

Efficient Quantum Hermite Transform

Siddhartha Jain^{1,2,*}, Vishnu Iyer^{2,*}, Rolando D. Somma¹, Ning Bao^{3,4}, and Stephen Jordan¹

¹Google Quantum AI, Venice, CA 90291, United States

²The University of Texas at Austin, Austin, TX 78712, United States

³Northeastern University, Boston, MA 02115, United States

⁴Brookhaven National Laboratory, Upton, NY 11973, United States

*These authors contributed equally to this work.

Abstract

We present a new primitive for quantum algorithms that implements a discrete Hermite transform efficiently, in time that depends logarithmically in both the dimension and the inverse of the allowable error. This transform, which maps basis states to states whose amplitudes are proportional to the Hermite functions, can be interpreted as the Gaussian analogue of the Fourier transform. Our algorithm is based on a method to exponentially fast forward the evolution of the quantum harmonic oscillator, which significantly improves over prior art. We apply this Hermite transform to give examples of provable quantum query advantage in property testing and learning. In particular, we show how to efficiently test the property of being close to a low-degree in the Hermite basis when inputs are sampled from the Gaussian distribution, and how to solve a Gaussian analogue of the Goldreich-Levin learning task efficiently. We also comment on other potential uses of this transform to simulating time dynamics of quantum systems in the continuum.

Contents

1	Introduction	3
1.1	Problem statement	4
1.2	Summary of results	5
2	Technical overview	6
3	Fast-forwarding of the QHO	9
3.1	The algorithm	12
3.2	Bounding nested commutators	13
4	Quantum Hermite transform	21
4.1	State preparation	21
4.2	The algorithm	33
5	Hermite sampling	34
5.1	Boolean-output functions	35
5.2	General functions	39
5.3	Property testing	44
5.4	Agnostic learning of sparse concepts	47
6	Open problems and outlook	48
A	Factorization of the QHO evolution operator	48
B	Centered discrete Fourier transform	51
C	Some properties of the Plancherel-Rotach asymptotics	51
D	Gaussian Goldreich-Levin	52

1 Introduction

Hermite polynomials and their corresponding Hermite functions are central in physics, signal analysis, statistics, and beyond. For example, Hermite functions are the well-known eigenfunctions of one of the fundamental models in quantum mechanics known as the quantum harmonic oscillator (QHO) [GS18]. Hermite functions can also be used to approximate arbitrary functions or probability distributions, since they form an orthonormal basis of functions weighted by a Gaussian envelope (cf. [BM98]). Therefore, an efficient Hermite transform that performs a change of basis to the Hermite functions would provide a fundamental tool to quickly switch into the “natural” basis of many quantum systems and functions. Moreover, the number of primitives from which most quantum algorithms are constructed, such as the quantum Fourier transform (QFT) and amplitude amplification, is relatively limited [NC00]. This scarcity restricts the range of problems for which quantum algorithms offer speedups, thereby motivating the search of other novel quantum primitives. Given that the QFT represents a quantization of a pre-existing classical numerical transform, it is logical to attempt to quantize other classical transforms, such as the Hermite transform [LRP⁺08], and to consider its applications in quantum computing.

This work is concerned with a quantum Hermite transform (QHT): constructing a quantum circuit that maps basis states into ‘Hermite’ states. These Hermite states are superposition states with amplitudes given by the Hermite functions. While formally a Hermite transform would be defined in the continuum (i.e., a mapping $L^2(\mathbb{R}) \rightarrow L^2(\mathbb{R})$), we consider a discrete and finite-dimensional version that can be implemented by a quantum circuit.

For a QHT to be useful and provide quantum advantage, we require it to be efficient and hence implemented using a quantum circuit of complexity that is logarithmic in the dimension of the Hilbert space on which it acts. It is also desirable to achieve complexity scaling polylogarithmically in the inverse of the allowable error. Remarkably, we are able to achieve this: our main result is a quantum circuit U of $\mathcal{O}((\log N + \log 1/\varepsilon)^3 \times \log(1/\varepsilon))$ gates that performs the desired basis change into the Hermite states labeled by $n \in \{0, \dots, N\}$ to within additive error ε . Note that a classical discrete Hermite transform would require time polynomial in N to be implemented. Our result is then comparable to the QFT, in that the QFT also transforms into another ‘natural’ basis given by Fourier states, in time logarithmic in N .

Throughout this manuscript, we primarily consider the one-dimensional Hermite transform, acting on an N -dimensional Hilbert space. That is, we consider the position basis on a line, discretized as a one-dimensional lattice of N points, and convert to the Hermite functions of degree zero to $N - 1$, which are also interpretable as the N lowest-energy eigenstates of the quantum Harmonic oscillator. In some contexts, particularly property testing of oracles, it is also useful to apply the n -dimensional Hermite transform. This is the n -fold tensor power of the one-dimensional Hermite transform, much as the n -dimensional Fourier transform is the n -fold tensor power of the one-dimensional Fourier transform.

The existence of an efficient QHT is also a fundamental algorithmic question in Harmonic analysis, since it allows one to perform Hermite sampling. That is, given a quantum state $\sum_{\vec{x}} f(\vec{x}) |\vec{x}\rangle$ for some function $f : \mathbb{R}^n \rightarrow \mathbb{R}$, one can use the (n -dimensional) QHT to sample from the probability distribution $\Pr(\vec{k}) = |\hat{f}(\vec{k})|^2$, where $\hat{f}(\vec{k})$ is the coefficient of the Hermite polynomial with index \vec{k} in the expansion. In the finite field setting of QFT, the analogous Fourier sampling subroutine features in many of the most prominent quantum algorithms [Sim97, Sho97, Reg09, Aar10, RT22, YZ24, JSW⁺25]. Using the QHT we expect that one can design continuous analogues of problems with quantum query advantage like Forrelation [AA18, Wu20]. We also expect QHT to be useful for learning geometric concepts over the Gaussian distribution [KOS08], and simulating nonlinear differential equations with Gaussian noise which we can be done by projecting onto low-degree Her-

mite polynomials [BMSZZ25]. A recent work of Marwaha et al. [MFGH25] also showed that the recent DQI algorithm [JSW⁺25] can be thought of as performing a *Kravchuk* transform, which is a particular discretization of the Hermite transform. While closely related, we do not believe our work easily gives an efficient Kravchuk transform, which would scale logarithmically in the degree.

1.1 Problem statement

In the continuum, a Hermite transform is a basis transformation that maps into the Hermite functions defined as

$$\psi_n(x) := \frac{(-1)^n}{\sqrt{2^n n! \sqrt{\pi}}} e^{-x^2/2} H_n(x), \quad (1)$$

where $H_n(x)$ is the n^{th} Hermite polynomial¹. The goal of a QHT is then to construct a quantum circuit that performs a similar basis transformation but in a discrete, finite dimensional space. To this end, we introduce the Hermite states

$$|\psi_n\rangle := \left(\frac{2\pi}{M}\right)^{1/4} \sum_{j=-M/2}^{M/2-1} \psi_n(x_j) |j\rangle \in \mathbb{C}^M, \quad (2)$$

where $x_j := j\sqrt{2\pi/M}$ and $M = 2^m$ is the dimension. These can be interpreted as discretizations of the Hermite functions, where the discretization size is $\sqrt{2\pi/M}$. We labeled the M basis states of \mathbb{C}^M from $-M/2$ to $M/2 - 1$ for convenience. Note that the above states both discretize and truncate the Hermite functions. The above choice of lattice spacing ensures that the truncation only cuts off a region in which the first M Hermite functions all have exponentially decaying tails.

The problem of a QHT is to find a quantum circuit that maps $|n\rangle \mapsto |\psi_n\rangle$. By taking the gate-by-gate inverse one also obtains a quantum circuit for the inverse quantum Hermite transform, of the same complexity.

Quantum Hermite Transform Problem. Let $N > 0$ be the dimension and $\varepsilon > 0$ the error. The goal of a QHT is to construct a quantum circuit U that performs the map

$$\sum_{n=0}^{N-1} \alpha_n |n\rangle \mapsto \sum_{n=0}^{N-1} \alpha_n |\psi_n\rangle \quad (3)$$

within additive error ε , where $\alpha_n \in \mathbb{C}$ are arbitrary and satisfy $\sum_{n=0}^N |\alpha_n|^2 = 1$. The quantum circuit acts on a Hilbert space of dimension $M \geq N$.

In principle, such transformations cannot be exactly unitary since the states $|\psi_n\rangle$ are not exactly orthonormal. However, for sufficiently large $M = \Omega(N)$, they can be shown to be almost orthonormal within error that is exponentially small in M , due to [Som16]. Hence, by fixing the error ε and the dimension N where the QHT occurs, we can choose M properly and satisfy (3) within the precision requirements. For our specific construction, we will require $M = \text{poly}(N, 1/\varepsilon)$.

¹There are two widely used normalizations for the Hermite polynomials: the physicist's Hermite polynomials and the probabilist's Hermite polynomials. We use the physicist's normalization throughout.

1.2 Summary of results

Our QHT relies on a novel result to fast-forward the evolution of the QHO. In this context, a bounded Hamiltonian H is said to be fast-forwardable if one can construct a quantum circuit W that approximates the time-evolution operator e^{-iHt} for time t as $\|W - e^{-iHt}\| \leq \varepsilon$, using a number of quantum gates that scales sublinearly in $\|H\|t$ [AA17, GSS21]. Such result would bypass a number of no-fast-forwarding theorems that show that this is not always possible [BACS07, CK10, AA17, HHKL21]. However, the lower bound $\Omega(\|H\|t)$ applies only to the worst case and, in contrast, quantum systems like the QHO can indeed be fast-forwarded. In the continuum, the QHO models a particle in a quadratic potential with Hamiltonian $\hat{H} = (\hat{x}^2 + \hat{p}^2)/2$, where \hat{x} is the position operator and \hat{p} is the momentum operator. We introduce a discretized, M -dimensional version of the QHO with Hamiltonian \bar{H} , and show the following.

Theorem 1 (Exponential fast-forwarding of the QHO). *Let N be the target dimension for fast-forwarding, $\bar{H} \in \mathbb{C}^{M \times M}$ be the Hamiltonian of a discrete QHO, and $t \in [-\pi, \pi]$. Then, we can choose $M = \Theta(N \log N)$ such that the evolution operator $e^{-i\bar{H}t}$ can be simulated within error $\mathcal{O}(\exp(-N/10))$ in the subspace spanned by the first N eigenvectors of \bar{H} using $\mathcal{O}(\log^2 N)$ gates.*

Note that we don't lose any generality due to the condition $t \in [-\pi, \pi]$ since the eigenvalues of the Harmonic oscillator are of the form $n+1/2$ with integer n , and hence $e^{-iH(t+2\pi)} = -e^{-iHt}$. Since $\|\bar{H}\| = \Theta(M)$ and $N = \text{poly}(M)$, Theorem 1 shows that exponential fast-forwarding of the QHO is possible. This result significantly improves over prior art [Som16], where a quantum algorithm for simulating $e^{-i\bar{H}t}$ of complexity $\sim \exp(\sqrt{\log N})$ was given, only describing a form of subexponential fast-forwarding. Theorem 1 is based on a succinct factorization of the evolution operator in the continuum that can be extended to the evolution operator in the finite-dimensional case, and contrasts the method in [Som16] based on product (Trotter-Suzuki) formulas. The complexity in Theorem 1 is dominated by that of multiplication using coherent arithmetic, which is $\mathcal{O}(\log^2 N)$ using schoolbook multiplication, and might be improved using sophisticated techniques.

The ability to fast forward a Hamiltonian also allows one to perform tasks like quantum phase estimation (QPE) more efficiently [AA17, GSS21]. Our efficient QHT relies on fast QPE and hence builds upon Theorem 1.

Theorem 2 (Efficient QHT, informal). *There exists a quantum circuit of complexity $\mathcal{O}((\log N + \log(1/\varepsilon))^3 \times \log(1/\varepsilon))$ that can perform an ε -approximate QHT of dimension N .*

Being equipped with an efficient QHT, we then consider some problems where it can be applied.

Property testing and learning. One main application of an efficient QHT is Hermite sampling, discussed in detail in Section 5. In this setting we are given black-box access to a function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ and we want to sample from its Hermite spectrum. To do so, we must first use queries to the black box to construct a state whose amplitudes are proportional to f . Then we use the (inverse) QHT n times, to map Hermite states to basis states.

Using Hermite sampling as a subroutine, we are also able to show that quantum algorithms can solve all the following tasks efficiently over the Gaussian distribution:

- (1) Test if f is close to a product of k sign functions;
- (2) Test if f is close to being degree d ;
- (3) Test if f is close to a Hermite polynomial;
- (4) Agnostically learn what we call sparse concepts.

We describe quantum algorithms for (1–3) in [Section 5.3](#) and give the learning application (4) in [Section 5.4](#). We also prove that we have quantum advantage for tasks (1) and (2) in [Section 5.3](#). A recent independent work of Lewis et al. [[LGM25](#)] also gave quantum advantage in learning real-valued functions, but our work is the first to show quantum advantage for property testing with real-valued functions.

We note that these quantum advantages are already attained in the limit of large n with $N = \text{poly}(n)$. Consequently, the polylogarithmic scaling in N that we achieve with our QHT circuit only achieves a polynomial quantum advantage in circuit size for property testing. Now that we have shown that the quantum Hermite transform can be efficiently applied at exponentially large N , we invite others to use this as a building block for new quantum algorithms achieving exponential advantage.

Hamiltonian simulation. Hamiltonian simulation is the problem of simulating quantum dynamics, induced by a Hamiltonian H and for time t , on a quantum computer. In particular, the Hermite functions represent what in physics are known as Fock states. Such states appear naturally in many quantum systems, where the QHO is only one example, and we expect the QHT to be generally applicable for Hamiltonian simulation in these systems.

Quantum systems defined in the continuum involve the position \hat{x} and momentum \hat{p} operators. These become sparse when represented using the Fock states or Hermite functions. Our QHT can then perform the change of basis efficiently, allowing us to work with sparse representations of the Hamiltonians. As the most efficient quantum algorithms for quantum dynamics or Hamiltonian simulation assume the sparse matrix access model (cf. [[BCC⁺15](#), [LC17](#)]), our efficient QHT might be used to reduce the complexity of Hamiltonian simulation in these systems.

Similarly, the QHT is expected to bring novel examples of fast-forwarding. Consider for example the well-known Jaynes-Cummings model that models the interaction of a two-level atom with the electromagnetic field (in the continuum) [[JC05](#)]. When described in the Fock basis, the Hamiltonian simply becomes a direct sum of 2×2 blocks that can be simply diagonalized. Hence, our QHT can also exponentially fast-forward the discrete version of this model.

Like the QFT, our efficient QHT opens the path to other case studies and potential applications. To this end, in [Section 6](#) we list open problems, charting the path for more examples of quantum advantage.

2 Technical overview

Our main result is an efficient quantum circuit for an M -dimensional unitary U , that transforms from the computational basis to the basis of Hermite states given in [\(2\)](#), with arbitrary accuracy. Hermite states are also accurate approximations of the eigenvectors of the ‘discrete’ QHO [[Som16](#)]. That is, we approximate the transformation defined by $U |n\rangle \mapsto |\psi_n\rangle$, where the Hermite states $|\psi_n\rangle$ are a discretization of the n^{th} eigenstate of the QHO Hamiltonian in the continuum $\hat{H} = (\hat{x}^2 + \hat{p}^2)/2$. Here, \hat{x} is the position operator and \hat{p} is the momentum operator: $\hat{x}f(x) = xf(x)$ and $\hat{p}f(x) = -i\frac{d}{dx}f(x)$, for arbitrary $f(x) \in L^2(\mathbb{R})$.

The steps in our efficient QHT are as follows. First, given index $n \in \{0, \dots, N\}$ for some $N > 0$, we prepare the Hermite state $|\psi_n\rangle \in \mathbb{C}^M$ while keeping a copy of $|n\rangle$ in some register. The actual dimension $M = 2^m$ satisfies $M > N$ and has to be chosen properly, as we discuss. This is done via a unitary transformation conditional on $|n\rangle$. To reset $|n\rangle$ to $|0\rangle^{\otimes m}$, i.e., to ‘uncompute’ $|n\rangle$, we infer the value of n from $|\psi_n\rangle$. That is, the sequence of state preparation steps to define the QHT

is

$$\begin{aligned}
|n\rangle &\rightarrow |n\rangle |0\rangle^{\otimes m} && \text{adjoin } m \text{ ancillas} \\
&\rightarrow |n\rangle |\psi_n\rangle && \text{Hermite state preparation} \\
&\rightarrow |0\rangle^{\otimes m} |\psi_n\rangle && \text{uncomputation} \\
&\rightarrow |\psi_n\rangle && \text{discard } m \text{ ancillas.}
\end{aligned}$$

We give an overview of how the main steps are accomplished.

Hermite state preparation. Given n , to prepare the state $|\psi_n\rangle \in \mathbb{C}^M$ we proceed in two steps: First, we prepare an approximation $|\phi_n\rangle \in \mathbb{C}^M$ such that $\langle \phi_n | \psi_n \rangle = \Omega(1)$, and second, we use fixed-point quantum search [YLC14] to transform $|\phi_n\rangle \mapsto |\psi_n\rangle$ efficiently. Amplitude amplification requires a sequence of reflections over $|\psi_n\rangle$ and $|\phi_n\rangle$. The latter can be efficiently implemented because the state $|\phi_n\rangle$ can also be efficiently prepared, but the reflection over $|\psi_n\rangle$ is more intricate. To this end, we design a ‘filtering’ algorithm that flags $|\psi_n\rangle$ and allows us to simulate this reflection by a reflection over a state $|0\rangle$ of an ancilla qubit. This filtering is based on fast QPE; it uses our fast-forwarding result for the QHO and can be implemented efficiently.

The states $|\phi_n\rangle$ are chosen as follows. A useful result for this task is that of Plancherel–Rotach asymptotics [Sze39], which gives approximate expressions for the Hermite functions $\psi_n(x)$ with a provable error bound. Such approximations are only valid in the domain $|x| < \sqrt{2n+1}$, where the points $\pm x_{\text{tp}} = \pm\sqrt{2n+1}$ are known as the ‘turning’ points in physics. Explicitly, these approximations read:

$$\psi_n(x) = \frac{(-1)^n 2^{\frac{1}{4}}}{\pi^{\frac{1}{2}} n^{\frac{1}{4}}} \frac{1}{\sqrt{\sin \varphi(x)}} \left(\sin \left[\left(\frac{n}{2} + \frac{1}{4} \right) (\sin(2\varphi(x)) - 2\varphi(x)) + \frac{3\pi}{4} \right] + \mathcal{O}\left(\frac{1}{n}\right) \right), \quad (4)$$

where $\varphi(x) := \arccos(x/\sqrt{2n+1})$ is such that $\pi > \varphi(x) > 0$.

We show how to use this approximation formula to construct the states $|\phi_n\rangle$ efficiently, which are now simply superposition states with amplitude modulated by $\frac{1}{\sqrt{\sin \varphi(x)}}$ and also a phase that depends on $\varphi(x)$. We also show that the states $|\phi_n\rangle$ have nonzero, constant overlap with the $|\psi_n\rangle$.

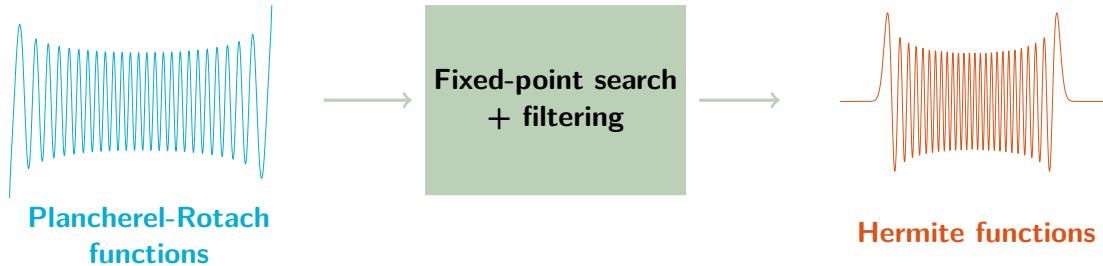


Figure 1: A visualization of the Quantum Hermite Transform. On the left we have the Plancherel–Rotach functions (visualized without the decaying envelope for simplicity), we prepare states corresponding to these, which is then fed into the fixed-point search algorithm using our fast-forwarding result as a subroutine. This allows us to prepare the states corresponding to the Hermite functions in superposition to arbitrary precision. Both the functions are visualized for $n = 10$.

Uncomputation. For the uncomputation step where we reset $|n\rangle \mapsto |0\rangle^{\otimes m}$, we use a version of Kitaev’s QPE algorithm [Kit95]. The Hermite functions are known eigenfunctions of the QHO Hamiltonian \hat{H} of eigenvalue $n + 1/2$. Similarly, the Hermite states $|\psi_n\rangle$ can be shown to be

accurate approximations of the eigenvectors $|\psi_n\rangle$ of the discrete QHO \bar{H} , with eigenvalues that are very close to $n + 1/2$ [Som16]. For a bounded Hamiltonian H satisfying $\|H\| \leq 1$, QPE is able to distinguish eigenvalues separated by a difference Δ by implementing unitary time evolutions of the form e^{-iHt} up to evolution times $t \sim 1/\Delta$. In our case, if $H = \bar{H}/M$ is the rescaled version of \bar{H} , we have $\Delta \sim 1/M$ and hence $t \sim M$. Then, to avoid any complexity polynomial in M , we use Theorem 1 that allows us to fast forward this time evolution and to perform fast QPE.

Last, we give an overview for the proof of Theorem 1, which is used in the state preparation for both filtering and uncomputation.

Fast-forwarding. Central to this result is a factorization of the evolution operator $e^{-i\hat{H}t}$, where $\hat{H} = (\hat{p}^2 + \hat{x}^2)/2$ is the QHO Hamiltonian in the continuum. We exploit the canonical commutation relations, namely $[\hat{x}, \hat{p}] = iI$, where I is the identity such that $If(x) = f(x)$. Then [QA07]

$$\exp(-i\hat{H}t) = \exp\left(-\frac{i \tan(t/2) \hat{p}^2}{2}\right) \exp\left(-\frac{i \sin(t) \hat{x}^2}{2}\right) \exp\left(-\frac{i \tan(t/2) \hat{p}^2}{2}\right). \quad (5)$$

We then consider a discrete version of the QHO, referred to as \bar{H} , and analyze the time complexity and the discretization error of this factorization. To this end, we define \bar{x} and \bar{p} to be a specific choice of discretizations of \hat{x} and \hat{p} , defined in [Som16], and let $\bar{H} := (\bar{p}^2 + \bar{x}^2)/2$. We show that the factorization of (5), when replacing $\hat{x} \rightarrow \bar{x}$ and $\hat{p} \rightarrow \bar{p}$, reproduces the evolution operator $e^{-i\bar{H}t}$ within accuracy that is exponentially small in N in the low-energy subspace, where $N \leq M = \text{poly}(N)$, and M is the Hilbert dimension of \bar{H} . The low-energy subspace is that spanned by the N eigenvectors of \bar{H} of smallest eigenvalue.

To prove this result, we consider the commutation relations of the discrete operators \bar{x} and \bar{p} and show they approximate those between \hat{x} and \hat{p} , in the low-energy subspace, the space spanned by the first N eigenvectors of \bar{H} . For example, in that subspace, $[\bar{x}, \bar{p}] - iI$ can be shown to have norm exponentially small in N , where I is now the N -dimensional identity. We also need to bound the errors of the *nested* commutators. Let $[\bar{x}^2, \bar{p}^2]_k = [\bar{x}^2, [\bar{x}^2, \bar{p}^2]_{k-1}]$ be the k -th nested commutator, where $[\bar{x}^2, \bar{p}^2]_1 = [\bar{x}^2, \bar{p}^2]$. We cannot directly use the fact that the norm of $[\bar{x}, \bar{p}] - iI$ is small on the low-energy subspace, because when nesting one would naively incur a cost which scales as $\approx M^{k-1}$ due to the multiplication of $k-1$ matrices after using the relation once. We show how to control the growth of these terms within the low-energy subspace by proving that (i) polynomials in the operators with degree t have norm which scale as N^t in the low-energy subspace, and (ii) certain operators which capture the discretization errors have norm $\text{poly}(M)$ on the entire space whose growth can be controlled by $t!$ when t is sufficiently greater than N . See Section 3 for more details. We believe this technique would be useful for more Hamiltonian simulation results as well.

The approximated evolution operator of the discrete QHO also involves three exponentials. The exponential of $i \sin(t) \bar{x}^2/2$ is a diagonal unitary that can be simply implemented with $\mathcal{O}(\log^2 N)$ two-qubit arbitrary gates regardless of t . (For simplicity throughout this paper we assume that arbitrary gates can be implemented perfectly, without any overhead in precision.) To this end, we use coherent arithmetic for multiplication and then use phase kickback. Since \bar{p} is obtained from \bar{x} via conjugation with the (centered) QFT, the exponentials involving \bar{p}^2 can also be implemented with $\mathcal{O}(\log^2 N)$ two-qubit arbitrary gates. This is then an example of exponential fast-forwarding, since it avoids the no-fast-forwarding bound $\Omega(\|H\|t)$, which would be linear in Nt in this case.

3 Fast-forwarding of the QHO

In this section we discuss [Theorem 1](#) and present the formal results on the evolution of the QHO. First, let us discuss the algebraic factorization of the time-evolution of the quantum harmonic oscillator in the infinite-dimensional case. Since the Hamiltonian is the sum of two terms, $\hat{H} = (\hat{x}^2 + \hat{p}^2)/2$, if the operators were commuting, we could simply factor by breaking up the sum. But the position and momentum operator do not commute. What we do know is the canonical commutation relation between them, $[\hat{x}, \hat{p}] = iI$. Combined with the Baker–Campbell–Hausdorff formula, this allows us to factor the time-evolution of the Hamiltonian. First, we notice these relations which can be checked by computation:

1. $[\hat{x}^2, \hat{p}^2] = 2i\{\hat{x}, \hat{p}\}$
2. $[\hat{x}^2, \{\hat{x}, \hat{p}\}] = 4i\hat{x}^2$
3. $[\hat{p}^2, \{\hat{x}, \hat{p}\}] = -4i\hat{p}^2$

Further, [Item 2](#) implies that $[\hat{x}^2, [\hat{x}^2, \{\hat{x}, \hat{p}\}]] = 0$. [Item 3](#) implies the symmetric statement about momentum. One thus finds that the Lie algebra generated by \hat{x}^2 and \hat{p}^2 is three dimensional, namely the span of \hat{x}^2 , \hat{p}^2 , and $\{\hat{x}, \hat{p}\}$. These facts about the nested commutators ‘kill off’ infinite terms in the BCH expansion and give us the following factorization for the evolution operator, also discussed in [\[QA07\]](#).

