

Complexity and multifunctional variants of the quantum-to-quantum Bernoulli factories

Francesco Hoch, Taira Giordani , Gonzalo Carvacho, Nicolò Spagnolo , and Fabio Sciarrino *Dipartimento di Fisica, Sapienza Università di Roma, Piazzale Aldo Moro 5, I-00185 Roma, Italy*

(Received 17 December 2025; accepted 26 May 2026; published 1 July 2026)

A Bernoulli factory is a model for randomness manipulation that transforms an initial Bernoulli random variable into another Bernoulli variable by applying a predetermined function relating the output bias to the input one. In literature, quantum-to-quantum Bernoulli factory schemes have been proposed, which encode both the input and output variables using qubit amplitudes. This fundamental concept can serve as a subroutine for quantum algorithms that involve Bayesian inference and Monte-Carlo methods, or that require data encryption, like in blind quantum computation. In this work, we present a characterization of the complexity of the quantum-to-quantum Bernoulli factory by providing a lower bound on the required number of qubits needed to implement the protocol, an upper bound on the success probability, and the quantum circuit that saturates the bounds. We also formalize and analyze two different variants of the original problem that address the possibility of increasing the number of input biases or the number of functions implemented by the quantum-to-quantum Bernoulli factory. The obtained results can be used as a framework for randomness manipulation via such an approach.

DOI: [10.1103/k8kd-58h8](https://doi.org/10.1103/k8kd-58h8)

I. INTRODUCTION

A Bernoulli factory is a paradigm of randomness processing first proposed by Keane and O'Brien [1] to manipulate Bernoulli distributions only from their sampling. More formally, a Bernoulli factory is an algorithm that, given independent samples from a Bernoulli distribution (a coin) with unknown bias p , exactly simulates a Bernoulli variable with bias $q = f(p)$, where $f : S \subseteq [0, 1] \rightarrow [0, 1]$ is a predetermined function called classical-to-classical Bernoulli factory. Starting from the original problem [2–4], various applications and variants [5–10] have been proposed over time. In particular, algorithms that implement the protocol for specific classes of functions [11–15] and an analysis of the computational complexity measured in terms of the average number of samples [15–17] have been addressed.

Due to the generality of the Bernoulli factory problem and the intrinsic stochastic nature of quantum mechanics, quantum extensions of the problem have been introduced. The first quantum extension was addressed by Dale *et al.* [18,19] in which the input classical coin is replaced with its corresponding quantum version. This problem shows interesting properties since it has a larger set of simulable functions and there is evidence of an advantage in terms of the average number of samples needed for the algorithm compared to the classical counterpart [20]. This version is called quantum-to-classical Bernoulli factory and has been

experimentally implemented on superconducting [21] and photonic [20] platforms. Subsequently, Jiang *et al.* [22] formalize a version called quantum-to-quantum Bernoulli factory (QQBF) in which the entire Bernoulli process is quantum, i.e., both the input and output states. Moreover, they prove that a complex function $f(z)$ is simulable by a QQBF if and only if it is a complex rational function. This proof was obtained by exploiting the field properties of the set of rational functions. In this regard, experimental implementations through photonic platforms have been devised [23–26], opening the path to the application of the Bernoulli factory as a subroutine for quantum algorithms such as the blind quantum computation [27–29].

Despite theoretical and experimental advances, how the complexity of the QQBF problem, in terms of qubit count and maximum success probability, depends on the implemented function remains an open question. In this article, we present a refined demonstration to characterize the set of simulable functions, offering significantly different perspectives over the existing literature [22]. While confirming the prior results, our approach directly yields insights into the protocol resources requirements, specifically, the number of qubits (spatial complexity) and the maximal success probability (time complexity). Furthermore, it enables the explicit construction of a quantum circuit with optimal performance and efficient to implement. In addition to the complexity analysis of the QQBF, two different extensions of the original problem are formalized and analyzed. The first one is called *multivariate quantum-to-quantum Bernoulli factory* and extends the QQBF problem to the possibility of having more quantum Bernoulli distributions with different biases at the input. The second extension introduces the *multifunctional quantum-to-quantum Bernoulli factory*, which formalizes the implementation of multiple functions within a single QQBF. While prior experimental demonstrations have featured gates

*Contact author: fabio.sciarrino@uniroma1.it

that can be interpreted in this context [22,25,26], a general theoretical framework for this class of problems has not been devised until now.

The work is organized as follows. In Sec. II, we provide some definitions and concepts at the basis of this study. Section III focuses on the demonstrations of the complexity of a quantum-to-quantum Bernoulli factory as well as on the analysis of the results. In Secs. IV and V, we formalize and analyze the two extensions of the original problem, respectively, the multivariate quantum-to-quantum Bernoulli factory and the multifunctional quantum-to-quantum Bernoulli factory. In Sec. VI, we present an application of the theory for the implementation of two elementary QQBF operations, such as the sum and the product between quantum states. Finally, in Sec. VII, we summarize the results and discuss the possible applications and directions opened by our analysis.

II. BACKGROUND AND DEFINITIONS

Quantum-to-quantum Bernoulli factories operate on the amplitudes of qubit states. In Refs. [18,19], the concept of a quantum coin (or quoin) defined as a qubit in a pure state $|C_p\rangle = \sqrt{p}|0_c\rangle + \sqrt{1-p}|1_c\rangle$ was introduced. This definition is motivated by the fact that, if the state is measured on the computational basis, it returns a classical Bernoulli variable with bias p . In this work, we use the more general parametrization of Refs. [25,26] in which each qubit state is associated with a complex number $z \in \mathbb{C}$ through the expression

$$|z\rangle := \frac{z|0_c\rangle + |1_c\rangle}{\sqrt{1+|z|^2}}, \quad (1)$$

where $|0_c\rangle$ and $|1_c\rangle$ are the two vectors of the computational basis. This parametrization is related to the bijective map associated with the stereographic projection that links each point in the complex plane to a point on the surface of the Bloch sphere. In this way, we can identify each quoin with the state $|C_p\rangle = |\sqrt{\frac{p}{1-p}}\rangle$ and extend the concept to all the Bloch sphere.

In this framework, a quantum-to-quantum Bernoulli factory associated with a complex function $f(z) : \mathbb{C} \rightarrow \mathbb{C}$ is the protocol that takes as input n qubits in the state $|z\rangle$ and returns one qubit in the state $|f(z)\rangle$ with a certain non-null success probability. In this context, we say that a complex function $f(z) : \mathbb{C} \rightarrow \mathbb{C}$ is *simulable* if there exists a QQBF that implements it. It is known from Ref. [22] that the set of simulable functions by a QQBF is the set of *complex rational functions*.

A complex rational function $r(z) \in \text{Rat}(z)$ is defined as the ratio of two polynomials $P(z)$ and $Q(z)$ with complex coefficients

$$r(z) = \frac{P(z)}{Q(z)}, \quad (2)$$

where $Q(z)$ is a polynomial different from zero and $P(z)$ and $Q(z)$ have no common factor. Furthermore, we define the degree of a complex rational function as the maximum

between the degrees of the two polynomials $\deg(r(z)) = \max\{\deg(P), \deg(Q)\}$.

