Quantum methods for machine learning and classical dynamics

Barthe, A.M.

CHAPTER 7

The complexity of simulating exponentially large Gaussian bosonic circuits

7.1. Introduction

The study of the power of quantum computers has been a central and fundamental topic in complexity theory. While it is known that these devices can solve problems at least as fast as classical probabilistic computers, we also know that they are unable to do so more than exponentially faster [31, 185]. This has raised the question: *What are the tasks that saturate this separation? I.e., what are the problems for which a quantum computer can achieve an exponential advantage over its classical counterparts?*

To answer such questions one starts with the class Bounded-Error Quantum Polynomial (BQP), the set of decision problems that a quantum computer can solve in polynomial time with a small constant probability of failure. Then, one determines the subset of problems that are the hardest therein, known as BQP-complete. Several BQP-complete problems are known, such as those based on the Harrow-Hassidim-Lloyd algorithm [171],

The contents of this chapter have been published in [39].

scattering in scalar quantum field theory [186], and more recently on the quantum simulation of exponentially many coupled classical oscillators [42]. The latter presents the intriguing perspective that simulating exponentially large linear and energy-preserving simple classical systems leads to BQP-completeness, and, under reasonable complexity theory assumptions, to an exponential quantum advantage over classical methods.

In this chapter we prove an analogous result to that in Ref. [42], namely, that the quantum simulation of particle-preserving GB circuits (i.e. passive linear optics) [187–189] acting on Gaussian initial states on exponentially many modes also leads to BQP-completeness (see Figure 7.1). At its core, our framework starts with the realization that a direct simulation of a bosonic system is intractable on a qubit-based quantum computer, as the associated Hilbert spaces are fundamentally different (with one being infinite-dimensional, and the other discrete). This issue can be avoided by restricting the simulation to the first and second moments of the quadrature operators. That is, we encode in a quantum state the position and momentum expectation values (and their covariance matrix) over the initial bosonic state. As such, instead of simulating the action of the GB circuit on the bosonic Hilbert space, we implement its effective action on the expectation values on a gate-based quantum computer.

In this context, we present a constructive dictionary that translates back-and-forth between the symplectic propagator associated with a universal set of GB gates (beamsplitters, phase and squeezing gates) and qubit circuits. The efficiency of our simulation framework relies on several key conditions, such as the input qubit-state being preparable in polynomial time, and the quantum circuit requiring only polynomially-many gates. Indeed, we present cases of interest for which these two conditions are satisfied, and therefore for which we can achieve an exponential quantum advantage.

Finally, we show that adding a layer of squeezing gates to interferometers boosts the complexity of the problem to PostBQP-complete, which is a very powerful complexity class [34] that, among others, contains QMA (Quantum Merlin-Arthur). In PostBQP, in addition to polynomially-sized quantum circuits one obtains the ability to post-select on measurement outcomes, that is, to exponentially amplify small probabilities.

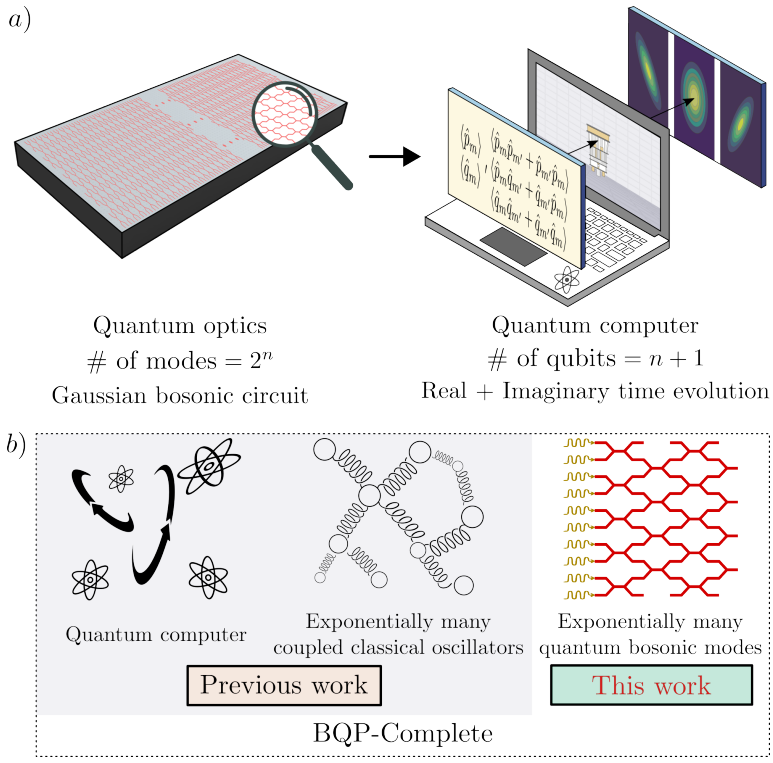

Figure 7.1.: **Schematic representation of our main results.** a) We present a framework for simulating the action of a GB circuit on the first and second moments of quadrature operators of a bosonic state on 2^n modes on an $(n+1)$-qubit gate-based quantum computer. b) We show that particle-preserving GB evolutions on Gaussian bosonic states are sufficient to define a problem that is BQP-complete, thus indicating that passive linear optics on exponentially many bosonic modes are as powerful as universal quantum computers.

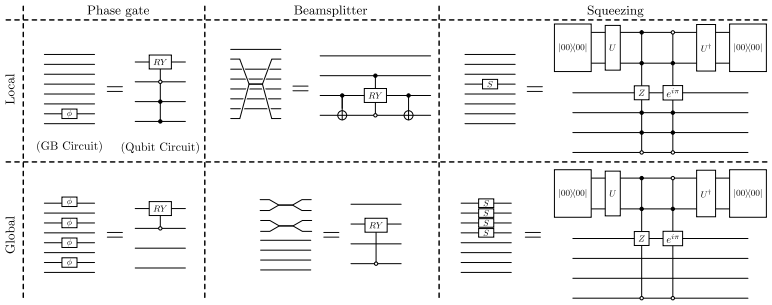

Figure 7.2.: **Examples of GB gates in the qubit picture.** We consider a bosonic system on $M = 8$ modes, leading to a circuit on 4 qubits. The local phase gate acts on the mode $m = 6 = 2^0 \times 0 + 2^1 \times 1 + 2^2 \times 1$. The local beamsplitter acts on the modes $m = 1$ and $m' = 7$, whose binary representations only share the least significant bit. The local squeezing gate acts on mode $m = 3 = 2^0 \times 1 + 2^1 \times 1 + 2^2 \times 0$, and is represented by an imaginary time evolution as a linear combination of unitaries with post-selection on two ancillary qubits (which have been added on top). The global phase gate acts on all modes whose index is even. The global beamsplitter is applied to the first half of the modes, pairing each mode with even index m to its nearest neighbor mode with index $m' = m + 1$. The global squeezing gate is applied to the first half of the modes.

7.2. Gate-Based simulation of Gaussian circuits

7.2.1. Initialization

To start the simulation on the quantum computer, we encode the normalized vector $\langle\hat{\vec{z}}\rangle$ (normalized matrix $\vec{\sigma}$) into a pure (mixed) $(n+1)$-qubit quantum state $\left|\hat{\vec{z}}\right\rangle \propto \langle\hat{\vec{z}}\rangle$ ($\varrho_{\vec{\sigma}} \propto \vec{\sigma}$). For instance, we have

$$\left|\hat{\vec{z}}\right\rangle = \frac{1}{\|\langle\hat{\vec{z}}\rangle\|_2} \sum_{m=1}^{2^n} \langle\hat{q}_m\rangle |0\rangle \otimes |m\rangle + \langle\hat{p}_m\rangle |1\rangle \otimes |m\rangle \ . \tag{7.1}$$

For our scheme to be efficient, such states need to be preparable in polynomial time. Such cases occur, e.g., when there are $\mathcal{O}(\text{poly}(n))$ non-zero known position and momentum expectation values. Equation (7.1) illustrates the privileged role of the first qubit [190], separating the Hilbert space into two subspaces, one associated with the positions and the other with the momenta. We will henceforth refer to the first qubit as the *symplectic qubit*. The remaining n qubits serve as a register for each of the 2^n modes, and we will refer to them as *register qubits*. In particular, in Equation (7.1) each mode label m is encoded via its binary decomposition as $m = 2^0 m_1 + 2^1 m_2 + \ldots + 2^{n-1} m_n$, with $m_l \in \{0, 1\}$, and with the least significant qubit being the top-most register qubit.

Here we note that when ρ_0 is Gaussian, then it is fully characterized by the first and second moments of the quadrature operators, meaning that $\left|\hat{\vec{z}}\right\rangle$ and $\varrho_{\vec{\sigma}}$ provide a full description of these states. Moreover, if the initial state is also coherent (eigenstates of $\hat{a}$), then $\varrho_{\vec{\sigma}}$ is the maximally mixed state on $(n+1)$ qubits. For other non-Gaussian states our framework is restricted to the information contained in $\hat{\vec{z}}$ and $\vec{\sigma}$.

7.2.2. Evolution

Once the initial state is prepared, we can evolve it with a quantum circuit that effectively implements the symplectic propagators associated with the gates in the GB circuit (see for instance Equation (2.39)). In particular, we present a dictionary to efficiently translate between standard GB and qubit gates. We also refer the reader to Figure 7.2 for an explicit circuit depiction of some GB gates in qubit circuit form.

The *phase gate* is a particle-preserving gate acting on a single mode

m. In terms of bosonic operators, its generator is $\hat{H} = \hat{p}_m^2 + \hat{q}_m^2$, yielding $\Omega K = 2iY \otimes |m\rangle\langle m|$ in the qubit picture. This corresponds to an R_y gate (rotation about the y-axis) on the symplectic qubit, conditioned on the $|m\rangle\langle m|$ state on the register.

The *beamsplitter* is a particle-preserving gate acting on two modes m and m'. It is generated by $\hat{H} = \hat{q}_m\hat{p}_{m'} - \hat{q}_{m'}\hat{p}_m$ (with $m \neq m'$), which results in $\Omega K = 2iI \otimes (i\,|m\rangle\langle m'| - i\,|m'\rangle\langle m|)$. This corresponds to an R_y rotation in the subspace spanned by $|m\rangle$ and $|m'\rangle$. This gate can be implemented by using controlled-not gates to transform $|m\rangle$ and $|m'\rangle$ into two computational-basis states that only differ in one qubit, then performing a controlled-R_y rotation on that qubit (conditioned on the other $n-1$ qubits in the register), and applying the same controlled-not gates to return to the original basis. We highlight the fact that this gate acts trivially on the symplectic qubit, as beamsplitters conserve total momentum and total position.

The *squeezing gate* is a non-particle-preserving gate that acts on a single mode m. Its generator is $\hat{H} = \pm\,(\hat{q}_m\hat{p}_m + \hat{p}_m\hat{q}_m)$, leading to $\Omega K = \pm 2X \otimes |m\rangle\langle m|$. This produces an imaginary-time evolution [94, 191–193], which can be implemented, e.g., with two ancillary qubits and post-selection. As illustrated in Figure 7.2 and further discussed in the SI, we propose to implement it as a linear combination of unitaries [194], with the latter being multi- controlled-Z and controlled-phase gates. Notably, the fact that states cannot be arbitrarily squeezed translates in our framework as the success probability of the imaginary-time evolution for infinite time being zero.

Finally, the *displacement gate*, a common non-particle-preserving Gaussian gate, cannot be included as a linear qubit gate in the proposed framework (see the SI for an additional discussion on this gate).

We stress that while our framework requires the implementation of multi-controlled qubit operations to simulate the action of some GB gates, these can be compiled exactly using only $\mathcal{O}(n)$ local gates [43]. Moreover, if instead of one or two modes, we consider GB gates that act on several (potentially exponentially many) modes, there can be simplifications that render them much easier to implement at the qubit level. As an important example, we show in Figure 7.2 (see also SI) how some global phase gates and beamsplitters acting on 2^{n-1} modes simplify to two-qubit controlled-R_y rotations, as well as how the number of control qubits is reduced for some global squeezing gates. This means that when the GB circuit is composed of polynomially many such local particle-preserving gates, the implementation of the quantum circuit is efficient. When non-particle-preserving squeezing gates are added, then the efficiency will ultimately

depend on how many such gates are added, as well as on their squeezing strength parameters.

At this point, we recall that the covariance matrix of coherent states leads to a maximally mixed state $\varrho_{\vec{\sigma}}$, and therefore it remains invariant when evolved with a purely unitary circuit (e.g., particle-preserving GB gates in an interferometer). This result is well aligned with the bosonic picture where coherent states going through interferometers remain coherent states. Then, as squeezing gates are not particle-preserving, their action on a coherent state corresponds to purifying the associated $\varrho_{\vec{\sigma}}$.

7.2.3. Measurements

At the output of the quantum circuit, we obtain states that represent the evolved expectation values and covariance matrix of quadrature operators (which we respectively denote as $\left|\hat{\vec{z}}'\right\rangle$ and $\varrho_{\vec{\sigma}'}$). We now discuss how measuring these states allows us to extract useful information about the GB circuit.

