# On Certified Randomness from Fourier Sampling or Random Circuit Sampling

Roozbeh Bassirian[1], Adam Bouland[2], Bill Fefferman[1], Sam Gunn[3], and Avishay Tal[3]

[1]University of Chicago
[2]Stanford University
[3]UC Berkeley

Certified randomness has a long history in quantum information, with many potential applications. Recently, Aaronson (2018, 2020) proposed a novel public certified randomness protocol based on existing random circuit sampling (RCS) experiments. The security of his protocol, however, relies on non-standard complexity-theoretic conjectures which were not previously studied in the literature.

Inspired by Aaronson's work, we study certified randomness in the quantum random oracle model (QROM). We show that quantum Fourier Sampling can be used to define a publicly verifiable certified randomness protocol with black-box security without any computational assumptions. In addition to giving a certified randomness protocol in the QROM, our work can also be seen as supporting Aaronson's conjectures for RCS-based randomness generation, as our protocol is in some sense the "black-box version" of Aaronson's protocol. In further support of Aaronson's proposal, we prove a Fourier Sampling version of Aaronson's conjecture by extending Raz and Tal's separation of BQP vs PH.

Our work complements the subsequent certified randomness protocol of Yamakawa and Zhandry (2022) in the QROM. Whereas the security of that protocol relied on the Aaronson-Ambainis conjecture, ours does not rely on any computational assumption — at the expense of requiring exponential-time classical verification. Our protocol also has a simple heuristic implementation.

Roozbeh Bassirian: roozbeh@uchicago.edu
Adam Bouland: abouland@stanford.edu
Bill Fefferman: wjf@uchicago.edu
Sam Gunn: gunn@berkeley.edu
Avishay Tal: atal@berkeley.edu

# 1 Introduction

The task of producing certified randomness – i.e. numbers that can be proved random to a skeptic, without any trust in the device – is a uniquely quantum ability, with a long history in quantum information. Certified randomness has many possible applications, for example in the certification of public lotteries, the selection of cryptographic keys, or proof of work cryptocurrencies (see e.g. [AM16] for a discussion). It was first realized that Bell inequality violations could enable certified randomness using multiple non-communicating devices [PAM+10]. Subsequently, single-device certified randomness schemes have been designed that use interactive protocols and assume post-quantum cryptography [BCMVV21, BKVV20, KCVY21, HG21, LG22]. Recently, in unpublished work, Aaronson [Aar18a, Aar20] has suggested that it might even be possible to generate public certified randomness with a single device using near-term random circuit sampling (RCS) experiments. Aaronson's proposal therefore offers the possibility that recent quantum advantage experiments [AAB+19, ZCC+22] might have useful applications.

The security of Aaronson's protocol, however, relies on a custom complexity-theoretic conjecture called the "long list quantum supremacy verification assumption," or LLQSV. This conjecture is both strong and nonstandard – it essentially conjectures that the output distribution of RCS is not only BQP-indistinguishable from random, but is indistinguishable for quantum variants of AM, even with access to exponentially many samples. It is therefore important to critically examine its validity, and more generally offer evidence that statistical tests for RCS certify the generation of entropy. More broadly, Aaronson's work opens the question of what other certified randomness protocols might be possible in the single-device, non-interactive setting – and whether or not it is possible to achieve certified randomness under weaker or different assumptions.

## 1.1 Our results in context

Our first result studies certified randomness in the context of Fourier Sampling in the quantum random oracle model (QROM). Here the task is, given black-box access to a random function $f$, output a sample from $f$'s Fourier spectrum. One can easily achieve this by querying $f$ on a uniform superposition and measuring in the Hadamard basis. We show that Fourier Sampling can be used to generate certified randomness. We prove that in this black-box setting, any quantum device passing a certain statistical test based on Fourier Sampling[1] must generate a high amount of min-entropy. We then use this test to construct a cryptographic protocol to generate certified randomness, non-interactively using a single device.

Our second result provides black-box evidence for Aaronson's LLQSV conjecture. Informally, LLQSV asks to distinguish whether an (exponentially long) list of random quantum circuits and outcomes $(C_i, s_i)$ are uncorrelated, or $s_i$ is sampled from the output distribution of $C_i$. *Black-Box* LLQSV replaces random circuits with random Boolean functions, and the output distribution is defined by the Fourier coefficients of $f_i$. We can prove that black-box LLQSV is not solvable in BQP or PH. Even though this is an oracle result, it can be seen as an attempt to come closer to attaining certified randomness in the white box setting, since the LLQSV conjecture was designed for this purpose [Aar20].

We believe these results are interesting for the following reasons. First, they provide complexity-theoretic support for Aaronson's certified randomness protocol. As we will discuss, the intellectual history of RCS is intimately tied with analogous developments in Fourier sampling (e.g. [Aar10]). Our Fourier sampling protocol is in some sense the "black-box" version of Aaronson's protocol – and therefore, our protocol's security is evidence in favor of the security of Aaronson's construction. To further elucidate this point, we prove a variant of Aaronson's LLQSV conjecture in the Fourier sampling domain, which requires a nontrivial extension of the recent BQP vs PH oracle separation of Raz and Tal [RT19] to the LLQSV setting. This provides evidence to back Aaronson's conjectures.

[1] The test checks that the outputs are heavy Fourier coefficients, similar to FourierFishing [Aar10] or Heavy Output Generation (HOG) [AC17].

| Protocol | [YZ24] | [Aar18b] | This Work, [AH23] |
|---|---|---|---|
| Verification | Efficient | Inefficient | Inefficient |
| Security | QROM + AA conjecture | Custom conjecture | QROM |
| Implementation | Not NISQ | RCS | RCS (heuristic) |

Table 1: Comparison of Theorem 1 to the certified randomness results of [YZ24, Aar18b]. See Section 1.2 for a discussion of the connections between our construction and RCS.

Second, our work provides a certified randomness protocol in its own right. Fourier Sampling is a well-studied computational primitive in the black-box model [Aar10] and a plausible candidate for a quantum supremacy experiment in a white-box model [FU16]. Our work shows this experiment is capable of generating certified randomness in the black-box setting, and it is plausible that it might be instantiable in the white-box setting via sufficiently strong cryptographic hash functions.

Third, our work complements a subsequent certified randomness protocol of Yamakawa and Zhandry [YZ24]. Assuming the Aaronson-Ambainis conjecture [AA14a], Yamakawa and Zhandry designed a certified randomness protocol in the QROM model which is both non-interactive and *efficiently verifiable* – i.e. the tests performed on the output can be done in polynomial time. Their work was the first to demonstrate that efficient verification of certified randomness is in principle possible using a non-interactive protocol. Our work, however, offers two advantages over Yamakawa and Zhandry's protocol. First, our protocol is closer to experimental feasibility, as their protocol not only requires instantiating the QROM, but also performing the list decoding of folded Reed-Solomon codes in superposition. Second, while the security of Yamakawa and Zhandry's protocol relies on the Aaronson-Ambainis conjecture, our result does not rely on computational assumptions. We summarize this comparison in Table 1.

Since we posted a first draft of our manuscript online, Aaronson and Hung [AH23] have made valuable contributions to the analysis of quantum advantage based certified randomness protocols. As noted in their work, our results have much in common. The main focus of [AH23] is to formalize the white-box certified randomness protocol introduced in [Aar20, Aar18b], assuming the hardness of LLQSV for QCAM/poly, the basic outline of which preceded and inspired our work. Their work also improves some of the results in this paper, in the sense that they give black-box evidence for hardness of LLQSV and the security of the certified randomness protocol in the random oracle model, a line of inquiry which was instigated by our work. We believe that both works together build a foundation to establish the first practical use-case of near-term quantum devices[2]. There are several differences between our works as well:

- Our result gives a AM (implied by our PH bound) and BQP lower bound for LLQSV in the black box model, which Aaronson and Hung improve to QCAM/poly. We note that our PH lower bound is incomparable to their result. Our work also finds connections to the Forrelation problem and uses different techniques that may be of independent interest.
- Our techniques for studying Fourier Sampling in QROM allow us to argue about linear min-entropy directly without an entropy accumulation theorem. We utilize a "derandomization" argument to establish a general trade-off between a strong lower bound with constant min-entropy generation, and a weaker lower bound with linear min-entropy generation.
- On the other hand, the proof techniques in [AH23], work against more general *entangled* quantum adversaries, where it is less clear how to extend our techniques in this way. We leave this extension as an interesting future direction.

[2]Instantiating oracles using pseudorandom functions can have several challenges on NISQ devices that we leave open for future works.

## 1.2 Connecting Fourier Sampling to Aaronson's protocol

The intellectual history of RCS as a quantum advantage experiment has deep roots in Fourier Sampling. In 2010 Aaronson used a relation version of the Fourier Sampling problem called Fourier Fishing to provide the first oracle separation between the relation variants of BQP and PH [Aar10]. The idea was to take advantage of the fact that the Fourier spectra of random Boolean functions obeys a "Porter-Thomas", or exponential, distribution in which some outcomes are sampled with considerably heavier probabilities than others. Aaronson showed in the black box model that no PH algorithm can sample from mostly heavy Fourier outcomes, whereas a quantum computer naturally does so by performing Fourier Sampling.

Subsequently, it was conjectured that no classical algorithm can output mostly heavy elements of the output distribution of random circuits [BIS+18, AC17, AG20]. These works essentially conjecture that the output distribution of random quantum circuits is as "unstructured" as the Fourier spectrum of a random Boolean function. In other words, the classical description of the circuit does not leak information about which outputs are heavy vs light in any efficiently accessible manner. In contrast, there are certain scenarios in which such a conjecture fails. For example, outputting heavy elements of Boson Sampling experiments is computationally easy due to information leakage from the circuit description [AA14b]. More recently, it has been shown that sufficiently shallow RCS circuits have additional structure that allows for classical algorithms to output heavy items with nontrivial bias [GKC+24]. Therefore in this sense, the classical hardness of quantum advantage experiments rests on this "unstructuredness" conjecture of deep RCS circuits.

Viewed in this light, our results can be seen as the analog of Aaronson's Fourier Fishing lower bound [Aar10] in the certified randomness setting. We are the first to demonstrate that certified randomness is possible in the black-box Fourier Sampling context, as we show that no quantum algorithm can output heavy Fourier elements with low entropy. Aaronson's prior work is conjecturing that precisely this same property holds in the white-box RCS setting. The security of his protocol can therefore be rested on the belief that RCS has highly "unstructured" output distributions – even hidden to (pseudo-deterministic) quantum algorithms. In this sense, RCS can be viewed as a heuristic implementation of our protocol.

## 1.3 Our Results

Our first result concerns the problem of outputting sufficiently heavy Fourier coefficients, which we call Fourier HOG (FHOG). Let $F = f_1, \ldots, f_m : \{0,1\}^n \to \{\pm 1\}$ be a list of random Boolean functions, and $Z = z_1, \ldots, z_m \in \{0,1\}^n$. Let $N = 2^n$. We call a Fourier coefficient heavy if $\frac{1}{N} < \widehat{f_i}(z_i)^2 \leq \frac{4}{N}$, and light if $\widehat{f_i}(z_i)^2 \leq \frac{1}{N}$. Intuitively, FHOG captures the statistical properties of the simple quantum algorithm that samples according to the Fourier spectrum. A simple calculation shows that on a random $f$ this simple quantum algorithm outputs a heavy element $\approx 54\%$ of the time, and outputs a light element $\approx 20\%$ of the time. Therefore, FHOG requires that the number of heavy elements among $z_1, \ldots, z_m$ is $\approx 0.54m$ and the number of light elements is $\approx 0.2m$. Our main result proves that *any* efficient quantum query algorithm that solves FHOG on a non-negligible fraction of inputs must generate linear min-entropy, and hence the simple Fourier sampling algorithm is essentially optimal in this sense. Starting from a *random* function to generate randomness might seem circular; however, this bound is on min-entropy *conditioned* on the choice of random function.

**Theorem 1.** *(informal) There is no sub-exponential-query quantum algorithm which, given black-box access to $F$, both (i) passes FHOG with non-negligible probability, and (ii) conditioned on passing FHOG, generates only $o(n)$ bits of min-entropy, for a non-negligible fraction of random functions $F$.*

This result can directly be used to construct a *single round* publicly verifiable proof of min-entropy protocol:

**Definition 2.** *Let $n, m \in \mathbb{N}$ and $m \geq n$. Let $F = f_1, \ldots, f_m$ be a random oracle representing $m$ random boolean functions $f_i : \{0,1\}^n \to \{\pm 1\}$. Suppose $A^F$ is a polynomial time quantum algorithm*

*that generates polynomial size classical strings $\pi$. Let $V^F$ be a randomized exponential time classical verifier that accepts or rejects $\pi$. $A$ and $V$ form a single round publicly verifiable proof of min-entropy protocol if and only if:*

- *Completeness: $V$ accepts string $\pi$ sampled according to the output distribution of $A$ with high probability:*
$$\Pr_{F,\pi\sim A^F}\left[V^F(\pi) \text{ accepts}\right] \geq 1 - \text{negl}(n).$$
- *Soundness: With high probability over the choice of random oracle $F$, if $V$ accepts $\pi$ with non-negligible probability, then the output distribution of $A^F$ must have min-entropy at least $h$:*
$$\Pr_F\left[\Pr_{\pi\sim A^F}[V^F(\pi) \text{ accepts}] \geq \delta(1/n) \wedge \Pr_{Z\sim\chi}[q_Z \geq 2^{-h}] \geq \text{negl}(n)\right] \leq \text{negl}(n).$$
*where $\chi$ is the output distribution of $A^F$ conditioned on $V$ accepting, and $q_Z$ is the probability of sampling $Z$ according to $\chi$*

Which immediately implies a single round publicly verifiable certified randomness protocol [YZ24].

**Remark 3.** *Certified randomness usually refers to* private *randomness expansion, where the goal is to expand a truly small random seed to a larger string that is statistically close to uniformly random by interacting with a quantum device. This definition is widely used in protocols based on Bell experiments [PAM+10], where the only assumption they make is that they have access to multiple devices that cannot communicate. Informally, they can show that a strategy that wins the CHSH game with high enough probability must also have high min-entropy, which can be used to extract uniformly random bits using randomness extractors. Furthermore, they can even show that these protocols are secure against quantum adversaries. In other words, even when the devices are manufactured adversarially, the conditional min-entropy (conditioned on the adversary's sub-system) must still be large. Motivated by Aaronson's proposal [Aar20], in this work we are concerned with* publicly *verifiable certified randomness relative to quantum random oracles, since the (adversarial) prover knows the string generated in the protocol. This makes our problem slightly easier to argue about since we do not need to worry about the adversary's side information. However, similar to [YZ24], we showed that the high min-entropy bound holds even conditioned on the random oracle.*

Crucially, our bounds hold not only for worst-case functions $F$ but also for *average-case* $F$, whose Fourier spectra share many common features with RCS (e.g. a Porter-Thomas-like distribution). We prove this theorem using a carefully constructed hybrid argument. The worst-case, constant-min-entropy proof is relatively straightforward: Suppose one has an efficient quantum algorithm that pseudo-deterministically outputs a heavy item for all functions $f$. On one hand, we know that by changing a relatively small number of entries of $f$ (say $O(2^{n/2})$), we can change a heavy Fourier coefficient to a light Fourier coefficient. On the other hand, any low-query quantum algorithm cannot notice the difference of switching these many entries. Simply because they represent an exponentially small fraction of the entries of $f$, and therefore this case follows from a standard hybrid argument. However, turning this idea into one that certifies *linear* min-entropy for *average-case* functions is much more involved. This is essentially because the above perturbation of the function $f$ does not preserve the average case, nor does it apply to quantum algorithms with higher min-entropy. We tune the hybrid argument to extend our bound to the average case (for constant min-entropy) by applying a combinatorial accounting of how these perturbations of the functions affect the average case. We then apply a novel "derandomization" argument which reduces the linear min-entropy case to the constant min-entropy case.

We then show how to leverage this result to produce a cryptographic certified randomness protocol, which is analogous to Aaronson's protocol. The basic idea is to ask the quantum algorithm to sample from the Fourier spectra of several different random functions and check that the number of sufficiently

"heavy" and "light" outcomes is roughly what is expected. This could be instantiated in a white-box setting as a cryptographic protocol for certified randomness, where the client sends several function descriptions (say of cryptographic hash functions), the honest server *efficiently* responds with Fourier spectrum samples, and the client checks (post-mortem) that most of the samples were heavy using an exponential time computation. We emphasize that this is only plausible because we can bound the *conditional* min-entropy (relative to the choice of random function).

Our second result concerns a certified randomness proposal due to Aaronson [Aar20]. Aaronson gave a reduction from the problem of certifying min-entropy to a certain decision problem called the Long List Quantum Supremacy Verification (LLQSV) problem. The LLQSV problem essentially evaluates the difficulty of distinguishing exponentially many RCS samples from uniformly random numbers. Aaronson showed that if this problem lies outside of QCAM – that is the class of problems solvable by AM protocols with classical messages and quantum verifiers – then no efficient quantum algorithm can pass the HOG test with low min-entropy. Analogously to [AC17], Aaronson explored potential algorithms for this problem and found they did not solve it, and subsequently conjectured such a QCAM algorithm does not exist. This is a custom assumption, and therefore deserves scrutiny – it is simultaneously conjecturing this problem lies outside of BQP, outside of AM, and beyond. In our second result, we give evidence towards its validity in the black-box setting. Namely, we show that the black-box LLQSV problem lies outside of BQP and even outside of PH (and hence outside of AM).

**Theorem 4.** *(informal) No* BQP *or* PH *algorithm can solve black-box* LLQSV*. Furthermore, our lower-bound extends even to the case in which the quantum algorithm is allowed to make* $O(2^{n/10})$ *queries, and the relation in the* PH *algorithm can be computed in time* $O(2^{n/c})$ *for some constant* $c$ *that depends on the level of the polynomial hierarchy.*

We give two independent proofs of the PH lower bound and one of the BQP lower bound. The first PH bound and the BQP bound are based on extending lower bounds for the MAJORITY function. The second PH bound is based on introducing a black-box variant of LLQSV that we call SquaredForrelation, which is also closely related to the Forrelation problem. In the problem we introduce, black-box access is given to two functions $f, g : \{0,1\}^n \to \{\pm 1\}$, and the task at hand is to distinguish whether $f, g$ are chosen uniformly at random or $g$ is correlated with the heavy Fourier coefficients of $f$. It is simple to show that the SquaredForrelation problem is strictly easier than LLQSV, because it reduces to LLQSV and it also admits a BQP algorithm. Intuitively, in SquaredForrelation, having access to $g$ allows one to sample heavy elements of the Fourier spectrum and therefore recreate a long list of samples for LLQSV. Nevertheless, we prove that even the SquaredForrelation problem is not in PH. This simultaneously proves a lower bound on black-box LLQSV and gives another oracle separation of BQP vs PH [RT19].