We can extend the concept by defining the *multivariate complex rational functions* as

$$t(z_1, \dots, z_k) = \frac{P(z_1, \dots, z_k)}{Q(z_1, \dots, z_k)}, \quad (3)$$

where $t(z_1, \dots, z_k) \in \text{Rat}(z_1, \dots, z_k)$ is a function of k variables and $P(z_1, \dots, z_k)$ and $Q(z_1, \dots, z_k)$ are two polynomials with complex coefficients. Similarly to the single variable case, the degree of the function related to the variable z_j is defined as the maximum between the degrees of the two polynomials in that particular variable $\deg_j(t(z_1, \dots, z_k)) = \max\{\deg_j(P), \deg_j(Q)\}$. For the multivariate complex rational functions, we will use hereafter this definition of degree in the performed derivations.

In this work, when representing states as bit strings, the ordering is performed from the least significant bit to the most significant one.

Since it will be used in the following demonstrations, we introduce the states $|s_j^n\rangle$ as the totally symmetric states of n qubits with j zeros, which in formula is

$$|s_j^n\rangle = \frac{1}{\sqrt{\binom{n}{j}}} \sum_{\substack{x \in \{0,1\}^n \\ \text{wt}(x)=n-j}} |x\rangle, \quad (4)$$

where $\text{wt}(x)$ is the Hamming weight of the string x . Those states are related to the Dicke state [30], and for a given size there are $n+1$ possible states.

III. QUANTUM-TO-QUANTUM BERNOULLI FACTORY COMPLEXITY

In the following, we provide a formal derivation of the class of simulable functions by a QQBF and the quantum resources needed to implement a given function. Our demonstrations do not assume any particular internal structure of the QQBF. This contrasts with previous demonstrations in Ref. [22] where the authors individuated the class of simulable functions assuming the fundamental operations of the complex field, i.e., sum, inversion, and product. We show that such a structure for the QQBF can be retrieved as a special case of the demonstration presented in this work. Furthermore, such a characterization of the set of simulable functions allows the derivation of bounds for the problem complexity in terms of the minimum number of qubits required for the implementation and the maximum success probability. Finally, it is also shown how to construct the quantum circuit for a given function that allows the saturation of the bounds.

The demonstration proceeded as follows: First, we derive the general circuit implementing a QQBF, i.e., a structure to which every other circuit can be reduced. In this stage, we do not consider the possibility of tracing out the states of the qubits. With that structure, we can derive a superset of the set of simulable functions, i.e., a set that contains all the simulable functions and maybe something more. For each element in the superset, we provide a lower bound on the number of qubits required to implement the QQBF. Subsequently, we show that the found bounds are tight by explicitly constructing

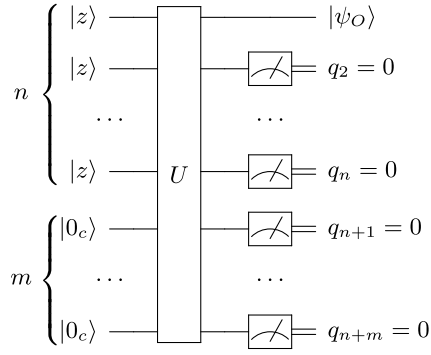


FIG. 1. Schematic representation of the general circuit for the quantum Bernoulli factory. The circuit takes as input n qubit in the state $|z\rangle$ and m ancillary qubits in the state $|0_c\rangle$. The resulting state evolves through a unitary evolution U . All qubits are then measured in the computational basis, except the first one, which carries the output state of the Bernoulli factory. The output state $|\psi_O\rangle$ is accepted if all the measurements $q_2, \dots, q_{n+m}$ return the outcome 0. This circuit is the most general one since every circuit implementing a quantum-to-quantum Bernoulli factory can be mapped into the one shown in the figure, as described in the main text.

a quantum circuit that implements the QQBF for each element in the superset. After that, we analyze the success probability and the gate complexity of the circuit. We also analyze the possibility of tracing qubit states, showing that they do not provide any advantage.

A. Generic circuit representation of the QQBF: Superset of simulable functions and lower bound for the number of qubits

The first step to characterize the set of simulable functions is to show that every circuit implementing a quantum-to-quantum Bernoulli factory can be mapped into a circuit in the form of Fig. 1. Since the hidden information in a Bernoulli factory circuit is provided only by the unknown state $|z\rangle$, we can divide the circuit into three principal components. The first part is the input state, which is composed of n copies of the state $|z\rangle$ and some ancillary qubits in known pure states. Subsequently, a unitary evolution and a measurement are performed as second and third part, respectively, such that at the end only a single qubit remains that encodes the output state. Using the deferred measurement principle [31,32], we can postpone all the measurements at the end of the circuit by eventually adding more ancillary qubits. In this way, we have only one known global unitary evolution between the initial state and the measurement. Furthermore, without loss of generality, we can assume that all ancillary qubits are in the state $|0_c\rangle$, since any other state can be generated by applying a unitary transformation that can be embedded in the global one. With a similar argument, we can say that all measurements are performed in the computational basis and that the result is accepted when all of them provide the outcome 0.

Using such a framework, we can identify the superset of the simulable functions, i.e., a set that contains the set of simulable functions and the lower bound on the required number of qubits to simulate a given function.

First, we write the input state of the circuit in Fig. 1 as

$$|\psi_I\rangle = |0_c\rangle^{\otimes m} \otimes \left(\frac{z|0_c\rangle + |1_c\rangle}{\sqrt{1+|z|^2}} \right)^{\otimes n} \\ = \left(\frac{1}{1+|z|^2} \right)^{\frac{n}{2}} \sum_{j=0}^n z^j \sqrt{\binom{n}{j}} |0_c\rangle^{\otimes m} \otimes |s_j^n\rangle. \quad (5)$$

It is important to note that the coefficients composing the state are monomial in z and span all the powers from 0 to n . Since the unitary evolution is linear, all the coefficients of the final state before the measurements are a linear combination of the input state coefficients:

$$|\psi\rangle = U|\psi_I\rangle = \frac{1}{(1+|z|^2)^{\frac{n}{2}}} \sum_{k=0}^{2^{n+m}-1} P_k(z) |k\rangle, \quad (6)$$

where

$$P_k(z) = \sum_{j=0}^n \sqrt{\binom{n}{j}} u_{kj} z^j \quad (7)$$

and $|k\rangle$ is the state representing the bitstring of the number k and $u_{kj} = \langle k|U(|0_c\rangle^{\otimes m} \otimes |s_j^n\rangle)$. This consideration demonstrates that all the coefficients of the state written in the computational basis are polynomial in z with the degree at most n . At this point, we apply the measurements. Since all are performed on the computational basis and the results must be all 0, the measure can be described by the operator $M = |0_c\rangle\langle k=0| + |1_c\rangle\langle k=1|$. This means that we are selecting the states $|k=0\rangle$ and $|k=1\rangle$ and that the output state of such a QQBF is in the form

$$|\psi_O\rangle = \frac{M|\psi\rangle}{\sqrt{\langle\psi|M^\dagger M|\psi\rangle}} \\ = \frac{P_0(z)|0_c\rangle + P_1(z)|1_c\rangle}{\sqrt{|P_0(z)|^2 + |P_1(z)|^2}} \\ = \left| f(z) = \frac{P_0(z)}{P_1(z)} \right\rangle. \quad (8)$$

