A Qubit, a Coin, and an Advice String Walk into a Relational Problem

Scott Aaronson
University of Texas at Austin, TX, USA
OpenAI, San Francisco, CA, USA

Harry Buhrman
QuSoft, Amsterdam, The Netherlands
Centrum Wiskunde & Informatica, Amsterdam, The Netherlands
University of Amsterdam, The Netherlands

William Kretschmer
Simons Institute for the Theory of Computing, Berkeley, CA, USA
University of California, Berkeley, CA, USA

Abstract

Relational problems (those with many possible valid outputs) are different from decision problems, but it is easy to forget just *how* different. This paper initiates the study of $\mathsf{FBQP/qpoly}$, the class of relational problems solvable in quantum polynomial-time with the help of polynomial-sized quantum advice, along with its analogues for deterministic and randomized computation (FP, FBPP) and advice ($\mathsf{/poly}$, $\mathsf{/rpoly}$).

Our first result is that $\mathsf{FBQP/qpoly} \neq \mathsf{FBQP/poly}$, *unconditionally*, with no oracle – a striking contrast with what we know about the analogous decision classes. The proof repurposes the separation between quantum and classical one-way communication complexities due to Bar-Yossef, Jayram, and Kerenidis. We discuss how this separation raises the prospect of near-term experiments to demonstrate "quantum information supremacy," a form of quantum supremacy that would not depend on unproved complexity assumptions.

Our second result is that $\mathsf{FBPP} \not\subset \mathsf{FP/poly}$ – that is, *Adleman's Theorem fails for relational problems* – unless $\mathsf{PSPACE} \subset \mathsf{NP/poly}$. Our proof uses $\mathsf{IP} = \mathsf{PSPACE}$ and time-bounded Kolmogorov complexity. On the other hand, we show that proving $\mathsf{FBPP} \not\subset \mathsf{FP/poly}$ will be hard, as it implies a superpolynomial circuit lower bound for $\mathsf{PromiseBPEXP}$.

We prove the following further results:

- *Unconditionally*, $\mathsf{FP} \neq \mathsf{FBPP}$ and $\mathsf{FP/poly} \neq \mathsf{FBPP/poly}$ (even when these classes are carefully defined).
- $\mathsf{FBPP/poly} = \mathsf{FBPP/rpoly}$ (and likewise for FBQP). For *sampling* problems, by contrast, $\mathsf{SampBPP/poly} \neq \mathsf{SampBPP/rpoly}$ (and likewise for $\mathsf{SampBQP}$).

2012 ACM Subject Classification Theory of computation → Complexity classes; Theory of computation → Quantum complexity theory

Keywords and phrases Relational problems, quantum advice, randomized advice, FBQP, FBPP

Digital Object Identifier 10.4230/LIPIcs.ITCS.2024.1

Related Version *Previous Version*: `https://arxiv.org/abs/2302.10332`

Funding *Scott Aaronson*: Supported by a Vannevar Bush Fellowship from the US Department of Defense, the Berkeley NSF-QLCI CIQC Center, a Simons Investigator Award, and the Simons "It from Qubit"collaboration.
Harry Buhrman: Supported in part by the Dutch Research Council (NWO/OCW), Gravitation Programmes Quantum Software Consortium (project number 024.003.037) and Networks (project number 024.002.003).
William Kretschmer: Supported by an NDSEG Fellowship and a Simons Quantum Postdoctoral Fellowship. Support is also acknowledged from the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator.

15th Innovations in Theoretical Computer Science Conference (ITCS 2024).
Editor: Venkatesan Guruswami; Article No. 1; pp. 1:1–1:24
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Acknowledgements We thank Daochen Wang and Alexandru Cojocaru for conversations that suggested the FBQP/poly versus FBQP/qpoly problem, and Lance Fortnow, Iordanis Kerenidis, Ashley Montanaro, Ronald de Wolf, and David Zuckerman for helpful discussions. We thank anonymous referees for constructive feedback.

1 Introduction

Here is a basic and underappreciated fact: there are computational problems – not distributed or cryptographic tasks, but just pure computational problems – that *provably* admit only randomized solutions. One simple example is: "output an n-bit Kolmogorov-random string." Another example is: "given as input a halting Turing machine M, output any string *other than* what M outputs when run on its own description."

Both of these are *relational problems*, defined by a relation $R \subseteq \{0,1\}^* \times \{0,1\}^*$. Given an input x, the goal in such a problem is to output any y such that $(x, y) \in R$. The class FP consists of all relations R for which there exists a deterministic polynomial-time algorithm to find a y such that $(x, y) \in R$ whenever one exists. (Ironically, the F stands for "functional," even though the whole point with relational problems is that they need *not* be functions.)

It is trickier to define FBPP and FBQP, the relational analogues of BPP and BQP respectively. For unlike with decision problems, we can no longer amplify success probabilities by taking majorities, so different allowed error probabilities could lead to different complexity classes. For this reason, a wide variety of definitions of FBPP have appeared in the literature [19, 4, 25, 27, 22]. Having said that, there is one choice that seems more natural than others, which Aaronson [4] made more than a decade ago and which we follow here.[1]

Call the relation $R \subseteq \{0,1\}^* \times \{0,1\}^*$ *polynomially-bounded* if there exists a polynomial p such that $|y| \le p(|x|)$ for all $(x, y) \in R$. Then:

▶ **Definition 1.** FBPP *is the class of polynomially-bounded relations $R \subseteq \{0,1\}^* \times \{0,1\}^*$ for which there exists a polynomial-time randomized algorithm A such that for all x for which there exists a y with $(x, y) \in R$ and all $\varepsilon > 0$,*

$$\Pr[(x, A(x, 0^{1/\varepsilon})) \in R] \ge 1 - \varepsilon,$$

where the probability is over A's outputs. FBQP *is exactly the same except that A can now be a quantum algorithm.*

A few comments on this definition: we require A to succeed for any given $\varepsilon > 0$ in order to avoid problems being in FBPP or FBQP for "accidental" reasons, i.e. that the fraction of strings y such that $(x, y) \notin R$ happens to fall below some arbitrary threshold. We allow time polynomial in $1/\varepsilon$ because, as we'll see, there are natural reductions that need such time. We demand that R be polynomially-bounded because otherwise, A might achieve smaller and smaller error probabilities ε by outputting longer and longer strings, rather than "doing better and better on the same strings," which is not what we intuitively wanted when we allowed $\mathrm{poly}(n, 1/\varepsilon)$ time. Finally, we do not require that membership in the relation be efficiently verifiable, in contrast to Goldreich's definition [19, Definition 3.1]. This is for fairness to quantum algorithms: we want FBQP to contain the relational analogues of problems like BosonSampling [6] and Random Circuit Sampling [7] that have played a

[1] We also found that GPT-4 [30], when prompted to give a definition for FBPP, settled on one similar to Definition 1. See the full version for the transcript.

central role in recently claimed demonstrations of quantum computational supremacy [12, 34]. However, it seems unlikely that such problems can admit efficient verification of membership in the relation.[2]

Already with FBPP and FBQP, some interesting phenomena rear their heads: for example, we'll observe in Section 4 that $\mathsf{FP} \neq \mathsf{FBPP}$, unconditionally. Note that, because of the requirement to succeed with probability $1 - \varepsilon$ for any $\varepsilon > 0$, this does *not* immediately follow from the examples with which we opened the paper, but it does follow from modifications of those examples, involving time-bounded Kolmogorov complexity or the time-bounded halting problem.

The message of this paper is that the story of FBPP and FBQP becomes wilder still – even more divergent from expectations formed from decision problems – once we bring classical and quantum *advice* into the picture.

1.1 Advice Classes

Karp and Lipton [23] introduced the nonuniform complexity class P/poly and proved the famous theorem that $\mathsf{NP} \subset \mathsf{P/poly}$ would imply the collapse of the polynomial hierarchy. Meanwhile, Adleman [10] proved that $\mathsf{BPP} \subset \mathsf{P/poly}$. Indeed, it is not hard to see that

$$\mathsf{BPP/rpoly} = \mathsf{BPP/poly} = \mathsf{P/rpoly} = \mathsf{P/poly},$$

where /rpoly means "with polynomial-sized randomized advice," and P/rpoly is the class of languages that admit nonuniform polynomial-time bounded-error randomized algorithms in which the only randomness comes from the advice. Note that the /rpoly advice is at least as powerful as the /poly advice as the /poly advice can be seen as a distribution with probability concentrated on a single string.

When we come to BQP, it's natural to ask what happens when the advice can be a quantum state on polynomially many qubits – perhaps a highly entangled state that's intractable to prepare on one's own. To capture this question, in 2003 Nishimura and Yamakami [29] defined the class BQP/qpoly, or Bounded-Error Quantum Polynomial-Time with polynomial-size quantum advice.

▶ **Definition 2.** BQP/qpoly *is the class of all languages $L \subseteq \{0,1\}^*$ for which there exists a polynomial-time quantum algorithm A, a polynomial p, and an infinite list of advice states $\{|\psi_n\rangle\}_{n\geq 1}$, where $|\psi_n\rangle$ is on $p(n)$ qubits, such that for all n and all $x \in \{0,1\}^n$,*

$$\Pr[A(x, |\psi_n\rangle) = L(x)] \geq \frac{2}{3}.$$

Studying BQP/qpoly is one way to formalize the old question of "how much information is in an n-qubit state." On the one hand, if we think of an n-qubit state $|\psi\rangle$ as a unit vector in $\mathbb{C}^{2^n}$, then it seems $|\psi\rangle$ could provide an exponential amount of information – say, about every possible input $x \in \{0,1\}^n$. On the other hand, Holevo's Theorem [21] implies that we can encode at most n bits into n qubits, in such a way that they can be reliably retrieved later by measuring them.

[2] For example, if the relation $R \in \mathsf{FBQP}$ defined in [6, Corollary 5.10] had efficient verification of membership, then the Gaussian Permanent Estimation problem $|\mathrm{GPE}|^2_{\pm}$ [6, Problem 1.2] would be solvable in $\mathsf{FP}^{\mathsf{PH}}$, thus refuting either the Permanent-of-Gaussians Conjecture [6, Conjecture 1.5], the Permanent Anti-Concentration Conjecture [6, Conjecture 1.6], or $\mathsf{P}^{\#\mathsf{P}} \not\subset \mathsf{PH}$.

So then, does $\mathsf{BQP/qpoly}$ collapse with $\mathsf{BQP/poly}$ – that is, BQP with polynomial-sized *classical* advice – or could it be vastly more powerful?

A priori, it's not even obvious that $\mathsf{BQP/qpoly} \neq \mathsf{ALL}$, where ALL is the class of all languages. Underscoring this worry, it's easy to show (for example) that $\mathsf{PostBQP/qpoly} = \mathsf{ALL}$, where $\mathsf{PostBQP}$ means quantum polynomial time with postselected measurements. To see this, given a language L and an input length n, we just need to consider the advice state

$$|\psi_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z\rangle|L(z)\rangle,$$

where $L(z) = 1$ if $z \in L$ and $L(z) = 0$ otherwise. Then given an input $x \in \{0,1\}^n$, we first measure $|\psi_n\rangle$ in the standard basis, then postselect on getting the outcome $|x\rangle|L(x)\rangle$.

