \leftarrow p]} \tag{38}$$

$$= \quad \frac{1}{|\text{Supp } p| \, \mathbf{P}[x = y \mid a, b \leftarrow p]}. \tag{39}$$

Definition 11. *Let G be a finite abelian group, and let $f \colon G \to \mathbb{C}$ be a nonzero function. Let p be the probability distribution defined by $p = |f| \, / \, \|f\|_1$. Then, the* ***linearity coefficient*** *of f is the quantity*

$$\eta(f) \quad = \quad \frac{\mathbf{P}[x + y = z + w \mid x, y, z, w \leftarrow p]}{\mathbf{P}[x = y \mid x, y \leftarrow p]}. \tag{40}$$

If S is a nonempty subset of G, then the linearity coefficient of S, denoted $\eta(S)$, is the linearity coefficient of the indicator function $\delta_{x \in S}$.

Proposition 2. *Let G be a finite abelian group and $f\colon G \to \mathbb{C}$ a nonzero function. Then, $\nu(f) \leq 1$, with equality if and only if $|f|$ is constant on* Supp f.

Proof. Let $p = |f| / \|f\|_1$. By the Cauchy-Schwartz inequality, we have

$$\begin{aligned} \nu(f)^{-1} &= \left(\sum_{x \in \text{Supp } p} p(x)^2\right)\left(\sum_{x \in \text{Supp } p} 1\right) && (41)\\ &\geq \left(\sum_{x \in \text{Supp } p} p(x) \cdot 1\right)^2 && (42)\\ &= 1, && (43) \end{aligned}$$

with equality if and only p is constant on Supp p. This completes the proof. □

Proposition 3. *Let G be a finite abelian group and let $f\colon G \to \mathbb{R}_{\geq 0}$ be a nonzero function. Then, $\eta(f) \leq 1$. Moreover, if $\eta(f) = 1$, then* Supp f *must be a coset of a subgroup of G.*

Proof. Let α denote the collision probability of p. By Proposition 1, we have

$$\begin{aligned} \mathbf{P}\left[x + y = z + w \mid x, y, z, w \leftarrow p\right] &= \sum_{y,w \in \text{Supp } p} p(y)p(w)\mathbf{P}[x + y = z + w \mid x, z \leftarrow p] && (44)\\ &\leq \sum_{y,w \in \text{Supp } p} p(y)p(w)\sqrt{\alpha^2} && (45)\\ &= \alpha. && (46) \end{aligned}$$

We conclude that $\eta(f) \leq 1$.

Now suppose that $\eta(f) = 1$. Then, equality occurs in line (45) above and therefore (also by Proposition 1) for any $y, w \in$ Supp p, the probability distributions $[x + y \mid x \leftarrow p]$ and $[z + w \mid z \leftarrow p]$ must be the same. In particular, this means that these two distributions have the same support. Therefore Supp p satisfies the following condition:

$$x, y, z \in \text{Supp } p \implies x + y - z \in \text{Supp } p. \tag{47}$$

Letting $H = (-y) + \text{Supp } p$, we have that for any $x, z \in$ Supp p, $(x-y)-(z-y) = x-z \in -y+\text{Supp } p = H$. We conclude that H is closed under differences:

$$a, b \in H \implies a - b \in H. \tag{48}$$

For any $b \in H$, the subtraction map $x \mapsto x - b$ on G is a permutation on G that maps H to itself, and therefore its inverse $x \mapsto x + b$ also maps H to itself. We conclude that H is also closed under addition. For any $a \in$ Supp p, since G is finite, we must have $n \cdot a = 0$ for some n, and therefore $0 = n \cdot a \in H$ and $-a = (n-1) \cdot a \in H$. We conclude that H is a subgroup of G. Therefore, Supp $p = y + H$ is a coset of a subgroup of G. □

Theorem 3. *Let G be a finite abelian group, and let $f, g\colon G \to \mathbb{C}$ be functions such that $\|g\|_2 = \|f\|_2 = 1$. Then,*

$$\left|\left\langle \hat{f}, g \right\rangle\right| \leq \left(\frac{|\text{Supp } f|\,|\text{Supp } g|\,\nu(f)\eta(f)}{|G|}\right)^{1/4}. \tag{49}$$

Before presenting the proof of Theorem 3, if we take $g = \hat{f}$, we note the following corollary.

Corollary 1. *Let G be a finite group and let $h\colon G \to \mathbb{C}$ be a nonzero function. Then,*

$$\frac{|\text{Supp } h| \left|\text{Supp } \hat{h}\right| \nu(h)\eta(h)}{|G|} \quad \geq \quad 1. \tag{50}$$

Proof. Apply Theorem 3 with $f = h/\left\|h\right\|_2$ and $g = \hat{f}$. □

This corollary implies that if the ratio of $|\text{Supp } h| \left|\text{Supp } \hat{h}\right|$ to $|G|$ is close to 1, then $\nu(h)$ and $\eta(h)$ must be close to 1. Thus, informally, if equality is nearly achieved in Theorem 2, then h is close to being uniformly supported on a coset of a subgroup of G.

Proof of Theorem 3. We begin by applying the Cauchy-Schwartz inequality twice to get an upper bound on $\left|\left\langle \hat{f}, g\right\rangle\right|$:

$$\begin{aligned}
\left|\left\langle \hat{f}, g\right\rangle\right|^4 &= \left|\sum_{x\in\text{Supp } g} \hat{f}(x)\overline{g(x)}\right|^4 && (51)\\
&\leq \left(\left(\sum_{x\in\text{Supp } g} \left|\hat{f}(x)\right|^2\right)\left(\sum_{x\in\text{Supp } g} |g(x)|^2\right)\right)^2 && (52)\\
&= \left(\left(\sum_{x\in G} \left|\hat{f}(x)\right|^2 \cdot \delta_{x\in\text{Supp } g}\right)^2 (1)^2\right)^2 && (53)\\
&\leq \left(\sum_{x\in G} \left|\hat{f}(x)\right|^4\right)\left(\sum_{x\in G} \delta^2_{x\in\text{Supp } g}\right) && (54)\\
&= \left(\sum_{x\in G} \left|\hat{f}(x)\right|^4\right)|\text{Supp } g| && (55)
\end{aligned}$$

Observing that the first factor in the product (55) is equal to $\left\|\hat{f}\cdot\hat{f}\right\|_2^2$, where $\hat{f}\cdot\hat{f}$ denotes the pointwise

product of $\hat{f}$ with itself, we have

$$\begin{aligned}
\left|\left\langle \hat{f}, g\right\rangle\right|^4 &\leq \left\|\hat{f}\cdot\hat{f}\right\|_2^2 |\text{Supp } g| && (56)\\
&= \left\|\widehat{f*f}\right\|_2^2 |\text{Supp } g| && (57)\\
&= \|f*f\|_2^2 |\text{Supp } g| && (58)\\
&= \left(\sum_{x\in G}(f*f)(x)\overline{(f*f)(x)}\right)|\text{Supp } g| && (59)\\
&= |G|^{-1}\left(\sum_{x\in G}\left(\sum_{\substack{y,z\in G\\ y+z=x}} f(y)f(z)\right)\left(\sum_{\substack{y',z'\in G\\ y'+z'=x}}\overline{f(y')f(z')}\right)\right)|\text{Supp } g| && (60)\\
&= |G|^{-1}\left(\sum_{\substack{y,z,y',z'\in G\\ y+z=y'+z'}} f(y)f(z)\overline{f(y')f(z')}\right)|\text{Supp } g| && (61)\\
&\leq |G|^{-1}\left(\sum_{\substack{y,z,y',z'\in G\\ y+z=y'+z'}} |f(y)f(z)f(y')f(z')|\right)|\text{Supp } g| && (62)
\end{aligned}$$

Let $p = |f| / \|f\|_1$, and let $\alpha = \mathbf{P}\left[x = y \mid x, y \leftarrow p\right]$ denote the collision probability for p. Note that

$$\begin{aligned}
\alpha &= \sum_{x\in G} p(x)^2 && (63)\\
&= \|f\|_1^{-2}\sum_{x\in G}|f(x)|^2 && (64)\\
&= \|f\|_1^{-2}. && (65)
\end{aligned}$$