We have then retrieved the same result of Ref. [22] that the space of simulable functions S is a subset of the set of rational functions $S \subseteq \text{Rat}(z)$. Most importantly, we note that in such a formulation of the problem, there is a direct relationship between the degree of the implemented function $f(z)$ and the number of resources. The functions implementable by a circuit with n copies of the state $|z\rangle$ as input have a degree of n at most. This result allows us to have a lower bound on the minimum number of qubits in the state $|z\rangle$ required to implement a given function so as the total number of qubits required. Indeed, the optimal QQBF in terms of resources requires at least as many qubits as the degree of the function:

$$n \geq \deg(f(z)). \quad (9)$$

B. Tightness of the bound and choice of the optimal unitary transformation

Now that we found an upper bound for the set of simulable functions our goal is to prove that it is indeed an equality by showing that $\text{Rat}(z) \subseteq S$. We also want to show that the lower

bound of Eq. (9) on the required number of bits is tight and no ancillary qubits are required ($m = 0$) except for the particular case of $n = 1$.

To accomplish this, for each tuple $(P(z), Q(z)) \in \mathcal{P}(\mathbb{C}) \times \mathcal{P}(\mathbb{C})$ we construct a circuit implementing a Bernoulli factory with an associated function $f(z) = P(z)/Q(z)$ that use a number of qubits n equal to the lower bound of Eq. (9) and do not require ancillary qubits. First, we describe the state at the output of the circuit in Fig. 1:

$$|\psi_O\rangle = \frac{|0_c\rangle\langle v_0||\psi_I\rangle + |1_c\rangle\langle v_1||\psi_I\rangle}{\sqrt{|\langle v_0||\psi_I\rangle|^2 + |\langle v_1||\psi_I\rangle|^2}}, \quad (10)$$

where we describe the two rows of the unitary matrix with two covectors $\langle v_0| = \langle 0_c|^{\otimes m} \otimes \langle 0_c|^{\otimes n-1} \otimes \langle 0_c|U$ and $\langle v_1| = \langle 0_c|^{\otimes m} \otimes \langle 0_c|^{\otimes n-1} \otimes \langle 1_c|U$. Since we aim at implementing a Bernoulli factory with the associated function $g(z) = P(z)/Q(z)$, we impose the following equalities:

$$\langle v_0||\psi_I\rangle = KP(z), \quad (11)$$

$$\langle v_1||\psi_I\rangle = KQ(z), \quad (12)$$

for some real non-null proportional factor K . Defining $P(z) = \sum_{j=0}^n p_j z^j$, $Q(z) = \sum_{j=0}^n q_j z^j$, and using the property that the monomials with different powers are linearly independent we can rewrite the previous equations in the form

$$\langle v_0|(|0_c\rangle^{\otimes m} \otimes |s_j^n\rangle) = K \frac{p_j}{\sqrt{\binom{n}{j}}}, \quad (13)$$

$$\langle v_1|(|0_c\rangle^{\otimes m} \otimes |s_j^n\rangle) = K \frac{q_j}{\sqrt{\binom{n}{j}}}. \quad (14)$$

Using the property that the vectors $|s_j^n\rangle$ are orthogonal to each other, we can write the two vectors $|v_0\rangle$ and $|v_1\rangle$ in the general form:

$$|v_0\rangle = \sum_{j=0}^n K \frac{p_j^*}{\sqrt{\binom{n}{j}}} |0_c\rangle^{\otimes m} \otimes |s_j^n\rangle + Kx|\theta_0\rangle, \\ |v_1\rangle = \sum_{j=0}^n K \frac{q_j^*}{\sqrt{\binom{n}{j}}} |0_c\rangle^{\otimes m} \otimes |s_j^n\rangle + Ky|\theta_0\rangle + Kw|\theta_1\rangle, \quad (15)$$

where $|\theta_0\rangle$ and $|\theta_1\rangle$ are two vectors orthogonal to each other and to all vectors $|s_j^n\rangle$, and x, y, w are free parameters (for more details on the derivation, see Sec. I of Supplemental Material [33]). Without loss of generality, we can assume that x and w are real positive parameters since the eventual phases can be absorbed by a redefinition of the vectors $|\theta_0\rangle$ and $|\theta_1\rangle$. Now, we have to impose that the covectors associated with the vectors $|v_0\rangle$ and $|v_1\rangle$ are proper rows of a unitary transformation. Thus, we need to impose that the two vectors are orthonormal.

Considering that there are four variables but only three equations, we solve the system as a function of the free parameter w . We first define the following variables:

$$a = \sum_{j=0}^n \frac{|q_j|^2}{\binom{n}{j}}, \quad b = \sum_{j=0}^n \frac{|p_j|^2}{\binom{n}{j}}, \quad c = \sum_{j=0}^n \frac{p_j q_j^*}{\binom{n}{j}}. \quad (16)$$

We can then solve the system of equations, leading to

$$x = \sqrt{\frac{l + |w|^2 + a - b}{2}}, \quad (17)$$

$$y = \frac{-c}{|c|} \sqrt{\frac{l - |w|^2 - a + b}{2}}, \quad (18)$$

$$K = \sqrt{\frac{2}{l + |w|^2 + a + b}}, \quad (19)$$

where $l = \sqrt{(|w|^2 + a - b)^2 + 4|c|^2}$.

It is possible to note that the solution exists for every combination of the polynomials coefficients and for every value of w . Hence, to reduce the number of required basis vectors, we fix $w = 0$, making the vector $|\theta_1\rangle$ unnecessary.

With those parameters, we can construct the orthonormal vectors $|v_{0/1}\rangle$ and, by completing them to an orthonormal basis (see Sec. II of Supplemental Material [33], which includes Ref. [34]), we can construct the corresponding unitary matrix U . The only remaining open issue is the possibility of finding a vector $|\theta_0\rangle$ that is orthogonal to all the vectors $|0_c\rangle^{\otimes m} \otimes |s_i^n\rangle$. A Hilbert space generated by $n + m$ qubits has dimension 2^{n+m} and the number of vectors $|0_c\rangle^{\otimes m} \otimes |s_i^n\rangle$ is $n + 1$. In order to exist a vector $|\theta_0\rangle$, we need that $2^{n+m} > n + 1$, which gives the condition $m > \log_2(n + 1) - n$. That condition means that for $n \geq 2$ no ancillary qubits are required, saturating the lower bound of Eq. (9), and that only a single ancillary qubit is needed for certain functions of degree one or less. We note also that for $n = 1$ there are functions where the ancillary qubit is not required. This happens when $x = 0$ and $y = 0$, which translates to the condition $a = b$ and $c = 0$.