## 1.4 Open Problems

We have shown that Fourier Sampling gives rise to certified randomness in the QROM, albeit without efficient verification. In contrast, Yamakawa-Zhandry protocol [YZ24] gives certified randomness in the QROM with efficient verification, but relies on the Aaronson-Ambainis conjecture. It is natural to ask if one can combine the strengths of both results and obtain a certified randomness protocol with efficient verification and unconditional security.

Another natural direction is to construct certified randomness protocols without the QROM heuristic in the white-box model. Aaronson's protocol [Aar20] is such an attempt that relies on the LLQSV conjecture, or alternatively, a belief that the output distribution of sufficiently deep random circuits is unstructured. It is an important open question whether or not one can base the security of these protocols on more natural hardness assumptions.

## 1.5 Proof Outline

### 1.5.1 Min-Entropy Generation

Our proof of Theorem 1 proceeds in three steps, where each step is a progressively stronger theorem.

**Worst-case, constant min-entropy bound.** In the first step, we show that any quantum algorithm that outputs a heavy Fourier coefficient for *any* function $f$ after $2^{o(n)}$ queries must generate a *constant* amount of min-entropy. A simple hybrid argument suffices for this case as sketched in section 1.3.

**Average-case, constant min-entropy bound.** Unfortunately, the above argument does not immediately say anything about quantum algorithms which only output a heavy Fourier coefficient for *most* functions $F$. This is essentially because the hybrid argument only shows how to *adversarially* construct "Bad" functions for which the quantum algorithm does not solve FHOG with non-negligible probability. It does not show that these Bad functions constitute a large fraction of the space.

In the second step of our proof, we prove exactly this – any low-query algorithm cannot pseudo-deterministically solve FHOG on a large fraction of inputs. In fact, we can show that the algorithm succeeds only on exponentially small choices of $F$. We prove this using a double-counting argument. Namely, given a quantum algorithm $A$ that solves FHOG with low min-entropy, label the functions on which the algorithm succeeds "Good", and those on which it *noticeably* fails "Bad." More formally, for a Bad $F$, approximately 28% of outcomes are "heavy" and 46% of outcomes are "light". For each Good choice of $F$ on which the algorithm passes FHOG, the hybrid argument constructs a nearby Bad function $F'$. Consider the bipartite graph where one side contains Good functions $F$, the other side contains Bad functions $F'$, and we draw an edge $(F, F')$ if $F'$ can be obtained from $F$ by our earlier construction. The hybrid argument gives us a lower bound on the degree of any Good vertex in this graph. However, to show the Bad choices are a large fraction of the space, we instead want to upper bound the degree of any Bad vertex. We obtain such a bound by counting the number of adjacent functions $F$ for which the most likely output of our algorithm on $F'$ is a heavy Fourier coefficient. In other words, we prove that the set of Bad functions is actually very large by showing that each Bad function $F'$ could only have come from a limited number of Good functions $F$. Therefore the Bad functions must constitute a large fraction of the space – which concludes our average-case bound.

**Average-case, linear min-entropy bound.** For the previous step, we crucially relied on the fact that we were only considering quantum algorithms with sub-constant min-entropy so that there was a unique majority output $Z$. This allowed us to consider shifting entries of $F$ to change $Z$ from a heavy to a light element and vice versa. Once we are in the case of algorithms with higher min-entropy $H$, this type of argument becomes much more difficult since there could now be many different elements $Z_1, Z_2, \ldots Z_{2^H}$ which are frequently output by the algorithm. The simplest approach to proving a hybrid bound is to try to shift around the heaviness of the Fourier coefficients of various subsets of these elements without affecting the others. But this becomes challenging, as the number of entries of $F$ one can change to alter certain Fourier coefficients but not others decays exponentially in the number of coefficients being considered. So our attempt to make a direct extension of our prior method fails in the average case.

Instead, we extend our theorem to the generation of a linear amount of min-entropy with a derandomization-like argument that uses the previous theorem as a black-box. While it's commonly said that one cannot "pull the randomness" out of quantum algorithms, in certain query settings it can be done. In particular, whenever one has a quantum algorithm $A$ which has an output distribution of min-entropy $H$, there is a simple way to pull the quantum randomness out of the algorithm: Run the quantum algorithm many ($\approx 4^H$) times, store the empirical distribution, and then classically rejection sample on the "heavy" portion of the empirical distribution. The empirical distribution will be close to the true distribution on heavy elements, so this new sampler $A'$ will faithfully reproduce the distribution of heavy outputs for a sufficiently large fraction of input choices. Critically, the randomness in $A'$ is now almost entirely classical, stemming from rejection sampling. This randomness can be "hard-wired" externally (modulo some technical issues regarding the imprecision caused by the additive error in the estimated distribution from the samples). For any fixed external randomness, the algorithm becomes pseudo-deterministic, at the cost of more queries.

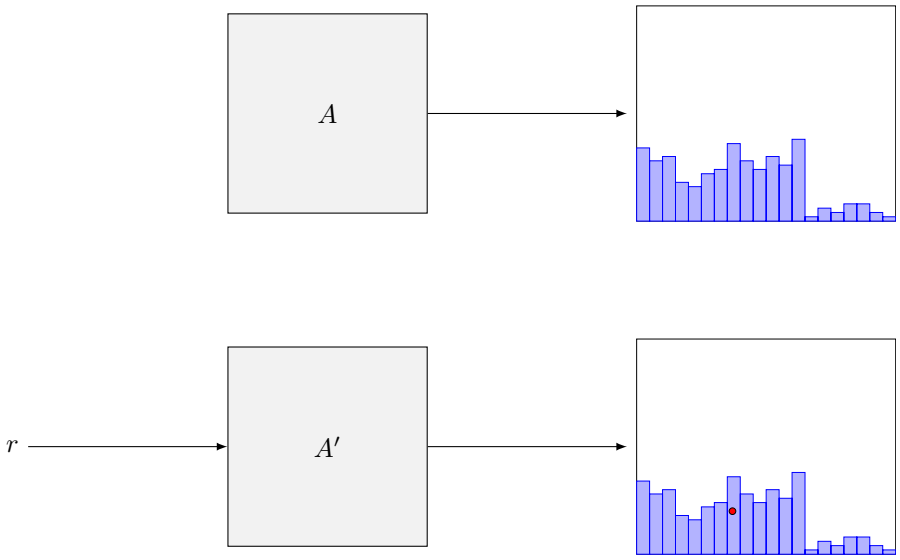


Figure 1: The algorithm $A'$ takes enough samples from $A$ to estimate the output distribution, then uses $r$ as a seed to rejection sample from that distribution. For random $r$, the output distributions of $A$ and $A'$ are identical. But for fixed $r$, the output of $A'$ is nearly-deterministic.

At first glance, the argument might appear overly expensive because it significantly increases the number of queries. Specifically, if $A$ makes $Q$ queries, then $A'$ makes $\approx Q \cdot 4^H$ queries, which in our case is exponential. Surprisingly, we show that it is still enough to reduce the constant min-entropy case to the linear min-entropy case. The crucial observation is that, for the constant min-entropy case, our query lower bound holds against *exponentially many* queries. Therefore, so long as $Q \cdot 4^H$ is less than this exponential, $A'$ does not make too many queries to $F$. We then show that one can hard-code the randomness for rejection sampling into our new algorithm, making it pseudo-deterministic and therefore "derandomizing" linear min-entropy algorithms. In summary, we have traded our constant-min entropy, large-exponential query bound for a linear min-entropy, smaller-exponential query bound.

### 1.5.2 The SquaredForrelation Problem and Black-Box LLQSV

In this section, we discuss PH and BQP lower bounds for the Black-Box LLQSV problem. First, we formally define the problem:

**Problem 5** (Black-Box LLQSV)**.** *Given oracle access to $\mathcal{O}$, distinguish the following two cases:*

- *$\mathcal{U}$: For each $i$, $f_i$ and $s_i$ are chosen uniformly at random.*
- *$\mathcal{D}$ : For each $i$, $f_i$ is a random Boolean function, and $s_i$ is sampled according to $\widehat{f_i}^2$.*

We observe there is a close connection between Black-Box LLQSV and the MAJORITY problem. To understand this, note that in either case the probability of sampling a pair $(f, s)$ only depends on the magnitude of the Fourier coefficient of $f$ at $s$, or equivalently $|h(f \cdot \chi_s) - N/2|$, where $h$ is the hamming weight, $\chi_s$ is the $s$-Fourier character (i.e., $\chi_s(x) = (-1)^{x \cdot s}$), and $f \cdot \chi_s$ is the entry-wise product of truth tables of $f$ and $\chi_s$. This allows us to write both distributions as a linear combination of simpler distributions $\mathcal{U}_d^N$ – the uniform distribution over all strings of hamming weight $N/2 + d$ or $N/2 - d$.

An averaging argument then implies that any algorithm for Black-Box LLQSV should also distinguish a pair of distributions: $\mathcal{U}_d^N$ and $\mathcal{U}_{d'}^N$. To prove the hardness of this task, we can focus on the distinguishability of $\mathcal{U}_0^N$ and $\mathcal{U}_d^N$, and since we are working with random Boolean functions, we can bound $d$ by $\text{poly}(n)/\sqrt{N}$. Lastly, we use known lower bounds for MAJORITY to prove that these two

distributions are indistinguishable for both BQP and PH algorithms. We discuss this in more detail in Section 3.

Perhaps more interestingly, we can show a reduction from SquaredForrelation, to Black-Box LLQSV. This enables us to get an alternative lower bound for Black-Box LLQSV, by proving a PH lower bound for SquaredForrelation. Crucially, it is not hard to see that SquaredForrelation is in BQP, which makes it a strictly easier problem than Black-Box LLQSV, and hence our lower bound is stronger. SquaredForrelation also gives an alternative oracle separation of BQP and PH, that has distinct advantages from previous similar results.

One advantage of SquaredForrelation is that it can be solved by a quantum algorithm that only makes *classical* queries to $g$. This property plays a critical role in the reduction between SquaredForrelation and Black-Box LLQSV. Furthermore, this property provides another benefit. It enables us to consider a more realistic instantiation of these oracles, especially when compared to [RT19], as we discuss next.

Recall that in [RT19], an oracle separation $\mathsf{BQP}^O \not\subseteq \mathsf{PH}^O$ was demonstrated using the Forrelation problem. Given oracle access to two functions $f$ and $g$, the problem asks to distinguish between two scenarios: $(i)$ $f$ and $g$ are completely random and independent or $(ii)$ the Fourier transform of $f$ correlates with $g$. The Forrelation problem can be solved via a simple efficient quantum algorithm that queries both $f$ and $g$ in superposition, but cannot be solved by a PH machine. One drawback of this problem is that there's seemingly no efficient implementation of the oracles under which the problem remains non-trivial. In particular, if $f$ is a random small circuit, then it seems any small circuit $g$ doesn't correlate with $f$'s Fourier transform. If one settles for having small circuits only for $f$ but not $g$ (or vice versa), then the problem remains non-trivial, but even in this scenario, the problem seems far from practical as a quantum algorithm would need to query an exponentially large oracle $g$ in superposition. SquaredForrelation is defined as follows:

**Problem 6** (simplified SquaredForrelation)**.** *Given oracle access to Boolean functions $f, g : \{0,1\}^n \to \{\pm 1\}$, distinguish the following two cases:*

1. *$f$ and $g$ are both chosen uniformly at random.*
2. *$f$ is chosen uniformly at random and $g$ is the indicator of the heavy Fourier coefficients of $f$.*

A Fourier coefficient is heavy if the coefficient squared is larger than its expected value $\frac{1}{N}$. The main difference between SquaredForrelation and Forrelation is that $g$ is correlated with *squared* Fourier coefficients rather than the sign of Fourier coefficients. Clearly, a simple quantum algorithm that queries $f$ in superposition, measures in the Hadamard basis, and then queries $g$ classically solves the problem. Notice that this algorithm is a combination of a quantum and classical algorithm. This means that in principle, if $f$ has a small circuit, then the quantum part of the algorithm can implemented efficiently, followed by a much longer classical "post-mortem" part that queries $g$. It is important to note that in both the Forrelation and SquaredForrelation problems, $g$ generally is not efficiently computable, even when $f$ can be succinctly represented.

In particular, following [AC17, Section 7.4], this suggests choosing the oracle $f$, the only function that is queried in superposition, from a pseudorandom family of functions. While this manuscript does not delve into these aspects, it is worth noting a distinction: our problem is a decision problem, contrasting with the problems presented in [AC17, Section 7.4] – known as Fourier Fishing and Fourier Sampling – which are sampling problems.

**Lower Bound for Black-Box LLQSV via SquaredForrelation** We summarize the second PH lower bound for Black-Box LLQSV in two steps. First, we prove a PH lower bound for SquaredForrelation, and then we show a reduction from SquaredForrelation to Black-Box LLQSV.

The first step of the proof proceeds by carefully incorporating the *squared* Fourier coefficients in the analysis of Raz and Tal [RT19]. Recall that the analysis of [RT19] proceeds by looking at a multivariate Gaussian as a stopped Brownian motion. This allows them to write the expected value of a multilinear function over the multivariate Gaussian as a telescopic sum, and bound each term in

the sum independently. Finally, they show that it is possible to convert this continuous distribution to a discrete distribution $\mathcal{D}$ while preserving the expected value by truncating each coordinate to the interval $[-1, 1]$ followed by randomized rounding.

A feature of Gaussians, which was heavily exploited in the analysis of [RT19], is that the sum of $t$ independent Gaussians is again a Gaussian. When dealing with squares of Gaussians, this is no longer true. Nevertheless, if $Z \sim \mathcal{N}(0, \sigma^2)$ then one can still write $Z^2 - \mathbf{E}[Z^2]$ as the result of a martingale composed of many small steps. To present $Z^2 - \mathbf{E}[Z^2]$ as a martingale, first observe that if $X$ (the "past") and $\Delta$ (the "next step") are two independent zero-mean Gaussians, then

$$(X + \Delta)^2 - \mathbf{E}[(X + \Delta)^2] = (X^2 - \mathbf{E}[X^2]) + \Delta^2 + 2\Delta \cdot X - \mathbf{E}[\Delta^2]$$

and thus $\mathbf{E}[\Delta^2 + 2\Delta \cdot X - \mathbf{E}[\Delta^2] \mid X] = 0$. Since a Gaussian $Z \sim \mathcal{N}(0, \sigma^2)$ can be written as a sum of $t$ independent Gaussians $Z_1, \ldots, Z_t \sim \mathcal{N}(0, \sigma^2/t)$, we see that $Z^2 - \mathbf{E}[Z^2]$ may be written as sum of $t$ small steps, each of the form $Z_i^2 + 2Z_i \cdot Z^{<i} - \mathbf{E}[Z_i^2]$, with expected value 0 even conditioned on the past $Z^{<i} = Z_1 + \ldots + Z_{i-1}$. The rest follows from the analysis of [RT19], which crucially relies on representing the final distribution as a sum of many small steps, each with an expected value of 0 As a consequence, we obtain a new oracle $O$ so that $\mathsf{BQP}^O \not\subseteq \mathsf{PH}^O$.

In our next step, the reduction from SquaredForrelation to black-box LLQSV, we make use of the fact that $g$ is not queried in superposition by the quantum algorithm. This observation follows by rejection sampling according to $g$; intuitively, this allows one to sample heavy elements of the Fourier spectrum and therefore recreate a long list of samples. So far, we have worked with one instance of the SquaredForrelation problem. However, we prove that our lower bound easily extends to the case that we have oracle access to an (exponentially) long list of samples in SquaredForrelation. Consequently, this shows that the Black-Box LLQSV problem is not in PH.

In our previous discussion, we made two oversimplifications which obscure the technical challenges in our argument. First, unlike in our simplified SquaredForrelation problem, the actual SquaredForrelation problem concerns a distribution over functions $f$ and $g$ that are obtained by taking multivariate Gaussians and randomized rounding them to have support over the Boolean cube. Second, rejection sampling according to $g$ samples a uniformly random heavy squared Fourier coefficient of $f$, which differs from Fourier transform distribution itself; we address these differences in detail in Section 4.4. Intuitively, to fix this issue, recall that the goal of these long list hardness results is to generate certifiable random numbers. We show that this task is achievable even when the quantum algorithm can sample heavy outcomes from the distribution generated by rejection sampling (i.e., we can think of this as a new benchmark test much like HOG, but with respect to a new distribution). Accordingly, we show that the same quantum algorithm that samples according to the Fourier transform distribution also outputs heavy outcomes from the rejection sampling distribution on average. To prove this, we need to combine the analysis of quantum algorithm's success probability for SquaredForrelation with tail bounds on the number of "heavy" coefficients.

## 2 Low-Entropy sampling bounds against BQP

In this section, our main goal is to prove that FHOG can be used as proof of min-entropy in the Fourier sampling setting, and the trivial Fourier sampling algorithm is almost optimal. Since we are checking a statistical property of the output distribution for our test, and the prover can be adversarial, we need to directly analyze the multiple sample version of the problem to deal with parallel repetition, and avoid making assumptions about the algorithm being memoryless. Let $F = f_1, \ldots, f_m$ be a list of Boolean functions $f_i : \{0,1\}^n \to \{\pm 1\}$ and $\widehat{f_i}(z) = \mathbf{E}_{x \in \{0,1\}^n}[f_i(x) \cdot (-1)^{z \cdot x}]$. We define Fourier HOG as follows:

**Problem 7** (FHOG)**.** *Given oracle access to $F$, output a list of outcomes $Z = z_1, \ldots, z_m$, $z_i \in \{0,1\}^n$ such that:*

$$|\mathcal{H}(F, Z) - T_{\mathcal{H}} \cdot m| \leq c \cdot m$$

$$|\mathcal{L}(F,Z) - T_{\mathcal{L}} \cdot m| \leq c \cdot m$$

where $\mathcal{H}$ and $\mathcal{L}$ are defined by:

$$\mathcal{H}(F,Z) = \left\{ i \in [m] \;\middle|\; \tfrac{1}{N} < \widehat{f}_i(z_i)^2 \leq \tfrac{4}{N} \right\}, \quad \mathcal{L}(F,Z) = \left\{ i \in [m] \;\middle|\; \widehat{f}_i(z_i)^2 \leq \frac{1}{N} \right\},$$

and $T_{\mathcal{H}} = \mathbf{E}_{Y \sim \mathcal{N}(0,1)}[Y^2 \cdot \mathbb{1}_{\{1<Y^2\leq 4\}}] \approx 0.54$, $T_{\mathcal{L}} = \mathbf{E}_{Y \sim \mathcal{N}(0,1)}[Y^2 \cdot \mathbb{1}_{\{Y^2\leq 1\}}] \approx 0.2$ and $c = 0.02$. As we show in section 2.4, these constants ($T_{\mathcal{H}}$, $T_{\mathcal{L}}$ and $c$) are chosen in a way that a Chernoff bound can show that the simple quantum algorithm that samples according to the Fourier spectrum generates a valid solution for FHOG with high probability over the choice of functions and outcomes.