Despite the sometimes unsettling power of randomized and quantum advice, in 2004, Aaronson [1] proved that $\mathsf{BQP/qpoly} \subseteq \mathsf{PostBQP/poly}$. Since Aaronson [2] also showed that $\mathsf{PostBQP} = \mathsf{PP}$, and since adding deterministic advice "commutes" with standard complexity class inclusions, this can be stated equivalently as $\mathsf{BQP/qpoly} \subseteq \mathsf{PP/poly}$.

This upper bound on the power of $\mathsf{BQP/qpoly}$ has a few implications. First, it immediately implies that $\mathsf{BQP/qpoly} \neq \mathsf{ALL}$, since $\mathsf{PP/poly} \neq \mathsf{ALL}$ is easy to show by a counting argument. Second, it means that there is no hope, in the present state of complexity theory, of proving that $\mathsf{BQP/poly} \neq \mathsf{BQP/qpoly}$. For any such proof would imply $\mathsf{BQP/poly} \neq \mathsf{PP/poly}$, and hence (for example) that PSPACE does not have polynomial-size circuits. At best, one could hope to show that $\mathsf{BQP}^A\mathsf{/poly} \neq \mathsf{BQP}^A\mathsf{/qpoly}$ for some oracle A. As it happens, even *this* is still open, although Aaronson and Kuperberg [9] showed the existence of a unitary oracle U such that $\mathsf{BQP}^U\mathsf{/poly} \neq \mathsf{BQP}^U\mathsf{/qpoly}$, and there's been recent progress toward replacing this with an ordinary classical oracle [16, 28].

1.2 Relational Complexity Classes with Advice

In quantum computing, it has repeatedly been found that it's easier to see the advantages of quantum algorithms over classical ones once we switch attention from decision problems to relational and sampling problems. This is what happened, for example, with BosonSampling [6], Random Circuit Sampling [7], and other sampling-based approaches to demonstrating quantum supremacy. It is also what happened with the recent breakthrough of Yamakawa and Zhandry [35], which achieved an exponential quantum speedup relative to a random oracle – but only by switching from decision problems (where the *Aaronson-Ambainis Conjecture* [5] asserts that no such separation is possible) to NP search problems, a particular kind of relational problem.[3]

In this paper, then, we do something that could've been done at any point in the past 20 years, but apparently wasn't: namely, we ask about the advantages of quantum over classical *advice* on relational problems.

▶ **Definition 3.** $\mathsf{FBQP/qpoly}$ *is the class of polynomially-bounded relations* $R \subseteq \{0,1\}^* \times \{0,1\}^*$ *for which there exists a polynomial-time quantum algorithm* Q*, a polynomial* $p(n,m)$*, and an infinite list of advice states* $\{|\psi_{n,m}\rangle\}_{n,m\geq 1}$*, where* $|\psi_{n,m}\rangle$ *is on* $p(n,m)$ *qubits, such that for all* x *for which there exists a* y *such that* $(x,y) \in R$ *and all* m*,*

$$\Pr[(x, Q(x, 0^m, |\psi_{n,m}\rangle)) \in R] \geq 1 - \frac{1}{m}.$$

[3] If one just wants a superpolynomial quantum speedup relative to a random oracle for *some* relational problem – not necessarily an NP search problem – then Aaronson [3] showed that the problem of outputting large Fourier coefficients of a random Boolean function does the job.

The one subtlety in this definition is that the advice state $|\psi_{n,m}\rangle$ is allowed to depend, not only on the input length n, but on the desired error probability $\varepsilon = 1/m$. We claim that this is simply the "right" choice: efficiency in this setting means time polynomial in n and $1/\varepsilon$, so the advice ought to be allowed to depend on both parameters as well.

Of course, it doesn't make much sense to feed quantum advice to a classical complexity class (e.g., $\mathsf{FP/qpoly}$). On the other hand, it's sensible to consider $\mathsf{FP/rpoly}$: this corresponds to classical algorithms that *only* get to use random bits if they come from the advice.

▶ **Definition 4.** $\mathsf{FP/rpoly}$ *is the class of polynomially-bounded relations* $R \subseteq \{0,1\}^* \times \{0,1\}^*$ *for which there exists a polynomial-time deterministic classical algorithm* A*, a polynomial* $p(n,m)$*, and an infinite list of advice distributions* $\{\mathcal{D}_{n,m}\}_{n,m\geq 1}$*, where* $\mathcal{D}_{n,m}$ *is supported on* $\{0,1\}^{p(n,m)}$*, such that for all* x *for which there exists a* y *such that* $(x,y) \in R$ *and all* m*,*

$$\Pr_{r \sim \mathcal{D}_{n,m}}[(x, A(x, 0^m, r)) \in R] \geq 1 - \frac{1}{m}.$$

We can similarly define $\mathsf{FBPP/rpoly}$, $\mathsf{FBQP/poly}$, and other possible combinations; we omit the details.

1.3 Our Results

We show that switching attention to relational problems dramatically changes the picture of randomized and quantum computation in the presence of advice.

Our first result is that quantum advice *unconditionally* provides more power than classical advice to solve relational problems:

▶ **Theorem 5.** $\mathsf{FBQP/qpoly} \neq \mathsf{FBQP/rpoly}$.

So in particular, $\mathsf{FBQP/qpoly} \neq \mathsf{FBQP/poly}$. Indeed, we shall see that $\mathsf{FBQP/qpoly}$ is not contained in $\mathsf{F}\mathcal{C}\mathsf{/poly}$ for arbitrarily powerful uniform complexity classes $\mathcal{C}$: for example, the class of all computable problems. This is despite the fact that $\mathsf{FBQP/qpoly}$ does *not* equal ALL – as can be seen, for example, by considering its restriction to Boolean-valued problems, where it coincides with $\mathsf{PromiseBQP/qpoly} \subseteq \mathsf{PromisePP/poly}$.

As we discuss in Section 3, this complexity class separation suggests the possibility of a near-term experiment, which would run an $\mathsf{FBQP/qpoly}$ protocol in order to check explicitly whether an entangled state of n qubits (where, say, $n \approx 20$) encodes $\gg n$ bits of classical information. We hope further work will clarify whether such an experiment is feasible with current devices.

Theorem 5 is nonconstructive, and does not give an explicit example of a relation in $\mathsf{FBQP/qpoly}$ but not $\mathsf{FBQP/rpoly}$ (not counting, e.g., the use of brute force to find the lexicographically first relation that works). We leave the "explicitization" of this separation as one of our central challenges.

Our second result shows that Adleman's Theorem [10], that $\mathsf{BPP} \subset \mathsf{P/poly}$, almost certainly does *not* extend to relational problems: [4]

[4] After this manuscript first appeared, Ilango, Li, and Williams [22] implicitly established a conceptually similar result that $\mathsf{FBPP} \not\subset \mathsf{FP/poly}$ under plausible assumptions. They show a conditional lower bound for the range avoidance problem AVOID, which lies in FBPP (whenever the stretch is at least linear). Roughly, [22, Theorem 28] shows that if subexponentially-secure indistinguishability obfuscation exits and coNP is not in $\mathsf{NP/poly}$ infinitely often, then AVOID $\notin \mathsf{FP/poly}$. Comparatively, our result seems to weaken the assumption required to separate FBPP from $\mathsf{FP/poly}$, but only in the sense that non-collapse of PH is a better-tested assumption than the existence of indistinguishability obfuscation.

▶ **Theorem 6.** *If* $\mathsf{FBPP} \subset \mathsf{FP/poly}$*, then* $\mathsf{PSPACE} \subset \mathsf{NP/poly}$ *(and hence* PH *collapses).*

We complement Theorem 6 with a result showing that an unconditional proof of $\mathsf{FBPP} \not\subset \mathsf{FP/poly}$ is unlikely in the current state of complexity theory, as it would imply breakthrough circuit lower bounds:

▶ **Theorem 7.** $\mathsf{FBPP} \subseteq \mathsf{FP}^{\mathsf{PromiseBPEXP}}$. *Hence, if* $\mathsf{PromiseBPEXP} \subset \mathsf{PromiseP/poly}$*, then* $\mathsf{FBPP} \subset \mathsf{FP/poly}$.

We also show that, when FP and FBPP are either both given advice or both *not* given advice, the separation between them becomes unconditional:

▶ **Theorem 8.** $\mathsf{FP} \neq \mathsf{FBPP}$.

▶ **Theorem 9.** $\mathsf{FP/poly} \neq \mathsf{FBPP/poly}$.

This underscores yet another difference between decision and relational problems: if $\mathcal{C}_1$ and $\mathcal{C}_2$ are two uniform classes of promise problems, then the question of whether $\mathcal{C}_1 \subset \mathcal{C}_2/\mathsf{poly}$ is equivalent to the question of whether $\mathcal{C}_1/\mathsf{poly} \subseteq \mathcal{C}_2/\mathsf{poly}$, since an advice string can just be appended to the input. With relational complexity classes such as FBPP, however, this equivalence is no longer immediate, since it doesn't account for how the length of the advice can depend on the error bound ε.

A last question is whether our separation between classical and quantum advice, in the relational setting, extends to a separation between deterministic and randomized advice. We show that the answer is no:

▶ **Theorem 10.** $\mathsf{FBPP/rpoly} = \mathsf{FBPP/poly} = \mathsf{FP/rpoly}$ *and* $\mathsf{FBQP/rpoly} = \mathsf{FBQP/poly}$.

See Figure 1 for the complexity class inclusion diagram that emerges from our results about relational classes.

We remark that several of our results are sensitive to the choices we made in defining FBPP and its variants, especially in regards to error reduction. In Section 5, we explore the consequences of choosing some alternative error bounds in Definition 1. There, we find that Theorems 6, 8, and 9 no longer hold unconditionally if we demand exponential error reduction, meaning that the algorithm outputs a sample consistent with the relation with probability $1 - \varepsilon$ in time *polylogarithmic* in $1/\varepsilon$.[5] So, our results could be interpreted in two different ways: either as showing a striking contrast between relational and decisional classes, or as showing the remarkable power of FBPP when we don't demand exponential error reduction. We leave it to the reader to decide, and hope that this work inspires more discussion about subtleties in the definitions.

1.4 Quantum Communication Complexity

As it turns out, essentially everything we need to prove Theorem 5 was proved 20 years ago, by Bar-Yossef, Jayram, and Kerenidis [13] – though the fact that this is so is buried in their paper. These authors considered separations between randomized and quantum *one-way communication complexities*. That is, they considered the setting where Alice has an input x, Bob has an input y, and Alice can send a message m_x to Bob, which should then allow Bob to compute some joint property of x and y.

[5] By contrast, Theorem 5 is unaffected by such a change in definition, because the $\mathsf{FBQP/qpoly}$ algorithm used in our proof will turn out to be errorless.