There are a variety of measurements of interest for Gaussian states. As detailed in the SI, photon counting can be implemented for coherent states by sampling bitstrings from $\left|\hat{\vec{z}}'\right\rangle$. To understand why this is the case, we recall that the energy for each mode is proportional to the probability of sampling the corresponding bitstring. Secondly, for any bosonic state homodyne measurements correspond to retrieving the position (momentum) of a specific mode. At the qubit level, these measurements can be implemented from a swap-Hadamard test between $\left|\hat{\vec{z}}'\right\rangle$ and some computational-basis state of interest. Then, our framework also allows us to estimate the fraction of total momentum and total position, as this value can be retrieved by measuring the symplectic qubit in $\left|\hat{\vec{z}}'\right\rangle$. Similarly, the fractional energy of the first and second half of the modes can be estimated by measuring the bottom-most (most significant) register qubit. Moreover, we note that combining computational basis measurements (or Hadamard tests) on $\left|\hat{\vec{z}}'\right\rangle$ and $\varrho_{\vec{\sigma}'}$ allows us to estimate the energy in a given mode. To finish, we note that while the total energy remains constant for particle-preserving GB circuits, this quantity can change when non-particle-preserving gates are included. In this case, while we cannot directly measure the total energy of the system (as the states need to be normalized), one can keep track of the total energy by using as a proxy the success probability of the imaginary-time evolutions.

7.3. BQP-completeness of Exponentially large interferometers

7.3.1. Problem definition

We now show that we can leverage our framework to devise a decision problem based on a restricted class of large optical quantum interferometers and prove that it is BQP-complete. We begin by introducing a family of quantum interferometers, that we refer to as *bit-structured*.

Definition 7.1 (Bit-structured interferometer)
A bit-structured interferometer acting on 2^n nodes consists of L global beamsplitters, such that each global beamsplitter acts on 2^{n-1} modes. A global beamsplitter is specified by two natural numbers, $k \neq l$, between 1 and n. The global beamsplitter then acts on all the modes with indices $\{m\}$ such that their k-th bit is equal to 0, by applying local beamsplitters between modes with indices m, m' that only differ in their l-th bit.

Our decision problem is then phrased as follows.

Problem 7.1
Consider a bit-structured interferometer (see Definition 7.1) acting on 2^n modes with $L \in \mathcal{O}(\text{poly}(n))$, and an input state such that the first mode is displaced in position by a real constant x while the state of the remaining modes is the vacuum. Then, decide whether the expectation value of the position on the first mode at the output of the interferometer is

$$1.\ \langle \hat{q}_1 \rangle > \frac{2}{3}x\,, \qquad \text{or} \qquad 2.\ \langle \hat{q}_1 \rangle < \frac{1}{3}x\,,$$

given the promise that either one or the other is true.

Problem 7.1 is illustrated in Figure 7.3, where we simulate an interferometer with ~ 8 billion modes (i.e., a 33-qubit circuit). There, we keep track of $\langle \hat{q}_1 \rangle / x$ (which corresponds to the overlap with the $|0\rangle^{\otimes n}$ state) as the state evolves through the beamsplitters.

7.3.2. Complexity of the problem

Our main result is the next theorem.

Theorem 7.1
Problem 7.1 is BQP-complete.

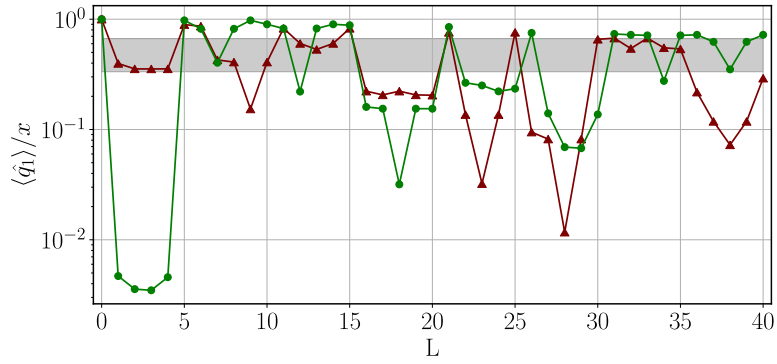

Figure 7.3.: **Simulation of a bit-structured interferometer on ~ 8 billion modes**. We illustrate Problem 7.1 by tracking two non-trivial evolutions of $\langle \hat{q}_1 \rangle / x$ along a large bit-structured interferometer, the green (red) plot corresponding to a YES (NO) instance. The gray region corresponds to $\frac{1}{3} < \langle \hat{q}_1 \rangle / x < \frac{2}{3}$. The simulations were performed with the open-source library `Qibo` [195, 196].

The proof of Theorem 7.1 can be found in the SI, but we give here a summary of the key points. First, we show that Problem 7.1 is contained in BQP. To do this, we simply use the mapping between beamsplitters and qubit gates explained previously to prove that a bit-structured interferometer with $\mathcal{O}(\text{poly}(n))$ layers always results in a polynomial-size quantum circuit, which is a necessary condition to be contained in BQP.

Finally, we need to prove that Problem 7.1 is BQP-hard. That is, if we can solve it, we can also solve any other problem in BQP with an additional overhead that is polynomial in n. This is done by first showing that each global beamsplitter gives rise to a controlled-R_y gate (acting when the control qubit is in the $|0\rangle$ state). Then, we use the result from [197] which states that controlled-R_y rotations constitute a universal gate set, in the sense that any quantum computation can be performed with these gates [198, 199].

7.4. Non-energy-preserving systems

7.4.1. Quantum algorithms for dissipative exponentially large differential equations

The main result of the previous section is to propose a new BQP-complete decision problem based on exponentially large interferometers. Other energy-preserving exponentially large systems [42, 200] yield BQP-complete decision problems. A natural question is whether non-energy-conserving systems can also be efficiently simulated. The answer is partly found in the literature of quantum algorithms to solve differential equations. Most results [174, 201–203] are based on the Harrow-Hassidim-Lloyd (HHL) [171] subroutine. Caveats for the HHL algorithm to provide an actual advantage have been well studied [173], in particular, the algorithm's scaling with the condition number of the matrix to invert.

In [174], a lower bound for the complexity of any quantum algorithm returning the solution to a differential equation $\partial_t x = Ax$ as an amplitude encoded state $|x\rangle = \frac{1}{|x\|_2} \sum_k x_k |k\rangle$ was provided. For some dissipative systems this complexity bound scales exponentially with the integration time. More precisely, noting that any stable system must have eigenvalues with non-positive real parts (otherwise it would diverge exponentially), the difference between the maximum and the minimum real part of eigenvalues $\{i\omega_k - \eta_k\}$ of A is defined as $\delta := |\max_k \eta_k - \min_k \eta_k|$. In [174], the worst case complexity to evolve the system for a time t is shown to be $\Omega(e^{\delta t})$, with a proof based on the distinguishability of non-orthogonal quantum states. This lower bound can also be understood in terms of the condition number of e^{At} [203] which is ultimately the linear transformation that is applied to the initial state. Indeed, considering that all eigenstates of A are orthogonal for simplicity, we can write $A = \sum (i\omega_k - \eta_k) |k\rangle\langle k|$, and find its condition number to be

$$\begin{aligned} \kappa(e^{At}) &= \frac{|\lambda_{\max}|}{|\lambda_{\min}|} = \frac{\max_k(|e^{(i\omega_k - \eta_k)t}|)}{\min_k(|e^{(i\omega_k - \eta_k)t}|)} \\ &= e^{t(\min_k(\eta_k) - \max_k(\eta_k))} = e^{\delta t} \end{aligned} \tag{7.2}$$

This means that the dissipation of energy yields a surge in the complexity of any quantum algorithm to be exponential in the time of integration. Note that for constant time, the complexity of the algorithm may remain polynomial, which is in line with existing literature about dissipative systems [172]. In contrast, time scaling at least linearly with the number of qubits, that is logarithmically with the ODE dimension, may increase

the complexity to be exponential. Such a complexity increase in the presence of dissipative terms is also found for classical algorithms solving ordinary differential equations. Although there is no strict mathematical definition, some ODEs are called stiff, when in practice their numerical resolution suffers from instability. In particular, in that context for linear ODEs, the stiffness ratio is defined as $\min_k(\eta_k)/\max_k(\eta_k)$. In summary, previous work has shown that energy dissipation in ODEs leads to an increase in the complexity of solving them with a quantum computer for integration times scaling logarithmically with the ODE dimension. In this section, we quantify such an increase by proving hardness results. We define the following problem.

Problem 7.2
Given a system of ODEs, whose dynamics are characterized by a matrix $A \in \mathbb{R}(2^n, 2^n)$, such that its spectral norm $\|A\| \leq R \in O(poly(n))$, a time t, an input state x_0 output the state $x(t) = \frac{e^{At}x_0}{\|e^{At}x_0\|_2}$.

The first step in analyzing the complexity of this problem is to realize that the imaginary-time evolution of a real Hamiltonian can be reduced to it. Indeed given a real Hamiltonian H, define $A = -H$ and $t = \beta$ and one has $e^{-\beta H} = e^{At}$. Notice that the converse is not true as A may not be symmetric, i.e. not a Hamiltonian.

7.4.2. The power of imaginary-time evolution

Imaginary-time evolution is a powerful tool. Aside heuristic approaches based on variational principles [81], two types of algorithms to perform imaginary-time evolution with theoretical guarantees exist. The approach in [194] is probabilistic, it is a sequence of steps each one involving post-selection. Another approach is Quantum Imaginary Time evolution (QITE) [191], which consists of approximating small steps of imaginary-time evolution with a time-dependent unitary, whose parameters are derived by performing tomography on the state. The complexity of both quantum algorithms is super-polynomial in general. We define the exact imaginary-time evolution problem as follows.

Problem 7.3
Given a Hamiltonian H with spectral norm $\|H\| \in poly(n)$, a time β, an input state $|\psi_0\rangle$ prepare the state $|\psi_t\rangle = \frac{e^{-\beta H}|\psi_0\rangle}{\|e^{-\beta H}|\psi_0\rangle\|_2}$.

In [34] PostBQP is proven to be equal to PP. Informally, PostBQP is the set of decision problems that one can solve with BQP equipped with post-selection, problems that can be solved with a probabilistic algorithm that

gives the correct answer with a probability of failure arbitrarily close to 1/2. In fact it follows from Proposition 5 in [34] that imaginary-time evolution combined with real-time evolution has a computational power equivalent to that of PostBQP, as it is allows for all invertible transformations, not only just unitary. We give an intuition on why imaginary-time evolution gives access to post-selection of events, even those with exponentially small probability. Consider that for $\varepsilon = e^{-q(n)}$ with q a polynomial, one is given the following state

$$|\phi\rangle = \sqrt{\varepsilon}\,|0\rangle\,|\phi_0\rangle + \sqrt{1-\varepsilon}\,|1\rangle\,|\phi_1\rangle\ . \tag{7.3}$$

The task is to post-select on the first qubit being $|0\rangle$. This has an exponentially small probability ε of occurring. We use access to imaginary-time evolution (see Problem 7.3) with input state $|\phi\rangle$, Hamiltonian $H = -Z \otimes I$ and time β, which yields the state

$$|\psi\rangle = \frac{e^{+\beta}\sqrt{\varepsilon}\,|0\rangle\,|\phi_0\rangle + e^{-\beta}\sqrt{1-\varepsilon}\,|1\rangle\,|\phi_1\rangle}{\sqrt{e^{+2\beta}\varepsilon + e^{-2\beta}(1-\varepsilon)}}. \tag{7.4}$$

Finally choosing $\beta = q(n)/2$ the probability p_0 of measuring the first qubit in $|0\rangle$ is very close to 1, as follows.

$$p_0 = \frac{e^{+2\beta}\varepsilon}{e^{+2\beta}\varepsilon + e^{-2\beta}(1-\varepsilon)} > \frac{1}{1+e^{-q(n)}}\,. \tag{7.5}$$

Therefore for time $\beta \in \Omega(\mathrm{poly}(n))$ imaginary-time evolution combined with real-time evolution is PostBQP-complete. Could one find a lower complexity class for lower integration time say, $\beta \in \Theta(\log(n))$?

It is well known that imaginary-time evolution is used to solve ground-state problems, including QMA-complete problems. For completeness we provide the constructive reduction of a QMA-complete problem to the imaginary-time evolution, in Section 7.6.5. At a high level we show that given an instance of the ground-energy problem for a 2-local real Hamiltonian [204] H over n qubits, one can use access to a solver of the imaginary-time evolution problem (Problem 7.3) with $|\psi_0\rangle$ taken at random (e.g. from a 2-design), H and $\beta \in \mathrm{poly}(n)$ to solve the ground-energy problem in polynomial time. The proof yields a lower bound on the time of integration, sufficient to guarantee that the ground energy problem can be resolved. This bound is tight, there exist a Hamiltonian for which this lower bound is also necessary. This lower bound on the integration time is inversely proportional to the promise gap, which is itself at most

polynomially small. The proof in Section 7.6.5 is super-seeded by the post-selection argument because QMA⊆PostBQP. In addition, because of this lower bound there is no scaling of β that would make the problem QMA-hard but not PostBQP-complete.

7.4.3. PostBQP-completeness of exponentially large non-energy-conserving systems

Combining the previous, we have that post-selection can be reduced to imaginary-time evolution for polynomial integration time β, which can in turn be reduced to non-energy-conserving exponentially large differential equations. With this we can conclude that the latter is PostBQP-hard for times poly-logarithmic in the system size (i.e, polynomial in the number of qubits n). We have also identified that squeezing gates in our framework correspond to imaginary time evolution of the $Z \otimes |m\rangle\langle m|$ Hamiltonian in Section 7.6.2. This is precisely the Hamitonian we use in Section 7.4.2 to illustrate how one may use imaginary-time evolution to perform post-selection. That means that adding squeezing gates to the exponentially large interferometer boosts its complexity from BQP-complete to PostBQP-complete, a dramatic surge in computational power (we provide more details in Section 7.6.6).