## 2.1 Worst-case, constant min-entropy: A simple BBBV argument

Let $Z_F = z_{f_1} \dots z_{f_m}$ ($z_{f_i} \in \{0,1\}^n$) be the most-probable output of $A^F$ (say, the first in lexicographical order if there are multiple such outputs). Then, let

$$P_{f_i} = \{x \in \{0,1\}^n : f_i(x) \cdot (-1)^{z_{f_i} \cdot x} = \operatorname{sgn}(\widehat{f}_i(z_{f_i}))\}.$$

In words, $P_{f_i}$ contains the inputs $x$ that contribute to $\widehat{f}_i(z_{f_i})^2$ being large; note that $P_{f_i}$ must have at least $N/2$ items. Second, let $E(f_i)$ be the set of functions that differ from $f_i$ in exactly $\sqrt{N}/2$ places that are all contained in $P_{f_i}$. Let $Q \subseteq [m]$, we can also define

$$E_Q(F) = \{f'_1 \dots f'_m \in \{\pm 1\}^N \mid \forall i \in Q : f'_i \in E(f_i) \wedge \forall i \notin Q : f'_i = f_i\}$$

$E_Q(F)$ is the set of all list of functions that differ with $F$ on elements of $Q$, and for each $i$ the new function is chosen from $E(f_i)$.

**Lemma 8.** *Let $A^F$ be a quantum algorithm that makes $T$ queries to $F$. For a $1 - N^{-1/4}$ fraction of $F' \in E_Q(F)$, we have $\delta(A^F, A^{F'}) \leq 2 \cdot |Q| \cdot TN^{-1/8}$ (where $\delta$ denotes the statistical distance between two distributions).*

*Proof.* Our proof closely mirrors the hybrid argument of [BBBV97]. At the $t$-th query to a phase oracle for $F$, let $\alpha^i_{t,x,w}$ be the amplitude on function $f_i$, query $x$, and workspace register $w$. The "query magnitude" on $\bigcup_i P_{f_i}$ is

$$\sum_{t=1}^{T} \sum_{i \in Q} \sum_{\substack{w \\ x \in P_{f_i}}} |\alpha^i_{t,x,w}|^2 \leq T$$

where $t$ is the time step and $w$ is the workspace register. Then for a random set $S = \bigcup_{i \in Q} S_i$, where $S_i \in \binom{P_{f_i}}{\sqrt{N}/2}$ defining a random function $f'_i(x) = f_i(x) \cdot (-1)^{1_{S_i}(x)} \in E(f_i)$,

$$\mathop{\mathbf{E}}_{S} \left[ \sum_{t=1}^{T} \sum_{i \in Q} \sum_{\substack{w \\ x \in S_i}} |\alpha^i_{t,x,w}|^2 \right] \leq \frac{|Q| \cdot T\sqrt{N}}{2 \min_i |P_{f_i}|} \leq \frac{|Q| \cdot T}{\sqrt{N}}.$$

By Markov's inequality,

$$\mathop{\mathbf{Pr}}_{S} \left[ \sum_{t=1}^{T} \sum_{i \in Q} \sum_{\substack{w \\ x \in S_i}} |\alpha^i_{t,x,w}|^2 \geq \frac{|Q| \cdot T}{N^{1/4}} \right] \leq \frac{1}{N^{1/4}},$$

So for the remainder of the proof, we assume that

$$\sum_{t=1}^{T} \sum_{i \in Q} \sum_{\substack{w \\ x \in S_i}} |\alpha^i_{t,x,w}|^2 \leq \frac{|Q| \cdot T}{N^{1/4}}.$$

By Cauchy-Schwartz,

$$\sum_{t=1}^{T} \sqrt{\sum_{i\in Q} \sum_{\substack{w \\ x\in S_i}} |\alpha^i_{t,x,w}|^2} \leq \frac{|Q|\cdot T}{N^{1/8}}.$$

Then by a hybrid argument, we can bound the total variation distance as

$$\delta(A^F, A^{F'}) \leq ||A^F|0\rangle - A^{F'}|0\rangle||_2 \leq \frac{2\cdot|Q|\cdot T}{N^{1/8}}. \qquad \square$$

In particular, this lemma implies that $\mathbf{Pr}[A^{F'} = z_F] \geq \mathbf{Pr}[A^F = z_F] - 2\cdot|Q|\cdot TN^{-1/8}$ for a $1 - N^{-1/4}$ fraction of $F' \in E_Q(F)$. From this it is already easy to see that, for any algorithm $A$ with very-low min-entropy (so that a decent majority of the time $A^F$ outputs one specific $Z$), there exist functions $F'$ for which $A^{F'}$ will fail to pass FHOG on $F'$. This follows since given a pair $(F, Z)$ such that $Z$ passes FHOG, we can simply set $Q$ to contain the index $i$ of all heavy outcomes $z_{f_i}$, and convert all of them randomly to light elements by picking a random function from $E(f_i)$. Next, we show that a similar min-entropy bound holds even when the algorithm only works on *average* over the choice of functions.

## 2.2 Average-case, constant min-entropy: Vertex degree in a bipartite graph

To extend this to an average-case statement about a list of random Boolean functions, first we notice that a direct application of the hybrid argument fails. Even though the worst-case argument can construct a large set of "Bad" functions (in which $A^F$ is not a solution for FHOG) from any list of "Good" functions (where $A^F$ passes FHOG), the size of all "Bad" lists might still be negligible compared to the size of "Good" functions. The concern is that many "Good" functions get pushed to the same small set of Bad ones. However, we show that under a careful double-counting argument, we can effectively bound the number of "Good" inputs that can produce any specific "Bad" input.

Let Good be the set of inputs that $A$ has constant min-entropy ($h = -\log(2/3)$) on, and the outcomes pass FHOG:

$$\mathsf{Good} = \left\{ F = f_1 \dots f_m \;\middle|\; \begin{array}{l} |\mathcal{H}(F, Z_F) - T_{\mathcal{H}}\cdot m| \leq c\cdot m \\ \wedge\, |\mathcal{L}(F, Z_F) - T_{\mathcal{L}}\cdot m| \leq c\cdot m \\ \wedge\, \mathbf{Pr}[Z_F \sim A^F] \geq 2^{-h} \end{array} \right\}$$

We let Bad be the set of inputs that the most probable outcome is "pretty bad", so most outcomes are light rather than heavy. Very specifically, we set $T^b_{\mathcal{H}} = T_{\mathcal{H}} - 0.26 \approx 0.28$ and $T^b_{\mathcal{L}} = T_{\mathcal{L}} + 0.26 \approx 0.46$ and define

$$\mathsf{Bad} = \left\{ F = f_1 \dots f_m \;\middle|\; \begin{array}{l} |\mathcal{H}(F, Z_F) - T^b_{\mathcal{H}}\cdot m| \leq c\cdot m \\ \wedge\, |\mathcal{L}(F, Z_F) - T^b_{\mathcal{L}}\cdot m| \leq c\cdot m \\ \wedge\, \mathbf{Pr}[Z_F \sim A^F] \geq 2^{-(h+0.01)} \end{array} \right\}$$

We now show that |Bad| is exponentially larger than |Good|, which implies that conditioned on $A$ being almost deterministic, $A$ passes FHOG with negligible probability (over the choice of random functions).

**Theorem 9.** *Suppose that $A$ makes at most $O(N^{1/9})$ queries to $F$. Then,*

$$|\mathsf{Bad}| \geq \exp(\Omega(m))\cdot|\mathsf{Good}|$$

**Corollary 10.** *Suppose that $A$ makes $O(N^{1/9})$ queries to $F$. Then, $\mathbf{Pr}_F[F \in \mathsf{Good}] \leq \exp(-\Omega(m))$.*

The corollary simply follows since $\mathbf{Pr}_F[F \in \mathsf{Good}] + \mathbf{Pr}_F[F \in \mathsf{Bad}] \leq 1$. Note that we can choose $m$ to be any large poly$(n)$, and make this probability as small as we need in next steps.

*Proof of Theorem 9.* Consider the following bipartite graph on nodes Good and Bad. Assume (without loss of generality) that $m$ is multiple of 50 and hence $0.26m$ is an integer. Draw an edge between $F \in \mathsf{Good}$ and $F' \in \mathsf{Bad}$ if $\exists Q, |Q| = 0.26m : F' \in E_Q(F)$ and $\delta(A^F, A^{F'}) \leq 2 \cdot |Q| \cdot TN^{-1/8}$. By Lemma 8, there are at least

$$(1 - N^{-1/4}) \cdot \sum_{F \in \mathsf{Good}, Q} |E_Q(F)| \geq (1 - N^{-1/4}) \cdot \binom{0.52m}{0.26m} \binom{N/2 + \sqrt{N}/2}{\sqrt{N}/2}^{0.26 \cdot m} |\mathsf{Good}|$$

edges incident on Good since for $(F, F')$ with $H_\infty(A^F) \leq h$ and $\delta(A^F, A^{F'}) \leq 2 \cdot |Q| \cdot TN^{-1/8} = o(1)$ we must have $H_\infty(A^{F'}) \leq h + o(1) \leq h + 0.01$. Moreover, if $(F, F')$ is an edge in the graph, since $\mathbf{Pr}[A^F = z_F] = 2^{-H_\infty(A^F)} \geq 2^{-h} \geq 2/3$ and $\delta(A^F, A^{F'}) = o(1)$ then $A^F$ and $A^{F'}$ have the same majority output (i.e., $Z_F = Z_{F'}$). This allows us to bound the number of edges on Bad from above:

$$\binom{0.48m}{0.26m} \binom{N/2}{\sqrt{N}/2}^{0.26m} |\mathsf{Bad}|$$

edges incident on Bad. Combining these bounds, we find that

$$\frac{|\mathsf{Bad}|}{|\mathsf{Good}|} \geq (1 - N^{-1/4}) \cdot \frac{\binom{0.52m}{0.26m} \cdot \binom{N/2+\sqrt{N}/2}{\sqrt{N}/2}^{0.26m}}{\binom{0.48m}{0.26m} \cdot \binom{N/2}{\sqrt{N}/2}^{0.26m}} \geq (1 - o(1)) \cdot \left(\frac{0.52}{0.48}\right)^{0.26 \cdot m} \cdot e^{\frac{1}{2} 0.26 \cdot m} \qquad \square$$

Intuitively, this theorem implies that the constant min-entropy portion of any quantum algorithm does not solve FHOG with high probability over the choice of functions. In other words, there is no quantum algorithm that has constant min-entropy on $\gg \exp(-m)$ fraction of inputs, if the heavy outcomes are good solutions to Problem 7. Next, we use this fact to extend this lower bound even to quantum algorithms with linear min-entropy by giving a reduction to the constant min-entropy version.

## 2.3 Average-case, linear min-entropy: A general reparameterization trick

Notice that we have an exponential query bound for a constant min-entropy algorithm. Using exponentially many queries, we can approximate the output distribution of a linear min-entropy algorithm. This allows us to trade our exponential query lower bound against *constant* min-entropy for a smaller-exponential query lower bound against *linear* min-entropy.

**Theorem 11.** *Suppose $A$ is any quantum algorithm making $O(N^{1/100})$ queries to an oracle, and let $F = f_1, \ldots, f_m : \{0,1\}^n \to \{\pm 1\}$ be a list of random Boolean functions, with $m \geq n$. For any polynomial $\delta(1/n)$, there exists a negligible function $\mathrm{negl}(n)$ such that the following holds:*

$$\mathop{\mathbf{Pr}}_{F}\left[\mathop{\mathbf{Pr}}_{A}[A^F \textit{ passes } \mathsf{FHOG}] \geq \delta(1/n) \wedge \mathop{\mathbf{Pr}}_{Z \sim \chi}[q_Z \geq 2^{-n/40}] \geq \mathrm{negl}(n)\right] \leq \mathrm{negl}(n)$$

*where $\chi$ is the output distribution of $A^F$ conditioned on passing FHOG and $q_Z$ is the probability to sample $Z$ according to $\chi$.*

In words, the theorem states that it is very unlikely to draw a collection of functions $F$ such that $A^F$ passes FHOG with non-negligible probability and the output of $A^F$ has high enough probability mass on elements that appear with probability at least $2^{-n/40}$. Note that it is crucial for us to analyze $\chi$ – the output distribution of $A$ conditioned on $F$ – and not the output distribution of $A$ averaged over random oracles. This implies that the output distribution of $A$ must be statistically close to a high min-entropy distribution even when conditioned on the choice of the random oracle, and hence, the generated entropy is inherently from the quantum algorithm.

*Proof.* Fix $\mathrm{negl}(n) = \gamma$, and suppose that there exists a quantum algorithm $A$ that does not satisfy the condition. This implies that on $1/\mathrm{poly}(n)$ fraction of inputs $A^F$ passes the test with probability at least $1/\mathrm{poly}(n)$ and that $\mathbf{Pr}_{Z\sim\chi}[q_Z \geq 2^{-n/40}] \geq \gamma$. First select randomness $r$ (to be fixed later in the algorithm), which will be used to generate an algorithm $A'_r$ that satisfies the conditions of Corollary 10. Intuitively, we use $r$ to extract the inherent randomness of the quantum algorithm, and by fixing it later in the process, we achieve the desired low min-entropy property. This algorithm will be nearly deterministic on a large fraction of possible inputs and goes as follows.

1. Take $O((mn)^2 \cdot 2^{n/10})$ samples from $A$ in order to get empirical estimates $\widetilde{p}_Z$ of all of the probabilities $p_Z = \mathbf{Pr}_A[A^F \text{ Samples } Z]$, for all $Z \in (\{0,1\}^n)^m$, to within additive error $2^{-n/20}$ with high probability.

2. Pick a random threshold $\tau$ which is an integer multiple of $2^{-n/20}$ in the range $[\varepsilon, 2\varepsilon]$ for $\varepsilon = 2^{-n/30}$.

3. Denote by $\mathcal{P} = \{Z : \widetilde{p}_Z \geq \tau\}$ the set of "probable" outcomes. Consider the renormalized distribution $\widetilde{p}_{Z|\mathcal{P}}$ over only the probable elements, i.e., for any $Z \in \mathcal{P}$ let $\widetilde{p}_{Z|\mathcal{P}} = \frac{\widetilde{p}_Z}{\sum_{Z\in\mathcal{P}} p_Z}$.

4. Use $r$ to rejection sample according to the probability distribution $\widetilde{p}_{Z|\mathcal{P}}$. Concretely, view $r$ as a list of uniformly random points $(\vec{x}_1, y_1), (\vec{x}_2, y_2), \cdots \in (\{0,1\}^n)^m \times [0,1]$. Output the first $\vec{x}_i$ such that $y_i$ is less than the estimated probability for $\vec{x}_i$. We denote the output of this procedure by $\mathrm{RejSamp}(\widetilde{p}_{Z|\mathcal{P}}, r)$. Notice that since we fix $r$ later in the algorithm, $r$ (and the precision of $y_i$) can be as large as we need.

We need to show that for some fixed choices of $(\tau, r)$, $A'_{\tau,r}$ is pseudo-deterministic and succeeds FHOG with probability $\gamma/\mathrm{poly}(n)$. Then we can invoke Corollary 10.

Fix an $F$ where the condition is not satisfied. First we notice that if $q_Z = \mathbf{Pr}[Z \sim \chi] \geq 2^{-n/40}$, then $\mathbf{Pr}_A[Z \sim A^F \wedge A^F \text{ solves FHOG}] \geq 2^{-n/40} \cdot 1/\mathrm{poly}(n) \geq 3 \cdot 2^{-n/30}$. This is clear since $\mathbf{Pr}_A[A^F \text{ passes FHOG}] \geq \frac{1}{\mathrm{poly}(n)}$. Thus,

$$\sum_{\substack{Z: p_Z \geq 3\cdot 2^{-n/30}, \\ Z \text{ solves FHOG}}} p_Z \geq \sum_{Z: p_Z \geq 3\cdot 2^{-n/30}} q_Z \cdot \delta(1/n) \geq \gamma/\mathrm{poly}(n). \tag{1}$$

So for any such $F$, we have $\frac{\gamma}{\mathrm{poly}(n)}$ probability mass on $Z : p_Z \geq 3 \cdot 2^{-n/30}$ that also solve FHOG.

Then, we note that by Chernoff bound the following event $\mathcal{E}$ happens with probability at least $1 - \exp(-mn)$: for all $Z$, $|\widetilde{p}_Z - p_Z| \leq 2^{-n/20}$.

Consider the process of rejection sampling over the true distribution $p$ and over the estimated distribution $\widetilde{p}$. Our first claim is:

**Claim 12.** *Conditioned on $\mathcal{E}$, with $1 - \exp(-\Omega(n))$ probability over the choice of $\tau$, the distributions $p_{Z|\mathcal{P}}$ and $\widetilde{p}_{Z|\mathcal{P}}$ are $\exp(-\Omega(n))$-close in statistical distance.*

We defer the proof to Appendix C. Fix a "good" $\tau$ that satisfies that $p_{Z|\mathcal{P}}$ and $\widetilde{p}_{Z|\mathcal{P}}$ are $\exp(-\Omega(n))$-close in statistical distance. This means that the output of Rejection Sampling will be identical for most choices of $r$ by the following claim.

**Claim 13.** *If $\mathcal{D}$, $\mathcal{D}'$ are two distributions over the same finite domain $\mathcal{X}$ with statistical distance $\varepsilon$ then $\mathbf{Pr}_r[\mathrm{RejSamp}(\mathcal{D}, r) \neq \mathrm{RejSamp}(\mathcal{D}', r)] = 2\varepsilon/(1+\varepsilon)$*

*Proof.* The probability that $\mathrm{RejSamp}(\mathcal{D}, r) \neq \mathrm{RejSamp}(\mathcal{D}', r)$ is exactly the probability that we land in one of the "bad" regions $(\min\{\mathcal{D}(x), \mathcal{D}'(x)\}, \max\{\mathcal{D}(x), \mathcal{D}'(x)\}]$ for $x \in \mathcal{X}$ before reaching one the "good" region $[0, \min\{\mathcal{D}(x), \mathcal{D}'(x)\}]$ for $x \in \mathcal{X}$. Indeed, the overall area of the bad regions equals twice the statistical distance between $\mathcal{D}$ and $\mathcal{D}'$. The overall area of the good regions equals $1 - \varepsilon$. Thus the probability of reaching a bad region before reaching a good region is $2\varepsilon/(2\varepsilon + 1 - \varepsilon) = 2\varepsilon/(1+\varepsilon)$. □

Note that for *any* $\tau$ whatsoever,

$$\sum_{\substack{Z: p_Z \geq \tau, \\ Z \text{ solves } \mathsf{FHOG}}} p_Z \geq \gamma/\mathrm{poly}(n)$$

using Equation (1) and the fact that $\tau < 3 \cdot 2^{-n/20}$. Furthermore, under the event $\mathcal{E}$, we have

$$\sum_{\substack{Z: \widetilde{p_Z} \geq \tau, \\ Z \text{ solves } \mathsf{FHOG}}} \widetilde{p}_Z \geq \sum_{\substack{Z: p_Z \geq 3 \cdot 2^{-n/30}, \\ Z \text{ solves } \mathsf{FHOG}}} (p_Z - 2^{-n/20}) \geq \gamma/\mathrm{poly}(n) - 2^{-\Omega(n)} \geq \gamma/\mathrm{poly}(n),$$

as well.