Theorem 3 (Factorization of the QHO evolution [\[QA07\]](#)). *The evolution operator of the QHO admits the following factorization:*

$$\exp(-i\hat{H}t) = \exp\left(-\frac{i \tan(t/2)\hat{p}^2}{2}\right) \exp\left(-\frac{i \sin(t)\hat{x}^2}{2}\right) \exp\left(\frac{-i \tan(t/2)\hat{p}^2}{2}\right). \quad (6)$$

For completeness, we include an independent proof of this in [Appendix A](#).

Now, if we want to fast-forward on a digital quantum computer, then we need to pick a discretization of the infinite dimensional Hamiltonian. We use the same definition of the discretization as the previous work on fast-forwarding the QHO [\[Som16\]](#). This sets \bar{x} to be a diagonal matrix of size $M \times M$, and \bar{p} as its conjugation by a centered discrete Fourier transform. Then we can set $\bar{H} = (\bar{x}^2 + \bar{p}^2)/2$. It is not at all clear a priori that this factorization is still faithful. In particular, it is no longer true that $[\bar{x}, \bar{p}] = iI$. Remarkably, we are able to carry the factorization to the case of the discrete QHO. Moreover, our error is *doubly-exponentially* small! We recall [Theorem 1](#) below.

Theorem 1 (Exponential fast-forwarding of the QHO). *Let N be the target dimension for fast-forwarding, $\bar{H} \in \mathbb{C}^{M \times M}$ be the Hamiltonian of a discrete QHO, and $t \in [-\pi, \pi]$. Then, we can choose $M = \Theta(N \log N)$ such that the evolution operator $e^{-i\bar{H}t}$ can be simulated within error $\mathcal{O}(\exp(-N/10))$ in the subspace spanned by the first N eigenvectors of \bar{H} using $\mathcal{O}(\log^2 N)$ gates.*

We now formally define our discretized QHO. We use the same conventions as [\[Som16\]](#), but change the notation slightly.

Discrete QHO. For given dimension $M > 0$, we discretize the space with a grid of discretization size $\sqrt{2\pi/M}$. We define the discretized position operator as

$$\bar{x} := \sqrt{\frac{2\pi}{M}} \begin{pmatrix} -\frac{M}{2} & 0 & \dots & 0 \\ 0 & -\frac{M}{2} + 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \frac{M}{2} - 1 \end{pmatrix}, \quad (7)$$

and the discrete momentum operator $\bar{p} := F^{-1}\bar{x}F$, where F is the centered M -dimensional discrete Fourier Transform. (The centered Fourier transform is equivalent to the standard discrete Fourier transform up to relabeling the indices j , as described in [Appendix B](#).) Then, the discrete QHO Hamiltonian is

$$\bar{H} = \frac{1}{2} (\bar{x}^2 + \bar{p}^2) . \quad (8)$$

We let $|\psi_n\rangle$ be the eigenstates of \bar{H} , for $0 \leq n \leq M-1$. In [\[Som16\]](#) it was shown that $|\psi_n\rangle$ are very close to the Hermite states

$$|\psi_n\rangle := \left(\frac{2\pi}{M}\right)^{1/4} \sum_{j=-M/2}^{M/2-1} \psi_n(x_j) |j\rangle , \quad (9)$$

where $\psi_n(x)$ is the n^{th} Hermite function. Below, we collect some facts about this discretization. We introduce $|\Psi_n\rangle$ as the bra-ket representation of the n th continuum QHO eigenstate.

Fact 4 ([\[Som16\]](#)). *There exist constants $\gamma, c \in (0, 1)$ such that for all M sufficiently large and all $k, \ell \leq cM$,*

1. $|\langle\psi_k|\psi_\ell\rangle - \delta_{k,\ell}| \leq \exp(-\gamma M)$.
2. For $a, b \leq 4$, $\left| \langle\bar{\psi}_k| \bar{x}^a \bar{p}^b |\bar{\psi}_\ell\rangle - \langle\Psi_k| \hat{x}^a \hat{p}^b |\Psi_\ell\rangle \right| \leq \exp(-\gamma M)$.

In other words, this discretization is highly effective in a subspace with bounded energy. We will prove that in a subspace within this one, we can perform the fast-forwarding with provably small error, as visualized in [Figure 2](#).

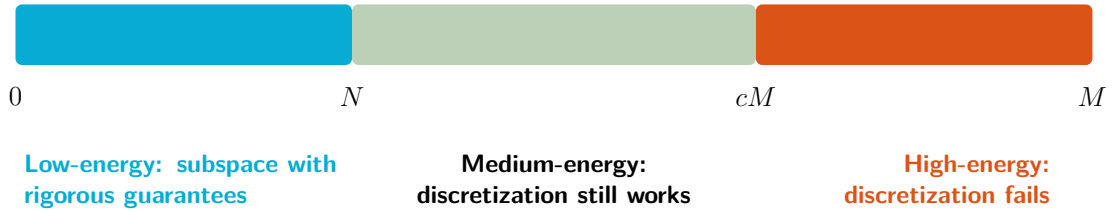


Figure 2: Visualization of discretization error for the QHO. Here $N = \Theta(M/\log M)$, as specified in [Theorem 5](#). In the “low-energy” subspace, the fast-forwarding algorithm provably works. Meanwhile, in the “medium-energy” subspace [Fact 4](#) still holds, although we no longer obtain rigorous guarantees on fast-forwarding.

Remark. You might notice that these statements do not necessarily imply that the k^{th} eigenstate of the discrete Hamiltonian \bar{H} is close to the k^{th} discrete Hermite state, in the case that eigenvalue gaps are exponentially small. We point out that we do not have a rigorous proof that the eigenvalue gaps are not exponentially small; in principle one could worry that eigenstates from the high energy subspace, upon discretization, could jump down to the low energy subspace and land exponentially close to a low eigen-energy. In fact, numerically one observes that the high eigen-energies, though less accurately conforming to their continuum values than the low eigen-energies, never cross all the way into the low energy subspace. Nonetheless, since we only care about the closeness to the discrete Hermite states, our claims about fast-forwarding are true irrespective of the eigenvalue gaps.

Note that our convention for basis states is such that $j \in \{-M/2, \dots, M/2 - 1\}$, which differs from the standard convention where $j \in \{0, \dots, M - 1\}$. This simplifies the exposition, since Hermite functions are defined in a domain where $x \in \mathbb{R}$ and we can directly associate j with a position in space. Transforming from one convention to the other is a cyclic permutation, i.e., $|-M/2\rangle \mapsto |0\rangle$, $|-M/2 + 1\rangle \mapsto |1\rangle$, and so on. However, we do not need to perform this permutation in the algorithm; the relevant observation is that F is not exactly the QFT, as explained in [Appendix B](#), but can still be implemented with $\mathcal{O}(\log^2 M)$ gates.

The following result shows that the factorization of the QHO's evolution operator in the continuum of [Theorem 3](#) can be carried to this discrete case.

Theorem 5. *There is a constant η such that for $N = \eta M / \log M$, we have the following. Let \bar{H} be the discretization with grid size $\sqrt{\frac{2\pi}{M}}$ and for $|t| \leq \pi/2$,*

$$\left\| \Pi_N \left(e^{-i\bar{H}t} - e^{-ia(t)\bar{p}^2} e^{-ib(t)\bar{x}^2} e^{-ia(t)\bar{p}^2} \right) \Pi_N \right\| \leq \exp(-N/2).$$

where

$$a(t) = \frac{\tan(t/2)}{2} \quad \text{and} \quad b(t) = \frac{\sin(t)}{2}.$$

We next comment on how to apply [Theorem 5](#) to decompose $e^{-i\hat{H}t}$ for arbitrary t . We first recall that, in the continuum, all eigenvalues of H are of the form $n + 1/2$ for integer n . Hence, the time evolution of the quantum harmonic oscillator is periodic in the sense that $e^{-iH2\pi} = -I$. Therefore, we can always subtract an integer multiple of 2π from t to bring t into the range $-\pi$ to π . As noted in [Theorem 3](#), the formal identity (6) holds for arbitrary t but one must be careful since the tangent function has divergences, in particular at argument $t/2 = \pm\pi/2$. In the discretized case it becomes important to keep the coefficients $a(t)$ and $b(t)$ bounded in order to keep the error bounded. To achieve this, whenever $|t| > \pi/2$, we use the factorization

$$e^{-i\hat{H}t} = \left(e^{-i\hat{H}(t/2)} \right)^2 \tag{10}$$

$$= \left(e^{-ia(t/2)\hat{p}^2} e^{-ib(t/2)\hat{x}^2} e^{-ia(t/2)\hat{p}^2} \right)^2 \tag{11}$$

$$= e^{-ia(t/2)\hat{p}^2} e^{-ib(t/2)\hat{x}^2} e^{-2ia(t/2)\hat{p}^2} e^{-ib(t/2)\hat{x}^2} e^{-ia(t/2)\hat{p}^2} \tag{12}$$

This factorization then translates to a quantum circuit to approximate $e^{-i\bar{H}t}$ using a total of five steps. Each step implements either the diagonal operator $e^{-ib\bar{x}^2}$ by phase kickback, or implements the operator $e^{-ia\bar{p}^2}$ using the quantum Fourier transform to change to its eigenbasis, then applying phase kickback, and then transforming back. When $|t| \leq \pi/2$ we would apply [Theorem 5](#) directly, which requires only three phase-kickback steps.

To prove [Theorem 5](#) it would suffice show that the total contribution of the nested commutators like $\left(\sum_{t=3}^{\infty} \frac{1}{t!} [\bar{x}^2, \bar{p}^2]_t \right)$ vanishes as the Hilbert space dimension goes to ∞ . This is in fact not true, but in [Theorem 14](#) we show this is true when we project down to the subspace corresponding to energy levels $N = O(M/\log M)$ for a Hilbert space of dimension M . We show a similar bound on the terms involving $[\bar{p}^2, \bar{x}^2]_t$ and $[\bar{p}^2, \{\bar{x}, \bar{p}\}]_t$, which suffices to prove [Theorem 5](#). Since we pay a $\log M$ cost to compute up to M , we can always run the discretization for an M such that $N = O(M/\log M)$ and project back down. More precisely, we prove the following theorem about the norm of the nested commutators. Below, γ is a constant to be declared later.

Theorem 6. For any constants c_1, c_2 such that $\max(|c_1|, |c_2|) \leq 1$, and $N = \gamma M / (40 \log(2M))$, we have

$$\begin{aligned} \left\| \Pi_N \left(\sum_{t=3}^{\infty} \frac{1}{t!} [c_1 \bar{x}^2, c_2 \bar{p}^2]_t \right) \Pi_N \right\| &\leq \exp(-\gamma N/2). \\ \left\| \Pi_N \left(\sum_{t=3}^{\infty} \frac{1}{t!} [c_1 \bar{p}^2, c_2 \bar{x}^2]_t \right) \Pi_N \right\| &\leq \exp(-\gamma N/2) \\ \left\| \Pi_N \left(\sum_{t=2}^{\infty} \frac{1}{t!} [c_1 \bar{p}^2, c_2 \{\bar{x}, \bar{p}\}]_t \right) \Pi_N \right\| &\leq \exp(-\gamma N/2). \end{aligned}$$

The main technical difficulty in proving this statement comes from the fact that when we have a nested commutator $[A, B]_t$ with a very large t , then the naive bound on this scales with an exponential in t , since we repeatedly use the norm of the matrices as a bound. We use a trick to split the sum into few-nestings and many-nestings to control the growth of these terms when projected to a low-energy subspace. In the next section, we discuss the explicit algorithm for the QHO and prove it is correct using this theorem. Then in [Section 3.2](#) we prove this theorem.

3.1 The algorithm

From the statement of [Theorem 5](#), the algorithm for fast-forwarding is simple, as given in [Algorithm 1](#).

Algorithm 1 Fast-forwarding QHO

```

1:  $t_2 \leftarrow t - 2\pi \lfloor t/2 \rfloor$  ▷ Shift  $t$  into the range  $[-\pi, \pi)$ 
2: if  $|t_2| > \pi/2$  then ▷ If  $t_2$  is too big halve it and use two repetitions.
3:    $\alpha \leftarrow \tan(t_2/4)/2$ 
4:    $\beta \leftarrow \sin(t_2/2)/2$ 
5:   Compute  $e^{-i\alpha \bar{p}^2} e^{-i\beta \bar{x}^2} e^{-i2\alpha \bar{p}^2} e^{-i\beta \bar{x}^2} e^{-i\alpha \bar{p}^2}$ 
6: else ▷ Otherwise use one repetition.
7:    $\alpha \leftarrow \tan(t_2/2)/2$ 
8:    $\beta \leftarrow \sin(t_2)/2$ 
9:   Compute  $e^{-i\alpha \bar{p}^2} e^{-i\beta \bar{x}^2} e^{-i\alpha \bar{p}^2}$ 

```

So let us now prove [Theorem 5](#) using [Theorem 6](#). We will give the proof of [Theorem 6](#) in the next subsection.

Proof of [Theorem 5](#). Let $\bar{H} = \frac{1}{2}(\bar{x}^2 + \bar{p}^2)$ be the discretized quantum harmonic oscillator Hamiltonian. We will denote $U(t) = \exp(-i\bar{H}t)$. Further, denote

$$\widetilde{U}(t) = \exp\left(-i \frac{\tan(t/2) \bar{p}^2}{2}\right) \exp\left(-i \frac{\sin(t) \bar{x}^2}{2}\right) \exp\left(-i \frac{\tan(t/2) \bar{p}^2}{2}\right)$$

We show in [Appendix A](#), [Lemma 70](#) that for $\alpha' = \tan(t/2)/2$, $\beta' = \sin(t)/2$,

$$\widetilde{U}(t)^{-1} \frac{d\widetilde{U}(t)}{dt} = -i\bar{H} + \beta' \sum_{t=3}^{\infty} \frac{1}{t! 2^{t/2}} [\beta' i \bar{x}^2, i \bar{p}^2]_t + \alpha' \sum_{t=3}^{\infty} \frac{1}{t! 2^{t/2}} [\alpha' i \bar{p}^2, i \bar{x}^2]_t + \alpha' \sum_{t=2}^{\infty} \frac{1}{t! 2^{t/2}} [\alpha' i \bar{p}^2, i \{\bar{x}, \bar{p}\}]_t$$

Now we can use [Theorem 6](#), but we need a bound on α', β' . Assume without loss of generality that $t \in [-\pi, \pi]$. If $|t| < \pi/2$ then we have that $|\alpha'|, |\beta'| \leq 1/2$. We also have $\dot{\alpha}', \dot{\beta}' \leq 2$. Hence we can conclude

$$\|\Pi_N \left(\widetilde{U(t)}^{-1} \frac{d\widetilde{U(t)}}{dt} + i\bar{H} \right) \Pi_N\| \leq 6 \exp(-\gamma N/2)$$

Let us represent this quantity in the brackets by η . Then by the Baker-Campbell-Hausdorff theorem we know that,

$$\exp(\eta)\widetilde{U(t)} = \exp\left(\eta + i\bar{H}t + \frac{it}{2} [\eta, \bar{H}] + \frac{it}{12} [\eta, \bar{H}]_2 + \dots\right)$$

Thus, we have that

$$\|\Pi_N (U(t) - \widetilde{U(t)}) \Pi_N\| \leq 6 \exp(-\gamma N/4)$$

It remains to bound the case when $|t|$ is in $(\pi/2, \pi)$. In this case, we can divide t by 2 and repeat the factorization twice. So define $\widetilde{U(t)}_2 = \left(\exp\left(\frac{i \tan(t/4) \bar{p}^2}{2}\right) \exp\left(\frac{i \sin(t/2) \bar{x}^2}{2}\right) \exp\left(\frac{i \tan(t/2) \bar{p}^2}{2}\right) \right)^2$. Now we have the same bounds on the nested commutators. Hence we can derive that

$$\|\Pi_N (U(t) - \widetilde{U(t)}_2) \Pi_N\| \leq 12 \exp(-\gamma N/4)$$

This proves that for all t the discrete Hamiltonian evolution can be factorized into 3 or 6 terms while being doubly-exponentially accurate. We use that $\gamma \geq 1/2$ to conclude the quantitative bound in our theorem. \square

Now, the size of the circuit to compute these factorizations in [Algorithm 1](#) is enough to perform fast-forwarding. Hence we are ready to prove [Theorem 1](#).

Proof of Theorem 1. Computing these factorizations has error $\exp(-N/10)$ due to [Theorem 5](#). Thus [Algorithm 1](#) is correct. We can compute these factorizations in $\mathcal{O}(\log^2 N)$ time because we can prepare $\exp(-i\bar{x})$ of dimension M in $\mathcal{O}(\log^2 N)$ time using the technique of phase kickback since \bar{x} is diagonal. Further, we can perform QFT in $\tilde{\mathcal{O}}(\log N)$ time [\[CW00\]](#) to prepare \bar{p} from \bar{x} , which is diagonal in the Fourier basis so allows us to prepare $\exp(-i\bar{p})$ in $\mathcal{O}(\log^2 N)$ time. Adding the trigonometric functions in the expression costs constant time by our assumption. Hence the total runtime is $\mathcal{O}(\log^2 N)$. \square

3.2 Bounding nested commutators

In this section we prove the aforementioned bounds on the nested commutators of \bar{x}^2, \bar{p}^2 and $\{\bar{x}, \bar{p}\}$. Going forward, we define

$$\Delta = [\bar{x}^2, \bar{p}^2]_2 - 4i\bar{x}^2 \tag{13}$$

to be the *discretization error*. Indeed, in the continuous case, $[\hat{x}^2, \hat{p}^2]_2 - 4i\hat{x}^2 = 0$. Choose

$$N' = \frac{\gamma M}{8 \log(2M)} \tag{14}$$

for some suitably small constant $\gamma > 0$ to be chosen later, and take

$$N = N'/5. \tag{15}$$

We define Π_N to be the projector onto the subspace spanned by the discrete eigenstates $|\overline{\psi_k}\rangle$ for $k \leq N$, and $\Pi_{N'}$ is defined analogously. Formally,

$$\Pi_N = \sum_{k=1}^N |\overline{\psi_k}\rangle \langle \overline{\psi_k}|, \quad \Pi_{N'} = \sum_{k=1}^{N'} |\overline{\psi_k}\rangle \langle \overline{\psi_k}|$$

We argue that, analogously to the continuous case, the discretized \overline{x}^a operators do not cause significant leakage from the bottom N eigenstates to eigenstates above level N' , provided that a is sufficiently small. First we show that the corresponding matrix elements in the discrete and continuous cases are close.

Lemma 7. *Let $a \leq \frac{\gamma M}{10 \log(2M)}$. Then whenever M is sufficiently large,*

$$\max_{\substack{k \leq N' \\ \ell \leq N}} \left| \langle \overline{\psi_k} | \overline{x}^a | \overline{\psi_\ell} \rangle - \langle \Psi_k | \hat{x}^a | \Psi_\ell \rangle \right| \leq \exp(-\gamma M/4)$$

Proof. We will first bound the distance between $\langle \psi_k | \overline{x}^a | \psi_\ell \rangle$ and $\langle \Psi_k | \hat{x}^a | \Psi_\ell \rangle$ then later show that the former is close to $\langle \overline{\psi_k} | \overline{x}^a | \overline{\psi_\ell} \rangle$. We can write $\langle \Psi_k | \hat{x}^a | \Psi_\ell \rangle = \int_{\mathbb{R}} x^a \psi_k(x) \psi_\ell(x) dx$. Recall that our discretization has the limits $[-L, L]$, where $L = \sqrt{\frac{\pi M}{2}}$. Define the strip $\mathcal{S} = \{z \in \mathbb{C} : \max\{|\operatorname{Re}(z)|, |\operatorname{Im}(z)|\} \leq L\}$. Within this region, applying Plancherel-Rotach asymptotic arguments (see, e.g. [Sze39]), we have the bound

$$\sup_{z \in \mathcal{S}} |\psi_k(z)| \leq K \cdot k^{-1/4} \sup_{z \in \mathcal{S}} |e^{-z^2}/2| \leq K \cdot \sup_{z \in \mathcal{S}} |e^{\operatorname{Im}(z)^2/2}| \leq K \cdot e^{L^2/2}. \quad (16)$$

This readily gives us the bound

$$\sup_{z \in \mathcal{S}} |x^a \psi_k(z) \psi_\ell(z)| \leq (L\sqrt{2})^a \cdot e^{L^2}$$

for some suitably large constant K . Thus, employing the exponentially convergent trapezoid rule [TCW14], we have

$$\left| \langle \psi_k | \overline{x}^a | \psi_\ell \rangle - \int_{-L}^L x^a \psi_k(x) \psi_\ell(x) dx \right| \leq 2(L\sqrt{2})^a \exp(L^2 - 2\pi M) = 2(L\sqrt{2})^a \exp(-\pi M). \quad (17)$$

Since $a \leq M/10 \log(2M)$ we can bound this term by $\exp(-M)$. Now we compute the error accrued from imposing the limits $\pm L$. That is,

$$\left| \int_{-L}^L x^a \psi_k(x) \psi_\ell(x) dx - \int_{\mathbb{R}} x^a \psi_k(x) \psi_\ell(x) dx \right| = 2 \left| \int_L^\infty x^a \psi_k(x) \psi_\ell(x) dx \right|.$$

We can bound $|x^a \psi_k(x) \psi_\ell(x)| \leq \pi^{-1/4} |x^a \psi_k(x)|$. Now, L is much larger than the turning point of $\psi_k(x)$. By standard results (such as, say [Som16, Eq. (A4)], there exists a constant c such that

$$|x^a \psi_k(x)| \leq c |x^a| \cdot e^{\sqrt{2k}x - x^2/2} = c e^{\sqrt{2k}x - a \log x - x^2/2} \leq e^{-x^2/3}$$

whenever M is sufficiently large. This gives us the bound

$$\left| \int_L^\infty x^a \psi_k(x) \psi_\ell(x) dx \right| \leq \left| \int_L^\infty e^{-x^2/3} dx \right| \leq e^{-L^2/6} \leq e^{-\pi M/12}.$$

We now show that $\langle \bar{\psi}_k | \bar{x}^a | \bar{\psi}_\ell \rangle$ is close to $\langle \psi_k | \bar{x}^a | \psi_\ell \rangle$. Indeed, we have

$$\left| \langle \bar{\psi}_k | \bar{x}^a | \bar{\psi}_\ell \rangle - \langle \psi_k | \bar{x}^a | \psi_\ell \rangle \right| = \left| \langle \bar{\psi}_k | \bar{x}^a | \bar{\psi}_\ell \rangle - \langle \bar{\psi}_k | \bar{x}^a | \psi_\ell \rangle \right| + \left| \langle \bar{\psi}_k | \bar{x}^a | \psi_\ell \rangle - \langle \psi_k | \bar{x}^a | \psi_\ell \rangle \right| \quad (18)$$

$$= \left| \langle \bar{\psi}_k | \bar{x}^a \left(|\bar{\psi}_\ell\rangle - |\psi_\ell\rangle \right) \right| + \left| \left(\langle \bar{\psi}_k | - \langle \psi_k | \right) \bar{x}^a | \psi_\ell \rangle \right| \quad (19)$$

$$\leq \left\| \bar{x}^a | \bar{\psi}_k \rangle \right\| \cdot \left\| |\bar{\psi}_\ell\rangle - |\psi_\ell\rangle \right\| + \left\| |\bar{\psi}_k\rangle - |\psi_k\rangle \right\| \cdot \left\| \bar{x}^a | \psi_\ell \rangle \right\| \quad (\text{Cauchy-Schwarz})$$

$$\leq \left\| \bar{x}^a \right\| \cdot \left\| |\bar{\psi}_\ell\rangle - |\psi_\ell\rangle \right\| + (1 + \exp(-\gamma M)) \left\| |\bar{\psi}_k\rangle - |\psi_k\rangle \right\| \cdot \left\| \bar{x}^a \right\| \quad (\text{Fact 4})$$

$$\leq \exp\left(-\frac{a \log(\pi M/2)}{2}\right) \cdot \left(\left\| |\bar{\psi}_\ell\rangle - |\psi_\ell\rangle \right\| + 2 \left\| |\bar{\psi}_k\rangle - |\psi_k\rangle \right\| \right) \quad (20)$$

$$\leq 3 \exp(\gamma M/10 - \gamma M) \quad (\text{Fact 4})$$

$$= 3 \exp(-9\gamma M/10). \quad (21)$$

Putting everything together, the overall bound we obtain is

$$(2M)^{a/2} \exp(-\pi M/2) + 2e^{-\pi M/12} + 3e^{-9\gamma M/10} \leq e^{-\gamma M/4}$$

for all M sufficiently large. \square

We use the above bound to show that low degree position operators result in very little leakage from energy at most N to energy above N' .

Lemma 8. *For all M sufficiently large and whenever $a \leq 4N$, $\|(I - \Pi_{N'})\bar{x}^a \Pi_N\| \leq \exp(-\gamma M/9)$, where N' and N are as defined in (14) and (15).*

Proof. Define

$$\delta_a = \max_{\substack{k \leq N' \\ \ell \leq N}} \left| \langle \bar{\psi}_k | \bar{x}^a | \bar{\psi}_\ell \rangle - \langle \Psi_k | \hat{x}^a | \Psi_\ell \rangle \right|, \quad \kappa_a = \max_{k \leq N} \left| \langle \bar{\psi}_k | \bar{x}^{2a} | \bar{\psi}_k \rangle - \langle \Psi_k | \hat{x}^{2a} | \Psi_k \rangle \right|$$

We claim that

$$\|(I - \Pi_{N'})\bar{x}^a \Pi_N\| \leq \left(\sqrt{N'} \cdot \delta_{2N} + \sqrt{\kappa_{2N}} \right) \cdot \sqrt{M}$$

Indeed, we need only show that

$$\max_{\substack{N' < k \leq M \\ \ell \leq N}} \left| \langle \bar{\psi}_k | \bar{x}^a | \bar{\psi}_\ell \rangle \right| = \max_{\substack{N' < k \leq M \\ \ell \leq N}} \left| \langle \bar{\psi}_k | \bar{x}^a | \bar{\psi}_\ell \rangle - \langle \Psi_k | \hat{x}^a | \Psi_\ell \rangle \right| \leq \sqrt{N'} \cdot \delta_{4N} + \sqrt{\kappa_{4N}}.$$

We can write

$$\bar{x}^a | \bar{\psi}_\ell \rangle = \beta | \bar{\psi} \rangle + \sum_{j \leq N'} \alpha'_j | \bar{\psi}_j \rangle, \quad \hat{x}^a | \Psi_\ell \rangle = \sum_{j \leq N'} \alpha_j | \Psi_j \rangle$$

where we have used the fact that $a \leq 4N$, and doesn't push the support above energy level N' . We have the bound $\left| \langle \bar{\psi}_k | \bar{x}^a | \bar{\psi}_\ell \rangle \right| \leq |\beta|$. We have $|\alpha_j - \alpha'_j| \leq \delta_a$ and

$$\left| \beta^2 + \sum_{j=1}^{N'} (\alpha_j - \alpha'_j)^2 \right| \leq \kappa_{4N}$$

From this we have the desired bound

$$|\beta| \leq \sqrt{N'} \cdot \delta_{4N} + \sqrt{\kappa_{4N}}$$

By Lemma 7, since $a \leq 4N \leq \gamma M / (10 \log(2M))$, we can bound

$$\delta_{4N} \leq \exp(-\gamma M/4), \quad \kappa_{4N} \leq \exp(-\gamma M/4)$$

Thus we have the bound

$$|\beta| \leq \sqrt{N'} \cdot e^{-\gamma M/4} + e^{-\gamma M/8} \leq 2e^{-\gamma M/8}. \quad (22)$$

Since $\|(I - \Pi_{N'})\bar{x}^a \Pi_N\| \leq |\beta| \cdot N'$, we have the bound

$$\|(I - \Pi_{N'})\bar{x}^a \Pi_N\| \leq 2\sqrt{M}e^{-\gamma M/8} \leq e^{-\gamma M/9}$$

for all M sufficiently large. \square

We now prove a number of desirable properties of the discretization error Δ . In particular, we show that Δ is small on the subspace spanned by the first N' eigenvectors, and then bound its overall operator norm. First, we recall a fundamental fact about Hermite polynomials.