We have

$$\begin{aligned}
\left|\left\langle \hat{f}, g\right\rangle\right|^4 &\leq |G|^{-1}\|f\|_1^4\left(\sum_{\substack{y,z,y',z'\in G\\ y+z=y'+z'}} p(y)p(z)p(y')p(z')\right)|\text{Supp } g| && (66)\\
&= |G|^{-1}\alpha^{-2}\left(\sum_{\substack{y,z,y',z'\in G\\ y+z=y'+z'}} p(y)p(z)p(y')p(z')\right)|\text{Supp } g| && (67)\\
&= |G|^{-1}\alpha^{-2}\left(\mathbf{P}\left[y+z=y'+z' \mid y,z,y',z'\leftarrow p\right]\right)|\text{Supp } g| && (68)\\
&= |G|^{-1}\alpha^{-1}\eta(f)\,|\text{Supp } g| && (69)\\
&= |G|^{-1}\,|\text{Supp } f|\,\nu(f)\eta(f)\,|\text{Supp } g|, && (70)
\end{aligned}$$

which implies the desired result. □

4 The GHZ Games

The GHZ games [11] are binary games played by 3 or more players.

Definition 12. *Let $k \geq 3$ be an integer. Then, the k-player game GHZ_k is defined as following:*

- *The input and output alphabets for each player are $\{0,1\}$.*
- *The input probability distribution is given as follows, for $\mathbf{x} \in \{0,1\}^k$:*

$$r(\mathbf{x}) \quad = \quad \begin{cases} 2^{-k+1} & \text{if } x_1 \oplus \cdots \oplus x_k = 0 \\ \\ 0 & \text{otherwise.} \end{cases} \tag{71}$$

- *The score is equal to 1 if*

$$x_1 + x_2 + \ldots + x_k + 2a_1 + 2a_2 + \ldots + 2a_k \quad \equiv \quad 0 \pmod 4. \tag{72}$$

and is equal to 0 otherwise.

The entangled value of GHZ_k is always 1, while the classical value can be shown to decrease exponentially in k by elementary arguments (see [11]). A considerably more difficult problem is to upper bound the classical value of the parallel repeated game GHZ_k^d when k is fixed and d tends to infinity. The following result was recently proved.

Theorem 4 (Theorem 1.1 in [4])**.** *The parallel repeated games GHZ_3^d satisfy*

$$\omega^c(GHZ_3^d) \quad \leq \quad \exp(-\Omega(d)). \quad \square \tag{73}$$

The following corollary is a consequence.

Corollary 2. *The parallel repeated games GHZ_4^d satisfy*

$$\omega^c(GHZ_4^d) \quad \leq \quad \exp(-\Omega(d)). \tag{74}$$

Proof. See Appendix A.1. $\square$

4.1 Parity-balanced subsets of $\mathbb{Z}_4^d$

Definition 13. *Let d be a positive integer. A set $S \subseteq \mathbb{Z}_4^d$ is a **parity-balanced subset** of $\mathbb{Z}_4^d$ if the quotient map*

$$\mathbb{Z}_4^d \quad \to \quad \mathbb{Z}_2^d \tag{75}$$

induces a bijection between S and $\mathbb{Z}_2^d$.

Informally, a subset of $\mathbb{Z}_4^d$ is parity-balanced if it is of size 2^d and if its residues mod 2^d are evenly distributed over $\mathbb{Z}_2^d$. A parity-balanced set $S \subseteq \mathbb{Z}_4^d$ naturally gives a deterministic strategy for a single player at the d-fold repeated GHZ game: for an input bit string $\mathbf{x}$, there is a unique element $s_{\mathbf{x}} \in S$ that is congruent mod 2 to $\mathbf{x}$, and the player returns the unique bit string $\mathbf{a}$ that satisfies

$$s_{\mathbf{x}} \quad = \quad \mathbf{x} + 2\mathbf{a}. \tag{76}$$

To specify a full deterministic strategy GHZ_k, it suffices to specify a parity-balanced set $S_j \subseteq \mathbb{Z}_4^d$ for the jth player, for $j \in \{1, 2, \ldots, k\}$. The expected winning probability of the corresponding strategy is then

$$\mathbf{P}\left[s_1 + s_2 + \ldots + s_k = 0 \mid (s_1, s_2, \ldots, s_k) \leftarrow (S_1, S_2, \ldots, S_k), s_1 + s_2 + \ldots + s_k \in 2\mathbb{Z}_4^d\right] \tag{77}$$

$$= \quad 2^d \cdot \mathbf{P}\left[s_1 + s_2 + \ldots + s_k = 0 \mid (s_1, s_2, \ldots, s_k) \leftarrow (S_1, S_2, \ldots, S_k)\right]. \tag{78}$$

Let T be a parity-balanced subset of $\mathbb{Z}_4^d$. In the case $k = 4$ and $S_1 = S_2 = T$, $S_3 = S_4 = -T$, we obtain the following expression for the winning probability of the associated GHZ_4^d-strategy,

$$2^d \cdot \mathbf{P}\left[t_1 + t_2 - t_3 - t_4 = 0 \mid t_1, t_2, t_3, t_4 \leftarrow T\right], \tag{79}$$

which is precisely equal to the linearity coefficient $\eta(T)$ of T. We therefore obtain the following proposition, which will be important in section 5.

Proposition 4. *Let T be a parity-balanced subset of $\mathbb{Z}_4^d$. Then,*

$$\eta(T) \quad \leq \quad \omega^c(GHZ_4^d). \tag{80}$$

As a consequence, by Corollary 2, any parity-balanced subset of $\mathbb{Z}_4^d$ has linearity coefficient that is upper-bounded by a uniform exponentially-vanishing function of d.

In analogy to Definition 5, we make the following definition

Definition 14. *Let d be a positive integer. A set $S \subseteq \mathbb{Z}_4^d$ is a **time-ordered parity-balanced subset** of $\mathbb{Z}_4^d$ if it is of the form*

$$S \quad = \quad \left\{\mathbf{x} + 2f(\mathbf{x}) \mid \mathbf{x} \in \{0,1\}^d\right\} \tag{81}$$

where $f\colon \{0,1\}^d \to \{0,1\}^d$ is a time-ordered function.

By the same construction as above, any time-ordered parity balanced subset $T \subseteq \mathbb{Z}_4^d$ yields a deterministic strategy for the sequential game $GHZ_4^{[d]}$ whose expected score is $\eta(T)$. Since $\omega^c(GHZ_4^{[d]}) = \omega^c(GHZ_4)^d = (3/4)^d$ (see Appendix A.2), we have the following.

Proposition 5. *Let T be a time-ordered parity-balanced subset of $\mathbb{Z}_4^d$. Then,*

$$\eta(T) \quad \leq \quad (3/4)^d. \tag{82}$$

5 A Nonlocal Game for Claw-States

Our goal in this section is to construct a family $\{H_d\}_{d\in\mathbb{N}}$ of two-player nonlocal games satisfying the following properties:

- The classical-to-quantum ratio is upper bounded by $\exp(-\Omega(d))$.
- For each n, there is an optimal strategy for G_n in which the steered states for one of the players are claw-states of length $O(d)$.
- The input and output alphabets are all of size $\exp(O(d))$.

Game $\mathbf{J}_d$, in Figure 1, will be shown to satisfy all three of the above conditions. It can be seen as a derivative of the Hidden Matching game [5] and the GHZ games (Definition 12). We additionally define Game $\mathbf{J}'_d$, (Figure 2)which is a sequential version of $\mathbf{J}_d$ in which the communication between the referee and the second player (Bob) is done in $(d+1)$ rounds.

