Taming Quantum Amplitudes with Gateset Limitations

Ross Rheingans-Yoo
Harvard School of Engineering and Applied Sciences, Cambridge, MA (USA)
rry@eecs.harvard.edu / ross@r-y.io

Note: *This is a work in progress; the version hosted at this address is liable to change without notice or record. This version has been modified from an assignment submitted for credit at MIT in December 2014. Any definitive and stable version will lack this notice.*

***Abstract*—Previous work by Aaronson[1] and others has established the complexity class PostBQP, the class of problems efficiently solvable (with bounded error) by a quantum computer, given the ability to "postselect" on the outcomes of subpolynomial measurements. Recent work by Kuperberg[2] has revealed desirable refinements to the original formulation of the class, namely, the restriction of the power of postselection to outcomes of probability $\Omega(\exp(-\textbf{poly}(n)))$. We survey results bounding, for particular gatesets, the rate at which amplitudes shrink asymptotically in number of gates applied. Most relevantly for PostBQP, we survey several sufficient conditions on a gateset Γ for $\mathsf{PostBQP}_\Gamma = \mathsf{PostBQP}$ (especially regarding Aaronson's formulation of 'tameness'), compare the essential ideas of certain extant proofs of a central relevant theorem in tameness, and provide minor results concerning the rate at which amplitudes shrink while applying known-to-be-tame gates after a constant number of not-known-to-be-tame ones. In this latter paradigm, we find that 'most' gates do not create fast-shrinking amplitudes after only a constant number of applications.**

I. Context and Related Work

'Postselection' is a hypothetical power in probabilistic computing, allowing one to discard all runs of a computation in which a given (random) event does not occur. It was introduced by that name in a 2005 paper by Aaronson[1], who proposed it as a way to ask about the power of quatum computation under slightly different quantum mechanics (as, say, a way of understanding where *exactly* 'the power of quantum computation comes from'), but who later also proved it classically useful when he demonstrated in the same paper $\mathsf{PostBQP} = \mathsf{PP}$, and, as a corollary, a simple proof that PP was closed under intersection.

Others have used expanded upon the concept of postselection, either applying it to other complexity classes than BQP[3], or by using $\mathsf{PostBQP} = \mathsf{PP}$ as a Rosetta Stone of sorts, to translate certain quantum results into *e.g.* the implied collapse of the polynomial hierarchy under certain hypotheses[4][5].

Unfortunately, recent work by Kuperberg revealed certain unjustified assumptions in Aaronson's original formulation[2], most notably the assumption of gateset-independence. By way of resolution, Kuperberg has proposed that we use "PostBQP" to refer to the class with postselection limited to outcomes with probability of occurrence $\Omega(\exp(-\text{poly}(n)))$; with this formulation, Aaronson's original proofs of, *inter alia*, $\mathsf{PostBQP} = \mathsf{PP}$ are valid as stated. However, it is currently an open problem whether or not the ability to postselect on sub-singly-exponential outcomes creates a separably *stronger* complexity class than the one obtained with this restriction, and we have no definitive results on this question to present (beyond the mention here of an obvious oracle relative to which separation can be demonstrated).

We will, however, survey the work of Kuperberg and others on the question of whether we can prevent the occurrence of *any* possible outcomes of probability $o(\exp(-\text{poly}(n)))$ by suitable restriction on the gateset, thus allowing, within PostBQP, postselection on any *nonzero* outcome, since such outcome will necessarily have probability $\Omega(\exp(-\text{poly}(n)))$. We present Aaronson's formulation of 'tameness', a useful such characterization in terms of the set of transition amplitudes, in section III (we also provide our own formulation of

'very-tame-ness', which captures most known cases of tameness with a tighter bound), and in section IV provide a few illustrative examples of very tame, tame and non-tame sets. In section V, we provide an exposition of Kuperberg's main result on the tameness of algebraic sets, as well as alternative proofs expressing the same concepts in the language of other mathematical fields.

We present new formulations of tameness in the language of transcendence theory (*i.e.* transcendental number theory) in section VI, along with minor novel results regarding not-known-to-be-tame numbers (or, alternatively, gates) which do not allow for non-tame blowups when applied a constant number of times amid many applications of others known to be tame. In section VII, we list a few questions which remain open.

II. Tameness: A Mathematical Formulation

This formulation of 'tameness' was proposed by Aaronson on MathOverflow[6]. The addition of 'very tame' is ours.

Let $A := a_1, \ldots, a_r$ be a fixed, finite set of Real $a_i \in [-1, 1]$. Such a set 'expresses' ('in n applications') the elements of the set

$$S_A(n) := \left\{ \sum_j^{2^n} \prod_k^n a_{i_{(j,k)}} \;\middle|\; a_{i_{(j,k)}} \in A\,\{-1, 0, 1\} \right\}, \tag{1}$$

i.e. 2^n-sums of n-products of arbitrary $a_i \in A \cup \{-1, 0, 1\}$. (Including $0, 1$ allows our sums and products to be "up to…" without loss of generality.) We're particularly interested in the smallest-absolute-value nonzero A-expressible number:

$$d_A(n) := \min_{x \in S_A^*(n)} \{|x|\}, \tag{2}$$

(where $S_A^*(n) := S_A(n) \backslash \{0\}$) and in particular, just how quickly it shrinks as n increases (asymptotically speaking). In particular, it will be useful to discuss the quantity $-\log d_A(n)$ as a function $f_A : \mathbb{N} \to \mathbb{R}$:

$$f_A(n) := -\log d_A(n). \tag{3}$$

Definition. We say that a set A is *tame* iff $f_A(n) = O(\text{poly}(n))$, and *non-tame* otherwise. Iff $f_A(n) = O(n)$, we say A is *very tame*.