Overall we get that for any "good" $F$, with high probability $\mathcal{E}$ and $\tau$ is "good". Conditioned on $\mathcal{E}$ and $\tau$ is "good", we have that $\mathrm{RejSamp}(\widetilde{p}_{Z|\mathcal{P}}, r) = \mathrm{RejSamp}(p_{Z|\mathcal{P}}, r)$ with high probability. Furthermore, under such conditioning $\mathrm{RejSamp}(\widetilde{p}_{Z|\mathcal{P}}, r)$ samples an element that passes $\mathsf{FHOG}$ with probability at least $\gamma/\mathrm{poly}(n)$. We say that $(\tau, r)$ are deterministically-good if

$$\Pr_{F \in \text{"Good Fs"}, A}[\mathrm{RejSamp}(p_{Z|\mathcal{P}}, r) \neq \mathrm{RejSamp}(\widetilde{p}_{Z|\mathcal{P}}, r)] \leq \mathrm{negl}(1/n)$$

Indeed we see that most choices of $(\tau, r)$ are deterministically-good. Let

$$\delta := \mathop{\mathbf{E}}_{\tau, r}[\Pr_{F \in \text{"Good Fs"}, A}[\mathrm{RejSamp}(\widetilde{p}_{Z|\mathcal{P}}, r) \text{ passes } \mathsf{FHOG}]] \geq \gamma/\mathrm{poly}(n)$$

We say that $(\tau, r)$ are $\mathsf{FHOG}$-good if

$$\Pr_{F \in \text{"Good Fs"}, A}[\mathrm{RejSamp}(\widetilde{p}_{Z|\mathcal{P}}, r) \text{ passes } \mathsf{FHOG}] \geq \delta/2.$$

By a simple Markov's inequality, we see that at least $\delta/2$ fraction of the choices of $(\tau, r)$ are $\mathsf{FHOG}$-good. Thus, there exists a choice of $(\tau, r)$ that is both $\mathsf{FHOG}$-good, and deterministically-good. However, this leads to a contradiction of Corollary 10. Indeed, we see that for this specific $(\tau, r)$ we have that at least $1/\mathrm{poly}(n)$ fractions of $F$ are "Good" in the sense that $A'_r$ outputs the constant value $\mathrm{RejSamp}(p_{Z|\mathcal{P}}, r)$ with probability close to 1, and at the same time $A'_r$ solves $\mathsf{FHOG}$ with probability at least $\gamma/\mathrm{poly}(n)$. This shows that $\mathbf{Pr}[F \in \mathsf{Good}] \geq \gamma/\mathrm{poly}(n)$ which is a contradiction to Corollary 10 for any $\gamma = 2^{-o(m)}$. □

## 2.4 Success of the high-entropy algorithm

We had better check that we can solve $\mathsf{FHOG}$ with a quantum algorithm with no restrictions on the min-entropy. Otherwise, our test would be impossible even for an honest algorithm! The simple quantum algorithm first prepares the following state using one query to the oracle for each $f_i$:

$$\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} f_i(x) \, |x\rangle$$

And then applies a Hadamard gate to all qubits and measures them in the computational basis. Here we verify that this usual high min-entropy algorithm solves $\mathsf{FHOG}$. Similar calculations can also be found in Lemma 8 of [Aar10].

**Fact 14.** *If $A$ is the usual quantum algorithm for sampling from $\widehat{f}_i$, then with probability $1 - \exp(\Omega(m))$ over the choice of functions and the internal randomness of $A$:*

$$|\mathcal{H}(F, A^F) - T_{\mathcal{H}} \cdot m| \leq c \cdot m, \qquad |\mathcal{L}(F, A^F) - T_{\mathcal{L}} \cdot m| \leq c \cdot m$$

*Proof.* For each $z$, $\widehat{f}(z)$ follows a normal distribution with mean 0 and variance $1/N$. So averaged over the choice of $f$, the probability that $A$ outputs a "light" outcome is given by:

$$\begin{aligned}\mathbf{Pr}[\widehat{f}(A_f)^2 \leq 1/N] &= \mathop{\mathbf{E}}_f\left[\sum_{z:\widehat{f}(z)^2\leq 1/N} \widehat{f}(z)^2\right] = \sum_{z\in\{0,1\}^n} \mathop{\mathbf{E}}_f\left[\widehat{f}(z)^2 \cdot \mathbb{1}_{\{\widehat{f}(z)^2\leq 1/N\}}\right] \\ &\approx N \cdot \mathop{\mathbf{E}}_{X\sim\mathcal{N}(0,1/N)}[X^2 \cdot \mathbb{1}_{\{X^2\leq 1/N\}}] = \mathop{\mathbf{E}}_{Y\sim\mathcal{N}(0,1)}[Y^2 \cdot \mathbb{1}_{\{Y^2\leq 1\}}] = T_{\mathcal{L}}.\end{aligned}$$

Similarly,

$$\mathbf{Pr}[1/N < \widehat{f}(A_f)^2 \leq 4/N] \approx \mathop{\mathbf{E}}_{Y\sim\mathcal{N}(0,1)}[Y^2 \cdot \mathbb{1}_{\{1<Y^2\leq 4\}}] = T_{\mathcal{H}}$$

Since $A$ repeats this $m$ times, a Chernoff bound followed by a union bound proves the claim. □

### 2.5 Proof of min-entropy

To specify a certified randomness protocol we consider a setting in which a prover can certify to a verifier that a bit string has been sampled from a distribution that is statistically close to uniformly random. We demand that the protocol is complete – there exists a prover that fails with non-negligible probability over the random $F$, and is sound – no dishonest prover can force the verifier to accept a heavily biased output with non-negligible probability. This is easily achievable if the verifier can access a high min-entropy source, since it can always use classical randomness extractors [GUV09] to extract uniformly random bits. Theorem 11 and Fact 14 give us the tools to construct a proof of min-entropy protocol. Let $m = \text{poly}(n)$, and consider the following protocol:

1. Given $F$, the prover attempts to pass FHOG, and sends $Z = z_1, \ldots, z_m$ as proof.
2. The verifier computes $|\mathcal{H}(F, Z)|$ and $|\mathcal{L}(F, Z)|$ (using exponential number of queries), and accepts if they are within the expected range.

To show completeness, we use Fact 14. This effectively shows that there exists a quantum algorithm that runs in polynomial time and finds a good solution that the verifier rejects with negligible probability.

The soundness follows from Theorem 11, which states that with high probability over the choice of $F$, the output distribution of any $\text{poly}(n)$ query quantum algorithm – conditioned on the verifier accepting – is $\text{negl}(n)$ close in total variation distance to a $\Omega(n)$ min-entropy distribution.

Note that this is similar to the definition of the min-entropy protocol defined in [YZ24] with two main differences. First, the verification is not efficient and requires an exponential number of queries to the oracle. Second, the soundness argument in [YZ24] requires that the output distribution must have high min-entropy with high probability over the choice of $F$. Our soundness requirement is less stringent and allows the distribution to be statistically close to a high min-entropy distribution. Using randomness extractors on a distribution that is close in total variation distance to a high min-entropy distribution would only affect the closeness of the random bits to the uniform distribution. As long as this statistical distance is negligible this minor difference does not affect the protocol.

## 3 Black Box LLQSV

So far we focused on how Fourier Sampling can independently be seen as a tool for certified random number generation in the QROM. In [Aar18a], Aaronson considers certified randomness in the white-box setting and is able to specify a protocol assuming the LLQSV conjecture. To give evidence for LLQSV in the following two sections we consider black-box variants of the LLQSV conjecture.

First, we formally define the black-box variant of LLQSV:

**Problem 15** (Black-Box LLQSV)**.** *Given oracle access to $\mathcal{O}$, a list of pairs of functions $f_i : \{0,1\}^n \to \{\pm 1\}$ and outcomes $s_i \in \{0,1\}^n$ of length $m$, distinguish whether $\mathcal{O}$ was sampled according to distribution $\mathcal{U}$ or $\mathcal{D}$, where:*

- *$\mathcal{U}$: For each $i \in [m]$, $f_i$ and $s_i$ are chosen uniformly at random.*
- *$\mathcal{D}$ : For each $i \in [m]$, $f_i$ is a random Boolean function, and $s_i$ is sampled according to $\widehat{f_i}^2$.*

We observe there is a close connection between Black-Box LLQSV and the MAJORITY problem. To see this we notice that in either case the probability of sampling a pair $(f, s)$ only depends on the magnitude of the Fourier coefficient of $f$ at $s$, or equivalently $|h(f \cdot \chi_s) - N/2|$, where $h$ is the hamming weight and $\chi_s$ is the $s$-Fourier character, i.e., $\chi_s(x) = (-1)^{x \cdot s}$) (For simplicity we also refer to the $2^n$ bit string generated by the truth table of functions as $f$). This allows us to write both distributions as a linear combination of simpler distributions $\mathcal{U}_d^N$ – the uniform distribution over all strings of hamming weight $N/2 + d$ or $N/2 - d$. To provide evidence for QCAM hardness, we unconditionally prove lower bounds against BQP and PH (And hence, against AM [BHZ87]).

First, we notice an alternative way to sample from the distribution $\mathcal{D}$ that makes our analysis easier. Since $\forall z \in \{0,1\}^n : \mathbf{Pr}_{\mathcal{D}}[s_i = z] = \frac{1}{N}$, we can sample from the joint distribution of a random function and a sample according to the Fourier distribution by first sampling a uniformly random outcome $s_i$, and then picking a random function $f_i$ weighted according to $\widehat{f_i}(s_i)^2$. Both of our results in this section follow two observations. Let $\mathcal{U}_d^N$ be the uniform distribution over the following set:

$$\{S \in \{0,1\}^N | h(S) = N/2 - d \vee h(S) = N/2 + d\}$$

First, for both distributions $\mathcal{U}$ and $\mathcal{D}$ the distribution over $f_i \cdot \chi_{s_i}$ is a linear combination of $\mathcal{U}_0^N, \mathcal{U}_1^N, \ldots, \mathcal{U}_{N/2}^N$. In the uniform case, this is clear since $f_i \cdot \chi_{s_i}$ is a uniformly random string. For $\mathcal{D}$, hamming weight of $f_i \cdot \chi_{s_i}$ specifies the Fourier coefficient $\widehat{f_i}(s_i)$, so all strings with hamming weight $N/2 + d$ or $N/2 - d$ occur with equal probability. So, we can write both probability distributions as:

$$\sum_{D := (d_1, \ldots, d_m) \in [N/2+1]^m} p_D \mathcal{U}_{d_1} \times \ldots \times \mathcal{U}_{d_m}$$

For some set of coefficients where $\sum_D p_D = 1$. Let us call these distributions $\chi_{\mathcal{D}}$ and $\chi_{\mathcal{U}}$ respectively.

Next, we use the fact that in both distributions $\mathcal{U}$ and $\mathcal{D}$ the marginal distribution over the functions is uniform. Thus, with high probability, the Fourier coefficients are bounded:

**Theorem 16.** *Given a random Boolean function $f : \{\pm 1\}^n \to \{0,1\}$, the probability that a squared Fourier coefficient of $f$ is larger than $\frac{p(n)^2}{N}$ is at most $2\exp(\frac{-p(n)^2}{6} + \ln N)$.*

*Proof.* This follows from a Chernoff bound. Let $X = h(f \cdot \chi_s)$. For every $s$, this is a uniformly random string, so we can write:

$$\mathbf{Pr}\left[X \leq \left(1 - \frac{p(n)}{\sqrt{N}}\right) N/2\right] \leq \exp(-p(n)^2/4)$$

$$\mathbf{Pr}\left[X \geq \left(1 + \frac{p(n)}{\sqrt{N}}\right) N/2\right] \leq \exp(-p(n)^2/6)$$

The claim follows from union bound. □

Note that in both $\mathcal{D}$ and $\mathcal{U}$, $f_i$ is a random Boolean function. So in either case by a union bound we can prove that with probability at least $1 - 2\exp(\frac{-p(n)^2}{6} + \ln N + \ln m)$ none of these functions have a squared Fourier coefficient larger than $\frac{p(n)^2}{N}$. So as long as $\ln m$ is polynomial in $n$ we can choose $p(n)$ in a way that this event happens with an exponentially small probability.

It is clear that distinguishing $\mathcal{D}$ and $\mathcal{U}$ is harder than distinguishing $\chi_{\mathcal{U}}$ and $\chi_{\mathcal{D}}$ since given $f_i, s_i$ we can compute $f_i \cdot \chi_{s_i}$. The other direction is not as clear since given a long list of strings $S_1, \ldots, S_m$,

we need $s_1, \ldots, s_m$ to recover $f_1, \ldots, f_m$. However, given a sample from $\chi_{\mathcal{D}}$ or $\chi_{\mathcal{U}}$, we can easily get a sample from $\mathcal{D}$ or $\mathcal{U}$ respectively, by simply choosing uniformly random $s_1, \ldots, s_m$. So, assuming we have access to a long list of random bits, any distinguisher for $\chi_{\mathcal{U}}$ and $\chi_{\mathcal{D}}$ also distinguishes $\mathcal{D}$ and $\mathcal{U}$. As we will see in analysis having access to an extra random oracle does not give any extra computation power to the BQP or PH algorithm. Combining Theorem 16 with this fact implies that any distinguisher for $\mathcal{U}$ and $\mathcal{D}$ must also distinguish the following two distributions with high probability:

- $\chi'_{\mathcal{U}} = \sum_{d_1 \ldots d_m \in [p(n)^2\sqrt{N}]} p_D \mathcal{U}_{d_1}^N \times \ldots \times \mathcal{U}_{d_m}^N$
- $\chi'_{\mathcal{D}} = \sum_{d_1 \ldots d_m \in [p(n)^2\sqrt{N}]} q_D \mathcal{U}_{d_1}^N \times \ldots \times \mathcal{U}_{d_m}^N$

Since $\chi_{\mathcal{U}}$ and $\chi_{\mathcal{D}}$ are statistically close to $\chi'_{\mathcal{U}}$ and $\chi'_{\mathcal{D}}$ respectively. Furthermore, since $\sum_D p_D \leq 1$ and $\sum_D q_D \leq 1$, by an averaging argument this distinguisher can also distinguish two distributions in the sum with a $1/\text{poly}(n)$ advantage. This reduces the problem to indistinguishability of $\mathcal{U}_{\mathcal{D}}$ and $\mathcal{U}_{D'}$, where $d_i$ and $d'_i$ are at most $p(n)\sqrt{N}$. Thus, to complete the proof we need to show BQP and PH lower bounds for the following problem:

**Problem 17** (BalanceChecking)**.** *Let $0 \leq d_i \leq p(n) \cdot \sqrt{N}$. Given oracle access to a list of strings $S = S_1, \ldots, S_m$, where $S_i \in \{0,1\}^N$, distinguish whether the oracle was sampled according to distribution $\mathcal{U}_D$ or $\mathcal{U}_0$, where:*

1. *$\mathcal{U}_D$: $S_i$ is drawn from $\mathcal{U}_{d_i}^N$.*
2. *$\mathcal{U}_0$: $S_i$ is drawn from $\mathcal{U}_0^N$.*

Note that indistinguishability of $\mathcal{U}_D$ and $\mathcal{U}_0$ implies indistinguishability of $\mathcal{U}_D$ and $\mathcal{U}_{D'}$. We say algorithm $A$ solves BalanceChecking with advantage $\delta$, if:

$$\left| \Pr_{S \sim \mathcal{U}_D} [A \text{ accepts } S] - \Pr_{S \sim \mathcal{U}_0} [A \text{ accepts } S] \right| \geq \delta$$

In our proofs, we use a hybrid argument to get the BQP lower bound. Furthermore, this reduction enables us to use an argument similar to what is given in [FSUV13, Aar10] to prove a bound against $\mathsf{AC}^0$. Informally, since this simplified problem is random self-reducible, combined with a circuit lower bound due to Håstad we can beat the hybrid argument, and extend the lower bound to an exponentially long list. Notice that black-box LLQSV is slightly different than BalanceChecking, since it also has access to a random string for each $S_i$ (which is the outcome $s_i$). To complete our proof, we need to show that having access to these extra random strings do not give us any extra computation power. This is straightforward from the hybrid argument for the BQP lower bound, and we can again use random self-reducibility of BalanceChecking to show the same claim for the PH argument.