5.1 A Quantum Strategy for $\mathbf{J}_d$

Proposition 6. *Let d be a positive integer. There exists a quantum strategy for $\mathbf{J}_d$ that achieves an expected score of $\sqrt{2}/2$.*

Proof. Let A and B be $(d+1)$-qubit registers, with $A = A_1 \otimes \ldots \otimes A_{d+1}$, $B = B_1 \otimes \ldots \otimes B_{d+1}$ and $A_i \cong B_i \cong \mathbb{C}^2$ for all $i \in \{1, 2, \ldots, d+1\}$. Let $\psi \in \mathcal{A} \otimes B$ be the maximally entangled state

$$\psi \quad = \quad 2^{-(d+1)/2} \sum_{\mathbf{z}\in\{0,1\}^d} |\mathbf{z}\rangle \otimes |\mathbf{z}\rangle\,. \tag{85}$$

For any $\mathbf{x}, \mathbf{a} \in \{0,1\}^{d+1}$ with $x_{d+1} = 1$, let $M_{\mathbf{x}}^{\mathbf{a}}$ denote the projector in A onto the subspace spanned by

$$\theta_{\mathbf{x}}^{\mathbf{a}} \quad = \quad \frac{1}{\sqrt{2}}\left(|a_1, a_2, \ldots, a_d, 0\rangle + (-1)^{a_{d+1}} |a_1 \oplus x_1, a_2 \oplus x_2, \ldots, a_d \oplus x_d, 1\rangle\right) \tag{86}$$

Game $\mathbf{J}_d$:

Parameter: A positive integer d
Parties: Referee, Alice, Bob.

1. Referee samples two bit strings $\mathbf{x}, \mathbf{y} \in \{0,1\}^{d+1}$ uniformly at random under the constraint $x_{d+1} = y_{d+1} = 1$.
2. Referee sends $\mathbf{x}$ to Alice and receives output $\mathbf{a} \in \{0,1\}^{d+1}$.
3. Referee sends $\mathbf{y}$ to Bob and receives output $\mathbf{b} \in \{0,1\}^{d+1}$.
4. Referee computes $\mathbf{u}, \mathbf{v} \in \mathbb{Z}^{d+1}$ as follows:

$$u_i = x_i(-1)^{a_i}, \tag{83}$$
$$v_i = y_i + 2b_i. \tag{84}$$

5. Referee assigns a score of $+1$ if $\mathbf{u} \cdot \mathbf{v}$ is congruent to 0 or 1 mod 4, and assigns a score of -1 if $\mathbf{u} \cdot \mathbf{v}$ is congruent to 2 or 3 mod 4.

Figure 1: The nonlocal game $\mathbf{J}_d$.

Game $\mathbf{J}'_d$:

Game $\mathbf{J}'_d$ is the same as Game $\mathbf{J}_d$, except that the following sequential communication step replaces Step 3:

3. For $i = 1, 2, 3, \ldots, d+1$, Referee sends y_i to Bob and receives output $b_i \in \{0,1\}^d$.

Figure 2: The nonlocal game $\mathbf{J}'_d$.

For any $\mathbf{y}, \mathbf{b} \in \{0,1\}^{d+1}$ with $y_{d+1} = 1$, let $N_{\mathbf{y}}^{\mathbf{b}}$ denote the projector in B onto the state

$$\phi_{\mathbf{y}}^{\mathbf{b}} \quad = \quad \left(\bigotimes_{j=1}^{d} \left(Z^{y_i/2} Z^{b_i} \left|+\right\rangle \right) \right) \otimes \left(Z^{1/4} Z^{b_{d+1}} \left|+\right\rangle \right) \tag{87}$$

We note (following previous work, e.g., [1]) that for any $j \in \{1, 2, 3, \ldots, d\}$, applying a gate of the form Z^c (with $c \in \mathbb{R}$) to the jth qubit of $\theta_{\mathbf{x}}^{\mathbf{a}}$ yields the same result as applying the gate

$$Z^{x_j (-1)^{a_j} c} \tag{88}$$

to the $(d+1)$st qubit of $\theta_{\mathbf{x}}^{\mathbf{a}}$. Therefore, if we let $U \colon (\mathbb{C}^2)^{\otimes(d+1)} \to (\mathbb{C}^2)^{\otimes(d+1)}$ be the following unitary operator (which maps $\left|+\right\rangle^{\otimes(d+1)}$ to $\phi_{\mathbf{y}}^{\mathbf{b}}$):

$$U \quad = \quad Z^{y_1/2} Z^{b_1} \otimes Z^{y_2/2} Z^{b_2} \otimes \cdots \otimes Z^{y_d/2} Z^{b_d} \otimes Z^{1/4} Z^{b_{d+1}}, \tag{89}$$

then,

$$\begin{aligned}
\psi^* \left(M_{\mathbf{x}}^{\mathbf{a}} \otimes N_{\mathbf{y}}^{\mathbf{b}} \right) \psi \quad &= \quad 2^{-(d+1)} \left| \left\langle \theta_{\mathbf{a}}^{\mathbf{x}} \mid \overline{\phi_{\mathbf{y}}^{\mathbf{b}}} \right\rangle \right|^2 && (90) \\
&= \quad 2^{-(d+1)} \left| \left\langle \theta_{\mathbf{a}}^{\mathbf{x}} \mid U^{-1}(+^{\otimes d}) \right\rangle \right|^2 && (91) \\
&= \quad 2^{-(d+1)} \left| \left\langle U\left(\theta_{\mathbf{a}}^{\mathbf{x}}\right) \mid (+^{\otimes d}) \right\rangle \right|^2 && (92) \\
&= \quad 2^{-(d+1)} \left| \left\langle Z_{A_{d+1}}^{K}\left(\theta_{\mathbf{a}}^{\mathbf{x}}\right) \mid (+^{\otimes d}) \right\rangle \right|^2 && (93)
\end{aligned}$$

where

$$\begin{aligned}
K \quad &= \quad 1/4 + b_{d+1} + \sum_{i=1}^{d} \left(\frac{y_i}{2} + b_i \right) x_i (-1)^{a_i} && (94) \\
&= \quad 1/4 + b_{d+1} + \sum_{i=1}^{d} \frac{u_i v_i}{2}. && (95)
\end{aligned}$$

We have

$$Z_{A_{d+1}}^{K} \theta_{\mathbf{x}}^{\mathbf{a}} \quad = \quad \frac{1}{\sqrt{2}} \left(\left|a_1, a_2, \ldots, a_d, 0\right\rangle + (-1)^{a_{d+1}+K} \left|a_1 \oplus x_1, a_2 \oplus x_2, \ldots, a_d \oplus x_d, 1\right\rangle \right), \tag{96}$$

and

$$a_{d+1} + K \quad = \quad 1/4 + (a_{d+1} + b_{d+1}) + \sum_{i=1}^{d} \frac{u_i v_i}{2}. \tag{97}$$

By inspection, we find that $a_{d+1} + b_{d+1} \equiv (u_{d+1} v_{d+1})/2 - 1/2 \pmod 2$, and therefore

$$Z_{A_{d+1}}^{K} \theta_{\mathbf{x}}^{\mathbf{a}} \quad = \quad \frac{1}{\sqrt{2}} \left(\left|a_1, a_2, \ldots, a_d, 0\right\rangle + (-1)^{-1/4 + \langle \mathbf{u}, \mathbf{v} \rangle / 2} \left|a_1 \oplus x_1, a_2 \oplus x_2, \ldots, a_d \oplus x_d, 1\right\rangle \right) \tag{98}$$