Tameness is of interest primarily because it is a sufficient condition for $\mathsf{PostBQP}_\Gamma = \mathsf{PostBQP}$ that

$$A_\Gamma := \{a \mid a \text{ is a transition amplitude of a gate } g \in \Gamma\} \tag{4}$$

is tame.

III. Examples of (Non-)Tameness

In this section, we give a few illustrative examples of very tame, tame and non-tame A.

A. $A = \{1/2\}$ *(very tame)*

Let $A := \{1/2\}$. Then any $\prod_k^n a_{i_{(k)}}$ takes the form $2^{-\ell}$ for some $\ell \leq n$, and elements of $S_A(n)$ take the form $h/2^\ell$ for $\ell \leq n$. The minimal number of this form is

$$d_A(n) = 1/2^n = 2^{-n}, \tag{5}$$

so $f_A(n) = n$, and A is very tame.

B. $A \in \mathbb{Q}^r$ *(very tame)*

Let $A := \{a_1, \ldots, a_r\} = \{p_1/q_1, \ldots, p_r/q_r\}$, with $p_i, q_i \in \mathbb{Z}$. Then any $\prod_k^n a_{i_{(k)}}$ takes the form

$$\prod_k^n a_{i_{(k)}} = \frac{\prod_k^n p_{i_{(k)}}}{\prod_k^n q_{i_{(k)}}} = \frac{\prod_i^r p_i^{e_i}}{\prod_i^r q_i^{e_i}} \tag{6}$$

for some e_i such that $\sum_i e_i = n$, and elements $s \in S_A(n)$ take the form

$$s = \sum_j^{2^n} \prod_k^n a_{i_{(j,k)}} = \sum_j^{2^n} \frac{\prod_i^r p_i^{e_{j,i}}}{\prod_i^r q_i^{e_{j,i}}} = \frac{h}{\prod_i^r q^{\max_j e_{j,i}}}, \tag{7}$$

where h is some polynomial in $\mathbb{Z}[x_i, y_i]$. Note that $\forall i, \max_j e_{j,i} \leq n$; then the least nonzero element is bounded below by letting $h = 1$ and every $\max_j e_{j,i} = n$:

$$d_A \geq \frac{1}{\prod_i^r y^n} = 2^{-n \sum_i^r \log y_i}, \tag{8}$$

so $f_A(n) \leq n \sum_i^r \log y_i = O(n)$, and A is very tame.

C. Arbitrarily non-tame A

A particular case of this construction was given by Achinger on MathOverflow[7] in response to Aaronson's question, demonstrating the existence of non-tame A. The simple generalization to 'arbitrarily non-tame' A is ours.

Claim III.1. *Let $g : \mathbb{N} \to \mathbb{N}$ be some abritrary function (for convenience, we will assume $g(n) > n$). Then there is an A such that $f_A(n) \neq O(g(n))$.*

Consider, for this purpose, $A = \left\{1/2, \sum_i 2^{-G(i)}\right\}$, where $G(0) := 1$ (or any appropriate initial condition) and $G(n+1) := g(G(n))$. Then, at least for $n \in G(\mathbb{N})$,

$$\begin{aligned} d_A(G(n)) &\leq \sum_i 2^{-G(i)} - \sum_i^n 2^{-G(i)} \\ &= \sum_{i=n+1} 2^{-G(i)} \\ &\leq 2 \cdot 2^{-G(n+1)} \\ &= 2 \cdot 2^{-g(G(n))}, \end{aligned} \tag{9}$$

so $f_A(n) \geq g(n) - 1$ whenever $n \in G(\mathbb{N})$, and, since $G(\mathbb{N})$ includes arbitrarily large elements whenever $g = \Omega(n)$, $f_A(n) \neq O(g)$.

Letting $g(n) := 2^n$, then, we show that there exist non-tame A.[1] Such constructions, which for $g(n) = \omega(n)$ involve a necessarily transcendent second element, have interpretations in transcendence theory, which are discussed in section VI below.

IV. Algebraic Results

Having observed the existence of both tame and arbitrarily non-tame A, the natural next question is: "What conditions on the a_i are necessary or sufficient for the tameness of A?" In this section, we survey three extant proofs of the tameness of algebraic sets, *i.e.* the following theorem:

Theorem IV.1. (Algebraic Tameness Theorem) *Let $A := \{a_1, \ldots, a_r\}$, with all a_i algebraic. Then A is very tame.*

By examples above, this bound is tight.

