How to decompose continuous-variable quantum logic gates

Seckin Sefi* and Peter van Loock†
Optical Quantum Information Theory Group, Max Planck Institute for the Science of Light, Günther-Scharowsky-Str.1/Bau 26, 91058 Erlangen, Germany and
Institute of Theoretical Physics I, Universität Erlangen-Nürnberg, Staudstr.7/B2, 91058 Erlangen, Germany

We present a general and relatively efficient method for decomposing an arbitrary exponential operator of bosonic mode operators into a set of universal logic gates. Our work is mainly oriented towards the field of continuous-variable quantum computation, but our results might have implications on any field that incorporates exponential operator decompositions such as quantum control, discrete-variable quantum computation or Hamiltonian simulation. As an important example and a potential application, we present the decompositions of self-Kerr and cross-Kerr interactions.

PACS numbers: 03.67.Lx,42.50.Dv

Introduction– Since quantum computation has been proposed as a generalization of computer science, one of its most important theoretical challenges is how to decompose an arbitrary gate into a universal set. The corresponding theory of discrete-variable decompositions is very extensive and mostly employs matrix representations of logic gates utilizing matrix decomposition techniques [1, 2]. On infinite-dimensional space, logic gates are no longer represented by matrices but by unitary exponential operators. In contrast to discrete-variable theory, there is not an established method to decompose an arbitrary operator in the continuous-variable (CV) regime except the proof-of-principle results on universal gate sets in Refs. [3, 4].

Reference [3] makes use of an exponential operator approximation and proves that by employing certain elementary gate sets (discussed below) one can derive any operator up to a certain error. In Ref. [4], it is proved that Gaussian operations can be efficiently simulated on a classical system. However, none of these works intend to present a constructive and efficient decomposition recipe. Moreover, the approximations used in Ref. [3], which are providing a scaling such that the number of elementary operations to simulate a given operator to any desired accuracy is not exponential, are nevertheless, from an operational and experiment-oriented point of view, still unsatisfactory.

The problem of decomposition is intrinsically related to the concept of universality. Universality means to have a set of operators that allows you to simulate any operator on a certain Hilbert space through concatenations of the elements of the universal set. So the problem of universality is equivalent to decomposing, at least approximately, an arbitrary unitary exponential operator to a set of elementary unitary exponential operators:

$$e^{it\mathcal{H}(a,a^\dagger)} = \{e^{it_1 H_1(a,a^\dagger)}, e^{it_2 H_2(a,a^\dagger)}, ..., e^{it_N H_N(a,a^\dagger)}\}.$$

Here, a and $a^\dagger$ are annihilation and creation operators, respectively, and $\{H_n\}$ are fixed Hermitian functions of mode operators. The coefficients $t_1, t_2, ...$ are interaction times of the Hamiltonians and are functions of t. Thus, different concatenations of elements of this set for varying interaction times should enable one to simulate an arbitrary operator. We assume that we have access to arbitrary interaction times for the initial set [18].

In our setting, there are now two important criteria for CV gate decompositions, namely how systematic and how efficient the decompositions are. Here we shall derive methods according to these criteria and present a systematical and relatively efficient framework for decomposing any given operator. Our general method is first expressing operators in terms of linear combinations of commutation operators and then realizing each commutation operator and their combinations through approximations. The idea behind this approach together with an important example, namely that of decomposing the unitary Kerr interactions, will be presented in the first part of the paper. In the second and third part, we then give a general and systematical recipe to decompose any unitary CV operator acting on bosonic modes to a universal set. In the fourth part of the article, we discuss the efficiency of the decompositions and present a guideline to obtain an arbitrary order of error. For this purpose, we employ a novel technique for obtaining efficient approximations [5]. Throughout, we use the convention $\hbar = 1/2$, i.e., the fundamental commutation relation is $[X, P] = i/2$ with $X \equiv (a^\dagger + a)/2$ and $P \equiv i(a^\dagger - a)/2$.

General Gaussian decompositions– For Gausian operators, i.e., second order operators, exact and finite decompositions to elementary sets are known. Here, order is defined as the polynomial order of the mode operators in the Hamiltonian of a given operator. For example, the Bloch-Messiah decomposition allows to decompose any second order operator, i.e., any unitary Gaussian operation, to passive linear multi-mode optics, single-mode squeezing, and displacement operations [6].