Therefore, calculating explicitly the inner product in (93),

$$\begin{aligned}
\psi^* \left(M_{\mathbf{x}}^{\mathbf{a}} \otimes N_{\mathbf{y}}^{\mathbf{b}} \right) \psi \quad &= \quad 2^{-(d+1)} \left| 2^{-1/2} \cdot 2^{-(d+1)/2} + 2^{-1/2} (-1)^{-1/4 + \langle \mathbf{u}, \mathbf{v} \rangle / 2} \cdot 2^{-(d+1)/2} \right|^2 && (99) \\
&= \quad 2^{-2(d+1)} \left| \frac{1 + (-1)^{-1/4 + \langle \mathbf{u}, \mathbf{v} \rangle / 2}}{\sqrt{2}} \right|^2 && (100) \\
&= \quad \begin{cases} 2^{-2(d+1)} \left(1 + \frac{1}{\sqrt{2}}\right) & \text{if } \langle \mathbf{u}, \mathbf{v} \rangle = 0 \text{ or } 1 \\ 2^{-2(d+1)} \left(1 - \frac{1}{\sqrt{2}}\right) & \text{if } \langle \mathbf{u}, \mathbf{v} \rangle = 2 \text{ or } 3 \end{cases} && (101)
\end{aligned}$$

For any fixed $\mathbf{x}, \mathbf{y} \in \{0,1\}^{d+1}$ with $x_{d+1} = y_{d+1} = 1$, it easily checked that exactly half of the 2^{2d+2} pairs $(\mathbf{a}, \mathbf{b})$ satisfy the condition $\langle \mathbf{u}, \mathbf{v} \rangle \in \{0,1\}$.[1] Therefore, if $\mathbf{x}, \mathbf{y}$ are given as input to Alice and Bob, then their output will achieve a score of $+1$ with probability $(1/2)(1 + 1/\sqrt{2})$ and a score of -1 with probability $(1/2)(1 - 1/\sqrt{2})$, yielding an expected score of

$$(1)(1/2)\left(1 + \frac{1}{\sqrt{2}}\right) + (-1)(1/2)\left(1 - \frac{1}{\sqrt{2}}\right) \quad = \quad \frac{1}{\sqrt{2}}, \tag{102}$$

as desired. □

Informally, we note that the strategy described in Proposition 6 also achieves an expected score of $\sqrt{2}/2$ at Game $\mathbf{J}'_n$. However, we will not need to formalize that fact here.

5.2 The Classical Value of $\mathbf{J}_d$

Theorem 5. *The games* $\{\mathbf{J}_d\}_{d \geq 1}$ *satisfy*

$$\beta^c(\mathbf{J}_d) \quad \leq \quad \exp(-\Omega(d)). \tag{103}$$

Proof. Let GHZ_4 denote the 4-player GHZ game (Definition 12). Our approach will be to prove the following inequality:

$$\beta_c(\mathbf{J}_d) \quad \leq \quad 2\omega_c(GHZ_4^d)^{1/4}, \tag{104}$$

from which inequality (103) then follows by Corollary 2.

Fix a positive integer d. Let (S, T) be a deterministic strategy for $\mathbf{J}_d$ such that the absolute value of the score achieved by (S, T) is $\beta_c(\mathbf{J}_d)$. We first compute a simple expression for the expected score achieved by (S, T). Let $U \subseteq \mathbb{Z}_4^{d+1}$ be the set of all vectors of the form

$$(x_1(-1)^{S_1(\mathbf{x})}, x_2(-1)^{S_2(\mathbf{x})}, \ldots, x_{d+1}(-1)^{S_{d+1}(\mathbf{x})}) \tag{105}$$

with $\mathbf{x} \in \{0,1\}^d \times \{1\}$. Expressed differently, U is the set of all possible values for the vector $\mathbf{u}$ in Figure 1 (considered as an element of $\mathbb{Z}_4^{d+1}$) when the Game $\mathbf{J}_d$ is played with strategy (S, T). Similarly, let $V \subseteq \mathbb{Z}_4^{d+1}$ be the set of all vectors of the form

$$(y_1 + 2T_1(\mathbf{y}), y_2 + 2T_2(\mathbf{y}), \ldots, y_{d+1} + 2T_{d+1}(\mathbf{y})). \tag{106}$$

with $\mathbf{y} \in \{0,1\}^d \times \{1\}$. The set V is the set of residues mod 4 of all possible values for the vector $\mathbf{v}$ in Figure 1. (We note that, although U is not a parity-balanced subset of $\mathbb{Z}_4^{d+1}$ according to Definition 13, it becomes a parity-balanced subset of $\mathbb{Z}_4^d$ if we drop the last coordinate of each vector that it contains. The same is true of V.) The expected score for the strategy (S, T) can then be succinctly represented as

$$\omega^c(\mathbf{J}_d, (S, T)) \quad = \quad \mathbf{E}\left[\mathrm{Re}\left[(1-i)i^{\mathbf{u}\cdot\mathbf{v}}\right] \mid \mathbf{u} \leftarrow U, \mathbf{v} \leftarrow V\right]. \tag{107}$$

From equation 107, we can derive a formula in terms of the Fourier transform. Let $g, f \colon \mathbb{Z}_4^n \to \mathbb{C}$ be defined by

$$g(\mathbf{z}) \quad = \quad 2^{-n/2}\delta_{\mathbf{z} \in U} \tag{108}$$

$$f(\mathbf{z}) \quad = \quad 2^{-n/2}\delta_{\mathbf{z} \in V}, \tag{109}$$

[1] The pairs that satisfy this condition are in one-to-one correspondence with the pairs that do not, via the NOT map on a_{d+1}.

Note that $\|f\|_2 = \|g\|_2 = 1$. We have

$$\begin{aligned}
\beta^c(\mathbf{J}_d) &= |\omega^c(\mathbf{J}_d, (S,T))| && (110)\\
&= \left| 2^{-2d} \mathrm{Re}\left[(1-i) \sum_{\substack{\mathbf{u}\in U \\ \mathbf{v}\in V}} i^{\mathbf{u}\cdot\mathbf{v}} \right] \right| && (111)\\
&= \left| 2^{-2d} \mathrm{Re}\left[(1-i) \sum_{\mathbf{u},\mathbf{v}\in\mathbb{Z}_4^{n+1}} i^{\mathbf{u}\cdot\mathbf{v}} \delta_{\mathbf{v}\in V} \delta_{\mathbf{u}\in U} \right] \right| && (112)\\
&= \left| 2^{-d} \mathrm{Re}\left[(1-i) \sum_{\mathbf{u},\mathbf{v}\in\mathbb{Z}_4^{n+1}} i^{\mathbf{u}\cdot\mathbf{v}} f(\mathbf{u}) g(\mathbf{v}) \right] \right| && (113)\\
&= \left| 2^{-d} \mathrm{Re}\left[(1-i) \left\langle 2^{d+1} \hat{f}, g \right\rangle \right] \right| && (114)\\
&= \left| 2 \cdot \mathrm{Re}\left[(1-i) \left\langle \hat{f}, g \right\rangle \right] \right| && (115)
\end{aligned}$$

which yields the inequality

$$\beta^c(\mathbf{J}_n) \leq 2\sqrt{2} \left| \left\langle \hat{f}, g \right\rangle \right|. \quad (116)$$

Next we apply Theorem 3. We have

$$\begin{aligned}
\beta^c(\mathbf{J}_d) &\leq 2\sqrt{2} \left| \left\langle \hat{f}, g \right\rangle \right| && (117)\\
&\leq 2\sqrt{2} \left(\frac{|\mathrm{Supp}\ f|\, |\mathrm{Supp}\ g|\, \nu(f)\eta(f)}{\left|\mathbb{Z}_4^{d+1}\right|} \right)^{1/4} && (118)
\end{aligned}$$

Noting that $|\mathrm{Supp}\ f| = |\mathrm{Supp}\ g| = 2^d$, $\left|\mathbb{Z}_4^{d+1}\right| = 4^{d+1}$, and $\nu(f) = 1$ (Proposition 2), we have

$$\begin{aligned}
\beta^c(\mathbf{J}_d) &\leq 2\sqrt{2} \left(\frac{\eta(f)}{4} \right)^{1/4} && (119)\\
&= 2\eta(f)^{1/4} && (120)\\
&= 2\eta(V)^{1/4}. && (121)
\end{aligned}$$

Let V' denote the subset of $\mathbb{Z}_4^d$ that arises from dropping the last coordinate of each vector in V. It is easy to see that $\eta(V) \leq \eta(V')$ (see Appendix A.3). The set V' is a parity-balanced subset of $\mathbb{Z}_4^d$, and so by applying Proposition 4, we have

$$\begin{aligned}
\beta^c(\mathbf{J}_d) &\leq 2\eta(V)^{1/4} && (122)\\
&\leq 2\eta(V')^{1/4} && (123)\\
&\leq 2(\omega^c(GHZ_4^d))^{1/4}, && (124)
\end{aligned}$$

as desired. □

We prove a stronger result for Game $\mathbf{J}'_d$.

