Efficient Classical Simulation of Continuous Variable Quantum Information Processes

Stephen D. Bartlett and Barry C. Sanders
Department of Physics and Centre for Advanced Computing–Algorithms and Cryptography, Macquarie University, Sydney, New South Wales 2109, Australia

Samuel L. Braunstein and Kae Nemoto
Informatics, Bangor University, Bangor, LL57 1UT, United Kingdom
(Received 11 September 2001; revised manuscript received 26 November 2001; published 14 February 2002)

We obtain sufficient conditions for the efficient simulation of a continuous variable quantum algorithm or process on a classical computer. The resulting theorem is an extension of the Gottesman-Knill theorem to continuous variable quantum information. For a collection of harmonic oscillators, any quantum process that begins with unentangled Gaussian states, performs only transformations generated by Hamiltonians that are quadratic in the canonical operators, and involves only measurements of canonical operators (including finite losses) and suitable operations conditioned on these measurements can be simulated efficiently on a classical computer.

DOI: 10.1103/PhysRevLett.88.097904 PACS numbers: 03.67.Lx, 02.20.–a, 42.50.–p

Quantum mechanics allows for information processing that could not be performed classically. In particular, it may be possible to perform an algorithm efficiently on a quantum computer that cannot be performed efficiently on a classical one. Significant effort is now underway to construct quantum algorithms and processes that yield such a speedup. The Gottesman-Knill (GK) theorem [1] for discrete variable (qubit) quantum information provides a valuable tool for assessing the classical complexity of a given process. Essentially, it states that any quantum algorithm that initiates in the computational basis and employs only a restricted class of gates (Hadamard, phase, CNOT, and Pauli gates), along with projective measurements in the computational basis, can be efficiently simulated on a classical computer. (For a precise formulation and proof of this remarkable theorem, see [2].) The GK theorem reveals that a large class of quantum algorithms does not provide a speedup over classical processes. In fact, recent work has placed even stronger constraints on the potential speedup of fermionic quantum computers [3].

In addition to the successes of qubit-based algorithms, quantum information over continuous variables (CV) has yielded many exciting advances, both theoretically and experimentally, in fields such as quantum teleportation [4,5], quantum cryptography [6–9], and potentially quantum computation [10]. CV algorithms could also perform computational tasks more efficiently than is possible classically. To assess the computational complexity of these tasks, it is necessary to develop an extension of the GK theorem: What continuous variable processes can be efficiently simulated on a classical computer? As a CV quantum information process involves coupled canonical systems, this question of efficient classical simulation is related to asking under what conditions a quantum mechanical system can be modeled by a classical one. As noted by Feynman [11], a key advantage of a quantum computer is its ability to simulate quantum systems that cannot be efficiently simulated classically.

The issue of efficient classical simulation of a CV process is more involved than for the discrete case. One notable difference is that the quantum states and the unitary transformations involved are described by real-valued (as opposed to integer-valued) parameters, and these parameters must be described on a discrete classical computer with some assumption of error or limited precision. Also, the states used in CV experiments are approximations to the idealized computational basis. These basis states are infinitely squeezed states, whereas any experimental implementation will involve finitely squeezed states thus deviating from their idealized form [10]. A good classical simulation must be robust against such deviations. Measurements are part of the quantum computation and, even in the computational basis, are subject to experimental constraints (such as photodetection efficiency). Classical simulation must also incorporate these measurements.

Despite these complications, we prove in the following an extension of the GK theorem for continuous variables; i.e., we present a set of sufficient conditions for a CV quantum information process which, if satisfied, ensures that it can be efficiently simulated on a classical computer. To prove this theorem, we employ the techniques of stabilizers [2] that are used for qubits. Using the stabilizer formalism, it is often possible to simulate a quantum information process by following the evolution of a set of operators, the Pauli operators, rather than the evolution of quantum states. For CV processes, we show that it is more natural to analyze stabilizers in terms of the *algebras* (i.e., Hamiltonians) that generate them, rather than the groups themselves. We define analogs of the Pauli and Clifford algebras and groups for CV and construct sets of gates (as unitary transformations) that can efficiently simulate any arbitrary transformation in these groups. Any algorithm or

process constructed out of these Clifford group transformations can be efficiently modeled by following the evolution of the Pauli operators rather than the states of the system.