This analysis proves that the set of simulable functions coincides with the set of rational functions $S = \text{Rat}(z)$. We also show the connection between the minimum number of qubits required to simulate a function and the degree of the function itself.

C. Success probability

Now, we analyze the success probability of the quantum circuit to generate the correct output state. The success probability is

$$\text{Pr}(z) = |\langle v_0||\psi_I\rangle|^2 + |\langle v_1||\psi_I\rangle|^2. \quad (20)$$

By using the expression obtained previously, we can write

$$\text{Pr}(z) = \frac{K^2(|\sum_{j=0}^n p_j z^j|^2 + |\sum_{j=0}^n q_j z^j|^2)}{(1 + |z|^2)^n}. \quad (21)$$

Optimization over the parameter w . First of all, we aim at finding the maximum success probability for a given number of exploited qubits (i.e., for fixed n). We maximize the success probability as a function of $|w|^2$, since it is the only free parameter. Calculating the derivative, we can see that the success probability $\text{Pr}(z)$ is always a decreasing function of $|w|^2$, independently of other parameters. Hence, the maximum probability is reached for $|w|^2 = 0$ showing that the previous construction of the vectors $|v_{0/1}\rangle$ is optimal for both the number of basis vectors and the success probability. Hence, the

maximum success probability $\text{Pr}_n(z)$ for a given number of qubits n is

$$\text{Pr}_n(z) = \frac{2(|\sum_{j=0}^n p_j z^j|^2 + |\sum_{j=0}^n q_j z^j|^2)}{(1 + |z|^2)^n [\sqrt{(a-b)^2 + 4|c|^2} + a + b]}. \quad (22)$$

Optimization over n . The next step is to find the maximum success probability by varying the number of qubits. A direct comparison between the success probabilities associated with two QQBF processes with a different number of qubits is not straightforward, since they depend on the states. Consequently, a well-defined optimization can be carried out by considering an input state ensemble and its probability distribution. To provide concrete insights, we therefore derive general bounds based on state ensemble analysis and complement them with a detailed examination of representative cases.

In general, if we use a number of qubits equal to the degree of the function $f(z)$, then the probability of success is nonzero for any value of z (also for $z \rightarrow \infty$). This property follows from the fact that the polynomials $P(z)$ and $Q(z)$ that compose the function $f(z)$ are coprime and thus possess no zeros in common. If we are interested in maximizing the success probability for a particular state $|z\rangle$ or of its mean value over a state ensemble, then we can consider the possibility of increasing the number of qubits employed and therefore the degree of the polynomials. To accomplish this, given the function $f(z) = P(z)/Q(z)$, we multiply both polynomials $P(z)$ and $Q(z)$ by the same factor $z - r$, which modifies the success probability, increasing it for some value and adding a zero for $z = r$. In this context, increasing only the number of employed qubits, leaving the polynomials unchanged, is equivalent to the case where $r \rightarrow \infty$.

As explicative examples, we analyze the case of the average success probability over the uniform distribution of all the qubits on the Bloch sphere. In such a scenario, the mean success probability will be

$$\langle \text{Pr}_n \rangle_U = \frac{2(a+b)}{(n+1)[\sqrt{(a-b)^2 + 4|c|^2} + a + b]}. \quad (23)$$

Instead, if we consider a uniform distribution only on the covariant states, i.e., states in the form $(e^{i\phi}|0\rangle + |1\rangle)/\sqrt{2}$, then the mean success probability is

$$\langle \text{Pr}_n \rangle_C = \frac{\sum_{j=0}^n |p_j|^2 + |q_j|^2}{2^n [\sqrt{(a-b)^2 + 4|c|^2} + a + b]}. \quad (24)$$

Figure 2 shows the trends of those mean probabilities for the function $g(z) = \eta z^2$ as a function of the parameter η and for different numbers of qubits n employed by the quantum circuit of the QQBF. We note that, as the parameter η changes, the number of optimal qubits changes in a nontrivial manner, and the regions are different depending on the set of states considered.

With these last considerations on success probabilities, we have fully characterized the quantum-to-quantum Bernoulli factory problem.

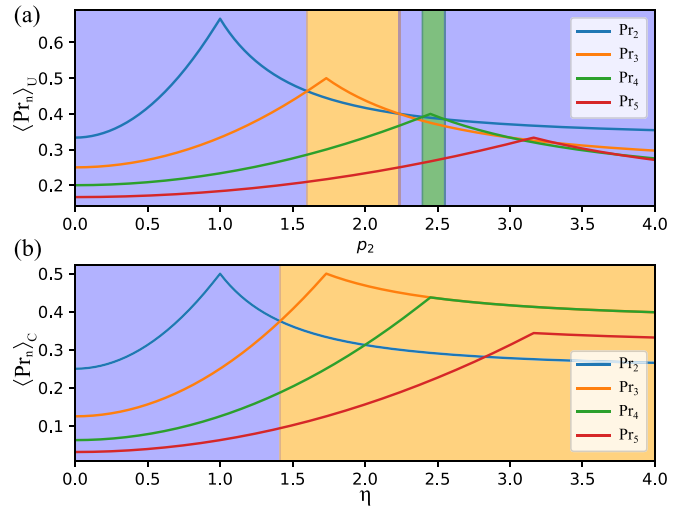


FIG. 2. Average success probabilities $\langle \text{Pr}_n \rangle_{U/C}$ for the function $g(z) = \eta z^2$. Representation of the success probability for the function $g(z) = \eta z^2$ for different numbers of qubits employed by the quantum circuit and for different sets of states. In panel (a), we considered the average over the uniform distribution of all the qubits, and in panel (b) we consider the average only on the equatorial states. The background color represents the region in which a particular probability is higher than the others. It can be deduced from the figures that the optimal number of qubits required depends strongly on both the function itself and the set of states considered.

D. Asymptotic behavior

In this section, we analyze the asymptotic behavior of the success probability and the gate count for implementing a QQBF. The success probability is related to the time complexity, since the inverse gives the average number of repetitions required to have a result. If we consider the worst-case scenario, i.e., the minimum success probability, we have that the probability goes down exponentially, with the degree of the function, but is not null (see Sec. III of Supplemental Material [33] for the demonstration, which includes Ref. [35]). If, instead of considering the worst-case scenario, we consider the average success probability calculated in Eq. (23), it scales as $\Theta(1/n)$. These considerations indicate that if we intend the Bernoulli factory as a protocol to implement specific states, it can become infeasible. However, when the protocol is used to apply a function to random states, as in cryptographic applications, it is efficient.

For the gate count, in Sec. IV of Supplemental Material [33] which includes Refs. [30,36,37], we provide a demonstration that the asymptotic complexity is polynomial. In particular, if we consider the universal set of gates $\{\text{CNOT}, R_y(\theta), R_z(\alpha), Ph(\delta)\}$, the complexity is $O(n^3)$.