Theorem 6. *The games* $\{\mathbf{J}'_d\}_{d\geq 1}$ *satisfy*

$$\beta^c(\mathbf{J}'_d) \leq 2 \cdot (3/4)^{d/4}. \quad (125)$$

Parameters:

q:	modulus
Q:	the binary length of integers mod q
m, n:	matrix dimensions
σ:	standard deviation for Gaussian noise
τ:	truncation parameter for Gaussian noise
d:	binary secret length

Assumptions:

- $n = \lambda$
- q is always an odd prime, and $q \leq \exp(O(\lambda))$
- $d \leq (\log \lambda)^{O(1)}$ and $d \leq \lambda$
- $Q = \lceil \log q \rceil$
- $m = (2Q + 1)n$
- $\tau = \lfloor q/(4mQ) \rfloor$
- $\omega(1) < \sigma \leq o(\tau/m)$

Figure 3: Parameters for Section 6. q, Q, m, n, d are positive-integer valued functions of λ, and σ, τ are functions of λ that take on positive real values.

Proof. The same proof as for Theorem 5 applies, with $\mathbf{J}_d$ replaced by $\mathbf{J}'_d$, and we merely need to observe that since Bob behaves sequentially in Game $\mathbf{J}'_d$, the set V' is time-ordered (Definition 14). Therefore, applying Proposition 5,

$$\begin{aligned} \beta^c(\mathbf{J}'_d) &\leq 2\eta(V')^{1/4} && (126) \\ &\leq 2 \cdot (3/4)^{d/4}, && (127) \end{aligned}$$

as desired. □

6 Proofs of Quantumness

The setup in this section is based on [1], and we use much of the same notation. Throughout this section, $\lambda \in \mathbb{N}$ denotes a security parameter. When we refer to an algorithm as "polynomial-time," we mean polynomial in λ.

Figure 6 states the assumed constraints for seven parameters $(n, m, q, Q, \sigma, \tau, d)$, each of which is assumed to be a function of λ. These constraints imply, in particular, that $q \geq \Omega(n^2\sigma)$. An example of parameters that satisfy all of the constraints given in Figure 6 is the following:

$$\begin{aligned} n(\lambda) &= \lambda \\ q(\lambda) &= \text{an odd prime between } \lambda^3 \text{ and } 2\lambda^3 \\ d(\lambda) &= \lfloor \log \lambda \rfloor \\ \sigma(\lambda) &= \sqrt{\lambda}, \end{aligned}$$

with Q, m, τ are set according to the formulas in Figure 6.

Definition 15. *For any positive real number s, the* ***discrete Gaussian distribution*** *on $\mathbb{Z}$ with standard deviation s, denoted by $G(s)$, is the probability distribution on $\mathbb{Z}$ given by*

$$G(s)(j) \quad = \quad \frac{e^{-j^2/2s^2}}{\sum_{j\in\mathbb{Z}} e^{-j^2/2s^2}}. \tag{128}$$

If t is a positive real number, the ***truncated discrete Gaussian*** *$G(s,t)$ is the distribution on $\mathbb{Z}$ that arises from restricting $G(s)$ to the subset $\{j \mid |j| \leq t\}$ and normalizing.*

6.1 Learning With Errors

The Learning With Errors problem (LWE) has multiple variants. We state a "decisional" version of the problem. In the following, χ represents a probability distribution on $\mathbb{Z}$.

The LWE(n,q,χ) **Problem.** Fix $s \leftarrow \mathbb{Z}_q^n$ and $b \leftarrow \{0,1\}$. Let $\mathcal{D}_0$ be an oracle that outputs samples in $\mathbb{Z}_q^{n+1}$ of the form

$$(a, a\cdot s + e) \tag{129}$$

where $a \leftarrow \mathbb{Z}_q^n$ and $e \leftarrow \chi$, and let $\mathcal{D}_1$ be an oracle that outputs uniformly random samples in $\mathbb{Z}_q^{n+1}$. Given oracle access to $\mathcal{D}_b$, compute b.

When we say that we assume that the LWE(n,q,χ) problem is hard, we mean that we assume that any non-uniform polynomial-time randomized classical algorithm solves the LWE(n,q,χ) problem with probability at most $\frac{1}{2} + \text{negl}(\lambda)$.

We will make use of random matrices in $\mathbb{Z}_q^{m\times n}$ that are generated with a trapdoor that allows for the efficient inversion of LWE samples. The following theorem comes from [12], although we will refer instead to a version from [1] because it includes an explicit error term.

Theorem 7. *There is a probabilistic polynomial-time algorithm* GenTrap() *and a deterministic polynomial-time algorithm* Invert(A,t,v) *satisfying the following conditions.*

- *The algorithm* GenTrap() *returns a pair (A,t) where $A \in \mathbb{Z}_q^{m\times n}$. The probability distribution of A on $\mathbb{Z}_q^{m\times n}$ is within statistical distance $nQ2^{-n/2}$ from a uniform distribution.*
- *If $(A,t) \leftarrow$ GenTrap and $s \in \mathbb{Z}_q^n, e \in \mathbb{Z}_q^m$ are vectors such that $\|e\|_\infty \leq 2\tau$, then* Invert$(A,t,As+e) = s$.

Proof. See Subsection 3.5 and Appendix C in [1]. □

Remark 2. *Theorem 7 implies that if $(A,t) \leftarrow$ GenTrap() and $v \in \mathbb{Z}_q^m$, there is at most one vector $s \in \mathbb{Z}_q^n$ such that $\|v - As\|_\infty \leq 2\tau$. If no such vector s exists, then we will assume that* Invert$(A,t,v) = \perp$.

We use Theorem 7 to build an encryption algorithm Encrypt, shown in Figure 4. The following proposition is easy to prove based on standard reductions.

Proposition 7. *Assume that $LWE(n,q,G(\sigma))$ is hard. Let $(x_1,\ldots,x_d) \leftarrow \{0,1\}^d$ and*

$$(A,v,t) \leftarrow \text{Encrypt}(x_1x_2\ldots x_d). \tag{130}$$

Then, the probability distribution of $(A,v,x_1x_2\ldots x_d)$ is computationally indistinguishable from the uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q \times \{0,1\}^d$. □

Algorithm Encrypt(h)**:**

Input: A bit string $h \in \{0,1\}^d$
Output: A matrix $A \in \mathbb{Z}_q^{m \times n}$, a vector $v \in \mathbb{Z}_q^m$, and a classical register t.

1. Compute $(A, t) \leftarrow \text{GenTrap}()$.
2. Compute $s \in \mathbb{Z}_q^n$ and $e \in \mathbb{Z}_q^m$ by sampling every entry of s and e independently from $G(\sigma, \tau)$.
3. Let $M \in \mathbb{Z}_q^n$ be a vector whose first $n-d$ entries are all zero and whose $n-d+j$th entry is h_j, and let $\gamma = (2s + M)$. Compute

$$v := A\gamma + e \in \mathbb{Z}_q^m.$$

   Return (A, v, t).

Figure 4: An encryption algorithm, in which (A, v) is the ciphertext and t is the secret key.