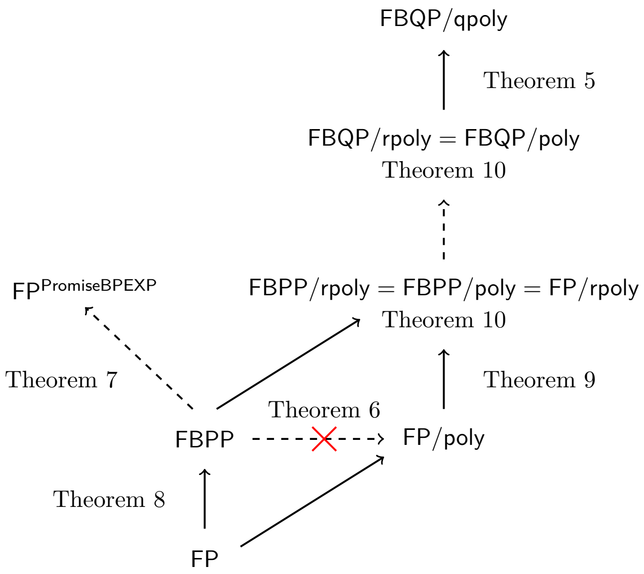

Figure 1 Relationships among classes of relational problems considered in this paper. A solid arrow from $\mathcal{C}_1$ to $\mathcal{C}_2$ indicates strict containment ($\mathcal{C}_1 \subsetneq \mathcal{C}_2$). A dashed arrow indicates a containment $\mathcal{C}_1 \subseteq \mathcal{C}_2$ that we conjecture to be strict, but a proof of strictness would require a breakthrough in complexity theory. A crossed dashed arrow indicates non-containment ($\mathcal{C}_1 \not\subseteq \mathcal{C}_2$) under the assumption that PH does not collapse.

Let T be a task, which might be the evaluation of a Boolean function $f(x, y)$, but might also be a sampling or relational problem. We define $D^1(T)$, $R^1(T)$, and $Q^1(T)$ to be the minimum number of bits sent from Alice to Bob in any deterministic, bounded-error randomized, or bounded-error quantum one-way communication protocol respectively that lets Bob perform the task for all valid input pairs (x, y) (with the number of bits maximized over all such input pairs). We assume no shared randomness or entanglement.

Clearly $D^1(T) \geq R^1(T) \geq Q^1(T)$ for all tasks T. A natural question is how large the separations between the measures can be. It's well-known that D^1 and R^1 can be exponentially separated: for example, for the N-bit EQUALITY function EQ, we have $D^1(\mathrm{EQ}) = N$ while $R^1(\mathrm{EQ}) = O(\log N)$. But what about R^1 versus Q^1?

To study this, Bar-Yossef, Jayram, and Kerenidis [13] defined a relation problem called *Hidden Matching* or HM. Here Alice is given a string $x \in \{0,1\}^N$ (with N even), while Bob is given a perfect matching y on the set $[N]$, consisting of $N/2$ edges. Bob's goal is to output $(i, j, x_i \oplus x_j)$ for *some* edge $(i, j) \in y$. The key result is then the following:

▶ **Theorem 11** ([13]). $Q^1(\mathrm{HM}) = O(\log N)$*, whereas* $R^1(\mathrm{HM}) = \Omega(\sqrt{N})$.

Crucially for us, Bar-Yossef, Jayram, and Kerenidis actually proved the following stronger statement:

▶ **Theorem 12** ([13, Proof of Theorem 4.1, page 373]). *Let $\mathcal{M}$ be any set of perfect matchings on $[N]$ that is pairwise edge-disjoint and satisfies $|\mathcal{M}| = \Omega(N)$. Let μ be the distribution over inputs to* HM *in which Alice's input is uniform in $\{0,1\}^N$ and Bob's input is uniform in $\mathcal{M}$. Then, any deterministic one-way protocol for* HM *that errs with probability at most $1/8$ with respect to μ requires $\Omega(\sqrt{N})$ bits of communication.*

To prove Theorem 5, in Section 2, we adapt Theorem 11 to the setting of FBQP/qpoly, treating the advice as one-way communication from an advisor to the FBQP algorithm.

To understand the situation more deeply, recall the result of Aaronson [1] from before, that $\mathsf{BQP/qpoly} \subseteq \mathsf{PP/poly}$. A direct analogue of that result for one-way communication complexity [1] says that $D^1(f)$ and $Q^1(f)$ are close whenever Bob's input is small:

▶ **Theorem 13** ([1]). *For all Boolean functions* $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ *(partial or total),* $D^1(f) = O(mQ^1(f) \log Q^1(f))$.

This paper is pointing out that Theorem 13, and $\mathsf{BQP/qpoly} \subseteq \mathsf{PP/poly}$, both *fail catastrophically* for sampling and relational problems. This seems not to have been known even to experts who we asked. One reason, perhaps, is that the original separation of Bar-Yossef, Jayram, and Kerenidis [13] was partly overshadowed by the later work of Gavinsky et al. [18]. The latter modified the Hidden Matching relational problem to obtain a partial Boolean function, called *Boolean Hidden Matching* or BHM. They then showed that $Q^1(\text{BHM}) = O(\log N)$ whereas $R^1(\text{BHM}) = \Omega(\sqrt{N})$.

We are calling attention to a surprising difference between the original Hidden Matching separation and the later Boolean Hidden Matching one. Namely: we can make Bob's input "small" (say, $O(\log n)$ bits) in the HM separation, *even though we cannot do the same in the* BHM *separation.* For Boolean f, Theorem 13 shows that an exponential gap between $D^1(f)$ and $Q^1(f)$ is possible only when Bob's input is "large."

1.5 Other Proofs

Let us make a few remarks about our other results, proved in Sections 2 and 4. To show that $\mathsf{FBPP/rpoly} = \mathsf{FBPP/poly}$, we just take deterministic advice that consists of $O(n/\varepsilon^2)$ independent samples from the randomized advice distribution, and then appeal to a Hoeffding and union bound. To show that $\mathsf{FP} \neq \mathsf{FBPP}$, we consider the problem of outputting an n-bit string with large time-bounded Kolmogorov complexity.[6] To show that $\mathsf{FBPP} \subseteq \mathsf{FP}^{\mathsf{PromiseBPEXP}}$, we give a simple polynomial-time algorithm that builds a string in the relation one bit at a time, using the $\mathsf{PromiseBPEXP}$ oracle.

Finally, and most interestingly, to show that a "relational Adleman's Theorem" ($\mathsf{FBPP} \subset \mathsf{FP/poly}$) is unlikely to hold, we build on an old idea due to Buhrman and Torenvliet [15]. We show that, if the problem of generating strings of high conditional time-bounded Kolmogorov complexity were in $\mathsf{FP/poly}$, then in the $\mathsf{IP} = \mathsf{PSPACE}$ protocol [32], we could replace the randomized verifier by a deterministic polynomial-size circuit. Roughly speaking, the verifier replaces each random challenge with a string of high time-bounded Kolmogorov complexity conditioned on the prior transcript of the protocol. To argue that this derandomization is sound, we just have to show that the "bad" choices of randomness (i.e. those that cause the verifier to accept when it should reject) all have low conditional time-bounded Kolmogorov complexity. We complete the proof by observing that this derandomization would put PSPACE into $\mathsf{NP/poly}$.

1.6 Sampling Problems

We conclude with some results about sampling problems, which are closely related to relation problems. A sampling problem is defined by a collection of probability distributions $\mathcal{D}_x$. Given an input x, the goal is to output a sample from $\mathcal{D}_x$, either exactly or approximately.

[6] An alternative approach (not shown here) is to prove $\mathsf{FP} \neq \mathsf{FBPP}$ using a direct diagonalization. The core idea of this argument is captured in [19, Section 3.1].

Like for relational problems, we call a sampling problem $S = \{\mathcal{D}_x\}_{x \in \{0,1\}^*}$ *polynomially-bounded* if there exists a polynomial p such that for every x, $\mathcal{D}_x$ is a distribution over strings of length at most $p(|x|)$. Again following Aaronson [4], we define the basic complexity class like so:

▶ **Definition 14.** SampBQP *is the class of polynomially-bounded sampling problems* $S = \{\mathcal{D}_x\}_{x \in \{0,1\}^*}$ *for which there exists a polynomial-time quantum algorithm* Q *such that for all* x *and all* $\varepsilon > 0$*,*

$$\|\mathcal{D}_Q(x, 0^{1/\varepsilon}) - \mathcal{D}_x\| \leq \varepsilon,$$

where $\mathcal{D}_Q(x, 0^{1/\varepsilon})$ *represents* Q*'s output distribution on input* $(x, 0^{1/\varepsilon})$ *and* $\|\|$ *represents total variation distance.*

Again, we can consider the classical analogue SampBPP (the deterministic version, SampP, doesn't make much sense). We can also combine with deterministic, randomized, and quantum advice like in Definition 3, to get SampBPP/poly, SampBQP/qpoly, and so on. For example:

▶ **Definition 15.** SampBPP/rpoly *is the class of polynomially-bounded sampling problems* $S = \{\mathcal{D}_x\}_{x \in \{0,1\}^*}$ *for which there exists a polynomial-time randomized algorithm* A*, a polynomial* $p(n, m)$*, and an infinite list of advice distributions* $\{\mathcal{D}_{n,m}\}_{n,m \geq 1}$*, where* $\mathcal{D}_{n,m}$ *is supported on* $\{0,1\}^{p(n,m)}$*, such that for all* x *and all* m*,*

$$\|\mathcal{D}_A(x, 0^m, \mathcal{D}_{n,m}) - \mathcal{D}_x\| \leq \frac{1}{m},$$

where $\mathcal{D}_A(x, 0^m, \mathcal{D}_{n,m})$ *represents* A*'s output distribution on input* $(x, 0^m, y)$ *averaged over* $y \sim \mathcal{D}_{n,m}$ *and* $\|\|$ *represents total variation distance.*

Note that our separations will also hold for the *exact* versions of these sampling classes, but the ε-approximate versions are more robust and seem of greater interest.

Our basic results, proved in Section 6, are as follows. First, we show that sampling classes are more powerful with randomized advice than with deterministic advice:

▶ **Theorem 16.** SampBPP/poly $\neq$ SampBPP/rpoly *and* SampBQP/poly $\neq$ SampBQP/rpoly*.*

To prove Theorem 16, we simply choose a probability distribution over $\{0,1\}^n$ randomly for each n, then appeal to a counting argument.

Second, as a straightforward corollary of Theorem 5, we show that quantum advice provides more power than classical advice for sampling problems:

▶ **Theorem 17.** SampBQP/rpoly $\neq$ SampBQP/qpoly*.*

Theorem 16 contrasts with the situation for relational problems, where FBPP/poly $=$ FBPP/rpoly by Theorem 10. This is noteworthy because Aaronson [4] used Kolmogorov complexity to prove a general connection between sampling problems and relational problems. This connection had the following implication, among others:

▶ **Theorem 18** ([4])**.** FBPP $=$ FBQP *if and only if* SampBPP $=$ SampBQP*.*

Yet as we now see, the "equivalence" does not force the question of the power of randomized advice to have the same answer for sampling problems that it has for relational problems.

See Figure 2 for a complexity class inclusion diagram that summarizes our results about sampling classes.