Fact 9.

$$xH_k(x) = kH_{k-1}(x) + \frac{1}{2}H_{k+1}(x)$$

Lemma 10. *For all M sufficiently large:*

1. $\|\Pi_{N'}\Delta\Pi_{N'}\| \leq \exp(-\gamma M/3)$
2. $\|\Delta\| \leq 17M^3$.

Proof. We have the bound

$$\|\Pi_{N'}\Delta\Pi_{N'}\| \leq \sqrt{M} \cdot \max_{\substack{k \leq N' \\ \ell \leq N'}} \left| \langle \bar{\psi}_k | \Delta | \bar{\psi}_\ell \rangle \right| = \sqrt{M} \cdot \max_{\substack{k \leq N' \\ \ell \leq N'}} \left| \langle \bar{\psi}_k | \Delta | \bar{\psi}_\ell \rangle - \langle \Psi_k | [\hat{x}^2, \hat{p}^2]_2 - 8i\bar{x}^2 | \Psi_\ell \rangle \right|,$$

where we recall that $[\hat{x}^2, \hat{p}^2]_2 = 8i\bar{x}^2$. We expand

$$\Delta = \bar{x}^4 \bar{p}^2 - 2\bar{x}^2 \bar{p}^2 \bar{x}^2 + \bar{p}^2 \bar{x}^4 - 8i\bar{x}^2.$$

We can use the triangle inequality to match terms of Δ and $[\hat{x}^2, \hat{p}^2]_2 - 8i\bar{x}^2$. In what follows, we make ample use of Fact 4. For the first such term, we bound

$$\left| \langle \bar{\psi}_k | \bar{x}^4 \bar{p}^2 | \bar{\psi}_\ell \rangle - \langle \Psi_k | \hat{x}^4 \hat{p}^2 | \Psi_\ell \rangle \right| \leq \exp(-\gamma M).$$

The same argument shows that

$$\left| \langle \bar{\psi}_k | \bar{p}^2 \bar{x}^4 | \bar{\psi}_\ell \rangle - \langle \Psi_k | \hat{p}^2 \hat{x}^4 | \Psi_\ell \rangle \right| \leq \exp(-\gamma M).$$

Furthermore, we have

$$\left| \langle \bar{\psi}_k | 8i\bar{x}^2 | \bar{\psi}_\ell \rangle - \langle \Psi_k | 8i\hat{x}^2 | \Psi_\ell \rangle \right| \leq 8 \exp(-\gamma M).$$

The most challenging term to bound is

$$\left| \langle \bar{\psi}_k | \bar{x}^2 \bar{p}^2 \bar{x}^2 | \bar{\psi}_\ell \rangle - \langle \Psi_k | \hat{x}^2 \hat{p}^2 \hat{x}^2 | \Psi_\ell \rangle \right|.$$

Our solution will be to write $\bar{x}^2 |\bar{\psi}_k\rangle$ as a linear combination of other states. Indeed, in the continuum, we can apply [Fact 9](#) twice to obtain $\hat{x}^2 |\Psi_k\rangle = k(k-1) |\Psi_{k-2}\rangle + k |\Psi_k\rangle + \frac{1}{4} |\Psi_{k+2}\rangle$. We write

$$\bar{x}^2 |\bar{\psi}_k\rangle = \alpha_1 |\bar{\psi}_{k-2}\rangle + \alpha_2 |\bar{\psi}_k\rangle + \alpha_3 |\bar{\psi}_{k+2}\rangle + \beta |\psi\rangle. \quad (23)$$

By [Fact 4](#), we have $|\alpha_1 - k(k-1)| \leq \exp(-\gamma M)$, $|\alpha_2 - k| \leq \exp(-\gamma M)$, and $|\alpha_3 - 1/4| \leq \exp(-\gamma M)$. Similarly, we have

$$\left| \langle \bar{\psi}_k | \bar{x}^4 |\bar{\psi}_k\rangle - \langle \Psi_k | \hat{x}^4 |\Psi_k\rangle \right| \leq \exp(-\gamma M).$$

This implies that

$$(\alpha_1^2 - k^2(k-1)^2) + (\alpha_2^2 - k^2) + \left(\alpha_1^2 - \frac{1}{16} \right) + \beta^2 \leq \exp(-\gamma M).$$

We can factor the left hand side as

$$(\alpha_1 + k(k-1))(\alpha_1 - k(k-1)) + (\alpha_2 + k)(\alpha_2 - k) + (\alpha_3 + 1/4)(\alpha_3 - 1/4) + \beta^2$$

This factorization gives us the bound

$$\begin{aligned} |\beta|^2 &\leq \exp(-\gamma M) + (\alpha_1 + k(k-1)) |\alpha_1 - k(k-1)| + (\alpha_2 + k) |\alpha_2 - k| + (\alpha_3 + 1/4) |\alpha_3 - 1/4| \\ &\leq \exp(-\gamma M) + (2k(k-1) + \exp(-\gamma M)) \exp(-\gamma M) \\ &\quad + (2k + \exp(-\gamma M)) \exp(-\gamma M) + (1/2 + \exp(-\gamma M)) \exp(-\gamma M) \\ &\leq 3 \left(k^2 + \frac{1}{16} \right) \exp(-\gamma M) + \exp(-\gamma M) \leq 4k^2 \exp(-\gamma M), \end{aligned}$$

so $|\beta| \leq 2k \exp(-\gamma M/2)$.

To bound the term $|\langle \psi_k | \bar{x}^2 \bar{p}^2 \bar{x}^2 | \psi_\ell \rangle - \langle \Psi_k | \hat{x}^2 \hat{p}^2 \hat{x}^2 | \Psi_\ell \rangle|$ we first use the canonical comutator relation to expand $\bar{x}^2 \bar{p}^2 \bar{x}^2 = \bar{x}^4 \bar{p}^2 - 4i\bar{x}^3 \bar{p} - 2\bar{x}^2 + \bar{x}^2 \Delta''$ where $\Delta'' = \bar{p}^2 \bar{x}^2 - (\bar{x}^2 \bar{p}^2 - 4i\bar{x} \bar{p} - 2I)$. After applying triangle inequality by splitting on the discrete minus the continuum operators, the same argument as the other terms implies an $O(\exp(-\gamma M))$ bound on the other 3 terms. The only non-trivial term here is $\bar{x}^2 \Delta''$.

To bound this term, we expand $|\langle \bar{\psi}_k | \bar{x}^2 \bar{p}^2 \bar{x}^2 | \bar{\psi}_\ell \rangle|$ using [\(23\)](#). We get

$$\left| \left(\alpha_1 \langle \bar{\psi}_{k-2} | + \alpha_2 \langle \bar{\psi}_k | + \alpha_3 \langle \bar{\psi}_{k+2} | + \beta \langle \psi | \right) \Delta'' | \bar{\psi}_\ell \rangle \right| \leq \exp(-\gamma M) + |\beta| \|\Delta''\|$$

But we know $|\beta| \leq 2k \exp(-\gamma M/2)$ and $\|\Delta''\| \leq 7M^2$. Overall, we have that

$$\left| \langle \bar{\psi}_k | \bar{x}^2 \bar{p}^2 \bar{x}^2 | \bar{\psi}_\ell \rangle - \langle \Psi_k | \hat{x}^2 \hat{p}^2 \hat{x}^2 | \Psi_\ell \rangle \right| \leq 40kM^2 \exp(-\gamma M/2).$$

Putting everything together, $\|\Pi_{N'} \Delta \Pi_{N'}\| \leq \exp(-\gamma M/3)$ for all M sufficiently large.

To see the second point, we simply write $\Delta = \bar{x}^4 \bar{p}^2 - 2\bar{x}^2 \bar{p}^2 \bar{x}^2 + \bar{p}^2 \bar{x}^4 - 8i\bar{x}^2$. Now, $\|\bar{x}\| = \|\bar{p}\| = \sqrt{\frac{\pi M}{2}}$. Thus we have

$$\|\Delta\| \leq \|\bar{x}^4 \bar{p}^2\| + 2 \|\bar{x}^2 \bar{p}^2 \bar{x}^2\| + \|\bar{p}^2 \bar{x}^4\| + 8 \|\bar{x}^2\| \quad (24)$$

$$= 4 \cdot \left(\frac{\pi M}{2} \right)^3 + 8 \left(\frac{\pi M}{2} \right) \quad (25)$$

$$\leq 16M^3 + 4\pi M \leq 17M^3. \quad \square$$

Our strategy to bound each level of the nested commutator tail will be to break the t -th order commutator into a noncommutative polynomial of \bar{x}^2 and Δ . First, we provide a bound on each monomial appearing in this expansion.

Lemma 11. *Let $a + b = t$. For all M sufficiently large,*

$$\left\| \Pi_N \bar{x}^{2a} \Delta \bar{x}^{2b} \Pi_N \right\| \leq \begin{cases} (51M^3 + 1) \cdot (2N)^t \cdot \exp(-\gamma M/9) & t \leq (N' - N)/2 \\ (51M^3 + 1) \cdot (2N)^t & t > (N' - N)/2 \end{cases}$$

Proof. Our strategy will be to introduce the projector $\Pi_{N'}$ onto the “medium energy” subspace spanned by the first N' eigenstates of \bar{H} . We write

$$\left\| \Pi_N \bar{x}^{2a} \Delta \bar{x}^{2b} \Pi_N \right\| = \left\| \Pi_N \bar{x}^{2a} (\Pi_{N'} + (I - \Pi_{N'})) \Delta (\Pi_{N'} + (I - \Pi_{N'})) \bar{x}^{2b} \Pi_N \right\|$$

We can break this up into four terms using the triangle inequality:

$$T_1 = \left\| \Pi_N \bar{x}^{2a} \Pi_{N'} \right\| \cdot \left\| \Pi_{N'} \Delta \Pi_{N'} \right\| \cdot \left\| \Pi_{N'} \bar{x}^{2b} \Pi_N \right\| \quad (26)$$

$$T_2 = \left\| \Pi_N \bar{x}^{2a} (I - \Pi_{N'}) \right\| \cdot \left\| (I - \Pi_{N'}) \Delta \Pi_{N'} \right\| \cdot \left\| \Pi_{N'} \bar{x}^{2b} \Pi_N \right\| \quad (27)$$

$$T_3 = \left\| \Pi_N \bar{x}^{2a} \Pi_{N'} \right\| \cdot \left\| \Pi_{N'} \Delta (I - \Pi_{N'}) \right\| \cdot \left\| (I - \Pi_{N'}) \bar{x}^{2b} \Pi_N \right\| \quad (28)$$

$$T_4 = \left\| \Pi_N \bar{x}^{2a} (I - \Pi_{N'}) \right\| \cdot \left\| (I - \Pi_{N'}) \Delta (I - \Pi_{N'}) \right\| \cdot \left\| (I - \Pi_{N'}) \bar{x}^{2b} \Pi_N \right\| \quad (29)$$

The overall norm is upper bounded by $T_1 + T_2 + T_3 + T_4$. We first consider T_1 . Applying [Lemma 10](#), we have

$$T_1 \leq (2N)^a \cdot \exp(-\gamma M/3) \cdot (2N)^b \leq (2N)^t \cdot \exp(-\gamma M/3).$$

For T_2, T_3, T_4 , we will use the trivial bound on the norm Δ – that is, we won’t use the projector. Applying [Lemma 8](#) and [Lemma 10](#), we have

$$T_2 \leq \exp(-\gamma M/9) \cdot 17M^3 \cdot (2N)^b \leq 17M^3 \cdot (2N)^t \cdot \exp(-\gamma M/9)$$

whenever $t \leq (N' - N)/2$. When $t > (N' - N)/2$ we recover the bound

$$T_2 \leq (2N)^a \cdot 17M^3 \cdot (2N)^b \leq 17M^3 \cdot (2N)^t$$

By symmetry, we recover the same bounds on T_3 . Finally, we use similar techniques to obtain the bounds

$$T_4 \leq \exp(-\gamma M/9) \cdot 17M^3 \cdot \exp(-\gamma M/9) \leq 17M^3 \cdot \exp(-2\gamma M)$$

when $t \leq (N' - N)/2$ and

$$T_2 \leq (2N)^a \cdot 17M^3 \cdot (2N)^b \leq 17M^3 \cdot (2N)^t$$

when $t > (N' - N)/2$. □

Next we bound the t -th order commutator by applying the triangle inequality along with the monomial bounds above.

Lemma 12. *For all M sufficiently large,*

$$\left\| \Pi_N [\bar{x}^2, \Delta]_t \Pi_N \right\| \leq \begin{cases} (51M^3 + 1) \cdot (4N)^t \cdot \exp(-\gamma M/9) & t \leq (N' - N)/2 \\ (51M^3 + 1) \cdot (4N)^t & t > (N' - N)/2 \end{cases}$$

Proof. We can expand

$$[\bar{x}^2, \Delta]_t = \sum_{s=0}^t \binom{t}{s} (-1)^s \bar{x}^{2s} \Delta \bar{x}^{2(t-s)}.$$

Applying the triangle inequality, we have

$$\|\Pi_N [\bar{x}^2, \Delta]_t \Pi_N\| \leq \sum_{s=0}^t \binom{t}{s} \|\Pi_N \bar{x}^{2s} \Delta \bar{x}^{2(t-s)} \Pi_N\|.$$

We use the identity $\sum_{s=0}^t \binom{t}{s} = 2^t$ and [Lemma 11](#) to obtain the result. \square

Before proving our bounds on the nested commutator tail of \bar{x}^2 and \bar{p} , we recall a useful fact about the tail of the power series of the exponential function.

Proposition 13.

$$\sum_{k=3a}^{\infty} \frac{a^k}{k!} \leq \exp(-a/4).$$

Proof. The sum is exactly e^a times the tail of the Poisson distribution with parameter a . Thus, from standard formulae for Poisson tail bounds, we have

$$\sum_{k=3a}^{\infty} \frac{a^k}{k!} \leq e^a \Pr[\text{Poisson}_a \geq 3a] \leq e^a \exp(-3a \ln 3 + 2a) \leq \exp(-3(\ln 3 - 1)a) \leq \exp(-a/4). \quad \square$$

We are now ready to prove the key technical ingredient of our fast-forwarding algorithm: that the higher-order nested commutators of \bar{x} and \bar{p} fall off sufficiently fast.

Theorem 14. *Choose $N = \gamma M / (40 \log(2M))$. Then*

$$\left\| \Pi_N \left(\sum_{t=3}^{\infty} \frac{1}{t!} [\bar{x}^2, \bar{p}^2]_t \right) \Pi_N \right\| \leq \exp(-\gamma N/2).$$

Proof. We observe that $[\bar{x}^2, \bar{p}^2]_2 = \Delta + 8i\bar{x}^2$. Thus, for $t \geq 3$, we can write

$$[\bar{x}^2, \bar{p}^2]_t = [\bar{x}^2, \Delta]_{t-2}.$$

Thus,

$$\left\| \Pi_N \sum_{t=3}^{\infty} \frac{[\bar{x}^2, \bar{p}^2]_t}{t!} \Pi_N \right\| = \left\| \Pi_N \sum_{t=3}^{\infty} \frac{[\bar{x}^2, \bar{p}^2]_{t-2}}{t!} \Pi_N \right\| \tag{30}$$

$$\leq \sum_{t=1}^{\infty} \frac{\|\Pi_N [\bar{x}^2, \bar{p}^2]_t \Pi_N\|}{(t+2)!} \tag{31}$$

$$\leq (51M^3 + 1) \left(e^{-\gamma M/9} \cdot \sum_{t=1}^{(N'-N)/2} \frac{(4N)^t}{t!} + \sum_{t=(N'-N)/2+1}^{\infty} (4N)^t \right) \tag{Lemma 12}$$

$$\leq (51M^3 + 1) \left(e^{-\gamma M/9} \cdot \sum_{t=0}^{\infty} \frac{(4N)^t}{t!} + \sum_{t=12N}^{\infty} (4N)^t \right) \tag{32}$$

$$\leq (51M^3 + 1) (e^{4N-\gamma M/9} + e^{-N}) \tag{Proposition 13}$$

$$\leq 2(51M^3 + 1)e^{-\gamma N} \leq e^{-\gamma N/2}. \quad \square$$

As a consequence of our proof technique, the analogous statement holds if we swap position and momentum in the nested commutator.

Corollary 15. *Choose $N = \gamma M / (40 \log(2M))$. Then*

$$\left\| \Pi_N \left(\sum_{t=3}^{\infty} \frac{1}{t!} [\bar{p}^2, \bar{x}^2]_t \right) \Pi_N \right\| \leq \exp(-\gamma N/2).$$

Proof. The bounds in the proofs of [Lemmas 8, 10](#) and [12](#) remain unchanged when swapping position and momentum. Thus, following the proof of [Theorem 14](#), we obtain the exact same bound on the projected higher-order nested commutators of \bar{p}^2 and \bar{x}^2 . \square

Theorem 16. *Choose $N = \gamma M / (40 \log(2M))$. Then*

$$\left\| \Pi_N \left(\sum_{t=2}^{\infty} \frac{1}{t!} [\bar{p}^2, \{\bar{x}, \bar{p}\}]_t \right) \Pi_N \right\| \leq \exp(-\gamma N/2).$$

Just as in the proof of [Corollary 15](#), the proofs of [Lemmas 8, 11](#) and [12](#) hold with the same scaling if \bar{p}^2 is nested instead of \bar{x}^2 . What remains is to bound the new defect $\Delta' = [\bar{p}^2, \{\bar{x}, \bar{p}\}] - 4i\bar{p}^2 = \bar{p}^2\bar{x}\bar{p} + \bar{p}^3\bar{x} - 4i\bar{p}^2$. In the continuum, the corresponding operator is 0, and we now prove an analogous statement to [Lemma 10](#) for this defect.

Lemma 17. *Let M be sufficiently large.*

1. $\|\Pi_N \Delta' \Pi_N\| \leq \exp(-\gamma M/2)$.
2. $\|\Delta'\| \leq 5M^2$

Proof. The proof will be very similar to that of [Lemma 10](#). First we show the the second point:

$$\|\Delta'\| \leq \|\bar{p}^2\bar{x}\bar{p}\| + \|\bar{p}^3\bar{x}\| + 4\|\bar{p}^2\| \leq 2\left(\frac{\pi M}{2}\right)^2 + 4\left(\frac{\pi M}{2}\right) \leq 5M^2$$

whenever M is sufficiently large. \square

To bound this quantity we will need the following bound.

Lemma 18. $\left| \langle \bar{\psi}_k | \bar{p}^2 \bar{x} \bar{p} | \bar{\psi}_l \rangle - \langle \Psi_k | \hat{p}^2 \hat{x} \hat{p} | \Psi_l \rangle \right| \leq 10 \exp(-\gamma M)$

Proof. We use the canonical commutation relation to derive $\bar{p}^2 \bar{x} \bar{p} = \bar{p}^3 \bar{x} - i\bar{p}^2 + \bar{p}^2 \Delta'$ where $\Delta' = \bar{p} \bar{x} - iI - \bar{x} \bar{p}$. Now, using the [Fact 4](#) we can bound the first two terms after applying triangle inequality. Thus, the only remaining task is to bound $|\langle \psi_k | \bar{p}^2 \Delta' | \psi_l \rangle|$ is small.

To do this we use the expansion,

$$\bar{p}^2 |\bar{\psi}_k\rangle = \alpha_1 |\bar{\psi}_{k-2}\rangle + \alpha_2 |\bar{\psi}_k\rangle + \alpha_3 |\bar{\psi}_{k+2}\rangle + \beta |\psi\rangle \quad (33)$$

where $|\beta| \leq 2 \exp(-\gamma M)$, as in the proof of [Lemma 10](#). Using this we can rewrite the above as

$$\left| \left(\alpha_1 \langle \bar{\psi}_{k-2} | + \alpha_2 \langle \bar{\psi}_k | + \alpha_3 \langle \bar{\psi}_{k+2} | + \beta \langle \psi | \right) \Delta' | \bar{\psi}_l \right| \leq 5 \exp(-\gamma M) + 7M^2 \exp(-\gamma M) \quad (34)$$

where the second term is just bounded using $|\beta| \|\Delta'\|$. \square

Now we are ready to prove [Theorem 6](#). We recall it below.

Theorem 6. For any constants c_1, c_2 such that $\max(|c_1|, |c_2|) \leq 1$, and $N = \gamma M / (40 \log(2M))$, we have

$$\begin{aligned} \left\| \Pi_N \left(\sum_{t=3}^{\infty} \frac{1}{t!} [c_1 \bar{x}^2, c_2 \bar{p}^2]_t \right) \Pi_N \right\| &\leq \exp(-\gamma N/2). \\ \left\| \Pi_N \left(\sum_{t=3}^{\infty} \frac{1}{t!} [c_1 \bar{p}^2, c_2 \bar{x}^2]_t \right) \Pi_N \right\| &\leq \exp(-\gamma N/2) \\ \left\| \Pi_N \left(\sum_{t=2}^{\infty} \frac{1}{t!} [c_1 \bar{p}^2, c_2 \{\bar{x}, \bar{p}\}]_t \right) \Pi_N \right\| &\leq \exp(-\gamma N/2). \end{aligned}$$

Proof of Theorem 6. Notice that the bound in Lemma 12 holds when replacing the operator \bar{x} (or \bar{p}) with $c\bar{x}$ where $|c| \leq 1$. Nothing else changes in the proofs. \square

4 Quantum Hermite transform

Building on our fast-forwarding result, we can implement an efficient QHT if we can implement the state preparation, filtering, and QPE algorithms efficiently. We now discuss these steps and then present the algorithm. The main result of this section is the formal version of Theorem 2.

Theorem 19 (Quantum Hermite transform, formal). *Let N be the dimension for the quantum Hermite transform and $\varepsilon > 0$ be the error. Then, there exists a quantum circuit that performs the transformation*

$$\sum_{n=0}^{N-1} \alpha_n |n\rangle \mapsto \sum_{n=0}^{N-1} \alpha_n |\psi_n\rangle \quad (35)$$

within additive error ε , where the coefficients α_n are arbitrary and satisfy $\sum_{n=0}^{N-1} |\alpha_n|^2 = 1$. The quantum circuit acts on a Hilbert space of dimension $M = \text{poly}(N, 1/\varepsilon)$ and, if $N > \log(1/\varepsilon)$, the complexity of the quantum circuit is

$$\mathcal{O}\left((\log N + \log(1/\varepsilon))^3 \times \log(1/\varepsilon)\right). \quad (36)$$

This result is based on the state preparation steps outlined in Section 2. More generally, we can choose any dimension $M \geq cN^{9/4}/\varepsilon^{13/4}$, where $c > 0$ is some constant. The cost of the QHT is then $\mathcal{O}(\log^3 M \times \log(1/\varepsilon))$, and choosing $M = \text{poly}(N, 1/\varepsilon)$ gives Theorem 19.

4.1 State preparation

We first show how to efficiently prepare a set of quantum states that have constant overlap with the Hermite states $|\psi_n\rangle$ of (2) in a low-energy subspace of interest. We will then use fixed-point amplitude amplification to increase the overlap with $|\psi_n\rangle$ arbitrarily. Our strategy is based on the Plancherel-Rotach approximation, which approximates the Hermite functions $\psi_n(x)$ in the ‘oscillatory’ region, specified by the domain $|x| < x_{\text{tp}} := \sqrt{2n+1}$.

Lemma 20 (Plancherel-Rotach asymptotics for Hermite functions, Thm. 8.22.9 [Sze39]). *Let $\varphi(x) = \arccos(x/\sqrt{2n+1})$. Let $c > 0$ be any fixed positive constant and define the domain*

$$\mathcal{D}_c = \{x \in \mathbb{R} : |x| < \sqrt{2n+1} \text{ and } c \leq \varphi(x) \leq \pi - c\}. \quad (37)$$

Then, for each $n > 0$ and all $x \in \mathcal{D}_c$, we have

$$\psi_n(x) = \frac{(-1)^n 2^{\frac{1}{4}}}{\pi^{\frac{1}{2}} n^{\frac{1}{4}}} \frac{1}{\sqrt{\sin \varphi(x)}} \left(\sin \left[\left(\frac{n}{2} + \frac{1}{4} \right) (\sin(2\varphi(x)) - 2\varphi(x)) + \frac{3\pi}{4} \right] + \mathcal{O}\left(\frac{1}{n}\right) \right). \quad (38)$$

In [Appendix C](#) we describe other properties of these approximations. For the case $n = 0$, it will suffice to approximate $\psi_0(x)$ by a constant like $\psi_0(0) \approx .75$, assuring constant overlap.

Hence, the Hermite functions can be approximated by an oscillatory term and an amplitude that depends on x via $1/\sqrt{\sin(\varphi(x))}$, in the oscillatory region. This motivates the definition of a set of quantum states that have constant overlap with the finite-dimensional Hermite states $|\psi_n\rangle$ by considering, for example, a domain included in the oscillatory region and far from the ‘turning points’ $\pm x_{\text{tp}}$ where, for example, $|x| \leq \sqrt{(3/4)(2n+1)}$. In the following we disregard the phase $(-1)^n$ in the definition of $\psi_n(x)$ to ease the exposition.

