Continuous-Variable Instantaneous Quantum Computing is Hard to Sample

Continuous-Variable Instantaneous Quantum Computing is Hard to Sample

T. Douce,[1,2,†] D. Markham,[2,3] E. Kashefi,[2,3,5] E. Diamanti,[2,3] T. Coudreau,[1] P. Milman,[1] P. van Loock,[4] and G. Ferrini[1,4,*]
[1]*Laboratoire Matériaux et Phénomènes Quantiques, Sorbonne Paris Cité, Université Paris Diderot, CNRS UMR 7162, 75013 Paris, France*
[2]*Laboratoire d'Informatique de Paris 6, CNRS, UPMC—Sorbonne Universités, 4 place Jussieu, 75005 Paris, France*
[3]*LTCI, CNRS, Télécom ParisTech, Université Paris-Saclay, 75013 Paris, France*
[4]*Institute of Physics, Johannes-Gutenberg Universität Mainz, Staudingerweg 7, 55128 Mainz, Germany*
[5]*School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh, EH8 9AB*
(Received 5 August 2016; revised manuscript received 23 December 2016; published 17 February 2017)

Instantaneous quantum computing is a subuniversal quantum complexity class, whose circuits have proven to be hard to simulate classically in the discrete-variable realm. We extend this proof to the continuous-variable (CV) domain by using squeezed states and homodyne detection, and by exploring the properties of postselected circuits. In order to treat postselection in CVs, we consider finitely resolved homodyne detectors, corresponding to a realistic scheme based on discrete probability distributions of the measurement outcomes. The unavoidable errors stemming from the use of finitely squeezed states are suppressed through a qubit-into-oscillator Gottesman-Kitaev-Preskill encoding of quantum information, which was previously shown to enable fault-tolerant CV quantum computation. Finally, we show that, in order to render postselected computational classes in CVs meaningful, a logarithmic scaling of the squeezing parameter with the circuit size is necessary, translating into a polynomial scaling of the input energy.

DOI: 10.1103/PhysRevLett.118.070503

The question of whether quantum systems practically allow information to be processed faster than classical devices, i.e., whether a quantum supremacy in information processing can be experimentally observed and exploited, is of paramount importance both at the technological and fundamental level. On the one hand, devices overcoming classical computational power would allow solving currently intractable problems, such as the simulation of quantum physical processes from chemistry [1], biology [2] and solid state physics [3,4], security breaking of several cryptosystems [5], and database search [6]. On the other hand, the observation of a quantum supremacy would disprove a foundational hypothesis in computer science, namely, the extended Church-Turing thesis, stating that any physical model of computation can be efficiently simulated on a classical computer, modeled by a Turing machine.

Although quantum algorithms outperforming classical capabilities have been proposed [5,6], building a universal quantum computer capable of running arbitrary quantum algorithms has been an elusive goal, so far. Thus, a recent trend has emerged, where subuniversal models of quantum computers are considered, instead. In these models, specific problems are addressed which can be solved by a dedicated quantum platform efficiently, i.e., in a number of rounds that scales polynomially with the size of the input while no classical efficient solution exists. An example of such a model is boson sampling [7], which is related to the problem of computing the permanent of a unitary matrix. Proof-of-principle experiments have recently been performed, yet are too small to challenge classical devices [8–11].

A distinct subuniversal model that has been recently defined in the context of discrete-variable (DV) systems is instantaneous quantum computing (IQP), where the "P" in the acronym stands for polytime [12–14]. An IQP circuit is composed of input Pauli-$\hat{X}$ eigenstates, gates diagonal in the Pauli-$\hat{Z}$ basis, and output Pauli-$\hat{X}$ measurements (Fig. 1, left). Since all the gates commute they can be performed in any order and possibly simultaneously, hence, the name "Instantaneous." The resulting output probability distribution has been proven to be hard to sample classically, provided some standard conjectures in computer science hold true.