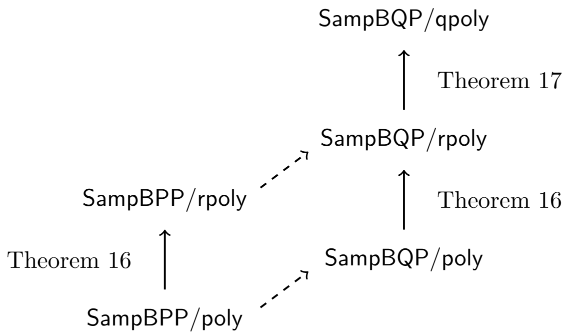

Figure 2 Relationships among classes of sampling problems considered in this paper. A solid arrow from $\mathcal{C}_1$ to $\mathcal{C}_2$ indicates strict containment ($\mathcal{C}_1 \subsetneq \mathcal{C}_2$). A dashed arrow indicates a containment $\mathcal{C}_1 \subseteq \mathcal{C}_2$ that we conjecture to be strict, but a proof of strictness would require a breakthrough in complexity theory.

2 Deterministic, Randomized, and Quantum Advice

We start this section by observing that for relational problems, randomized advice gives no more power than deterministic advice.

▶ **Theorem 10.** $\mathsf{FBPP/rpoly} = \mathsf{FBPP/poly} = \mathsf{FP/rpoly}$ *and* $\mathsf{FBQP/rpoly} = \mathsf{FBQP/poly}$.

Proof. We first prove that $\mathsf{FBPP/rpoly} = \mathsf{FBPP/poly}$. The proof of $\mathsf{FBQP/rpoly} = \mathsf{FBQP/poly}$ is identical but with quantum algorithms in place of randomized algorithms, so we omit it. Let R be a relational problem in $\mathsf{FBPP/rpoly}$, decided by an algorithm A. Fix an input length n and an $\varepsilon > 0$. Let $\mathcal{D}_{n,\varepsilon}$ be the distribution over advice strings. Then for all $x \in \{0,1\}^n$, we must have

$$\Pr_{w \sim \mathcal{D}_{n,\varepsilon}}\left[(x, A(x, 0^{1/\varepsilon}, w)) \in R\right] \geq 1 - \varepsilon.$$

In our $\mathsf{FBPP/poly}$ simulation, we'll take (say) $k = 100n/\varepsilon^2$ independent samples $w_1, \ldots, w_k$ from $\mathcal{D}_{n,\varepsilon/2}$ as the advice. Given an input x, we'll then just pick $i \in \{1, \ldots, k\}$ uniformly at random and output $A(x, 0^{2/\varepsilon}, w_i)$. By Hoeffding's inequality, we have that for any fixed $x \in \{0,1\}^n$,

$$\Pr_{w_1,\ldots,w_k}\left[\Pr_i\left[A(x, 0^{2/\varepsilon}, w_i) \in R\right] < 1 - \varepsilon\right] \leq \exp\left(-k\varepsilon^2/2\right).$$

Hence, by a union bound over all $x \in \{0,1\}^n$, there exists some choice of $w_1, \ldots, w_k$ that allows the $\mathsf{FBPP/poly}$ simulation to succeed with probability at least $1 - \varepsilon$ on every x.

Lastly, we also have $\mathsf{FBPP/rpoly} = \mathsf{FP/rpoly}$, since the randomized advice to an FP machine can include as many uniformly random bits as are needed to simulate any desired FBPP machine. ◀

We now prove the unconditional separation between FBQP with quantum advice and FBQP with classical advice.

▶ **Theorem 5.** $\mathsf{FBQP/qpoly} \neq \mathsf{FBQP/rpoly}$.

Proof. From Theorem 10, it suffices to show that $\mathsf{FBQP/qpoly} \neq \mathsf{FBQP/poly}$. Let $F = \{f_n\}_{n \geq 1}$ be an infinite family of Boolean functions, with $f_n : \{0,1\}^n \to \{0,1\}$. Then we define the following relation problem:

$$R_F = \{(x, (y, b)) : x, y \in \{0,1\}^n, b \in \{0,1\}, f_n(y) \oplus f_n(y \oplus x) = b\}.$$

In other words, given an input $x \in \{0,1\}^n$, the problem is to output another string $y \in \{0,1\}^n$, along with a bit b, such that $f_n(y)$ and $f_n(y \oplus x)$ XOR to b.

We first show that, for all F, this problem is in $\mathsf{FBQP/qpoly}$. The quantum advice state is simply

$$|\psi_n\rangle := \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{f_n(y)} |y\rangle.$$

Given an input $x \in \{0,1\}^n$, along with $|\psi_n\rangle$, the algorithm is now as follows. If $x = 0^n$, then just output $(y, 0)$ for any $y \in \{0,1\}^n$. Otherwise, first find a matrix $A \in \mathbb{F}_2^{(n-1)\times n}$ whose nullspace is $\{0, x\}$. Then map $|\psi_n\rangle$ to

$$\frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{f_n(y)} |y\rangle |Ay\rangle$$

and measure the $|Ay\rangle$ register in the computational basis, to reduce the $|y\rangle$ register to the form

$$\frac{(-1)^{f_n(y)}|y\rangle + (-1)^{f_n(y \oplus x)}|y \oplus x\rangle}{\sqrt{2}}$$

for some y. Then measure the above state in the $\{|y\rangle \pm |y \oplus x\rangle\}$ basis, to learn the relative phase $b := f(y) \oplus f(y \oplus x)$. Finally, output y, b. This algorithm succeeds with certainty for every x.

By contrast, Theorem 12 implies that, with probability 1 over the choice of F, the problem is not in $\mathsf{FBQP/poly}$, or indeed in $\mathsf{FBQP/rpoly}$. For each possible input $x \neq 0^n$ gives rise to a matching $\mathcal{M}_x := \{(y, y \oplus x) \mid y \in \{0,1\}^n\}$ on $\{0,1\}^n$, and these matchings are pairwise edge-disjoint. So, if we imagine that Alice holds the truth table of a random Boolean function f_n, consisting of $N = 2^n$ bits, while Bob holds a random index x of the matching, we find that Alice must send $\Omega(\sqrt{N}) = \Omega(2^{n/2})$ classical bits to Bob to allow him to satisfy the relation R_F with a success probability of at least $7/8$.

In the actual problem, of course, the function f_n is fixed for each n, rather than chosen by an Alice, and the $\mathsf{FBQP/poly}$ algorithm Q's behavior depends on the f_n's via the classical advice, rather than a message from Alice. Given a choice of F, let $a_{F,n,m} \in \{0,1\}^{\mathrm{poly}(n,m)}$ be the advice string for inputs of length n with error $1/m$. Then in order for Q to be correct on $x \in \{0,1\}^n$, we require that for all m,

$$\Pr\left[(x, Q(x, 0^m, a_{F,n,m})) \in R_F\right] \geq 1 - 1/m.$$

If we imagine that $F = \{f_n\}_{n\geq 1}$ is chosen uniformly at random, then we can bound the probability that Q satisfies this condition on all inputs of length n, i.e.

$$\begin{aligned}
&\Pr_F\left[\forall x \in \{0,1\}^n : \Pr\left[(x, Q(x, 0^m, a_{F,n,m})) \in R_F\right] \geq 1 - 1/m\right] \\
\leq &\Pr_{F, x\sim\{0,1\}^n}\left[\Pr\left[(x, Q(x, 0^m, a_{F,n,m})) \in R_F\right] \geq 1 - 1/m\right] \\
\leq &\frac{m}{m-1} \Pr_{F, x\sim\{0,1\}^n}\left[(x, Q(x, 0^m, a_{F,n,m})) \in R_F\right],
\end{aligned}$$

where the last line uses Markov's inequality. Choose $m = 16$, so that $a_{F,n,m}$ is a string of length $\mathrm{poly}(n) = o\left(2^{n/2}\right)$. Then combining the above bound with Theorem 12 implies that

$$\Pr_F\left[\forall x \in \{0,1\}^n : \Pr\left[(x, Q(x, 0^m, a_{F,n,m})) \in R_F\right] \geq 1 - 1/m\right] \leq \frac{16}{15} \cdot \frac{7}{8} = \frac{14}{15}$$

for all sufficiently large n. Moreover, this probability is independent for each $n \in \mathbb{N}$, because each f_n is chosen independently, so the overall probability that any choice of advice allows Q to compute R_F is at most $\prod_{n=1}^{\infty} 14/15 = 0$. This is to say that a uniformly random F satisfies $R_F \notin \mathsf{FBQP/poly}$ with probability 1. ◀

Note that, in the proof of $R_F \notin \mathsf{FBQP/poly}$, we nowhere needed the fact that the algorithm was an efficient quantum algorithm (i.e., FBQP), but only that the algorithm succeeds with bounded error. Hence we can conclude more generally that $R_F \notin \mathsf{F}\mathcal{C}\mathsf{/poly}$ for uniform complexity classes $\mathcal{C}$ with arbitrarily large computational power, such as PSPACE, EXP, BPEXP, R, and so on. We additionally get $R_F \notin \mathsf{FBQP/rpoly}$, because $\mathsf{FBQP/rpoly} = \mathsf{FBQP/poly}$.[7] On the other hand, we cannot say that $R_F \notin \mathsf{F}\mathcal{C}\mathsf{/rpoly}$ for any $\mathcal{C}$, because of the way the success conditions of certain complexity classes interact with randomized advice: as an example, $\mathsf{PostBPP/rpoly} = \mathsf{ALL}$, and so a reasonably defined relational analogue $\mathsf{FPostBPP/rpoly}$ certainly *would* contain R_F.

It is interesting to ask just how efficient we can make the quantum algorithm of Theorem 5. We describe how to implement the measurement on $|\psi_n\rangle$ via a simpler circuit, without the need to compute the matrix-vector multiplication Ay. We claim the following: first, the quantum circuit for measuring $|\psi_n\rangle$ and learning the output string y, b can be taken to be a stabilizer circuit. Second, this stabilizer circuit has $O(n)$ size and can be constructed in $O(n)$ time.

To see why, suppose for example that the input x is 001111. Suppose we measure $|\psi_n\rangle$ according to the circuit in Figure 3, and get the result $z = z_1z_2z_3z_4z_5z_6$. We claim that this measurement result corresponds to collapsing the input state to

$$\frac{|y\rangle + (-1)^b|x \oplus y\rangle}{\sqrt{2}},$$

where $y = z_1z_2z_3z_4z_50$ and $b = z_6$. The easiest way to see why is to consider the resulting state when we apply the inverse circuit to $|z\rangle$.

For a general x of Hamming weight $k \geq 1$, we choose an arbitrary i for which $x_i = 1$, and let qubit i play the role of measuring b. The circuit will consist of $k - 1$ CNOT gates between qubit i and the other qubits j for which $x_j = 1$, followed by a single Hadamard gate on qubit i to measure b.

One more comment: our proof of Theorem 5 was nonconstructive, in the sense that we did not exhibit any particular F such that $R_F \notin \mathsf{FBQP/poly}$, but merely used counting to show that a random F works with probability 1. Thus, it is natural to wonder whether we could find an "explicit" F, say $F \in \mathsf{FPSPACE}$, such that $R_F \notin \mathsf{FBQP/poly}$ under a plausible hardness assumption. We do not know, but we would like to observe that for the *promise problem* versions of these classes – namely $\mathsf{PromiseBQP/poly}$ and $\mathsf{PromiseBQP/qpoly}$ – general principles imply (perhaps surprisingly) that, if there is any separation at all, then the separation can be witnessed "explicitly":

[7] Alternatively, $R_F \notin \mathsf{FBQP/rpoly}$ can be shown directly by a small modification of the above proof: simply replace the advice string $a_{F,n,m}$ with a sample from an advice distribution. This works because Theorem 12 lower-bounds *randomized* one-way communication complexity, not just deterministic, by Yao's principle [36].