Lemma 21 (Plancherel-Rotach states). *Let $N > 0$ be the dimension for the QHT and $\varepsilon > 0$ be the error. For all $0 \leq n \leq N - 1$, let*

$$\phi_n(x) := \frac{2^{\frac{1}{4}}}{\pi^{\frac{1}{2}} n^{\frac{1}{4}}} \frac{1}{\sqrt{\sin \varphi(x)}} \left(\sin \left[\left(\frac{n}{2} + \frac{1}{4} \right) (\sin(2\varphi(x)) - 2\varphi(x)) + \frac{3\pi}{4} \right] \right) \times g_n(x), \quad (39)$$

where $\varphi(x) := \arccos(x/\sqrt{2n+1})$, be the Plancherel-Rotach approximation of the n^{th} Hermite function. The function $g_n(x)$ is some smooth approximation to the indicator function and satisfies

$$g_n(x) := \begin{cases} 0 & \text{if } |x| \geq \sqrt{(3/4)(2n+1)} + 1/(10\sqrt{2n+1}), \\ 1 & \text{if } |x| \leq \sqrt{(3/4)(2n+1)}, \\ \in (0, 1) & \text{if } \sqrt{(3/4)(2n+1)} + 1/(10\sqrt{2n+1}) > |x| > \sqrt{(3/4)(2n+1)}. \end{cases} \quad (40)$$

For any $M > N$, define the M -dimensional ‘Plancherel-Rotach’ quantum states

$$|\phi_n\rangle := \left(\frac{2\pi}{M} \right)^{1/4} \sum_{j=-J(n)}^{J(n)-1} \phi_n(x_j) |j\rangle, \quad 0 \leq n \leq N - 1, \quad (41)$$

where $x_j := j\sqrt{2\pi/M}$ denotes the discretized space coordinate, and

$$J(n) := \left\lceil \sqrt{\frac{3}{4} \frac{(2n+1)M}{2\pi}} \right\rceil \quad (42)$$

is such that $J(n)\sqrt{2\pi/M} \approx \sqrt{(3/4)(2n+1)}$ and $J(n) < M/2$. Let $|\psi_n\rangle$ be Hermite states of [\(2\)](#), that is,

$$|\psi_n\rangle := \left(\frac{2\pi}{M} \right)^{1/4} \sum_{j=-M/2}^{M/2-1} \psi_n(x_j) |j\rangle, \quad 0 \leq n \leq N - 1. \quad (43)$$

Then, there exist constants $c > 0$ and $c' > 0$ such that, for all $M \geq c(N)^{9/4}/\varepsilon^{13/4}$ and all $0 \leq n \leq N - 1$, the overlap is

$$\langle \psi_n | \psi_n \rangle \geq c'. \quad (44)$$

For every such M there exists $N_{\text{high}} = \mathcal{O}(N/\varepsilon)$ satisfying $N < N_{\text{high}} < M$ and, for all $n \leq N - 1$,

$$\|\Pi_{>N_{\text{high}}} |\phi_n\rangle\|^2 \leq \varepsilon, \quad (45)$$

where $\Pi_{>N_{\text{high}}}$ is a ‘high-energy’ projector onto the subspace orthogonal to the subspace spanned by $\{|\psi_n\rangle\}_{0 \leq n \leq N_{\text{high}}}$. (Note that $N_{\text{high}} \ll M$ asymptotically.)

Proof. The quantum states $|\phi_n\rangle$ are suggested by the Plancherel-Rotach approximation of [Lemma 20](#). Asymptotically, they can be shown to be subnormalized for $n \leq N-1$ because we are cutting off the domain by choosing $J(n) < M/2$. Our goal is then to carry the Plancherel-Rotach approximation to the discrete space, which involves approximating integrals by finite sums. We also note that in the subspace of interest, where $n \leq N-1$, we will satisfy $n \ll M$ asymptotically.

For each $n \leq N-1$, we are selecting as the domain of interest one where $|x| \leq x_{\max} := \sqrt{(3/4)(2n+1)}$. In the definition of $|\phi_n\rangle$, we let x_j run up to $\pm J(n)\sqrt{2\pi/M}$, and our choice of $J(n)$ is such that $|x_j|$ is upper bounded by x_{\max} up to an asymptotically small correction. This domain is purposely far from, and does not include, the turning points $\pm x_{\text{tp}} = \pm\sqrt{(2n+1)}$ where the Plancherel-Rotach approximations are known to fail (e.g., $\varphi(x) = 0$ at $x = x_{\text{tp}}$).

We will start by obtaining some properties of these approximations in the domain of interest. Note that rather than considering [Lemma 20](#) directly in this domain, we are modifying the approximations slightly to avoid issues when considering the momentum operator and the Fourier transform. For example, rather than assuming the functions to be exactly 0 for all x such that $|x| > x_{\max}$ and oscillating otherwise, we introduced smooth envelope functions $g_n(x)$ in the definition with the following properties (for each $n \geq 0$):

$$g_n(x) := \begin{cases} 0 & \text{if } |x| \geq x_{\max} + 1/(10\sqrt{2n+1}), \\ 1 & \text{if } |x| \leq x_{\max}, \\ \in (0,1) & \text{if } x_{\max} + 1/(10\sqrt{2n+1}) > |x| > x_{\max}. \end{cases} \quad (46)$$

There is nothing special about the term $1/(10\sqrt{2n+1})$, other than it still guarantees the relevant x to be far from the turning points, and that the magnitudes of the derivatives of $g_n(x)$ can be properly bounded. A good choice for these functions is given in Ref. [\[Som19\]](#) and obtained by convolving the indicator function with the bump function. Formally, if $\delta := 1/(20\sqrt{2n+1})$, these are the convolutions

$$g_n(x) := \frac{2a}{\delta} \int_{-x_{\max}-\delta}^{x_{\max}+\delta} dx' \exp\left(-\frac{1}{1-4(x'-x)^2/\delta^2}\right) \quad (47)$$

The constant is $a \approx 2.25$. We will use these to prove [Lemma 21](#), but note that other choices can also work. Besides the properties in [\(46\)](#), they also satisfy $\frac{d}{dx}g_n(x) = \frac{d^2}{dx^2}g_n(x) = 0$ for $|x| > x_{\max} + 1/(10\sqrt{2n+1})$ and $|x| < x_{\max}$. Also, $|\frac{d}{dx}g_n(x)| = \mathcal{O}(\sqrt{2n+1})$ and $|\frac{d^2}{dx^2}g_n(x)| = \mathcal{O}(2n+1)$. From now on the domain where $|x| \leq x_{\max} + 1/(10\sqrt{2n+1})$ will be referred to as the ‘domain of interest’.

We will first establish the desired properties by working in the continuum, and use the following properties of the relevant functions. In the domain of interest, the Hermite functions satisfy $|\psi_n(x)| = \mathcal{O}(1/n^{1/4})$ and we can use the property $\frac{d}{dx}\psi_n(x) = \frac{1}{\sqrt{2}}(\sqrt{n}\psi_{n-1}(x) - \sqrt{n+1}\psi_{n+1}(x))$ to show that $|\frac{d}{dx}\psi_n(x)| = \mathcal{O}(n^{1/4})$, and Schrödinger equation $\frac{d^2}{dx^2}\psi_n(x) = (x^2 - (2n+1))\psi_n(x)$ to show that $|\frac{d^2}{dx^2}\psi_n(x)| = \mathcal{O}(n^{3/4})$. According to [Lemma 20](#), we have $\phi_n(x) = \psi_n(x) + \mathcal{O}(1/n^{5/4})$ in this domain. Also, we can use the bounds in [Appendix C](#) and the chain rule for $\phi_n(x) = \tilde{\phi}_n(x) \times g_n(x)$ to determine $|\phi_n(x)| = \mathcal{O}(1/n^{1/4})$, $|\frac{d}{dx}\phi_n(x)| = \mathcal{O}(n^{1/4})$, and $|\frac{d^2}{dx^2}\phi_n(x)| = \mathcal{O}(n^{3/4})$ in the domain of interest.

These properties allow us to establish a lower bound on the overlap:

$$\int_{-\infty}^{\infty} dx \psi_n(x) \phi_n(x) = \int_{-x_{\max}-1/(10\sqrt{2n+1})}^{x_{\max}+1/(10\sqrt{2n+1})} dx \psi_n(x) \phi_n(x) \quad (48)$$

$$= \int_{-x_{\max}-1/(10\sqrt{2n+1})}^{x_{\max}+1/(10\sqrt{2n+1})} dx \psi_n(x) (\psi_n(x) + \mathcal{O}(1/n^{5/4})) \quad (49)$$

$$= \int_{-x_{\max}}^{x_{\max}} dx |\psi_n(x)|^2 + \mathcal{O}(1/(n+1/2)) . \quad (50)$$

In addition,

$$\int_{-x_{\max}}^{x_{\max}} dx |\psi_n(x)|^2 = 1 - 2 \int_{x_{\max}}^{\infty} dx |\psi_n(x)|^2 \quad (51)$$

$$\geq 1 - \frac{2}{(x_{\max})^2} \int_{x_{\max}}^{\infty} dx x^2 |\psi_n(x)|^2 \quad (52)$$

$$\geq 1 - \frac{2}{(x_{\max})^2} \int_0^{\infty} dx x^2 |\psi_n(x)|^2 \quad (53)$$

$$= 1 - \frac{1}{2(x_{\max})^2} (2n+1) \quad (54)$$

$$= 1/3 . \quad (55)$$

Hence, the overlap is lower bounded by $1/3 + \mathcal{O}(1/n)$. Numerical calculations show that this overlap actually approximates $2/3$ and remains close to $2/3$ for all $n \geq 0$.

Next, we show that the functions $\phi_n(x)$ have negligible overlap with the high-energy sector, defined by some N_{high} . This proof is the one that will use the smoothness property of $g_n(x)$ (i.e., a bounded second derivative); otherwise, a sharp cutoff could result in high energies. Recall that in the continuum, the QHO Hamiltonian is $\frac{1}{2}(-\frac{d^2}{dx^2} + x^2)$. The expected value of x^2 on $\phi_n(x)$, corresponding to the potential term, satisfies

$$\int_{-\infty}^{\infty} dx x^2 |\phi_n(x)|^2 \leq \int_{-x_{\max}}^{x_{\max}} dx x^2 |\phi_n(x)|^2 \quad (56)$$

$$= \int_{-x_{\max}}^{x_{\max}} dx x^2 |\psi_n(x) + \mathcal{O}(1/n^{5/4})|^2 \quad (57)$$

$$= \int_{-x_{\max}}^{x_{\max}} dx x^2 |\psi_n(x)|^2 + \mathcal{O}((x_{\max})^3/n^{3/2}) \quad (58)$$

$$= \int_{-x_{\max}}^{x_{\max}} dx x^2 |\psi_n(x)|^2 + \mathcal{O}(1) , \quad (59)$$

and we also know for the Hermite functions

$$\int_{-x_{\max}}^{x_{\max}} dx x^2 |\psi_n(x)|^2 \leq \int_{-\infty}^{\infty} dx x^2 |\psi_n(x)|^2 = n + 1/2 . \quad (60)$$

It follows that

$$\int_{-\infty}^{\infty} dx x^2 |\phi_n(x)|^2 = \mathcal{O}(n + 1/2) . \quad (61)$$

The expected value of the kinetic term satisfies

$$- \int_{-\infty}^{\infty} dx \phi_n(x) \frac{d^2}{dx^2} \phi_n(x) = - \int_{-x_{\max}-1/(10\sqrt{2n+1})}^{x_{\max}+1/(10\sqrt{2n+1})} dx \phi_n(x) \frac{d^2}{dx^2} \phi_n(x) \quad (62)$$

$$= \mathcal{O}(n + 1/2) , \quad (63)$$

where we used the above properties of $\phi_n(x)$. It follows that the energy given by these functions, which is the expectation of the QHO Hamiltonian on $\phi_n(x)$, satisfies

$$\mathbb{E} \left[\frac{1}{2} \left(-\frac{d^2}{dx^2} + x^2 \right) \right] \leq C(n + 1/2) , \quad (64)$$

for some $C > 0$ that can be determined. We can then use Markov's inequality to bound the support of $\phi_n(x)$ in the high-energy space, spanned by Hermite functions with $n' > N_{\text{high}}$; that is

$$\sum_{n'=N_{\text{high}}+1}^{\infty} \left(\int_{-\infty}^{\infty} dx \phi_n(x) \psi_{n'}(x) \right)^2 \leq \frac{C(n + 1/2)}{N_{\text{high}} + 1/2} . \quad (65)$$

We readily proved some desired features of the approximated Hermite functions $\phi_n(x)$ in the oscillatory domain of interest. Our next goal is to prove that the finite-dimensional Plancherel-Rotach states of (41) satisfy similar properties: their overlaps with the discrete Hermite states $|\psi_n\rangle$ is bounded by a constant, and their support on the high-energy subspace can be arbitrarily bounded. We will obtain these results via approximations of integrals by finite sums. We will make repeatedly use of a standard trapezoidal rule:

$$\left| \int_a^b dx f(x) - h \sum_{k=1}^M \frac{f(x_{k-1}) + f(x_k)}{2} \right| \leq \frac{(b-a)h^2}{12} \max_{x \in (a,b)} \left| \frac{d^2}{dx^2} f(x) \right| . \quad (66)$$

Here h is the size of the discretization, $M = (b-a)/h$, and $x_k = a + kh$. While this rule will suffice because the scaling of the algorithm is only logarithmic in the dimension, we note that improved results could be obtained with a detailed analysis that uses exponentially convergent trapezoidal rules, since the functions are smooth. Nevertheless, we follow the standard trapezoidal rule to simplify the proof.

Consider the overlap

$$\langle \psi_n | \phi_n \rangle = \left(\frac{2\pi}{M} \right)^{1/2} \sum_{j=-M/2}^{M/2} \psi_n(x_j) \phi_n(x_j) , \quad (67)$$

which approximates (48) using a discretization of size $\sqrt{2\pi/M}$. Indeed, using the trapezoidal rule above we can show that $\langle \psi_n | \phi_n \rangle \approx \int_{-\infty}^{\infty} dx \psi_n(x) \phi_n(x)$ within additive error

$$\mathcal{O} \left(\frac{n + 1/2}{M} \right) \quad (68)$$

since $\phi_n(x)$ is zero for $|x| \geq x_{\text{max}} + 1/(10\sqrt{2n+1})$. For this we used the properties of the functions to show

$$\left| \frac{d^2}{dx^2} (\psi_n(x) \phi_n(x)) \right| \leq \left| \frac{d^2}{dx^2} \psi_n(x) \phi_n(x) \right| + 2 \left| \frac{d}{dx} \psi_n(x) \frac{d}{dx} \phi_n(x) \right| + \left| \psi_n(x) \frac{d^2}{dx^2} \phi_n(x) \right| \quad (69)$$

$$= \mathcal{O}(n^{1/2}) \quad (70)$$

Then, a lower bound to $\langle \psi_n | \phi_n \rangle$ is

$$1/3 + \mathcal{O} \left(\frac{n + 1/2}{M} \right) + \mathcal{O} \left(\frac{1}{n + 1/2} \right) . \quad (71)$$

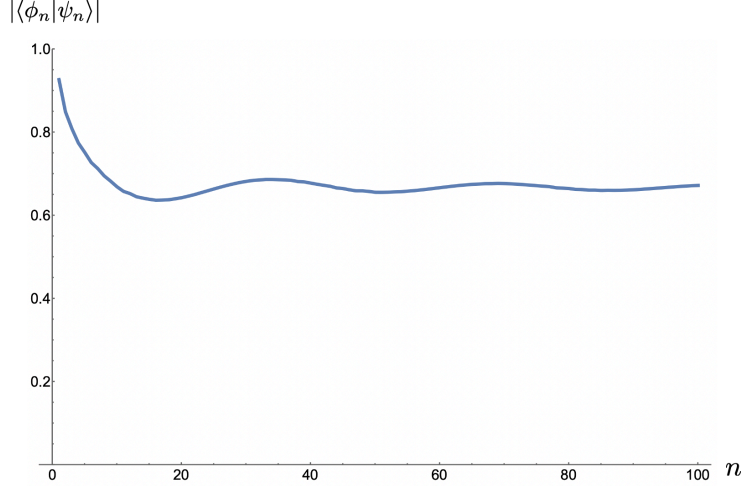


Figure 3: The overlap between the Plancherel-Rotach states and the Hermite states for dimension $M = 10^5$ and $0 \leq n \leq 100$. The overlap approaches $2/3$, which corresponds to the probability mass of the Hermite functions in the domain $|x| \leq \sqrt{(3/4)(2n+1)}$.

Note that we obtained a constant lower bound in the asymptotic regime, which suffices for our goal of the efficient Hermite transform (i.e., we will always choose M large enough to make $(n+1/2)/M$ very small), but a suitable value of $c > 0$ in (44) for all $n \geq 0$ can be obtained with a detailed analysis. Indeed, numerical simulations show that this overlap is approximately $2/3$ for many n 's. See Figure 3.

Our next goal is to prove that the support of the Plancherel-Rotach states $|\phi_n\rangle$, where $0 \leq n \leq N-1$, is arbitrarily small in the subspace of the discrete QHO states specified by an $N_{\text{high}} > N$. In the continuum we already proved that, expressing $\phi_n(x) = \sum_{n'=0}^{\infty} \alpha_{n,n'} \psi_{n'}(x)$, then

$$\sum_{n' > N_{\text{high}}} |\alpha_{n,n'}|^2 \leq C \frac{n+1/2}{N_{\text{high}}+1/2}. \quad (72)$$

This is equivalent to (65) since Hermite functions are orthogonal. Consider now $|\phi_n\rangle$ and $|\psi_{n'}\rangle$ for $0 \leq n \leq N-1$ and $0 \leq n' \leq N_{\text{high}}$. Note that, in general for all $x \in \mathbb{R}$,

$$|\psi_{n'}(x)| \lesssim 1.086, \quad \left| \frac{d}{dx} \psi_{n'}(x) \right| \leq c(2n'+1)^{1/4}, \quad \left| \frac{d^2}{dx^2} \psi_{n'}(x) \right| \leq c'(2n'+1)^{3/4}. \quad (73)$$

for some constants $c > 0$ and $c' > 0$. Since n' can be larger than n , then we cannot use improved bounds for these functions. It follows that

$$\left| \frac{d^2}{dx^2} (\psi_{n'}(x) \phi_n(x)) \right| = \mathcal{O} \left((N_{\text{high}} + 1/2)^{3/4} \right). \quad (74)$$

Then, using the trapezoidal rule we have $\langle \psi_{n'} | \phi_n \rangle \approx \int_{-\infty}^{\infty} dx \psi_{n'}'(x) \phi_n(x)$ within additive error

$$\mathcal{O} \left(\frac{(n+1/2)^{1/2} (N_{\text{high}} + 1/2)^{3/4}}{M} \right) = \mathcal{O} \left(\frac{(N_{\text{high}} + 1/2)^{5/4}}{M} \right). \quad (75)$$

since we only need to integrate in the domain of interest. Then,

$$\langle \psi_{n'} | \phi_n \rangle = \alpha_{n,n'} + \mathcal{O} \left(\frac{(N_{\text{high}} + 1/2)^{5/4}}{M} \right). \quad (76)$$

The trapezoidal rule also implies

$$\| |\phi_n\rangle \|^2 = \int_{-x_{\text{max}} - 1/(10\sqrt{2n+1})}^{x_{\text{max}} + 1/(10\sqrt{2n+1})} dx |\phi_n(x)|^2 + \mathcal{O} \left(\frac{(n + 1/2)^{5/4}}{M} \right) \quad (77)$$

$$= \sum_{n'=0}^{\infty} |\alpha_{n,n'}|^2 + \mathcal{O} \left(\frac{(n + 1/2)^{5/4}}{M} \right), \quad (78)$$

since the prior bounds imply $|\frac{d^2}{dx^2} \phi_n(x)| = \mathcal{O}(n^{3/4})$ in the domain of interest.

Let $M > N_{\text{high}} > N$. Consider the subspace spanned by $\{|\psi_n\rangle\}_{0 \leq n \leq N_{\text{high}}}$ and its orthogonal complement; both span \mathbb{C}^M . Let $\Pi_{>N_{\text{high}}}$ be the projector onto the latter. Without loss of generality we can write

$$|\phi_n\rangle = \sum_{n'=0}^{N_{\text{high}}} \beta_{n,n'} |\psi_{n'}\rangle + |\phi_n^\perp\rangle \quad (79)$$

where $|\phi_n^\perp\rangle = \Pi_{>N_{\text{high}}} |\phi_n\rangle$ is subnormalized and the amplitudes are $\sum_{n'=0}^{N_{\text{high}}} |\beta_{n,n'}|^2 \leq 1$. Note that $\langle \psi_{n'} | \phi_n \rangle = \beta_{n,n'} + \mathcal{O}(N_{\text{high}} \exp(-\Omega(M)))$ for $n' \leq N_{\text{high}}$. Our goal is to bound $\| |\phi_n^\perp\rangle \|$. Combining the prior results we have

$$\| |\phi_n^\perp\rangle \|^2 = \| |\phi_n\rangle \|^2 - \left\| \sum_{n'=0}^{N_{\text{high}}} \beta_{n,n'} |\psi_{n'}\rangle \right\|^2 \quad (80)$$

$$= \sum_{n'=0}^{\infty} |\alpha_{n,n'}|^2 + \mathcal{O} \left(\frac{(n + 1/2)^{5/4}}{M} \right) - \sum_{n'=0}^{N_{\text{high}}} |\beta_{n,n'}|^2 + \mathcal{O}(N_{\text{high}} \exp(-\Omega(M))) \quad (81)$$

$$= \sum_{n'=0}^{\infty} |\alpha_{n,n'}|^2 + \mathcal{O} \left(\frac{(n + 1/2)^{5/4}}{M} \right) - \sum_{n'=0}^{N_{\text{high}}} |\langle \psi_{n'} | \phi_n \rangle|^2 + \mathcal{O}((N_{\text{high}})^2 \exp(-\Omega(M))) \quad (82)$$

$$= \sum_{n'=0}^{\infty} |\alpha_{n,n'}|^2 + \mathcal{O} \left(\frac{(n + 1/2)^{5/4}}{M} \right) - \sum_{n'=0}^{N_{\text{high}}} |\alpha_{n,n'}|^2 + \mathcal{O} \left(N_{\text{high}} \frac{(N_{\text{high}} + 1/2)^{5/4}}{M} \right) \quad (83)$$

$$= \sum_{n' > N_{\text{high}}} |\alpha_{n,n'}|^2 + \mathcal{O} \left(\frac{N_{\text{high}}^{9/4}}{M} \right) \quad (84)$$

$$= \mathcal{O} \left(\frac{N + 1/2}{N_{\text{high}} + 1/2} \right) + \mathcal{O} \left(\frac{(N_{\text{high}} + 1/2)^{9/4}}{M} \right). \quad (85)$$

We dropped the term exponentially small in M since it is asymptotically subdominant. To establish $\| |\phi_n^\perp\rangle \|^2 = \mathcal{O}(\varepsilon)$ it suffices to choose $N_{\text{high}} = \Omega(N/\varepsilon)$ and $M = \Omega((N_{\text{high}})^{9/4}/\varepsilon)$. This shows (45) and completes the proof. \square

Efficient preparation of the Plancherel-Rotach states. Thus far we considered the Plancherel-Rotach states defined in (41) as good initial states to prepare the corresponding $|\psi_n\rangle$, since they have overlap bounded by a positive constant. For the quantum Hermite transform to be efficient, we need to show that these states can be efficiently prepared. Note that it suffices to produce $\mathcal{O}(\varepsilon)$ -approximations to the $|\phi_n\rangle$ since this will imply a QHT with error $\mathcal{O}(\varepsilon)$. Unfortunately, we cannot allow for a constant-error approximation to $|\phi_n\rangle$ because we need to make sure that the support of the state in the high-energy space is still bounded by $\mathcal{O}(\varepsilon)$.

Lemma 22 (Efficient state preparation). *Let $0 \leq n \leq N - 1$ and ε the error. Then there is a quantum circuit that performs the map*

$$|n\rangle \mapsto |n\rangle \frac{|\phi_n\rangle}{\| |\phi_n\rangle \|} \quad (86)$$

within error ε using $\mathcal{O}((\log N + \log(1/\varepsilon))^3)$ gates.

Proof. The states $|\phi_n\rangle$ admit a simple form, being a linear combination of basis states with amplitudes proportional to

$$A_n(x) := \frac{1}{\sqrt{\sin \varphi(x)}} \times g_n(x) = \frac{1}{\sqrt{1 - \frac{x^2}{2n+1}}} \times g_n(x) \quad (87)$$

and phases

$$\pm \Theta_n(x) := \pm \left[\left(\frac{n}{2} + \frac{1}{4} \right) \left(\sin(2\varphi(x) - 2\varphi(x)) + \frac{3\pi}{4} \right) \right], \quad (88)$$

where $\varphi(x) = \arccos(x/\sqrt{2n+1})$. That is, $\phi_n(x) \propto A_n(x)(e^{+i\Theta_n(x)} - e^{-i\Theta_n(x)})$. We will describe a method to prepare a state with one of these phases, say $+\Theta_n(x)$, and the linear combination can be obtained via a simple Hadamard gate. This is because, while $|\phi_n\rangle$ are subnormalized, they have norm bounded by a positive constant. There are several known state preparation methods that can be useful for our context. For example, we could repurpose the algorithm of conditional rotations [Zal98, GR02] and, to restrict the domain to within the oscillatory region we can use quantum rejection sampling [ORR12]. A more recent approach is that based on inequality testing in [SLSB19] and is the one we will follow here.

For each $0 \leq n \leq N - 1$, the states $|\phi_n\rangle$ are superpositions over basis states $|j\rangle$ where, in our convention, $-J(n) \leq j \leq J(n) - 1$, and $J(n)$ is described in Lemma 21. They are in the space \mathbb{C}^M , where the number of qubits is $m = \log_2 M$. To simplify the details of state preparation, we are going to use the standard convention where basis states are labeled as $\{|0\rangle, |1\rangle, \dots, |M-1\rangle\}$. As mentioned, we can go from one convention to the other via a cyclic permutation (see below). Initially, we will consider setting the amplitudes proportional to $A_n(x)$ and then we set the phases $e^{i\Theta_n(x)}$. For the amplitudes we assume access to an oracle **amp** that computes $A(x)$ with r bits of precision in an additional register. Note that $A(x)$ is bounded by a constant in the oscillatory region of interest. We are going to introduce ancillary registers in many steps, but the relevant parts are flagged by the states $|0\rangle$.