7.5. Outlook

Our work contributed to the body of knowledge of schemes leading to BQP-complete tasks. In particular, along with Ref. [42], we show examples of how linear and energy-preserving evolutions of exponentially many simple physical systems can be efficiently simulated on a quantum computer. A key unique feature of our framework is that we translate a sequence of gates from one physical system to another (product of exponentials) rather than performing real-time evolution of a Hamiltonian (exponential of a sum).

This main part of our work opens up several interesting research directions. For instance, we have shown how to simulate the evolution of the first and second moments of bosonic states. This makes the simulation complete only for Gaussian states. Hence, we envision two possible paths to extend our proposed framework to better approximate the simulation of non-Gaussian states. First, we could find ways to simulate the evolution of higher moments. To what extent this would improve the quality of a simulation for non-Gaussian states, such as Fock states, remains open.

Second, because bosonic states can be written as a continuous sum over coherent states, approximating them on a grid of coherent states may also be a viable strategy to simulate non-Gaussian states.

Additionally, we also show that for time poly-logarithmic in the system size a set of non-energy-conserving systems yield PostBQP-completeness. This is compatible with existing literature which devises quantum algorithms that are efficient for constant times only [172]. Moreover, we prove that adding squeezing gates boosts the computational power of interferometers from BQP-complete to PostBQP-complete.

We hope that this chapter sharpens the community's understanding of the power of quantum computers to simulate large dynamical linear systems. The next frontier is non-linear systems, which are particularly relevant because they include computational fluid dynamics. Can we classify some non-linear classical dynamical problems with respect to quantum complexity classes such as BQP, QMA or PostBQP?

7.6. Appendix

7.6.1. Framework

Time evolution of quadrature operators in phase space

Let us consider a system of bosons with M modes, and let us assume $\hbar = 1$. The state space of such a system is $\mathcal{H} = \bigotimes_{m=1}^{M} \mathcal{F}_m$, where $\mathcal{F}_m$ is the Fock space associated to the m-th mode. That is, each $\mathcal{F}_m$ is spanned by the infinitely-many basis vectors $\{|k\rangle_m\}_{k\in\mathbb{N}}$ indicating the occupancy number of the mode. For example, if we fix the number of bosons to 3 and let the number of modes be $M = 4$, the basis state $|0,1,2,0\rangle \equiv |0\rangle \otimes |1\rangle \otimes |2\rangle \otimes |0\rangle$ corresponds to the state with one boson occupying the second mode and two bosons occupying the third mode. These basis states are eigenstates of the particle number operator, since they have a fixed number of particles, and are known as Fock states. The (non-Hermitian) creation $\hat{a}_m^\dagger$ and annihilation $\hat{a}_m$ operators are defined by their action on Fock states as follows,

$$\begin{aligned} \hat{a}_m^\dagger |N_0,\ldots,N_m,\ldots,N_M\rangle &= \sqrt{N_m+1}\ |N_0,\ldots,N_m+1,\ldots,N_M\rangle\ , \\ \hat{a}_m |N_0,\ldots,N_m,\ldots,N_M\rangle &= \sqrt{N_m}\ |N_0,\ldots,N_m-1,\ldots,N_M\rangle\ . \end{aligned} \tag{7.6}$$

They satisfy the commutation relations

$$\begin{aligned}[\hat{a}_m^\dagger, \hat{a}_{m'}^\dagger] &= [\hat{a}_m, \hat{a}_{m'}] = 0\,, \\ [\hat{a}_m, \hat{a}_{m'}^\dagger] &= \delta_{m,m'}\,.\end{aligned} \tag{7.7}$$

The (Hermitian) particle number operator is given by $\hat{a}_m^\dagger \hat{a}_m$. The (Hermitian) position $\hat{q}_m$ and momentum $\hat{p}_m$ operators can be defined from the creation and annihilation operators as

$$\hat{q}_m = \frac{\hat{a}_m + \hat{a}_m^\dagger}{\sqrt{2}}\,, \qquad \hat{p}_m = i\,\frac{\hat{a}_m^\dagger - \hat{a}_m}{\sqrt{2}}\,. \tag{7.8}$$

Which in turn conversely implies that

$$\hat{a}_m = \frac{\hat{q}_m + i\hat{p}_m}{\sqrt{2}}\,, \qquad \hat{a}_m^\dagger = \frac{\hat{q}_m - i\hat{p}_m}{\sqrt{2}}\,. \tag{7.9}$$

The corresponding commutation relations for position and momentum are

$$\begin{aligned}[\hat{q}_m, \hat{q}_{m'}] &= [\hat{p}_m, \hat{p}_{m'}] = 0\,, \\ [\hat{q}_m, \hat{p}_{m'}] &= i\delta_{m,m'}\,.\end{aligned} \tag{7.10}$$

Let us collect the positions and momenta in a vector

$$\hat{\vec{z}} = (\hat{q}_1, \ldots, \hat{q}_M, \hat{p}_1, \ldots, \hat{p}_M)^T$$

. This allows us to write the commutation relations in Equation (7.10) as

$$\left[\hat{\vec{z}}, \hat{\vec{z}}^T\right] = i\Omega\,, \tag{7.11}$$

where the Ω matrix is

$$\Omega = \begin{pmatrix} 0 & I_M \\ -I_M & 0 \end{pmatrix} = iY \otimes I_M\,. \tag{7.12}$$

Here, Y is the usual 2×2 Pauli matrix and I_M the $M \times M$ identity matrix. It will be convenient for us to explicitly write down the matrix entries of Ω, which are

$$\Omega_{\gamma,\gamma'} = \delta_{\gamma,\gamma'-M} - \delta_{\gamma,\gamma'+M}\,. \tag{7.13}$$

Let us assume that our quantum bosonic system is governed by a quadratic time-independent Hamiltonian of the form

$$\hat{H} = \frac{1}{2}\vec{\hat{z}}^T K \vec{\hat{z}}, \tag{7.14}$$

where K is a real $2M \times 2M$ symmetric matrix. In the Heisenberg picture, the equation of motion of an observable $\hat{O}$ is

$$\frac{\partial \hat{O}}{\partial t} = i[\hat{H}, \hat{O}]\,. \tag{7.15}$$

Therefore, we find

$$\begin{aligned}
\frac{\partial \hat{\vec{z}}_\gamma}{\partial t} &= i[\hat{H}, \hat{\vec{z}}_\gamma] = \frac{i}{2}\Big[\sum_{\alpha\beta} \hat{\vec{z}}_\alpha K_{\alpha\beta} \hat{\vec{z}}_\beta, \hat{\vec{z}}_\gamma\Big] \\
&= \frac{i}{2}\sum_{\alpha\beta} K_{\alpha\beta}\Big[\hat{\vec{z}}_\alpha \hat{\vec{z}}_\beta, \hat{\vec{z}}_\gamma\Big] = \frac{i}{2}\sum_{\alpha\beta} K_{\alpha\beta}\left(\hat{\vec{z}}_\alpha\Big[\hat{\vec{z}}_\beta, \hat{\vec{z}}_\gamma\Big] + \Big[\hat{\vec{z}}_\alpha, \hat{\vec{z}}_\gamma\Big]\hat{\vec{z}}_\beta\right) \\
&= \frac{i}{2}\sum_{\alpha\beta} K_{\alpha\beta}\left(\hat{\vec{z}}_\alpha i(\delta_{\beta,\gamma-M} - \delta_{\beta,\gamma+M}) + i(\delta_{\alpha,\gamma-M} - \delta_{\alpha,\gamma+M})\hat{\vec{z}}_\beta\right) \\
&= \frac{1}{2}\sum_{\alpha\beta} K_{\alpha\beta}\left(-\hat{\vec{z}}_\alpha \Omega_{\beta\gamma} - \Omega_{\alpha\gamma}\hat{\vec{z}}_\beta\right) = \frac{1}{2}\sum_{\alpha\beta}\left(\Omega_{\gamma\beta}K_{\beta\alpha}\hat{\vec{z}}_\alpha + \Omega_{\gamma\alpha}K_{\alpha\beta}\hat{\vec{z}}_\beta\right) \\
&= \left(\Omega K \hat{\vec{z}}\right)_\gamma\,,
\end{aligned} \tag{7.16}$$

where we used $[AB, C] = A[B, C] + [A, C]B$, and the fact that K is symmetric and Ω anti-symmetric. Hence, we arrive at

$$\frac{\partial \hat{\vec{z}}}{\partial t} = \Omega K \hat{\vec{z}}. \tag{7.17}$$

The solution to this differential equation is given by

$$\hat{\vec{z}}(t) = e^{t\Omega K}\hat{\vec{z}}(0)\,. \tag{7.18}$$

The solution of Equation (7.17) must preserve the commutation relations of Equation (7.10) in order to leave the kinematics invariant. Let us call $Q(t) = e^{t\Omega K}$ the propagator that takes the vector $\hat{\vec{z}}(0)$ at time 0 to the vector $\hat{\vec{z}}(t)$ at time t. We impose $\Big[\hat{\vec{z}}(t), \hat{\vec{z}}(t)^T\Big] = [\hat{\vec{z}}(0), \hat{\vec{z}}(0)^T]$, which leads

to

$$\left[Q(t)\hat{\vec{z}}(0), (Q(t)\hat{\vec{z}}(0))^T\right]_{\alpha\beta} = \left[\left(\sum_\gamma Q(t)_{\alpha\gamma}\hat{\vec{z}}_\gamma\right), \left(\sum_{\gamma'} Q(t)_{\beta\gamma'}\hat{\vec{z}}_{\gamma'}\right)\right] \tag{7.19}$$

$$= \sum_{\gamma,\gamma'} Q(t)_{\alpha\gamma} Q(t)_{\beta\gamma'} \left[\hat{\vec{z}}_\gamma, \hat{\vec{z}}_{\gamma'}\right] \tag{7.20}$$

$$= i \sum_{\gamma,\gamma'} Q(t)_{\alpha\gamma} Q(t)_{\beta\gamma'} (\delta_{\gamma,\gamma'-M} - \delta_{\gamma,\gamma'+M}) \tag{7.21}$$

$$= i \sum_{\gamma,\gamma'} Q(t)_{\alpha\gamma} \Omega_{\gamma,\gamma'} Q(t)^T_{\gamma'\beta} \tag{7.22}$$

$$= i \left(Q(t)\,\Omega\,Q^T(t)\right)_{\alpha\beta} . \tag{7.23}$$

It is clear then that $Q(t)\,\Omega\,Q^T(t) = \Omega$ if we are to maintain the commutation relations between positions and momenta. This is precisely the defining condition of symplectic matrices. Hence, the time evolution of $\hat{\vec{z}}$ in phase space is given by a $2M \times 2M$ real symplectic matrix belonging to the group $\mathbb{SP}(M, \mathbb{R})$.

Let us now address the question of how the expectation value $\langle\hat{\vec{z}}\rangle = (\langle\hat{q}_1\rangle, \ldots, \langle\hat{q}_M\rangle, \langle\hat{p}_1\rangle, \ldots, \langle\hat{p}_M\rangle)^T$ of $\hat{\vec{z}}$ evolves in time, given an initial quantum state ρ_0. We find that

$$\frac{\partial\langle\hat{\vec{z}}_\gamma\rangle}{\partial t} = \frac{\partial\ \mathrm{Tr}\left[\hat{\vec{z}}_\gamma\rho_0\right]}{\partial t} = \mathrm{Tr}\left[\frac{\partial\hat{\vec{z}}_\gamma}{\partial t}\rho_0\right] = \mathrm{Tr}\left[(\Omega K\hat{\vec{z}})_\gamma\rho_0\right] =$$
$$= \mathrm{Tr}\left[\left(\sum_{\alpha\beta}\Omega_{\gamma\alpha}K_{\alpha\beta}\hat{\vec{z}}_\beta\right)\rho_0\right] = \sum_{\alpha\beta}\Omega_{\gamma\alpha}K_{\alpha\beta}\,\mathrm{Tr}\left[\hat{\vec{z}}_\beta\rho_0\right] = (\Omega K\langle\hat{\vec{z}}\rangle)_\gamma\,, \tag{7.24}$$

which implies

$$\frac{\partial\langle\hat{\vec{z}}\rangle}{\partial t} = \Omega K\langle\hat{\vec{z}}\rangle\,, \tag{7.25}$$

and

$$\langle\hat{\vec{z}}\rangle(t) = e^{t\Omega K}\langle\hat{\vec{z}}\rangle(0)\,. \tag{7.26}$$

We can also collect the expectation value of products of quadrature operators over ρ_0 in the $2M \times 2M$ positive-definite covariance matrix $\vec{\sigma}$

whose entries are given by

$$\vec{\sigma}_{\alpha\beta} = \frac{1}{2}\langle \hat{\vec{z}}_\alpha \hat{\vec{z}}_\beta + \hat{\vec{z}}_\beta \hat{\vec{z}}_\alpha \rangle - \langle \hat{\vec{z}}_\alpha \rangle \langle \hat{\vec{z}}_\beta \rangle \,. \tag{7.27}$$