In Ref. [4] the following set is presented as a single-mode Gaussian universal set: $\{e^{i\frac{\pi}{2}(X^2+P^2)}, e^{it_1 X}, e^{it_2 X^2}\}$, and in Ref. [7], similar to the Bloch-Messiah decomposition, a recipe is given to decompose any single-mode transformation of second order to this set with no more than four steps. These exact decompositions emerge from

the fact that mode transformations through second order unitary operations are linear, and thus, one can utilize matrix representations and matrix decomposition techniques. In fact, for Gaussian operator decompositions, one can find infinitely many elementary sets and decompositions, and instead of those sets above, one may choose the one that suits best the given situation and purpose.

Universal decompositions– In order to decompose an arbitrary single-mode operator in CV systems, it has been shown that, in principle, adding a nonlinear element (of order three or more) to the toolbox is sufficient [3]. In the present work we use the following set:

$$\{e^{i\frac{\pi}{2}(X^2+P^2)}, e^{it_1X}, e^{it_2X^2}, e^{it_3X^3}\}. \tag{1}$$

This set is not unique, and one may use different Gaussian elements as explained above and a different nonlinear element. However, this particular set turns out to be useful for describing CV quantum computation in the one-way model using CV cluster states [8, 9]. Note that one can simplify this elementary set further by omitting the second order Hamiltonian, since $e^{it^2X^2} = e^{it^4\frac{2}{27}}e^{it\frac{2}{3}P}e^{itX^3}e^{-it\frac{2}{3}P}e^{-itX^3}e^{i\frac{t^3}{3}X}$, together with the Fourier transformation whose action is given in Eq. (2) below. Even though this simplification has value from an academical point of view, as it reduces the minimal number of elementary gates, we are basically motivated by decomposing an arbitrary gate to a set of experimentally accessible gates. All second order gates are relatively easy to implement, and replacing them by third order Hamiltonians will increase the complexity of the gate sequence. Therefore we shall use the overcomplete set (1) in our decompositions without loss of generality. One may also prefer a further extended set depending on a certain experimental situation in order to reduce the complexity of the decompositions.

In addition, one can obtain *some* nonlinear operations through unitary conjugation: $Ue^{itH(a,a^\dagger)}U^\dagger \rightarrow e^{itH(UaU^\dagger,(UaU^\dagger)^\dagger)}$. An important unitary conjugation is the Fourier transform:

$$e^{i\frac{\pi}{2}(X^2+P^2)}e^{itX^m}e^{-i\frac{\pi}{2}(X^2+P^2)} = e^{itP^m}. \tag{2}$$

Employing unitary conjugation, with the set (1), one can now generate certain nonlinear gates exactly. For example, $e^{itX^3}e^{itP^2}e^{-itX^3} = e^{it(P-t\frac{3}{2}X^2)^2}$, which is a fourth order operator, or, $e^{itP^2}e^{itX^3}e^{-itP^2} = e^{it(X+tP)^3}$, using similar ideas to obtain higher order operations. However, there is only a limited number of such decomposable nonlinear operators, and therefore we will make use of the idea of operator approximations.

Besides the abstract notion of universality [3], how can a given unitary exponential operator be decomposed to the elementary set (1)? What is a systematical and efficient way? Efficiency, of course, is a relative concept, and so we will discuss what the available tools are and present a well-defined problem for which we aim at a decomposition as efficient as possible. The tools we use for CV gate decompositions includes Gaussian operator decompositions, unitary conjugation, and exponential operator approximations which we define and discuss later.

Before proceeding to the general case, let us demonstrate how to realise a particular nonlinear exponential operator using the above tools and the set (1). A very important operator in quantum information processing is the Kerr interaction operator. It allows to convert a coherent state into a cat state [10] and to realize a controlled quantum gate for qubits [11]. The Kerr interaction, up to a quadratic Gaussian element, is defined as follows,

$$e^{it(X^2+P^2)^2} = e^{it(X^4+X^2P^2+P^2X^2+P^4)}.$$

In order to decompose the Kerr operation to the set (1), we first write Kerr Hamiltonian as the linear combination of commutators and then realize them through operator approximations. The following relations, together with the Fourier transform (2), are enough to realize this gate up to a phase:

$$X^4 = -\frac{2}{9}[X^3,[X^3,P^2]], \tag{3a}$$

$$X^2P^2 + P^2X^2 = -\frac{4i}{9}[X^3,P^3]. \tag{3b}$$

In other words, in order to decompose the Kerr interaction to the set (1), it is sufficient to realize the above commutators and their linear combinations.