Game R:

Parties: Referee (verifier) and Alice (prover)

1. Referee samples random bit strings $\mathbf{x}, \mathbf{y} \in \{0,1\}^{d+1}$ subject to the constraint $x_{d+1} = y_{d+1} = 0$.
2. Referee computes

$$(A, v, t) := \text{Encrypt}(x_1 x_2 \dots x_d).$$

   Referee sends A and v to Alice.
3. Alice returns a vector $w \in \mathbb{Z}_q^m$ and an indexed set of bits $\{\ell_j\}_{j \in S}$, where

$$S \quad = \quad \{1, 2, \dots, nQ\} \setminus \{(n-d+1)Q, (n-d+2)Q, \dots, nQ\}.$$

4. Referee computes $z := \text{Invert}(A, t, w)$, $z' := \text{Invert}(A, t, w + v)$,[2] and assigns

$$a_j \quad := \quad \begin{cases} 0 & \text{if } z_{n-d+j} \text{ is even,} \\ 1 & \text{otherwise.} \end{cases}$$

   for $i = 1, 2, \dots, d$, and

$$a_{d+1} \quad := \quad \bigoplus_{j \in S} \left(\left([z]_j \oplus [z']_j \right) \wedge \ell_j \right).$$

5. Referee sends the vector $\mathbf{y}$ to Alice. Alice returns a vector $\mathbf{b} \in \{0,1\}^{n+1}$.
6. Referee computes $u_j := x_j (-1)^{a_j}$ and $v_j = y_j + 2b_j$ for $j = 1, 2, \dots, n+1$. If $\mathbf{u} \cdot \mathbf{v}$ is equal to 0 or 1 mod 4, then Referee awards a score of $+1$. Otherwise, Referee awards a score of -1.

Figure 5: An Interactive Proof of Quantumness

Game R′:

Game $\mathbf{R}'$ is the same as Game $\mathbf{R}$ except that Step 5 is replaced with the following sequential interaction between Referee and Alice.

5. For $j = 1, 2, 3, \ldots, d+1$, Referee sends y_j to Alice and receives output $b_j \in \{0,1\}^{d+1}$.

Figure 6: A Modified Interactive Proof of Quantumness

Step 3. Alice prepares the state

$$\phi \quad = \quad \frac{1}{\sqrt{2q^n(2\tau+1)^m}} \sum_{r \in \mathbb{Z}_q^n} \sum_{c \in \{0,1\}} \sum_{\substack{z \in \mathbb{Z}_q^m \\ \|z\|_\infty \leq \tau}} |s\rangle\,|c\rangle\,|Ar - cv + z\rangle\,. \tag{131}$$

Alice measures the third register of this state to obtain a state of the form $\psi \otimes |w\rangle$ where $w \in \mathbb{Z}_q^m$ and ψ is a pure state on $\mathbb{Z}_q^n \times \{0,1\}$. She converts ψ into a state ψ' of $(nQ+1)$-qubits by applying binary representation to $\mathbb{Z}_q^n$ (see Remark 1). For each $j \in S$, she measures the jth qubit of ψ' in the X-basis and records the result as $\ell_j \in \{0,1\}$. She sends w and $\{\ell_j\}_{j \in S}$ to Referee.

Step 5. For $j = 1, 2, \ldots, d$, Alice measures the $((n-d+j)Q)$th qubit of ψ' in the X-basis if $y_j = 0$, or in Y-basis if $y_j = 1$, and records result as a_j. Alice measures the $(nQ+1)$th qubit of ψ' in the $(X+Y)/\sqrt{2}$ basis and records the result as a_{d+1}. She sends $\mathbf{a}$ to Referee.

Figure 7: A Quantum Strategy for Alice in Game $\mathbf{R}$.

6.2 The Central Games

Game $\mathbf{R}$, shown in Figure 5, is a proof of quantumness based on an interaction between a prover (Alice) and a verifier (Referee). Game $\mathbf{R}$ is based on Game $\mathbf{J}_d$ (Figure 1), and Game $\mathbf{R}'$ (Figure 6) is a modification of Game $\mathbf{R}$ that is based on Game $\mathbf{J}'_d$ (Figure 2).

We prove that a quantum prover can play Game $\mathbf{R}$ with a score approaching that of the optimal score for Game $\mathbf{J}_d$.

Proposition 8. *Suppose that Alice behaves in Game* $\mathbf{R}$ *according to the strategy given in Figure 7. Then, her expected score is at least*

$$\frac{\sqrt{2}}{2} - o(1), \tag{132}$$

where $o(1)$ *denotes a vanishing function of* λ.

We will base our proof of Proposition 8 on the proof of Proposition 6. However, we must first address the possibility that the process followed by Alice in Step 3 fails to produce a proper claw-state.

Proof of Proposition 8. Let

$$z := \mathrm{Invert}(A, t, w) \quad \text{and} \quad z' := \mathrm{Invert}(A, t, w+v). \tag{133}$$

Either $\|Az - w\|_\infty \leq \tau$, or $\|Az' - w\|_\infty \leq \tau$, or both. The state ψ is then (respectively) one of the following:

$$|z\rangle\,|0\rangle\,, \tag{134}$$

$$|z'\rangle\,|1\rangle\,, \tag{135}$$

$$\frac{1}{\sqrt{2}}\left(|z\rangle\,|0\rangle + |z'\rangle\,|1\rangle\right). \tag{136}$$

Let E be the event that both $\|Az - w\|_\infty \leq \tau$ and $\|Az' - w\|_\infty \leq \tau$. Let F be the event that for all $j \in \{1, 2, \ldots, n\}$, $|z_j| > |\gamma_j|$.[3]

If both E and F occur, then

$$\psi \quad = \quad \frac{1}{\sqrt{2}} \left(|z\rangle |0\rangle + |z'\rangle |1\rangle \right). \tag{137}$$

and $z' = z + \gamma$, where $v = A\gamma + e$ and γ, e are the vectors generated in the Encrypt algorithm (Figure 4). Since $|z_j| > |\gamma_j| \ \forall j$, the relationship $z' = z + \gamma$ holds not only over $\mathbb{Z}_q^n$, but also when z', z, γ are considered as vectors over $\mathbb{Z}^n$. Therefore, the following parity relationship holds:[4]

$$[z]_Q \oplus [z']_Q \quad = \quad [\gamma]_Q \tag{138}$$

$$\quad = \quad 0^{n-d} || x_1 x_2 \ldots x_d. \tag{139}$$

The $(d+1)$-qubit state that remains for Alice at the end of Step 3 is therefore precisely

$$\frac{1}{\sqrt{2}} \left(|a_1 a_2 \ldots a_d\rangle + (-1)^{a_{n+1}} |(a_1 \oplus x_1)(a_2 \oplus x_2) \ldots (a_d \oplus x_d)\rangle \right). \tag{140}$$

It follows by the same calculations as in the proof of Proposition 6 that, conditioned on $E \cap F$, Alice achieves an expected score of $\sqrt{2}/2$ at Game **R**. Therefore, to prove Proposition 8, it will suffice to show that $\mathbf{P}(E \cap F) \geq 1 - o(1)$.

Consider the sets

$$\text{Image}(A) + [-\tau, \tau]^m \tag{141}$$

and

$$\text{Image}(A) - v + [-\tau, \tau]^m \tag{142}$$

For each vector $f \in \mathbb{Z}_q^n$, the set

$$Af + [-\tau, \tau]^m \tag{143}$$

overlaps with the set

$$A(f + \gamma) - v + [-\tau, \tau]^m \quad = \quad Af + e + [-\tau, \tau]^m \tag{144}$$

and otherwise does not overlap with set (142). The set $Af + [-\tau, \tau]^m$ is of size $(2\tau + 1)^m$, while the overlap region is of size

$$\prod_{j=1}^{m} (2\tau + 1 - 2|e_j|). \tag{145}$$

Therefore,

$$\mathbf{P}[E \mid e] \quad = \quad \frac{\prod_{j=1}^{m} (2\tau + 1 - 2|e_j|)}{(2\tau + 1)^m} \tag{146}$$

$$\quad = \quad \prod_{j=1}^{m} \left(1 - \frac{2|e_j|}{2\tau + 1} \right) \tag{147}$$

$$\quad \geq \quad 1 - \sum_{j}^{m} \frac{2|e_j|}{2\tau + 1} \tag{148}$$

$$\quad = \quad 1 - \frac{\|e\|_1}{2\tau + 1} \tag{149}$$

[3] The absolute value here is taken within the ring $\mathbb{Z}_q$. See Section 2 for conventions regarding absolute value notation.