Unsurprisingly, the three proofs discussed are effectively equivalent from a sufficiently general perspective, and follow the basic form:

- Let our a_i generate some finite algebraic field extension $K \supseteq \mathbb{Q}$.
- Bound below the quantity

$$\prod_{\sigma_i : K \hookrightarrow \mathbb{C}} |\sigma_i s|_{\mathbb{C}}\,, \tag{10}$$

  where s is the amplitude under investigation and σ runs over the embeddings $K \hookrightarrow \mathbb{C}$.
- Bound above the $|\sigma_i s|_{\mathbb{C}}$, similarly bounding below each (but most importantly for our purposes, the natural embedding).

For readers who prefer explicit formalizations in one theory or another, we survey three different formulations of the proof, which express the above idea in the language of valuation theory, linear algebra, and Galois theory, respectively. But first, a short note about the theorem's implications:

A. Applications of the Algebraic Tameness Theorem

Since the Hadamard and Toffoli gates exhibit only algebraic transition amplitudes (namely $\{0, 1, 1/\sqrt{2}\}$), no possible outcome of a Hadamard-Toffoli circuit is less likely than $\Omega(2^{-n})$. So $\mathsf{PostBQP}_{\{\mathrm{H,CCNOT}\}} = \mathsf{PostBQP}$, for PostBQP as refined by Kuperberg[2]. Since $\{\mathrm{H}, \mathrm{CCNOT}\}$ is universal for PostBQP, this implies, speaking colloquially, that any postselection algorithm that isn't making explicit use of gateset peculiarities should be no stronger than PostBQP.

B. Proof In Valuation Theory, by Rosen

This proof was provided by Rosen on MathOverflow[8] in response to Aaronson's question. Proofs of certain elementary lemmas, or surveys of such proofs provided elsewhere, are ours.

Let $A := \{a_1, \ldots, a_r\}$ be a finite set of algebraic numbers, and let $K := \mathbb{Q}(a_1, \ldots, a_r)$ be a number field containing them (along with, necessarily, all rationals). Then a standard result in valuation theory (proved in Appendix A) is

$$\forall x \in K^*, \prod_v |x|_v = 1 \tag{11}$$

$$\sum_v \log |x|_v = 0, \tag{12}$$

where v runs over (normalized) places on K. Then, letting v_0 be the place from the natural embedding

[1] Letting $g(n) := n^2$, by contrast, we find a not-very-tame A. If, as we suspect but cannot here prove, the bound on this A is tight, it gives the example of a tame A which is not very tame.

of K in $\mathbb{R}$, *i.e.* the absolute value of an element so embedded, we see

$$-\log|x|_{v_0} = \sum_{v\neq v_0} \log|x|_v \tag{13}$$

and so, we can bound above the left side by bounding above the right.

Considering $|a_i|_v$ for fixed $\left\{a_i = \frac{p_i}{q_i}\right\}$ (with relatively prime $p_i, q_i \in \mathbb{Z}[\alpha_1, \ldots, \alpha_s]$ for suitable independent algebraic roots α_j) over non-Archimedian places v, we see

$$|a_i|_v > 1 \iff v\big|q_i, \tag{14}$$

and so, since q_i has a finite set of divisors, there exists a finite set of places $P_{a_i} := \left\{z \in K^* \;\middle|\; z\big|q_i\right\}$ such that

$$v \in P_{a_i} \iff \log|a_i|_v > 0. \tag{15}$$

Then, seeing that

$$\begin{aligned}\log\left|\prod_k^n a_{i_{(k)}}\right|_v &= \log\prod_k^n \left|a_{i_{(k)}}\right|_v \\ &= \sum_k^n \log\left|a_{i_{(k)}}\right|_v,\end{aligned} \tag{16}$$

we conclude

$$\log\left|\prod_k^n a_{i_{(k)}}\right|_v > 0 \iff v \in \bigcup_i^s P_{a_i}. \tag{17}$$

Defining $P_A := P_{\text{arch}} \cup \bigcup_i^s P_{a_i}$ (which is finite, since the finiteness of the extension implies finiteness of P_{arch}), we see

$$\log\left|\sum_j^{2^n}\prod_k^n a_{i_{(j,k)}}\right|_v > 0 \iff v \in P_A, \tag{18}$$

and so reduce the infinite-sum bound above to the finite-sum bound

$$-\log|x|_{v_0} \leq \sum_{v\in P_A^*} \log|x|_v, \tag{19}$$

where $P_A^* := P_A \setminus \{v_0\}$.

Since, for fixed v, $\log \max_{x\in S_A(n)} \{|x|_v\} = O(n)$ (proof in Appendix B), we see

$$\begin{aligned} f_A(n) &= \max_{x\in S_A(n)} \left\{-\log|x|_{v_0}\right\} \\ &\leq \max_{x\in S_A(n)} \left\{\sum_{v\in P_A^*} \log|x|_v\right\} \\ &\leq \sum_{v\in P_A^*} \max_{x\in S_A(n)} \{\log|x|_v\} \\ &\leq |P_A^*|\, O(n) \\ &= O(n). \end{aligned} \tag{20}$$

C. Proof In Linear Algebra, by Sawin

This proof was provided by Sawin on MathOverflow[9] in response to Aaronson's question.