## 3.1 BQP Lower Bound for black-box LLQSV

**Theorem 18.** *Any $T$ query quantum algorithm for* BalanceChecking *has advantage at most $p(n) \cdot TN^{-1/8}$.*

*Proof.* This follows from a BBBV style argument. Suppose that $S$ is drawn from $\mathcal{U}_{d_1}^N \times \ldots \times \mathcal{U}_{d_m}^N$. We can modify each $S_i$ in at most $p(n) \cdot \sqrt{N}$ entries to make each $S_i$ balanced. Let this new string be $S'$. Let $P_i$ be the set of possible entries for each string $S_i$, and $P = \bigcup_i P_i$. Then given a quantum algorithm $A$, we can write the query magnitude of each $P_i$ as:

$$\sum_{t=1}^{T} \sum_{\substack{w \\ x \in P_i}} |\alpha_{t,x,w}|^2 \leq T_i$$

and $\sum_i T_i = T$. So if we choose a random subset $\Delta = \bigcup_i \Delta_i$ for the modified entries of each $S_i$, we can write the expected value of the query magnitude as:

$$\mathop{\mathbf{E}}_{\Delta}\Big[\sum_{t=1}^{T}\sum_{i}^{m}\sum_{\substack{w\\x\in\Delta_i}}|\alpha_{t,x,w}|^2\Big] = \sum_{i}^{m}\mathop{\mathbf{E}}_{\Delta_i}\Big[\sum_{t=1}^{T}\sum_{\substack{w\\x\in\Delta_i}}|\alpha_{t,x,w}|^2\Big] \leq \sum_{i}^{m}\frac{T_i p(n)\sqrt{N}}{2|P_i|} \leq \frac{p(n)T}{\sqrt{N}}$$

And by Markov's inequality and Cauchy-Schwartz, we get that for $1 - N^{-1/4}$ fraction of $S'$:

$$\delta(A(S), A(S')) \leq 4 \cdot p(n) \cdot TN^{-1/8}$$

However, this random modification also preserves the distribution in this case. To sample according to $\mathcal{U}_0$, we can first sample from $\mathcal{U}_d$ and then randomly flip the excess bits to make the string balanced. So the advantage of $A$ is at most:

$$N^{-1/4} + 4 \cdot p(n) \cdot TN^{-1/8} \leq 8 \cdot p(n) \cdot TN^{-1/8}$$

□

**Theorem 19** (BQP Bound)**.** *Any quantum algorithm for Black-Box* LLQSV *with advantage* $\delta = 1/\mathrm{poly}(n)$ *must make at least* $\Omega(N^{1/10})$ *queries to the oracle.*

*Proof.* Suppose there exists a $O(N^{1/10})$ quantum query algorithm for black-box LLQSV. First we notice that the same hybrid argument works without any modification if in BalanceChecking we have access to $(S_i, s_i)$, where $s_i$ is a uniformly random string. Now we can use $s_i$ to recover $f$ by computing $S_i \cdot \chi_{s_i}$. From Theorem 16, any distinguisher for black-box LLQSV must also solve BalanceChecking (with the additional access to $s_i$) with advantage at least $\delta' = \delta - 2\exp(\frac{-p(n)^2}{6} - \ln N - \ln m)$. We can choose an appropriate polynomial $p$ so that $\frac{p(n)^2}{6} - \ln N - \ln m \geq n$. Then for large enough $n$, this implies $\delta' \geq \delta/2 = 1/\mathrm{poly}(n)$. However, we know that:

$$\delta' \leq 8 \cdot p(n) \cdot cN^{1/10} \cdot N^{-1/8} = O(N^{-1/40})$$

Which gives us a contradiction. □

## 3.2 PH Lower Bound for black-box LLQSV

We start from a well known $\mathsf{AC}^0$ lower bound [Hås86]:

**Lemma 20.** *Given an $N$ bit string $S$, any depth $d$ circuit that accepts all $S$ such that $h(S) = N/2+1$ and rejects them if $h(S) = N/2$ has size:*

$$\exp\left(\Omega(N^{1/(d-1)}\right)$$

First we notice that the same bound holds for distinguishing $h(S) = N/2$ from $|h(S) - N/2| = 1$. The next step is to prove analog of Theorem 18 against PH.

**Theorem 21.** *Any depth $d$ circuit that solves* BalanceChecking *with* $1/\mathrm{poly}(n)$ *advantage has size:*

$$\exp\left(\Omega(N^{1/(2d+4)})\right)$$

*Proof.* Suppose there exists a circuit $C$ of size $s$ and depth $d$ that solves BalanceChecking with advantage $\delta = 1/\mathrm{poly}(n)$. Using $C$ we can construct a circuit $C'$ of size $s' = \mathrm{poly}(s, N)$ and depth $d + 3$ that solves the problem in Lemma 20 for length $\sqrt{N}/p(n)$. Given a $\sqrt{N}/p(n)$ bit string $t$, for each $i$, we copy the string $d_i$ times and then pad it with an equal number of zeros and ones to have length $N$. We

then take a random permutation of this string and flip all bits with probability 1/2 to get $S_i$. Note that if the original string is balanced $S_i \sim \mathcal{U}_0^N$, and otherwise $S_i \sim \mathcal{U}_D^N$. Then we know:

$$\left| \mathbf{Pr}\left[A \text{ accepts } S | t \text{ balanced}\right] - \mathbf{Pr}\left[A \text{ accepts } S | t \text{ not balanced}\right] \right| \geq \delta$$

We can repeat this $r = \text{poly}(1/\delta, N)$ times. By Chernoff bound, we get a $1/\delta$ gap with arbitrary large probability $\exp\left(-\text{poly}(N)\right)$, which is detectable by an approximate majority circuit (see [Aar10, Vio07] for more detail). Let us call this new circuit $C'$. We can then fix the randomness in a way that the new circuit $C'$ succeeds on every input simultaneously. This new circuit has depth $d+3$ and size $\text{poly}(s, N)$. So $s$ must be at least:

$$\exp\left(\Omega(\sqrt{N}^{-1/(d+2)}\right) = \exp\left(\Omega(N^{1/(2d+4)}\right)$$

□

**Corollary 22.** *Any depth $d$ circuit that solves black-box* LLQSV *with* $1/\text{poly}(n)$ *advantage has size:*

$$\exp\left(\Omega(N^{1/(2d+4)})\right)$$

*Proof.* Similar to the BQP bound, the first step is to prove the same $\mathsf{AC}^0$ bound for BalanceChecking even when the algorithm has additional access to a long list of random outcomes $s_1, \ldots, s_m$. This immediately follows from the proof idea of Theorem 21, since we can choose uniformly random $s_i$ in the circuit for each instance separately (without accessing the oracle, while preserving the distribution), and later fix them in the circuit. Furthermore, from Theorem 16, any $1/\text{poly}(n)$ distinguisher for Black-Box LLQSV would also work for BalanceChecking with the additional outcome oracle by choosing the polynomial $p$ to be large enough. □

Corollary 22 and the standard conversion between PH and $\mathsf{AC}^0$ proves a PH lower bound for solving Black-Box LLQSV.

## 4 The SquaredForrelation Problem and Black-Box LLQSV

In this section, we first prove an alternative oracle separation between BQP and PH, and then show a reduction from SquaredForrelation to a problem similar to Black-Box LLQSV. To prove the lower bound we build on the previous work of Raz and Tal [RT19] to define a distribution $\mathcal{D}$ over pairs of Boolean functions $(f, g)$ that is indistinguishable from uniform in the polynomial hierarchy, and yet a simple quantum algorithm is able to distinguish them.

This hardness result does not immediately follow from previous oracle separations and requires careful modifications of Raz and Tal analysis to make them work with squared Fourier coefficients for both the PH lower bound and the quantum algorithm. Furthermore, we extend these results to the "long list" setting and prove that having oracle access to an exponentially long list of samples does not make the problem any easier.

Before getting into the formal results, let us start with the simplified problem 6. One can choose the threshold parameter to be the median of squared Fourier coefficients of a random Boolean function, so that almost half of the coefficients are indicated as heavy on average, i.e $\mathbf{Pr}_{x,f}[g(x) = 1] \approx 1/2$.

Then one can easily find random heavy Fourier coefficients by finding a random $x$ such that $g(x) = 1$. The distribution $\mathcal{D}$ that we define next is similar to simplified SquaredForrelation in the sense that we use randomized rounding on squared Fourier coefficients and we can prove that on average, heavy Fourier coefficients have a slightly higher chance of having $g(x) = 1$. We leverage this to reduce SquaredForrelation to a black-box variant of LLQSV.

Let us first summarize the separation result that we are going to use to give evidence for LLQSV. Similar to [RT19], to show an oracle separation of BQP and PH it suffices to find a distribution $\mathcal{D}$

that is pseudorandom for $\mathsf{AC}^0$ circuits, but not for efficient quantum algorithms making few queries. First, we start by defining distribution $\mathcal{D}$ using truncated multivariate Gaussians. Let $n \in \mathbb{N}$, $N = 2^n$. Let $\varepsilon = 1/(C \ln N)$ for a constant $C \geq 20$ to be chosen later. Define $\mathcal{G}$ to be a multivariate Gaussian distribution over $\mathbb{R}^N \times \mathbb{R}^N$ with mean 0 and covariance matrix:

$$\varepsilon \cdot \begin{pmatrix} I_N & H_N \\ H_N & I_N \end{pmatrix}$$

Where $H_N$ is the Hadamard transform. To take samples from $\mathcal{G}$, we can first sample $X = x_1, \ldots, x_N \sim \mathcal{N}(0, \varepsilon)$, and let $Y = H_N \cdot X$. Define $\mathcal{G}'$ to be the distribution over $Z = (X, Y^2 - \varepsilon)$. Let $\mathrm{trnc}(a) = \min(1, \max(-1, a))$. The distribution $\mathcal{D}$ over $\{\pm 1\}^{2N}$, first draws $Z \sim \mathcal{G}'$. Then for each $i \in [2N]$ draws $z'_i = 1$ with probability $\frac{1+\mathrm{trnc}(z_i)}{2}$ and $z'_i = -1$ with probability $\frac{1-\mathrm{trnc}(z_i)}{2}$. Now we can define the following promise problem:

**Problem 23** (SquaredForrelation)**.** *Given oracle access to Boolean functions $f, g : \{0,1\}^n \to \{\pm 1\}$, distinguish whether they are sampled according to $\mathcal{D}$ or uniformly at random.*

Recall that we can write the multilinear expansion of a Boolean function $F : \mathbb{R}^{2N} \to \mathbb{R}$ as:

$$F(z) = \sum_{S \subseteq [2N]} \widehat{F}(S) \prod_{i \in S} z_i$$

Similar to the original proof, it is not hard to see that the randomized rounding step does not change the expected value of the outcome for multilinear functions:

$$\mathop{\mathbf{E}}_{z \sim \mathcal{G}'}[F(\mathrm{trnc}(z))] = \mathop{\mathbf{E}}_{z' \sim \mathcal{D}}[F(z')]$$

Hence we can ignore step 3 in our analysis. More importantly, because of the choice of $\varepsilon$, truncations happen with negligible probability, and in the event that they happen, it is possible to bound the difference.

$$\mathop{\mathbf{E}}_{z \sim \mathcal{G}'}[F(\mathrm{trnc}(z))] \approx \mathop{\mathbf{E}}_{z \sim \mathcal{G}'}[F(z)]$$

The rest of the analysis is to prove indistinguishability of $(X, Y^2 - \varepsilon)$ from the uniform distribution. More specifically, to use the tail bound from [Tal17] for the Fourier coefficients of bounded depth circuits to bound:

$$\left|\mathbf{E}[F(X, Y^2 - \varepsilon)] - \mathbf{E}[F(\mathcal{U}_{2N})]\right| = \left|\mathbf{E}[F(X, Y^2 - \varepsilon) - F(0,0)]\right|$$

The idea is to use the same telescopic sum as Raz and Tal for analyzing the expected value of $F$ and think of $\mathcal{G}'$ as a Brownian motion, but also consider the squared inputs and the $\varepsilon$ difference. One important step is to also break the $\varepsilon$ bias in the telescopic sum. Let $t \in \mathbb{N}$, and for $i \in [t]$, let $X^{(i)} = X^{(i-1)} + \Delta_X^{(i)}$ and $Y^{(i)} = H_N \cdot X^{(i)}$, where $\Delta_X^{(i)} \sim \mathcal{N}(0, \varepsilon/t)$. Now we can write:

$$F(X^{(t)}, (Y^{(t)})^2 - \varepsilon) - F(0,0) = \sum_{i=1}^{t} \left\{ F\left(X^{(i)}, (Y^{(i)})^2 - \tfrac{\varepsilon \cdot i}{t}\right) - F\left(X^{(i-1)}, (Y^{(i-1)})^2 - \tfrac{\varepsilon \cdot (i-1)}{t}\right) \right\}$$

Then we can use known bounds for each term in the sum and the triangle inequality to bound the sum. In the limit of $t \to \infty$, we are dealing with a stochastic integral so one can also prove this result using stochastic calculus. However, we decided not to present the proof using the language of stochastic calculus and instead picked $t$ to be a large enough polynomial in $N$ (similar to [RT19]).

## 4.1 Truncated Gaussians

It is not hard to see that any multilinear function $F : \mathbb{R}^{2N} \to \mathbb{R}$ still has similar expectation under $\mathcal{D}$ and $\mathcal{G}'$, where:

$$F(z) = \sum_{S \subseteq [2N]} \widehat{F}(S) \cdot \prod_{i \in S} z_i$$

First, we need to show that:

$$\mathop{\mathbf{E}}_{z' \sim \mathcal{D}} [F(z')] = \mathop{\mathbf{E}}_{z \sim \mathcal{G}'} [F(\mathrm{trnc}(z))]$$

And since we can still prove that the truncations happen with negligible probability, we only need to adapt the rest of the proof to work with squared Fourier coefficients. The proof of the first part works without any modifications from the definition of distributions $\mathcal{D}$ and $\mathcal{G}'$:

$$\begin{aligned} \mathbf{E}[F(z') \mid z] &= \mathbf{E}\left[ \sum_{S \subseteq [2N]} \widehat{F}(S) \cdot \prod_{i \in S} z'_i \,\middle|\, z \right] = \sum_{S \subseteq [2N]} \widehat{F}(S) \cdot \prod_{i \in S} \mathbf{E}[z'_i \mid z] \\ &= \sum_{S \subseteq [2N]} \widehat{F}(S) \cdot \prod_{i \in S} \mathrm{trnc}(z_i) = F(\mathrm{trnc}(z)) \end{aligned} \tag{2}$$

The next fact is stated as Claim 5.1 in [RT19], and is unaffected by our modification.

**Fact 24.** *Let $F : \mathbb{R}^{2N} \to \mathbb{R}$ be a multilinear function that maps $\{\pm 1\}^{2N}$ to $[-1, 1]$. Let $z = (z_1, \ldots, z_{2N}) \in \mathbb{R}^{2N}$. Then, $|F(z)| \leq \prod_{i=1}^{2N} \max(1, |z_i|)$.*

The next two theorems are equivalent to Claim 5.2 and Claim 5.3 of [RT19] respectively, where they are proven over distribution $\mathcal{G}$. One can verify that they also hold over distribution $\mathcal{G}'$. In fact, by choosing $\varepsilon$ to be small enough, they even hold over $\mathcal{G}'^{\mathrm{poly}(N)}$, where we are given oracle access to an exponentially long list of samples from $\mathcal{G}'$. This is crucial for extending this PH bound to the long list problem. We provide their proofs in Appendix A for completeness.

**Theorem 25.** *For any constant $c \geq 2$ there exists a choice of a constant $C$ in the definition of $\mathcal{G}'$ such that: $\mathbf{E}_{(x,y) \sim \mathcal{G}'} \left[ \prod_{i=1}^{N} \max(1, |x_i|) \cdot \prod_{i=1}^{N} \max(1, |y_i|) \cdot \mathbb{1}_{(x,y) \neq \mathrm{trnc}(x,y)} \right] \leq 4 \cdot N^{-c}$.*

**Theorem 26.** *For any constant $c \geq 2$ there exists a choice of a constant $C$ in the definition of $\mathcal{G}'$ such that the following holds. Let $0 \leq p, p_0$ such that $p + p_0 \leq 1$. Let $F : \mathbb{R}^{2N} \to \mathbb{R}$ be a multilinear function that maps $\{\pm 1\}^{2N}$ to $[-1, 1]$. Let $z_0 \in [-p_0, p_0]^{2N}$. Then,*

$$\mathop{\mathbf{E}}_{z \sim \mathcal{G}'} [|F(\mathrm{trnc}(z_0 + p \cdot z)) - F(z_0 + p \cdot z)|] \leq 8 \cdot N^{-c}$$

## 4.2 Quantum Algorithm for Distinguishing $\mathcal{D}$ and $U_{2N}$

Here, for completeness, we provide a quantum algorithm for distinguishing $U_{2N}$ and $\mathcal{D}$. Note that this quantum algorithm does not extend to solve Black-Box LLQSV, and does not contradict the LLQSV conjecture. As we will show, a problem similar to Black-Box LLQSV is harder than SquaredForrelation. However, we use these calculations in the next sections. Given to Boolean functions $f, g : \{\pm 1\}^N$ we use the following algorithm $A$ to distinguish between functions sampled from $\mathcal{D}$ and $U_{2N}$:

1. Apply Fourier transform on $f$ and sample $x$ from the distribution induced by $\widehat{f}$.
2. Accept if $g(x) = 1$, and reject otherwise.

We can see that the success probability of this algorithm is given by $\sum_{x, g(x)=1} \widehat{f}(x)^2 = \frac{1+\varphi(f,g)}{2}$, where $\varphi(f, g) = \varphi(X, Y)$ is defined as follows:

$$\varphi(X, Y) = \frac{1}{N} \sum_i (\sum_j H_{ij} X_i)^2 Y_i = \mathbf{Pr}[A \text{ Accepts}] - \mathbf{Pr}[A \text{ Rejects}]$$

We first analyze this quantity for when the samples are taken from $\mathcal{G}'$. In fact, we can show that the multilinear part of $\varphi(X,Y)$, denoted by $\varphi_{i\neq j}(X,Y)$ is large on average. Lastly, we can use Theorem 26 to show that a similar bound holds for samples from $\mathcal{D}$ while the quadratic part of $\varphi(X,Y)$ is 0 on average. To summarize, we show that:

$$\mathop{\mathbf{E}}_{(X,Y)\sim\mathcal{D}}[\varphi(X,Y)] = \mathop{\mathbf{E}}_{(X,Y)\sim\mathcal{D}}[\varphi_{i\neq j}(X,Y)] \approx \mathop{\mathbf{E}}_{(X,Y)\sim\mathcal{G}'}[\varphi_{i\neq j}(X,Y)] = O(\varepsilon^2)$$

**Theorem 27.** $\mathbf{E}_{(X,Y)\sim U_{2N}}[\varphi(X,Y)] = 0$.

*Proof.* For every $i,j,k \in [N]$, $\mathbf{E}_{(X,Y)\sim U_{2N}}[X_jX_kY_i] = 0$ because $Y_i$ is independent of $X$ and has mean 0. By linearity of expectation $\mathbf{E}_{(X,Y)\sim U_{2N}}[\varphi(X,Y)] = 0$. □

**Theorem 28.** $\mathbf{E}_{(X,Y')\sim\mathcal{G}'}[\varphi_{i\neq j}(X,Y')] = \varepsilon^2\cdot(2-2/N)$.

*Proof.* By the definition of $\mathcal{G}'$ and $\varphi_{i\neq j}(X,Y')$ we can write:

$$\begin{aligned}
\mathop{\mathbf{E}}_{(X,Y')\sim\mathcal{G}'}[\varphi_{i\neq j}(X,Y')] &= \frac{1}{N}\sum_i\sum_{j\neq k} H_{ij}H_{ik}\,\mathbf{E}[X_jX_kY_i'] \\
&= \frac{1}{N}\sum_i\sum_{j\neq k} H_{ij}H_{ik}\,\mathbf{E}[X_jX_kY_i^2] - \varepsilon\,\mathbf{E}[X_jX_k] \\
&= \frac{1}{N}\sum_i\sum_{j\neq k} H_{ij}H_{ik}(\sigma'_{ii}\sigma'_{jk} + 2\sigma_{ij}\sigma_{ik}) \\
&= \frac{1}{N}\sum_i\sum_{j\neq k} H_{ij}^2H_{ik}^2 2\varepsilon^2 = \frac{2(N-1)}{N}\varepsilon^2
\end{aligned}$$