In particular, we are concerned with the definition of IQP within continuous-variable (CV) systems. Unlike DV, CV hardware for quantum information processing offers the possibility of deterministically preparing large resource states, such as multimode squeezed states and cluster states [15–18], containing up to 10^6 entangled modes in a recent experiment [19]. Furthermore, typical detection techniques available in this context, such as homodyne detection, have near unity detection efficiencies. Despite these specific features, only a few works exist that address subuniversal models of quantum computation (QC) featuring input squeezed states [20–23] and, to our knowledge, none with homodyne detection.

In this Letter, we define IQP circuits in CV, involving input squeezed states and output finite-precision homodyne detectors, and we prove these circuits are hard to simulate classically. The use of CVs requires specific tools to handle errors associated with finite squeezing. We deal with this by using Gottesman-Kitaev-Preskill (GKP) states [24], which were shown to enable fault-tolerant CV quantum

computation [24–26]. GKP encoding consists essentially in discretizing quantum information through encoding a qubit into the infinite-dimensional Hilbert space of a harmonic oscillator, e.g., the quantized electromagnetic field. As such, it enables us to link CV quantum complexity classes to ordinary DV ones. Interestingly, in order to properly establish this link for the classes relevant for this work (namely, postselected ones), it will be necessary to assume a specific scaling of the input squeezing with the size of the circuit. This requirement supports the role of energy as an essential parameter entering the definition of CV computational classes, as time and space do [27]. Inclusion of finite resolution in modeling homodyne detection allows us, on the one hand, to discretize the measurement outcomes; on the other hand, it incorporates in the model an intrinsic experimentally relevant imperfection.

The model.—In order to map the IQP paradigm from DV to CV, we use the correspondence between universal gate sets introduced in Ref. [28]. Thereby, in CV, IQP circuits have the following structure: input momentum-squeezed states $|\sigma\rangle_p = [1/(\sqrt{\sigma}\pi^{1/4})]\int dt e^{-(t^2/2\sigma^2)}|t\rangle_p$, gates diagonal in the position quadrature $\hat{q}$, and homodyne $\hat{p}$ measurements (Fig. 1, right). We restrict to the finite set of logical gates [24] $\{\hat{Z} = e^{i\hat{q}\sqrt{\pi}}, \hat{C}_Z = e^{i\hat{q}_1\hat{q}_2}, \hat{T} = e^{i(\pi/4)[2(\hat{q}/\sqrt{\pi})^3+(\hat{q}/\sqrt{\pi})^2-2(\hat{q}/\sqrt{\pi})]}\}$, all diagonal in the $\hat{q}$ operator. This would be a universal gate set for CV QC on GKP-encoded states, if a Hadamard gate was included, implemented on the CV level by the Fourier transform $\hat{F} = e^{i(\pi/2)(\hat{p}^2+\hat{q}^2)}$ [24]. Input GKP states are assumed being all in the $|\tilde{+}_L\rangle = (|\tilde{0}_L\rangle + |\tilde{1}_L\rangle)/\sqrt{2}$ state, with (up to a normalization constant)

$$\langle q|\tilde{0}_L\rangle \propto \sum_n \exp\left(-\frac{(2n)^2\pi\Delta^2}{2}\right)\exp\left(-\frac{(q-2n\sqrt{\pi})^2}{2\Delta^2}\right),$$

$$\langle q|\tilde{1}_L\rangle \propto \sum_n \exp\left(-\frac{(2n+1)^2\pi\Delta^2}{2}\right) \times \exp\left(-\frac{(q-(2n+1)\sqrt{\pi})^2}{2\Delta^2}\right),$$