The abstract-algebraic ideas of Rosen's proof can be expressed in linear-algebraic terms, for readers who find such formulations more intuitive:

Consider the d-degree field extension $K = \mathbb{Q}[\alpha_1, \ldots, \alpha_s] \supseteq \mathbb{Q}$ as a d-degree vector space over $\mathbb{Q}$; then we can express multiplication by any $x \in K$ as an operator linear in the basis elements, so linear $K \to K$. So identify it with a matrix with entries in $\mathbb{Q}$ and note that the natural real absolute value of an element is given by the eigenvalue corresponding to the eigenvector $(|e_1|_{\sigma_0}^{-1}, \ldots, |e_d|_{\sigma_0}^{-1})$, where $|e_1|_{\sigma_0}$ is the real absolute value of $(1, 0, \ldots, 0)$ and $|e_d|_{\sigma_0}$ is the real absolute value of $(0, \ldots, 0, 1)$, *etc.*

NB: The essential relation to Kuperberg's proof (below, in V.D) here is that the other eigenvectors are similarly of the form $(\ldots, |e_i|_{\sigma_j}^{-1}, \ldots)$, for σ_j some other embedding $K \hookrightarrow \mathbb{C}$, and the determinant, naturally, is their product.

We quote the remainder of Sawin's proof:

> We can lower bound it by lower bounding the determinant and upper bounding the other eigenvalues. Observe:
>
> The entries grow at most exponentially, so the other eigenvalues grow at most exponentially. Because the number field is a field, the element is invertible, so the determinant is nonzero. The denominators of the entries grow at most exponentially, so the denominator of the determinant grows at most exponentially.

Then you get a lower bound on one eigenvalue by division and the fact that the numerator of the determinant must be at least 1.[9]

D. Proof in Galois Theory, by Kuperberg

This proof is given by Kuperberg[2]. His proof is more succint, but we are slightly more careful here to prove very-tame-ness where he only proved tameness.

Given a n-degree $\mathbb{Q}$-polynomial in r algebraic variables a_i (which together generate a finite extension $K \supset \mathbb{Q}$ of degree d), we have by the Primitive Element Theorem of Galois that K has some primitive root α, *i.e.* each a_i is epxressible as some d-degree polynomial $q_i(\alpha)$. So it suffices to consider $r = 1$ (and, say, $a_1 = \alpha$), n increasing only by a linear factor of d.

Then let $\alpha_2, \ldots, \alpha_d$ be distinct Galois conjugates of α (*i.e.* replacing α with one of them gives us a different embedding $K \hookrightarrow \mathbb{C}$). Note then that each $|p(\alpha_i)|$ is bounded above by $|\alpha_i|^n 2^n P_{\max}$, for $P_{\max}$ the largest coefficient in p, itself bounded by $(Q_\Sigma^n 2^n)$, for Q_Σ the sum of all coefficients in the q_i above.

The product

$$q'\left(\frac{x_1}{y_1}, \ldots, \frac{x_d}{y_d}\right) := \prod_i^d p(\alpha_i) \tag{21}$$

is some rational polynomial of degree $d\deg(p)$ in $\frac{x_1}{y_1}, \ldots, \frac{x_d}{y_d}$ the rational coordinates of α; since the arguments are fixed, we can bound it below (in absolute value) by $\left(\prod_i^d y_i\right)^{-n} P_{\text{lcm}}$ for P_{lcm} the least common multiple in the denominators of the coefficients in p, itself bounded below by $(Q_{\text{lcm}})^{-n}$, for Q_{lcm} the least common multiple of all coefficients in the q_i above.

So, for some p of degree n, we bound $|p(\alpha)|$ below by $2^{\Omega(n)}$ with the bounds

$$\left|\prod_i^d p(\alpha_i)\right| = 2^{\Omega(n)} \tag{22}$$

$$\forall i, |p(\alpha_i)| = 2^{O(n)}. \tag{23}$$

V. Transcendence Results

A. A Brief Layover in Liouville

A *Liouville number* α has the property

$$\forall r, \exists p/q \in \mathbb{Q} : \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^r}; \tag{24}$$

in fact, this $\exists$ finds infinitely many distinct p/q (Proof: Note that any particular p/q approximates only to q^{-R} only for some finite R, and take the p'/q' given for $r = R + 1$. Repeat.), and we call this ability to be approximated to within q^{-r} by infinitely many p/q "r-approximability". Similarly, non-Liouville numbers β can be assigned a finite *irrationality coefficient* $\mu(\beta) \in \mathbb{R}_+$ by

$$\mu(\beta) := \inf\{r \in \mathbb{R}_+ \mid \alpha \text{ is } r\text{-approximable}\}. \tag{25}$$

(It is conventional to assign Liouville numbers α an irrationality coefficient of ∞.)

It follows readily that $p/q \in \mathbb{Q} \implies \mu(p/q) = 1$, and the Thue-Siegel-Roth Theorem states that β is algebraic $\implies \mu(\beta) = 2$. Note, however, that this is not biconditional—there are transcendental γ such that $\mu(\gamma) = 2$, and in fact, $\{\gamma \in \mathbb{R} \mid \mu(\gamma) > 2\}$ is a set of measure zero in $\mathbb{R}$.