- Step 1: Given n , compute the smallest integer q that satisfies $2^q \geq 2J(n)$. Apply q Hadamard gates to map $|0\rangle^{\otimes m} \mapsto \frac{1}{\sqrt{2^q}} \sum_{j=0}^{2^q-1} |j\rangle$. Apply an inequality test to obtain $\frac{1}{\sqrt{2^q}} (\sum_{j=0}^{2J(n)-1} |j\rangle |0\rangle + \sum_{j=2J(n)}^{2^q-1} |j\rangle |1\rangle)$, which flags the relevant support.

- Step 2: Use **amp** and inequality test to perform the map $|j\rangle \mapsto |j\rangle |\bar{A}_n(x_j)\rangle \frac{1}{\sqrt{2^r}} (\sum_{z=0}^{\bar{A}_n(x_j)-1} |z\rangle |0\rangle + \sum_{\bar{A}_n(x_j)}^{2^r} |z\rangle |1\rangle)$, where $\bar{A}_n(x_j)$ is an r -bit approximation of $A_n(x_j)$ (rescaled by a constant).
- Step 3: Apply r Hadamard gates and the inverse of **amp** to map the prior state to $|j\rangle \frac{\bar{A}_n(x_j)}{2^r} |0\rangle^{\otimes r+1} + |\omega_j^\perp\rangle$, where $|\omega_j^\perp\rangle$ is orthogonal to $|0\rangle^{\otimes r+1}$ and subnormalized.

Following this steps we have essentially prepared the state

$$\frac{1}{\sqrt{2^q}} \sum_{j=0}^{2J(n)-1} \frac{\bar{A}_n(x_j)}{2^r} |j\rangle |0\rangle^{\otimes r+2} + |\omega_n^\perp\rangle \quad (89)$$

where again $|\omega_n^\perp\rangle$ is subnormalized and orthogonal to $|0\rangle^{\otimes r+2}$. We can use fixed point amplitude amplification to select the desired part of this state and obtain an $\mathcal{O}(\varepsilon)$ approximation to

$$\frac{\sum_{j=0}^{2J(n)-1} \frac{\bar{A}_n(x_j)}{2^r} |j\rangle}{\left\| \sum_{j=0}^{2J(n)-1} \frac{\bar{A}_n(x_j)}{2^r} |j\rangle \right\|}. \quad (90)$$

Amplitude amplification introduces a multiplicative cost that is $\mathcal{O}(\log(1/\varepsilon))$, since the relevant overlaps are constant.

We discuss the relevant complexities of this approach. First note that it suffices to prepare an $\mathcal{O}(\varepsilon)$ approximation to $|\phi_n\rangle$, since the QHT is performed within this precision and $|\phi_n\rangle$ has overlap with $|\psi_n\rangle$ bounded by a constant. It then suffices to compute the amplitudes $A(x)$ within multiplicative error $\mathcal{O}(\varepsilon)$, but since these are bounded from above by a constant, we can compute them within additive error $\mathcal{O}(\varepsilon)$. It follows that the number of bits of precision is $r = \mathcal{O}(\log(1/\varepsilon))$. We can then construct **amp** using coherent arithmetics; one procedure would involve first computing $\varphi(x)$ within error $\mathcal{O}(\varepsilon)$, which follows if $x/\sqrt{2n+1}$ is obtained within that complexity, and then computing $1/\sqrt{\sin \varphi(x)}$ within this error. For this step it suffices to first compute $\sqrt{2\pi/M}/\sqrt{2n+1}$ within error $\mathcal{O}(\varepsilon/M)$, which can be accomplished with cost $\mathcal{O}((\log M + \log(1/\varepsilon))^2)$. Then we multiply with j , and since j is expressed with $\log M$ bits, this is subdominant. We also need to compute $g_n(x)$ within error $\mathcal{O}(\varepsilon)$. Since $g_n(x)$ can be obtained by rescaling some $g(x)$ [Som19], this translates to computing $g(x)$ within error $\mathcal{O}(\varepsilon/\sqrt{n})$. This function involves the bump function and for this precision the cost is $\tilde{\mathcal{O}}((\log n + \log(1/\varepsilon))^2)$, hiding a doubly logarithmic cost. This function is smooth and also involves an integral, and this increases the cost by a factor of $\mathcal{O}(\log(1/\varepsilon))$. So the total cost of computing $g_n(x)$ is $\mathcal{O}((\log n + \log(1/\varepsilon))^2 \log(1/\varepsilon))$.

There are additional gates used in the procedure, the Hadamard gates and those for inequality tests, which are also subdominant.

The next step involves including the phases. Again, it suffices to compute these phases within $r' = \mathcal{O}(\log(1/\varepsilon))$ bits of precision. We can construct an oracle **phase** that performs the map $|j\rangle \mapsto |j\rangle |\bar{\Theta}(x_j)\rangle$ and then use phase kickback and the inverse of **phase** and obtain $e^{i\bar{\Theta}(x_j)} |j\rangle$. To this end it suffices to compute $\varphi(x)$ within additive error $\mathcal{O}(\varepsilon/N)$. This follows if $x/\sqrt{2n+1}$ is computed with that error which again can be done with cost $\mathcal{O}((\log M + \log(1/\varepsilon))^2)$, as explained in the construction of **amp**.

The last step is to perform the cyclic permutation, since in the standard convention the states $|\phi_n\rangle$ involve a superposition of basis states from $-J(n) + M/2$ to $J(n) - 1 + M/2$. This can be accomplished with gate cost that is $\log^2 M$ using the standard QFT, as explained in [Som16].

According to Lemma 21, $M = \text{poly}(N, 1/\varepsilon)$ and including the cost of amplitude amplification to obtain the normalized state, the result follows. \square

Fast eigenstate filtering. The next step in the QHT is that of state ‘filtering’, which is a transformation that ideally would flag the Hermite state and perform the map

$$|\phi_n\rangle \mapsto \beta_n |\psi_n\rangle |0\rangle^{\otimes m} + |0_n^\perp\rangle, \quad (91)$$

where $\beta_n = \langle \psi_n | \phi_n \rangle$ is the (bounded) overlap, and $|0\rangle^{\otimes q}$ and $|0_n^\perp\rangle$ are orthogonal states of the ancilla qubits. Since we would like to implement this transformation for an exponentially large set of values of $0 \leq n \leq N-1$, we will combine the fast-forwarding results for the discrete QHO in [Section 3](#) with the conventional QPE algorithm [\[Kit95\]](#).

Lemma 23. *Let $0 \leq n \leq N-1$ and ε the error, where $N > \log(1/\varepsilon)$. Then there is a quantum circuit that performs the map in (91) within error ε using $\mathcal{O}((\log N + \log(1/\varepsilon))^3)$ gates.*

Proof. For given N and ε , we set M and N_{high} according to [Lemma 21](#). We also write $M = 2^m$ and let $U(t) = e^{-i\bar{H}t}$ be the time-evolution unitary for the discrete QHO $\bar{H} \in \mathbb{C}^{M \times M}$, where $|t| \leq 2\pi$. Plancherel-Rotach states are mostly supported in the subspace where $n \leq N_{\text{high}}$. For all $0 \leq n \leq N_{\text{high}}$ define $U_n := U(2\pi/M)e^{i(2\pi/M)(n+1/2)t}$. In the low-energy subspace of interest, where $n \leq N_{\text{high}}$, we already proved $U(t)|\psi_n\rangle = e^{-i(n+1/2)t}|\psi_n\rangle + \mathcal{O}(\exp(-\Omega(M)))$ and hence,

$$\frac{1}{M}(\mathbb{1} + U_n^{2^{m-1}}) \dots (\mathbb{1} + U_n) |\psi_{n'}\rangle = \mathcal{O}(\exp(-\Omega(M))), \quad (92)$$

for all $0 \leq n, n' \leq N_{\text{high}}$ and $n \neq n'$. It follows that if we were to run the standard QPE algorithm with m ancillas and controlled- $U_n^{2^j-1}$ unitaries, we would already be performing the desired eigenstate filtering within exponentially small error $\mathcal{O}(\exp(-\Omega(M)))$, which is subdominant. This approach, however, requires implementing U a number of times that is exponential and scales with N or M .

To fast forward eigenstate filtering, we are going to replace

$$U_n^{2^j} \rightarrow W_{n,j} := V(2^j(2\pi/M))e^{i2^j(2\pi/M)(n+1/2)}, \quad (93)$$

where $V(t)$ is the approximation to $U(t) = e^{-i\bar{H}t}$ using the sequence of three exponentials as in [Theorem 5](#). The new QPE circuit would then have controlled- $W_{n,j}$ operations rather than the controlled- $U_n^{2^j-1}$. Our fast-forwarding results also imply

$$\frac{1}{M}(\mathbb{1} + W_{n,m-1}) \dots (\mathbb{1} + W_{n,1}) |\psi_n\rangle = |\psi_n\rangle + \mathcal{O}(\exp(-\Omega(N))) \quad (94)$$

$$\frac{1}{M}(\mathbb{1} + W_{n,m-1}) \dots (\mathbb{1} + W_{n,1}) |\psi_{n'}\rangle = \mathcal{O}(\exp(-\Omega(N))), \quad (95)$$

again for $0 \leq n, n' \leq N_{\text{high}}$ and $n \neq n'$.

Consider now an arbitrary input Plancherel-Rotach state $|\phi_n\rangle$. We have shown $|\phi_n\rangle = \sum_{n=0}^{N_{\text{high}}} \beta_n |\psi_n\rangle + |\phi_n^\perp\rangle$, where $\|\phi_n^\perp\| = \mathcal{O}(\varepsilon)$, for our choice of parameters in [Lemma 21](#). Hence, for this state our QPE algorithm performs

$$|\phi_n\rangle \mapsto \beta_n |\psi_n\rangle |0\rangle^{\otimes m} + |0_n^\perp\rangle \quad (96)$$

within error that is $\mathcal{O}(\varepsilon + \exp(-\Omega(N)))$. Assuming $N > \log(1/\varepsilon)$, the $\mathcal{O}(\varepsilon)$ term dominates, and this is the desired eigenstate filtering operation of [\(91\)](#).

The number of operations for eigenstate filtering can be estimated as follows. Each W_j involves three exponentials, and there are $m-1$ calls to them. We already established that each exponential requires $\mathcal{O}((\log M)^2)$ gates (using schoolbook arithmetics). Then, the gate cost is $\mathcal{O}((\log M)^3) = \mathcal{O}((\log N + \log(1/\varepsilon))^3)$. □

Fixed-point amplitude amplification. As a next step we need to show that amplitude amplification enables the efficient preparation of the Hermite states from the Plancherel-Rotach states, even when the overlaps for different $n \leq N$ are different, but still bounded from below by a positive constant. After eigenstate filtering, our goal is to implement the map

$$\sum_{n=0}^{N-1} \frac{\alpha_n}{\|\phi_n\|} |n\rangle (\beta_n |\psi_n\rangle |0\rangle^{\otimes m} + |0_n^\perp\rangle) \mapsto \sum_{n=0}^{N-1} \alpha_n |n\rangle |\psi_n\rangle, \quad (97)$$

where the α_n are arbitrary and $\beta_n = \langle \psi_n | \phi_n \rangle$. To this end we start from results on fixed-point amplitude amplification in Refs. [YLC14, GSLW19]. These will ultimately give the desired mapping even when the overlaps β_n are different.

Lemma 24. *Let $N > 0$ and ε the error. Let $R_0 = (\mathbb{1} - 2|0\rangle\langle 0|^{\otimes m})$ be the reflection over the ancilla state $|0\rangle^{\otimes m}$ and $\mathcal{U} := \sum_{n=0}^{N-1} |n\rangle\langle n| \otimes \mathcal{U}_n + \sum_{n=N}^{M-1} |n\rangle\langle n| \otimes \mathbb{1}$ be a conditional unitary, where \mathcal{U}_n is the unitary that prepares the Plancherel-Rotach states $|\phi_n\rangle / \|\phi_n\|$, and let $\mathcal{V} := \sum_{n=0}^{N-1} |n\rangle\langle n| \otimes \mathcal{V}_n + \sum_{n=N}^{M-1} |n\rangle\langle n| \otimes \mathbb{1}$ be another conditional unitary, where \mathcal{V}_n is the unitary that performs eigenstate filtering. Then there is a quantum circuit that performs the map in (97) within error ε using \mathcal{U} , \mathcal{V} , R_0 , their inverses, and arbitrary one qubit gates $\mathcal{O}(\log(1/\varepsilon))$ times.*

Before providing the proof, we note that our result relies on, and generalizes the following fixed-point amplitude amplification.

Lemma 25 (Fixed-point amplitude amplification, Thm. 27 of Ref. [GSLW19]). *Let U be a unitary and Π be an orthogonal projector such that $a|\Psi_G\rangle = \Pi U |\Psi_0\rangle$, and $a > \delta > 0$. There is a unitary circuit \tilde{U} such that $\| |\Psi_G\rangle - \tilde{U} |\Psi_0\rangle \| \leq \varepsilon$, which uses a single ancilla qubit and consists of $\mathcal{O}(\log(1/\varepsilon)/\delta)$ U , U^\dagger , $C_\Pi NOT$, $C_{|\Psi_0\rangle\langle\Psi_0|} NOT$, and $e^{i\phi\sigma_z}$ one qubit gates.*

Here, a is unknown but the lower bound δ is known. The operation $C_\Pi NOT$ is simply an operation that coherently checks whether the state is supported in Π or not, and flips the state of another qubit based on the outcome. Similarly, $C_{|\Psi_0\rangle\langle\Psi_0|} NOT$ performs a flip on the qubit depending on whether the state is $|\Psi_0\rangle$ or not. Also, fixed point amplitude amplification uses an ancillary qubit, which starts in $|0\rangle$ and ends in $|0\rangle$ within error ε . This is important for (97) to avoid changing the amplitudes α_n . A generalization of this lemma, which we give below as it can be of independent interest, is used in the proof of Lemma 24.

Lemma 26 (Fixed-point amplitude amplification in subspaces). *Let $N > 0$ be the dimension. For all $0 \leq n \leq N-1$, let U_n be a unitary, Π_n be an orthogonal projector such that $a_n |\Psi_G^n\rangle = \Pi_n U_n |\Psi_0^n\rangle$, and $a_n > \delta > 0$. There is a unitary quantum circuit \tilde{U} such that $\| \sum_{n=0}^{N-1} \alpha_n |n\rangle |\Psi_G^n\rangle - \tilde{U} \sum_{n=0}^{N-1} \alpha_n |n\rangle |\Psi_0^n\rangle \| \leq \varepsilon$, where the amplitudes α_n are arbitrary and $\sum_n |\alpha_n|^2 = 1$, which uses a single ancilla qubit and consists of $\mathcal{O}(\log(1/\varepsilon)/\delta)$ \mathcal{U} , \mathcal{U}^\dagger , $C_\Pi NOT$, $C_{\Pi_0} NOT$, and $e^{i\phi\sigma_z}$ one qubit gates, where $\mathcal{U} = \sum_n |n\rangle\langle n| \otimes U_n$, $\Pi = \sum_n |n\rangle\langle n| \otimes \Pi_n$, and $\Pi_0 = \sum_n |n\rangle\langle n| \otimes |\Psi_0^n\rangle\langle\Psi_0^n|$.*

Proof. Fixed-point amplitude amplification is based on Chebyshev approximations; in the case of Lemma 25, we can assume these to be, for example, linear combinations of Chebyshev polynomials of

$$B = \begin{pmatrix} 0 & A \\ A^\dagger & 0 \end{pmatrix}, \quad A := |\Psi_0\rangle\langle\Psi_0| U^\dagger \Pi = \bar{a} |\Psi_0\rangle \langle\Psi_G|, \quad (98)$$

where \bar{a} is the complex conjugate. The linear combination can be implemented with techniques like QSVT and implements the map $|\Psi_0\rangle \mapsto |\Psi_G\rangle$. The complexity is determined by the degree of the

Chebyshev polynomials in the approximation, and this is $\mathcal{O}(\log(1/\varepsilon)/\delta)$; even when a is unknown (but δ is known), the polynomial allows for the correct mapping.

To work in subspaces, we simply replace B by the direct sum: $B := \bigoplus_n B_n$, where

$$B_n := \begin{pmatrix} 0 & A_n \\ A_n^\dagger & 0 \end{pmatrix}, \quad A_n := |\Psi_0^n\rangle\langle\Psi_0^n| U_n^\dagger \Pi_n = \bar{a}_n |\Psi_0^n\rangle\langle\Psi_G^n|. \quad (99)$$

The Chebyshev polynomial approximation in each subspace will perform the mapping $|\Psi_0^n\rangle \mapsto |\Psi_G^n\rangle$, within error ε , and the transformation carries to an arbitrary state $\sum_{n=0}^{N-1} \alpha_n |n\rangle |\Psi_0^n\rangle$ due to linearity. Note that while fixed-point amplitude amplification uses an ancilla qubit, the ancilla state stays in $|0\rangle$ at the end, within error $\mathcal{O}(\varepsilon)$, for all n . Since we are using the same approximation, the degree is unchanged and still $\mathcal{O}(\log(1/\varepsilon)/\delta)$.

We also note that $B \equiv \sum_n |n\rangle\langle n| \otimes B_n$, and accordingly we can define

$$A := \left(\sum_n |n\rangle\langle n| \otimes |\Psi_0^n\rangle\langle\Psi_0^n| \right) \left(\sum_n |n\rangle\langle n| \otimes U_n^\dagger \right) \left(\sum_n |n\rangle\langle n| \otimes \Pi_n \right) = \sum_n |n\rangle\langle n| \otimes A_n. \quad (100)$$

It follows that we can build the walk operator to implement the Chebyshev polynomials using \mathcal{U} , $C_{\Pi}NOT$, $C_{\Pi_0}NOT$, their inverses and arbitrary gates, a constant number of times. The result follows from multiplying these complexities with the degree. \square

Proof of Lemma 24: Given N and ε , the dimension M is set according to Lemma 21. As mentioned, the proof relies on Lemma 26 and we need to define the corresponding operations. For all $0 \leq n \leq N-1$, we let $|\Psi_0^n\rangle = |0\rangle^{\otimes 2m}$ and $|\Psi_G^n\rangle = |\psi_n\rangle |0\rangle^{\otimes m}$. The unitaries U_n are a sequence of two unitaries, the unitary \mathcal{U}_n to prepare the Plancherel-Rotach state $|\phi_n\rangle / \|\phi_n\|$ and another unitary \mathcal{V}_n that performs eigenstate filtering as in Lemma 23:

$$\frac{\beta_n}{\|\phi_n\|} |\psi_n\rangle |0\rangle^{\otimes m} = (\mathbb{1} \otimes |0\rangle\langle 0|^{\otimes m}) U_n |0\rangle^{\otimes 2m}. \quad (101)$$

The projectors are then $\Pi_n = |0\rangle\langle 0|^{\otimes m}$ for all n . The subspace where $M-1 \geq n \geq N$ is irrelevant since we only need to perform the right transform when $n \leq N-1$. Hence, we can freely define U_n and Π_n in that subspace; for example we can set $U_n = \mathbb{1}$ and $\Pi_n = |0\rangle\langle 0|^{\otimes m}$ for $n \geq N$.

With these definitions we fit the framework of Lemma 26. Note that, since we showed $\beta_n / \|\phi_n\|$ is bounded from below by a positive constant, the number of amplitude amplification rounds is $\mathcal{O}(\log(1/\varepsilon))$. This is the largest degree of the Chebyshev polynomial in the approximation to implement fixed-point amplitude amplification. The overall complexity, as determined by the uses of $\mathcal{U} = \sum_n |n\rangle\langle n| \otimes \mathcal{U}_n$, $\mathcal{V} = \sum_n |n\rangle\langle n| \otimes \mathcal{V}_n$, $R_0 = \mathbb{1} - 2|0\rangle\langle 0|^{\otimes m}$, and their inverses, is then $\mathcal{O}(\log(1/\varepsilon))$. The number of one-qubit gates scales similarly due to Lemma 25. \square

Last we comment on the complexity of implementing the conditional unitaries. The unitary \mathcal{U}_n is discussed in Lemma 22. It requires performing a sequence of computations that depend on n , including $J(n)$, $x_j/\sqrt{2n+1}$, and it uses *amp*. We can run these computations coherently without adding a relevant factor to the gate cost and produce a version of *amp* that now is not only conditional on $|j\rangle$ but also on $|n\rangle$. Hence the gate complexity of the conditional gate \mathcal{U} is dominated by the largest gate complexity of the \mathcal{U}_n 's, which is the one of Lemma 22. The unitary \mathcal{V}_n is discussed in Lemma 23. It requires implementing a version of QPE with unitaries $W_{n,j}$ that depend on n in that there is a phase $e^{i2^j(2\pi/M)(n+1/2)}$, but all other operations are independent of n ; see (93). This is a simple phase gate on $|n\rangle$ that needs to be performed for $0 \leq j \leq m-1$, but does not add a relevant factor to the overall gate complexity either. Hence, implementing \mathcal{U} and \mathcal{V} can also be done with complexity $\mathcal{O}((\log N + \log(1/\varepsilon))^3)$. For more general results on constructing conditional unitaries efficiently, Cf. [BFGH10].

Uncomputation via quantum phase estimation. The last step is to ‘uncompute’ the register that contains $|n\rangle$, that is, to perform the map

$$|n\rangle |\psi_n\rangle \mapsto |0\rangle^{\otimes m} |\psi_n\rangle . \quad (102)$$

Similar to eigenstate filtering, we can leverage the fast-forwarding property to perform exponentially-precise QPE that would allow us to obtain $|n\rangle$ on input $|\psi_n\rangle$. QPE can then be used to uncompute.

Lemma 27. *Let $0 \leq n \leq N - 1$ and ε the error, where $N > \log(1/\varepsilon)$. Then there is a quantum circuit that performs the map in (102) within error ε using $\mathcal{O}((\log N + \log(1/\varepsilon))^3)$ gates.*

Proof. As before, for given N and ε , we set the dimension $M = 2^m$ and N_{high} as in Lemma 21. Let $V_j := V(2^j(2\pi/M))e^{i2^j(2\pi/M)/2}$ for $0 \leq j \leq m - 1$, where $V(t)$ is the approximation to $U(t) = e^{-i\mathbf{H}t}$ using the three exponentials in Theorem 5. Consider the action of the QPE algorithm using m ancilla qubits initially in uniform superposition and using controlled- V_j , on the Hermite state. Prior to the action of the QFT, the state is transformed as

$$\frac{1}{\sqrt{M}} \sum_{l_0, \dots, l_{m-1} \in \{0,1\}} |l_0 \dots l_{m-1}\rangle |\psi_n\rangle \mapsto \frac{1}{\sqrt{M}} \sum_{l_0, \dots, l_{m-1} \in \{0,1\}} |l_0 \dots l_{m-1}\rangle (V_{m-1})^{l_{m-1}} \dots (V_0)^{l_0} |\psi_n\rangle , \quad (103)$$

and using Theorem 5 this is

$$\frac{1}{\sqrt{M}} \sum_{l_0, \dots, l_{m-1} \in \{0,1\}} e^{-i(2\pi n/M)(l_0 + \dots + 2^{m-1}l_{m-1})} |l_0 \dots l_{m-1}\rangle |\psi_n\rangle + \mathcal{O}(\exp(-\Omega(N))) . \quad (104)$$

We now apply the QFT to complete the QPE. Since the ancillary system is a superposition over basis states $|j\rangle$ with phases $e^{-i2\pi nj/M}$, then the QFT maps it to $|n\rangle |\psi_n\rangle$ within error $\mathcal{O}(\exp(-\Omega(N)))$ that is subdominant under the assumption $N > \log(1/\varepsilon)$. QPE applied then the inverse of (102), so the quantum circuit for uncomputation is the inverse of this QPE procedure.

Like in eigenstate filtering, the gate complexity of this approach is given by that of all the V_j 's. This is also $\mathcal{O}(\log^3(M))$, since each V_j involves three exponentials of complexity $\mathcal{O}(\log^2(M))$ each. Since $M = \text{poly}(N, 1/\varepsilon)$, the result follows. \square

4.2 The algorithm

We are now ready to provide a quantum algorithm that implements the QHT. This essentially follows the steps outlined in Section 2.

Algorithm 2 Quantum Hermite Transform

- 1: Let $N > 0$ be the dimension of the QHT and $\epsilon > 0$ be the error. Set $M = \mathcal{O}(N^{9/4}/\epsilon^{13/4})$ according to Lemma 21 and let $m = \log_2 M$.
 - 2: For an m -qubit state $\sum_{n=0}^{N-1} \alpha_n |n\rangle$, use Lemma 22 to prepare $\sum_{n=0}^{N-1} \alpha_n |n\rangle |\phi_n\rangle / \|\phi_n\|$.
 - 3: Use eigenstate filtering and fixed-point amplitude amplification in Lemma 25 to prepare $\sum_{n=0}^{N-1} \alpha_n |n\rangle |\psi_n\rangle$.
 - 4: Use uncomputation in Lemma 27 to reset the state $|n\rangle$ and prepare $\sum_{n=0}^{N-1} \alpha_n |\psi_n\rangle$.
-

Proof of Theorem 19. The combination of the above steps and results allows us to perform the map

$$\sum_{n=0}^{N-1} \alpha_n |n\rangle \mapsto \sum_{n=0}^{N-1} \alpha_n |\psi_n\rangle, \quad (105)$$

within additive error ε , and hence imply the QHT. Before using amplitude amplification, for both the preparation of Plancherel-Rotach states and eigenstate filtering, the size of the circuit is $\mathcal{O}((\log N + \log(1/\varepsilon))^3)$. Combining this with the complexity of amplitude amplification itself, we have an overall complexity of

$$\mathcal{O}\left((\log N + \log(1/\varepsilon))^3 \times \log(1/\varepsilon)\right). \quad (106)$$

□

In Theorem 19 we assumed $N > \log(1/\varepsilon)$. This implies that all error terms $\mathcal{O}(\exp(-\Omega(N)))$ are subdominant. As N is exponentially large in some problem size, this assumes ε not to be double-exponentially small. Nevertheless, it is also possible to avoid this assumption and follow the same steps of our proofs, while keeping track of all errors that are exponentially small in N .

5 Hermite sampling

In this section we discuss an application of the Hermite transform in theoretical computer science. We solve problems in property testing and learning using Hermite sampling as a subroutine. The goal here is to return a sample $v \in \mathbb{N}^n$ with probability $|\widehat{f}_v|^2$, where \widehat{f}_v is the coefficient of the Hermite polynomial corresponding to v in the representation of f . This gives a simple algorithm to solve the Gaussian Goldreich-Levin problem, an analogue of the well-known Goldreich-Levin problem in boolean functions and cryptography, in the Hermite function basis. We also show some property testing results which also hold for boolean functions using QFT as a subroutine, although we do not elaborate on that here.