Let us derive the corresponding equation of motion. We start by considering

$$\begin{aligned}
\frac{\partial(\hat{\vec{z}}_\gamma \hat{\vec{z}}_\delta)}{\partial t} &= i[\hat{H}, \hat{\vec{z}}_\gamma \hat{\vec{z}}_\delta] = \frac{i}{2}\Big[\sum_{\alpha\beta} \hat{\vec{z}}_\alpha K_{\alpha\beta} \hat{\vec{z}}_\beta, \hat{\vec{z}}_\gamma \hat{\vec{z}}_\delta\Big] = \frac{i}{2}\sum_{\alpha\beta} K_{\alpha\beta}\Big[\hat{\vec{z}}_\alpha \hat{\vec{z}}_\beta, \hat{\vec{z}}_\gamma \hat{\vec{z}}_\delta\Big] \\
&= \frac{i}{2}\sum_{\alpha\beta} K_{\alpha\beta}\Bigg(\hat{\vec{z}}_\alpha\Big[\hat{\vec{z}}_\beta, \hat{\vec{z}}_\gamma\Big]\hat{\vec{z}}_\delta + \Big[\hat{\vec{z}}_\alpha, \hat{\vec{z}}_\gamma\Big]\hat{\vec{z}}_\beta \hat{\vec{z}}_\delta \\
&+ \hat{\vec{z}}_\gamma \hat{\vec{z}}_\alpha\Big[\hat{\vec{z}}_\beta, \hat{\vec{z}}_\delta\Big] + \hat{\vec{z}}_\gamma\Big[\hat{\vec{z}}_\alpha, \hat{\vec{z}}_\delta\Big]\hat{\vec{z}}_\beta\Bigg) \\
&= -\frac{1}{2}\sum_{\alpha\beta} K_{\alpha\beta}\left(\hat{\vec{z}}_\alpha(\delta_{\beta,\gamma-M} - \delta_{\beta,\gamma+M})\hat{\vec{z}}_\delta + (\delta_{\alpha,\gamma-M} - \delta_{\alpha,\gamma+M})\hat{\vec{z}}_\beta \hat{\vec{z}}_\delta\right. \\
&\left.+\hat{\vec{z}}_\gamma \hat{\vec{z}}_\alpha(\delta_{\beta,\delta-M} - \delta_{\beta,\delta+M}) + \hat{\vec{z}}_\gamma(\delta_{\alpha,\delta-M} - \delta_{\alpha,\delta+M})\hat{\vec{z}}_\beta\right) \\
&= -\frac{1}{2}\sum_{\alpha\beta} K_{\alpha\beta}\left(\hat{\vec{z}}_\alpha \Omega_{\beta\gamma}\hat{\vec{z}}_\delta + \Omega_{\alpha\gamma}\hat{\vec{z}}_\beta \hat{\vec{z}}_\delta + \hat{\vec{z}}_\gamma \hat{\vec{z}}_\alpha \Omega_{\beta\delta} + \hat{\vec{z}}_\gamma \Omega_{\alpha\delta}\hat{\vec{z}}_\beta\right) \\
&= -(\hat{\vec{z}}^T K\Omega)_\gamma \hat{\vec{z}}_\delta - \hat{\vec{z}}_\gamma(\hat{\vec{z}}^T K\Omega)_\delta = (\Omega K\hat{\vec{z}})_\gamma \hat{\vec{z}}_\delta + \hat{\vec{z}}_\gamma(\Omega K\hat{\vec{z}})_\delta \,,
\end{aligned} \tag{7.28}$$

where we used that $[AB, CD] = A[B, C]D + [A, C]BD + CA[B, D] + C[A, D]B$, and the fact that K (Ω) is symmetric (anti-symmetric). In matrix form, we get

$$\frac{\partial(\hat{\vec{z}}\hat{\vec{z}}^T)}{\partial t} = \Omega K\hat{\vec{z}}\hat{\vec{z}}^T - \hat{\vec{z}}\hat{\vec{z}}^T K\Omega \,. \tag{7.29}$$

Let us now look at the evolution of the expectation value of two-point

correlators. Analogously to Equation (7.24), we have

$$\begin{aligned}
\frac{\partial\langle\hat{\vec{z}}_\gamma\hat{\vec{z}}_\delta\rangle}{\partial t} &= \frac{\partial\ \mathrm{Tr}\left[\hat{\vec{z}}_\gamma\hat{\vec{z}}_\delta\rho\right]}{\partial t} = \mathrm{Tr}\left[\frac{\partial\hat{\vec{z}}_\gamma}{\partial t}\hat{\vec{z}}_\delta\rho + \hat{\vec{z}}_\gamma\frac{\partial\hat{\vec{z}}_\delta}{\partial t}\rho\right] \\
&= \mathrm{Tr}\left[(\Omega K\hat{\vec{z}})_\gamma\hat{\vec{z}}_\delta\rho + \hat{\vec{z}}_\gamma(\Omega K\hat{\vec{z}})_\delta\rho\right] \\
&= \mathrm{Tr}\left[\left(\sum_{\alpha\beta}\Omega_{\gamma\alpha}K_{\alpha\beta}\hat{\vec{z}}_\beta\right)\hat{\vec{z}}_\delta\rho + \hat{\vec{z}}_\gamma\left(\sum_{\alpha\beta}\Omega_{\delta\alpha}K_{\alpha\beta}\hat{\vec{z}}_\beta\right)\rho\right] \\
&= \sum_{\alpha\beta}\Omega_{\gamma\alpha}K_{\alpha\beta}\,\mathrm{Tr}\left[\hat{\vec{z}}_\beta\hat{\vec{z}}_\delta\rho\right] + \sum_{\alpha\beta}\Omega_{\delta\alpha}K_{\alpha\beta}\,\mathrm{Tr}\left[\hat{\vec{z}}_\gamma\hat{\vec{z}}_\beta\rho\right] \\
&= (\Omega K\langle\hat{\vec{z}}\hat{\vec{z}}^T\rangle)_{\gamma\delta} - (\langle\hat{\vec{z}}\hat{\vec{z}}^T\rangle K\Omega)_{\gamma\delta}\,,
\end{aligned} \tag{7.30}$$

or, in matrix form,

$$\frac{\partial(\langle\hat{\vec{z}}\hat{\vec{z}}^T\rangle)}{\partial t} = \Omega K\langle\hat{\vec{z}}\hat{\vec{z}}^T\rangle - \langle\hat{\vec{z}}\hat{\vec{z}}^T\rangle K\Omega\,. \tag{7.31}$$

Therefore, we arrive at

$$\frac{\partial\vec{\sigma}}{\partial t} = \Omega K\vec{\sigma} - \vec{\sigma}K\Omega\,. \tag{7.32}$$

If K represents a particle-preserving Hamiltonian, then $[\Omega, K] = 0$ according to Proposition 7.2, so we can write

$$\frac{\partial\vec{\sigma}}{\partial t} = [\Omega K, \vec{\sigma}]\ . \tag{7.33}$$

The solution to this equation is

$$\vec{\sigma} = e^{\Omega Kt}\,\vec{\sigma}(0)\,e^{-\Omega Kt}\,. \tag{7.34}$$

If instead K represents a non-particle-preserving Hamiltonian such that $\{\Omega, K\} = 0$, we can write

$$\frac{\partial\vec{\sigma}}{\partial t} = \{\Omega K, \vec{\sigma}\}\ , \tag{7.35}$$

whose solution is

$$\vec{\sigma}(t) = e^{\Omega Kt}\,\vec{\sigma}(0)\,e^{\Omega Kt}\,. \tag{7.36}$$

Pauli basis for the symplectic algebra

Here we present a useful Supplemental Proposition that provides a Pauli basis for the symplectic algebra $\mathfrak{sp}(M, \mathbb{R})$.

Proposition 7.1
An orthogonal basis for the standard representation of the $\mathfrak{sp}(M, \mathbb{R})$ algebra, where $M = 2^n$, is given by the set

$$B_{\mathfrak{sp}(M,\mathbb{R})} \equiv i\{Y \otimes P_s\} \cup i\{I \otimes P_a\} \cup \{X \otimes P_s\} \cup \{Z \otimes P_s\}\,, \quad (7.37)$$

where P_s and P_a belong to the sets of arbitrary symmetric and anti-symmetric Pauli strings on n qubits, respectively, and I, X, Y, Z are the usual 2×2 Pauli matrices.

Proof. We first recall that any $2M \times 2M$ matrix A satisfying $A^T\Omega = -\Omega A$ belongs to $\mathfrak{sp}(M, \mathbb{R}) \subset \mathrm{End}(\mathbb{R}^{2M})$. Clearly, the (phased) Pauli operators on $n+1$ qubits in Equation (7.37) constitute $2^{n+1} \times 2^{n+1} = 2M \times 2M$ matrices, with $M = 2^n$. Also, note they are all real-valued (although not all anti-Hermitian), which follows from the fact that a Pauli string is real (purely imaginary) when it contains an even (odd) number of Y's, i.e. when it is symmetric (anti-symmetric). Thus, $B_{\mathfrak{sp}(M,\mathbb{R})} \subset \mathrm{End}(\mathbb{R}^{2M})$. We know from Proposition 1 in Ref. [190] that they satisfy the symplectic property, implying $B_{\mathfrak{sp}(M,\mathbb{R})} \subset \mathfrak{sp}(M, \mathbb{R})$. Given that they are Hilbert-Schmidt orthogonal, and that $|B_{\mathfrak{sp}(M,\mathbb{R})}| = M(2M+1) = \dim(\mathfrak{sp}(M, \mathbb{R}))$, to prove they constitute an orthogonal basis for $\mathfrak{sp}(M, \mathbb{R})$ it simply remains to show that they are closed under commutation.

To do so, we first recall that the commutator of two anti-symmetric or symmetric matrices is anti-symmetric, whereas the commutator of a symmetric matrix and an anti-symmetric one is symmetric. We start with the (non-zero) commutator $X \otimes P_s$ and $X \otimes P'_s$, which gives an operator of the following form

$$[X \otimes P_s, X \otimes P'_s] \propto \pm iI \otimes P_a\,. \quad (7.38)$$

The $\pm i$ factor follows from the fact that the Pauli strings P_s and P'_s differ at an odd number of sites. The same is true if we replace X by Z on the first qubit,

$$[Z \otimes P_s, Z \otimes P'_s] \propto \pm iI \otimes P_a\,. \quad (7.39)$$

We continue by computing the (non-zero) commutator of two operators of the form $X \otimes P_s$ and $Z \otimes P'_s$,

$$[X \otimes P_s, Z \otimes P'_s] \propto \pm iY \otimes P''_s\,. \quad (7.40)$$

Again, the $\pm i$ factor follows from the fact that $X \otimes P_s$ and $Z \otimes P'_s$ differ at an odd number of sites. Next, let us look at the non-zero commutator of operators $X \otimes P_s$ or $Z \otimes P_s$ with $iI \otimes P_a$,

$$[X \otimes P_s, iI \otimes P_a] \propto \pm X \otimes P'_s \quad \text{or} \quad [Z \otimes P_s, iI \otimes P_a] \propto \pm Z \otimes P'_s \,. \tag{7.41}$$

Here, the i factor arising from commuting the Pauli strings cancels out with the i in $iI \otimes P_a$. Similarly, the non-zero commutator of $X \otimes P_s$ or $Z \otimes P_s$ with $iY \otimes P'_s$ is as follows

$$[X \otimes P_s, iY \otimes P'_s] \propto \pm Z \otimes P''_s \quad \text{or} \quad [Z \otimes P_s, iY \otimes P'_s] \propto \pm X \otimes P''_s \,. \tag{7.42}$$

Furthermore, commuting $iY \otimes P_s$ and $iY \otimes P'_s$, or $iI \otimes P_a$ with $iI \otimes P'_a$ leads to either zero or an operator of the form

$$[iY \otimes P_s, iY \otimes P'_s] \propto \pm iI \otimes P_a \quad \text{or} \quad [iI \otimes P_a, iI \otimes P'_a] \propto \pm iI \otimes P''_a \,. \tag{7.43}$$

Finally, the non-zero commutator of $iY \otimes P_s$ and $iI \otimes P_a$ gives $\pm iY \otimes P_s$,

$$[iY \otimes P_s, iI \otimes P_a] \propto \pm iY \otimes P_s \,. \tag{7.44}$$

Therefore, we conclude that the set $B_{\mathfrak{sp}(M,\mathbb{R})} \subset \mathfrak{sp}(M,\mathbb{R})$ of mutually orthogonal operators is closed under commutation and satisfies

$$\dim(B_{\mathfrak{sp}(M,\mathbb{R})}) = M(2M+1) = \dim(\mathfrak{sp}(M,\mathbb{R}))\,.$$

Thus, it constitutes an orthogonal basis for the standard representation of $\mathfrak{sp}(M,\mathbb{R})$. □

Particle-preserving gates

Next, we show that particle-preserving Gaussian bosonic (GB) gates lead to unitary evolutions at the qubit level.

Proposition 7.2
When a gate generator is of the form

$$\hat{H} = \sum_{m,m'=1}^{M} h_{mm'}\, \hat{a}^\dagger_m \hat{a}_{m'} + \frac{\mathrm{Tr}[h]}{2} I_{2M}\,, \tag{7.45}$$

where h is a Hermitian matrix, then $[\Omega, K] = 0$, and the propagator $e^{t\Omega K}$

is the real time evolution under the effective Hamiltonian $-i\Omega K$.