B. Applied Irrationality

In demonstrating the existence of arbitrarily non-tame A above, we saw that, by using only a single application of one transcendent gate and several applications of a rational one—a small piece of the expressivity of our sum-product form—we could produce amplitudes which shrank arbitrarily fast. Thus inspired, we define

$$d_a^\alpha(n) := \min((\alpha S_{\{a\}}(n) + S_{\{a\}}(n)) \setminus \{0\}) \tag{26}$$

$$f_a^\alpha(n) := -\log d_\alpha^a, \tag{27}$$

which denotes the minimal amplitude (or the logarithm of its shrinkage) after one application of the α gate and n applications of the a gate. A little more suggestively, we attempt to capture whether a number has an 'bounded' or 'unbounded' amount of non-tameness by considering whether or not a single application can make otherwise tame numbers non-tame, even as the fraction of otherwise-tame numbers applied approaches 1 without bound.

Definition. We say that a number α is *safe* (for one application) iff $f_A^\alpha(n) = O(\text{poly}(n))$ for any

algebraic[2] A, and *non-safe* otherwise. Iff $f_A^\alpha(n) = O(\text{poly}(n))$, we say α is *very safe*.

In general, $f_{\{a,\alpha\}} = \Omega(f_a^\alpha)$, and our results from section IV above can be written thus

$$f_A = \Omega\left(f_{1/2}^{\left(\sum_i 2^{-G(i)}\right)}\right) \neq O(g). \tag{28}$$

i.e. there exist α which are arbitrarily unsafe, even for a single application.

We also have the theorem:

Theorem V.1. $f_{1/2}^\alpha(n) \neq O(n^{1+\epsilon}) \implies \mu(\alpha) = \infty$.

Corollary V.1. $\mu(\alpha) < \infty \implies f_{1/2}^\alpha(n) = \widetilde{O}(n)$.

(proved in Appendix C) So safeness is a more general condition than non-Liouville-ness—that is, while our examples of non-safeness involve an application of some Liouville α and its approximation by dyadics, the Liouville-ness of α is insufficient to produce non-safeness, and in 'most' cases only produces non-very-safeness. Note, however, that safeness is also a more general condition than tameness, so this result does not resolve whether tameness is or more or less general than non-Liouville-ness.

At a minimum, though, it *does* imply that several constants of known-bounded irrationality[10] are safe for at least one application, including e^{-1}, π^{-1}, π^{-2}, $(\ln 2)^{-1}$, $(\ln 3)^{-1}$, $(\zeta_3)^{-1}$, after noting that the Liouville-Roth coefficient is invariant under Möbius transforms[11].

C. Unsafe Unions

Unforuntately, this result (that non-Liouville-ness of α guarantees very-safeness) is not robust under the obvious set-union. If we take α, β such that $f_{1/2}^\alpha(n), f_{1/2}^\beta(n) = O(n)$, it is nevertheless possible for $f_{1/2}^{\alpha,\beta}$ (defined with one application *each* of α, β and n applications of $1/2$) to grow arbitrarily quickly!

Example. Fix some arbitrarily-unsafe γ (say, $:= \sum_i 2^{-G(i)}$ for some fast-growing g), and consider (α, β) of the form $(\alpha, \gamma - \alpha)$. Since α with $\mu(\alpha) > 2$ have measure zero in $\mathbb{R}$, so too does $\{\alpha \in \mathbb{R} \mid \mu(\alpha) > 2 \text{ or } \mu(\gamma - \alpha) > 2\}$; so both elements of this tuple have $\mu(*) = 2$ for almost all α—it follows that $f_{1/2}^\alpha(n), f_{1/2}^\beta(n) = O(n)$. But $\gamma = \alpha + \beta$ by construction, so $\gamma \in S_{1/2}^{\alpha,\beta}(n)$, so $f_{1/2}^{\alpha,\beta}(n) \neq O(g)$.

This construction, interestingly enough, works even if:

- the only gates corresponding to α and β are applied once each on (at the time) unentangled registers (using the above $(\alpha, \gamma - \alpha)$),
- the only gates corresponding to α and β are single-wire gates applied once each, immediately after one another on the same wire (using $(\alpha, \gamma/\alpha)$ with similar measure-theoretic proof).

D. Recovering the Single-α Case for (Constant) Multiple Applications

So two gates which are (very) safe individually can be combined to produce a set which is arbitrarily non-safe after only a single application of each—can the same be true of a (very) safe gate and *itself*? *i.e.* slightly more generally: if α is safe for a single application, is it safe for some constant number of applications? In terms of transcendence theory, we might make the following conjectures:

Conjecture V.1. *(Weak Form)* $\mu(\alpha) < \infty \implies \mu(p(\alpha)) < \infty$*, for any polynomial* p*.*

Conjecture V.2. *(Strong Form)* $\mu(\alpha) \geq \mu(p(\alpha))$*, for any polynomial* p*.*

This says, intuitively, that we cannot make a number 'more irrational' by mapping it by some polynomial. (The version restricted to algebraic and rational numbers is quite obviously true.) The disproofs of additive and multiplicative closure in general don't apply here to, say, tuples $(\alpha, p(\alpha))$, as they require enforcing a different dependence between the elements than the algebraic one requested here. However, we do not at this time have a proof; see VI.E for the best alternative we are prepared to present.