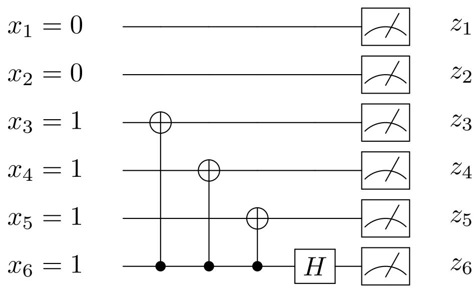

Figure 3 A circuit for measuring the state $|\psi_n\rangle$ in Theorem 5. Note that the circuit will depend on the input x; an example with $x = 001111$ is shown. First, all qubits i such that $x_i = 0$ are measured in the computational basis. Next, the qubits i such that $x_i = 1$ are measured to determine two things: (i) a computational basis state modulo a NOT gate being applied to each qubit; and (ii) the relative phase between those two basis states, one with the NOT gates applied and the other without (this is the purpose of the sole Hadamard gate).

▶ **Proposition 19.** *Suppose* $\mathsf{PromiseBQP/poly} \neq \mathsf{PromiseBQP/qpoly}$*. Then there is a* $\mathsf{PromisePP}$ *problem in* $\mathsf{PromiseBQP/qpoly}$ *but not in* $\mathsf{PromiseBQP/poly}$*.*

Proof. We prove the contrapositive. Suppose

$$\mathsf{PromisePP} \cap \mathsf{PromiseBQP/qpoly} \subseteq \mathsf{PromiseBQP/poly}.$$

Let $\Pi = (\Pi_Y, \Pi_N)$ be a promise problem in $\mathsf{PromiseBQP/qpoly}$. Aaronson [1] showed that $\mathsf{PromiseBQP/qpoly} \subseteq \mathsf{PromisePP/poly}$. Let $\{w_n\}_{n\geq 1}$ be the advice strings for the $\mathsf{PromisePP/poly}$ machine. Then we define a new promise problem Π', whose yes-instances have the form (x, w_n) for $x \in \Pi_Y \cap \{0,1\}^n$, and whose no-instances have the form (x, w_n) for $x \in \Pi_N \cap \{0,1\}^n$. Clearly $\Pi' \in \mathsf{PromisePP}$. We also have $\Pi' \in \mathsf{PromiseBQP/qpoly}$, since we can just ignore w_n. By assumption, then, $\Pi' \in \mathsf{PromiseBQP/poly}$. But moving w_n back to the advice, this means that $\Pi \in \mathsf{PromiseBQP/poly}$ as well. Therefore $\mathsf{PromiseBQP/qpoly} = \mathsf{PromiseBQP/poly}$. ◀

So in particular, under a plausible complexity assumption, namely $\mathsf{BQP/poly} \neq \mathsf{BQP/qpoly}$, there *is* an explicit problem in $\mathsf{FBQP/qpoly}$ but not in $\mathsf{FBQP/poly}$ – for observe that promise problems are a special case of relational problems.

Of course, for relational problems we would like to do better than this observation, by constructing an explicit problem in $\mathsf{FBQP/qpoly} \setminus \mathsf{FBQP/poly}$ under a "standard" hardness assumption, one about complexity classes like EXP or PSPACE or $\mathsf{P/poly}$.

3 Toward Quantum Information Supremacy

The extreme simplicity of the circuit in Figure 3 to measure the advice state $|\psi_n\rangle$ – namely, a linear number of 1- and 2-qubit Clifford gates – raises the question of whether an experiment "witnessing" the separation between $\mathsf{FBQP/rpoly}$ and $\mathsf{FBQP/qpoly}$ might be feasible with current technology, and on a large enough scale to be interesting.

As it happens, Kumar, Kerenidis, and Diamanti [24] reported an experimental demonstration of the Bar-Yossef-Jayram-Kerenidis Hidden Matching protocol [13] in 2018. However, their experiment used an optical coherent state with 2^n modes, and tiny average photon number per mode, in order to simulate n qubits. It therefore didn't directly test the question of whether n qubits (encoded, say, using n entangled particles) require $\exp(n) \gg n$ bits to simulate classically. This is the question that we propose to test now.

We are finally in the era of small programmable quantum computers: devices that can run more-or-less arbitrary circuits (subject to locality constraints) on ~ 100 qubits and ~ 1000 gates, and then extract a detectable signal on measurement. Within the past few years, these devices have been used to assert the milestone of "quantum computational supremacy" – that is, a clear advantage over currently-available classical algorithms and hardware – for contrived tasks such as Random Circuit Sampling and BosonSampling (see, e.g., [12, 34]).

Notably, these quantum supremacy tasks are validated using, e.g., Google's *Linear Cross-Entropy Benchmark* [12], which lets us see them as literally *relational problems.* In Random Circuit Sampling, for example, we are given as input a classical description of an n-qubit quantum circuit C. We are then asked to output any distinct strings $s_1, \ldots, s_k \in \{0,1\}^n$ that satisfy an inequality such as

$$\sum_{i=1}^{k} |\langle s_i|C|0^n\rangle|^2 \geq \frac{1.002k}{2^n}.$$

When, say, $k \approx n$, the above yields a relational problem in FBQP that is plausibly conjectured not to be in FBPP (see, e.g., Aaronson and Gunn [8]).

Of course, any conjecture of this sort rests on unproved computational hardness assumptions: if nothing else, then $\mathsf{P} \neq \mathsf{PSPACE}$! Alas, "standard" hardness assumptions have not sufficed here. The fundamental drawback of current quantum supremacy experiments is that, with each concession that we need to make to experimental reality – for example, depolarizing noise, photon losses, a limited number of qubits (to keep the classical verification feasible), limited circuit depth (to control the noise), limited qubit connectivity, etc. – the relevant hardness assumptions move to shakier and shakier ground. Furthermore, the worry about classical spoofing is far from hypothetical! Classical algorithms for simulating noisy random quantum circuits *have* improved, both in theory and in practice (see, e.g., [17, 31, 11]) – if not enough to kill the current claims of quantum supremacy outright, then enough to call them into reasonable doubt.

Thus, wouldn't it be great if a meaningful quantum supremacy experiment could be designed based on *no* unproved hardness assumptions? Such an experiment might, for example, try to falsify the hypothesis that every "realistic" entangled state of n qubits is secretly describable using $p(n)$ classical bits, for some small polynomial p, whether due to noise or experimental limitations or even a breakdown of quantum mechanics itself. Note that this marks a fundamental difference compared to existing experiments based on (say) Bell inequality violations – whereas the Bell/CHSH experiments test the nonlocal nature of quantum correlations, they in no way test the exponential dimensionality of Hilbert space. As far as we know, the experiments we propose here would be the first directly to test the latter without relying on any unproved computational assumptions.

In such an experiment, we might first prepare a random n-qubit entangled state $|\psi\rangle$, then measure $|\psi\rangle$ in a basis B chosen randomly and "on the fly" – just like Alice's and Bob's measurement bases in the Bell/CHSH experiment are ideally chosen when the entangled photons are already in flight. We would repeat this process many times, with a new random basis B each time, collect statistics on the measurement outcomes, and then argue that no $p(n)$-bit classical digest of $|\psi\rangle$ could possibly have allowed those statistics to be reproduced.

This is exactly what we suggest to do, by leveraging the unconditional separation between $\mathsf{FBQP/rpoly}$ and $\mathsf{FBQP/qpoly}$, which in turn is based on the unconditional separation between randomized and quantum one-way communication complexities. Note that such an experiment would almost certainly be impractical with current hardware, if the required measurements on $|\psi\rangle$ were complicated ones. In practice, then, it is essential that we have not merely an exponential separation in one-way communication complexities for a relational problem, but one wherein Bob's measurements are "simple" – which is the content of $\mathsf{FBQP/rpoly} \neq \mathsf{FBQP/qpoly}$.

The detailed consideration of such an experiment is beyond this paper's scope. Briefly, though, laying the groundwork for this experiment would involve refining and improving the $\mathsf{FBQP/rpoly} \neq \mathsf{FBQP/qpoly}$ separation in several ways. Firstly, one would want a separation between randomized and quantum advice length that was as *quantitatively tight* as possible, and that also included concrete bounds for particular small numbers of qubits n, such as 20 or 30. Secondly, one would want to account for the complexity of *preparing* the advice state $|\psi\rangle$: for example, what if we chose $|\psi\rangle = C|0^n\rangle$, where C is a random quantum circuit with m gates? Thirdly, one would, if possible, want the measurements of $|\psi\rangle$ to be *even simpler* than the one from Figure 3, and lower-depth: for example, could one even measure each qubit separately? Fourthly, one would want an analysis that accounted for $|\psi\rangle$ being *extremely noisy* – as it will be, in any near-term implementation – and that carefully quantified the experimental resources needed to achieve a clear separation between randomized and quantum advice length even in the teeth of the noise. See Section 7 for further discussion of these challenges, especially the quantitative tightness one.

Once all the challenges are taken into account, the separation between randomized and quantum information achievable with current devices might be rather modest, as it was in the earlier work by Kumar, Kerenidis, and Diamanti [24]. For example, perhaps it will be possible to perform an experiment with $n \approx 20$ qubits, using 2-qubit gates of 99.8% fidelity or whatever, to verify that any secretly classical description of the qubits' state (even a probabilistic description) would need at least ~ 100 bits, in order to explain the observed success at measuring the state to solve a relational problem. In our view, though, this would already be a historic result, sufficient to disturb the certainty of those who regard the vastness of Hilbert space as just a theoretical fiction. We hope to address some of the challenges in future work.

4 The Power of FBPP

In this section we show several senses in which FBPP behaves differently from its decision-problem counterpart. We start with an unconditional separation between FP and FBPP.

▶ **Theorem 8.** $\mathsf{FP} \neq \mathsf{FBPP}$.

Proof. Recall the definition of Levin's time-bounded Kolmogorov complexity: for a string y,

$$\mathrm{Kt}(y) := \min_{P:P()=y} (|P| + \log_2 t(P)) :$$

that is, we minimize the length of a program P (in some fixed programming language) plus the logarithm of P's runtime, over all programs P that output y given a blank input. Now consider the relation

$$R = \{(x,y) : |x| = |y|, \mathrm{Kt}(y) \geq \frac{|y|}{2}\}.$$

We first show that $R \in \mathsf{FBPP}$. Given an input of length n, the strategy depends on the allowed error probability ε. If $\varepsilon \geq \frac{1}{2^{n/2}}$, then we can simply output a uniformly random $y \in \{0,1\}^n$; a counting argument will then imply that $\mathrm{Kt}(y) \geq \frac{n}{2}$ with probability at least $1-\varepsilon$. If, on the other hand, $\varepsilon < \frac{1}{2^{n/2}}$, then we can use brute force to find and output the lexicographically first string $y \in \{0,1\}^n$ such that $\mathrm{Kt}(y) \geq \frac{n}{2}$. This takes time exponential in n, so polynomial in $\frac{1}{\varepsilon}$.