Proof. Expressed in terms of position and momentum operators, we find

$$\begin{aligned}\hat{H} &= \frac{1}{2}\sum_{m,m'=1}^{2^n} h_{mm'}\,(q_m - ip_m)(q_{m'} + ip_{m'}) + \frac{\mathrm{Tr}[h]}{2} I_{2M} \\ &= \frac{1}{2}\sum_{m,m'=1}^{2^n} h_{mm'}\,(q_m q_{m'} + p_m p_{m'} + iq_m p_{m'} - ip_m q_{m'}) + \frac{\mathrm{Tr}[h]}{2} I_{2M} \\ &= \frac{1}{2}\sum_{m=1}^{2^n} h_{mm}\,(q_m^2 + p_m^2) + \sum_{\substack{m,m'=1 \\ m'>m}}^{2^n} \mathrm{Re}[h_{mm'}]\,(q_m q_{m'} + p_m p_{m'}) \\ &+ \sum_{\substack{m,m'=1 \\ m'>m}}^{2^n} \mathrm{Im}[h_{mm'}]\,(q_m p_{m'} - p_m q_{m'})\,, \end{aligned} \tag{7.46}$$

where we used the commutation relations from Equation (7.10). In other words, particle-preserving gate generators are such that the K matrix is a real linear combination of Paulis of the form $I \otimes P_s$ (corresponding to the first two sums in Equation (7.46)) and/or $Y \otimes P_a$ (corresponding to the last sum in Equation (7.46)). This automatically implies that $[\Omega, K] = 0$. Finally, either ΩK is a real combination of Paulis of the form $(iY \otimes I_M)(I \otimes P_s) = iY \otimes P_s$ or $(iY \otimes I_M)(Y \otimes P_a) = iI \otimes P_a$ (both of which are in the symplectic algebra according to Proposition 7.1). That is, ΩK is anti-Hermitian and the symplectic propagator $e^{t\Omega K}$ is unitary. Hence, these types of gate generators result in unitary dynamics in phase space. □

Non-particle-preserving gates

We here show that a family of non-particle-preserving GB gates lead to an imaginary-time evolution at the qubit level.

Proposition 7.3
When a gate generator is of the form

$$\hat{H} = \sum_{m,m'=1}^{M} \Delta^{\dagger}_{mm'}\,\hat{a}_m \hat{a}_{m'} + \sum_{m,m'=1}^{M} \Delta_{mm'}\,\hat{a}^{\dagger}_m \hat{a}^{\dagger}_{m'}\,, \tag{7.47}$$

where Δ is a symmetric matrix, then $\{\Omega, K\} = 0$, and the propagator $e^{t\Omega K}$ is an imaginary time evolution under the effective Hamiltonian $-\Omega K$.

Proof. In terms of positions and momenta, we find

$$\begin{aligned}
\hat{H} &= \frac{1}{2} \sum_{m,m'=1}^{2^n} \Delta^{\dagger}_{mm'} (q_m + ip_m)(q_{m'} + ip_{m'}) \\
&+ \frac{1}{2} \sum_{m,m'=1}^{2^n} \Delta_{mm'} (q_m - ip_m)(q_{m'} - ip_{m'}) \\
&= \frac{1}{2} \sum_{m,m'=1}^{2^n} \Delta^{\dagger}_{mm'} (q_m q_{m'} - p_m p_{m'} + iq_m p_{m'} + ip_m q_{m'}) \\
&+ \frac{1}{2} \sum_{m,m'=1}^{2^n} \Delta_{mm'} (q_m q_{m'} - p_m p_{m'} - iq_m p_{m'} - ip_m q_{m'}) \\
&= \sum_{m,m'=1}^{2^n} \mathrm{Re}\left[\Delta_{mm'}\right] (q_m q_{m'} - p_m p_{m'}) \\
&+ \sum_{m,m'=1}^{2^n} \mathrm{Im}\left[\Delta_{mm'}\right] (q_m p_{m'} + p_m q_{m'}) \,. \qquad (7.48)
\end{aligned}$$

In this case, the K matrix is a real linear combination of Paulis of the form $Z \otimes P_s$ (corresponding to the first sum in Equation (7.48)) and/or $X \otimes P_s$ (corresponding to the second sum in Equation (7.48)). This implies that $\{\Omega, K\} = 0$. Then, either ΩK is a real combination of Paulis of the form $(iY \otimes I_M)(Z \otimes P_s) = X \otimes P_s$ or $(iY \otimes I_M)(X \otimes P_s) = Z \otimes P_s$ (both of which are in the symplectic algebra according to Proposition 7.1). That is, ΩK is Hermitian and the symplectic propagator $e^{t\Omega K}$ is given by the imaginary-time evolution of the effective gate generator $-\Omega K$. □

7.6.2. From bosonic gates to qubit gates

Local gates

- **Phase gate:** This gate is described by the generator $\hat{H} = \hat{q}_m^2 + \hat{p}_m^2$ in terms of bosonic operators. Therefore the real symmetric K matrix

can be expressed as

$$\begin{aligned} K &= 2\left(|m\rangle\langle m| + |m+M\rangle\langle m+M|\right) \\ &= 2\left(|0\rangle\langle 0| \otimes |m\rangle\langle m| + |1\rangle\langle 1| \otimes |m\rangle\langle m|\right) \\ &= 2I \otimes |m\rangle\langle m| \,. \end{aligned} \tag{7.49}$$

The associated generator acting on the qubit picture is $\Omega K = 2iY \otimes |m\rangle\langle m|$, and thus

$$\begin{aligned} e^{t\Omega K} &= \sum_{s=0}^{\infty} \frac{(t\Omega K)^s}{s!} = \sum_{s=0}^{\infty} \frac{(2it\, Y \otimes |m\rangle\langle m|)^s}{s!} \\ &= I_{2M} + (\cos(2t) - 1) I \otimes |m\rangle\langle m| + i \sin(2t) Y \otimes |m\rangle\langle m| \\ &= I \otimes \overline{|m\rangle\langle m|} + I \otimes |m\rangle\langle m| \\ &+ (\cos(2t) - 1) I \otimes |m\rangle\langle m| + i \sin(2t) Y \otimes |m\rangle\langle m| \\ &= I \otimes \overline{|m\rangle\langle m|} + (\cos(2t)) I \otimes |m\rangle\langle m| + i \sin(2t) Y \otimes |m\rangle\langle m| \\ &= I \otimes \overline{|m\rangle\langle m|} + e^{2itY} \otimes |m\rangle\langle m| \,. \end{aligned} \tag{7.50}$$

Above we have used the fact that $I_{2M} = I \otimes |m\rangle\langle m| + I \otimes \overline{|m\rangle\langle m|}$ where $\overline{|m\rangle\langle m|} \coloneqq I - |m\rangle\langle m|$ is the projector onto the orthogonal complement of $|m\rangle$. Hence this gate acts trivially when the state in the register qubits is $|m'\rangle$ such that $m' \neq m$, while it applies an $R_y(4t)$ rotation on the symplectic qubit otherwise (here we assume the standard definition $R_y(\theta) = e^{-i\theta Y/2}$). Hence, the associated qubit gate is a SELECT-$R_y(4t)$.

- **Beamsplitter:** This gate is described by $\hat{H} = \hat{q}_m \hat{p}_{m'} - \hat{q}_{m'} \hat{p}_m$, where $m \neq m'$, in bosonic operators. Therefore the real symmetric K matrix can be expressed as

$$\begin{aligned} K &= 2\left(|m' + M\rangle\langle m| + |m\rangle\langle m' + M| \right. \\ &\quad \left. - |m + M\rangle\langle m'| - |m'\rangle\langle m + M|\right) \\ &= 2iY \otimes \left(|m\rangle\langle m'| - |m'\rangle\langle m|\right). \end{aligned} \tag{7.51}$$

Therefore $\Omega K = 2iI \otimes (i\,|m\rangle\langle m'| - i\,|m'\rangle\langle m|)$. Here, instead of directly exponentiating this operator and finding a closed formula (as we did with the phase gate), we will derive a sequence of gates whose combined actions lead to $e^{\Omega K}$.

We begin by noting that ΩK acts trivially on the symplectic qubit.

Therefore we focus on the action on the register qubits, where it corresponds to a y rotation in the subspace spanned by $|m\rangle$ and $|m'\rangle$. We write the associated classical bitstrings as $m = m_n \cdots m_1$, and analogously for m'. We denote the bitstring operation $\overline{x}$ as taking the bit-wise negation of each individual bit. We separate the bitstring indices between those where the bits of m and m' match, and those where they differ. We call the first set $e = \{e_j\}_{1 \leq j \leq E}$, such that $m_{e_j} = m'_{e_j}\ \forall j$, and the second set $d = \{d_j\}_{1 \leq j \leq D}$, such that $m_{d_j} = \overline{m'_{d_j}}\ \forall j$, where $E + D = n$. We can then factorize Equation (7.51) to obtain

$$\Omega K = 2iI \otimes \left(\prod_{j=1}^{E} \left|m_{e_j}\right\rangle\!\left\langle m_{e_j}\right|_{e_j} \cdot \left(i \left|m_d\right\rangle\!\left\langle \overline{m_d}\right| - i \left|\overline{m_d}\right\rangle\!\left\langle m_d\right|\right)_d \right), \tag{7.52}$$

where the notation $\left|m_{e_j}\right\rangle\!\left\langle m_{e_j}\right|_{e_j}$ indicates a projector on $|e_j\rangle$ on qubit e_j and identity on the rest, and $\left(i \left|m_d\right\rangle\!\left\langle \overline{m_d}\right| - i \left|\overline{m_d}\right\rangle\!\left\langle m_d\right|\right)_d$ acts non-trivially on the qubits whose indexes belong in d. In fact, it is a y-rotation in the subspace spanned by $\left(\left|\overline{m_d}\right\rangle, \left|m_d\right\rangle\right)$. We (arbitrarily) choose to map this rotation to the least-significant qubit where the m and m' bitstrings differ, that is, on qubit d_1. To do so we are going to implement a change of basis using controlled multi-NOTs, so that $|m_d\rangle \to |0\rangle \otimes |0\rangle^{\otimes D-1}$ and $\left|\overline{m_d}\right\rangle \to |1\rangle \otimes |0\rangle^{\otimes D-1}$. First, we apply $B \coloneqq X_{d_1}^{m_{d_1}}$ so that the least-significant qubit matches the previous expression. Then we apply the two following controlled multi-NOT:

$$C_0 \coloneqq \mathrm{CTRL}(|0\rangle\!\langle 0|_{d_1}) \prod_{j=2}^{D} X_{d_j}^{m_{d_j}}, C_1 \coloneqq \mathrm{CTRL}(|1\rangle\!\langle 1|_{d_1}) \prod_{j=2}^{D} X_{d_j}^{\overline{m_{d_j}}}, \tag{7.53}$$

where $\mathrm{CTRL}(\Pi)U_k$ is the gate U applied to qubits from set k controlled on the single-qubit local projector Π, for example, $\mathrm{CTRL}(|1\rangle\!\langle 1|_5)X_1$ is an X-gate on qubit 1 controlled by the qubit 5. Then we can apply the SELECT-R_y gate with a target on the qubit whose index is d_1, whose gate generator is as follows.

$$SY \coloneqq \prod_{j=1}^{E} \left|m_{e_j}\right\rangle\!\left\langle m_{e_j}\right|_{e_j} \prod_{j=2}^{D} |0\rangle\!\langle 0|_{d_j} Y_{d_1}. \tag{7.54}$$

Finally, we apply the Hermitian conjugate of the change of basis $B^\dagger C_0^\dagger C_1^\dagger = BC_0C_1$ to return to our original basis. Overall the transformation goes as follows:

$$\begin{aligned} e^{2itI\otimes i(|m\rangle\langle m'|-|m'\rangle\langle m|)} &= e^{2itI\otimes C_1C_0BSYBC_0C_1} \\ &= I\otimes C_1C_0Be^{2itSY}BC_0C_1\,, \\ \text{with}\quad e^{2itSY} &= \text{SELECT}\left(\prod_{j=1}^{E}\left|m_{e_j}\right\rangle\!\left\langle m_{e_j}\right|_{e_j}\prod_{j=2}^{D}|0\rangle\langle 0|_{d_j}\right)R_y(4t)_{d_1} \end{aligned} \tag{7.55}$$

where $\text{SELECT}(\Pi)U_k$ is the gate U applied to qubits from set k controlled on the projector Π, for example, $\text{SELECT}(|0\rangle\langle 0|_3\,|1\rangle\langle 1|_5)X_1$ is an X-gate on qubit 1 controlled by the qubit 5 and 0-controlled by qubit 3.