Let us now generalize our approach to an arbitrary Hamiltonian. Obviously, any single-mode Hamiltonian as a polynomial of bosonic mode operators consists of operators of the form $cX^mP^n + c^*P^nX^m$. Now we show that any such operator can be written as a linear combination of commutation operators. First note that $cX^mP^n + c^*P^nX^m = \mathrm{Re}(c)(X^mP^n + P^nX^m) + i\mathrm{Im}(c)[X^m,P^n]$, and then one can derive the following two identities,

$$X^m = -\frac{2}{9}[X^{m-1},[X^3,P^2]], \tag{4}$$

$$X^mP^n + P^nX^m = -\frac{4i}{(n+1)(m+1)}[X^{m+1},P^{n+1}] - \frac{4}{n+1}\sum_{k=1}^{n-1}[P^{n-k},[X^m,P^k]]. \tag{5}$$

Equation (4) is necessary to obtain arbitrary powers of X and P operators with the Fourier conjugation (2), and Eq. (5) basically prescribes how to systematically decompose an elementary Hamiltonian to commutation operations of orders of X and P and their combinations where we can use the tools we have. Also, due to the Jacobi identity, we have $[P^{n-k},[X^m,P^k]] = [P^k,[X^m,P^{n-k}]]$, and this may also lead to some simplification depending on the value of n.

For multi-mode operators one needs an extended elementary set including an entangling operation [3], for example, the beam splitter operation, $e^{it(X_1\otimes P_2 - P_1\otimes X_2)}$, where the subscripts denote different modes. Using Gaussian decomposition methods, for simplicity, we may assume that we have access to the following gate without loss of generality, $e^{itX_1\otimes X_2}$. For multi-mode Hamiltonians we can again use the simplifications for a single mode and Eq. (5), because of the fact that the operators on one mode commute with the operators on the other mode. However, for this purpose, we initially need to realize the two-mode operations with arbitrary powers of X and P in both modes, similar to the single-mode relation (4). The following relation together with Fourier conjugation (2) and Eq. (4), is sufficient to realize the two-mode operations with arbitrary powers of X and P,

$$P_1^n \otimes P_2^s = -\frac{1}{(n+1)(s+1)}[P_2^{s+1}, [P_1^{n+1}, X_1 \otimes X_2]]. \quad (6)$$

Then, we can use the Eq. (5) again with the single-mode operations to realize an arbitrary two-mode expression. As an example, consider the cross-Kerr Hamiltonian up to a Gaussian transformation: $(X^2+P^2)_1 \otimes (X^2+P^2)_2 = X_1^2 \otimes X_2^2 + X_1^2 \otimes P_2^2 + P_1^2 \otimes X_2^2 + P_1^2 \otimes P_2^2$. Thus, the relation, $[P_2^3, [P_1^3, X_1 \otimes X_2]]$ is sufficient.

From an academical perspective, equations (4), (5) and (6) are universal not only for any Hamiltonian, but also for any initial universal set with a nonlinear gate different from X^3 because of the well known equations: $\frac{\partial F}{\partial P} = -2i[X, F]$, $\frac{\partial F}{\partial X} = 2i[P, F]$, where F is a function of operators X and P. Thus, any initial nonlinear Hamiltonian can be reduced to a form X^m. But, from a practical perspective, it would be unwise to use equations (4) and (5) for any given Hamiltonian and any given initial set because of the increased complexity. Instead, one should derive an optimized expression (in terms of the number of operators needed for the decomposition) utilizing the available tools for every other Hamiltonian and every other universal set.