E. Summary

In summary, we have identified the set of simulable functions by showing that it coincides with the set of rational functions $S = \text{Rat}(z)$. We also show that the minimum number of qubits required for the simulation of a function $f(z) \in \text{Rat}(z)$ is $n = \deg(f(z))$ and no ancillary qubit is required ($m = 0$), except in the case $\deg(f(z)) = 1$, where at most one

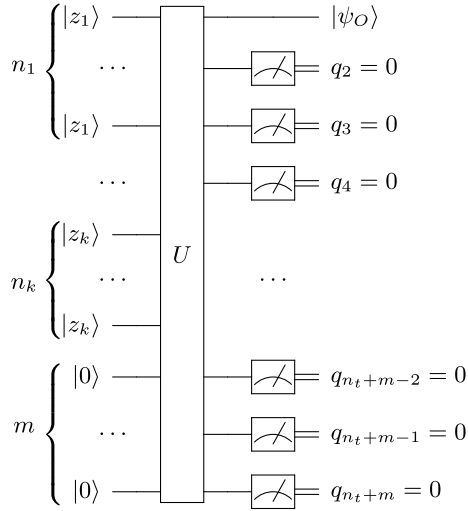


FIG. 3. Multivariate quantum-to-quantum Bernoulli factory general circuit. The circuit takes in input n_k qubits in the state $|z_k\rangle$ for a total of n_t and m ancillary qubits in the state $|0\rangle$. The rest of the circuit is similar to that of Fig. 1. As before, this circuit is the most general one implementing a multivariate quantum-to-quantum Bernoulli factory.

is needed. In addition, a systematic procedure for constructing the quantum circuit related to a particular function was presented, showing how the circuit is the most efficient in terms of qubits used and success probability. In this analysis, the possibility of tracing some qubits instead of measuring them was not discussed. In Sec. V of Supplemental Material [33], we show that this possibility does not bring any advantage in terms of resources or success probability.

IV. MULTIVARIATE QUANTUM-TO-QUANTUM BERNOULLI FACTORY

In the following, we present an extension of the quantum-to-quantum Bernoulli Factory problem, taking into account the possibility of having more than one “hidden” state at the input of the circuit. This means that instead of having a state $|z\rangle$, we have a set of different states $\{|z_1\rangle, \dots, |z_k\rangle\}$. In addition, the function becomes a multivariate one: $g(z_1, \dots, z_k)$. We refer to this variant of the problem as multivariate quantum-to-quantum Bernoulli factory. Here, we characterize all relevant aspects of this extension following the same method previously presented for the original problem.

The more general circuit implementing the multivariate quantum-to-quantum Bernoulli factory is the same as the previous case, with the difference that the input can be composed of more than one hidden state, as depicted in Fig. 3. Analogously to the approach of Sec. III, it can be shown that the set of constructible functions $g(z_1, \dots, z_k)$ is a subset of the set of multivariate complex rational functions $\text{Rat}(z_1, \dots, z_k)$. Moreover, adapting the previous construction method, it is possible to show that for every function of the form $g(z_1, \dots, z_k) \in \text{Rat}(z_1, \dots, z_k)$ it is possible to construct a quantum circuit implementing the associated multivariate Bernoulli factory. In addition, one can make the circuit use the minimum number of qubits for each variable that corresponds

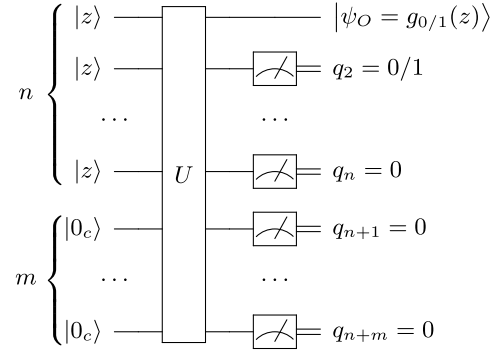


FIG. 4. Multifunctional quantum Bernoulli factory general circuit. This circuit implementing a multifunctional quantum Bernoulli factory is similar to Fig. 1. The difference is at the measurement stage. Previously, all the measures had to return the outcome 0. In this case, if the measure q_2 returns 0, the circuit implements the function $g_0(z)$, while if the outcome is 1 the circuit implements the function $g_1(z)$. As before, this circuit is the most general one implementing a multifunctional quantum-to-quantum Bernoulli factory.

to the lower bound $n_j = \deg_j(g(z_1, \dots, z_k))$ and without the necessity of ancillary. The only exception in the possibility of not using ancillary qubits is when $\forall j \deg_j(g(z_1, \dots, z_k)) = 1$, in such a situation an ancillary qubit is needed. An explicit demonstration is reported in Sec. VI of Supplemental Material [33].

V. MULTIFUNCTIONAL QUANTUM-TO-QUANTUM BERNOULLI FACTORY

This second extension is motivated by the intrinsic probabilistic nature of the quantum-to-quantum Bernoulli factory, which requires heralding on specific measurement outcomes to implement the desired function. Extending such a consideration, we can say that the Bernoulli factory implements a different function for each measurement outcome. Therefore, this leads to the definition of a second extension of the quantum-to-quantum Bernoulli factory problem, where we examine the possibility of implementing more than one function at the same time.

We define a multifunctional quantum-to-quantum Bernoulli factory associated with a tuple of functions $(g_0, \dots, g_l)$ as a QQBF implementing the functions $g_0, \dots, g_l$ depending on the output of the heralding measurement. Below, we consider only the simplest case of two functions, but the analysis can also be extended to cases involving more functions. Starting from considerations similar to those used for the original problem, namely, that all the hidden information is only in the input states, we can say that the most general quantum circuit implementing a multifunctional quantum-to-quantum Bernoulli factory for two functions is the one depicted in Fig. 4. The circuit is identical to the one implementing the QQBF with the difference that the measurement of the second qubit q_2 indicates which function $g_0(z)$ or $g_1(z)$ is implemented by the circuit. Given two simulable functions, it is always possible to construct a multifunctional quantum-to-quantum Bernoulli factory (see Sec. VII of Supplemental Material [33], which includes

Ref. [38]). However, the success probabilities of individual functions will almost always turn out to be lower than the corresponding probabilities if one constructs a set of quantum-to-quantum Bernoulli factories implementing the single functions.

With this consideration in mind, we propose a slightly different definition. More specifically, we introduce a hierarchy for the functions, which means that we prioritize the success probability of some functions over the others. In this context, we say that a function $g_1(z)$ is *compatible* with a function $g_0(z)$ if it is possible to implement a multifunctional quantum-to-quantum Bernoulli factory, where the success probability of the function $g_0(z)$ is the same achievable with a dedicated quantum-to-quantum Bernoulli factory. To understand why we suggest this notion of compatibility, let us consider the following scenario. We suppose that, to implement a specific algorithm, it is necessary to perform two different QQBFs with the same input states that, respectively, implement the functions $g_0(z)$ and $g_1(z)$. If the function $g_1(z)$ is compatible with the function $g_0(z)$, we can implement a multivariate quantum-to-quantum Bernoulli factory without changing the success probability of the function $g_0(z)$, but with the additional functionality that, if the circuit returns a sample from the function $g_1(z)$, we can in principle store the output state to be used in a second moment when needed, increasing the overall efficiency of the algorithm.