The standard Pauli group $\mathcal{G}_n$ for CV quantum computation on n coupled oscillator systems is the Heisenberg-Weyl group [HW(n)], which consists of phase-space displacement operators for the n oscillators. Unlike the discrete Pauli group for qubits, the group HW(n) is a continuous (Lie) group, and can therefore only be generated by a set of continuously parametrized operators. The algebra hw(n) that generates this group is spanned by the $2n$ canonical operators $\hat{q}_i$, $\hat{p}_i$, $i = 1, \ldots, n$, along with the identity operator $\hat{I}$, satisfying the commutation relations $[\hat{q}_i, \hat{p}_j] = i\hbar\delta_{ij}\hat{I}$. For a single oscillator, the $n = 1$ algebra is spanned by the canonical operators $\{\hat{q}, \hat{p}, \hat{I}\}$ which generate the single oscillator Pauli operators

$$X(q) = e^{-(i/\hbar)q\hat{p}}, \qquad Z(p) = e^{(i/\hbar)p\hat{q}}, \tag{1}$$

with $q, p \in \mathbb{R}$. The Pauli operator $X(q)$ is a position-translation operator (translating by an amount q), whereas $Z(p)$ is a momentum boost operator (kicking the momentum by an amount p). These operators are noncommutative and obey the identity

$$X(q)Z(p) = e^{-(i/\hbar)qp}Z(p)X(q). \tag{2}$$

On the computational basis of position eigenstates $\{|s\rangle; s \in \mathbb{R}\}$ [10,12,13], the Pauli operators act as

$$X(q)|s\rangle = |s + q\rangle, \qquad Z(p)|s\rangle = \exp\left(\frac{i}{\hbar}ps\right)|s\rangle. \tag{3}$$

Note that it is conventional to use highly squeezed states to approximate position eigenstates; these states satisfy the orthogonality relation $\langle s | s'\rangle = \delta(s - s')$ in the limit of infinite squeezing.

The Pauli operators for one system can be used to construct a set of Pauli operators $\{X_i(q_i), Z_i(p_i); i = 1, \ldots, n\}$ for n systems (where each operator labeled by i acts as the identity on all other systems $j \neq i$). This set generates the Pauli group $\mathcal{G}_n$. Note that the Pauli group is only a subgroup of all possible unitary transformations. It is not possible to construct an arbitrary unitary transformation using only the Pauli operators $X(q)$ and $Z(p)$; the Pauli group describes only transformations generated by Hamiltonians that are linear in the canonical variables.

For issues of classical simulation, we will be interested in transformations that lie in the *Clifford group*. The Clifford group $N(\mathcal{G}_n)$ is the group of transformations, acting by conjugation, that preserves the Pauli group $\mathcal{G}_n$; i.e., it is the normalizer of the Pauli group in the (infinite-dimensional) group of all unitary transformations.

Theorem 1: *The Clifford group $N(\mathcal{G}_n)$ for continuous variables is the semidirect product group* [HW(n)]Sp($2n, \mathbb{R}$)*, consisting of all phase-space translations along with all one-mode and two-mode squeezing transformations. This group is generated by inhomogeneous quadratic polynomials in the canonical operators.*

Proof: The most straightforward method to identify the Clifford group will be to identify its algebra. The Clifford algebra consists of all Hamiltonian operators $\hat{H}_c$ satisfying $[\hat{H}_{hw}, \hat{H}_c] \in \text{hw}(n)$ for all $\hat{H}_{hw} \in \text{hw}(n)$. This algebra must obviously include the algebra hw(n), and thus hw(n) is a subalgebra of the Clifford algebra. In addition, this algebra includes all homogeneous quadratic polynomials in the canonical operators $\{\hat{q}_i, \hat{p}_i; i = 1, \ldots, n\}$. This algebra of quadratics consists of Hamiltonians that generate one-mode squeezing transformations [for example, the Hamiltonian $\hat{H}_S = \frac{1}{2}(\hat{q}\hat{p} + \hat{p}\hat{q})$], and also interaction Hamiltonians that generate two-mode squeezing transformations (for example, the interaction Hamiltonian $\hat{H}_{int} = \hat{q}_1 \otimes \hat{p}_2$). The algebra of homogeneous quadratic polynomials in the canonical operators is known as the linear symplectic algebra sp($2n, \mathbb{R}$).