Efficiency– Besides having a systematical framework, we also require the decomposition to be relatively efficient. We define efficiency as the number of operators needed to realize a given operator with a certain ignorable error (note that this definition slightly differs from previous ones [3] where efficiency is the scaling of the number of operators with respect to the error). Now recall that, in general, our decompositions are based on writing a general Hamiltonian as linear combination of commutators using Eqs. (5), (4) and employing operator approximations. We discussed how to rewrite Hamiltonians in the preceding sections, and next, we will now focus on the efficiency of operator approximations.

Let us start with a few definitions. In the following equation,

$$e^{tC} = e^{t_1 A} e^{t_2 B} e^{t_3 A} ... e^{t_M B}, \quad (7)$$

if the Taylor expansion of both sides matches for the orders of t up to t^m, then it is called mth order decomposition which we denote as $Q_m(t)$ [19]. For example, an important case is when $C = A + B$, for which we will use the term *splitting*. Another important case is when C is the commutation of A and B. Throughout the article, we call an exponential operator with exponent $[A, B]$ the *commutation operator*. For example, the identity below is a well-known second order approximation for a commutation operator. It has been exploited already as an important tool in quantum control [12], in discrete-variable quantum computation [13], CV quantum computation [3], or, in general, Hamiltonian simulation theory [14],

$$e^{t^2[A,B]} = e^{itB} e^{itA} e^{-itB} e^{-itA} + f(t^3, A, B) + \dots \quad (8)$$

It basically says that, for $t < 1$, the concatenation order is the same as applying the commutation operator of A and B, up to some error where the dominant term is of the order t^3. Now in order to obtain more reliable gates, a straightforward way to improve accuracy is using smaller interaction times, $t \to t/n$, and applying the decomposition n^2 times to obtain the same interaction time as before,

$$e^{t^2[A,B]} = \left(e^{iB\frac{t}{n}} e^{iA\frac{t}{n}} e^{-iB\frac{t}{n}} e^{-iA\frac{t}{n}}\right)^{n^2} + f\left(\frac{t^3}{n}, A, B\right).$$

For the rest of the article, we call this approach rescaling. Besides improving accuracy, rescaling is necessary to realize further nested commutations. One can replace operator tA by $t^2[B, A]$ in Eq. (8) to simulate the nested commutation operator $e^{it^3[B,[B,A]]} = e^{itB} e^{t^2[B,A]} e^{-itB} e^{-t^2[B,A]} + f'(t^4, A, B)$ and make use of the same idea for further nested commutations. However, in this identity, we are also supposed to approximate $[B, A]$ using approximation (8), and so we get an operator, whose interaction time is of the same order as the dominant error term, which makes the approximation meaningless and invalid. To obtain a reasonable decomposition, the order of dominant error should be smaller than t^3. Thus, we again need rescaling. However, rescaling requires relatively many operators to enhance accuracy.

In a certain decomposition, using the above-mentioned approximations, the number of operators to approximate a single commutation operator with coefficient 0.1 and order of dominant error term 10^{-3}, requires 4000 operators and for the nested commutation operator, for the same values, the number of operators will be 2×10^7; thus, for approximating a Kerr interaction with coefficient 0.1, one needs about 10^8 operations which is an unsatisfactorily high number. Hence, deriving better approximations is a crucial part of our decomposition framework. What we use is a novel method for obtaining higher-order approximations [5], based on generalized Baker Campbell

Hausdorff series (gBCH) [15]. With this idea, the concatenation converges much faster to an arbitrary set of commutations and linear combinations of these, reducing the number of operators from the order of 10^8 to the order of 10^2. How this works will be briefly explained below.

As a first step, consider an arbitrary concatenation of the two exponential operators $\prod_i e^{it_i A} e^{it_i' B}$ like on the right hand side of (7). The resulting operator of this sequence, like operator C on the left hand side of (7), can be calculated through gBCH. It will correspond to a linear combination of many operators. Each of the coefficients of the operators in C corresponds itself to a polynomial. Then, we solve these polynomials in order to eliminate undesired operators and keep the desired ones. Since solving polynomials is in general a hard task, the above procedure will be limited. After obtaining a certain order of approximations, as a second step, we use a concatenation of these first-step approximations to derive approximations of much higher order. This step is similar to the Suzuki method [16]. The difference is, however, instead of improving step by step and obtaining each order recursively, we obtain a by many orders higher approximation in one step, again, utilizing gBCH.