- **Squeezing Gate:** This gate is described by the generator $\hat{H} = \pm(\hat{p}_m\hat{q}_m + \hat{q}_m\hat{p}_m)$. Therefore the real symmetric K matrix can be expressed as

$$\begin{aligned} K &= 2(|m\rangle\langle m+M| + |m+M\rangle\langle m|) && (7.56)\\ &= 2(|0\rangle\langle 1| + |1\rangle\langle 0|)\otimes|m\rangle\langle m| && (7.57)\\ &= 2X\otimes|m\rangle\langle m|\,. && (7.58) \end{aligned}$$

The associated qubit generator is $\Omega K = \pm 2Z\otimes|m\rangle\langle m|$. It is an imaginary time evolution $e^{\pm 2tZ\otimes|m\rangle\langle m|} = e^{\mp it'2Z\otimes|m\rangle\langle m|}$, where $t' = it$, under the effective Hamiltonian ΩK. For small t we have $e^{\pm 2tZ\otimes|m\rangle\langle m|} = I \pm 2tZ\otimes|m\rangle\langle m| + O(t^2)$. And therefore we want the state $\left|\hat{\vec{z}}\right\rangle$ to be transformed (up to normalization) as

$$\begin{aligned} \left|\hat{\vec{z}}\right\rangle \to (1\pm 2t)\langle\hat{q}_m\rangle\,|0\rangle\otimes|m\rangle + (1\mp 2t)\langle\hat{p}_m\rangle\,|1\rangle\otimes|m\rangle \\ + \sum_{m'\neq m}\langle\hat{q}_{m'}\rangle\,|0\rangle\otimes|m'\rangle + \langle\hat{p}_{m'}\rangle\,|1\rangle\otimes|m'\rangle\,. \end{aligned} \tag{7.59}$$

This can be implemented by a heralded protocol as a Linear Combi-

nation of Unitaries (LCU) of the form

$$aI + b(I \otimes |m\rangle\langle m| - I \otimes \overline{|m\rangle\langle m|}) \\ + c(Z \otimes |m\rangle\langle m| + I \otimes \overline{|m\rangle\langle m|}) + d(-Z \otimes |m\rangle\langle m| + I \otimes \overline{|m\rangle\langle m|}) , \tag{7.60}$$

with $a+b+c+d=1$ and $a,b,c,d \geq 0$. Applied to the state $\left|\hat{\vec{z}}\right\rangle$ the above LCU yields the following state

$$(a+b+c-d)\langle \hat{q}_m \rangle |0\rangle |m\rangle + (a+b-c+d)\langle \hat{p}_m \rangle |1\rangle |m\rangle \\ + (a-b+c+d) \sum_{m' \neq m} \langle \hat{q}_{m'} \rangle |0\rangle \left|m'\right\rangle + \langle \hat{p}_{m'} \rangle |1\rangle \left|m'\right\rangle . \tag{7.61}$$

We want this state to be proportional to the one in Equation (7.59) by a factor $\gamma < 1$. We thus need to solve the linear system of equations

$$\begin{cases} a+b+c+d &= 1 \\ a+b+c-d &= \gamma(1 \pm 2t) \\ a+b-c+d &= \gamma(1 \mp 2t) \\ a-b+c+d &= \gamma \end{cases} , \tag{7.62}$$

whose solution is

$$a = \frac{3\gamma - 1}{2} , \quad b = \frac{1-\gamma}{2} , \quad c = \frac{1-\gamma \pm 2\gamma t}{2} , \quad d = \frac{1-\gamma \mp 2\gamma t}{2} . \tag{7.63}$$

Since c and d need to be larger than 0,

$$\gamma \leq \frac{1}{1 \mp 2t} , \qquad \gamma \leq \frac{1}{1 \pm 2t} . \tag{7.64}$$

In order to maximize the probability of success we should choose the maximum γ that satisfies these constraints. Depending on the sign of $\hat{H}$ one or the other inequalities above is saturated. Therefore we choose $\gamma = 1/(1+2t)$. This yields

$$a = \frac{1-t}{1+2t} , \qquad b = \frac{t}{1+2t} , \qquad c = \frac{t \pm t}{1+2t} , \qquad d = \frac{t \mp t}{1+2t} . \tag{7.65}$$

Let us calculate the probability of success as the norm of the state

in Equation (7.61) for small t,

$$\frac{1}{(1+2t)^2}\left((1\pm 2t)^2\langle q_m\rangle^2+(1\mp 2t)^2\langle p_m\rangle^2+(1-\langle q_m\rangle^2-\langle p_m\rangle^2)\right) \approx \frac{1\pm 4t\langle q_m\rangle^2\mp 4t\langle p_m\rangle^2}{1+4t}. \quad (7.66)$$

When $\hat{H}=\hat{p}_m\hat{q}_m+\hat{q}_m\hat{p}_m$, we can see that the best case is $\langle q_m\rangle=1$ and $\langle p_m\rangle=0$, which yields a probability of failure of 0, and the worst case is $\langle p_m\rangle=1$, which yields a probability of failure of $\sim 8t$.

For a squeezing gate, we are given a bitstring description of the mode to which it applies, and the squeezing parameter t. This allows us to compute (a,b,c,d) as per the above equations. In practice, we add two ancillary qubits initialized to zero. We design a unitary U such that $|00\rangle \xrightarrow{U} \sqrt{a}\,|00\rangle+\sqrt{b}\,|01\rangle+\sqrt{c}\,|10\rangle+\sqrt{d}\,|11\rangle$, and apply it to the ancillary register. Then we apply the SELECT-unitaries as per the LCU, derived above. As one unitary is the identity, we do not need to apply this gate, and as either c or d is zero we do not need to apply the corresponding gate either. Each SELECT gate also has controls on the register to select the mode it is being applied to). If the gate generator $\hat{H}$ has a positive sign, then $d=0$, and we apply successively:

$$B \coloneqq \mathrm{SELECT}(|01\rangle\langle 01|_a)(e^{i\pi})_0\mathrm{SELECT}(|m\rangle\langle m|)_r \quad (7.67)$$
$$C \coloneqq \mathrm{SELECT}(|10\rangle\langle 10|_a)Z_0\mathrm{SELECT}(|m\rangle\langle m|)_r\,. \quad (7.68)$$

We denote $O_{a/0/r}$ operations applied to the ancillary/ symplectic/ register qubit(s). We then apply the hermitian conjugate of the state preparation $U^\dagger$, and post-select those states where the ancillary qubits are measured to be the $|00\rangle$ state. Overall the transformation is $|00\rangle\langle 00|_a U_a^\dagger BCU_a\,|00\rangle\langle 00|_a$.

- **Displacement gate:** Displacement gates cannot be implemented as qubit gates on a single copy of the input states. Indeed displacement implies adding a number to an amplitude, whereas unitaries acting on a single copy of a state can only multiply amplitudes. While access to multiple copies could in principle be used to implement non-linear transformations [205], we do not consider this setting here.

Global bit-structured gates

In this section, we present a list of global bosonic gates that can be easily translated to qubit gates. In particular, the local interferometric gates map to global qubit gates composed of multi-qubit controlled operations. To mitigate this issue, we can combine local GB gates into global ones, such that their qubit counterparts require fewer multi-qubit controls. We will henceforth refer to the GB gates which effectively translate into local qubit operations as *global bit-structured Gaussian gates*.

- **Phase gate:** It is defined with a binary condition describing which modes the same local gate is applied to. It is given as pairs of indices and binary values. For example, $((1,1),(3,0))$ translates into the binary condition $m_1\overline{m_3}=1$, which means that the least significant bit should be 1 and the third bit should be 0. For 2^3 modes this implies that the rotation gates apply to modes $001=1$ and $011=3$. In the corresponding qubit gate, this bitstring condition directly translates into a SELECT on the register. We denote these gates as $P(((k_j,b_j))_j,t)$. Using the same notations as for the local gates, and using 0 as the index for the symplectic qubit, for the example $m_1\overline{m_3}=1$ we find

$$P(((1,1)(3,0)),t)\rightarrow \text{SELECT}\left(|1\rangle\langle 1|_1\,|0\rangle\langle 0|_3\right)R_y(4t)_0\,. \tag{7.69}$$

  The shorter the bitstring condition of the phase gate is, the more local the operation is in qubits (fewer controls in the SELECT) and the less local it is in the interferometer (more modes are acted upon non-trivially). In the case no bit condition is given, the same rotation gate is applied to all modes and therefore it is simply an R_y on the symplectic qubit.

- **Global Beamsplitter:** It is also defined with a binary condition describing which modes the same local gate is applied to. But as a beamsplitter is a two-mode gate, an additional index l is given to determine how the modes are paired. The l-th bit cannot be part of the bitstring condition. Each mode whose index satisfies the bitstring condition is paired with the one whose index has all bits in common but the l-th one.

  For example, the global bit-structured beamsplitter on 2^3 modes described by $((3,0))$, $l=1$ is applied to the second half of the modes ($\overline{m_3}=1$), pairing even modes $0m_20$ with odd modes $0m_21$. Therefore it pairs modes $(000,001)$ and $(010,011)$. We denote these gates as

$BS(((k_j, b_j))_j, l, t)$. The example gate may then be written as

$$BS(((3,0)),1,t) \to \mathrm{CTRL}\left(|0\rangle\langle 0|_3\right) R_y(4t)_1 \,. \tag{7.70}$$

Note that this particular example is of interest because it corresponds to the 0-controlled-R_y gate that is used extensively in the BQP-completeness proof.

- **Squeezing gate:** The modes to which the squeezing applies are also described as a bitstring condition. It is the same as for the rotation gates but with the squeezing apparatus on the ancillary register instead of the R_y on the symplectic qubit. We denote them as $S(((k_j, b_j))_j, r)$.

Notice that when the binary condition applies to all bits, then we retrieve one local gate from the previous section.

7.6.3. BQP-completeness

Here we provide proof that Problem 1 is BQP-complete. Let us first recall Definition 7.2 and Problem 7.4.

Definition 7.2 (Bit-structured interferometer)
A bit-structured interferometer acting on 2^n nodes consists of L global beamsplitters, such that each global beamsplitter acts on 2^{n-1} modes. A global beamsplitter is specified by two natural numbers, $k \neq l$, between 1 and n. The global beamsplitter then acts on all the modes with indices $\{m\}$ such that their k-th bit is equal to 0, by applying local beamsplitters between modes with indices m, m' that only differ in their l-th bit.

Problem 7.4
Consider a bit-structured interferometer (see Definition 7.2) acting on 2^n modes with $L \in \mathcal{O}(\mathrm{poly}(n))$, and an input state such that the first mode is displaced in position by a real constant x while the state of the remaining modes is the vacuum. Then, decide whether the expectation value of the position on the first mode at the output of the interferometer is

$$1.\, \langle \hat{q}_1 \rangle > \frac{2}{3}x \,, \qquad \text{or} \qquad 2.\, \langle \hat{q}_1 \rangle < \frac{1}{3}x \,,$$

given the promise that either one or the other is true.

We prove our main result by showing that Problem 7.4 reduces to a BQP-complete problem and vice-versa.

Theorem 7.2
Problem 7.4 is BQP-complete.

Proof. We recall the following problem, known to be BQP-complete.

Problem 7.5
Given a uniform family of quantum circuits on n qubits with $J \in \mathcal{O}(\mathrm{poly}(n))$ local gates $\{U_j\}_{1\leq j\leq J}$ taken from a universal gate set $\mathcal{S}$, which are applied to the state $|0\rangle^{\otimes n}$ to produce $|\psi\rangle = \prod_j U_j |0\rangle^{\otimes n}$, decide whether

1. *$|\psi\rangle$ has an overlap larger than 2/3 with $|0\rangle^{\otimes n}$, or*
2. *$|\psi\rangle$ has an overlap smaller than 1/3 with $|0\rangle^{\otimes n}$,*

given the promise that either one or the other is true.

Inclusion in BQP

First, we prove that Problem 7.4 is in BQP by showing that Problem 7.4 can be efficiently reduced to Problem 7.5. We are given access to an algorithm to solve Problem 7.5 and a bit-structured interferometer composed of polynomially many layers of global beamsplitters. The initial state in Problem 7.4 is a tensor product of coherent states such that $\langle \hat{q}_m \rangle = x\delta_{m=1}$ and $\langle \hat{p}_m \rangle = 0$. We consider a quantum circuit over $n+1$ qubits, composed of the symplectic qubit and the n register qubits, as explained in the main text. The initial coherent state then corresponds to an input state $(1, 0, \ldots, 0)^T = |0\rangle^{\otimes n+1}$ in the qubit picture.

We recall that a uniform family of quantum circuits is a set of circuits $\{C_n\}$ such that a classical Turing machine can produce a description of C_n on input n in time polynomial in n. In our case, the classical description of the beamsplitter gates is a pair of natural numbers smaller or equal than n for a problem of size n. As such, this description can be efficiently translated to a circuit description using the dictionary we provided in Section 7.6.2, as we know that a single layer of global beamsplitters can be mapped to a 0-controlled-R_y gate on the register (see Definition 7.2). Therefore, we can construct a uniform family of quantum circuits implementing the action in phase space of bit-structured interferometers over 2^n modes.

We use access to the solver of Problem 7.5 with the polynomial-size sequence of 0-controlled-R_y gates corresponding to the global beamsplitters to determine whether the output state has an overlap with $|0\rangle^{\otimes n+1}$ that is $> 2/3$ or $< 1/3$. This directly answers the question of whether the final coherent state has a position expectation value for the first mode

$> 2x/3$ or $< x/3$. We have therefore proved that Problem 7.4 reduces to Problem 7.5, implying that it is in BQP.

As a side note, in Section 7.6.2 we show that a broader class of particle-preserving gates can be simulated efficiently by a quantum computer. Indeed we have mapped each local and bit-structured global interferometric gate to a constant number of multi-controlled qubit gates. Each of the multi-controlled gates can be decomposed into $\mathcal{O}(n)$ two-qubit gates. Therefore any interferometer made of a polynomial number of local or bit-structured global gates over 2^n modes can be simulated efficiently by a polynomial-depth circuit acting on $(n+1)$ qubits.

BQP hardness

Second, we prove that Problem 7.4 is BQP-hard. To do so, we show that Problem 7.5 efficiently reduces to Problem 7.4. As for the inclusion proof, the reduction is based on the fact that the beamsplitters composing a bit-structured interferometer as in Definition 7.2 translate to 0-controlled-R_y rotations between all pairs of register qubits (as proven in Section 7.6.2). The key point for the hardness is that 0-controlled-R_y gates constitute a universal gate set for quantum computation, as stated in the following Lemma (which is a restatement of a result in [197]).