The third line follows from the fact that $(X,Y)$ is a multivariate normal distribution, and the last inequality holds for $N \geq 2$. Furthermore, $\sigma'_{ij}$ is the covariance of $(X_i,X_j)$ and $(Y_i,Y_j)$, and $\sigma_{ij}$ is the covariance of $(Y_i,X_j)$. □

**Theorem 29.** $\mathbf{E}_{(X,Y)\sim\mathcal{D}}[\varphi(X,Y)] \geq \varepsilon^2$.

*Proof.* Since $\mathbf{E}[Y_i] = 0$, by linearity of expectation we can write:

$$\begin{aligned}
\mathop{\mathbf{E}}_{(X,Y)\sim\mathcal{D}}[\varphi(X,Y)] &= \frac{1}{N}\sum_i\sum_{j\neq k} H_{ij}H_{ik}\,\mathbf{E}[X_jX_kY_i] + \frac{1}{N}\sum_i\sum_j H_{ij}^2\,\mathbf{E}[X_j^2Y_i] \\
&= \frac{1}{N}\sum_i\sum_{j\neq k} H_{ij}H_{ik}\,\mathbf{E}[X_jX_kY_i] + \frac{1}{N}\sum_i\sum_j H_{ij}^2\,\mathbf{E}[Y_i] \\
&= \mathop{\mathbf{E}}_{(X,Y)\sim\mathcal{D}}[\varphi_{i\neq j}(X,Y)]
\end{aligned}$$

Note that $\varphi_{i\neq j}(X,Y)$ is a multilinear function that takes $\{\pm1\}^{2N}$ to $[-2,2]$ since the subtracted quadratic part maps $\{\pm\}^{2N}$ to $[-1,1]$ and $\varphi(X,Y) \in [-1,1]$. So we can use Theorem 26 with $p_0 = 0, p = 1$ and Equation 2 to write:

$$\left|\mathop{\mathbf{E}}_{(X,Y)\sim\mathcal{D}}[\varphi_{i\neq j}(X,Y)] - \mathop{\mathbf{E}}_{(X,Y)\sim\mathcal{G}'}[\varphi_{i\neq j}(X,Y)]\right| \leq 16\cdot N^{-2}$$

Then we can get a lower bound on $\mathbf{E}_{(X,Y)\sim\mathcal{D}}[\varphi(X,Y)]$:

$$\mathop{\mathbf{E}}_{(X,Y)\sim\mathcal{D}}[\varphi_{i\neq j}(X,Y)] \geq \mathop{\mathbf{E}}_{(X,Y)\sim\mathcal{G}'}[\varphi_{i\neq j}(X,Y)] - 16\cdot N^{-2} \geq \varepsilon^2$$ □

## 4.3 Classical Hardness

Let $L_{1,2}(F) = \sum_{S\subseteq[2N],|S|=2} |\widehat{F}(S)|$. The results in this section combined with the tail bound from [Tal17], suffices to prove a lower bound on the size of any $\mathsf{AC}^0$ circuit that distinguishes $\mathcal{D}$ from uniform.

**Theorem 30** ([CHLT19, Claim A.5])**.** *Let $f$ be a multi-linear function on $\mathbb{R}^N$ and $x \in [-1/2, 1/2]^N$. There exists a distribution over random restrictions $\mathcal{R}_x$ such that for any $y \in \mathbb{R}^N$:*

$$f(x+y) - f(x) = \mathop{\mathbf{E}}_{\rho\sim\mathcal{R}_x}[f_\rho(2\cdot y) - f_\rho(0)]$$

**Theorem 31.** *Let $t = N^{c-1}$ for a sufficiently large universal constant $c$ (e.g., $c = 40$). Let $(X, Y) \in [-1/2, 1/2]^{2N}$, $\Delta X \sim \mathcal{N}(0, \varepsilon/t)$ and $\Delta Y = H \cdot \Delta X$. Let $F : \mathbb{R}^{2N} \to \mathbb{R}$ be a multilinear function where for all random restrictions $L_{1,2}(F_\rho) \le \ell$:*

$$(*) = \left| \mathop{\mathbf{E}}_{\Delta X}\left[F\big(X + \Delta X, (Y+\Delta Y)^2 - \tfrac{i\cdot\varepsilon}{t}\big)\right] - \mathbf{E}\left[F\big(X, Y^2 - \tfrac{(i-1)\cdot\varepsilon}{t}\big)\right]\right| \le \frac{O(\varepsilon\cdot\ell)}{t\sqrt{N}}$$

*Proof.* Let $Y' = Y^2 - \frac{\varepsilon\cdot(i-1)}{t}$. We can rewrite $(*)$ as follows:

$$(*) = \mathop{\mathbf{E}}_{\Delta X}\left[F(X+\Delta X, Y' + 2Y\cdot\Delta Y + \Delta Y^2 - \tfrac{\varepsilon}{t}) - F(X, Y')\right]$$

Note that $Y' \in [-1/2, 1/2]^N$. Using Theorem 30 we can write this value using random restrictions of $F$:

$$(*) = \mathop{\mathbf{E}}_{\Delta X,\rho}\left[F_\rho\big(2\cdot\Delta X, 2\cdot\Delta Y'\big) - F_\rho(0,0)\right]$$

Where $\Delta Y' = 2Y\cdot\Delta Y + \Delta Y^2 - \frac{\varepsilon}{t}$. Let $Z = (2\Delta X, 2\Delta Y')$. Next we can expand $(*)$ in terms of multilinear expansion of $F_\rho$. From the Isserlis' theorem [Iss18] we can see that monomials of degree $k > 2$ in the variables $Z$ scale like $O(\frac{k^k}{t^{k/2}})$, and there are at most $N^k$ such monomials. Since we can choose $t$ to be an arbitrarily large power of $N$, their contribution would be negligible, i.e., $o(\varepsilon/t\sqrt{N})$. Furthermore, since for every input variable $X_i$ of $F_\rho$, $\mathbf{E}[Z_i] = 0$ (using the fact that $\mathbf{E}[\Delta Y^2 - \frac{\varepsilon}{t}] = 0$) we can also ignore monomials of degree 1. Note that this is precisely why we also break $\varepsilon$ in the telescopic sum. The remaining step is to bound monomials of degree 2.

To account for monomials of degree 2, we upper bound the covariances of all pairs of variables from $Z = (2\Delta X, 2\Delta Y')$ by $O(\frac{\varepsilon}{t\sqrt{N}})$. First, for $i \ne j$ we have that $(\Delta X)_i$ and $(\Delta X)_j$ are independent and thus have covariance 0. Second, we bound $\left|\mathbf{Cov}\left(2\left(\Delta X\right)_i, 2\left(\Delta Y'\right)_j\right)\right|$ for any $(i,j)$ by:

$$|4\cdot 2Y_j\,\mathbf{Cov}((\Delta X)_i, (\Delta Y)_j) + 4\cdot\mathbf{Cov}((\Delta X)_i, (\Delta Y)_j^2)| \le \frac{4\varepsilon}{t\sqrt{N}} + O\left(\tfrac{1}{t^{3/2}}\right) = O\left(\frac{\varepsilon}{t\sqrt{N}}\right)$$

Similarly, we can bound $|\mathbf{Cov}\left(2(\Delta Y')_i, 2(\Delta Y')_j\right)|$ for $i \ne j$

$$4\cdot 4Y_iY_j\,\mathbf{Cov}\left((\Delta Y)_i, (\Delta Y)_j\right) + O\left(\frac{1}{t^{3/2}}\right) \le O\left(\frac{\varepsilon}{t\sqrt{N}}\right)$$

Finally, we can bound $(*)$:

$$\begin{aligned}
\left|\mathop{\mathbf{E}}_{\Delta X,\rho}[F_\rho(Z) - F_\rho(0^{2N})]\right| &\le \sum_{i,j}\left|\mathop{\mathbf{E}}_{\Delta X,\rho}[\widehat{F_\rho}(\{i,j\})\cdot Z_iZ_j]\right| + o\left(\tfrac{\varepsilon\ell}{t\sqrt{N}}\right)\\
&\le \max_{i,j}|\mathbf{Cov}(Z_i,Z_j)|\cdot\max_\rho\sum_{\substack{S\subseteq[2N],\\|S|=2}}|\widehat{F_\rho}(S)| + o\left(\tfrac{\varepsilon\ell}{t\sqrt{N}}\right)\\
&\le O\left(\frac{\varepsilon\ell}{t\sqrt{N}}\right).
\end{aligned}$$

□

**Theorem 32.** *Let $\ell \geq 1$. Let $F : \{\pm 1\}^{2N} \to \{\pm 1\}$ be a multilinear function with bounded spectral norm $L_{1,2}(F) \leq \ell$. Then:*

$$(*) = \mathop{\mathbf{E}}_{(X,Y')\sim\mathcal{D}} \Big[F(X,Y') - F(0,0)\Big] \leq O\left(\frac{\varepsilon \cdot \ell}{\sqrt{N}}\right)$$

*Proof.* From Equation 2, it suffices to show:

$$\mathop{\mathbf{E}}_{(X,Y)\sim\mathcal{G}} \Big[F\big(\operatorname{trnc}(X), \operatorname{trnc}(Y^2 - \varepsilon)\big) - F(0,0)\Big] \leq O\left(\frac{\varepsilon \cdot \ell}{\sqrt{N}}\right)$$

We start by writing this value as a telescoping sum. Let $t = N^{c-1}$ for $c$ the constant guaranteed by Theorem 31. Set $C$ in the definition of $\varepsilon$ to guarantee that the error in Theorem 26 is at most $8 \cdot N^{-c}$ and that $e^{-1/(8\varepsilon)} \leq N^{-(c+1)}$. Then we can write:

$$(*) = \sum_{i=1}^{t} \mathbf{E}\left[F(\operatorname{trnc}(X^{(i)}), \operatorname{trnc}(Y^{(i)^2} - \tfrac{\varepsilon\cdot i}{t})) - F(\operatorname{trnc}(X^{(i-1)}), \operatorname{trnc}(Y^{(i-1)^2} - \tfrac{\varepsilon\cdot(i-1)}{t}))\right]$$

where $X^{(i)} = X^{(i-1)} + \Delta X$, $Y^{(i)} = Y^{(i-1)} + \Delta Y$ and $\Delta X \sim \mathcal{N}(0, \varepsilon/t)$ and $\Delta Y = H \cdot \Delta X$. We are going to use Theorem 8 to bound each term in the sum to get the final result. Let $E_{i-1}$ be the event that $(X^{(i-1)}, Y^{(i-1)} - \frac{\varepsilon\cdot(i-1)}{t}) \in [-1/2, 1/2]^{2N}$. We can prove that $E_{i-1}$ happens with high probability:

$$\mathbf{Pr}[(X^{(i-1)}, Y^{(i-1)}) \notin [-1/2, 1/2]^{(2N)}] \leq 2N \cdot \mathbf{Pr}[|\mathcal{N}(0,\varepsilon)| \geq 1/2] \leq 2N \cdot 2e^{-1/(8\varepsilon)} \leq 4N^{-c}$$

It is also clear that if $(X^{(i-1)}, Y^{(i-1)}) \in [-1/2, 1/2]^{2N}$ then $(X^{(i-1)}, Y^{(i-1)^2} - \frac{\varepsilon\cdot(i-1)}{t}) \in [-1/2, 1/2]^{2N}$. So $\mathbf{Pr}[E_{i-1}] \geq 1 - 4N^{-c}$. Next, we just have to use Theorems 26 and 31 combined with triangle inequality to prove the desired claim. We can bound the $i$-th term in the sum, $S_i$, by:

$$\begin{aligned} S_i \leq\ & \mathbf{E}\left[F(X^{(i)}, Y^{(i)^2} - \tfrac{\varepsilon\cdot i}{t}) - F(X^{(i-1)}, Y^{(i-1)^2} - \tfrac{\varepsilon\cdot(i-1)}{t})\middle| E_{i-1}\right] \\ & + \mathbf{E}\left[F(\operatorname{trnc}(X^{(i)}), \operatorname{trnc}(Y^{(i)^2} - \tfrac{\varepsilon\cdot i}{t})) - F(X^{(i)}, Y^{(i)^2} - \tfrac{\varepsilon\cdot i}{t})\middle| E_{i-1}\right] \\ & + 2\,\mathbf{Pr}[\neg E_{i-1}] \leq O\left(\frac{\varepsilon \cdot \ell}{t\sqrt{N}}\right) + O(N^{-c}) \end{aligned}$$

So we can bound the sum $(*) \leq O(\frac{\varepsilon\cdot\ell}{\sqrt{N}}) + O(tN^{-c}) \leq O(\frac{\varepsilon\cdot\ell}{\sqrt{N}})$. □

**Remark 33.** *Note that this proof can easily be extended to the "long list" version of the problem, where we are given oracle access to a list of pairs of functions $(f_i, g_i)$ rather than a single pair that has been shown. We have already shown this for Theorem 25 and 26 in Appendix A, which directly proves Theorem 31. The only remaining step that we need to verify in Theorem 32 is the probability of the event $E_i$. Similar to what has been shown in Appendix A, we can choose $\varepsilon$ to be small enough so that $p(N) \cdot e^{-1/(8\varepsilon)}$ remains exponentially small, and the rest of the proof follows immediately. Later we will use this result to give evidence for* LLQSV.

## 4.4 More details on the relation between SquaredForrelation and Long List

As mentioned before, our goal is to use samples $(f, g) \sim \mathcal{D}$, and then use $g$ to get samples according to the Fourier spectrum. However, if we choose a uniformly random sample such that $g(x) = 1$, we would not get a sample *exactly* according to the Fourier distribution of $f$. Intuitively, this is a "flattened version" of the Fourier transform distribution of $f$, but we can still prove a PH lower bound for this variant of Black-Box LLQSV, where the samples are taken according to this flattened distribution. We show that this distinction does not matter, by first noting that we can define a modified HOG score – Rejection Sampling HOG (RHOG) – so that RHOG and the flattened distribution have the same

relation as HOG and Black-Box LLQSV. Furthermore, we prove that a quantum algorithm can still solve both HOG and RHOG by sampling according to the Fourier transform distribution of $f$. Let $\mathcal{D}$ be the distribution defined in the previous section, and let $\mathcal{D}_f$ be the marginal distribution over $g$ for a fixed $f$. Given a random Boolean function $f$, $\mathcal{R}_f$ samples $s \in \{0,1\}^n$ as follows:

- Sample $g \sim \mathcal{D}_f$.
- Sample $x \in \{0,1\}^n$ uniformly at random and output $x$ if $g(x) = 1$.
- Output a random element after $4n^2$ unsuccessful attempts.

Suppose we are given access to oracle $\mathcal{O}$ which is a long (exponentially large) list of random Boolean functions $f_1, f_2, \ldots, f_T : \{\pm 1\}^n \to \{0,1\}$ paired with strings $s_1, s_2, \ldots, s_T$. Here we define Black-Box LLQSV to be the problem of distinguishing samples from $\mathcal{R}_f$ from uniform. One can hope that since $g$ is correlated with squared Fourier coefficients of $f$, these samples are also close to the "Fourier distribution". In fact, we later show that on average (over the random Boolean function and the samples), $\mathcal{R}_f$ generates heavy Fourier coefficients. The same argument also works to prove that an honest quantum sampler, that samples according to the Fourier coefficients, passes the following score:

**Problem 34.** (RHOG) *Let $b = 1 + \mathrm{poly}(1/n)$. Given a random Boolean function $f : \{0,1\}^N \to \{\pm 1\}$, output an outcome $s \in \{0,1\}^N$ such that:*

$$\mathop{\mathbf{E}}_{f,s}\left[\mathbf{Pr}\left[\mathcal{R}_f \text{ samples } s\right]\right] \geq \frac{b}{N}$$

One can easily verify that the existence of a deterministic quantum algorithm for solving RHOG also gives a QCAM algorithm for (modified) Black-Box LLQSV. This follows from a collision finding algorithm similar to the original LLQSV argument (see Appendix B). Here we prove that first, the usual quantum algorithm that samples according to the Fourier distribution passes solves RHOG. Next, we show that SquaredForrelation can be reduced to Black-Box LLQSV, which implies that Black-Box LLQSV is not in PH.

We prove the first result by using two properties of the distribution $\mathcal{G}'$. The first directly follows from a tail bound of Chi-square variables:

**Lemma 35** ([LM00])**.** *Let $(Y_1, \ldots, Y_N) \sim \mathcal{N}(0,1)$ and let $a_1, \ldots, a_N \geq 0$. Let*

$$Z = \sum_i a_i (Y_i^2 - 1)$$

*Then for any $\Delta > 0$ we have:*

- $\mathbf{Pr}\left[Z \geq 2|a|_2\sqrt{\Delta} + 2|a|_\infty \Delta\right] \leq \exp(-\Delta)$
- $\mathbf{Pr}\left[Z \leq -2|a|_2\sqrt{\Delta}\right] \leq \exp(-\Delta)$

**Theorem 36.** *Let $(X,Y) \sim \mathcal{G}'$, then $\mathbf{Pr}\left[\left|\sum_i Y_i\right| \geq 3\sqrt{N}\right] \leq 2\exp(-1/\varepsilon)$.*

*Proof.* Using Lemma 35 by letting $a = (\varepsilon, \ldots, \varepsilon)$ and $\Delta = \frac{1}{\varepsilon}$ we get:

- $\mathbf{Pr}\left[Z \geq 2\sqrt{N} + 2\right] \leq \exp(-\frac{1}{\varepsilon})$
- $\mathbf{Pr}\left[Z \leq -2\sqrt{N}\right] \leq \exp(-\frac{1}{\varepsilon})$

And a union bound gives us the claim. □

Recall that for $(X,Y) \in \mathcal{G}'$ with high probability we have $\mathrm{trnc}(X,Y) = (X,Y)$:

**Theorem 37.** *Let $(X,Y) \sim \mathcal{G}'$, then $\mathbf{Pr}\left[\mathrm{trnc}(X,Y) \neq (X,Y)\right] \leq 2N^{-2}$.*

**Corollary 38.** *Let $(X,Y) \sim \mathcal{D}$ and $\delta = N^{-1/3}$, then with probability at least $1 - 5N^{-2}$ we have:*

$$(1-\delta)\frac{N}{2} \leq \left|\{i|Y_i = 1\}\right| \leq (1+\delta)\frac{N}{2}$$

*Proof.* This follows from a Chernoff bound applied to Theorem 36 and 37. Given $(X',Y') \sim \mathcal{G}'$, by a union bound we get that the probability that both requirements $\mathrm{trnc}(X',Y') = (X',Y')$ and $|\sum Y_i'| < 3\sqrt{N}$ are satisfied is at least $1 - 4N^{-2}$. In such a case, recall that $Y$ is attained from $Y'$ by randomized rounding (without truncations since $Y' = \mathrm{trnc}(Y')$. Let $\delta' = \delta/2$. Then by Chernoff bound, with probability $1 - \exp(\Omega(\delta^2 N)) \geq 1 - N^{-2}$:

$$|\{i|Y_i = 1\}| \leq (1+\delta')\left(\frac{N}{2} + 3\sqrt{N}\right) \leq (1+\delta)\frac{N}{2}$$

and,

$$|\{i|Y_i = 1\}| \geq (1-\delta')\left(\frac{N}{2} - 3\sqrt{N}\right) \geq (1-\delta)\frac{N}{2}$$

for large enough $N$. This means that the claim holds over $\mathcal{D}$ with probability at least $1 - 5N^{-2}$. □

Another direct consequence of this property is that we can bound the success probability of getting a non-uniform sample after $4n^2$ steps in rejection sampling. Note that the probability of the rejection sampling failing is bounded by $\left((1+\delta)/2\right)^{4n^2}$. For large enough $N$ and $\delta = 1/N^{1/3}$, we know $((1+\delta)/2)^2 \leq 1/2$, and thus

$$((1+\delta)/2)^{4n^2} \leq 2^{-2n^2} \ll N^{-2}$$

Now we can prove that given random Boolean function $f : \{\pm 1\}^N \to \{0,1\}$, sampling according to the Fourier coefficients of $f$ solves RHOG. Define $\mathcal{C}_f$ to be the Fourier transform distribution over outcomes according to $f$, i.e., $\mathcal{C}_f$ samples $x$ with probability $\widehat{f}(x)^2$.