E. The Single-α Case in Probability

Theorem V.2. *For a real* α *chosen uniformly at random on some interval, with probability 1,* $\mu(p(\alpha)) \leq 2$ *for all finite-degree polynomials* p *with algebraic coefficients.*[3]

[2] We might instead define this for *tame* A, but it is unclear at this time how and if that condition differs from algebraicity, and in any case, we find things easier to prove in this formulation, the existence of which is otherwise only conjectured.

[3] Obviously, the stronger statement of this theorem is $\mu(p(\alpha)) \leq 2$; here we express it as an upper bound for clarity.

Corollary V.2. *The theorem holds for real α chosen at random from any uniformly continuous distribution on $\mathbb{R}$.*

The corollary means, among other things, that if we choose an angle θ uniformly at random from some interval, and let $a_1, \ldots, a_r$ be algebraics, then $\sin\theta$ is, with probability 1, very safe for any constant number of applications.

In fact, they both generalize to the s-dimensional case:

Theorem V.3. *For a real $(\alpha_1, \ldots, \alpha_s)$ chosen uniformly at random on $[0,1]^s$, with probability 1, $\mu(p(\alpha_1, \ldots, \alpha_s)) \leq 2$ for all finite-degree polynomials p with algebraic coefficients.*

Corollary V.3. *The theorem holds for vectors chosen at random from any uniformly continuous distribution on $\mathbb{R}^s$.*

Here we prove the first theorem; we'll address its extensions to the other claims in Appendix D.

Outline of proof: It suffices to consider nonconstant algebraic-coefficient polynomials, of which there are only countably many. For each such p, each $z \in \mathbb{R}$ is expressible as $p(x)$ for only finitely many distinct x. So the set of x which can be mapped into some y with $\mu(y) > 2$ is the sum of at most countably many images of $\{y \mid \mu(y) > 2\}$ under almost everywhere absolutely continuous mappings, and so has measure zero.

Proof. It suffices to consider nonconstant algebraic-coefficient polynomials, of which there are only countably many. (Recall that there are only countably many algebraic numbers.) For each such p_i and arbitrary $c \in \{1, \ldots, |p_i|\}$, define $q_{i,c}$:

$$q_{i,c}(y) := \left(p^{-1}(y)\right)_{\min\{c, \#p^{-1}(y)\}}, \tag{29}$$

i.e. the inverse of $p^{-1}(y)$ at points where the preimage has only 1 point, and at all others either the cth-least preimage point, or the greatest preimage point (if c is greater than the cardinality of the preimage). Such functions are almost everywhere absolutely continuous. Then, if $y = p_i(x)$ for some p_i, we have $q_{i,c}(y) = x$ for some c. So define B:

$$B := \bigcup_i \bigcup_c^d q_{i,c}\left\{y \mid \mu(y) > 2\right\}, \tag{30}$$

the set of points which are mapped into some y with high Liouville-Roth coefficient by some algebraic-coefficient polynomial of degree $\leq d$. Then, since the latter set has measure zero, it is mapped by each (a.e.a.c.) q to a set of measure zero, and the union-set has measure zero by the countable subadditivity of measure. □

VI. Still-Open Questions

While PostBQP is not really new, the restriction of postselection to outcomes of probability $\Omega(\exp(-\text{poly}(n)))$ is. Various questions remain open, which we present here by way of conclusion, without commentary:

- Are there gatesets Γ for which $\mathsf{PostBQP}_\Gamma \supsetneq \mathsf{PostBQP}$?
- Are there reasonable gatesets with non-tame transition amplitudes which are nonetheless tame? (*i.e.* when actually built into circuits)
- Are there sufficient conditions for tameness more general than algebraicity?
- Are there useful nonobvious conditions for safeness? (either in one or multiple α_i)
- Conjectures VI.1 and VI.2: Does safeness for one application imply safeness for d applications?
- Are there useful generalizations of safeness to *e.g.* safeness for $\log n$ applications?
- What further quantum-algorithmic questions rely on answers to these questions in tameness/safeness?

Acknowledgements

The author would be much remiss not to acknowledge the assistance of Scott Aaronson, of MIT, for guidance in research, assistance in developing the vocabulary of tameness, and willingness to publish this project on his blog[4]; Benedict Gross, of Harvard, for helpful explanations of, and pointers in, algebraic number theory; Noam Elkies, also of Harvard, for numerous counterexamples and for making clear the usefulness of measure theory; and Joshua Zelinsky, student at BU, for generous effort correcting mathematical and notational errors in early drafts.

[4] Quantum Complexity Theory Student Project Showcase 3. *Shtetl-Optimized* http://www.scottaaronson.com/blog/?p=2109

APPENDIX A
PROOF: PRODUCT RULE ON VALUATIONS

Proposition A.1. *Let K be a finite extension of $\mathbb{Q}$. Then $\forall x \in K, \prod_v |x|_v = 1$, letting v run over the (normalized) valuations of primes on K.*

We begin by proving the case $K = \mathbb{Q}$:

Lemma A.1. $\forall x \in \mathbb{Q}, \prod_v |x|_v = 1$.