Lemma 7.1
The set of 0-controlled-$R_y(\theta)$ rotation gates with control qubit k and target qubit l, with $1 \leq k \neq l \leq n+2$ and $\theta \in [0, 2\pi]$, applied to the initial state $|0\rangle^{\otimes n+2}$, is universal for quantum computation on n qubits.

Proof. Let us suppose that we have an n-qubit quantum state

$$|\psi\rangle = \sum_{r=0}^{2^n-1} a_r e^{i\theta_r} |r\rangle \ , \tag{7.71}$$

where the a_r and θ_r are real numbers, together with the following universal gate set,

$$R_z(\tau) = \begin{pmatrix} e^{i\tau} & 0 \\ 0 & 1 \end{pmatrix} , \quad R_y(\tau) = \begin{pmatrix} \cos(\tau/2) & -\sin(\tau/2) \\ \sin(\tau/2) & \cos(\tau/2) \end{pmatrix} , \tag{7.72}$$

$$F\left(\frac{\pi}{2}\right) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} , \tag{7.73}$$

where our $R_z(\tau)$ is equivalent to the standard one, as they only differ by a global phase and a relabeling $\tau \to -\tau$. Moreover, our $F(\pi/2)$ gate can be readily mapped to that in the universal set from Ref. [197], by using single-qubit X gates. Since $R_z(\tau)$ and $R_y(\tau)$ can generate any single-qubit gate, both gate sets are equivalent and hence universal.

Let us furthermore suppose that we have an $(n+1)$-qubit quantum state with real amplitudes,

$$|\phi\rangle = \sum_{r=0}^{2^n-1} a_r \cos\theta_r |r\rangle |0\rangle + a_r \sin\theta_r |r\rangle |1\rangle \ . \tag{7.74}$$

Clearly, the states in Equation (7.71) and Equation (7.74) contain the same information. We refer to the extra qubit in $|\phi\rangle$ as the ancilla. The action of the universal gates as in Equation (7.72) on $|\psi\rangle$, such that $|\psi\rangle \to |\psi'\rangle$, will then induce an action $|\phi\rangle \to |\phi'\rangle$. We need to show that this induced action can be efficiently implemented using controlled-R_y rotations that act non-trivially when the control qubit is in the $|0\rangle$ state.

We begin with the R_z gate, whose action on a single-qubit state is

$$R_z(r_0 e^{i\theta_0} |0\rangle + r_1 e^{i\theta_1} |1\rangle) = r_0 e^{i(\theta_0+\tau)} |0\rangle + r_1 e^{i\theta_1} |1\rangle \ . \tag{7.75}$$

The induced evolution is

$$\begin{gathered} r_0 \cos\theta_0 |0\rangle |0\rangle + r_0 \sin\theta_0 |0\rangle |1\rangle + r_1 \cos\theta_1 |1\rangle |0\rangle + r_1 \sin\theta_1 |1\rangle |1\rangle \\ \downarrow \\ r_0 \cos(\theta_0+\tau) |0\rangle |0\rangle + r_0 \sin(\theta_0+\tau) |0\rangle |1\rangle + r_1 \cos\theta_1 |1\rangle |0\rangle + r_1 \sin\theta_1 |1\rangle |1\rangle \ . \end{gathered} \tag{7.76}$$

This can be achieved by performing a 0-controlled-$R_y(\tau)$ gate where the control is the first qubit (i.e., the qubit on which $R_z(\tau)$ would act) and the target is the ancilla.

Next, let us look at the action of $R_y(\tau)$. To implement this gate, we simply need an additional auxiliary qubit in the $|0\rangle$ state and to apply a 0-controlled-R_y gate conditioned on this extra qubit.

Finally, we have the $F\left(\frac{\pi}{2}\right)$ gate, whose action on a two-qubit state is given by

$$\begin{gathered} r_0 e^{i\theta_0} |00\rangle + r_1 e^{i\theta_1} |01\rangle + r_2 e^{i\theta_2} |10\rangle + r_3 e^{i\theta_3} |11\rangle \\ \downarrow \\ r_1 e^{i\theta_1} |00\rangle - r_0 e^{i\theta_0} |01\rangle + r_2 e^{i\theta_2} |10\rangle + r_3 e^{i\theta_3} |11\rangle \ . \end{gathered} \tag{7.77}$$

The corresponding induced action is

$$\begin{aligned}
&r_0\cos\theta_0\,|000\rangle + r_0\sin\theta_0\,|001\rangle + r_1\cos\theta_1\,|010\rangle + r_1\sin\theta_1\,|011\rangle + \\
&r_2\cos\theta_2\,|100\rangle + r_2\sin\theta_2\,|101\rangle + r_3\cos\theta_3\,|110\rangle + r_3\sin\theta_3\,|111\rangle \\
&\qquad\qquad\qquad\qquad\downarrow \\
&r_1\cos\theta_1\,|000\rangle + r_1\sin\theta_1\,|001\rangle - r_0\cos\theta_0\,|010\rangle - r_0\sin\theta_0\,|011\rangle + \\
&r_2\cos\theta_2\,|100\rangle + r_2\sin\theta_2\,|101\rangle + r_3\cos\theta_3\,|110\rangle + r_3\sin\theta_3\,|111\rangle\ . \qquad (7.78)
\end{aligned}$$

The previous can be achieved by simply applying a 0-controlled-$R_y(\pi)$ in the first two qubits (i.e. the ancilla is not necessary). Therefore, we conclude that the set of 0 is universal for quantum computation, given the initial state $|0\rangle^{\otimes n+2}$. □

We are given a circuit composed of a polynomial number of 0-controlled-R_y gates. We are also given access to a solver for Problem 7.4. We add a qubit on top of the given circuit which is acted trivially upon, and consider it as the symplectic qubit. We query the given solver with the sequence of global bit-structured beamsplitters corresponding to the sequence of 0-controlled-R_y gates as input. Similarly to the inclusion proof, because the input state is the all-zero state, the reduction directly follows. We conclude that Problem 7.4 is BQP-complete. □

7.6.4. From unitary quantum circuits to interferometers

Separating real and imaginary parts of the amplitudes of a quantum state

Consider a unitary quantum circuit on n qubits. Such a circuit is applied to a complex state on n qubits of the following form

$$|\psi\rangle = \sum_{r=0}^{2^n-1} (a_r + b_r i)\,|r\rangle\ . \qquad (7.79)$$

Adding one qubit (as the left-most in the tensor product) which we call the symplectic qubit for reasons that will become clear later, we can define the real-valued state over $n+1$ qubits.

$$|\phi\rangle = \sum_{r=0}^{2^n-1} a_r\,|0\rangle\,|r\rangle + b_r\,|1\rangle\,|r\rangle\ . \qquad (7.80)$$

First, we recall that a set of universal one-qubit gates, together with any entangling gate forms a universal set. We can use Rz and Ry gates to generate any Rx gate we wish, and thus Rz and Ry form a universal gate set for unitaries. Therefore together with CRy, they form a universal gate set for unitaries on n qubits. This yields the following lemma.

Lemma 7.2
The set of gates $\{Rz, Ry, CRy\}$ is universal.

We are going to prove that this universal set of gates $\{Ry, Rz, CRy\}$ for unitary circuits can be translated to a specific set of orthogonal gates on $n+1$ qubits. It is easy to see that for any real gate, such as Ry, the gate is simply applied to the register.

$$Ry(\tau) = \begin{pmatrix} \cos(\tau/2) & -\sin(\tau/2) \\ \sin(\tau/2) & \cos(\tau/2) \end{pmatrix} \rightarrow$$
$$I \otimes Ry(\tau/2) = \begin{pmatrix} \cos(\tau/2) & -\sin(\tau/2) & 0 & 0 \\ \sin(\tau/2) & \cos(\tau/2) & 0 & 0 \\ 0 & 0 & \cos(\tau/2) & -\sin(\tau/2) \\ 0 & 0 & \sin(\tau/2) & \cos(\tau/2) \end{pmatrix}$$
$$= \exp(-i\tau I \otimes Y/2). \quad (7.81)$$

This is also true for controlled-Ry, which yields the same controlled-Ry on the register

$$C_k Ry_l(\tau/2) \rightarrow I \otimes C_k Ry_l(\tau/2) = \exp(-i\tau I \otimes |1\rangle\langle 1|_k Y_l/2). \quad (7.82)$$

For complex gates, the symplectic qubit is involved in the corresponding orthogonal gate. We show a derivation for Rz below,

$$Rz(\tau/2)\,|a+ic, b+id\rangle = \begin{pmatrix} 1 & 0 \\ 0 & \cos(\tau/2) + i\sin(\tau/2) \end{pmatrix} \begin{pmatrix} a+ic \\ b+id \end{pmatrix} =$$
$$\begin{pmatrix} a+ic \\ (\cos(\tau/2)b + \sin(\tau/2)d) + i(-\cos(\tau/2)d + \sin(\tau/2)b) \end{pmatrix}. \quad (7.83)$$

Finally we conclude that $Rz(\tau/2) \rightarrow C_1 RY_0(\tau/2) = \exp(-i\tau Y \otimes |k\rangle\langle k|\,/2)$

$$C_1 RY_0(\tau/2)\,|a,b,c,d\rangle \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(\tau/2) & 0 & -\sin(\tau/2) \\ 0 & 0 & 1 & 0 \\ 0 & \sin(\tau/2) & 0 & \cos(\tau/2) \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}. \quad (7.84)$$

We take note that for all of the gates in a universal set, we have derived an orthogonal gate that belongs to the unitary symplectic algebra as in Section 7.6.1, with the generators of $I \otimes Ry \in \{iI \otimes P_a\}$, those of $I \otimes CRy \in \{iI \otimes P_a\}$ and those of $Rz \to C_k Ry_0 \in \{iY \otimes P_s\}$.

Unitary gates to global bit-structured interferometric gates

We now show that each of the gates derived in the previous section maps in turn to a global bit-structured interferometric gate, as follows.

- An Rz gate on qubit k gate is mapped to a $C_k Ry_0$ gate in the symplectic picture. Its corresponding GB gate is the phase gate on half of the modes, whose k-th bit of the index is 1. Using notation from Section 7.6.2 it is $\mathrm{P}((k,1))$.

- An Ry gate on qubit k gate is mapped to a Ry_k gate in the symplectic picture. Its corresponding GB gate is the beamsplitter where all modes are paired such that their index differs only by their k-th qubit. Using notation from Section 7.6.2 it is $\mathrm{BS}(\varnothing, k)$.

- A CRy gate controlled on qubit l and target on qubit k gate is mapped to a $C_l Ry_k$ gate in the symplectic picture. Its corresponding GB gate is the beamsplitter where all the modes whose l-th bit of the index is 1 are paired such that their indices only differ by their k-th qubit. Using notation from Section 7.6.2 it is $\mathrm{BS}((l,1),k)$.

We summarize the previous equivalences in the below table.

Unitary gate	Symplectic gate	GB gate
Rz_k	$C_k Ry_0$	$\mathrm{P}((k,1))$
Ry_k	$I \otimes Ry_k$	$\mathrm{BS}(\varnothing, k)$
$C_l Ry_k$	$I \otimes C_l Ry_k$	$\mathrm{BS}((l,1),k)$

Table 7.1.: Mapping between unitary, symplectic and bosonic gates.

From unitary circuits to interferometers

In this subsection, we show how a unitary qubit computation can be mapped to the evolution by an interferometer of the first moments of expectation values of quadrature operators of coherent states over exponentially many modes.

Gates. Based on the derivations above, given a unitary on n qubits composed of L gates from the universal set $\{Rz, Ry, CRy\}$, we can map it to an equivalent interferometer on 2^n modes composed of exactly L global bit-structured interferometric gates (global bit-structured beamsplitters and global bit-structured phase gates). In that picture, the k-th mode tracks the amplitude of the qubit state on the computational-basis state $|m\rangle$ with the position as the real part and the momentum as the imaginary part.

State preparation. To prepare a sparse qubit state, we start from the vacuum, and each non-zero entry $a + ib$ is position displaced by a and momentum displaced by b for the corresponding mode. Note we have a degree of freedom to upload a state $|\psi\rangle$ onto our modes up to a multiplicative coefficient. For example the state $((1+i)|0\rangle - \sqrt{2}|1\rangle)/2$ can be prepared as $q_0 = 1, p_0 = 1, q_1 = \sqrt{2}$ but also as $q_0 = 10, p_0 = 10, q_1 = 10\sqrt{2}$. We use the expectation value of the sum of the number operator for each mode $\langle \hat{n}_m \rangle = \frac{1}{2}\langle \sum_m \hat{q}_m^2 + \hat{p}_m^2 \rangle$ to characterize this degree of freedom when encoding qubit states into bosonic states. This expectation value also corresponds to the number of photons $P = \sum_m \langle \hat{n}_m \rangle$ in the circuit. We recall that coherent states are eigenstates of the annihilation operator $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$, therefore $\langle \hat{n} \rangle = \langle \hat{a}^\dagger \hat{a} \rangle = |\alpha|^2 = \frac{1}{2}\left(\langle \hat{q} \rangle^2 + \langle \hat{p} \rangle^2\right)$.