Next we show that $R \notin \mathsf{FP}$. Let A be a deterministic algorithm with polynomial running time $p(n)$; then for all n, we clearly have

$$\mathrm{Kt}(A(0^n)) \leq |A| + \log_2 n + \log_2 p(n).$$

But the above is less than $\frac{n}{2}$ for all sufficiently large n, which proves that A cannot compute R. ◀

Next we show that the unconditional separation still holds if FP and FBPP both have polynomial-sized advice.

▶ **Theorem 9.** $\mathsf{FP/poly} \neq \mathsf{FBPP/poly}$.

Proof. For each n and $x \in \{0,1\}^n$, choose a subset $S_x \subset \{0,1\}^n$ uniformly at random and independently subject to $|S_x| = 2^{n/2}$. We then define the following relational problem R:

$$R = \{(x,y) : |y| = |x|, y \notin S_x\}.$$

In other words: given as input an n-bit string x, the problem is to output an n-bit string y that is not in S_x.

We first claim that $R \notin \mathsf{FP/poly}$, with probability 1 over the choice of S_x's. This is because, for any fixed $\mathsf{FP/poly}$ algorithm C and any n, we have

$$\Pr_{\{S_x\}_{x\in\{0,1\}^n}}[(x, C(x)) \in R \;\forall x \in \{0,1\}^n] \leq \left(1 - \frac{1}{2^{n/2}}\right)^{2^n} = \frac{1}{\exp(2^{n/2})},$$

which remains small even after we take a union bound over all possible C's.

By contrast, we claim that $R \in \mathsf{FBPP/poly}$. The algorithm is as follows: if $\varepsilon \geq 1/2^{n/2}$, then just output a uniformly random $y \in \{0,1\}^n$. If, on the other hand, $\varepsilon < 1/2^{n/2}$, then the advice string can have size $2^n n = \mathrm{poly}(n, 1/\varepsilon)$, and can therefore just provide a giant list containing some $y \notin S_x$ for each possible $x \in \{0,1\}^n$. ◀

Finally, we give strong evidence that $\mathsf{FBPP} \not\subset \mathsf{FP/poly}$.

▶ **Theorem 6.** *If* $\mathsf{FBPP} \subset \mathsf{FP/poly}$*, then* $\mathsf{PSPACE} \subset \mathsf{NP/poly}$ *(and hence* PH *collapses).*

Proof. We use an idea of Buhrman and Torenvliet [15], which is in turn based on the $\mathsf{IP} = \mathsf{PSPACE}$ theorem and conditional time-bounded Kolmogorov complexity.[8]

Given strings x and y, we define

$$\mathrm{Kt}(y|x) := \min_{P:P(x)=y} (|P| + \log_2 t(P,x)),$$

or the *time-bounded Kolmogorov complexity of* y *conditioned on* x, to be the minimum, over all programs P (in some fixed programming language) such that $P(x) = y$, of the bit-length of P plus the log of its runtime on input x.

We now define the following relation:

$$R^* := \{((x, 0^n), y) : y \in \{0,1\}^n, \mathrm{Kt}(y|x) \geq n/2\}.$$

[8] Buhrman and Torenvliet [15] used these ideas to prove that $\mathsf{PSPACE} \subseteq \mathsf{NP}^{R_s^{CS}}$, where R_s^{CS} is an oracle to decide whether a given string has maximal space-bounded conditional Kolmogorov complexity. We, by contrast, are interested in the nonuniform complexity of *relational* problems. Outputting strings of large time-bounded conditional Kolmogorov complexity is a convenient relational problem for proving the implication we want.

In other words, given as input x (which could have some arbitrary length $m = \text{poly}(n)$) and 0^n, the problem is to output an n-bit string y that cannot be computed too quickly by any short, deterministic program given x.

Our first claim is that $R^* \in \mathsf{FBPP}$. The argument is the same as in the proof of Theorem 8; the fact that we condition on x makes no difference. And so – we save this fact for later – if $\mathsf{FBPP} \subset \mathsf{FP/poly}$, then R^* is also decided by some polynomial-size family of circuits $\{C_{m,n}\}_{m,n\geq 1}$.

We now recall the relevant facts about the proof of $\mathsf{IP} = \mathsf{PSPACE}$ (see [32] for details). Let ϕ be an instance of $TQBF$, the canonical PSPACE-complete problem. Then to verify that $\phi \in TQBF$, the verifier engages the prover in an n-round conversation about a certain complicated (but polynomial-sized) arithmetic expression of the form

$$P = \sum_{x_1\in\{0,1\}} R_{x_1} \prod_{x_2\in\{0,1\}} R_{x_1}R_{x_2} \sum_{x_3\in\{0,1\}} R_{x_1}R_{x_2}R_{x_3} \cdots \prod_{x_n\in\{0,1\}} R_{x_1}\cdots R_{x_n}\varphi(x_1,\ldots,x_n)$$

over the finite field $\mathbb{F}_q$, where we take q to be a prime such that $q > 16^{n^2}$. The expression involves three types of quantifiers over variables: sums, products, and so-called *degree reduction operators* (these are the R_{x_i}'s).

The expression P is constructed by carefully arithmetizing ϕ to maintain the following properties:

1. $P = 1$ if $\phi \in TQBF$ while $P = 0$ if $\phi \notin TQBF$.
2. For any t, if we substitute field values $r_1, \ldots, r_{t-1} \in \mathbb{F}_q$ at the first $t-1$ quantifiers in an appropriate way, remove the t^{th} quantifier, and keep in place everything to the right of the t^{th} quantifier, then we are left with a univariate polynomial $h_t(x_i)$ of degree at most $\text{poly}(n)$ over $\mathbb{F}_q$, where x_i is the variable that appears in the t^{th} quantifier. (The whole purpose of the degree reduction operators is to ensure this.)

The conversation proceeds in $T \leq n^2 + 1$ rounds, one for each quantifier. At round t, the prover sends the verifier a univariate polynomial $g_t : \mathbb{F}_q \to \mathbb{F}_q$, and makes the crucial claim that $g_t = h_t$ as polynomials over $\mathbb{F}_q$, where h_t is the univariate polynomial discussed previously, which depends on the random finite field values $r_1, \ldots, r_{t-1} \in \mathbb{F}_q$ chosen by the verifier in the previous rounds. After applying some preliminary checks, the verifier then tests the prover's claim by choosing a new $r_t \in \mathbb{F}_q$ uniformly at random and sending it to the prover, and the conversation continues. Finally, at the very last round, the verifier can check g_T directly against a polynomial obtained by arithmetizing ϕ.

The key fact is that, by the Fundamental Theorem of Algebra, if $g_t \neq h_t$ as polynomials, then $g_t(r)$ and $h_t(r)$ can coincide on at most $\max\{\deg(g_t), \deg(h_t)\} = n^{O(1)}$ values of r. And these are the only values of $r \in \mathbb{F}_q$ that can cause the protocol to fail at round t (in the sense that the verifier will now accept even though $\phi \notin TQBF$).

For technical reasons to be explained later, let $s \in \{0,1\}^{n^{O(1)}}$ be a polynomial-sized string that is chosen uniformly at random and then fixed.

We now make the following observation: *in place of a uniformly random $r_t \in \mathbb{F}_q$, the verifier could send any $r_t \in \mathbb{F}_q$ such that* $\mathrm{Kt}(r_t | s, \phi, r_1, \ldots, r_{t-1}, g_t) \geq 2n^2$.

To see why, consider a "bad" r_t: that is, one such that $g_t(r_t) = h_t(r_t)$, even though $g_t \neq h_t$ as polynomials. As we said, there can be at most $n^{O(1)}$ such bad r_t's. Furthermore, we claim that the complete list of bad r_t's can be generated in $2^T n^{O(1)}$ time, given ϕ and $s, r_1, \ldots, r_{t-1}$ and g_t as input, with overwhelming probability over the choice of s.

To generate the list, we first compute h_t explicitly as a polynomial over $\mathbb{F}_q$, by simply "brute-forcing" every sum and product over a variable $x_i \in \{0,1\}$ and every degree reduction operator that appears to the right of the t^{th} quantifier. This takes time $2^{T-t} n^{O(1)}$, since we pick up a factor of 2 for every quantifier that needs to be brute-forced. We next factor the polynomial $g_t(r) - h_t(r)$ over the finite field $\mathbb{F}_q$ – for example, by using the randomized algorithm due to Berlekamp [14], which runs in $\mathrm{poly}(n, \log q) = \mathrm{poly}(n)$ time, and which fails with probability at most $1/2^{p(n)}$, where p is a polynomial that we can make as large as needed by choosing a large enough randomness string s to feed to Berlekamp's algorithm. Finally, from the degree-1 irreducible factors of $g_t - h_t$, we extract the solutions $r \in \mathbb{F}_q$ to $g_t(r) = h_t(r)$.

Thus, letting Π be a program that does the above, for any bad r_t, we have

$$\mathrm{Kt}(r_t|s, \phi, r_1, \ldots, r_{t-1}, g_t) \leq |\Pi| + \log_2 \deg(g_t - h_t) + \log_2(2^T n^{O(1)}),$$

which is less than $2T$ for all large enough n and $T \approx n^2$. And so, taking the contrapositive, if r_t has conditional time-bounded Kolmogorov complexity at least $2T$, then it cannot be bad.

But if we set $x := \langle s, \phi, r_1, \ldots, r_{t-1}, g_t \rangle$, then the problem of finding an r_t such that

$$\mathrm{Kt}(r_t|s, \phi, r_1, \ldots, r_{t-1}, g_t) \geq 2T$$

can be solved by finding a $y \in \{0,1\}^{4n^2}$ such that $((x, 0^{4n^2}), y)$ is in the relation R^*. And we said that, by the assumption $\mathsf{FBPP} \subset \mathsf{FP/poly}$, there is a polynomial-size circuit family $\{C_{m,n}\}_{m,n\geq 1}$ that does this.

Hence we can decide $TQBF$ in $\mathsf{NP/poly}$, as follows. Given as input a $TQBF$ instance $\phi(x_1, \ldots, x_n)$, the polynomial-sized advice provides a description of an appropriate circuit $C_{m,4n^2}$, along with a hardwired value for the randomness string s. Given ϕ and given this advice, the NP prover is asked to provide a complete transcript for the $\mathsf{IP} = \mathsf{PSPACE}$ protocol, *assuming that the verifier generates each of its messages using* $C_{m,4n^2}$. Finally, the NP verifier checks each step in this transcript, using C_n to make sure that the prover computed the IP verifier's messages correctly.

By the reasoning above, this derandomization of $\mathsf{IP} = \mathsf{PSPACE}$ is sound: any failure would imply that $C_{m,4n^2}$ had generated a message of small time-bounded conditional Kolmogorov complexity. Or more precisely, this is true with overwhelming probability over the choice of s, which means that there must exist fixed s's that work when hardwired into the advice. Therefore $\mathsf{PSPACE} \subset \mathsf{NP/poly}$ as claimed. ◀

We conclude this section by observing a barrier to any unconditional proof of $\mathsf{FBPP} \not\subset \mathsf{FP/poly}$, as it would lead to new circuit lower bounds.