Defining $g_0(z) = P(z)/Q(z)$ and $g_1(z) = R(z)/T(z)$, the condition of compatibility of $g_1(z)$ respect $g_0(z)$ is equivalent to the following conditions:

$$d_1 = \sum_j \left(\frac{p_j^*}{x} - \frac{q_j^*}{y} \right) \frac{r_j}{\binom{n}{j}} = 0, \quad (25)$$

$$d_2 = \sum_j \left(\frac{p_j^*}{x} - \frac{q_j^*}{y} \right) \frac{t_j}{\binom{n}{j}} = 0, \quad (26)$$

where p_j, q_j, r_j, t_j are the coefficients, respectively, of the polynomials $P(z), Q(z), R(z), T(z)$, and x and y are the values defined by Eqs. (17) and (18) with $w = 0$. To prove the statement, we show that the two conditions are necessary and sufficient for the existence of a unitary transformation according to the general circuit of Fig. 4.

Similar to the procedure used in Eq. (10), we call the first four rows of the unitary transformation as the covectors $\langle v_0|$, $\langle v_1|$, $\langle v_2|$, and $\langle v_3|$. The first two rows are fixed by the fact that we want to obtain a success probability for $g_0(z)$ equal to the one achievable with a dedicated quantum-to-quantum Bernoulli factory. Hence, $|v_0\rangle$ and $|v_1\rangle$ have the following forms:

$$|v_0\rangle = \sum_{j=0}^n K \frac{p_j^*}{\sqrt{\binom{n}{j}}} |0_c\rangle^{\otimes m} \otimes |s_j^n\rangle + Kx|\theta_0\rangle \quad (27)$$

and

$$|v_1\rangle = \sum_{j=0}^n K \frac{q_j^*}{\sqrt{\binom{n}{j}}} |0_c\rangle^{\otimes m} \otimes |s_j^n\rangle + Ky|\theta_0\rangle, \quad (28)$$

where x, y , and K are those found in Eqs. (17)–(19) with $w = 0$. The other two vectors can be expressed in the general

forms as

$$|v_2\rangle = \sum_{j=0}^n H \frac{r_j^*}{\sqrt{\binom{n}{j}}} |0_c\rangle^{\otimes m} \otimes |s_j^n\rangle + Ha_1|\theta_0\rangle + Ha_2|\theta_1\rangle \quad (29)$$

and

$$|v_3\rangle = \sum_{j=0}^n H \frac{t_j^*}{\sqrt{\binom{n}{j}}} |0_c\rangle^{\otimes m} \otimes |s_j^n\rangle + Ha_3|\theta_0\rangle + Ha_4|\theta_1\rangle + Ha_5|\theta_2\rangle, \quad (30)$$

where H is the normalization factor and a_1, a_2, a_3, a_4 , and a_5 are free parameters. To ensure that the four vectors represent four rows of a unitary transformation, they must be orthonormal between each other as $\langle v_i | v_j \rangle = \delta_{i,j}$. While some orthonormality conditions are already satisfied (namely, $\langle v_0 | v_0 \rangle = 1$, $\langle v_1 | v_1 \rangle = 1$, and $\langle v_0 | v_1 \rangle = 0$), the remaining four are the critical ones since there are four equations and two free parameters. The following two conditions correspond to

$$\langle v_0 | v_2 \rangle = 0 \Rightarrow \sum_j \frac{p_j r_j^*}{\binom{n}{j}} + x^* a_1 = 0, \quad (31)$$

$$\langle v_1 | v_2 \rangle = 0 \Rightarrow \sum_j \frac{q_j r_j^*}{\binom{n}{j}} + y^* a_1 = 0. \quad (32)$$

A parameter a_1 that solves both the equations exists if Eq. (25) is satisfied. The other constraint descends from the remaining set of orthonormality conditions. If Eqs. (25) and (26) are satisfied, then it is possible to derive the values of a_1 and a_3 . The orthonormality of states $|v_i\rangle$ allow us always to derive the parameters a_2, a_4 , and H . Furthermore, fixing the free parameter $a_5 = 0$, we can reach the maximum achievable probability. With this, we have the first four rows of the unitary matrix U . By completing to an orthonormal basis, we can construct the circuit implementing the desired multifunctional quantum-to-quantum Bernoulli factory.

In this way, we prove the necessity and sufficiency of the conditions in Eqs. (25) and (26) to test if a function $g_1(z)$ is compatible with a function $g_0(z)$. Also, we explicitly construct a quantum circuit that implements the most efficient multifunctional quantum-to-quantum Bernoulli factory associated with the functions.

VI. APPLICATION TO THE SUM AND PRODUCT OPERATION

This section shows an application of the theory developed in this paper for a specific case. In particular, we will construct the multivariate QQBFs corresponding to the sum ($z_1 + z_2$) and product ($z_1 z_2$) functions and compare them with those presented in the article by Jiang *et al.* [22], where the QQBF was first proposed. We will then analyze the compatibility of the two functions and eventually construct the corresponding multifunctional QQBF.

A. Product $z_1 z_2$

The first operation that we analyze is the product operation $g(z_1, z_2) = z_1 z_2$; since it has degree one in both variables, this tells us that we need only one qubit per variable. The

coefficients of the function are $p_{1,1} = 1$, $q_{0,0} = 1$, $p_{i,j} = 0$ for $(i, j) \neq 1, 1$, and $q_{i,j} = 0$ for $(i, j) \neq (0, 0)$. This gives us $a = 1$, $b = 1$, $c = 0$, leading to $x = 0$, $y = 0$, $K = 1$. Since $a = b$ and $c = 0$, this means that ancillary qubits are not required. The two vectors v_0 and v_1 are

$$|v_0\rangle = |00\rangle, \quad (33)$$

$$|v_1\rangle = |11\rangle, \quad (34)$$

and the final unitary transformation is

$$U = |00\rangle\langle 00| + |10\rangle\langle 11| + |11\rangle\langle 10| + |01\rangle\langle 01|, \quad (35)$$

which is a CNOT where the first qubit acts as a control and the second qubit is the target, as presented in Ref. [22]. The corresponding success probability is

$$\text{Pr.}(z_1, z_2) = \frac{|z_1 z_2|^2 + 1}{(1 + |z_1|^2)(1 + |z_2|^2)}. \quad (36)$$

B. Sum $z_1 + z_2$

The second operation that we analyze is the sum $g(z_1, z_2) = z_1 + z_2$. It is also a function of degree one in both variables, which implies that it can be implemented with one qubit for each variable. The coefficients of the function are $p_{i,i} = 0$, $p_{i,j} = 1$ for $i \neq j$, $q_{0,0} = 1$, and $q_{i,j} = 0$ for $(i, j) \neq (0, 0)$. This gives us $a = 1$, $b = 2$, $c = 0$, leading to $x = 0$, $y = 1$, $K = 2^{-1/2}$. Since $a \neq b$, this means that the operation requires an ancillary qubit. Choosing $|\theta_0\rangle = |001\rangle$, the two vectors v_0 and v_1 are

$$|v_0\rangle = \frac{|010\rangle + |100\rangle}{\sqrt{2}}, \quad (37)$$

$$|v_1\rangle = \frac{|110\rangle + |001\rangle}{\sqrt{2}}, \quad (38)$$

and the corresponding unitary transformation deduced with the algorithm presented in Sec. II of Supplemental Material [33] is

$$U = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 & 0 \\ -\frac{1}{\sqrt{2}} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad (39)$$

where the states are ordered with the least significant bit on the left. The corresponding success probability is

$$\text{Pr}_+(z_1, z_2) = \frac{|z_1 + z_2|^2 + 1}{2(1 + |z_1|^2)(1 + |z_2|^2)}. \quad (40)$$