As an example, using our method, the required number of operators for a Kerr interaction with coefficient 0.1 and the dominant error term 10^{-3} is now around 250. However, using the fourth-order elementary gate X^4 in our elementary set instead of the cubic one will reduce this number to around 70. For deriving these numbers, we used Eq. (3) and the following approximations. For decomposing the three-party splitting of the operator $e^{i(A+B+C)}$, we used the following concatenation series: $\prod_i e^{it_i A} e^{it_i' B} e^{it_i'' C}$. A third-order decomposition is then comprised of 10 operators with the following parameters: 0.4515, 0, 0.4515, 0, 1.0824, 0.6308, 0.6308, 1.1367, 1.1367, −0.0824, 0, −1.2191, 0, −1.2191 where the order of parameters match with the concatenation order. A fifth-order decomposition for the commutation operator $e^{t^2[A,B]}$ is comprised of 16 operators with the following parameters: −2.12133, −1.68068, −0.019988, 1.60205, 2.02532, 2.74368, 0.0612175, −1.17081, −3.23589, 0.0187355, 1.51902, −0.989126, 0.571647, 0.476157 where the order of the parameters match that of concatenation (7). Similarly, a fifth-order decomposition for the nested commutation operator $e^{it^3[A,[A,B]]}$ consists of 15 operators with the following parameters: 0, 0.5, −0.912433, −1.000141, 2.439891, −0.531940, 0.184788, 2.000998, −0.477395, −1.659152, −0.761744, 1.465192, 1.181123, −1.312200, −1.654230, 0.537205.

In summary, we presented a systematical method to decompose arbitrary CV unitary gates into an elementary set of gates using approximations with much higher efficiency than in any of the existing proof-of-principle methods. In fact, different from the previous proof-of-principle demonstrations, our treatment brings the abstract notions of decomposition theory for CV quantum computation close to experimental realizations.

* Electronic address: seckin.sefi@mpl.mpg.de
† Electronic address: peter.vanloock@mpl.mpg.de

[1] M. Mottonen and J. Vartiainen, arXiv:quant-ph/0504100 (2005).
[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).
[3] S. Lloyd and S. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).
[4] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, Phys. Rev. Lett. **88**, 097904 (2002).
[5] S. Sefi and P. van Loock (in preparation).
[6] S. Braunstein, Phys. Rev. A **71**, 55801 (2005).
[7] R. Ukai, J. Yoshikawa, N. Iwata, P. van Loock, and A. Furusawa, Phys. Rev. A **81**, 32315 (2010).
[8] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[9] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, Phys. Rev. Lett. **97**, 110501 (2006).
[10] B. Yurke and D. Stoler, Phys. Rev. Lett. **57**, 13 (1986).
[11] I. L. Chuang and Y. Yamamoto, Phys. Rev. A **52**, 3489 (1995).
[12] J. Clark, D. Lucarelli, and T. Tarn, Int. J. Mod. Phys. B **17**, 5397 (2003).
[13] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).
[14] K. Brown, W. Munro, and V. Kendon, arXiv:1004.5528 (2010).
[15] M. Reinsch, J. Math. Phys. **41**, 2434 (2000).
[16] M. Suzuki, Phys. Lett. A **146**, 319 (1990).
[17] A. Papageorgiou and C. Zhang, arXiv:1005.1318 (2010).
[18] Note that compared to the discrete-variable approaches to universal quantum computing [2], this assumption is very generous. In fact, if we allow for arbitrary rotation angles when transforming a single qubit, together with a fixed two-qubit gate, any multi-qubit unitary can be *exactly* achieved. The need for using an elementary qubit gate set with discrete rotation angles and considering *approximate* decompositions stems from the requirements of fault-tolerant quantum processing. In the CV case here, the universal gate sets are derived independent of the notion of fault tolerance, but dependent on the requirement to simulate Hamiltonians of arbitrary order [3].
[19] Note that having a good approximation does not only depend on the *order* of the decomposition, but also on the actual *values* of the interaction times for the individual gates and the *norms* of the corresponding operators [14, 17]. In the present work, we only discuss how to obtain a certain order of decomposition and not how to obtain a certain absolute error. The latter shall be investigated in a future work.