Together, the algebras hw(n) and sp($2n, \mathbb{R}$) form a larger algebra, consisting of *inhomogeneous* quadratic Hamiltonians in the canonical operators $\{\hat{q}_i, \hat{p}_i; i = 1, \ldots, n\}$. This algebra is the semidirect sum algebra [hw(n)]sp($2n, \mathbb{R}$), with hw(n) as an ideal. The group generated by this algebra is the semidirect product group [HW(n)]Sp($2n, \mathbb{R}$). This group includes phase-space displacements (the Pauli group), as well as the squeezing transformations (both one and two mode) of quantum optics [14]. *(QED)*

In order to describe a quantum information process as a circuit, it is necessary to find a set of transformations (gates) that generate the Clifford group; these gates will serve as building blocks for arbitrary Clifford group transformations. Following the derivation by Gottesman *et al.* [15], a set of gates will be defined in terms of the elements of the Clifford algebra (i.e., the Hamiltonians) that generate the transformations.

The SUM gate is the CV analog of the CNOT gate and provides the basic interaction gate for two oscillator systems 1 and 2; it is defined as

$$\text{SUM} = \exp\left(-\frac{i}{\hbar}\,\hat{q}_1 \otimes \hat{p}_2\right). \tag{4}$$

This gate is an interaction gate operation on the Pauli group $\mathcal{G}_2$ for two systems. Referring to the definition (1) for the Pauli operators for a single system, the action of this gate on the $\mathcal{G}_2$ Pauli operators is given by

$$\begin{aligned} \text{SUM: } & X_1(q) \otimes I_2 \to X_1(q) \otimes X_2(q), \\ & Z_1(p) \otimes I_2 \to Z_1(p) \otimes I_2, \\ & I_1 \otimes X_2(q) \to I_1 \otimes X_2(q), \\ & I_1 \otimes Z_2(p) \to Z_1(p)^{-1} \otimes Z_2(p). \end{aligned} \tag{5}$$

This gate describes the unitary transformation used in a backaction evasion or quantum nondemolition process [14].

The Fourier transform F is the CV analog of the Hadamard transformation. It is defined as

$$F = \exp\left(\frac{i}{\hbar}\frac{\pi}{4}(\hat{q}^2 + \hat{p}^2)\right), \tag{6}$$

and the action on the Pauli operators is

$$F: X(q) \to Z(q), \quad Z(p) \to X(p)^{-1}. \tag{7}$$

The "phase gate" $P(\eta)$ is a squeezing operation for CV, defined by

$$P(\eta) = \exp\left(\frac{i}{2\hbar}\eta\hat{q}^2\right), \tag{8}$$

and the action on the Pauli operators is

$$P(\eta): X(q) \to e^{(i/2\hbar)\eta q^2} X(q) Z(\eta q), \quad Z(p) \to Z(p). \tag{9}$$

[The operator $P(\eta)$ is called the phase gate, in analogy to the discrete variable phase gate P [15], because of its similar action on the Pauli operators.]

For discrete variables, it is possible to generate the Clifford group using only the SUM, F, and P gates [15]. However, for the CV definitions above, the operators SUM, F, and $P(\eta)$ are all elements of $\mathrm{Sp}(2n, \mathbb{R})$; they are generated by homogeneous quadratic Hamiltonians only. Thus, they are in a subgroup of the Clifford group. In order to generate the entire Clifford group, one requires a continuous HW(1) transformation [i.e., a linear Hamiltonian that generates a one-parameter subgroup of HW(1)] such as the Pauli operator $X(q)$. This set $\{\mathrm{SUM}, F, P(\eta), X(q); \eta, q \in \mathbb{R}\}$ generates the Clifford group.