In Ref. [22], the authors do not propose the sum operation but a slightly different operation where the sum is divided by $\sqrt{2}$, $g(z_1, z_2) = \frac{z_1 + z_2}{\sqrt{2}}$. In this case, we find with our construction $a = 2$, $b = 2$, $c = 0$, leading to $x = 0$, $y = 0$, $K = 2^{-1/2}$,

which implies that there is no need for an ancillary qubit. The corresponding unitary transformation is

$$U = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \end{pmatrix}, \quad (41)$$

which is the same unitary matrix found in Ref. [22]. The corresponding probability is

$$\text{Pr}_+(z_1, z_2) = \frac{|z_1 + z_2|^2 + 2}{2(1 + |z_1|^2)(1 + |z_2|^2)}. \quad (42)$$

To compare our results with existing approaches in the literature, we can construct the sum operation using the circuits proposed in Ref. [22] by concatenating the previous circuit with a product operation having as input a qubit with $z = \sqrt{2}$. In that case, the total success probability will be

$$\text{Pr}_+(z_1, z_2) = \frac{|z_1 + z_2|^2 + 1}{3(1 + |z_1|^2)(1 + |z_2|^2)}. \quad (43)$$

Thus, the circuits known in the literature provide lower efficiency than the optimal circuit found in Eq. (40) with our approach.

C. Compatibility between the sum and the product operation

In this section, we identify a multifunctional QQBF that implements both the product and the sum operation, testing if the sum operation is compatible with the product one, or vice versa.

First, we test if the sum is compatible with the product operation by evaluating the two conditions in Eqs. (25) and (26). Since both x and y are null, we need to modify the functions as $g_0(z_1, z_2) = z_1 z_2 + \epsilon$ and then take the limit for $\epsilon \rightarrow 0$. Performing all the calculations, we obtain $x = 2^{-1/2}\epsilon$, $y = (3/2)^{1/2}\epsilon$, leading to $d_1 = 0$, $d_2 = (3/2)^{1/2} - 2^{1/2}/\epsilon$. In the limit $\epsilon \rightarrow 0$, the condition s_2 is not satisfied, implying that the sum operation is not compatible with the product.

Now, we verify whether the product operation is compatible with the sum. Similar to the previous case, since $x = 0$ we need to modify the sum operation $g_0(z_1, z_2) = z_1 + z_2 + \epsilon$. Performing all calculations described above, we obtain $x = \epsilon(1 - \epsilon^2)$, $y = 1 + \epsilon^2$, leading to $d_1 = 0$, $d_2 = 2\epsilon^2$. In this case, both conditions are satisfied in the limit of $\epsilon \rightarrow 0$ meaning that the product operation is compatible with the sum operation. Proceeding with the calculation to find the unitary matrix as described above, we obtain the four vectors

$$|v_0\rangle = \frac{|010\rangle + |100\rangle}{\sqrt{2}}, \quad (44)$$

$$|v_1\rangle = \frac{|110\rangle + |001\rangle}{\sqrt{2}}, \quad (45)$$

$$|v_2\rangle = \frac{|000\rangle + |101\rangle}{\sqrt{2}}, \quad (46)$$

$$|v_3\rangle = \frac{|110\rangle - |001\rangle}{\sqrt{2}}, \quad (47)$$

and the final unitary matrix

$$U = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \quad (48)$$

In this case, the success probability of the sum operation is equal to the optimal one of Eq. (40). On the contrary, the success probability of the product is

$$\Pr.(z_1, z_2) = \frac{|z_1 z_2|^2 + 1}{2(1 + |z_1|^2)(1 + |z_2|^2)}, \quad (49)$$

which is half of the optimal one reported in Eq. (36).

VII. DISCUSSION

In this work, we provide a comprehensive analysis of the problem of a quantum-to-quantum Bernoulli factory. The article presents a constructive proof for the characterization of the quantum-to-quantum Bernoulli factory, independently establishing the set of simulable functions as the rational functions. While the proof aligns with previous results [22], our approach enables a direct complexity analysis, explicitly quantifying the protocols' qubit requirements and success probability. In particular, we show that the minimum number of required qubits coincides with the degree of the function without the necessity of ancillary qubits, except for degree one, where at most one ancillary qubit is required. We also provide an analytical expression for the maximal success probability and a procedure for the construction of the quantum circuit that saturates those bounds.

Moreover, we formalize and analyze two extensions of the original problem called, respectively, the multivariate

quantum-to-quantum Bernoulli factory and the multifunctional quantum-to-quantum Bernoulli factory. In those variants, we allow, respectively, the possibility to employ more than one “hidden” variable at the input of the circuit or the implementation of more than one function within the same protocol. Similarly to the original problem, we analyze the computational complexity of the two extensions and provide a procedure for the construction of the quantum circuit implementing the desired protocol.

With those analyses, we provide a comprehensive overview of the protocol, opening the possibility of employing the quantum-to-quantum Bernoulli factory as a subroutine for larger quantum computation and quantum communication protocols, and the possibility of more efficient experimental implementation. Furthermore, this work can be at the basis of further theoretical developments of the algorithm and of the proposal of extensions of the problem, such as different input/output states or different resources employed, such as the one proposed in Ref. [39].

ACKNOWLEDGMENTS

We acknowledge support from the ERC Advanced Grant No. QU-BOSS (QUantum advantage via nonlinear BO-Son Sampling, Grant Agreement No. 884676), from the ERC Proof of Concept grant POQUB (PhOtonics QUantum Bernoulli factory, Grant Agreement No. 101212872), from the project QU-DICE, Fare Ricerca in Italia, Ministero dell'università e della ricerca (QUantum ranDomness and sImulation proCEssing via nonlinear boson sampling, code: R20TRHTSPA), and from PNRR MUR Project No. PE0000023-NQSTI (National Quantum Science and Technology Institute, Spoke 4).

DATA AVAILABILITY

The data that support the findings of this article are not publicly available. The data are available from the authors upon reasonable request.