Measurements. We consider the photon counting measurement and show that it corresponds to sampling bitstrings from the qubit circuit. The probability of detecting p photons on the m-th mode is a Poissonian distribution $\Pr(p) = \exp(-e_m)e_m^p/p!$ with an average equal to the energy of the mode $e_m = \langle \hat{n}_m \rangle$. We recall that the Poissonian distribution expresses the probability of a given number of events occurring when these events occur independently at a known constant mean rate, which is in that case e_m. Therefore considering that a number of photons $P = \sum_m \langle \hat{n}_m \rangle$ has been injected at the beginning of the interferometer we should get P photons at the output, distributed according to a compound Poissonian distribution where each mode has a rate of occurrence e_m. Effectively we are getting P bitstring samples according to the distribution $[e_0, e_1, \cdots, e_m]$. Recalling that $e_m = \frac{1}{2}\left(\langle \hat{q} \rangle^2 + \langle \hat{p} \rangle^2\right)$, which is effectively proportional to the probability of sampling the bitstring m at the output of the qubit circuit. The more energy injected at the beginning of the circuit the more samples we get.

Now we consider homodyne detection which measures in the basis of $\hat{p}$, $\hat{q}$ or any combination of the two $\hat{x} = \cos\theta\hat{q} + \sin\theta\hat{p}$. This yields a Gaussian distribution centered around $\langle \hat{x} \rangle$, and for coherent states, with variance 1/2. Effectively this is equivalent to doing a Hadamard test to access either the real part or the imaginary part of the amplitude of a state on the

computational basis, which is affected by shot noise. Increasing the energy at the input of the interferometers increases the precision with which we can measure the real and imaginary parts of the amplitude on $|m\rangle$.

7.6.5. Imaginary time evolution is QMA-hard

Reduction

Finding the ground energy of a Hamiltonian is crucial in areas like quantum chemistry and condensed matter physics. This information is often key for understanding quantum phase transitions, chemical reactions or material properties. It can be formulated as a decision problem which is the essence of the class QMA. We recall the QMA-complete ground energy problem below [206].

Problem 7.6
Given a Hamiltonian $H = \sum_{r=1}^{R} H_r$, with $R \in O(\text{poly}(n))$, and each term H_r k-local, whose norm $\|H\| \in O(\text{poly}(n))$, and two real numbers $a < b$ with $b - a \in \Omega(\text{poly}(n)^{-1})$, decide whether the ground state energy λ_0 is

1. *$\lambda_0 > b$ or*

2. *$\lambda_0 < a$*

given that either one is true.

In this appendix, we prove that the ground energy problem, Problem 7.6, can be efficiently reduced to imaginary time evolution, Problem 7.3.

Given a Hamiltonian H on n qubits, a time β and an input state $|x\rangle$, we derive the expectation value of H of the state prepared by the imaginary time evolution. In particular, we are trying to upper bound such a value based on the value of the ground energy λ_0. Then we provide a lower bound on β such that if λ_0 is smaller than a value a with high probability when $|x\rangle$ is taken randomly from a 2-design for each round, which is equivalent to the maximally mixed state

First, we write the eigendecomposition of the Hamiltonian as $H = \sum_k \lambda_k |k\rangle\langle k|$ with λ_0 the ground energy. We also write our input state as $\rho = I/2^n$. The result of the normalised imaginary time evolution is:

$$\rho \to \frac{\sum_k e^{-2\beta\lambda_k} |k\rangle\langle k|}{\sum_k e^{-2\beta\lambda_k}}. \tag{7.85}$$

The expectation value of such a state is as follows.

$$\langle H\rangle = \frac{\sum_k \lambda_k e^{-2\beta\lambda_k}}{\sum_k e^{-2\beta\lambda_k}} = \frac{\lambda_0 + \sum_{k>0} \lambda_k e^{-2\beta(\lambda_k-\lambda_0)}}{1+\sum_{k>0} e^{-2\beta(\lambda_k-\lambda_0)}}\,. \tag{7.86}$$

As β grows bigger the term vanishing the least fast in the sum will be the smallest $\lambda_k - \lambda_0$. In the worst case the first excited state is fully degenerate and we have $\lambda_k = \lambda_1, \forall k \geq 1$. Writing the following quantity $A \coloneqq 2^n - 1$, this yields :

$$\langle H\rangle \leq \frac{\lambda_0 + A\lambda_1 e^{-2\beta(\lambda_1-\lambda_0)}}{1+Ae^{-2\beta(\lambda_1-\lambda_0)}}\,. \tag{7.87}$$

We want to upper bound that quantity for any λ_1, so we consider the function $\lambda_1 \to \frac{\lambda_0+A\lambda_1 e^{-2\beta(\lambda_1-\lambda_0)}}{1+Ae^{-2\beta(\lambda_1-\lambda_0)}}$, its derivative with respect to λ_1 is proportional (positively) to

$$\begin{aligned}
&A(-2\beta\lambda_1+1)e^{-2\beta(\lambda_1-\lambda_0)}\left(1+Ae^{-2\beta(\lambda_1-\lambda_0)}\right)\\
&-\left(\lambda_0+A\lambda_1 e^{-2\beta(\lambda_1-\lambda_0)}\right)\left(-2\beta Ae^{-2\beta(\lambda_1-\lambda_0)}\right)\\
&= Ae^{-2\beta(\lambda_1-\lambda_0)}\left((-2\beta\lambda_1+1)\left(1+Ae^{-2\beta(\lambda_1-\lambda_0)}\right)\right.\\
&\left.-(\lambda_0+A\lambda_1)\left(e^{-2\beta(\lambda_1-\lambda_0)}\right)(-2\beta)\right)\\
&= Ae^{-2\beta(\lambda_1-\lambda_0)}\left(Ae^{-2\beta(\lambda_1-\lambda_0)}+1-2\beta(\lambda_1-\lambda_0)\right)\,.
\end{aligned} \tag{7.88}$$

The maximum is reached when $2\beta(\lambda_1-\lambda_0) \geq 0$ is equal to the value that solves $Ae^{-x}+1-x=0$, that is $x = 1+W(A/e)$ where W is the Lambert W function (this follows from the identity $W(x)e^{W(x)} = x$). The maximum is then

$$\frac{\lambda_0 + A\lambda_1 e^{-2\beta(\lambda_1-\lambda_0)}}{1+Ae^{-2\beta(\lambda_1-\lambda_0)}} = \frac{\lambda_0+\lambda_1(2\beta(\lambda_1-\lambda_0)-1)}{1+2\beta(\lambda_1-\lambda_0)-1} = \lambda_1 - \frac{1}{2\beta}\,. \tag{7.89}$$

We know that the solution that the Lambert function is such that $\ln(X) - \ln(\ln(x)) \leq W(x) \leq \ln(x)$ in the limit of large x. Therefore we have

$$2\beta(\lambda_1-\lambda_0) = 1+W(A/e) \leq 1+\ln A/e\,, \tag{7.90}$$

$$\lambda_1 \leq \frac{1+\ln A/e}{2\beta} + \lambda_0\,. \tag{7.91}$$

Finally we get

$$\langle H \rangle \leq \frac{\ln A/e}{2\beta} + \lambda_0 \,. \tag{7.92}$$

We suppose we can estimate $\langle H \rangle$ as $\hat{h}$ up to an error ε such that with high probability $\hat{h} \geq \langle H \rangle - \varepsilon$. For reasons that will become clear, we choose $\varepsilon = (1-\alpha)(b-a)$ for any constant $0 < \alpha < 1$. Therefore $\varepsilon \in \text{poly}(n)^{-1}$, and for a polynomial error the estimation of the expectation values of H such that $\|H\| \in \text{poly}(n)$ can be done with quantum phase estimation or direct measurements using a polynomial number of calls to the state preparation algorithm. We are looking to find conditions for $\hat{h}$ to be smaller than b when the input state is the maximally mixed state. In order to have $\langle H \rangle \leq b - \varepsilon$, it is sufficient to have

$$\frac{\ln 2^n/e}{2\beta} + a \leq b - \varepsilon \tag{7.93}$$

$$\beta \geq \frac{n\ln(2) - 1}{b - a - \varepsilon} = \frac{n\ln(2) - 1}{\alpha(b-a)} \tag{7.94}$$

Therefore for any Hamiltonian H choosing β as prescribed above we are guaranteed with high probability that given that the ground state energy of H is smaller than a, the H expectation value of the maximall mixed state that has been imaginary time evolved by H is smaller than b. The end-to-end reduction goes as follows: we prepare a state $|x\rangle$ sampled from a 2-design using a polynomial quantum circuit, and we call the solver for imaginary time evolution with parameters $(|x\rangle, H, \beta)$ and repeat that the number of times necessary to estimate the H expectation value (QPE or direct measurements) of such a state up to error ε as prescribed above. This number of iterations is polynomial, as the spectral norm of the Hamiltonian is polynomial and the error is inverse polynomial. If the estimated value is greater than b we decide we are in the no case of Problem 7.6 and otherwise we decide yes. With high probability this is a successful protocol. In addition because the gap is inverse polynomial, we know that $\beta \in \Theta(\text{poly}(n))$. This concludes the reduction from the ground energy problem to imaginary time evolution.

In addition, one can see that this sufficient condition on β for imaginary time evolution to be able to resolve a QMA-complete problem, also becomes necessary for a specific Hamiltonian. Consider a Hamiltonian with the following spectrum: one ground energy λ_0, and a first excited state with energy λ_1 with $2^n - 1$ degeneracy, with λ_1 corresponding to the value that

maximizes the right hand side of Equation (7.87) for the optimal β.

Mixed time evolutions

Similarly, given a Hamiltonian H on n qubits, a time β and an input state $|x\rangle$, we derive the expectation value of H of the state prepared by mixed time evolution for a time β. In particular, we are trying to upper bound such a value based on the value of the ground energy λ_0. Then we will derive probabilities of such a value to be smaller than a value a when $|x\rangle$ is taken Haar random and the expectation is estimated up to ε error.

First, we write the eigendecomposition of the Hamiltonian as $H = \sum_k \lambda_k |k\rangle\langle k|$ with λ_0 the ground energy. We consider that we add arbitrary oscillatory terms to such a Hamiltonian,

$$A \coloneqq \sum_k (\lambda_k + i\omega_k) |k\rangle\langle k| \ . \tag{7.95}$$

The result of the normalised time evolution of the maximally mixed state with A is:

$$\frac{\sum_k e^{-\beta\lambda_k} e^{-i\beta\omega_k} |k\rangle\langle k| e^{-\beta\lambda_k} e^{+i\beta\omega_k}}{\sum_k e^{-2\beta\lambda_k}} \ . \tag{7.96}$$

It is easy to see that the complex parts cancel out and that, the expectation value of such a state is as follows,

$$\langle H \rangle = \frac{\sum_k \lambda_k e^{-2\beta\lambda_k}}{\sum_k e^{-2\beta\lambda_k}} \ . \tag{7.97}$$

Which corresponds exactly to the purely imaginary time evolution case. The whole proof follows unchanged, showing that the addition of oscillatory terms doesn't affect the power of the imaginary time evolution.

7.6.6. Exponentially large interferometers equipped with squeezing gates are PostBQP-hard

In Section 7.4.2 we have seen that the imaginary time evolution of $Z \otimes I$ for times $\beta \in \Theta(\text{poly}(n))$ yields the power to perform post-selection. Suppose we are given an real unitary (i.e. orthogonal) U and $\varepsilon = e^{-q(n)}$ with q a polynomial, such that:

$$U |0\rangle = |\phi\rangle = \sqrt{\varepsilon} |0\rangle |\phi_0\rangle + \sqrt{1-\varepsilon} |1\rangle |\phi_1\rangle \ . \tag{7.98}$$

The task is to post-select on the first register qubit to be $|0\rangle$, which has an exponentially small probability ε of occurring. We use the mapping in Section 7.6.3 to have an interferometer preparing the GB state such that:

$$\langle \hat{q}_{2k} \rangle = \sqrt{\varepsilon} \langle k \mid \phi_0 \rangle \tag{7.99}$$

$$\langle \hat{q}_{2k+1} \rangle = \sqrt{1-\varepsilon} \langle k \mid \phi_1 \rangle \tag{7.100}$$

$$\langle \hat{p}_k \rangle = 0\,. \tag{7.101}$$

Applying a squeezing to all even modes for squeezing parameter β yields the following state,

$$\langle \hat{q}_{2k} \rangle = e^{\beta} \sqrt{\varepsilon} \langle k \mid \phi_0 \rangle \tag{7.102}$$

$$\langle \hat{q}_{2k+1} \rangle = \sqrt{1-\varepsilon} \langle k \mid \phi_1 \rangle \tag{7.103}$$

$$\langle \hat{p}_k \rangle = 0\,. \tag{7.104}$$

Which effectively yields the power of post-selection following arguments from Section 7.4.2.

Definition 7.3 (bit-structured Gaussian Circuit)
This is the family of circuits composed of any circuit as defined in Definition 7.2, followed by a layer of squeezing gates applied to every other mode with squeezing parameter β.

We define the following problem.

Problem 7.7
Consider a bit-structured Gaussian Circuit (see Definition 7.3) acting on 2^n modes with $L \in \mathcal{O}(\mathrm{poly}(n))$ and $\beta \in poly(n)$, and an input state such that the first mode is displaced in position by a real constant x while the state of the remaining modes is the vacuum. Then, decide whether the expectation value of the position on the first mode at the output of the interferometer is

$$1.\, \langle \hat{q}_1 \rangle > \frac{2}{3} x\,, \qquad \text{or} \qquad 2.\, \langle \hat{q}_1 \rangle < \frac{1}{3} x\,,$$

given the promise that either one or the other is true.

And from the previous, we find that the following theorem holds.

Theorem 7.3
Problem 7.7 is Post-BQP-hard.