We now have the necessary components to prove the main theorem of this paper regarding efficient classical simulation of a CV process. We employ the stabilizer formalism used for discrete variables and follow the evolution of the Pauli operators rather than the states. To start with, let us consider the ideal case of a system with an initial state in the computational basis of the form $|q_1, q_2, \ldots, q_n\rangle$. This state may be fully characterized by the eigenvalues of the generators of n Pauli operators $\{\hat{q}_1, \hat{q}_2, \ldots, \hat{q}_n\}$. Any continuous variable process or algorithm that is expressed in terms of Clifford group transformations can then be modeled by following the evolution of the generators of these n Pauli operators, rather than by following the evolution of the states in the Hilbert space $\mathcal{L}^2(\mathbb{R}^n)$. The Clifford group maps linear combinations of Pauli operator generators to linear combinations of Pauli operator generators (each $\hat{q}_i$ and $\hat{p}_i$ is mapped to sums of $\hat{q}_j$, $\hat{p}_j$, $j = 1, \ldots, n$ in the Heisenberg picture). For each of the n generators describing the initial state, one must keep track of $2n$ real coefficients describing this linear combination. To simulate such a system, then, requires following the evolution of $2n^2$ real numbers.

In the simplest case, measurements (in the computational basis) are performed at the end of the computation. An efficient classical simulation involves simulating the statistics of linear combinations of Pauli operator generators. In terms of the Heisenberg evolution, the $\hat{q}_j$ are described by their initial eigenvalues, and the $\hat{p}_j$ in the sum by a uniform random number. This prescription reproduces the statistics of all multimode correlations for measurements of these operators.

Measurement in the computational basis plus feed-forward *during* the computation may also be easily simulated for a sufficiently restricted class of feed-forward operations; in particular, operations corresponding to feed-forward displacement (not rotation or squeezing, though this restriction will be dropped below) by an amount proportional to the measurement result. Such feed-forward operations may be simulated by the Hamiltonian that generates the SUM gate with measurement in the computational basis delayed until the end of the computation. In other words, feed-forward from measurement can be treated by employing conditional unitary operations with delayed measurement [2], thus reducing feed-forward to the case already treated.

In practice, infinitely squeezed input states are not available. Instead, the initial states will be of the form

$$\hat{S}_1(r_1) \otimes \hat{S}_2(r_2) \otimes \cdots \otimes \hat{S}_n(r_n)\,|0, 0, \ldots, 0\rangle, \tag{10}$$

where $|0\rangle$ is a vacuum state and $\hat{S}(r)$, $r \in \mathbb{R}$ is the squeezing operation which can be expressed directly in terms of elements of the Clifford group. Now the vacuum states may *also* be described by stabilizers $\{\hat{q}_1 + i\hat{p}_1, \hat{q}_2 + i\hat{p}_2, \ldots, \hat{q}_n + i\hat{p}_n\}$ which are complex linear combinations of the generators. Combining the initial squeezing operators into the computation, a classical simulation requires following the evolution of $4n^2$ numbers (twice that of infinitely squeezed inputs due to the real and imaginary parts). Measurements in the computational basis are again easily simulated in terms of this Heisenberg evolution, by treating each of the q_i and p_i as random numbers independently sampled from a Gaussian distribution with widths described by the vacuum state. Simulation of measurement plus feed-forward follows exactly the same prescription as before.

The condition for ideal measurements can be relaxed. Finite efficiency detection can be modeled by a linear loss mechanism [16]. Such a mechanism may be described by quadratic Hamiltonians and hence simulated by the Clifford group. Note that the Clifford group transformations are precisely those that preserve Gaussian states; i.e., they transform Gaussians to Gaussians; this observation allows us to remove our earlier restriction on feed-forward gates and allow for classical feed-forward of any Clifford group operation. Note that non-Gaussian components to the states cannot be modeled in this manner.

Finally, it should be noted that modeling the evolution requires operations on real-valued (continuous) variables, and thus must be discretized when the simulation is done on a discrete (as opposed to analog) classical computer. The discretization assumes a finite error, which will be

bounded by the smaller of the initial squeezing or the final detector "resolution" due to finite efficiency, and this error must remain bounded throughout the simulation. As only the operations of addition and multiplication are required, the discretization error can be kept bounded with a polynomial cost to efficiency.