-
- [1] M. S. Keane and G. L. O'Brien, A Bernoulli factory, *ACM Trans. Model. Comput. Simul.* **4**, 213 (1994).
 - [2] R. P. Leme and J. Schneider, Multiparameter Bernoulli factories, *Ann. Appl. Probab.* **33**, 3987 (2023).
 - [3] R. Niazadeh, R. P. Leme, and J. Schneider, Bernoulli factories for flow-based polytopes, *SIAM J. Discrete Math.* **38**, 726 (2024).
 - [4] R. Niazadeh, R. P. Leme, and J. Schneider, Combinatorial Bernoulli factories, *Bernoulli* **29**, 1246 (2023).
 - [5] J. M. Flegal and R. Herbei, Exact sampling for intractable probability distributions via a Bernoulli factory, *Electron. J. Stat.* **6**, 10 (2012).
 - [6] D. Vats, F. B. Gonçalves, K. Łatuszyński, and G. O. Roberts, Efficient Bernoulli factory Markov chain Monte Carlo for intractable posteriors, *Biometrika* **109**, 369 (2022).
 - [7] F. B. Gonçalves, K. Łatuszyński, and G. O. Roberts, Exact Monte Carlo likelihood-based inference for jump-diffusion processes, *J. R. Stat. Soc. B* **85**, 732 (2023).
 - [8] R. Herbei and L. M. Berliner, Estimating ocean circulation: An MCMC approach with approximated likelihoods via the Bernoulli factory, *J. Am. Stat. Assoc.* **109**, 944 (2014).
 - [9] J. Koskela, K. Łatuszyński, and D. Spanò, Bernoulli factories and duality in Wright–Fisher and Allen–Cahn models of population genetics, *Theor. Popul. Biol.* **156**, 40 (2024).
 - [10] G. Morina, K. Łatuszyński, P. Nayar, and A. Wendland, From the Bernoulli factory to a dice enterprise via perfect sampling of Markov chains, *Ann. Appl. Probab.* **32**, 327 (2022).
 - [11] V. Goyal and K. Sigman, On simulating a class of Bernstein polynomials, *ACM Trans. Model. Comput. Simul.* **22**, 1 (2012).
 - [12] E. Mossel and Y. Peres, New coins from old: Computing with unknown bias, *Combinatorica* **25**, 707 (2005).
 - [13] K. Łatuszyński, I. Kosmidis, O. Papaspiliopoulos, and G. O. Roberts, Simulating events of unknown probabilities via reverse time martingales, *Random Struct. Algorithms* **38**, 441 (2011).
 - [14] S. Nacu and Y. Peres, Fast simulation of new coins from old, *Ann. Appl. Probab.* **15**, 93 (2005).

- [15] L. Mendo, An asymptotically optimal Bernoulli factory for certain functions that can be expressed as power series, *Stochastic Processes Appl.* **129**, 4366 (2019).
- [16] P. Flajolet, M. Pelletier, and M. Soria, On Buffon machines and numbers, in *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms* (Society for Industrial and Applied Mathematics, Philadelphia, PA, 2011).
- [17] O. Holtz, F. Nazarov, and Y. Peres, New coins from old, smoothly, *Constr. Approx.* **33**, 331 (2011).
- [18] H. Dale, D. Jennings, and T. Rudolph, Provable quantum advantage in randomness processing, *Nat. Commun.* **6**, 8203 (2015).
- [19] H. Dale, Quantum coins and quantum sampling, Ph.D. thesis, Imperial College London, 2016.
- [20] R. B. Patel, T. Rudolph, and G. J. Pryde, An experimental quantum Bernoulli factory, *Sci. Adv.* **5**, eaau6668 (2019).
- [21] X. Yuan, K. Liu, Y. Xu, W. Wang, Y. Ma, F. Zhang, Z. Yan, R. Vijay, L. Sun, and X. Ma, Experimental quantum randomness processing using superconducting qubits, *Phys. Rev. Lett.* **117**, 010502 (2016).
- [22] J. Jiang, J. Zhang, and X. Sun, Quantum-to-quantum Bernoulli factory problem, *Phys. Rev. A* **97**, 032303 (2018).
- [23] X. Zhan, K. Wang, L. Xiao, Z. Bian, and P. Xue, Experimental demonstration of quantum-to-quantum Bernoulli factory, *Phys. Rev. A* **102**, 012605 (2020).
- [24] Y. Liu, J. Jiang, P. Zhu, D. Wang, J. Ding, X. Qiang, A. Huang, P. Xu, J. Zhang, G. Tian, X. Fu, M. Deng, C. Wu, X. Sun, X. Yang, and J. Wu, General quantum Bernoulli factory: Framework analysis and experiments, *Quantum Sci. Technol.* **6**, 045025 (2021).
- [25] F. Hoch, T. Giordani, L. Castello, G. Carvacho, N. Spagnolo, F. Ceccarelli, C. Pentangelo, S. Piacentini, A. Crespi, R. Osellame, E. F. Galvão, and F. Sciarrino, Modular quantum-to-quantum Bernoulli factory in an integrated photonic processor, *Nat. Photonics* **19**, 12 (2025).
- [26] G. Rodari, F. Hoch, A. Suprano, T. Giordani, E. Negro, G. Carvacho, N. Spagnolo, E. F. Galvão, and F. Sciarrino, Polarization-encoded photonic quantum-to-quantum Bernoulli factory based on a quantum dot source, *Sci. Adv.* **10**, eado6244 (2024).
- [27] E. Kashefi and A. Pappa, Multiparty delegated quantum computing, *Cryptography* **1**, 12 (2017).
- [28] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind quantum computation, *Phys. Rev. A* **96**, 012303 (2017).
- [29] B. Polacchi, D. Leichtle, L. Limongi, G. Carvacho, G. Milani, N. Spagnolo, M. Kaplan, F. Sciarrino, and E. Kashefi, Multi-client distributed blind quantum computation with the Qline architecture, *Nat. Commun.* **14**, 7743 (2023).
- [30] A. Bäertschi and S. Eidenbenz, Deterministic preparation of Dicke states, in *Fundamentals of Computation Theory*, edited by G. L. Antoni, J. Jesper, and L. Christos (Springer International Publishing, Cham, Switzerland, 2019), pp. 126–139.
- [31] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2009).
- [32] Y. Gurevich and A. Blass, Quantum circuits with classical channels and the principle of deferred measurements, *Theor. Comput. Sci.* **920**, 21 (2022).
- [33] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/k8kd-58h8> for further demonstrations of the main results reported in the main text.
- [34] W. T. V. William, H. Press, and S. A. Teukolsky, *Numerical Recipes: The Art of Scientific Computing*, 3rd ed. (Cambridge University Press, Cambridge, England, 2007).
- [35] E. Fricain, A. Hartmann, W. T. Ross, and D. Timotin, An analytic approach to estimating the solutions of Bézout’s polynomial identity, [arXiv:2310.12734](https://arxiv.org/abs/2310.12734).
- [36] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Elementary gates for quantum computation, *Phys. Rev. A* **52**, 3457 (1995).
- [37] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Experimental realization of any discrete unitary operator, *Phys. Rev. Lett.* **73**, 58 (1994).
- [38] E. Levy and O. M. Shalit, Dilation theory in finite dimensions: The possible, the impossible and the unknown, *Rocky Mt. J. Math.* **44**, 203 (2014).
- [39] T. J. Yoder, Building and bounding quantum Bernoulli factories, 2025, <https://www.scottaaronson.com/6s899/tedyoder.pdf>.