Proof. Note that this product formula is a homomorphism over multiplication, *i.e.* that

$$\prod_v |xy|_v = \left(\prod_v |x|_v\right)\left(\prod_v |y|_v\right), \tag{31}$$

so it suffices to prove the claim for prime and unit x. Note then that, on units,

$$\prod_v |x|_v = \prod_v 1 = 1 \tag{32}$$

and on primes,

$$\begin{aligned}\prod_v |x|_v &= |x|_x \cdot |x|_\infty \cdot \prod_{v\notin\{x,\infty\}} |x|_v \\ &= x^{-1}\cdot x \cdot \prod_{v\notin\{x,\infty\}} 1 \\ &= 1,\end{aligned} \tag{33}$$

as desired. □

We then proceed to prove the original proposition for general K a finite extension of $\mathbb{Q}$.

Proof.

$$\begin{aligned}\prod_{v\in\text{val}(K)} |x|_v &= \prod_{p\in\overline{\text{Spec}}(K)} |x|_p \\ &= \prod_{q\in\overline{\text{Spec}}(\mathbb{Q})} \left|\|x\|_{K/\mathbb{Q}}\right|_q^{1/[K:\mathbb{Q}]} \qquad (*) \\ &= \left(\prod_{q\in\overline{\text{Spec}}(\mathbb{Q})} \left|\|x\|_{K/\mathbb{Q}}\right|_q\right)^{1/[K:\mathbb{Q}]} \\ &= \left(\prod_{v\in\text{val}(\mathbb{Q})} \left|\|x\|_{K/\mathbb{Q}}\right|_q\right)^{1/[K:\mathbb{Q}]} \\ &= 1^{1/[K:\mathbb{Q}]} \qquad \text{(by 32)} \\ &= 1\end{aligned} \tag{34}$$

$*$: *The second step follows from the definition of* $\|\cdot\|_{K/\mathbb{Q}}$:

$$\|x\|_{K/\mathbb{Q}} := \prod_{\sigma_i : K\hookrightarrow\mathbb{C}} |\sigma_i x|_{\mathbb{C}}\,, \tag{35}$$

which should be reminiscent of the other proofs above. Readers seeking a deeper understanding of the details should refer to a text in algebraic number theory. We consulted lecture notes from Milne's course at Michigan[12] for this purpose. □

APPENDIX B
PROOF: $|x^n|_v = 2^{O(n)}$

For any fixed v, we note the bound $\log \max_{x\in S_A(n)} \{|x|_v\} = O(n)$ in both the Archimedian case:

$$\begin{aligned}s \in S_A(n) \implies \log|s|_v &= \log\left|\sum_j^{2^n}\prod_k^n a_{i_{(j,k)}}\right|_v \\ &\le \log 2^n \left|\prod_k^n \max_j{}^{|\cdot|_v} a_{i_{(j,k)}}\right|_v \\ &= n + \log\prod_k^n \max_j \left\{\left|a_{i_{(j,k)}}\right|_v\right\} \\ &\le n + \sum_k^n \log\max_i \{|a_i|_v\} \\ &\le n + n\log\max_i\{|a_i|_v\} \\ &= O(n)\end{aligned} \tag{36}$$

and the non-Archimedian:

$$\begin{aligned}s \in S_A(n) \implies \log|s|_v &= \log\left|\sum_j^{2^n}\prod_k^n a_{i_{(j,k)}}\right|_v \\ &\le \log\left|\prod_k^n \max_j{}^{|\cdot|_v}\left\{a_{i_{(j,k)}}\right\}\right|_v \\ &\le \log\prod_k^n \max_j\left|a_{i_{(j,k)}}\right|_v \\ &\le \sum_k^n \log\max_i |a_i|_v \\ &= n\log\max_i|a_i|_v \\ &= O(n).\end{aligned} \tag{37}$$

APPENDIX C
PROOF: $f^{\alpha}_{1/2}(n) \neq O(n^{1+\epsilon}) \implies \mu(\alpha) = \infty$

Fix some positive ϵ; then, by hypothesis, there exist infinitely many n such that

$$\begin{aligned} -\log\left|\alpha\frac{q_n}{2^n} - \frac{p_n}{2^n}\right| &> n^{1+\epsilon} \\ \left|\alpha\frac{q_n}{2^n} - \frac{p_n}{2^n}\right| &< \frac{1}{2^{n^{1+\epsilon}}} \\ \left|\alpha - \frac{p_n}{q_n}\right| &< \frac{1}{q_n 2^{n^{1+\epsilon}-n}}. \end{aligned} \tag{38}$$

But, noting for any fixed r that $n^{1+\epsilon} - n = \Omega(n(r-1))$, we can choose sufficiently large n such that

$$\begin{aligned} \left|\alpha - \frac{p_n}{q_n}\right| &< \frac{1}{q_n 2^{n^{1+\epsilon}-n}} && \text{(by 37)} \\ &< \frac{1}{q_n 2^{n(r-1)}} && \text{(for } n \text{ sufficiently large)} \\ &\leq \frac{1}{q_n q_n^{r-1}} && (\tfrac{q_n}{2^n} \leq 1 \implies q_n \leq 2^n) \\ &= \frac{1}{q_n^r}, && \end{aligned} \tag{39}$$

so $\mu(\alpha) = \infty$. The corollary follows contrapositively.