Suppose we have a function $f : \mathbb{R}^n \rightarrow [-1, 1]$ and a discrete set of input points $S \subseteq \mathbb{R}$. We fix $P \in \mathbb{N}$ assume that f is constant over subcubes of \mathbb{R}^n whose endpoints are integer multiples of 2^{-P_1} . In other words, f acts with P_1 bits of precision. Furthermore, we assume the output of f is recorded with P_2 bits of precision. Finally, we assume that f is “well-conditioned” in the sense that there exists a *distortion* $\kappa > 0$ such that $\|f\| \geq \kappa^{-1}$. This distortion parameter captures the “spikiness” of f , it is the max value of f (one can imagine the tails are cut off) divided by the average ℓ_2 -norm of f under the Gaussian distribution. The dependence on this parameter comes from the complexity of preparing a state whose amplitudes are proportional to the values of f using phase kickback, conditional rotations, and postselection.

We note that technically we do not need the full power of the Hermite transform in this section. In particular, we do not need to perform the uncomputation step (Lemma 27) to be able to sample proportional to $|\widehat{f}_v|^2$, since the absolute value is agnostic to the relative phase.

In the following section, we give an algorithm that takes an oracle to $f : \mathbb{R}^n \rightarrow \{-1, 1\}$ and implements Hermite sampling, for a cleaner exposition. Later in Section 5.2, we generalize this to general functions $f : \mathbb{R}^n \rightarrow \mathbb{R}$. Finally, in Sections 5.3 and 5.4 we give applications in property testing and learning, respectively.

5.1 Boolean-output functions

In this section we restrict our attention to Boolean-output functions – that is, functions whose outputs are in $\{-1, +1\}$. Since there is no output precision, we write P , as opposed to P_1 , to be the input precision of f , for simplicity.

For a *resolution parameter* h and bound $L > 0$ define

$$\mathcal{S}_h[-L, L] = \{kh : k \in \mathbb{Z}, -L \leq kh < L\}.$$

This constitutes a set of points with $\log(1/h)$ bits of precision over which we will discretize the QHO eigenstates. Define $M = |\mathcal{S}_h[-L, L]| = \lfloor 2L/h \rfloor$. This is the number of evaluation points. We will use the state preparation algorithm from [Section 4.1](#) to construct approximate hermite states of dimension

$$M = \max\{2C^{-1}L \cdot 2^P P \cdot (n + \log n + \log(8/\varepsilon)), 40\gamma D \log(2D)\}.$$

For simplicity, we first give an algorithm for the case where the output of f is $\{-1, +1\}$.

Algorithm 3 Approximate Boolean Hermite Sampling

- 1: Let P be the number of bits of precision that f acts with.
 - 2: Choose $M = \max\{2\gamma^{-1}L \cdot 2^P P \cdot (n + \log n + \log(8/\varepsilon)), 40\gamma D \log(2D)\}$, let $m = \log_2 M$.
 - 3: Let V that implements the Hermite transform up to degree D and ambient dimension M .
 - 4: Prepare the state $|\overline{\psi}_0\rangle^{\otimes n} = (V|0^m\rangle)^{\otimes n}$.
 - 5: Apply the oracle U_f to $|\overline{\psi}_0\rangle^{\otimes n}$.
 - 6: Apply $V^{\dagger \otimes n}$ to the state $U_f |\overline{\psi}_0\rangle^{\otimes n}$.
 - 7: Measure in the computational basis and return the result.
-

In the remainder of the section, we will prove the correctness of [Algorithm 3](#). For succinctness we write for some $x \in \{0, 1\}^n$, $|\overline{\psi}_{x_1}\rangle \otimes \dots \otimes |\overline{\psi}_{x_n}\rangle$ as $|\overline{\psi}_x\rangle$ in the rest of this section. We begin by employing a standard result in approximation theory which states that Riemann sums converge exponentially fast for analytic functions such as the hermite functions.

Fact 28 ([[TCW14](#)]). *Let $f : \mathbb{C} \rightarrow \mathbb{C}$ be analytic on a strip $\mathcal{S} = \{z \in \mathbb{C} : \text{Re}(z) \in [a, b], |\text{Im}(z)| \leq a\}$ and suppose further that $|f(z)| \leq Q$ for z in this strip. Then we have*

$$\left| \frac{1}{M} \sum_{\ell=0}^{M-1} f\left(a + \frac{(b-a)\ell}{M}\right) - \int_a^b f(t)dt \right| \leq \frac{2\pi Q}{e^{2\pi aM} - 1} \leq 4\pi Q e^{-2\pi aM}.$$

We show that the product of convergent univariate Riemann sums converges to the product of the corresponding integrals.

Proposition 29. *Let $\{a_i^{(k)}\}_{i=1}^M$ be finite sequences for $k \in [n]$. For each k choose a b_k such that*

$$\left| \sum_{i=1}^M a_i^{(k)} - b_k \right| \leq \varepsilon.$$

Furthermore, suppose that there exists an Q such that for all k

$$\left| \sum_{i=1}^M a_i^{(k)} \right| \leq L, \quad |b_k| \leq Q.$$

Then we have

$$\left| \prod_{k=1}^n \sum_{i=1}^M a_i^{(k)} - \prod_{k=1}^n b_k \right| \leq nQ^{n-1}\varepsilon.$$

Proof. The proof proceeds via a simple hybrid argument. Let

$$H_0 = \prod_{k=1}^n \sum_{i=1}^M a_i^{(k)}, \quad H_1 = b_1 \cdot \prod_{k=2}^n \sum_{i=1}^M a_i^{(k)}, \quad \dots, \quad H_n = \prod_{k=1}^n b_k.$$

For $\ell \in [n]$ we bound the difference between the hybrids H_ℓ and $H_{\ell-1}$. We have

$$\begin{aligned} |H_\ell - H_{\ell-1}| &= \left| \prod_{k=1}^{\ell} b_k \cdot \prod_{k=\ell+1}^n \sum_{i=1}^M a_i^{(k)} - \prod_{k=1}^{\ell-1} b_k \cdot \prod_{k=\ell}^n \sum_{i=1}^M a_i^{(k)} \right| \\ &= \left| \prod_{k=1}^{\ell-1} b_k \cdot \prod_{k=\ell+1}^n \sum_{i=1}^M a_i^{(k)} \right| \cdot \left| \sum_{i=1}^M a_i^{(\ell)} - b_\ell \right| \\ &= Q^{\ell-1} \cdot Q^{n-\ell} \cdot \left| \sum_{i=1}^M a_i^{(\ell)} - b_\ell \right| \leq Q^{n-1} \varepsilon. \end{aligned}$$

Since this holds for any choice of $\ell \in [n]$, we have

$$\left| \prod_{k=1}^n \sum_{i=1}^M a_i^{(k)} - \prod_{k=1}^n b_k \right| = |H_0 - H_n| \leq \sum_{\ell=1}^n |H_{\ell+1} - H_\ell| \leq n Q^{n-1} \varepsilon. \quad \square$$

Next, we bound the probability mass of hermite functions outside the region L . In the sections that follow, we denote by ν the Gaussian probability density function $e^{-x^2}/\sqrt{2\pi}$. Recall that $\int_{\mathbb{R}} H_k(x) H_\ell(x) \nu(x) dx = \delta_{k\ell}$.

Proposition 30. *Fix $L > 1$ and let $R = [-L, L]$. We have*

$$\int_{\mathbb{R}^n \setminus R^n} f(x) H_v(x) \nu(x) \leq e^{-nL^2/4}$$

Proof. Define $R = [-L, L]^n$. We have

$$\begin{aligned} \left| \int_{\mathbb{R}^n \setminus R} f(x) H_v(x) \nu(x) dx \right| &= \left| \int_{\mathbb{R}^n \setminus R} f(x) \nu^{1/2}(x) H_v(x) \nu^{1/2}(x) dx \right| \\ &\leq \sqrt{\int_{\mathbb{R}^n \setminus R} f(x)^2 \nu(x)} \sqrt{\int_{\mathbb{R}^n \setminus R} H_v(x)^2 \nu(x)} \quad (\text{Cauchy-Schwarz}) \\ &\leq \sqrt{\int_{\mathbb{R}^n \setminus R} \nu(x)} \sqrt{\int_{\mathbb{R}^n} H_v(x)^2 \nu(x)} \\ &\leq \left(2 \int_L^\infty \nu(x) \right)^{n/2} \leq e^{-nL^2/4}. \quad \square \end{aligned}$$

As our first major step towards proving the correctness of [Algorithm 3](#), we show that Riemann sums that are approximately induced by the discretized QHO eigenstates converges to the correct quantity.

Proposition 31. *Let $f : \mathbb{R}^n \rightarrow [-1, 1]$ be constant on subsets of the form $[2^{-P}k, 2^{-P}(k+1)]$. For a sufficiently large $M \in \mathbb{N}$, take $h = \sqrt{\frac{2\pi}{M}}$, $L = \sqrt{\frac{\pi M}{2}}$, and $S_1 = \mathcal{S}_h[-L, L]$. Then for any $v \in \mathbb{N}^n$,*

$$\left| \sum_{x \in S_1^n} M^{-n} f(x) H_v(x) \nu(x) - \int_{\mathbb{R}^n} f(x) H_v(x) \nu(x) \right| \leq 2n \cdot (2L \cdot 2^P)^n e^{-2^{-P} \cdot (M/2L)^2} + e^{-nL^2/4}$$

Proof. For each $x \in S$, define $S_2(x) = \mathcal{S}_h[x - 2^{-P}, x]$ and $T_2(x) = \{[x, x + h] : x \in S_2(x)\}$. We remark that the $T_2(x)^n$ are cubes over which f is constant, by assumption. We denote

$$R = \sum_{x \in S_1^n} M^{-n} f(x) H_v(x) \nu(x).$$

This is a Riemann sum that approximates the integral $f(x) H_v(x) \nu(x)$ within the region $[-L, L]$. First we bound the error of this approximation and later show using [Proposition 30](#) that restricting to this region accrues very little error.

$$\begin{aligned} \left| R - \int_{[-L, L]^n} f(x) H_v(x) \nu(x) dx \right| &= \left| \sum_{x \in S_2^n} \left(M^{-n} \sum_{y \in S_2(x)^n} f(y) H_v(y) \nu(y) - \int_{T_2(x)} f(y) H_v(y) \nu(y) dy \right) \right| \\ &= \left| \sum_{x \in S_2^n} f(x) \left(M^{-n} \sum_{y \in S_2(x)^n} H_v(y) \nu(y) - \int_{T_2(x)} H_v(y) \nu(y) dy \right) \right| \\ &\leq \sum_{x \in S_2^n} \left| M^{-n} \sum_{y \in S_2(x)^n} H_v(y) \nu(y) - \int_{T_2(x)} H_v(y) \nu(y) dy \right| \end{aligned}$$

We will bound the inner term of the above sum. First, we observe that the both the sum and the integral can be expressed as products of individual sums and integrals. Thus, applying [Proposition 29](#), we have

$$\left| M^{-n} \sum_{y \in S_2(x)^n} H_v(y) \nu(y) - \int_{T_2(x)} H_v(y) \nu(y) dy \right| \leq n \cdot \max_{i \in [n]} \left| \frac{1}{M} \sum_{z \in S_2(x_i)} H_{v_i}(z) \nu(z) - \int_{T_2(x_i)} H_{v_i}(z) \nu(z) dz \right|$$

Note that the variable z above is univariate. We can now use [Fact 28](#) to bound the inner term. Indeed, invoking the application of the trapezoid rule in [\(17\)](#), we have for any $i \in [n]$

$$\left| \frac{1}{M} \sum_{z \in S_2(x_i)} H_{v_i}(z) \nu(z) - \int_{T_2(x_i)} H_{v_i}(z) \nu(z) dz \right| \leq e^{-2^{-P} \cdot (M/2L)^2}$$

whenever $M > 3 \cdot 2^P$. The sum over S_2^n results in an additional multiplicative factor of $(2L2^P)^n$. As such, we have

$$\left| R - \int_{[-L, L]^n} f(x) H_v(x) \nu(x) dx \right| \leq 2n \cdot (2L \cdot 2^P)^n e^{-2^{-P} \cdot (M/2L)^2}$$

We now conclude the proof by showing that the exclusion of the region $\mathbb{R}^n \setminus [-L, L]^n$ results in a very small additive error. Indeed, applying [Proposition 30](#) we have

$$\begin{aligned} \left| R - \int_{\mathbb{R}^n} f(x) H_v(x) \nu(x) \right| &\leq \left| R - \int_{[-L, L]^n} f(x) H_v(x) \nu(x) dx \right| + \left| \int_{\mathbb{R}^n \setminus [-L, L]^n} f(x) H_v(x) \nu(x) dx \right| \\ &\leq 2n \cdot (2L \cdot 2^P)^n e^{-2^{-P} \cdot (M/2L)^2} + \left| \int_{\mathbb{R}^n \setminus [-L, L]^n} f(x) H_v(x) \nu(x) dx \right| \\ &\leq 2n \cdot (2L \cdot 2^P)^n e^{-2^{-P} \cdot (M/2L)^2} + e^{-nL^2/4}. \quad \square \end{aligned}$$

Now we show that applying the oracle to the discrete, unnormalized ground state $|\psi_0^n\rangle$ and measuring in the $|\psi_v\rangle$ basis corresponds to a Riemann sum that converges to $\hat{f}(v)$.

Lemma 32. For each $v \in [D]^n$, let $|\psi_v\rangle = \otimes_{i=1}^n |\psi_{v_i}\rangle$, where each $|\psi_{v_i}\rangle$ is formed with resolution parameter $h = M^{-1}$ and limit L . We have, for every $v \in [D]^n$

$$\left| \langle \psi_v | U_f | \psi_{0^n} \rangle - \hat{f}(v) \right| \leq \varepsilon/4.$$

Proof. We can write

$$\langle \psi_v | U_f | \psi_{0^n} \rangle = M^{-n} \sum_{x \in S_1^n} f(x) H_v(x) \nu(x).$$

By [Proposition 31](#), we have the bound

$$\left| \langle \psi_v | U_f | \psi_{0^n} \rangle - \hat{f}(v) \right| \leq 2n \cdot (2L \cdot 2^P)^n e^{-2^{-P} \cdot (M/2L)^2} + e^{-nL^2/4}.$$

For our choice of M we have that the right hand side of this is bounded by $\varepsilon/8 + \varepsilon/8 = \varepsilon/4$. \square

Since the (orthonormal) approximations $|\bar{\psi}\rangle$ of the discrete QHO eigenstates are very close in trace distance to the $|\psi\rangle$ above, we can show that they satisfy a similar property.

Corollary 33. For each $v \in [D]^n$, let $|\bar{\psi}_v\rangle = \otimes_{i=1}^n |\bar{\psi}_{v_i}\rangle$, where each $|\bar{\psi}_{v_i}\rangle$ is formed with resolution parameter $h = M^{-1}$. We have, for every $v \in [D]^n$

$$\left| \langle \bar{\psi}_v | U_f | \bar{\psi}_{0^n} \rangle - \hat{f}(v) \right| \leq \varepsilon/2.$$

Proof. Now we argue that replacing $|\psi_{0^n}\rangle$ with $|\bar{\psi}_{0^n}\rangle$ doesn't result in too much error. Recall that we assume the existence of a constant γ such that

$$\text{dist}_{\text{tr}}(|\psi_{0^n}\rangle, |\bar{\psi}_{0^n}\rangle) \leq n \text{dist}_{\text{tr}}(|\psi_0\rangle, |\bar{\psi}_0\rangle) \leq n \exp(-\gamma M).$$

Thus we have

$$\begin{aligned} \left| \langle \bar{\psi}_v | U_f | \bar{\psi}_{0^n} \rangle - \hat{f}(v) \right| &\leq \left| \langle \bar{\psi}_v | U_f | \bar{\psi}_{0^n} \rangle - \langle \bar{\psi}_v | U_f | \psi_{0^n} \rangle \right| + \left| \langle \bar{\psi}_v | U_f | \psi_{0^n} \rangle - \hat{f}(v) \right| \\ &= \left| \langle \bar{\psi}_v | U_f \left(|\bar{\psi}_{0^n}\rangle - |\psi_{0^n}\rangle \right) \right| + \left| \langle \bar{\psi}_v | U_f | \psi_{0^n} \rangle - \hat{f}(v) \right| \\ &\leq n \exp(-\gamma M) + \left| \langle \bar{\psi}_v | U_f | \psi_{0^n} \rangle - \hat{f}(v) \right| \\ &\leq \varepsilon/12 + \left| \langle \bar{\psi}_v | U_f | \psi_{0^n} \rangle - \langle \psi_v | U_f | \psi_{0^n} \rangle \right| + \left| \langle \psi_v | U_f | \psi_{0^n} \rangle - \hat{f}(v) \right| \\ &\leq \left| \langle \bar{\psi}_v | U_f | \psi_{0^n} \rangle - \langle \psi_v | U_f | \psi_{0^n} \rangle \right| + \varepsilon/3 \\ &= \left| \left(\langle \bar{\psi}_v | - \langle \psi_v | \right) U_f | \psi_{0^n} \rangle \right| + \varepsilon/3 \\ &\leq n \exp(-\gamma M) + \varepsilon/3 \leq \varepsilon/2. \end{aligned} \quad \square$$

Now, we are ready to prove the correctness of [Algorithm 3](#).

Theorem 34. For each $v \in [D]^n$, [Algorithm 3](#) outputs v with a probability p_v such that $|p_v - \hat{f}(v)| \leq \varepsilon$. Furthermore, it runs in time $\mathcal{O}(n \text{polylog}(n, D, 1/\varepsilon))$.

Proof. The correctness of the algorithm follows from [Corollary 33](#). Indeed, for every $v \in [D]^n$ we have

$$\begin{aligned} |p_v - \hat{f}(v)| &= \left| \left| \langle \bar{\psi}_S | U_f | \bar{\psi}_{0^n} \rangle \right|^2 - \hat{f}(v)^2 \right| \\ &= \left| \left| \langle \bar{\psi}_S | U_f | \bar{\psi}_{0^n} \rangle \right| + \hat{f}(v) \right| \cdot \left| \left| \langle \bar{\psi}_S | U_f | \bar{\psi}_{0^n} \rangle \right|^2 - \hat{f}(v)^2 \right| \\ &\leq 2 \left| \left| \langle \bar{\psi}_S | U_f | \bar{\psi}_{0^n} \rangle \right|^2 - \hat{f}(v)^2 \right| \leq \varepsilon. \end{aligned}$$

[Corollary 33](#)

We now analyze the time complexity. We will prepare the QHO ground states $|\overline{\psi_{0^n}}\rangle$ with precision M and approximation error $\varepsilon/3n$. Using [Theorem 19](#) this can be done in time $\mathcal{O}((\log n + \log D + \log(1/\varepsilon))^3 \log n \log(1/\varepsilon))$. Then, after applying the oracle, we apply the unitary that maps $|\overline{\psi_k}\rangle$ to $|k\rangle$ for k in the low-energy subspace for each qubit, with approximation error $\varepsilon/6n$. Since these states lie in a Hilbert space of dimension M this also takes $\mathcal{O}((\log n + \log D + \log(1/\varepsilon))^3 \log n \log(1/\varepsilon))$ time for each $i \in [n]$. Overall, the runtime is $\mathcal{O}(n \text{polylog}(n, D, 1/\varepsilon))$, and the additional error from implementing the states $|\overline{\psi_{0^n}}\rangle$ and inverse Hermite transform unitary is $\varepsilon/2$, for an overall error of ε . \square

Furthermore, with a slight overhead in runtime, we can guarantee that our Hermite sampling procedure approximates the true distribution in total variation distance.

Corollary 35. *Let f be v -concentrated on Hermite coefficients with univariate degree at most D . With a runtime overhead of $\mathcal{O}(n \log D)$, [Algorithm 3](#) returns a distribution $\mathcal{D} = \{p_v\}_{v \in [D]^n}$ such that the total variation distribution between \mathcal{D} and the true Hermite distribution is at most $\varepsilon + v$.*

Proof. This follows easily from [Theorem 34](#) by choosing an error $\varepsilon' = \varepsilon \cdot (D+1)^{-n}$ and applying the union bound over all elements in $\{0, 1, \dots, D\}^n$. The overhead in incurred runtime is $n \log D$. \square

5.2 General functions

In this section, we describe how to generalize our algorithm to functions whose output is now in $[-1, 1]$. We remark that the algorithm is effectively the same as in the Boolean case, with the addition of a quantum multiplication step that multiplies the amplitude of each $|x\rangle$ by $f(x)$. This involves controlled rotations and postselection. These steps require a more careful analysis and increase the query and time complexity by a factor depending on the “well-behavedness” of f . This property is what we call distortion, as defined below.

Definition 36 (Distortion).

$$\kappa(f) = \frac{\|f(x)\sqrt{\nu(x)}\|_\infty}{\|f(x)\sqrt{\nu(x)}\|_2}$$

We denote this by κ when f is clear from context. Note that $\kappa = 1$ for all functions $f : \mathbb{R}^n \rightarrow \{-1, +1\}$.

We first show that the probability distribution generated by [Algorithm 4](#) is close to the true Hermite distribution pointwise. Recall that, when the output of f is non-Boolean, the Hermite distribution q_v is defined to be $\hat{f}(v)^2 / \|f\|^2$ for all $v \in \mathbb{N}^n$.

Lemma 37. *Define q_v to be the distribution induced on \mathbb{N}^n by the Hermite coefficients of f and let p_v be the probability of sampling $v \in [D]^n$ in [Algorithm 4](#).*

$$|p_v - q_v| \leq \varepsilon.$$

Proof. Let $|\overline{\psi}\rangle$ represents the state of the algorithm after the postselection step, assuming the initial state was instead $|\psi_{0^n}\rangle \otimes |0^{P_2}\rangle |0\rangle$. We have that

$$|\overline{\psi}\rangle = \frac{\sum_{x \in S_1^n} M^{-n/2} f(x) \nu^{1/2}(x) |x\rangle}{\sqrt{\sum_{x \in S_1^n} M^{-n} f(x)^2 \nu(x)}}.$$

Algorithm 4 Approximate Hermite Sampling

- 1: Let P_1 and P_2 be the number of input and output bits of precision, respectively, for f . Furthermore, let κ be the distortion parameter for f .
 - 2: Choose $M = \max\{2^{P_1} \cdot (n + P_1 + \log(24\kappa/\varepsilon)) \log(1/\varepsilon), 40\gamma D \log D\}$, let $m = \log_2 M$.
 - 3: Let V that implements the Hermite transform up to degree D and ambient dimension M .
 - 4: **repeat**
 - 5: Prepare the state $|\overline{\psi_0}\rangle^{\otimes n} |0^{P_2}\rangle |0\rangle$
 - 6: Apply the oracle U_f controlled on register 1 to register 2.
 - 7: Define the controlled rotation $R|f(x)\rangle |0\rangle \rightarrow \sqrt{1-f(x)^2}|f(x)\rangle |0\rangle + f(x)|f(x)\rangle |1\rangle$.
 - 8: Apply R controlled by register 2 onto register 3.
 - 9: Measure register 3 in the computational basis.
 - 10: **until** $|1\rangle$ is measured
 - 11: Uncompute by applying U_f controlled on register 1 to register 2.
 - 12: Measure register 2 in the computational basis and let $|\tilde{\psi}\rangle$ be the state of register 1.
 - 13: Prepare a unitary V that takes $|\psi_k\rangle$ to $|k\rangle$ for all $k \in [D]$.
 - 14: **return** The result of applying $V^{\otimes n}$ to $|\psi\rangle$, and measuring in the computational basis.
-

The denominator (call it \sqrt{P}) is the normalization factor, and we show that it is very close to $\|f\|$. Applying [Proposition 31](#), we have

$$\left| \sum_{x \in S_1^n} M^{-n} f(x)^2 \nu(x) - \|f\|^2 \right| = \left| \sum_{x \in S_1^n} M^{-n} f(x)^2 \nu(x) - \int_{\mathbb{R}^n} f(x)^2 dx \right| \leq \frac{\varepsilon \cdot \|f\|}{12}$$

Thus, we can bound

$$\left| \sqrt{\sum_{x \in S_1^n} M^{-n} f(x)^2 \nu(x)} - \|f\| \right| = \frac{\left| \sum_{x \in S_1^n} M^{-n} f(x)^2 \nu(x) - \int_{\mathbb{R}^n} f(x)^2 dx \right|}{\sqrt{\sum_{x \in S_1^n} M^{-n} f(x)^2 \nu(x)} + \|f\|} \leq \frac{\varepsilon \cdot \|f\|}{12 \cdot \|f\|} \leq \frac{\varepsilon}{12}.$$

We can write:

$$\langle \psi_v | \overline{\psi} \rangle = \frac{1}{\sqrt{P}} \sum_{x \in S_1^n} M^{-n} f(x) H_v(x) \nu(x).$$

We show using [Proposition 31](#) that this is a Riemann sum which well-approximates $\frac{\hat{f}(v)}{\|f\|}$.

$$\begin{aligned} \left| \langle \psi_v | \overline{\psi} \rangle - \frac{\hat{f}(v)}{\|f\|} \right| &= \left| \frac{1}{\sqrt{P}} \sum_{x \in S_1^n} M^{-n} f(x) H_v(x) \nu(x) - \frac{\hat{f}(v)}{\|f\|} \right| \\ &\leq \frac{1}{\sqrt{P}} \left| \sum_{x \in S_1^n} M^{-n} f(x) H_v(x) - \hat{f}(v) \right| - \left| \hat{f}(v) \right| \left| \frac{1}{\sqrt{P}} - \frac{1}{\|f\|} \right| \\ &\leq \frac{\varepsilon}{12} + \left| \frac{1}{\sqrt{P}} - \frac{1}{\|f\|} \right| \\ &\leq \frac{\varepsilon}{12} + \frac{\varepsilon}{12} \leq \frac{\varepsilon}{6}. \end{aligned}$$

Now, let $|\tilde{\psi}\rangle$ be the actual state of the algorithm after [Line 12](#). We compute $\| |\overline{\psi}\rangle - |\tilde{\psi}\rangle \|$. Recall that $\| |\psi_0\rangle - |\overline{\psi_0}\rangle \| \leq n\sqrt{2} \exp(-\gamma M)$. It is a standard fact that postselection which occurs successfully

with probability p blows up this distance by a factor of p^{-1} . The postselection in [Line 10](#) of the algorithm succeeds with probability at least $\frac{1}{2\|f\|}$, so we have that

$$\left\| |\bar{\psi}\rangle - |\tilde{\psi}\rangle \right\| \leq 2\sqrt{2}n \|f\| \cdot \exp(-\gamma M) \leq \varepsilon/12$$

We replace $|\psi_v\rangle$ with $|\bar{\psi}_v\rangle$, which gives us

$$\left| \langle \bar{\psi}_v | \bar{\psi} \rangle - \frac{\hat{f}(v)}{\|f\|} \right| \leq \left| \langle \bar{\psi}_v | \bar{\psi} \rangle - \langle \psi_v | \bar{\psi} \rangle \right| + \left| \langle \psi_v | \bar{\psi} \rangle - \frac{\hat{f}(v)}{\|f\|} \right| \leq \varepsilon/4$$

Finally, we replace $|\psi_{0^n}\rangle$ with $|\bar{\psi}_{0^n}\rangle$, which swaps and bound:

$$\left| \langle \bar{\psi}_v | \tilde{\psi} \rangle - \frac{\hat{f}(v)}{\|f\|} \right| \leq \left| \langle \bar{\psi}_v | \tilde{\psi} \rangle - \langle \bar{\psi}_v | \bar{\psi} \rangle \right| + \left| \langle \bar{\psi}_v | \bar{\psi} \rangle - \frac{\hat{f}(v)}{\|f\|} \right| \leq \frac{\varepsilon}{3}$$

Recalling that the probability of sampling $v \in [D]^n$ in [Algorithm 4](#) is exactly $\left| \langle \bar{\psi}_v | \tilde{\psi} \rangle \right|^2$ and that $q_v = \frac{\hat{f}(v)^2}{\|f\|^2}$, we conclude by bounding

$$\begin{aligned} |p_v - q_v| &= \left| \left| \langle \bar{\psi}_v | \tilde{\psi} \rangle \right|^2 - \frac{\hat{f}(v)^2}{\|f\|^2} \right| \\ &= \left| \left| \langle \bar{\psi}_v | \tilde{\psi} \rangle \right| + \frac{\hat{f}(v)}{\|f\|} \right| \cdot \left| \left| \langle \bar{\psi}_v | \tilde{\psi} \rangle \right| - \frac{\hat{f}(v)}{\|f\|} \right| \\ &\leq 3 \left| \left| \langle \bar{\psi}_v | \tilde{\psi} \rangle \right| - \frac{\hat{f}(v)}{\|f\|} \right| \leq \varepsilon. \end{aligned} \quad \square$$

The proof of the above lemma also gives us the following stronger result:

Lemma 38. *Let $|\tilde{\psi}\rangle$ be the state of [Algorithm 4](#) after [Line 11](#). Then*

$$\left| \langle \bar{\psi}_v | \psi \rangle - \frac{\hat{f}(v)}{\|f\|} \right| \leq \frac{\varepsilon}{6}.$$

We are now ready to prove the correctness of [Algorithm 4](#).