▶ **Theorem 7.** $\mathsf{FBPP} \subseteq \mathsf{FP}^{\mathsf{PromiseBPEXP}}$. *Hence, if* $\mathsf{PromiseBPEXP} \subset \mathsf{PromiseP/poly}$*, then* $\mathsf{FBPP} \subset \mathsf{FP/poly}$.

Proof. We prove the first part of the theorem; the second part is an immediate consequence. Let $R \in \mathsf{FBPP}$. For simplicity, suppose there exists a polynomial $p(|x|)$ such that for every $(x, y) \in R$, $|y| = p(|x|)$ (which can always be assumed under a suitable efficient encoding).

Let $A(x, 0^{1/\varepsilon})$ be the probabilistic algorithm for computing R with probability at least $1 - \varepsilon$ in time $\mathrm{poly}(|x|, 1/\varepsilon)$. Fix $\varepsilon(|x|) = 4^{-p(|x|)}$.

Let Π be the following promise problem of, given an input (x, z), to decide whether:

(YES) With probability at least $2/3 \cdot 3^{-|z|}$, the prefix of $A(x, 0^{1/\varepsilon(|x|)})$ is $z1$, or

(NO) With probability at most $1/3 \cdot 3^{-|z|}$, the prefix of $A(x, 0^{1/\varepsilon(|x|)})$ is $z1$,

promised that one of (YES) or (NO) is the case.

Observe that $\Pi \in \mathsf{PromiseBPEXP}$: the algorithm runs $A(x, 0^{1/\varepsilon(|x|)})$ on (say) $100^{|z|}$ independent random strings, and outputs YES or NO depending on whether than more than a $1/2 \cdot 3^{-|z|}$ fraction of the strings begin with $z1$. A Chernoff bound guarantees that the algorithm is correct with high probability, so long as (x, z) is in the promise.

Next, we claim that $R \in \mathsf{FP}^{\Pi}$. The algorithm for outputting $(x, y) \in R$ is as follows. Let $z_0 = \emptyset$. For each $i \in p(|x|)$, compute $z_i = z_{i-1}\Pi(x, z_{i-1})$. That is, we obtain z_i by appending 1 to z_{i-1} if the Π oracle answers YES on (x, z_{i-1}), and by appending 0 otherwise. Finally, output $z_{p(|x|)}$.

The correctness of the algorithm follows by observing that after step i of the algorithm, $A(x, 0^{1/\varepsilon(|x|)})$ has probability at least 3^{-i} of outputting a string that starts with z_i. The proof is by induction on i: either (x, z_{i-1}) satisfies the promise, in which case $z_i = z_{i-1}\Pi(x, z_{i-1})$ appears as a prefix with probability at least $2 \cdot 3^{-i}$, or else both $z_{i-1}0$ and $z_{i-1}1$ appear as a prefix with probability at least 3^{-i}. Then, $y = z_{p(|x|)}$ must be a string that $A(x, 0^{1/\varepsilon(|x|)})$ outputs with probability at least $3^{-p(|x|)}$. But since A errs with probability at most $\varepsilon(|x|) = 4^{-p(|x|)}$, we conclude that $(x, y) \in R$. ◀

5 Alternative Error Bounds

In this section, we consider some of the consequences of modifying the error bounds in the definition of FBPP.

Define the class $\mathsf{FBPP}_{\log}$ exactly the same way as FBPP, except that now the algorithm is required to take $\operatorname{poly}(n, \log 1/\varepsilon)$ time rather than merely $\operatorname{poly}(n, 1/\varepsilon)$. In other words, we mandate that the algorithm can reduce the error probability to an exponentially small quantity in polynomial time. Clearly $\mathsf{FP} \subseteq \mathsf{FBPP}_{\log} \subseteq \mathsf{FBPP}$.

As we shall see here, the complexity situation for $\mathsf{FBPP}_{\log}$ differs dramatically from that for FBPP. First, we observe that $\mathsf{FBPP}_{\log}$ *cannot* be unconditionally separated from FP:

▶ **Proposition 20.** *If* $\mathsf{P} = \mathsf{NP}$*, then* $\mathsf{FBPP}_{\log} = \mathsf{FP}$*.*

Proof. Let $R \in \mathsf{FBPP}_{\log}$, and let p be a polynomial such that $|y| \le p(n)$ for all $(x, y) \in R$ with $|x| \le n$. Set $\varepsilon := 1/4^{p(n)}$. Then there exists a randomized algorithm A that, given $x \in \{0,1\}^n$, outputs a $y \in \{0,1\}^{\le p(n)}$ such that $(x, y) \in R$, with success probability at least $1 - \varepsilon$, in $\operatorname{poly}(n, \log 1/\varepsilon) = \operatorname{poly}(n)$ time.

This means that, under the assumption $\mathsf{P} = \mathsf{NP}$ (and hence $\mathsf{P} = \mathsf{PH}$), in FP we can use Stockmeyer approximate counting [33] to find a $y \in \{0,1\}^{\le p(n)}$ such that (say) $\Pr[A(x) = y] \ge \frac{0.1}{2^{p(n)}}$, which must exist by an averaging argument. Such a y must then satisfy $(x, y) \in R$, by the assumption that A succeeds with probability at least $1 - \varepsilon$. ◀

Second, we observe that the analogue of Adleman's Theorem [10] *does* hold for $\mathsf{FBPP}_{\log}$:

▶ **Proposition 21.** $\mathsf{FBPP}_{\log} \subset \mathsf{FP/poly}$.

Proof. Set $\varepsilon := 1/4^n$. Then the $\mathsf{FBPP}_{\log}$ machine takes $\operatorname{poly}(n, \log 1/\varepsilon) = \operatorname{poly}(n)$ time, and we can fix as the $\mathsf{FP/poly}$ advice a single randomness string that works for all inputs $x \in \{0,1\}^n$, which must exist by the union bound. ◀

Combining Proposition 21 with Theorem 6 implies that $\mathsf{FBPP}_{\log} \ne \mathsf{FBPP}$, unless the polynomial hierarchy collapses. To summarize, then, $\mathsf{FBPP}_{\log}$ behaves more like the decision class BPP than it does like FBPP.

A different choice would be to consider $\mathsf{FBPP}_{\mathrm{negl}}$, which we define as the class of all polynomially-bounded relations $R \subseteq \{0,1\}^* \times \{0,1\}^*$ for which there exists a polynomial-time randomized algorithm that, given x, outputs a y such that $(x, y) \in R$ (whenever one exists) with success probability at least $1 - \varepsilon(n)$, for some negligible function $\varepsilon(n) = \frac{1}{n^{\omega(1)}}$.

We have the following unconditional result, which supersedes the analogues of Theorems 6, 8, and 9:

▶ **Theorem 22.** $\mathsf{FBPP}_{\text{negl}} \not\subset \mathsf{FP/poly}$.

Proof. The relation R that witnesses the separation is the same one from the proof of Theorem 9, involving a "bad output set" $S_x \subset \{0,1\}^n$ chosen uniformly at random for each $x \in \{0,1\}^n$ subject to $|S_x| = 2^{n/2}$. We already showed in Theorem 9 that $R \notin \mathsf{FP/poly}$. For $R \in \mathsf{FBPP}_{\text{negl}}$, the algorithm is just to output an n-bit string uniformly at random, independent of x. ◀

What is the relationship between $\mathsf{FBPP}_{\text{negl}}$ and FBPP? In one direction we have:

▶ **Proposition 23.** $\mathsf{FBPP}_{\text{negl}} \not\subset \mathsf{FBPP}$.

Proof. Consider the relation

$$R = \{(x, y) : |x| = |y|, \mathrm{K}(y) \geq \frac{|y|}{2}\},$$

where K is Kolmogorov complexity. We have $R \in \mathsf{FBPP}_{\text{negl}}$ by simply outputting a random string of length $n = |x|$. On the other hand, if R had an FBPP algorithm, then by setting $\varepsilon := 1/4^n$ and then searching for the lexicographically first string that the algorithm output with probability at least (say) $\frac{0.1}{2^n}$, we could deterministically compute an n-bit string such that $\mathrm{K}(x) \geq n/2$, which is impossible. ◀

In the other direction, we leave open whether $\mathsf{FBPP} \subset \mathsf{FBPP}_{\text{negl}}$ or whether the two classes are incomparable. Clearly we do have $\mathsf{FBPP}_{\text{log}} \subset \mathsf{FBPP}_{\text{negl}}$, by setting (say) $\varepsilon = 1/2^n$.

6 Sampling Problems

We now show that the analogue of Theorem 10 is *false* for sampling problems:

▶ **Theorem 16.** $\mathsf{SampBPP/poly} \neq \mathsf{SampBPP/rpoly}$ *and* $\mathsf{SampBQP/poly} \neq \mathsf{SampBQP/rpoly}$.

Proof. Like in Theorem 10, we prove the separation involving FBPP, as the separation involving FBQP is completely analogous. It suffices to choose some family of nonempty sets $S_n \subset \{0,1\}^n$, one for each n. Then consider the problem of outputting a uniformly random element of S_n on input $x \in \{0,1\}^n$. This problem is clearly in $\mathsf{SampBPP/rpoly}$, since we can take the randomized advice itself to be a uniformly random element of S_n. But if the S_n's are chosen uniformly at random, then a counting argument shows that the problem has probability 0 of being in $\mathsf{SampBPP/poly}$. ◀

Lastly, we observe that Theorem 5 gives rise to a separation of sampling classes with randomized and quantum advice:

▶ **Theorem 17.** $\mathsf{SampBQP/rpoly} \neq \mathsf{SampBQP/qpoly}$.

Proof. Consider the problem of sampling from the output distribution of the errorless algorithm that solves the relation problem R_F in the proof of Theorem 5. This sampling problem is in $\mathsf{SampBQP/qpoly}$. On the other hand, if this sampling problem were in $\mathsf{SampBQP/rpoly}$, this would imply $R_F \in \mathsf{FBQP/rpoly}$, because sampling from the distribution within total variation distance ε would solve R_F with probability $1 - \varepsilon$. But this would violate Theorem 5. ◀

7 Open Problems

We gave an example of a relational problem R_F in FBQP/qpoly but not in FBQP/rpoly: indeed, one that is easy to solve using n qubits of quantum advice, but requires $\Omega(2^{n/2})$ bits of classical randomized advice. While this separation is tight for R_F itself, is there a different relational problem, solvable with n qubits of advice, for which the lower bound on randomized advice reaches its maximum of $\Omega(2^n)$?

We note that Montanaro [26] showed in 2019 that $\Omega(2^n)$ bits of classical advice are needed to perform certain sampling tasks, for which n qubits of quantum advice suffice. In the other direction, Gosset and Smolin [20] have shown that, for decision and promise problems solvable with n qubits of quantum advice, $O(2^{n/2})$ bits of classical randomized advice suffice. The case of relational problems remains open. We conjecture that the answer is closer to 2^n than $2^{n/2}$.