**Claim 39.**

$$\mathop{\mathbf{E}}_{\substack{f,\\ x\sim\mathcal{C}_f}}\left[\mathbf{Pr}\left[\mathcal{R}_f \text{ samples } x\right]\right] \geq \frac{1+\mathrm{poly}(\varepsilon)}{N}$$

*Proof.* From Theorem 29, we know that $\mathbf{E}_{\mathcal{D}}\left[\sum_{g(x)=1}\widehat{f}(x)^2\right] \geq \frac{1}{2} + \frac{\varepsilon^2}{4}$. Let $E$ be the event that :

1. $(1-\delta)\frac{N}{2} \leq \left|\{i|Y_i = 1\}\right| \leq (1+\delta)\frac{N}{2}$
2. The rejection sampling algorithm outputs an $s$ such that $g(s) = 1$.

where $\delta = N^{-1/3}$. We know that $\mathbf{Pr}[E] \geq 1 - 10/N^2$ and $\mathbf{E}_{\mathcal{D}}\left[\sum_{g(x)=1}\widehat{f}(x)^2 | E\right] \geq \frac{1}{2} + \frac{\varepsilon^2}{8}$. We can lower bound

$$\mathop{\mathbf{E}}_{\substack{f,\\ x\sim\mathcal{C}_f}}\left[\mathbf{Pr}\left[\mathcal{R}_f \text{ samples } x\right]\right] \geq \mathbf{Pr}[E] \cdot \mathop{\mathbf{Pr}}_{\substack{f,\\ x\sim\mathcal{C}_f}}\left[\mathcal{R}_f \text{ samples } x | E\right].$$

Note further that conditioned on $E$, the rejection sampling algorithm draws a random element from the set $\{y : g(y) = 1\}$. Thus we may rewrite

$$\begin{aligned}
\mathbf{Pr}[E] \cdot \mathop{\mathbf{Pr}}_{\substack{f,\\ x\sim\mathcal{C}_f}}\left[\mathcal{R}_f \text{ samples } x | E\right] &= \mathbf{Pr}[E] \cdot \mathop{\mathbf{E}}_{(f,g)\sim\mathcal{D}}\left[\frac{\sum_{g(x)=1}\widehat{f}(x)^2}{|\{y : g(y) = 1\}|} \;\middle|\; E\right] \\
&\geq \mathbf{Pr}[E] \cdot \frac{1/2 + \varepsilon^2/8}{(1+\delta)N/2} \\
&\geq \mathbf{Pr}[E] \cdot \frac{(1-\delta)(1+\varepsilon^2/4)}{N}
\end{aligned}$$

which is at least $\frac{1+\varepsilon^2/8}{N}$ for $N$ large enough (where we used the fact that $\varepsilon = \Theta(1/\log N)$ is much larger than $10/N^2$ and $\delta$). □

The only remaining step is to prove the hardness of (modified) Black-Box LLQSV. First, we define the following problem:

**Problem 40.** *Given oracle access to a length $T = 2^{3n}$ list of triplets $(f_i, g_i, s_i)$ where $f_i, g_i : \{\pm 1\}^N \to \{0,1\}$ and $s_i \in \{0,1\}^N$ is sampled according to the rejection sampling algorithm applied to $g_i$ distinguish between the following two cases:*

1. *For every $i$, $f_i, g_i$ are chosen uniformly at random.*
2. *For every $i$. $f_i, g_i$ are sampled according to $\mathcal{D}$.*

We can use this to prove our final result:

**Theorem 41.** *No constant depth Boolean circuit of size* quasipoly$(N)$ *can solve Black-Box* LLQSV *with advantage more than* polylog$(N)/\sqrt{N}$.

*Proof.* First, it is clear that we can reduce Problem 40 to Black-Box LLQSV since we have access to the list $(f_i, s_i)$. To prove the same oracle separation result using Problem 40, we first notice that we can prove the same $\mathsf{AC}^0$ lower bound if we only had access to $(f_i, g_i)$, but not $s_i$ (Remark 33). Furthermore, by choosing $\varepsilon$ in the definition of $\mathcal{D}$ small enough, the lower bound even holds for a list of length $2 \cdot 2^{n^3}$. The final step is to prove that $s_i$'s do not give us extra computation power. Suppose there exists a circuit $C$ of size $s$ and depth $d$ for Problem 40, we can convert this circuit to work without having access to $s_i$. First, we can replace $s_i$ with a small circuit that given $r_i \in \{0,1\}^{\text{poly}(n)}$, the random seed of the rejection sampling, simulate rejection sampling, making $O(n^2)$ queries to $g_i$ and outputs $s_i$. Such a computation can be described by a decision tree on that reads $r_i$ and at most $O(n^2)$ entries of $g_i$, and thus also by a DNF of size $2^{\text{poly}(n)} = \text{quasipoly}(N)$. Making all these replacements everywhere gives a new circuit with size $s' = s \cdot \text{quasipoly}(N)$ (which is still quasi-polynomial in $N$) and depth $d+2$. Furthermore, if we have access to a list of length $2 \cdot 2^{n^3}$ of pairs of functions, we can use the second half as the random seed, instead of accessing $r_i$ directly. So this new circuit of size $s'$ and depth $d+2$ must also distinguish the two distributions with the same advantage, having only access to a list of length $2 \cdot 2^{n^3}$ of $(f_i, g_i)$. Thus, the same lower bound applies to the size of the starting circuit $s$. □

## Acknowledgements

We thank Scott Aaronson and Umesh Vazirani for helpful discussions. A.B. was supported in part by the AFOSR under grant FA9550-21-1-0392. B.F. and R.B. acknowledge support from AFOSR (YIP number FA9550-18-1-0148 and FA9550-21-1-0008). This material is based upon work partially supported by the National Science Foundation under Grant CCF-2044923 (CAREER) and by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers (Q-NEXT) as well as by DOE QuantISED grant DE-SC0020360. A.T. was supported in part by the National Science Foundation under Grant CCF-2145474 (CAREER) and by a Sloan Research Fellowship.

## References

[AA13] S. Aaronson and A. Arkhipov. The computational complexity of linear optics. *Theory Comput.*, 9:143–252, 2013. doi:10.4086/toc.2013.v009a004.

[AA14a] S. Aaronson and A. Ambainis. The need for structure in quantum speedups. *Theory Comput.*, 10:133–166, 2014. doi:10.4086/TOC.2014.V010A006.

[AA14b] S. Aaronson and A. Arkhipov. Bosonsampling is far from uniform. *Quantum Inf. Comput.*, 14(15-16):1383–1423, 2014. doi:10.26421/QIC14.15-16-7.

[AA18] S. Aaronson and A. Ambainis. Forrelation: A problem that optimally separates quantum from classical computing. *SIAM J. Comput.*, 47(3):982–1038, 2018. doi:10.1137/15M1050902.

[AAB+19] F. Arute, K. Arya, R. Babbush, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019. doi:10.1038/s41586-019-1666-5.

[Aar10] S. Aaronson. BQP and the polynomial hierarchy. In L. J. Schulman, editor, *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010*, pages 141–150. ACM, 2010. doi:10.1145/1806689.1806711.

[Aar18a] S. Aaronson. Certified randomness from quantum supremacy. *Talk at CRYPTO 2018*, October 2018.

[Aar18b] S. Aaronson. Quantum supremacy and its applications. *Talk at the Simons Institute for the Theory of Computing*, June 2018.

[Aar20] S. Aaronson. On entropy from random circuit sampling. *Talk at the Simons Institute for the Theory of Computing*, May 2020.

[AC17] S. Aaronson and L. Chen. Complexity-theoretic foundations of quantum supremacy experiments. In R. O'Donnell, editor, *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, volume 79 of *LIPIcs*, pages 22:1–22:67. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017. doi:10.4230/LIPIcs.CCC.2017.22.

[AG20] S. Aaronson and S. Gunn. On the classical hardness of spoofing linear cross-entropy benchmarking. *Theory Comput.*, 16:1–8, 2020. doi:10.4086/TOC.2020.V016A011.

[AH23] S. Aaronson and S. Hung. Certified randomness from quantum supremacy. In B. Saha and R. A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 933–944. ACM, 2023. doi:10.1145/3564246.3585145.

[AM16] A. Acín and L. Masanes. Certified randomness in quantum physics. *Nature*, 540(7632):213–219, 2016. doi:10.1038/nature20119.

[BBBV97] C. H. Bennett, E. Bernstein, G. Brassard, and U. V. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997. doi:10.1137/S0097539796300933.

[BCMVV21] Z. Brakerski, P. F. Christiano, U. Mahadev, U. V. Vazirani, and T. Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *J. ACM*, 68(5):31:1–31:47, 2021. doi:10.1145/3441309.

[BFLL21] A. Bouland, B. Fefferman, Z. Landau, and Y. Liu. Noise and the frontier of quantum supremacy. In *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*, pages 1308–1317. IEEE, 2021. doi:10.1109/FOCS52979.2021.00127.

[BFNV19] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani. On the complexity and verification of quantum random circuit sampling. *Nature Physics*, 15(2):159–163, 2019. doi:10.1038/s41567-018-0318-2.

[BHZ87] R. B. Boppana, J. Håstad, and S. Zachos. Does co-NP have short interactive proofs? *Inf. Process. Lett.*, 25(2):127–132, 1987. doi:10.1016/0020-0190(87)90232-8.

[BIS+18] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, et al. Characterizing quantum supremacy in near-term devices. *Nature Physics*, 14(6):595–600, 2018. doi:10.1038/s41567-018-0124-x.

[BJS10] M. J. Bremner, R. Jozsa, and D. J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 467:459–472, 2010. doi:10.1098/rspa.2010.0301.

[BKVV20] Z. Brakerski, V. Koppula, U. V. Vazirani, and T. Vidick. Simpler proofs of quantumness. In S. T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2020, Riga, Latvia, June 9-12, 2020*, volume 158 of *LIPIcs*, pages 8:1–8:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPICS.TQC.2020.8.

[BMS16] M. J. Bremner, A. Montanaro, and D. J. Shepherd. Average-case complexity versus approximate simulation of commuting quantum computations. *Phys. Rev. Lett.*, 117(8):080501, 2016. doi:10.1103/PhysRevLett.117.080501.

[BV97] E. Bernstein and U. V. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26(5):1411–1473, 1997. doi:10.1137/S0097539796300921.

[CCY20] N. Chia, K. Chung, and T. Yamakawa. Classical verification of quantum computations with efficient verifier. In R. Pass and K. Pietrzak, editors, *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part III*, volume 12552 of *Lecture Notes in Computer Science*, pages 181–206. Springer, 2020. doi:10.1007/978-3-030-64381-2_7.

[CHHL19] E. Chattopadhyay, P. Hatami, K. Hosseini, and S. Lovett. Pseudorandom generators from polarizing random walks. *Theory Comput.*, 15:1–26, 2019. doi:10.4086/toc.2019.v015a010.

[CHLT19] E. Chattopadhyay, P. Hatami, S. Lovett, and A. Tal. Pseudorandom generators from the second fourier level and applications to AC0 with parity gates. In A. Blum, editor, *10th Innovations in Theoretical Computer Science Conference, ITCS 2019, January 10-12, 2019, San Diego, California, USA*, volume 124 of *LIPIcs*, pages 22:1–22:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. doi:10.4230/LIPIcs.ITCS.2019.22.

[CSV21] M. Coudron, J. Stark, and T. Vidick. Trading locality for time: Certifiable randomness from low-depth circuits. *Communications in Mathematical Physics*, 382(1):49–86, Feb. 2021. doi:10.1007/s00220-021-03963-w.

[FSUV13] B. Fefferman, R. Shaltiel, C. Umans, and E. Viola. On beating the hybrid argument. *Theory Comput.*, 9:809–843, 2013. doi:10.4086/toc.2013.v009a026.

[FU16] B. Fefferman and C. Umans. On the power of quantum fourier sampling. In A. Broadbent, editor, *11th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2016, Berlin, Germany, September 27-29, 2016*, volume 61 of *LIPIcs*, pages 1:1–1:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016. doi:10.4230/LIPICS.TQC.2016.1.

[GG11] E. Gat and S. Goldwasser. Probabilistic search algorithms with unique answers and their cryptographic applications. *Electron. Colloquium Comput. Complex.*, page 136, 2011. URL `https://eccc.weizmann.ac.il/report/2011/136`.

[GGR13] O. Goldreich, S. Goldwasser, and D. Ron. On the possibilities and limitations of pseudodeterministic algorithms. In R. D. Kleinberg, editor, *Innovations in Theoretical Computer Science, ITCS '13, Berkeley, CA, USA, January 9-12, 2013*, pages 127–138. ACM, 2013. doi:10.1145/2422436.2422453.

[GIPS21] S. Goldwasser, R. Impagliazzo, T. Pitassi, and R. Santhanam. On the pseudodeterministic query complexity of NP search problems. In V. Kabanets, editor, *36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference)*, volume 200 of *LIPIcs*, pages 36:1–36:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.CCC.2021.36.

[GKC+24] X. Gao, M. Kalinowski, C.-N. Chou, et al. Limitations of linear cross-entropy as a measure for quantum advantage. *PRX Quantum*, 5:010334, Feb 2024. doi:10.1103/PRXQuantum.5.010334.

[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219, 1996. doi:10.1145/237814.237866.

[GUV09] V. Guruswami, C. Umans, and S. P. Vadhan. Unbalanced expanders and randomness extractors from parvaresh-vardy codes. *J. ACM*, 56(4):20:1–20:34, 2009. doi:10.1145/1538902.1538904.

[Hås86] J. Håstad. *Computational limitations for small depth circuits*. PhD thesis, Massachusetts Institute of Technology, 1986.

[HG21] S. Hirahara and F. L. Gall. Test of quantumness with small-depth quantum circuits. In F. Bonchi and S. J. Puglisi, editors, *46th International Symposium on Mathematical Foundations of Computer Science, MFCS 2021, August 23-27, 2021, Tallinn, Estonia*, volume 202 of *LIPIcs*, pages 59:1–59:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.MFCS.2021.59.

[HKEG19] D. Hangleiter, M. Kliesch, J. Eisert, and C. Gogolin. Sample complexity of device-independently certified "quantum supremacy". *Physical Review Letters*, 122(21), May 2019. doi:10.1103/physrevlett.122.210502.

[Iss18] L. Isserlis. On a formula for the product-moment coefficient of any order of a normal frequency distribution in any number of variables. *Biometrika*, 12(1/2):134–139, 1918. doi:10.2307/2331932.

[KCVY21] G. D. Kahanamoku-Meyer, S. Choi, U. V. Vazirani, and N. Y. Yao. Classically-verifiable quantum advantage from a computational bell test. *CoRR*, abs/2104.00687, 2021. arXiv:2104.00687, doi:10.1038/s41567-022-01643-7.

[KGN19] H. Kobayashi, F. L. Gall, and H. Nishimura. Generalized quantum arthur-merlin games. *SIAM J. Comput.*, 48(3):865–902, 2019. doi:10.1137/17M1160173.

[KMM21] Y. Kondo, R. Mori, and R. Movassagh. Quantum supremacy and hardness of estimating output probabilities of quantum circuits. In *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*, pages 1296–1307. IEEE, 2021. doi:10.1109/FOCS52979.2021.00126.

[Kro22] H. Krovi. Average-case hardness of estimating probabilities of random quantum circuits with a linear scaling in the error exponent. *CoRR*, abs/2206.05642, 2022. arXiv:2206.05642, doi:10.48550/ARXIV.2206.05642.

[LG22] Z. Liu and A. Gheorghiu. Depth-efficient proofs of quantumness. *Quantum*, 6:807, Sept. 2022. doi:10.22331/q-2022-09-19-807.

[LM00] B. Laurent and P. Massart. Adaptive estimation of a quadratic functional by model selection. *The Annals of Statistics*, 28(5):1302 – 1338, 2000. doi:10.1214/aos/1015957395.

[Mov19] R. Movassagh. Cayley path and quantum computational supremacy: A proof of average-case #p-hardness of random circuit sampling with quantified robustness. *CoRR*, abs/1909.06210, 2019. arXiv:1909.06210, doi:10.48550/arXiv.1909.06210.

[PAM+10] S. Pironio, A. Acín, S. Massar, et al. Random numbers certified by bell's theorem. *Nature*, 464(7291):1021–1024, Apr 2010. doi:10.1038/nature09008.

[PT56] C. E. Porter and R. G. Thomas. Fluctuations of nuclear reaction widths. *Phys. Rev.*, 104:483–491, Oct 1956. doi:10.1103/PhysRev.104.483.

[RT19] R. Raz and A. Tal. Oracle separation of BQP and PH. In M. Charikar and E. Cohen, editors, *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23-26, 2019*, pages 13–23. ACM, 2019. doi:10.1145/3313276.3316315.

[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. doi:10.1137/S0097539795293172.

[Tal17] A. Tal. Tight bounds on the Fourier spectrum of AC0. In R. O'Donnell, editor, *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, volume 79 of *LIPIcs*, pages 15:1–15:31. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017. doi:10.4230/LIPIcs.CCC.2017.15.

[TD04] B. M. Terhal and D. P. DiVincenzo. Adaptive Quantum Computation, Constant Depth Quantum Circuits and Arthur-Merlin Games. *Quant. Inf. Comput.*, 4(2):134–145, 2004. arXiv:quant-ph/0205133, doi:10.26421/QIC4.2-5.