Theorem 39. *Let p_v be the distribution induced by the Hermite spectrum of a function f with distortion κ . [Algorithm 4](#) succeeds in sampling $v \in [D]^n$ with probability p_v such that $|p_v - q_v| \leq \varepsilon$. Moreover it runs in time $\mathcal{O}(\kappa n \text{polylog}(n, D, 1/\varepsilon))$ and makes $\mathcal{O}(\kappa)$ queries in expectation to f .*

Proof. By [Lemma 37](#), we recover the bound $|p_v - q_v| \leq \varepsilon$. It remains to analyze the runtime and query complexity of the algorithm. The postselection step in [Line 10](#) succeeds with probability at least $\frac{\|f\|}{2} \geq \frac{1}{2\kappa}$. Each attempts makes a single query to f and the only other time a query is made to f is in the uncomputation in [Line 11](#). Thus the query complexity is $\mathcal{O}(\kappa)$.

Now we analyze the computational complexity. Preparing each initial state using [Theorem 19](#) this can be done in time $\mathcal{O}((\log n + \log(1/\varepsilon))^3 \log n \log(1/\varepsilon))$. So, overall, this step takes time $\mathcal{O}(\kappa n \text{polylog}(n, 1/\varepsilon))$. The remainder of the complexity is dominated by the preparation of V , which takes circuit complexity at most $\mathcal{O}(n \log M) = \mathcal{O}(n \text{polylog}(n, D, 1/\varepsilon))$. Thus the overall runtime is $\mathcal{O}(\kappa n \text{polylog}(n, D, 1/\varepsilon))$. \square

Again, we can boost the guarantee to total variation distance with an additional factor of $\mathcal{O}(n \log D)$.

Corollary 40. *Let f be v -concentrated on Hermite coefficients with univariate degree at most D . With a runtime overhead of $\mathcal{O}(n \log D)$, [Algorithm 4](#) returns a distribution $\mathcal{D} = \{p_v\}_{v \in [D]^n}$ such that the total variation distribution between \mathcal{D} and the true Hermite distribution is at most $\varepsilon + v$.*

The proof is identical to that of [Corollary 35](#).

Applications. Inspired by the work of Klivans et al. [[KOS08](#)], we give applications of our algorithm in the form of learning and property testing algorithms. In PAC learning, we are given samples of the form $f(x)$ where f belongs to some known concept class \mathcal{C} and x is drawn from a known distribution \mathcal{D} . For us \mathcal{D} will always be the Gaussian distribution. The goal is to learn some g which agrees with f with high probability on a random input from \mathcal{D} . Sometimes learning tasks are also studied assuming query access to f instead of samples. In property testing, we have an easier task. We are given query access to f , and we simply want to test if f is in \mathcal{C} or disagrees with all functions in \mathcal{C} with high probability. For more background, we refer readers to surveys on learning theory [[KV94](#), [AW17](#)] and property testing [[Can22](#), [MW16](#)]. We go over some preliminaries needed for this section below.

We will use a seminal result in the theory of Sobolev spaces, specialized for the Gaussian distribution. This is known as the Gaussian Poincaré inequality.

Lemma 41 (Gaussian Poincaré inequality [[Poi90](#), [BLM13](#)]). *For $\mathbf{x} \sim \mathcal{N}(0, I)$, and a differentiable function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ we have that*

$$\text{Var}(f(\mathbf{x})) \leq \mathbb{E} \|\nabla f(\mathbf{x})\|_2^2$$

The quantity on the right is known as the Hardy-Krause variation of f ($\sigma_{HK}(f)$) in the literature on Quasi Monte-Carlo methods [[Fis06](#)]. This inequality tells us that for the Gaussian distribution vanilla MC suffices to get a good sample complexity. We will also need a result about the approximation of smooth functions by Hermite polynomials. We state it below.

Lemma 42 (Polynomial approximation of smooth functions ([[DKK⁺24](#), [KTZ19](#)])). *Denote by $P_{>m}f$ the Hermite expansion of f truncated to only include terms with total degree greater than m . Then for all almost-everywhere differentiable functions, we have that*

$$\mathbb{E}_{x \sim \mathcal{N}} [P_{>m}f(x)^2] \leq O\left(\frac{1}{m}\right) \mathbb{E}_{x \sim \mathcal{N}} \|\nabla f(x)\|_2^2$$

For this section we will also need some lemmas about the classical complexity of computing for Hermite coefficients of restricted functions, which we prove below.

Definition 43. For a function $f : \mathbb{R}^n \rightarrow \mathbb{R}$, set $J \subseteq [n]$ and $z \in \mathbb{R}^{\bar{J}}$. Then define $f_{J|z}(y) : \mathbb{R}^J \rightarrow \mathbb{R}$ to be the function where the scalars in \bar{J} is restricted to z .

Definition 44. For a differentiable function $f : \mathbb{R}^n \rightarrow \mathbb{R}$, define $\gamma_f := \mathbb{E}_{x \sim \mathcal{N}} \|\nabla f\|_2^2$. We will denote this by γ when f is clear from context.

Lemma 45. *Let $f : \mathbb{R}^n \rightarrow \mathbb{R}$ and $S \in \mathbb{N}^J$, then we say $J \subseteq [n]$ is the set of indices where $S_i > 0$. For $z \in \mathbb{R}^{\bar{J}}$, write $F_S f(z) = \widehat{f_{J|z}}(S)$. Then we have that*

$$\widehat{F_S f}(T) = \widehat{f}(S \cup T)$$

Proof. For every $U \in \mathbb{N}^n$ we write $U = S \cup T$ where $S \in \mathbb{N}^J$ and $T \in \mathbb{N}^{\bar{J}}$. We also use the notation $h_U = h_S h_T$ where h_U is the Hermite polynomial with coefficient U and h_S, h_T are defined so that they only contain variables in S and T respectively. Then we have that

$$f(x) = \sum_{U \in \mathbb{N}^n} \widehat{f}(U) h_U = \sum_{S \in \mathbb{N}^J, T \in \mathbb{N}^{\bar{J}}} \widehat{f}(S \cup T) h_S h_T = \sum_{S \in \mathbb{N}^J} \left(\sum_{T \in \mathbb{N}^{\bar{J}}} \widehat{f}(S \cup T) h_T \right) h_S$$

If the variables in T are fixed to z then as a function of the variables in S the coefficient on the polynomial h_S is $\sum_{T \in \mathbb{N}^{\bar{J}}} \widehat{f}(S \cup T) h_T(z)$. Thus, we have that $\widehat{F_S f}(T) = \widehat{f}(S \cup T)$ as desired. \square

We can use [Lemma 45](#) to derive a quantity which we can estimate efficiently.

Definition 46. Let

$$\mathbf{W}^S(f) = \sum_{T \in \mathbb{N}^{\bar{J}}} \widehat{f}(S \cup T)^2$$

Corollary 47 (Corollary of [Lemma 45](#)).

$$\mathbf{W}^S(f) = \int_{\mathbb{R}^{\bar{J}}} \widehat{f_{J|z}}(S)^2 \nu(z) dz$$

Proof.

$$\begin{aligned} \int_{\mathbb{R}^{\bar{J}}} \widehat{f_{J|z}}(S)^2 \nu(z) dz &= \int_{\mathbb{R}^{\bar{J}}} F_S f(z)^2 \nu(z) dz \\ &= \sum_{T \in \mathbb{N}^{\bar{J}}} \widehat{F_S}(T)^2 && \text{(Parseval's)} \\ &= \sum_{T \in \mathbb{N}^{\bar{J}}} f(S \cup T)^2 \end{aligned}$$

\square

Using our corollary, we can estimate $\mathbf{W}^S(f)$ efficiently.

Lemma 48. For any $S \in \mathbb{N}^n$ an algorithm with query access to a differentiable function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ can compute an estimate of $\mathbf{W}^S(f)$ that is accurate to within $\pm \varepsilon$ with probability $1 - \delta$ using $\text{poly}(\gamma/\varepsilon) \log(1/\delta)$ queries.

Proof. We rewrite $\mathbf{W}^S(f)$ in a way which can be estimated using Monte-Carlo integration.

$$\begin{aligned} \mathbf{W}^S(f) &= \int_{\mathbb{R}^{\bar{J}}} \widehat{f_{J|z}}(S)^2 \nu(z) dz = \int_{\mathbb{R}^{\bar{J}}} \left(\int_{\mathbb{R}^J} f(y, z) h_S(y) \nu(y) dy \right)^2 \nu(z) dz \\ &= \int_{\mathbb{R}^{\bar{J}}} \left(\int_{\mathbb{R}^J} f(y, z) f(y', z) h_S(y) h_S(y') \nu(y) \nu(y') dy dy' \right) \nu(z) dz \\ &= \mathbb{E}_{z \sim \mathcal{N}^{\bar{J}}} \mathbb{E}_{y, y' \sim \mathcal{N}^J} [f(y, z) f(y', z) h_S(y) h_S(y')] \end{aligned}$$

This quantity can be estimated by a Monte-Carlo method, and due to [Lemma 41](#) we know that $\text{Var}(f(x)) \leq \gamma^2$, so we can get an estimate of this quantity which is accurate up to $\pm \varepsilon$ with probability $1 - \delta$ using $\frac{\gamma^2}{\varepsilon^2} \log(1/\delta)$ samples. \square

5.3 Property testing

In this section, we give quantum algorithms for property testing using our Approximate Hermite Sampling subroutine. In our first two examples, we give provable quantum advantage. Throughout this section, our notion of distance will be Gaussian inner product.

Definition 49 (Distance). We say that $f, g : \mathbb{R}^n \rightarrow \mathbb{R}$ are ε -close if we have that

$$\int_{\mathbb{R}^n} f(x)g(x)\nu(x) \geq 1 - \varepsilon$$

Conversely, we say that f, g are ε -far if the inequality does not hold.

5.3.1 Provable quantum advantage for sign functions

The problem we consider here is to test if a given function f is close to a product of k sign function or far from every product of k sign functions.

Definition 50 (Product sign functions).

$$\chi_S(x) = \prod_{i \in S} \text{sgn}(x_i)$$

Definition 51 (Testing k -product sign functions). Given black-box access to $f : \mathbb{R}^n \rightarrow \mathbb{R}$ and given $\varepsilon_2 > \varepsilon_1 > 0$ determine whether

- $f(x)$ is ε_1 -close to $\chi_S(x)$ for some $S \subseteq [n]$ such that $|S| = k$, or
- $f(x)$ is ε_2 -far from all k -product sign functions.

Let $\varepsilon = \varepsilon_2 - \varepsilon_1$.

Lemma 52. *Product sign functions can be tolerantly tested with $O(1/\varepsilon^2)$ quantum queries.*

Proof. Note that if $f(x) = \chi_S(x)$ for some $S \subseteq [n]$ then the only non-zero Hermite coefficients of f are the ones which non-zero on indices in S . We can use Approximate Hermite Sampling (Algorithm 3) setting the TV distance to be less than $\varepsilon/2$ (Corollary 35) and observe a sample T , then let S be its support. Set $S^*(i) = *$ whenever $i \in S$ and 0 otherwise. Then we can estimate $\mathbf{W}^{S^*}(f)$ upto $\pm\varepsilon/4$ using $O(1/\varepsilon^2)$ queries by Lemma 48 and accept if it is at least $1 - \frac{\varepsilon_1 + \varepsilon_2}{2}$. \square

We prove a classical lower bound of $\Omega(k)$ for this problem. We use the framework of Blais et al. [BBM11], and use a reduction in the communication setting from Disjointness, for which we know tight lower bounds.

Theorem 53. *Any classical algorithm for testing k -product sign functions requires $\Omega(k)$ queries.*

Proof. It proceeds by starting from a hard distribution for Disjointness where we sample two sets A, B such that $|A| = |B| = \frac{k}{2} + 1$ and with probability $1/2$ $A \cap B = \emptyset$ and with probability $1/2$ we have $|A \cap B| = 1$.

For our reduction, given such sets A, B Alice produces $\chi_A = \prod_{i \in A} \text{sgn}(x_i)$ and Bob produces $\chi_B = \prod_{i \in B} \text{sgn}(x_i)$ and they want to test $\chi_{AB} = \chi_A \cdot \chi_B$.

We have

$$\deg(\chi_{AB}) = \begin{cases} k + 2, & \text{if } A \cap B = \emptyset \\ k, & \text{if } |A \cap B| = 1 \end{cases}$$

because if $i \in A \cap B$ then $\chi_A \cdot \chi_B$ does not depend on x_i , since $\text{sgn}(x_i)^2 = 1$. To prove our property testing lower bound, it suffices to prove the following claim.

Lemma 54. *For any set $S : |S| = k + 2$ and $T : |T| = k$, the functions χ_S and χ_T are $\Omega(1)$ -far wrt to the Gaussian distribution.*

Proof.

$$\begin{aligned} d(\chi_S, \chi_T) &= 1 - \int_{\mathbb{R}^n} \chi_S(x) \chi_T(x) \nu(x) dx \\ &= 1 - \int_{\mathbb{R}^n} \chi_{S \Delta T}(x) \nu(x) dx \\ &= 1 \end{aligned}$$

Here we used that $S \Delta T$ is non-empty since S is strictly larger than T . \square

Therefore, deciding whether the input is close to a product sign function on k variables or not allows us to decide the output of the Disjointness function. This must take $\Omega(k)$ queries. \square

Using the lower bound for testing sign functions, we can infer a $\Omega(n)$ lower bound on the classical query complexity of Gaussian Goldreich-Levin. We recall that it is known that one can solve the Goldreich-Levin problem with constant success probability with $O(n/\tau^2)$ classical queries [Gol01]. The factor $1/\tau^2$ is optimal since Parseval's only guarantees that the list L of τ -correlated functions is of size $O(1/\tau^2)$. In the quantum case, we can do much better and get $O(1/\tau^2)$ queries. Here, we ask a similar question but for functions over the domain \mathbb{R}^n .

Definition 55 (Gaussian Goldreich-Levin). Given query access to a function $f : \mathbb{R}^n \rightarrow \mathbb{R}$, return a list L of indices of Hermite polynomials such that

- $|\hat{f}(S)| \geq \tau \implies S \in L$
- $S \in L \iff |\hat{f}(S)| \geq \tau/2$

To derive this we will need an observation about the Hermite expansion of sign functions.

Lemma 56. *For $f(x) = \prod_{i \in T} \text{sgn}(x_i)$ we have that for any $S \in \mathbb{N}^n$, $\hat{f}(S) \leq 1/\exp(k)$ where k is the max degree of a variable in S from T .*

Proof. Let $f(x) = \text{sgn}(x)$, and let $\hat{f}(k)$ be the coefficient of f for the degree k univariate Hermite polynomial. Then we first show that $\hat{f}(k) \leq 1/\exp(k)$. Note that for even k , this coefficient is always 0 since $h_k(x)$ is an even function. For odd k , $h_k(x)$ is an odd function and thus we have the following.

$$\begin{aligned} \hat{f}(k) &= \int_{\mathbb{R}} \text{sgn}(x) h_k(x) \nu(x) dx = \int_0^\infty h_k(x) \nu(x) dx - \int_{-\infty}^0 h_k(x) \nu(x) dx \\ &= 2 \int_0^\infty h_k(x) \nu(x) dx \\ &\leq 1/\exp(k) \end{aligned}$$

In general, if $f(x) = \prod_{i \in T} \text{sgn}(x_i)$ then for any $S \in \mathbb{N}^n$ with non-zero number in any index outside of T , the coefficient $\hat{f}(S) = 0$. For any S supported entirely on T , we can factor the integral for computing the Hermite coefficient based on each variable in T and infer a lower bound from the univariate case. \square

Corollary 57. *Any classical algorithm for Gaussian Goldreich-Levin requires $\Omega_\varepsilon(n)$ queries.*

Proof. Using [Lemma 56](#), we can see that any algorithm for Gaussian Goldreich-Levin with parameter $\tau = \frac{1}{\log(1/\varepsilon)}$ can be used to test if a function f is ε -close to a product of k sign functions. But we know that for $k = \Omega(n)$ this problem requires $\Omega(n)$ queries classically. \square

We also give a classical algorithm that has a matching linear dependence on n for the number of queries, but we defer this to [Appendix D](#). Using the Quantum Hermite Transform, we can get rid of the dependence on n entirely which gives quantum query advantage for this problem. Bel

5.3.2 Tolerant low-degree testing

We are now concerned with testing if a function $f : \mathbb{R}^n \rightarrow \{-1, +1\}$ is well-approximated by a low-degree Hermite expansion.

Definition 58. We say that f is (ε, d) -low-degree if

$$\sum_{\substack{S \in \mathbb{N}^n \\ |S| \leq d}} |\hat{f}(S)|^2 \geq 1 - \varepsilon.$$

Definition 59 (Testing degree- d). Given black-box access to $f : \mathbb{R}^n \rightarrow \{-1, +1\}$ and given $\varepsilon_2 > \varepsilon_1 > 0$ determine whether

- f is (ε_1, d) -low-degree, or
- f fails to be (ε_2, d) -low-degree

With Hermite sampling, the idea is once again simple: use samples from the Hermite distribution and compute the empirical fraction of samples below degree d . This will be a low-bias estimate of the low-degree mass, using which we can distinguish the two cases. Denoting $\varepsilon = \varepsilon_2 - \varepsilon_1$, this approach yields an algorithm with query complexity $\text{poly}(1/\varepsilon)$. Moreover, by importing the lower bound for sign functions ([Theorem 53](#)) we can prove that any classical algorithm requires $\Omega(\frac{d}{\log 1/\varepsilon})$ queries, giving provable quantum advantage in the regime where d is large.

Algorithm 5 Tolerant Low-Degree Testing

```

1: Define  $X = 0$  and  $\varepsilon = \varepsilon_2 - \varepsilon_1$ .
2: Set  $m = O(\log(1/\delta)/\varepsilon^2)$ .
3: for  $i = 1$  to  $m$  do
4:   Perform Hermite sampling on  $f$  to obtain  $S = (v_1, \dots, v_n) \in \mathbb{N}^n$ .
5:   if  $|S| \leq d$  then
6:     Update  $X = X + 1/m$ .
7: if  $X > (\varepsilon_1 + \varepsilon_2)/2$  then
8:   accept
9: else
10:  reject
```

Theorem 60. [Algorithm 5](#) makes $O(\log(1/\delta)/\varepsilon^2)$ quantum queries to f and succeeds with probability at least $1 - \delta$.

Proof. We will run Approximate Hermite Sampling ([Algorithm 3](#)) with TV distance $\varepsilon/10$ which requires a $\text{poly}(n, \log d, \log(1/\varepsilon))$ runtime ([Corollary 35](#)) and constant query complexity. Since we

need to perform Hermite sampling m times and each sampling takes $O(1)$ queries, the total number of queries is $O(m)$.

To see that the algorithm outputs the correct answer with probability $1 - \delta$ notice that X would be an unbiased estimator of the distance of f to being (ε, d) -low-degree if we were getting perfect samples. Since we are using approximate Hermite sampling, X has bias $b = \varepsilon/10$. Therefore, by a Chernoff bound $m = O(\log(1/\delta)/\varepsilon^2)$ independent samples suffice to get an estimate which is $(\varepsilon/4 + b)$ -close with probability $1 - \delta$. This distinguishes the two cases. \square

Corollary 61. *Any classical algorithm for testing if f is (ε, d) -low-degree requires $\Omega_\varepsilon(d)$ queries.*

Proof. We can get a lower bound by considering the special case of product of sign functions. Let $k = d$, then a product of k sign functions is $(\varepsilon, ck \log 1/\varepsilon)$ -low-degree by Lemma 56. Also note that $k + 2$ product functions are not $(\varepsilon, ck \log 1/\varepsilon)$ -low-degree. Since we have a $\Omega(k)$ lower bound for distinguishing these two cases, we have a lower bound for testing if f is $(\varepsilon, ck \log 1/\varepsilon)$ -degree. \square

5.3.3 Tolerant testing Hermite polynomials

For this subsection, we consider the problem of testing closeness to a product of Hermite polynomials.

Definition 62 (Testing product of Hermite polynomials). Given black-box access to $f : \mathbb{R}^n \rightarrow \mathbb{R}$ and given $\varepsilon_2 > \varepsilon_1 > 0$ such that either

- $f(x)$ is ε_1 -close to h_S for some $S \in \mathbb{N}^n$ such that S has k non-zero entries, or
- $f(x)$ is ε_2 -far from every Hermite polynomial on k variables.

Let $\varepsilon = \varepsilon_2 - \varepsilon_1$.

Lemma 63. *Hermite polynomials can be tolerantly tested using $O(1/\varepsilon^2)$ quantum queries.*

Proof. If f is ε -close to a Hermite polynomial, then for some S we have that $\hat{f}(S) \geq 1 - \varepsilon$. If we perform Hermite sampling $O(\log 1/\varepsilon)$ times then we see it with high probability. We can then estimate it to $\pm \varepsilon/2$ and accept if it's at least $1 - \frac{\varepsilon_1 + \varepsilon_2}{2}$. \square

We conjecture that classically this problem requires $\Omega(k)$ queries like in the case of product sign functions. Note that using a classical Gaussian Goldreich-Levin algorithm, we can solve it classically using $O(n)$ queries so this would be tight for $k = \Omega(n)$.

Conjecture 64. *Testing Hermite polynomials on k variables requires $\Omega(k)$ queries classically.*

5.4 Agnostic learning of sparse concepts

We define sparse concepts over real-valued functions, for which we give quantum and classical learning algorithms. First, we define cutoff weight.

Definition 65 (Cutoff weight). For a parameter $\tau \in \mathbb{R}$, we define the cutoff weight of a function f as

$$\mathbf{W}_\tau(f) = \sum_{S: \hat{f}(S) \geq \tau} \hat{f}(S)^2$$

Definition 66 ((s, ε) -sparse concepts). Let \mathcal{C} be a concept comprising of functions $f : \mathbb{R}^n \rightarrow \mathbb{R}$ such that $\mathbb{E}_{x \sim \mathcal{N}} \|\nabla f\|_2^2 \leq \gamma$. We say that \mathcal{C} is (s, ε) -sparse if for all $f \in \mathcal{C}$, if there exists a $\tau(s, \varepsilon) = \text{poly}(\varepsilon/s)$ such that there are at most s Hermite coefficients larger than τ and $\mathbf{W}_\tau(f) \geq 1 - \varepsilon$.

As a consequence of [Algorithm 3](#) we get learning algorithms for sparse concepts.

Lemma 67. *For any (s, ε) -sparse concept \mathcal{C} let κ be the max distortion for any $f \in \mathcal{C}$, and let γ be the max L_2 -norm of ∇f for $f \in \mathcal{C}$. Then there is an agnostic learner with $\text{poly}(s\kappa/\varepsilon)$ quantum queries and $\text{poly}(ns\gamma/\varepsilon)$ classical queries.*

Proof. Since we know the concept is (s, ε) -sparse we know that for every $f \in \mathcal{C}$ there is a τ such that running an algorithm for the Gaussian Goldreich-Levin problem gives us an improper agnostic learner for the function. We know that we can do this in $\text{poly}(\kappa/\tau) = \text{poly}(s\kappa/\varepsilon)$ quantum queries and $\text{poly}(n\gamma/\tau) = \text{poly}(n\gamma\kappa/\varepsilon)$ classical queries. \square

Corollary 68 (Learning juntas). *Let \mathcal{C} be the class of $f : \mathbb{R}^n \rightarrow \{-1, +1\}$ such that f is a polynomial on k variables with individual degree 1. Then \mathcal{C} can be agnostically learned with error ε using $\text{poly}(\frac{1}{\varepsilon}^k)$ quantum queries and $\text{poly}(n\frac{1}{\varepsilon}^k)$ classical queries.*

6 Open problems and outlook

The most pressing question regarding our work is to find additional practical problems for which the QHT gives quantum advantage. To give more precise directions, we consider the following problems.

- To realize the promise of quantum advantage for learning geometric concepts [\[KOS08\]](#), we ask: are there other examples of natural concept classes which are sparse concepts as in [Definition 66](#)?
- Can the QHT be used to obtain learning algorithms for Linear Threshold Functions, or generally Polynomial Threshold Functions that beat the classical query lower bounds?
- Is there a large class of differential equations that can be simulated on a quantum computer efficiently using the QHT, while being hard for classical computers?
- Can other quantum systems be fast forwarded using the QHT?