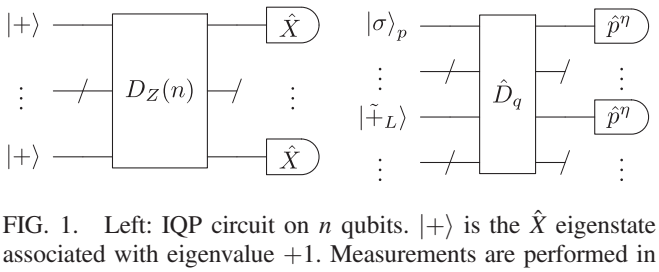

FIG. 1. Left: IQP circuit on n qubits. $|+\rangle$ is the $\hat{X}$ eigenstate associated with eigenvalue $+1$. Measurements are performed in the $\{|\pm\rangle\}$ basis. We denote $D_Z(n) = \prod_{z\in\mathbb{Z}_2^n} \exp(i\theta(z,n)\bigotimes_{j=1}^{n} Z^{z_j})$. Right: IQP circuit in CVs. $|\sigma\rangle_p$ are finitely squeezed states with variance σ in the $\hat{p}$ representation and $|\tilde{+}_L\rangle$ are finitely squeezed GKP states. The gate $\hat{D}_q$ is a uniform combination of elementary gates from the set mentioned in the text. The finitely resolved homodyne measurement $\hat{p}^\eta$ has resolution 2η.

where the tilde emphasizes that we consider finitely squeezed GKP states and where Δ describes the squeezing degree [29]. This allows us to respect the IQP-analog pattern: $\hat{X}$-diagonal input states, $\hat{Z}$-diagonal evolution, and $\hat{X}$-diagonal measurement.

Homodyne detection is modeled by the finitely resolved $\hat{p}^\eta$ operator that we define as [30]

$$\hat{p}^\eta = \sum_{k=-\infty}^{\infty} p_k \int_{-\infty}^{\infty} dp \chi_k^\eta(p)|p\rangle\langle p| \equiv \sum_{k=-\infty}^{\infty} p_k \hat{P}_k, \quad (1)$$

with $\chi_k^\eta(p) = 1$ for $p \in [p_k - \eta, p_k + \eta]$ and 0 outside, $p_k = 2\eta k$, and 2η the resolution, associated with the width of the detector pixels [31]. It is easy to check that this is still a projective measurement, since $\sum_{k=-\infty}^{\infty} \hat{P}_k = \mathcal{I}$, and $\hat{P}_k\hat{P}_{k'} = \hat{P}_k\delta_{k,k'}$ [32]. Note that this modelization is distinct from modeling imperfect detection efficiency [30,33,34].

We refer to this newly defined class of circuits as CVrIQP, where the label "r" stands for "realistic," incorporating both finite squeezing and finite resolution in the homodyne detection.

Recalling the proof of hardness of DV IQP.—In DV, the proof of hardness of IQP [14] follows a general structure that can also be used to prove the hardness of other models [7,35,36]. In general, given a restricted model of quantum computing, if that model becomes universal when supplemented with the ability to postselect on a subset of the outputs, then that model cannot be simulated classically, otherwise, widely held conjectures of complexity theory would be violated. Classical simulation of IQP corresponds to a black box made of classical circuits that outputs bit strings according to a probability distribution multiplicatively close to the quantum probability. The details of this argument, involving Toda's theorem and the polynomial hierarchy, have been explained in detail, e.g., in Refs. [14,37].

Universality through postselection in IQP circuits is achieved through the so-called "Hadamard gadget," Fig. 2. This gadget is measurement based; i.e., the input state is entangled to an ancillary $|+\rangle$ state, and then measured [39]. In the postselected scenario, only those trials where a desired value for a chosen output qubit is measured are retained [40]. Postselecting the circuit of Fig. 2 on the outcome $+1$ allows us to implement the Hadamard gate, thereby promoting IQP to the most general postselected QC, in other words,