[Vio07] E. Viola. On approximate majority and probabilistic time. In *22nd Annual IEEE Conference on Computational Complexity (CCC 2007), 13-16 June 2007, San Diego, California, USA*, pages 155–168. IEEE Computer Society, 2007. doi:10.1109/CCC.2007.16.

[VV17] G. Valiant and P. Valiant. An automatic inequality prover and instance optimal identity testing. *SIAM J. Comput.*, 46(1):429–455, 2017. doi:10.1137/151002526.

[Wu22] X. Wu. A stochastic calculus approach to the oracle separation of BQP and PH. *Theory of Computing*, 18(17):1–11, 2022. doi:10.4086/toc.2022.v018a017.

[YZ24] T. Yamakawa and M. Zhandry. Verifiable quantum advantage without structure. *J. ACM*, 71(3):20, 2024. doi:10.1145/3658665.

[ZCC+22] Q. Zhu, S. Cao, F. Chen, et al. Quantum computational advantage via 60-qubit 24-cycle random circuit sampling. *Science Bulletin*, 67(3):240–245, 2022. doi:https://doi.org/10.1016/j.scib.2021.10.017.

[ZDQ+21] H.-S. Zhong, Y.-H. Deng, J. Qin, et al. Phase-programmable gaussian boson sampling using stimulated squeezed light. *Phys. Rev. Lett.*, 127:180502, Oct 2021. doi:10.1103/PhysRevLett.127.180502.

[ZWD+20] H.-S. Zhong, H. Wang, Y.-H. Deng, et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, Dec 2020. doi:10.1126/science.abe8770.

## A Truncated Gaussians - Proofs

Here we prove a long list version of Theorems 25 and 26. The core statements are the same, but the expectation is over the distribution $\mathcal{G}'^{p(N)}$ for some polynomial $p$. In LLQSV we are interested in the case where $p(N) = N^3$. We show that for any polynomial $p$ we can always choose $\varepsilon = 1/(C \ln N)$, to make expectation values in the next theorems arbitrarily small ($N^{-c}$ for some constant $c$ that depends on $p$ and $C$).

*Proof of Thm. 25.* We can write:

$$
\begin{aligned}
(*) &= \mathop{\mathbf{E}}_{(x,y)\sim\mathcal{G}'^{p(n)}}\left[\prod_{i=1}^{p(N)\cdot N}\max\left(1,|x_i|\right)\cdot\prod_{i=1}^{p(N)\cdot N}\max\left(1,|y_i|\right)\cdot\mathbb{1}_{(x,y)\neq\mathrm{trnc}(x,y)}\right]\\
&= \mathop{\mathbf{E}}_{(x,y)\sim\mathcal{G}'^{p(n)}}\left[\prod_{i=1}^{p(N)\cdot N}\max\left(1,|x_i|\right)\cdot\prod_{i=1}^{p(N)\cdot N}\max\left(1,|y_i|\right)\right]\\
&- \mathop{\mathbf{E}}_{(x,y)\sim\mathcal{G}'^{p(n)}}\left[\prod_{i=1}^{p(N)\cdot N}\max\left(1,|x_i|\right)\cdot\prod_{i=1}^{p(N)\cdot N}\max\left(1,|y_i|\right)\cdot\mathbb{1}_{(x,y)=\mathrm{trnc}(x,y)}\right]\\
&= \mathop{\mathbf{E}}_{(x,y)\sim\mathcal{G}'^{p(n)}}\left[\prod_{i=1}^{p(N)\cdot N}\max\left(1,|x_i|\right)\cdot\prod_{i=1}^{p(N)\cdot N}\max\left(1,|y_i|\right)\right]-\mathbf{Pr}\left[(x,y)=\mathrm{trnc}(x,y)\right]
\end{aligned}
$$

Let $z \coloneqq (x,y)$ and $\varepsilon = \frac{1}{2k\ln(p(N)\cdot N)}$ for some constant $k$. We first bound the second term:

$$
\mathbf{Pr}\left[z=\mathrm{trnc}(z)\right]\geq 1-\sum_i \mathbf{Pr}[z\neq\mathrm{trnc}(z)] = 1-2N\cdot p(N)\cdot e^{-1/(2\varepsilon)}\geq 1-N^{-k+1}
$$

Next we can bound the first term using Cauchy-Schwarz:

$$
\begin{aligned}
&\leq \sqrt{\mathop{\mathbf{E}}_{x}\left[\prod_{i=1}^{p(N)\cdot N}\max\left(1,x_i^2\right)\right]}\cdot\sqrt{\mathbb{E}_x\left[\prod_{i=1}^{p(N)\cdot N}\max\left(1,(x_i^2-\varepsilon)^2\right)\right]}\\
&= \mathop{\mathbf{E}}_{x}\left[\max\left(1,x_i^2\right)\right]^{p(N)\cdot N/2}\cdot\mathop{\mathbf{E}}_{x}\left[\max\left(1,(x_i^2-\varepsilon)^2\right)\right]^{p(N)\cdot N/2}
\end{aligned}
$$

We can write the first expectation value as:

$$
\begin{aligned}
2\int_0^1\frac{1}{\sqrt{2\pi\varepsilon}}e^{-x^2/2\varepsilon}dx+2\int_1^\infty\frac{x^2}{\sqrt{2\pi\varepsilon}}e^{-x^2/2\varepsilon}dx &\leq 1+\varepsilon\cdot\mathrm{erfc}(1/\sqrt{2\varepsilon})+\sqrt{2\varepsilon/\pi}\cdot e^{-1/2\varepsilon}\\
&\leq 1+\varepsilon e^{-1/2\varepsilon}+\sqrt{2\varepsilon/\pi}e^{-1/2\varepsilon}\\
&\leq 1+N^{-k+1}\cdot p(N)^{-k}
\end{aligned}
$$

For the second expectation value:

$$
\begin{aligned}
&2\int_0^{\sqrt{1+\varepsilon}}\frac{1}{\sqrt{2\pi\varepsilon}}e^{-x^2/2\varepsilon}dx+2\int_{\sqrt{1+\varepsilon}}^\infty\frac{(x^2-\varepsilon)^2}{\sqrt{2\pi\varepsilon}}e^{-x^2/2\varepsilon}dx\\
&\leq 2\int_0^{\sqrt{1+\varepsilon}}\frac{1}{\sqrt{2\pi\varepsilon}}e^{-x^2/2\varepsilon}dx+2\int_1^\infty\frac{x^4}{\sqrt{2\pi\varepsilon}}e^{-x^2/2\varepsilon}\\
&\leq 1+3\varepsilon^2\,\mathrm{erfc}(1/\sqrt{2\varepsilon})+\frac{\varepsilon(1+3\varepsilon)}{\sqrt{2\pi\varepsilon}}e^{-1/2\varepsilon}\\
&\leq 1+3\varepsilon^2e^{1/2\varepsilon}+\frac{\varepsilon(1+3\varepsilon)}{\sqrt{2\pi\varepsilon}}e^{-1/2\varepsilon}\leq 1+N^{-k+1}\cdot p(N)^{-k}
\end{aligned}
$$

So we can bound the first term by $(1+N^{-k+1}\cdot p(N)^{-k})^{N\cdot p(N)}\leq 1+N^{-k+2}$. Combining both we get the claim:

$$
(*)\leq 1+N^{-k+2}-(1-N^{-k+1})\leq 2N^{-k+2}
$$

□

*Proof of Thm. 26.* The original proof works without any change with the modified Claim 5.2.

$$\begin{aligned}
&\mathop{\mathbf{E}}_{z\sim\mathcal{G}'^{p(N)}}\left[\left|F\left(\mathrm{trnc}\left(z_0+p\cdot z\right)\right)-F\left(z_0+p\cdot z\right)\right|\right]\\
&\leq \mathop{\mathbf{E}}_{z\sim\mathcal{G}'^{p(N)}}\left[\left(1+\left|F\left(z_0+p\cdot z\right)\right|\right)\cdot\mathbb{1}_{\mathrm{trnc}(z_0+p\cdot z)\neq z_0+p\cdot z}\right]\\
&\leq \mathop{\mathbf{E}}_{z\sim\mathcal{G}'^{p(N)}}\left[\left(1+\left|F\left(z_0+p\cdot z\right)\right|\right)\cdot\mathbb{1}_{z\neq\mathrm{trnc}(z)}\right]\\
&\leq \mathop{\mathbf{E}}_{z\sim\mathcal{G}'^{p(N)}}\left[\left(1+\prod_{i=1}^{2N\cdot p(N)}\max\left(1,\left|\left(z_0\right)_i+p\cdot z_i\right|\right)\right)\cdot\mathbb{1}_{z\neq\mathrm{trnc}(z)}\right]\\
&\leq \mathop{\mathbf{E}}_{z\sim\mathcal{G}'^{p(N)}}\left[2\cdot\prod_{i=1}^{2N\cdot p(N)}\max\left(1,\left|\left(z_0\right)_i+p\cdot z_i\right|\right)\cdot\mathbb{1}_{z\neq\mathrm{trnc}(z)}\right]
\end{aligned}$$

And since we know $\prod_{i=1}^{2N\cdot p(N)}\max\left(1,\left|\left(z_0\right)_i+p\cdot z_i\right|\right)\leq\prod_{i=1}^{2N\cdot p(N)}\max\left(1,p_0+p\left|z_i\right|\right)\leq\prod_{i=1}^{2N\cdot p(N)}\max\left(1,\left|z_i\right|\right)$, we can write:

$$\begin{aligned}
&\mathop{\mathbf{E}}_{z\sim\mathcal{G}'^{p(N)}}\left[\left|F\left(\mathrm{trnc}\left(z_0+p\cdot z\right)\right)-F\left(z_0+p\cdot z\right)\right|\right]\\
&\quad\leq \mathop{\mathbf{E}}_{z\sim\mathcal{G}'^{p(N)}}\left[2\cdot\prod_{i=1}^{2N\cdot p(N)}\max\left(1,\left|z_i\right|\right)\cdot\mathbb{1}_{z\neq\mathrm{trnc}(z)}\right]\leq 4\cdot N^{-k+2}.
\end{aligned}$$

□

# B Aaronson's Certified Random Number Generation

For completeness, we summarize how certified random number generation is possible from "long list" conjectures. Consider the following problem:

**Problem 42.** *Given a random quantum circuit $C$ on $n$ qubits, output a sample $s$ such that:*

$$\mathop{\mathbf{E}}_{C}\left[P_C(s)\right]\geq\frac{b}{N}$$

*where $P_C(s)=\left|\left\langle s\right|C\left|0^n\right\rangle\right|^2$ and $b=1+\varepsilon$ and $\varepsilon=poly(1/n)$.*

We already know that the trivial quantum algorithm that samples from the output distribution of $C$ is a solution for this problem [PT56, BIS+18], and in fact, we have strong evidence that current NISQ devices are capable of solving this problem [AAB+19]. If we can prove that any algorithm in BQP for Problem 42 has min-entropy larger than the random seed required by our pseudorandom generator, we can connect cryptographic assumptions to certified random bit generation. Our main tool for proving such a claim is the hardness of LLQSV. Suppose we are given access to oracle $\mathcal{O}$ which is a long (exponentially large) list of $n$ qubit random quantum circuits $C_1, C_2, \ldots, C_T$ paired with strings $s_1, s_2, \ldots, s_T$. We can informally define the Long List Hardness Assumption (LLHA):

**Conjecture 43.** (LLHA) *Given oracle access to $\mathcal{O}$ it is* QCAM*-Hard to distinguish the following two cases:*

1. *Each $s_i$ is sampled uniformly at random.*
2. *Each $s_i$ is sampled from the output distribution of $C_i$.*

To summarize the overall proof strategy, we focus on refuting the existence of a deterministic BQP algorithm for Problem 42. The key idea is that if we have access to a deterministic function solving Problem 42, we can use this function in an approximate counting argument to count the number of

collisions between the output of that function and the output of the quantum circuit. Furthermore, if the list in the conjecture is long enough, we can use Chernoff bound to separate the two cases which gives a QCAM protocol for LLQSV. Suppose we are given an instance of LLQSV, where $T = N^3 = 2^{3n}$. Let $S = \sum_i^T P_{C_i}(s_i)$. Then by Hoeffding's inequality, we have:

$$\mathbf{Pr}\left[S \leq bN^2 - \frac{\varepsilon}{2}N^2\right] \geq \exp(-\frac{\varepsilon^2 N^4}{N^3}) \geq \exp(-O(n))$$

Let $V = |\{i | s_i \in Q(C_i)\}|$. Next, we can use Chernoff bound to separate the two cases:

1. $\mathbf{Pr}\left[V \geq (1+\delta)N^2\right] \leq \exp(-\frac{\delta^2}{2+\delta}N^2) \leq \exp(-N)$
2. $\mathbf{Pr}\left[V \leq (1-\delta)((1+\frac{\varepsilon}{2})N^2)\right] \leq \exp(-\frac{\delta}{2}(1+\frac{\varepsilon}{2})N^2) \leq \exp(-N)$

By setting $\delta = \varepsilon^2$, with high probability:

1. In the uniform case $V < (1+\varepsilon^2)N^2$.
2. Otherwise $V > (1+\frac{\varepsilon}{4})N^2$

Lastly, we can use approximate counting to estimate this value up to a multiplicative factor of $(1+\varepsilon^2)$ to decide between these two cases with high probability. In [Aar20], Aaronson provides further evidence that this argument can be extended to constant min-entropy algorithms and provides methods to accumulate entropy.

## C Proof of Claim 12

We restate the claim.

**Claim 44.** *Conditioned on $\mathcal{E}$, with $1 - \exp(-\Omega(n))$ probability over the choice of $\tau$, the distributions $p_{Z|\mathcal{P}}$ and $\widetilde{p}_{Z|\mathcal{P}}$ are $\exp(-\Omega(n))$-close in statistical distance.*

*Proof.* We assume that $F$ is good in the sense that Eq.(1) holds. This means that $Z : p_Z \geq \tau$ and $Z : \widetilde{p}_Z \geq \tau$ capture at least $\gamma/\mathrm{poly}(n) \geq 2^{-o(n)}$ of the probability mass of the two distributions $p$ and $\widetilde{p}$.

Recall that $\tau$ is a uniformly random integer multiple of $2^{-n/20}$ in the range $[2^{-n/30}, 2 \cdot 2^{-n/30}]$, and there are $2^{-n/30+n/20} + 1 = 2^{n/60} + 1$ such choices.

Consider the $2^{n/60}$ choices of $\tau$. They partition the values of $p_Z$ into buckets. For $i = 0, 1, \ldots, 2^{n/60} - 1$, the $i$-th bucket contain all $Z : p_Z \in [2^{-n/30} + i \cdot 2^{-n/20}, 2^{-n/30} + (i+1) \cdot 2^{-n/20})$. Finally, let the last bucket contain all $Z : p_Z \geq 2 \cdot 2^{-n/30}$. The key idea is that there cannot be too many buckets whose probability mass is large. More precisely, the $i$-th bucket is *problematic* if its probability mass is at least $2^{-n/80}$. There cannot be more than $2^{n/80}$ problematic buckets. Thus, most buckets are non-problematic, and in fact, most consecutive three buckets are non-problematic. Say we pick $\tau$ to be $2^{-n/30} + i \cdot 2^{-n/20}$ for $i$ such that both $i-1$ and $i$ are non-problematic.

Note that due to event $\mathcal{E}$ each $Z$ would get either the same bucket according to $p_Z$ and $\widetilde{p}_Z$ or a bucket off by 1 (either up or down). Thus if both $i-1$ and $i$ are non-problematic bucket than picking the threshold $\tau = 2^{-n/30} + i \cdot 2^{-n/20}$ guarantees that

$$\sum_{Z : p_Z \geq \tau, \widetilde{p_Z} < \tau} p_Z \leq \sum_{Z : p_Z \in [\tau, \tau + 2^{-n/20})} p_Z \leq 2^{-n/80}$$

and

$$\sum_{Z : p_Z < \tau, \widetilde{p_Z} \geq \tau} p_Z \leq \sum_{Z : p_Z \in [\tau - 2^{-n/20}, \tau)} p_Z \leq 2^{-n/80}$$

and so the sums $S := \sum_{Z:p_Z \geq \tau} p_Z$ and $\widetilde{S} := \sum_{Z:\widetilde{p_Z} \geq \tau} \widetilde{p}_Z$ are close since

$$\begin{aligned}
|S - \widetilde{S}| &= \left| \sum_{Z:p_Z \geq \tau} p_Z - \sum_{Z:\widetilde{p_Z} \geq \tau} \widetilde{p}_Z \right| \\
&\leq \left| \sum_{Z:p_Z \geq \tau} p_Z - \sum_{Z:\widetilde{p_Z} \geq \tau} p_Z \pm 2^{-n/20} \right| \\
&\leq \left| \sum_{Z:p_Z \geq \tau} p_Z - \sum_{Z:\widetilde{p_Z} \geq \tau} p_Z \right| + 2^{-n/60} \\
&\leq 2^{-n/80} + 2^{-n/80} + 2^{-n/60} = 2^{-\Omega(n)}
\end{aligned}$$

On the other hand both sums are at least $\gamma/\mathrm{poly}(n) = \exp(-o(n))$ and thus their ratio is $1 \pm \exp(-\Omega(n))$ and $|\frac{1}{S} - \frac{1}{\widetilde{S}}| \leq \exp(-\Omega(n))$. Finally, we have

$$\begin{aligned}
&\sum_Z \left| \frac{1}{S} \cdot |p_Z \cdot \mathbb{1}_{p_Z \geq \tau}| - \frac{1}{\widetilde{S}} \cdot |\widetilde{p}_Z \cdot \mathbb{1}_{\widetilde{p_Z} \geq \tau}| \right| \\
&\leq \sum_{Z:p_Z \geq \tau, \widetilde{p_Z} < \tau} \frac{1}{S} |p_Z| + \sum_{Z:p_Z < \tau, \widetilde{p_Z} \geq \tau} \frac{1}{\widetilde{S}} |\widetilde{p}_Z| + \sum_{Z:p_Z, \widetilde{p_Z} \geq \tau} \left| \frac{1}{S} p_Z - \frac{1}{\widetilde{S}} \widetilde{p}_Z \right|
\end{aligned}$$

We already got that the first two sums are $2^{-\Omega(n)}$. As for the third sum, we use triangle inequality to bound it by $\sum_{Z:p_Z, \widetilde{p_Z} \geq \tau} \left| \frac{1}{S} p_Z - \frac{1}{S} \widetilde{p}_Z \right| + \sum_{Z:p_Z, \widetilde{p_Z} \geq \tau} \left| \frac{1}{S} - \frac{1}{S} \right| \widetilde{p}_Z$, where both terms are $\exp(-\Omega(n))$ small. □