APPENDIX D
EXTENSIONS OF THEOREM VI.2

From Theorem VI.2, we prove Corollary VI.2:

Proof. Let X be a uniformly continuous probability distribution; let $F : \mathbb{R} \to [0, 1]$ be its CDF, which is thus absolutely continuous. (Proof: By a theorem of Lesbegue, any measure can be decomposed into an absolutely continuous part, a singular part, and an atomic part. But X has neither of the latter two, by its uniform continuity. So the integral with respect to its measure, *i.e.* its CDF, is absolutely continuous.) Define $B \subseteq \mathbb{R}$:

$$B := \{\alpha \in \mathbb{R} \mid \exists p : \mu(p(\alpha)) > 2\}, \tag{40}$$

for some polynomial p. Then, by the probability integral transform, we have

$$P(X \in B) = P(F^{-1}(U) \in B), \tag{41}$$

where $U \sim \text{Unif}[0, 1]$. Note $F^{-1}(U) \in B \iff U \in F(B)$, so

$$P(F^{-1}(U) \in B) = P(U \in F(B)) \tag{42}$$

But since B has measure zero, it has measure zero under any absolutely continuous mapping. Thus $F(B)$ has measure zero, and $P(U \in F(B)) = 0$. □

We prove the second theorem by reducing to the first: Note again that it suffices to consider nonconstant p_i, note that there exist countably many such polynomials, that each produces an at most $(s-1)$-dimensional manifold $\subset \mathbb{R}^s$ as the preimage of any point y. So, for almost all α_s, the preimage of any point y is an $(s-2)$-dimensional manifold. By finite induction, we reduce to the $s = 1$ case with probability 1.

We prove the second corollary from the second theorem by identical argument to the first.

APPENDIX E
THE NUMBER ZOO

For the reader's reference, we summarize here important fixtures in the hierarchy of tameness/safeness, and state a few facts, either common results or consolidations of results surveyed or proven here. For conciseness, we omit "or above" and "or below" when obviated by the inclusion relations.

$$\begin{aligned} \mathbb{Q} &\subsetneq \overline{\mathbb{Q}} && (43) \\ &\subsetneq \{\gamma \mid \mu(\gamma) = 2\} && (44) \\ &\subsetneq \{\beta \mid \mu(\beta) < \infty\} = \mathbb{L}^c && (45) \\ &\subsetneq \left\{\alpha \;\middle|\; f^{\{\alpha\}^{(d)}}_{\{a_1,\ldots,a_r\}}(n) = O(n)\right\} && (46) \end{aligned}$$

- The first line has measure 0, as does the complement of the second. ($\mathbb{L}^c$ is the complement of the Liouville numbers.)
- The first line is countable; the second is uncountable. All lines have uncountable complement.
- Sets of numbers from the first line are known to be very tame.
- With probability 1, sets of numbers from any line are known to be very safe for d applications.
- There exist pairs of numbers from the second line, each individually safe for d applications, which together are arbitrarily unsafe for one application each. Such pairs, however, have measure zero in $\mathbb{R}^2$.

REFERENCES

[1] S. Aaronson. Quantum Computing, Postselection, and Probabilistic Polynomial-Time. *Proc. Roy. Soc. London*, A461:3473-3482, 2005. *quant-ph/0412187*.

[2] G. Kuperberg. How hard is it to approximate the Jones polynomial? To appear in *Theory Comput. arXiv:0908.0512v2*, 2014.

[3] M. Bremner, R. Jozsa, D. Shepherd. Classical Simulation of Commuting Quantum Computations Implies Collapse of the Polynomial Hierarchy. *Proc. Roy. Soc. London*, A467:459–472, 2011. *arXiv:1005.1407*.

[4] S. Aaronson, A. Arkhipov. The Computational Complexity of Linear Optics. *Proc. ACM STOC*, 43:333-342, 2011. *arXiv:1011.3245*

[5] T. Morimae, K. Fuii, J. Fitzsimons. On the Hardness of Classically Simulating the One Clean Qubit Model. *Phys. Rev. Lett.*, 112:130502, 2014. *arXiv:1312.2496*

[6] S. Aaronson. Question: Massive Cancelations. *MathOverflow*, ret. 11 Dec. 2014. q/187995.

[7] P. Achinger. Answer to: Massive Cancelations. *MathOverflow*, ret. 11 Dec. 2014. a/188000.

[8] J. Rosen, ed. T. Chow. Answer to: Massive Cancelations. *MathOverflow*, ret. 11 Dec. 2014. a/188010.

[9] W. Sawin. Answer to: Massive Cancelations. *MathOverflow*, ret. 11 Dec. 2014. a/188162.

[10] E. Weisstein. Irrationality Measure. *MathWorld* (Wolfram Web Resource). ret. 11 Dec. 2014 http://mathworld.wolfram.com/IrrationalityMeasure.html

[11] K. Choi, J. Vaaler. Diophantine Approximation in Projective Space. *Number Theory* (Ottawa, ON, 1996), 55-65, *CRM Proc. Lecture Notes*, 19, *Amer. Math. Soc.,* 1999.- http://www.cecm.sfu.ca/ choi/paper/metric.pdf.

[12] J. Milne. *Course Notes: Algebraic Number Theory.* ret. 11 Dec. 2014. http://www.jmilne.org/math/CourseNotes/ANTe6.pdf.