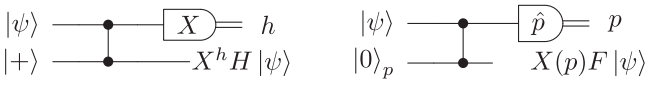

FIG. 2. Left: Hadamard gadget in a postselected IQP circuit, where h takes value 0 if $+1$ is measured, while $h = 1$ if the result is -1. Right: Ideal Fourier gadget in CVs, exact translation of the Hadamard gadget. $|0\rangle_p$ represents an infinitely $\hat{p}$-squeezed state with $\sigma = 0$, thus, satisfying $\hat{p}|0\rangle_p = 0$.

$$\text{PostIQP} \supseteq \text{PostBQP}, \tag{2}$$

where BQP stands for "bounded quantum polytime" and corresponds to the decision problems efficiently solved by quantum computers.

Hardness of CVrIQP: structure of the proof.—We use the same proof structure as in the DV case, and in particular, we aim at proving that postselected CVrIQP circuits yield postselected universal QC, i.e., that

$$\text{PostCV}r\text{IQP} \supseteq \text{PostBQP}. \tag{3}$$

As an intermediate step, it will be useful to prove that PostCVrIQP contains the class of GKP-encoded CV measurement-based quantum computations (MBQC) with ancillary finitely squeezed and GKP states [26,28,46] and finite resolution, i.e., that CVrMBQC $\subseteq$ PostCVrIQP. We structure our proof via the following steps. (1) Fourier gadget: Adding postselection to CVrIQP yields a universal set for QC. This requires a CV analog of the Hadamard gadget in DV. As for DV, it will be measurement-based. This easily shows that CVrMBQC $\subseteq$ PostCVrIQP. (2) Error correction: Adding finite resolution in the homodyne detection preserves fault-tolerance for sufficiently high resolution, i.e., CVrMBQC $=$ BQP. Previous results [26] already show that CVMBQC $=$ BQP, where CVMBQC displays ancillary finitely squeezed states, but perfect homodyne detection [28,46]. Combining items 1 and 2, we have BQP $\subseteq$ PostCVrIQP. (3) Postselection: The logical, qubit postselection procedure defining the class PostBQP can be mapped to the CV hardware, thereby, completing the demonstration of Eq. (3). This requires imposing a well-defined scaling of the squeezing with the circuit size. In what follows, we address, separately, each of the three steps of the proof.

Fourier gadget.—In analogy to the Hadamard gadget, we consider a toolbox circuit where an intermediate step of the computation $|\psi\rangle$ is entangled to a squeezed state by means of a $\hat{C}_Z$ gate—the latter belonging to the model. Figure 2 represents an idealized version with infinitely squeezed ancilla and infinite resolution. Obtaining the outcome $p = 0$ after the homodyne measurement yields the Fourier transform of the input state, which, in GKP encoding, translates onto the Hadamard gate. The probability of selecting $p = 0$ is not zero because of finite resolution, and its scaling with the number of iterations of the gadget is not conceptually worse than for the DV case [41]. We stress that as in DV, this postselection should be regarded as a mathematical tool for the hardness proof, and its actual implementation is not required in practice.

In the actual gadget, finite resolution, as well as finite squeezing, affects the postselected output state. The leading order in η yields the usual pure state that would be obtained if the resolution was infinite

$$|\psi\rangle^{(1)}_{k=0,\text{cond}} = \frac{1}{\pi^{1/4}\sqrt{\sigma}} \int dq dt e^{-\frac{(t-q)^2}{2\sigma^2}} \psi(q)|t\rangle_p, \tag{4}$$

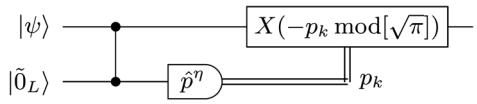

FIG. 3. Procedure to correct for errors in the $\hat{q}$ quadrature. $|\psi\rangle$ is the data qubit and $|\tilde{0}_L\rangle$ is a realistic, i.e., noisy, GKP state. After measurement on the second mode, the result p_k is used to shift the first mode back.

where the Gaussian convolution factor is due to finite squeezing [46,47]. As will be addressed next, and in more detail in [41], both the Gaussian convolution and the mixedness can be corrected by GKP error correction.