Thus, we have proved the extension of the GK theorem for continuous variables:

Theorem 2 (efficient classical simulation): *Any continuous variable quantum information process that initiates with Gaussian states (products of squeezed displaced vacuum states) and performs only (i) linear phase-space displacements (given by the Pauli group), (ii) squeezing transformations on a single oscillator system, (iii)* SUM *gates, (iv) measurements in position- or momentum-eigenstate basis (measurements of Pauli group operators) with finite losses, and (v) Clifford group* $[\mathrm{HW}(n)]\mathrm{Sp}(2n,\mathbb{R})$ *operations conditioned on classical numbers or measurements of Pauli operators (classical feed-forward), can be* efficiently *simulated using a classical computer.*

We could summarize the conditions *(i)–(iii)* by simply stating *(i-iii) transformations generated by Hamiltonians that are inhomogeneous quadratics in the canonical operators* $\{\hat{q}_i, \hat{p}_i; i = 1, \ldots, n\}$, which is equivalent. Thus, any circuit built up of components described by one- or two-mode quadratic Hamiltonians [such as the set of gates SUM, F, $P(\eta)$, and $X(q)$], that initiates with finitely squeezed states and involves only measurements of canonical variables may be efficiently classically simulated.

As with the discrete variable case, these conditions do not mean that entanglement between the n oscillator systems is not allowed; for example, starting with (separable) position eigenstates, the Fourier transform gate combined with the SUM gate can lead to entanglement. Thus, algorithms that produce entanglement between systems may still satisfy the conditions of the theorem and hence may be simulated efficiently on a classical computer; included are those used for CV quantum teleportation [4], quantum cryptography [6–9], and error correction for CV quantum computing [12,13]. Although these processes are of a fundamentally quantum nature and involve entanglement between systems, this theorem demonstrates that they do not provide any speedup over a classical process. Thus, our theorem provides a valuable tool in assessing the classical complexity of simulating these quantum processes.

As shown in [10], in order to generate all unitary transformations given by an arbitrary polynomial Hamiltonian (as is necessary to perform universal CV quantum computation), one must include a gate described by a Hamiltonian other than an inhomogeneous quadratic in the canonical operators, such as a cubic or higher-order polynomial. Transformations generated by these Hamiltonians do not preserve the Pauli group, and thus cannot be described by the stabilizer formalism. Moreover, *any* such Hamiltonian is sufficient [10]. One example would be to include an optical Kerr nonlinearity [17], but there is a lack of sufficiently strong nonlinear materials with low absorption. Alternatively, it has recently been proposed that a measurement-induced nonlinearity (using ideal photodetection) could be used in an optical scheme without the need for nonlinear materials in the computation [15,18]. The physical realization of such nonlinearities is an important quest for quantum information theory over continuous variables. These nonlinear transformations can be used in CV algorithms that do not satisfy the criteria of this theorem, and which may provide a significant speedup over any classical process.

This project has been supported by an Australian Research Council Large Grant. S. L. B. and K. N. are funded in part under project QUICOV as part of the IST-FET-QJPC programme.

[1] D. Gottesman, in *Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics,* edited by S. P. Corney *et al.* (International Press, Cambridge, MA, 1999), p. 32.
[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000), p. 464.
[3] E. Knill, quant-ph/0108033; B. M. Terhal and D. P. DiVincenzo, quant-ph/0108010.
[4] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
[5] A. Furusawa *et al.,* Science **282**, 706 (1998).
[6] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (2000).
[7] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[8] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
[9] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[10] S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).
[11] R. P. Feynman, Found. Phys. **16**, 507 (1986).
[12] S. L. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).
[13] S. L. Braunstein, Nature (London) **394**, 47 (1998).
[14] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer, Berlin, 1994).
[15] D. Gottesman *et al.,* Phys. Rev. A **64**, 012310 (2001).
[16] H. P. Yuen and J. H. Shapiro, IEEE Trans. Inf. Theory **26**, 78 (1980).
[17] G. J. Milburn and D. F. Walls, Phys. Rev. A **28**, 2065 (1983).
[18] S. D. Bartlett and B. C. Sanders, Phys. Rev. A (to be published), quant-ph/0110039.