[4] See Remark 1 for an explanation of the base-2 notation used here.

So, using Lemma A.2 from [1],

$$\begin{aligned}\mathbf{P}[E] &\geq 1 - \mathbf{E}\left[\frac{\|e\|_1}{2\tau+1} \mid e \leftarrow G(\sigma,\tau)\right] &(150)\\ &\geq 1 - \frac{m\sigma}{2\tau+1}, &(151)\end{aligned}$$

which, by the assumptions made about σ in Figure 6, implies $\mathbf{P}[E] \geq 1 - o(1)$.

We apply similar reasoning to derive a lower bound on $\mathbf{P}[F]$. The vector z is uniformly distributed over $\mathbb{Z}_q^n$, which is of size q^n, while the set

$$\left\{z \in \mathbb{Z}_q^n \mid \forall j \;\; |z_j| > |\gamma_j|\right\} \tag{152}$$

is of size

$$\prod_{j=1}^{m} (q - 2|\gamma_j| - 1) \tag{153}$$

Therefore,

$$\begin{aligned}\mathbf{P}[F \mid \gamma] &= q^{-m} \cdot \prod_{j=1}^{m} (q - 2|\gamma_j| - 1) &(154)\\ &= \prod_{j=1}^{m} \left(1 - \frac{2|\gamma_j|+1}{q}\right) &(155)\\ &\geq 1 - \sum_{j=1}^{m} \frac{2|\gamma_j|+1}{q} &(156)\\ &= 1 - \frac{\|\gamma\|_1 + m}{q}. &(157)\end{aligned}$$

From the Encrypt procedure, we have $\gamma = 2s + M$, where $\|M\|_1 \leq d$ and (using Lemma A.2 from [1]) $\mathbf{E}[\|s\|_1] \leq \sigma$. Therefore,

$$\begin{aligned}\mathbf{P}[F] &\geq 1 - \frac{\mathbf{E}\left[\|\gamma\|_1\right] + m}{q} &(158)\\ &\geq 1 - \frac{2\mathbf{E}\left[\|s\|_1\right] + d + m}{q} &(159)\\ &\geq 1 - \frac{2\sigma + d + m}{q} &(160)\end{aligned}$$

and the quantity (160) is easily to see to tend to 1 as a function of λ by the inequalities assumed in Figure 6. Therefore $\mathbf{P}(E \cap F) \geq 1 - \mathbf{P}(\neg E) - \mathbf{P}(\neg F) \geq 1 - o(1)$. This completes the proof. □

Lastly, we note that the strategy in Figure 7 is also a valid strategy for Game $\mathbf{R}'$, and so by the same proof we have the following.

Proposition 9. *Suppose that Alice behaves in Game $\mathbf{R}'$ according to the strategy given in Figure 7. Then, her expected score is at least*

$$\frac{\sqrt{2}}{2} - o(1), \tag{161}$$

where $o(1)$ denotes a vanishing function of λ.

6.3 Classical Soundness

In this section, we use the expression $\text{Score}(\mathbf{x}, \mathbf{y}, \mathbf{a}, \mathbf{b})$ to denote the score assigned to $(\mathbf{x}, \mathbf{y}, \mathbf{a}, \mathbf{b})$ in Game $\mathbf{J}_n$ (Figure 1).

Theorem 8. *Suppose that Alice behaves in Game* $\mathbf{R}$ *according to the model shown in Figure 6.3. Then, the bias of her strategy is upper bounded by* $\exp(-\Omega(d)) + \text{negl}(\lambda)$.

Proof. Our proof method follows [10]. Let s denote Alice's expected score in Game $\mathbf{R}$. Consider Experiment S_1 shown in Figure 6.3, in which the process of generating Alice's responses is shared with a second player, Bob. In Experiment S_1, Alice and Bob play $\mathbf{J}'_d$, but with a possible advantage: the referee has shared an encryption of Alice's input bits $x_1 x_2 \ldots x_d$ with both players in advance, and has also shared the trapdoor t for the encryption matrix with Alice. The probability distribution of $(\mathbf{x}, \mathbf{y}, \mathbf{a}, \mathbf{b})$ is exactly that generated by Alice's original strategy in Game $\mathbf{R}$, and so

$$s \quad = \quad \mathbf{E}_{S_1} \left[\text{Score}(\mathbf{x}, \mathbf{y}, \mathbf{a}, \mathbf{b}) \right]. \tag{162}$$

In Experiment S_2 (Figure 6.3), Alice skips computing her output string $\mathbf{a}$ directly, and instead predicts exactly what behavior Bob will exhibit on all of his possible inputs $\mathbf{y}$ (by running SecondResponse 2^d times). Alice then chooses her output $\mathbf{b}$ so as to optimize the expected score against all possible inputs to Bob. This new strategy can only increase the score achieved by Alice and Bob (since we have left Bob's behavior fixed and optimized Alice's behavior), and thus we have

$$s \quad \leq \quad \mathbf{E}_{S_2} \left[\text{Score}(\mathbf{x}, \mathbf{y}, \mathbf{a}, \mathbf{b}) \right]. \tag{163}$$

Importantly, since we have assumed $d \leq (\log \lambda)^{O(1)}$, the process of Alice executing SecondResponse 2^d only takes a polynomial amount of time.

Finally, in Experiment S_3, there is one additional change: the Referee no longer provides Alice and Bob with an encryption (A, v) of Alice's input bits $x_1 x_2 ... x_n$. Instead, Alice merely generates a uniformly random (A, v) and shares it with Bob. This change should not be noticeable to the polynomial-time processes in S_2, and therefore its effect on the expected score is negligible:

$$s \quad \leq \quad \mathbf{E}_{S_3} \left[\text{Score}(\mathbf{x}, \mathbf{y}, \mathbf{a}, \mathbf{b}) \right] + \text{negl}(\lambda). \tag{164}$$

Experiment S_3 is merely Alice and Bob playing Game $\mathbf{J}_d$ with a randomized classical strategy, and therefore by Theorem 5,

$$\begin{aligned} s \quad &\leq \quad \omega^c(\mathbf{J}_d) + \text{negl}(\lambda) && (165) \\ &\leq \quad \exp(-\Omega(n)) + \text{negl}(\lambda). && (166) \end{aligned}$$

An analogous argument shows that

$$s \quad \geq \quad -\exp(-\Omega(n)) - \text{negl}(\lambda), \tag{167}$$

which completes the proof. □

By repeating the same reasononing with Game $\mathbf{R}$ replaced by Game $\mathbf{R}'$ and Game $\mathbf{J}_d$ replaced by Game $\mathbf{J}'_d$, we obtain (using Theorem 6):

Theorem 9. *The bias of any classical polynomial-time strategy for Game* $\mathbf{R}'$ *is upper bounded by*

$$(3/4)^{-d/4} + \text{negl}(\lambda). \tag{168}$$

1. *Step 2:* Alice chooses the value of *coins* uniformly at random and computes

$$(w, \{\ell_j\}, mem) \leftarrow \text{FirstResponse}(A, v, coins), \tag{169}$$

where FirstResponse is a non-uniform polynomial-time deterministic algorithm. She sends $(A, \{\ell_j\})$ to Referee.

2. *Step 5:* Alice computes

$$\mathbf{b} \leftarrow \text{SecondResponse}(\mathbf{y}, mem), \tag{170}$$

where SecondResponse is a polynomial-time deterministic algorithm. She sends $\mathbf{b}$ to Referee.

Figure 8: A model for the behavior of a classical prover (Alice) in Game **R**. The register *coins* denotes initial randomness and the register *mem* denotes internal memory between responses. Both registers are of polynomial size.

1. Before the game begins, Alice samples *coins* uniformly at random, and shares its value with Bob.

2. Referee computes

$$(A, v, t) \leftarrow \text{Encrypt}(x_1 x_2 \dots x_d). \tag{171}$$

Referee sends (A, v, t) to Alice and sends (A, v) to Bob.