Error correction.—The fault-tolerance proof of Ref. [26] shows that errors which accumulate due to finite squeezing can be corrected by means of the GKP error-correcting gadget [24,25]. This can be generalized to the case of finitely resolved homodyne detectors [24,41].

The error correction consists in nondestructively measuring $\hat{q} \bmod \sqrt{\pi}$ on the data qubit by measuring $\hat{p}$ on an ancillary GKP state entangled to it (Fig. 3) [48]. The measurement effectively projects the error onto a specific value q and determines the shift that needs to be applied to the data qubit to correct it. q is a random variable whose distribution is given by the noise in the data qubit. The value of q is recovered by the measurement outcome up to the noise of the ancilla and the finite resolution. If these are too high, namely, exceeding a $\sqrt{\pi}$-long window, the error is recovered as $q \pm \sqrt{\pi}$, resulting in a logical error after shifting the data qubit back.

Most importantly, this procedure replaces the original noise in $\hat{q}$ with the one coming from the ancilla and the finite resolution. Therefore, it can be kept under control, if the characteristic parameters—GKP squeezing and detector resolution—are sufficiently small. Thus, repeating this protocol after a Fourier transform enables correcting errors in both quadratures.

Postselection.—The definition of the class PostBQP is based on the conditional probability of obtaining the answer of the decision problem on the second qubit, conditioned on having obtained a given outcome, say +, on the first. Mapping PostBQP onto a PostCVrIQP circuit requires approximating this conditional probability. This, in turn, requires approximating multiplicatively the probability of the conditioning event $P(+_1)$ by the simulation on the PostCVrIQP circuit $P_s(+_1)$, i.e., $1/cP(+_1) < P_s(+_1) < cP(+_1)$ with $1 \leq c \leq 2^{1/4}$ [14,49].

Realistic GKP states $|\tilde{\pm}_L\rangle$ are not orthogonal. So, projective measurements like homodyne detection cannot perfectly distinguish between the two. By binning the real axis, using $\sqrt{\pi}$-long windows centered at integer multiples of $\sqrt{\pi}$, such that peaks of the $|\tilde{+}_L\rangle$ ($|\tilde{-}_L\rangle$) state are centered on an even (odd) bin, one can associate an outcome of a homodyne measurement belonging to an even (odd) bin with the $|\tilde{+}_L\rangle$ ($|\tilde{-}_L\rangle$) state. Doing so, the probability P_e of

wrongly associating an outcome with a state is given by summing the contributions from the tails of all the Gaussians, yielding an approximate upper bound as a function of the squeezing [24]

$$P_e < \frac{2\Delta}{\pi} e^{-\frac{\pi}{4\Delta^2}}. \quad (5)$$

Additionally, we assume that the resolution η defined previously matches the $\sqrt{\pi}$ binning, i.e., $\sqrt{\pi}/\eta \in \mathbb{N}$. Overall we require that the error probability P_e is upper bounded by a fraction of the target probability $P(+_1)$, i.e., that

$$P_e < \frac{1}{10} P(+_1), \quad (6)$$

which ensures the above mentioned multiplicative approximation of $P(+_1)$ with $P_s(+_1)$.

On the other hand, the definition of the class PostBQP requires the conditioning probability to scale as [50]

$$P(+_1) \sim \frac{1}{2^n}. \quad (7)$$

Combining Eqs. (5), (6), and (7) yields the following scaling law for the squeezing of the GKP states:

$$\Delta^2_{\mathrm{dB}} > 10\log_{10}\left(n \ln 2 - \ln\frac{\pi}{20}\right) + 10\log_{10}\frac{2}{\pi}, \quad (8)$$

with $\Delta^2_{\mathrm{dB}} = -10\log_{10}(2\Delta^2)$ the squeezing in decibels, resulting in an energy scaling $E \propto \Delta^2 \sim \mathcal{O}(n)$. Incidentally, we remark that a similar scaling of the squeezing parameter was found in the Supplemental Material of Ref. [51] to ensure that noise accumulated in a CV teleportation chain lies below a fixed value (see, also, [52]). Eventually, we note that the exponential precision needed for the consistent definition of PostBQP can be attained with faulty gates and error correction by means of concatenation and a polynomial overhead of resources, as ensured by the Threshold theorem, provided the error rate is below a given threshold [53].