As we discussed in Section 3, the gap between 2^n and $2^{n/2}$ would be *extremely* useful to close, as a prerequisite to any possible quantum information supremacy experiment based on the FBQP/rpoly $\neq$ FBQP/qpoly separation. Other complexity results that would bear directly on such an experiment include:

1. a lower bound on the amount of classical randomized advice needed to simulate *noisy* quantum advice for some relational problem – say, as a function of the fidelity δ between the actual advice state and a desired pure state;
2. a quantitative refinement of FBQP/rpoly $\neq$ FBQP/qpoly that took into account the circuit complexity of *preparing* the n-qubit quantum advice state (which, in practice, would likely have to be much less than 2^n); and
3. a reproof of FBQP/rpoly $\neq$ FBQP/qpoly in which the circuit to measure the quantum advice state was made *as simple as possible* – could it even measure each of the n qubits independently from the rest?

Moving on, is there any sense in which FBQP/qpoly contains "more" problems than FBQP/rpoly – i.e., can the classes be separated by counting the number of problems in each?

Can we separate FBQP/qpoly from FBQP/rpoly via an "explicit" problem, rather than relying on the probabilistic method? More concretely: can we show that, under some plausible hardness assumption, there is a relation in (say) FBQP/qpoly $\cap$ FPSPACE that is not in FBQP/rpoly? Such a result would create more "symmetry" between that separation and our FP/poly $\neq$ FP/rpoly separation. For the latter, Theorem 6 gave an explicit relational problem that plausibly realizes the nonconstructively proven separation: namely, the problem of outputting a string of high time-bounded Kolmogorov complexity, conditional on an input string x.

Would FBPP $\subset$ FP/poly have even stronger consequences than PSPACE $\subset$ NP/poly, such as PSPACE $\subset$ P/poly or even EXP $\subset$ P/poly? Also, is there a *relativizing* proof that FBPP $\subset$ FP/poly would have unlikely consequences?

Does $\mathsf{FBPP}_{\log}$ = FP under some plausible derandomization assumption? Is FBPP $\subset$ $\mathsf{FBPP}_{\mathrm{negl}}$? (Recall that $\mathsf{FBPP}_{\log}$ is the subclass of FBPP where we require $\mathrm{poly}(n, \log 1/\varepsilon)$ time to achieve error ε, while $\mathsf{FBPP}_{\mathrm{negl}}$ is the variant where we require only that the error probability be negligible.)

Are there examples of problems in FBPP, FBQP, FP/rpoly, or the other relational classes studied in this paper, for which $\mathrm{poly}(1/\varepsilon)$ (rather than, say, $\mathrm{polylog}(1/\varepsilon)$) running time is actually needed to achieve error ε? (Certainly we've given examples of *reductions* where such running time is needed.) For example, can we show that $\mathsf{FBPP}_{\log} \neq$ FBPP *unconditionally*, without assuming noncollapse of the polynomial hierarchy?

References

1 Scott Aaronson. Limitations of quantum advice and one-way communication. *Theory of Computing*, 1(1):1–28, 2005. doi:10.4086/toc.2005.v001a001.

2 Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. *Proceedings of the Royal Society A*, 461:3473–3482, 2005. doi:10.1098/rspa.2005.1546.

3 Scott Aaronson. BQP and the polynomial hierarchy. In *Proceedings of the Forty-Second ACM Symposium on Theory of Computing*, STOC '10, pages 141–150, New York, NY, USA, 2010. Association for Computing Machinery. doi:10.1145/1806689.1806711.

4 Scott Aaronson. The equivalence of sampling and searching. *Theory of Computing Systems*, 55(2):281–298, 2014. doi:10.1007/s00224-013-9527-3.

5 Scott Aaronson and Andris Ambainis. The need for structure in quantum speedups. *Theory of Computing*, 10(6):133–166, 2014. doi:10.4086/toc.2014.v010a006.

6 Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. *Theory of Computing*, 9(4):143–252, 2013. doi:10.4086/toc.2013.v009a004.

7 Scott Aaronson and Lijie Chen. Complexity-Theoretic Foundations of Quantum Supremacy Experiments. In Ryan O'Donnell, editor, *32nd Computational Complexity Conference (CCC 2017)*, volume 79 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 22:1–22:67, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.CCC.2017.22.

8 Scott Aaronson and Sam Gunn. On the classical hardness of spoofing linear cross-entropy benchmarking. *Theory of Computing*, 16(11):1–8, 2020. doi:10.4086/toc.2020.v016a011.

9 Scott Aaronson and Greg Kuperberg. Quantum versus classical proofs and advice. *Theory of Computing*, 3(7):129–157, 2007. doi:10.4086/toc.2007.v003a007.

10 Leonard Adleman. Two theorems on random polynomial time. In *19th Annual Symposium on Foundations of Computer Science (SFCS 1978)*, pages 75–83, 1978. doi:10.1109/SFCS.1978.37.

11 Dorit Aharonov, Xun Gao, Zeph Landau, Yunchao Liu, and Umesh Vazirani. A polynomial-time classical algorithm for noisy random circuit sampling. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, pages 945–957, New York, NY, USA, 2023. Association for Computing Machinery. doi:10.1145/3564246.3585234.

12 Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fowler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew P. Harrigan, Michael J. Hartmann, Alan Ho, Markus Hoffmann, Trent Huang, Travis S. Humble, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul V. Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, David Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandrà, Jarrod R. McClean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Ostby, Andre Petukhov, John C. Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin J. Sung, Matthew D. Trevithick, Amit Vainsencher, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, and John M. Martinis. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019. doi:10.1038/s41586-019-1666-5.

13 Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing*, STOC '04, pages 128–137, New York, NY, USA, 2004. Association for Computing Machinery. doi:10.1145/1007352.1007379.

14 Elwyn R. Berlekamp. Factoring polynomials over large finite fields. *Mathematics of Computation*, 24(111):713–735, 1970. doi:10.2307/2004849.

15 Harry Buhrman and Leen Torenvliet. Randomness is hard. *SIAM Journal on Computing*, 30(5):1485–1501, 2000. `doi:10.1137/S0097539799360148`.

16 Bill Fefferman and Shelby Kimmel. Quantum vs. Classical Proofs and Subset Verification. In Igor Potapov, Paul Spirakis, and James Worrell, editors, *43rd International Symposium on Mathematical Foundations of Computer Science (MFCS 2018)*, volume 117 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 22:1–22:23, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. `doi:10.4230/LIPIcs.MFCS.2018.22`.

17 Xun Gao, Marcin Kalinowski, Chi-Ning Chou, Mikhail D. Lukin, Boaz Barak, and Soonwon Choi. Limitations of linear cross-entropy as a measure for quantum advantage, 2021. `arXiv:2112.01657`.

18 Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM Journal on Computing*, 38(5):1695–1708, 2009. `doi:10.1137/070706550`.

19 Oded Goldreich. *In a World of P=BPP*, pages 191–232. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011. `doi:10.1007/978-3-642-22670-0_20`.

20 David Gosset and John Smolin. A Compressed Classical Description of Quantum States. In Wim van Dam and Laura Mančinska, editors, *14th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2019)*, volume 135 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 8:1–8:9, Dagstuhl, Germany, 2019. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. `doi:10.4230/LIPIcs.TQC.2019.8`.

21 Alexander S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problems Inform. Transmission*, 9(3):177–183, 1973. Translated from Russian.

22 Rahul Ilango, Jiatu Li, and R. Ryan Williams. Indistinguishability obfuscation, range avoidance, and bounded arithmetic. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, pages 1076–1089, New York, NY, USA, 2023. Association for Computing Machinery. `doi:10.1145/3564246.3585187`.

23 Richard M. Karp and RIchard J. Lipton. Turing machines that take advice. *L'Enseignement Mathématique*, 28:191–209, 1982. `doi:10.5169/seals-52237`.

24 Niraj Kumar, Iordanis Kerenidis, and Eleni Diamanti. Experimental demonstration of quantum advantage for one-way communication complexity surpassing best-known classical protocol. *Nature Communications*, 10(1):4152, 2019. `doi:10.1038/s41467-019-12139-z`.

25 Ryan L. Mann. *Quantum computation and combinatorial structures*. PhD thesis, University of Technology Sydney, February 2019. `doi:10453/133334`.

26 Ashley Montanaro. Quantum states cannot be transmitted efficiently classically. *Quantum*, 3:154, June 2019. `doi:10.22331/q-2019-06-28-154`.

27 Tomoyuki Morimae and Takashi Yamakawa. Quantum advantage from one-way functions, 2023. `arXiv:2302.04749`.

28 Anand Natarajan and Chinmay Nirkhe. A Distribution Testing Oracle Separating QMA and QCMA. In Amnon Ta-Shma, editor, *38th Computational Complexity Conference (CCC 2023)*, volume 264 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 22:1–22:27, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. `doi:10.4230/LIPIcs.CCC.2023.22`.

29 Harumichi Nishimura and Tomoyuki Yamakami. Polynomial time quantum computation with advice. *Information Processing Letters*, 90(4):195–204, 2004. `doi:10.1016/j.ipl.2004.02.005`.

30 OpenAI. GPT-4 technical report, 2023. `arXiv:2303.08774`.

31 Feng Pan, Keyang Chen, and Pan Zhang. Solving the sampling problem of the sycamore quantum circuits. *Phys. Rev. Lett.*, 129:090502, August 2022. `doi:10.1103/PhysRevLett.129.090502`.

32 Adi Shamir. IP = PSPACE. *J. ACM*, 39(4):869–877, October 1992. `doi:10.1145/146585.146609`.

33 Larry Stockmeyer. On approximation algorithms for #P. *SIAM Journal on Computing*, 14(4):849–861, 1985. doi:10.1137/0214060.

34 Yulin Wu, Wan-Su Bao, Sirui Cao, Fusheng Chen, Ming-Cheng Chen, Xiawei Chen, Tung-Hsun Chung, Hui Deng, Yajie Du, Daojin Fan, Ming Gong, Cheng Guo, Chu Guo, Shaojun Guo, Lianchen Han, Linyin Hong, He-Liang Huang, Yong-Heng Huo, Liping Li, Na Li, Shaowei Li, Yuan Li, Futian Liang, Chun Lin, Jin Lin, Haoran Qian, Dan Qiao, Hao Rong, Hong Su, Lihua Sun, Liangyuan Wang, Shiyu Wang, Dachao Wu, Yu Xu, Kai Yan, Weifeng Yang, Yang Yang, Yangsen Ye, Jianghan Yin, Chong Ying, Jiale Yu, Chen Zha, Cha Zhang, Haibin Zhang, Kaili Zhang, Yiming Zhang, Han Zhao, Youwei Zhao, Liang Zhou, Qingling Zhu, Chao-Yang Lu, Cheng-Zhi Peng, Xiaobo Zhu, and Jian-Wei Pan. Strong quantum computational advantage using a superconducting quantum processor. *Phys. Rev. Lett.*, 127:180501, October 2021. doi:10.1103/PhysRevLett.127.180501.

35 Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 69–74, Los Alamitos, CA, USA, November 2022. IEEE Computer Society. doi:10.1109/FOCS54457.2022.00014.

36 Andrew Chi-Chih Yao. Probabilistic computations: Toward a unified measure of complexity. In *18th Annual Symposium on Foundations of Computer Science (SFCS 1977)*, pages 222–227, 1977. doi:10.1109/SFCS.1977.24.