3. Referee sends $\mathbf{x}$ to Alice. Alice computes

$$(w, \{\ell_j\}, mem) \leftarrow \text{FirstResponse}(A, v, coins), \tag{172}$$

and then computes the vector $\mathbf{a} \in \{0,1\}^{d+1}$ via the procedure in Step 4 of Figure 5. She sends $\mathbf{a}$ to Referee.

4. Referee sends $\mathbf{y}$ to Bob. Bob also computes

$$(w, \{\ell_j\}, mem) \leftarrow \text{FirstResponse}(A, v, coins), \tag{173}$$

and computes

$$\mathbf{b} \leftarrow \text{SecondResponse}(\mathbf{y}, mem) \tag{174}$$

and sends $\mathbf{y}$ to Referee.

Figure 9: Experiment S_1, in which Alice and Bob play Game $\mathbf{J}_d$ with extra advice from the referee.

1. Before the game begins, Alice samples *coins* uniformly at random, and shares its value with Bob.

2. Referee computes

$$(A, v, t) \leftarrow \text{Encrypt}(x_1 x_2 \dots x_d). \tag{175}$$

   Referee sends (A, v) to both Alice and Bob.

3. Referee sends $\mathbf{x}$ to Alice. Alice computes

$$(w, \{\ell_j\}, mem) \leftarrow \text{FirstResponse}(A, v, coins), \tag{176}$$

   and then computes a vector $\mathbf{a} \in \{0,1\}^{d+1}$ which maximizes the expectation

$$\mathbf{E}\left[\text{Score}(\mathbf{x}, \mathbf{y}, \mathbf{a}, \text{SecondResponse}(\mathbf{y}, mem)) \mid \mathbf{y} \leftarrow \{0,1\}^d \times \{1\}\right]. \tag{177}$$

   She sends $\mathbf{a}$ to the Referee.

4. Referee sends $\mathbf{y}$ to Bob. Bob also computes

$$(w, \{\ell_j\}, mem) \leftarrow \text{FirstResponse}(A, v, coins), \tag{178}$$

   and computes

$$\mathbf{b} \leftarrow \text{SecondResponse}(\mathbf{y}, mem) \tag{179}$$

   and sends $\mathbf{y}$ to Referee.

Figure 10: Experiment S_2. Since we have assumed that d is upper bounded by a polynomial function of $\log \lambda$, all of the procedures in this experiment can be performed in polynomial time.

Experiment S_3 is the same as Experiment S_2, except that Step 2 is replaced with the following.

2. Alice samples $(A, v) \leftarrow \mathbb{Z}_q^{d+1}$ and shares (A, v) with Bob.

Figure 11: Experiment S_3. The game $\mathbf{J}_d$ is now played by Alice and Bob without any advice from Referee.

A Supporting Proofs

A.1 Proof of Corollary 2

We need only to show that for any $d \in \mathbb{N}$,

$$\omega^c(GHZ_4^d) \quad \leq \quad \omega^c(GHZ_3^d). \tag{180}$$

Fix $d \in \mathbb{N}$, and let (S, T, U, V) be a deterministic strategy for GHZ_4^d which achieves the optimal expected score. For any bit strings $\mathbf{t}, \mathbf{z} \in \{0,1\}^d$,

$$F_{\mathbf{t}}(\mathbf{z}) \quad = \quad U(\mathbf{t}) \oplus V(\mathbf{t} \oplus \mathbf{z}) \oplus (\neg \mathbf{z} \wedge \mathbf{t}). \tag{181}$$

Suppose that Alice, Bob, and Charlie play GHZ_3^d as follows:

1. Charlie samples $\mathbf{t} \leftarrow \{0,1\}^d$.
2. Upon receiving their input strings, Alice, Bob, and Charlie use the functions S, T, and $F_{\mathbf{t}}$ respectively to compute their outputs.

By direct computation, one can see that the expected score achieved by this strategy is the same as the expected score achieved by (S, T, U, V) at GHZ_4^d, which is $\omega^c(GHZ_4^d)$. Therefore, at least one of the deterministic strategies $(S, T, F_{\mathbf{t}})$ must achieve an expected score at GHZ_3^d of at least $\omega^c(GHZ_4^d)$. This completes the proof.

A.2 The Classical Value of GHZ_4

We follow [11]. Suppose that (F_1, F_2, F_3, F_4) is a deterministic strategy for GHZ_4, and let

$$v_j \quad = \quad \frac{(-1)^{F_j(0)} + i \cdot (-1)^{F_j(1)}}{\sqrt{2}} \in \mathbb{C}. \tag{182}$$

Then, the expected score achieved by this strategy is

$$\frac{1}{2} + \frac{\mathrm{Re}[v_1 v_2 v_3 v_4]}{4} \tag{183}$$

Since each v_i is a unit-length complex number, the quantity above obviously cannot exceed $3/4$. And, setting $F_1(x) = F_2(x) = 0$ and $F_1(x) = F_2(x) = x$ achieves a score of $3/4$.

A.3 Comment on the proof of Theorem 5

We have

$$\eta(V) \quad = \quad \frac{\mathbf{P}[\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}_3 + \mathbf{v}_4 \mid \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4 \leftarrow V]}{\mathbf{P}[\mathbf{v}_1 = \mathbf{v}_2 \mid \mathbf{v}_1, \mathbf{v}_2 \leftarrow V]} \tag{184}$$

The set V contains 2^n elements, one from each coset

$$(x_1, x_2, \ldots, x_n, 1) + 2\mathbb{Z}_4^n \tag{185}$$

with $x_1, x_2, \ldots, x_n \in \{0,1\}$. The set V' is obtained by dropping the last coordinate of each vector in V. This operation has no effect on the denominator in (184) (which is 2^{-n} for both V and V') and cannot decrease the numerator in (184), and so we find that

$$\eta(V) \quad \leq \quad \eta(V'). \tag{186}$$

References

[1] Yusuf Alnawakhtha, Atul Mantri, Carl A Miller, and Daochen Wang. Lattice-based quantum advantage from rotated measurements. *Quantum*, 8:1399, 2024.

[2] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[3] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *Journal of the ACM (JACM)*, 68(5):1–47, 2021.

[4] Mark Braverman, Subhash Khot, and Dor Minzer. Parallel repetition for the ghz game: Exponential decay, 2022.

[5] Harry Buhrman, Oded Regev, Giannicola Scarpa, and Ronald De Wolf. Near-optimal and explicit bell inequality violations. In *2011 IEEE 26th Annual Conference on Computational Complexity*, pages 157–166. IEEE, 2011.

[6] Adrian Cho. Ordinary computers can beat google's quantum computer after all. *Science*, 377(6606), 2022.

[7] David L. Donoho and Philip B. Stark. Uncertainty principles and signal recovery. *SIAM Journal on Applied Mathematics*, 49(3):906–931, 1989.

[8] Rodrigo Gallego, Lars Erik Würflinger, Rafael Chaves, Antonio Acín, and Miguel Navascués. Nonlocality in sequential correlation scenarios. *New Journal of Physics*, 16(3):033037, 2014.

[9] Gregory D Kahanamoku-Meyer, Soonwon Choi, Umesh V Vazirani, and Norman Y Yao. Classically verifiable quantum advantage from a computational bell test. *Nature Physics*, 18(8):918–924, 2022.

[10] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum advantage from any non-local game. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1617–1628, 2023.

[11] N. David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, 65:1838–1840, Oct 1990.

[12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 700–718. Springer, 2012.

[13] Ran Raz. A parallel repetition theorem. In *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*, pages 447–456, 1995.

[14] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

[15] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[16] Terence Tao. An uncertainty principle for cyclic groups of prime order. *Mathematical Research Letters*, 12:121–127, 2005.

[17] Avi Wigderson and Yuval Wigderson. The uncertainty principle: variations on a theme. *Bulletin of the American Mathematical Society*, 58(2):225–261, 2021.