To summarize, Eq. (3) means that any PostBQP computation can be mapped onto a cleverly chosen PostCV*r*IQP circuit. Qubits are encoded within GKP states and gates diagonal in the computational basis correspond to evolutions diagonal in $\hat{q}$. All Hadamard gates are implemented through the measurement-based procedure described in the first step. The second step ensures that the subsequent circuit retains the fault tolerance feature. The last one guarantees that the PostCV*r*IQP circuit multiplicatively approximates the original PostBQP computation, at the cost of a scaling of the squeezing parameters with the computation size. Computer science theorems and assumptions then imply that this result makes CV*r*IQP impossible to simulate efficiently classically.

Concluding remarks and perspectives.—We have proven the hardness of CV*r*IQP circuits. To our knowledge, this is the first subuniversal model involving homodyne detection. The proof has required assuming a logarithmic scaling of the input squeezing with the circuit size, which corroborates the emerging idea that energy, as time and space, must enter the definition of CV complexity classes. Input squeezed states can be easily produced and homodyne detection efficiently performed. Methods have been proposed to perform high-order evolutions diagonal in the position representation [54–60]. Thus, this work takes a significant step towards the demonstration of quantum advantage.

On the other hand, the experimental realization of GKP states is challenging. An interesting question is whether CV*r*IQP circuits remain hard-to-sample without explicitly assuming available input GKP states. In this context, one would rather consider a continuous family of $\hat{q}$-diagonal gates. The Fourier gadget allows obtaining CV universality [46]. Hence, there is a (possibly big) fixed size circuit that generates a GKP state. Adding a polynomial number of such circuits ensures fault tolerance and sums up to a polynomial size circuit; hence, the proof goes through as considered in this work. The continuous gates, however, should be bounded, to ensure a physical and energy-efficient model. Then, issues arise from this constraint: how many times should these gates be repeated to achieve universality? Would the resulting family of circuits still be uniform, as required for IQP?

Assuming GKP states available at the input yields a conceptually simpler framework, where these issues do not need to be addressed. We leave a possible removal of this hypothesis for future work, in connection to the very general question of specifying the minimal resources, possibly quantified in terms of non-Gaussianity [61], that yield quantum advantage.

We thank N. Menicucci, R. Alexander, and F. Arzani for helpful discussions. We also thank the anonymous Referees for their insightful reports that have allowed us to improve the presentation of this Letter. This work was supported by the ANR COMB Project, Grant No. ANR-13-BS04-0014 of the French Agence Nationale de la Recherche, and by the DAAD-Campus France Project Procope No. 35465RJ. G. F. acknowledges support from the European Union through the Marie Sklodowska-Curie Grant agreement No. 704192.

*giulia.ferrini@gmail.com
†Tom.Douce@lip6.fr

[1] I. Kassal, S. P. Jordan, P. J. Love, M. Mohseni, and A. Aspuru-Guzik, Proc. Natl. Acad. Sci. U.S.A. **105**, 18681 (2008).
[2] M. Reiher, N. Wiebe, K. M. Svore, D. Wecker, and M. Troyer, arXiv:1605.03590.
[3] S. Lloyd, Science **273**, 1073 (1996).
[4] D. S. Abrams and S. Lloyd, Phys. Rev. Lett. **79**, 2586 (1997).
[5] P. W. Shor, SIAM Rev. **41**, 303 (1999).
[6] L. K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).

[7] S. Aaronson and A. Arkhipov, Theory Comput. **9**, 143 (2013).
[8] M. Tillmann, B. Dakic, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, Nat. Photonics **7**, 540 (2013).
[9] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys *et al.*, Science **339**, 798 (2013).
[10] N. Spagnolo, C. Vitelli, D. J. Brod, A. Crespi, F. Flamini, S. Giacomini, G. Milani, R. Ramponi, P. Mataloni, R. Osellame *et al.*, Nat. Photonics **8**, 615 (2014).
[11] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, and A. G. White, Science **339**, 794 (2013).
[12] D. Shepherd and M. J. Bremner, Proc. R. Soc. A **465**, 1413 (2009).
[13] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert, arXiv:1602.00703.
[14] M. J. Bremner, R. Josza, and D. Shepherd, Proc. R. Soc. A **467**, 459 (2010).
[15] J. Roslund, R. Medeiros de Araújo, S. Jiang, C. Fabre, and N. Treps, Nat. Photonics **8**, 109 (2014).
[16] S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J.-i. Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, Nat. Photonics **7**, 982 (2013).
[17] X. Su, Y. Zhao, S. Hao, X. Jia, C. Xie, and K. Peng, Opt. Lett. **37**, 5178 (2012).
[18] M. Chen, N. C. Menicucci, and O. Pfister, Phys. Rev. Lett. **112**, 120505 (2014).
[19] J.-i. Yoshikawa, S. Yokoyama, T. Kaji, C. Sorphiphatphong, Y. Shiozawa, K. Makino, and A. Furusawa, APL Photonics **1**, 060801 (2016).
[20] A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. OBrien, and T. C. Ralph, Phys. Rev. Lett. **113**, 100502 (2014).
[21] J. P. Olson, K. P. Seshadreesan, K. R. Motes, P. P. Rohde, and J. P. Dowling, Phys. Rev. A **91**, 022317 (2015).
[22] K. P. Seshadreesan, J. P. Olson, K. R. Motes, P. P. Rohde, and J. P. Dowling, Phys. Rev. A **91**, 022334 (2015).
[23] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, arXiv:1612.01199v1.
[24] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001).
[25] S. Glancy and E. Knill, Phys. Rev. A **73**, 012325 (2006).
[26] N. C. Menicucci, Phys. Rev. Lett. **112**, 120504 (2014).
[27] N. Liu, J. Thompson, C. Weedbrook, S. Lloyd, V. Vedral, M. Gu, and K. Modi, Phys. Rev. A **93**, 052304 (2016).
[28] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, Phys. Rev. Lett. **97**, 110501 (2006).
[29] For consistency and simplicity, it is natural (though unessential) to assume that the GKP states and input squeezed states possess the same squeezing degree, i.e., $\Delta = \sigma$. This choice greatly simplifies the calculations in Ref. [26]. Keeping this in mind, we will carry out our calculations maintaining two independent squeezing parameters Δ and σ, respectively, for the GKP states and the squeezed states. This will allow us to keep trace of the origin of the requirements on the squeezing scaling that we will find later in this Letter.
[30] M. G. A. Paris, M. Cola, and R. Bonifacio, Phys. Rev. A **67**, 042104 (2003).
[31] Note that this model turns out to be equivalent to an ideal scheme with perfectly resolving homodyne detectors and a discretization (binning) of the measurement outcomes.
[32] This result uses that $\int_{-\infty}^{\infty} dp' \chi^{\eta}_{k'}(p') \langle p'|\delta(p-p') = \chi^{\eta}_{k'}(p)\langle p|$ despite $\chi^{\eta}_{k'}(p')$ is not a smooth function, which can be verified with Riemann sum formalism.
[33] U. Leonhardt, *Measuring the Quantum State of Light*, 1st ed. (Cambridge University Press, New York, 1997).
[34] U. Leonhardt and H. Paul, Phys. Rev. A **48**, 4598 (1993).
[35] E. Farhi and A. W. Harrow, arXiv:1602.07674.
[36] T. Morimae, K. Fujii, and J. F. Fitzsimons, Phys. Rev. Lett. **112**, 130502 (2014).
[37] We mention that the DV IQP hardness proof has been strengthened recently to additive approximation of IQP circuits by classical computers in [38].
[38] M. J. Bremner, A. Montanaro, and D. Shepherd, Phys. Rev. Lett. **117**, 080501 (2016).
[39] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[40] The probability of success of the Hadamard gadget is $1/2$ at each iteration [41]. Given that the number of postselected lines l is of order of the total number of lines in the circuit n, $l \sim O(n)$, the overall success probability distribution $1/2^l$ is exponentially low in the circuit size.
[41] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.118.070503 for calculation details, which includes Refs. [42–45].
[42] J. Watrous, *Encyclopedia of Complexity and Systems Science* (Springer, New York, 2009), pp. 7174–7201.
[43] S. Aaronson, The Complexity Zoo, https://complexityzoo.uwaterloo.ca/Complexity_Zoo.
[44] S. Aaronson, Proc. R. Soc. A **461**, 3473 (2005).
[45] G. Kuperberg, Theory Comput. **11**, 183 (2015).
[46] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, Phys. Rev. A **79**, 062318 (2009).
[47] R. N. Alexander, S. C. Armstrong, R. Ukai, and N. C. Menicucci, Phys. Rev. A **90**, 062324 (2014).
[48] The $|\tilde{0}_L\rangle$ state needed for this error-correction gadget can be obtained from the $|\tilde{+}_L\rangle$ states that we have in our model by a Fourier transform through postselection.
[49] This ensures that, for the conditional probability $P_s(m_2/+_1)$, a multiplicative approximation also holds, i.e., that $(1/c')P(m_2/+_1) < P_s(m_2/+_1) < c'P(m_2/+_1)$ with $1 \le c' \le \sqrt{2}$.
[50] S. Aaronson, PostBQP Postscripts: A Confession of Mathematical Errors, www.scottaaronson.com/blog/?p=2072.
[51] R. Ukai, N. Iwata, Y. Shimokawa, S. C. Armstrong, A. Politi, J. I. Yoshikawa, P. van Loock, and A. Furusawa, Phys. Rev. Lett. **106**, 240504 (2011).
[52] R. N. Alexander, N. Gabay, P. P. Rohde, and N. C. Menicucci, arXiv:1606.00446v1.
[53] Assuming that the limiting factor in relevant experiments is the squeezing degree and, thus, neglecting finite resolution effects, we obtain that stringent error probabilities of 10^{-6} would result in a squeezing of roughly 20.5 dB [41].
[54] P. Marek, R. Filip, and A. Furusawa, Phys. Rev. A **84**, 053802 (2011).

[55] M. Yukawa, K. Miyata, H. Yonezawa, P. Marek, R. Filip, and A. Furusawa, Phys. Rev. A **88**, 053816 (2013).
[56] K. Park, P. Marek, and R. Filip, Phys. Rev. A **90**, 013804 (2014).
[57] K. Marshall, R. Pooser, G. Siopsis, and C. Weedbrook, Phys. Rev. A **91**, 032321 (2015).
[58] J. Etesse, B. Kanseri, and R. Toualle-Brouri, Opt. Express **22**, 30357 (2014).
[59] F. Arzani, N. Treps, and G. Ferrini (to be published).
[60] K. Miyata, H. Ogawa, P. Marek, R. Filip, H. Yonezawa, J.-i. Yoshikawa, and A. Furusawa, Phys. Rev. A **93**, 022301 (2016).
[61] H. Pashayan, J. J. Wallman, and S. D. Bartlett, Phys. Rev. Lett. **115**, 070501 (2015).