Acknowledgements

We thank Scott Aaronson, Robbie King, Daniel Rockmore, Troy Sewell, and Sophia Simon for helpful discussions. S. Jain was partially supported by a Berkeley CIQC grant and an Amazon AI Fellowship. VI is supported by an NSF Graduate Research Fellowship. NB is supported by the DOE Office of Science-ASCR, in particular the grant Novel Quantum Algorithms from Fast Classical Transforms.

A Factorization of the QHO evolution operator

In this appendix we prove [Theorem 3](#).

Theorem 3 (Factorization of the QHO evolution [\[QA07\]](#)). *The evolution operator of the QHO admits the following factorization:*

$$\exp(-i\hat{H}t) = \exp\left(-\frac{i \tan(t/2)\hat{p}^2}{2}\right) \exp\left(-\frac{i \sin(t)\hat{x}^2}{2}\right) \exp\left(\frac{-i \tan(t/2)\hat{p}^2}{2}\right). \quad (6)$$

We will first prove a general algebraic claim, from which we will infer our required factorization.

Claim 69. *Let K_1, K_2, K_3 be three operators obeying*

$$[K_1, K_2] = -2K_3, \quad [K_3, K_1] = 2K_2, \quad [K_3, K_2] = -2K_1.$$

Then for all $t \in \mathbb{R}$,

$$e^{(K_1+K_2)t} = e^{\alpha K_1} e^{\beta K_2} e^{\alpha K_1},$$

where

$$\alpha = \frac{\tan(t/\sqrt{2})}{\sqrt{2}}, \quad \beta = \frac{\sin(\sqrt{2}t)}{\sqrt{2}}.$$

Proof. Let

$$U(t) = e^{\alpha K_2} e^{\beta K_1} e^{\alpha K_2}.$$

If we can prove

$$U(t)^{-1} \frac{dU}{dt} = K_1 + K_2,$$

then the claim follows.

By direct calculation,

$$\frac{dU}{dt} = \dot{\alpha} K_2 e^{\alpha K_2} e^{\beta K_1} e^{\alpha K_2} + e^{\alpha K_2} \dot{\beta} K_1 e^{\beta K_1} e^{\alpha K_2} + e^{\alpha K_2} e^{\beta K_1} \dot{\alpha} K_2 e^{\alpha K_2}.$$

Hence,

$$U^{-1} \frac{dU}{dt} = e^{-\alpha K_2} e^{-\beta K_1} e^{-\alpha K_2} \left(\frac{dU}{dt} \right).$$

Using the Campbell–Hausdorff lemma

$$e^X Y e^{-X} = \sum_{j=0}^{\infty} \frac{1}{j!} [X, Y]_j, \quad [X, Y]_0 = Y, \quad [X, Y]_1 = [X, Y], \quad [X, Y]_2 = [X, [X, Y]], \dots,$$

we compute the conjugations step by step:

$$e^{-\alpha K_2} K_1 e^{\alpha K_2} = K_1 - 2\alpha K_3 + 2\alpha^2 K_2,$$

$$e^{-\beta K_1} K_2 e^{\beta K_1} = K_2 + 2\beta K_3 + 2\beta^2 K_1,$$

$$e^{-\alpha K_2} K_3 e^{\alpha K_2} = K_3 - 2\alpha K_2.$$

Substituting these into the expression for $U^{-1} dU/dt$ and collecting terms yields

$$U^{-1} \frac{dU}{dt} = A_1 K_1 + A_2 K_2 + A_3 K_3,$$

with

$$A_1 = 2\alpha\dot{\beta} + \dot{\beta}, \quad A_2 = 2\dot{\alpha} - 4\dot{\alpha}\beta\alpha + 4\dot{\alpha}\beta\alpha^2 + 2\dot{\beta}\alpha^2, \quad A_3 = 2\dot{\alpha}\beta - 4\dot{\alpha}\beta^2\alpha - 2\dot{\beta}\alpha.$$

Differentiating α, β gives

$$\dot{\alpha} = \frac{1}{2} \sec^2\left(\frac{t}{\sqrt{2}}\right), \quad \dot{\beta} = \cos(t\sqrt{2}).$$

Substituting back and simplifying trigonometrically shows that

$$A_1 = 1, \quad A_2 = 1, \quad A_3 = 0.$$

Thus

$$U^{-1} \frac{dU}{dt} = K_1 + K_2,$$

which implies

$$U(t) = e^{(K_1 + K_2)t}.$$

□

Proof of Theorem 3. Define $K_1 = \frac{i}{\sqrt{2}} \hat{x}^2, K_2 = \frac{i}{\sqrt{2}} \hat{p}^2, K_3 = \frac{i}{2} \{\hat{x}, \hat{p}\}$. Then we get the factorization

$$\exp\left(\frac{i}{\sqrt{2}} (\hat{x}^2 + \hat{p}^2)\right) = \exp\left(\frac{\alpha i}{\sqrt{2}} \hat{x}^2\right) \exp\left(\frac{\beta i}{\sqrt{2}} \hat{p}^2\right) \exp\left(\frac{\alpha i}{\sqrt{2}} \hat{x}^2\right)$$

This implies that for $\hat{H} = \frac{1}{2} (\hat{x}^2 + \hat{p}^2)$ we have

$$\exp(-i\hat{H}t) = \exp\left(\frac{i \tan(t/2) \hat{p}^2}{2}\right) \exp\left(\frac{i \sin(t) \hat{x}^2}{2}\right) \exp\left(\frac{i \tan(t/2) \hat{p}^2}{2}\right).$$

□

We can similarly infer that in the discretized case, this factorization is accurate upto the weighted sum of the nested commutators.

Lemma 70. Let $\widetilde{U}(t) = \exp\left(i \frac{\tan(t/2) \bar{p}^2}{2}\right) \exp\left(i \frac{\sin(t) \bar{x}^2}{2}\right) \exp\left(i \frac{\tan(t/2) \bar{p}^2}{2}\right)$, then we have that

$$\begin{aligned} \widetilde{U}(t)^{-1} \frac{d\widetilde{U}(t)}{dt} &= -i\bar{H} + \dot{\beta} \sum_{t=3}^{\infty} \frac{1}{t!2^{t/2}} [\beta' i \bar{x}^2, i \bar{p}^2]_t + \dot{\alpha} \sum_{t=3}^{\infty} \frac{1}{t!2^{t/2}} [\alpha' i \bar{p}^2, i \bar{x}^2]_t \\ &\quad + \dot{\alpha} \sum_{t=2}^{\infty} \frac{1}{t!2^{t/2}} [\alpha' i \bar{p}^2, i \{\bar{x}, \bar{p}\}]_t + \eta' \end{aligned}$$

where $\|\Pi_N \eta' \Pi_N\| \leq \exp(-N/4)$, $\alpha' = \tan(t/2)/2, \beta' = \sin(t)/2, \dot{\alpha} = \frac{1}{2} \sec^2(\frac{t}{2}), \dot{\beta} = \cos(t)$.

Proof. We instantiate the operators as above but with the discretized versions, that is $K_1 = \frac{i}{\sqrt{2}} \bar{x}^2, K_2 = \frac{i}{\sqrt{2}} \bar{p}^2, K_3 = \frac{i}{2} \{\bar{x}, \bar{p}\}$. Now, the proof does not go through as is but we do the same substitutions but keep the terms that ‘went to 0’ due to the commutator relations.

$$\begin{aligned} e^{-\frac{\alpha i}{\sqrt{2}} \bar{p}^2} \frac{i}{\sqrt{2}} \bar{x}^2 e^{\frac{\alpha i}{\sqrt{2}} \bar{p}^2} &= K_1 - 2\alpha K_3 + 2\alpha^2 K_2 + \sum_{t=3}^{\infty} \frac{1}{t!2^{t/2}} [\alpha i \bar{p}^2, i \bar{x}^2]_t, \\ e^{-\frac{i\beta}{\sqrt{2}} \bar{x}^2} \frac{i}{\sqrt{2}} \bar{p}^2 e^{\frac{i\beta}{\sqrt{2}} \bar{x}^2} &= K_2 + 2\beta K_3 + 2\beta^2 K_1 + \sum_{t=3}^{\infty} \frac{1}{t!2^{t/2}} [\beta i \bar{x}^2, i \bar{p}^2]_t, \\ e^{-\frac{\alpha i}{\sqrt{2}} \bar{p}^2} \frac{i}{2} \{\bar{x}, \bar{p}\} e^{\frac{\alpha i}{\sqrt{2}} \bar{p}^2} &= K_3 - 2\alpha K_2 + \sum_{t=2}^{\infty} \frac{1}{t!2^{t/2}} [\alpha i \bar{p}^2, i \{\bar{x}, \bar{p}\}]_t. \end{aligned}$$

Substituting this into the expression

$$\frac{d\widetilde{U}}{dt} = \dot{\alpha} K_2 e^{\alpha K_2} e^{\beta K_1} e^{\alpha K_2} + e^{\alpha K_2} \dot{\beta} K_1 e^{\beta K_1} e^{\alpha K_2} + e^{\alpha K_2} e^{\beta K_1} \dot{\alpha} K_2 e^{\alpha K_2} + \eta$$

yields that upto an additive term multiplied by η with $\|\eta\|$ exponentially small,

$$\begin{aligned} \widetilde{U(t)}^{-1} \frac{d\widetilde{U(t)}}{dt} &= -i\bar{H} + \dot{\beta} \sum_{t=3}^{\infty} \frac{1}{t!2^{t/2}} [\beta' i\bar{x}^2, i\bar{p}^2]_t + \dot{\alpha} \sum_{t=3}^{\infty} \frac{1}{t!2^{t/2}} [\alpha' i\bar{p}^2, i\bar{x}^2]_t \\ &\quad + \dot{\alpha} \sum_{t=2}^{\infty} \frac{1}{t!2^{t/2}} [\alpha' i\bar{p}^2, i\{\bar{x}, \bar{p}\}]_t + \eta'. \end{aligned} \quad \square$$

B Centered discrete Fourier transform

The centered discrete Fourier transform $F \in \mathbb{C}^{M \times M}$ used in [Som16], where $M = 2^m$, is defined via its entries:

$$F_{jk} = \frac{1}{\sqrt{M}} \exp\left(i \frac{2\pi jk}{M}\right), \quad (107)$$

where $-M/2 \leq j, k \leq M/2 - 1$ label the rows and columns of the matrix. The difference with the standard QFT is only due to the shifting of these labels, where $0 \leq j, k \leq M - 1$, and hence these transforms are related via cyclic permutations. In particular, if $m \geq 2$, we can write

$$F = \sigma_z^0 \cdot QFT \cdot \sigma_z^0, \quad (108)$$

where σ_z^0 is the diagonal Pauli matrix acting on the last of the m qubits; i.e., $\sigma_z^0 = \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_2 \otimes \sigma_z$ with $\mathbb{1}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

The complexity of F is then that of the QFT plus two single qubit gates. For the schoolbook version of the QFT, this complexity is also $\mathcal{O}(m^2)$. Using the quasilinear time algorithm for QFT [CW00] this can be implemented with $\tilde{\mathcal{O}}(m)$ gates.

C Some properties of the Plancherel-Rotach asymptotics

For $n \geq 1$, consider the Plancherel-Rotach asymptotic functions

$$\tilde{\phi}_n(x) := \frac{2^{\frac{1}{4}}}{\pi^{\frac{1}{2}} n^{\frac{1}{4}}} \frac{1}{\sqrt{\sin \varphi(x)}} \left(\sin \left[\left(\frac{n}{2} + \frac{1}{4} \right) (\sin(2\varphi(x)) - 2\varphi(x)) + \frac{3\pi}{4} \right] \right), \quad (109)$$

in a domain \mathcal{D}_c where $|x| \leq c' \sqrt{2n+1}$ and $0 \leq c' < 1$. Here, $\varphi(x) := \arccos(x/\sqrt{2n+1})$ satisfies $\pi - c \geq \varphi(x) \geq c$. It follows that $\sqrt{\sin \varphi(x)}$ is bounded from below by a constant and, in this domain, we can simply bound the magnitude as

$$|\tilde{\phi}_n(x)| = \mathcal{O}(1/n^{1/4}). \quad (110)$$

Next we consider the derivative. We obtain

$$\begin{aligned} \frac{d}{dx} \tilde{\phi}_n(x) &= \frac{2^{\frac{1}{4}}}{\pi^{\frac{1}{2}} n^{\frac{1}{4}}} \left(-\frac{\cos(\varphi(x)) \frac{d}{dx} \varphi(x)}{2(\sin \varphi(x))^{3/2}} \sin \left[\left(\frac{n}{2} + \frac{1}{4} \right) (\sin(2\varphi(x)) - 2\varphi(x)) + \frac{3\pi}{4} \right] + \right. \\ &\quad \left. \frac{1}{\sqrt{\sin \varphi(x)}} \cos \left[\left(\frac{n}{2} + \frac{1}{4} \right) (\sin(2\varphi(x)) - 2\varphi(x)) + \frac{3\pi}{4} \right] \left(\frac{n}{2} + \frac{1}{4} \right) (\cos(2\varphi(x)) - 2) \frac{d}{dx} \varphi(x) \right). \end{aligned} \quad (111)$$

Since $\cos(\varphi(x))$ and $\sin(\varphi(x))$ are bounded by constants, and noting

$$\frac{d}{dx}\varphi(x) = \frac{1}{\sqrt{2n+1-x^2}} \implies \left| \frac{d}{dx}\varphi(x) \right| = \mathcal{O}(1/n^{1/2}) \text{ for } x \in \mathcal{D}_c, \quad (112)$$

we obtain

$$\left| \frac{d}{dx}\tilde{\phi}_n(x) \right| = \mathcal{O}(n^{1/4}) \quad (113)$$

in \mathcal{D}_c .

Last, we consider the magnitude of the second derivative. To this end we note

$$\frac{d^2}{dx^2}\varphi(x) = \frac{x}{(2n+1-x^2)^{3/2}} \implies \left| \frac{d^2}{dx^2}\varphi(x) \right| = \mathcal{O}(1/n) \text{ for } x \in \mathcal{D}_c. \quad (114)$$

Using the chain rule it is possible to show that

$$\left| \frac{d^2}{dx^2}\tilde{\phi}_n(x) \right| = \mathcal{O}(n^{3/4}) \quad (115)$$

in \mathcal{D}_c . The term that determines this upper bound is a term that contains

$$\frac{2^{\frac{1}{4}}}{\pi^{\frac{1}{2}} n^{\frac{1}{4}}} \left(\frac{n}{2} + \frac{1}{4} \right)^2 \left(\frac{d}{dx}\varphi(x) \right)^2 = \mathcal{O}(n^{3/4}). \quad (116)$$

D Gaussian Goldreich-Levin

In this section, we study a fundamental learning problem first introduced by Goldreich-Levin [GL89] in the context of cryptography.

Definition 71 (Goldreich-Levin problem, informal). Given query access to $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, output a list of all the linear functions which are τ -correlated with f .

It is known that one can solve the Goldreich-Levin problem with constant success probability with $\mathcal{O}(n/\tau^2)$ classical queries [Gol01]. The factor $1/\tau^2$ is optimal since Parseval's only guarantees that the list L of τ -correlated functions is of size $\mathcal{O}(1/\tau^2)$. In the quantum case, we can do much better and get $\mathcal{O}(1/\tau^2)$ queries. Here, we ask a similar question but for functions over the domain \mathbb{R}^n .

Definition 72 (Gaussian Goldreich-Levin). Given query access to a function $f : \mathbb{R}^n \rightarrow \mathbb{R}$, return a list L of indices of Hermite polynomials such that

- $|\hat{f}(S)| \geq \tau \implies S \in L$
- $S \in L \iff |\hat{f}(S)| \geq \tau/2$

The main claim of this section is that this real-analogue of the Goldreich-Levin problem is also tractable. To prove this, we will need to build some machinery analogous to the classical Goldreich-Levin algorithm, a great exposition for which can be found in the book by O'Donnell [O'D14]. We now prove an analogue of the Goldreich-Levin theorem for Hermite coefficients. Below $\gamma_f = \mathbb{E}_{x \sim \mathcal{N}} \|f(x)\|_2$, and we drop the subscript f when it's clear from context.

Algorithm 6 Gaussian Goldreich-Levin learning algorithm

```
1: Set  $m = O(\frac{\gamma^2}{\tau})$ 
2:  $L \leftarrow (*, *, \dots, *)$ 
3: for  $k = 1$  to  $n$  do
4:   for each  $S \in L, S = (a_1, \dots, a_{k-1}, *, \dots, *)$  do
5:     for  $a_k = 0$  to  $m$  do
6:       Let  $S_{a_k} = (a_1, \dots, a_{k-1}, a_k, *, \dots, *)$ 
7:       Estimate  $\mathbf{W}^{S_{a_k}}(f)$  to within  $\pm\tau^2/4$  with probability at least  $1 - \delta$  Lemma 48
8:       if the estimate of  $\mathbf{W}^{S_{a_k}}(f)$  is at least  $\tau^2/2$  then
9:         Add  $S_{a_k}$  to  $L$ 
10:      Remove  $S$  from  $L$ 
11: return  $L$ 
```

Theorem 73 (Gaussian Goldreich-Levin). *Given query access to a function $f : \mathbb{R}^n \rightarrow \mathbb{R}$, [Algorithm 6](#) runs in time $\text{poly}(n\gamma/\tau)$. It returns a list L of indices of Hermite polynomials such that*

- $|\hat{f}(S)| \geq \tau \implies S \in L$
- $S \in L \iff |\hat{f}(S)| \geq \tau/2$

Proof. Because $(\tau/2)^2 + \tau^2/4 \leq \tau^2/2$, the only Hermite coefficients in L are ones which are at least $\tau/2$. Since $\tau^2 - \tau^2/4 > \tau^2/2$, all Hermite coefficients which are at least τ are in the set L . The runtime can be analysed by multiplying the runtime of all three loops and the complexity of estimation.

- The outermost loop runs for n steps,
- The middle loop runs in $O(1/\tau^2)$ steps since at any given point $|L| \leq O(1/\tau^2)$,
- The runtime of the inner loop is $m = \theta(\gamma^2/\tau)$,
- The query complexity of estimation is $\text{poly}(\gamma/\tau)$ by [Lemma 48](#).

Thus, the overall query complexity and runtime is $\text{poly}(n\gamma/\tau)$. □

Note that while our algorithm assumes knowledge of γ_f , one can always estimate γ_f by simulating gradient queries.

References

- [AA17] Yosi Atia and Dorit Aharonov. Fast-forwarding of Hamiltonians and exponentially precise measurements. *Nature communications*, 8(1):1572, 2017.
- [AA18] Scott Aaronson and Andris Ambainis. Forrelation: a problem that optimally separates quantum from classical computing. *SIAM J. Comput.*, 47(3):982–1038, 2018. [doi: 10.1137/15M1050902](#).
- [Aar10] Scott Aaronson. BQP and the polynomial hierarchy. In *STOC'10—Proceedings of the 2010 ACM International Symposium on Theory of Computing*, pages 141–150. ACM, New York, 2010.

- [AW17] Srinivasan Arunachalam and Ronald de Wolf. Guest column: A survey of quantum learning theory. *SIGACT News*, 48(2):41–67, June 2017. doi:[10.1145/3106700.3106710](https://doi.org/10.1145/3106700.3106710).
- [BACS07] Dominic W. Berry, Graeme Ahokas, Richard Cleve, and Barry C. Sanders. Efficient quantum algorithms for simulating sparse Hamiltonians. *Communications in Mathematical Physics*, 270:359–371, 2007.
- [BBM11] Eric Blais, Joshua Brody, and Kevin Matulef. Property testing lower bounds via communication complexity. In *26th Annual IEEE Conference on Computational Complexity*, pages 210–220. IEEE Computer Soc., Los Alamitos, CA, 2011.
- [BCC⁺15] Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma. Simulating Hamiltonian dynamics with a truncated Taylor series. *Physical review letters*, 114(9):090502, 2015.
- [BFGH10] Debajyoti Bera, Stephen Fenner, Frederic Green, and Steven Homer. Efficient universal quantum circuits. *Quantum Information & Computation*, 10(1):16–28, 2010.
- [BLM13] Stéphane Boucheron, Gábor Lugosi, and Pascal Massart. *Concentration Inequalities: A Nonasymptotic Theory of Independence*. Oxford University Press, 02 2013. doi:[10.1093/acprof:oso/9780199535255.001.0001](https://doi.org/10.1093/acprof:oso/9780199535255.001.0001).
- [BM98] Sergei Blinnikov and Richhild Moessner. Expansions for nearly Gaussian distributions. *Astronomy and Astrophysics Supplement Series*, 130(1):193–205, 1998.
- [BMSZZ25] Sergey Bravyi, Robert Manson-Sawko, Mykhaylo Zayats, and Sergiy Zhuk. Quantum simulation of a noisy classical nonlinear dynamics, 2025. arXiv:[2507.06198](https://arxiv.org/abs/2507.06198).
- [Can22] Clément L. Canonne. Topics and techniques in distribution testing: A biased but representative sample. *Foundations and Trends in Communications and Information Theory*, 19(6):1032–1198, 2022. URL: <http://dx.doi.org/10.1561/0100000114>, doi:[10.1561/0100000114](https://doi.org/10.1561/0100000114).
- [CK10] Andrew M. Childs and Robin Kothari. Limitations on the simulation of non-sparse Hamiltonians. *Quantum Information & Computation*, 10(7):669–684, 2010.
- [CW00] Richard Cleve and John Watrous. Fast parallel circuits for the quantum Fourier transform. In *41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000)*, pages 526–536. IEEE Comput. Soc. Press, Los Alamitos, CA, 2000. doi:[10.1109/SFCS.2000.892140](https://doi.org/10.1109/SFCS.2000.892140).
- [DKK⁺24] Ilias Diakonikolas, Daniel M. Kane, Vasilis Kontonis, Christos Tzamos, and Nikos Zarifis. Agnostically learning multi-index models with queries. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1931–1952, Los Alamitos, CA, USA, October 2024. IEEE Computer Society. doi:[10.1109/FOCS61266.2024.00116](https://doi.org/10.1109/FOCS61266.2024.00116).
- [Fis06] George S. Fishman. *A first course in Monte Carlo*. Duxbury advanced series. Duxbury, Thomson Brooks/Cole, Belmont, CA, 2006.
- [GL89] O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing, STOC*

- '89, page 25–32, New York, NY, USA, 1989. Association for Computing Machinery. doi:[10.1145/73007.73010](https://doi.org/10.1145/73007.73010).
- [Gol01] Oded Goldreich. *Foundations of Cryptography*. Cambridge University Press, 2001.
 - [GR02] Lov Grover and Terry Rudolph. Creating superpositions that correspond to efficiently integrable probability distributions. *quant-ph/0208112*, 2002.
 - [GS18] David J. Griffiths and Darrell F. Schroeter. *Introduction to quantum mechanics*. Cambridge university press, 2018.
 - [GSLW19] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st annual ACM SIGACT symposium on theory of computing*, pages 193–204, 2019.
 - [GSS21] Shouzheng Gu, Rolando D. Somma, and Burak Şahinoğlu. Fast-forwarding quantum evolution. *Quantum*, 5:577, 2021.
 - [HHKL21] Jeongwan Haah, Matthew B. Hastings, Robin Kothari, and Guang Hao Low. Quantum algorithm for simulating real time evolution of lattice Hamiltonians. *SIAM Journal on Computing*, 52(6):FOCS18–250, 2021.
 - [JC05] Edwin T. Jaynes and Frederick W. Cummings. Comparison of quantum and semiclassical radiation theories with application to the beam maser. *Proceedings of the IEEE*, 51(1):89–109, 2005.
 - [JSW⁺25] Stephen P. Jordan, Noah Shutty, Mary Wootters, Adam Zalcman, Alexander Schridhuber, Robbie King, Sergei V. Isakov, and Ryan Babbush. Optimization by decoded quantum interferometry, 2025. URL: <https://arxiv.org/abs/2408.08292>, [arXiv:2408.08292](https://arxiv.org/abs/2408.08292).
 - [Kit95] Alexei Yu Kitaev. Quantum measurements and the Abelian stabilizer problem. *quant-ph/9511026*, 1995.
 - [KOS08] Adam R. Klivans, Ryan O’Donnell, and Rocco A. Servedio. Learning geometric concepts via Gaussian surface area. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 541–550. IEEE Computer Society, 2008. doi:[10.1109/FOCS.2008.64](https://doi.org/10.1109/FOCS.2008.64).
 - [KTZ19] Vasilis Kontonis, Christos Tzamos, and Manolis Zampetakis. Efficient truncated statistics with unknown truncation. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science*, pages 1578–1595. IEEE Comput. Soc. Press, Los Alamitos, CA, [2019] ©2019. doi:[10.1109/FOCS.2019.00093](https://doi.org/10.1109/FOCS.2019.00093).
 - [KV94] Michael J. Kearns and Umesh V. Vazirani. *An introduction to computational learning theory*. MIT Press, Cambridge, MA, 1994.
 - [LC17] Guang Hao Low and Isaac L. Chuang. Optimal Hamiltonian simulation by quantum signal processing. *Physical review letters*, 118(1):010501, 2017.
 - [LGM25] Laura Lewis, Dar Gilboa, and Jarrod R. McClean. Quantum advantage for learning shallow neural networks with natural data distributions, 2025. URL: <https://arxiv.org/abs/2503.20879>, [arXiv:2503.20879](https://arxiv.org/abs/2503.20879).

- [LRP⁺08] Gregory Leibon, Daniel N. Rockmore, Wooram Park, Robert Taintort, and Gregory S. Chirikjian. A fast Hermite transform. *Theoretical computer science*, 409(2):211–228, 2008.
- [MFGH25] Kunal Marwaha, Bill Fefferman, Alexandru Gheorghiu, and Vojtech Havlicek. On the complexity of decoded quantum interferometry, 2025. URL: <https://arxiv.org/abs/2509.14443>, [arXiv:2509.14443](https://arxiv.org/abs/2509.14443).
- [MW16] Ashley Montanaro and Ronald de Wolf. *A Survey of Quantum Property Testing*. Number 7 in Graduate Surveys. Theory of Computing Library, 2016. URL: <http://www.theoryofcomputing.org/library.html>, doi:10.4086/toc.gs.2016.007.
- [NC00] Michael Nielsen and Isaac Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000. doi:10.1017/CBO9780511976667.
- [O’D14] Ryan O’Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014.
- [ORR12] Maris Ozols, Martin Roetteler, and Jérémie Roland. Quantum rejection sampling. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ITCS ’12*, page 290–308, New York, NY, USA, 2012. Association for Computing Machinery. doi:10.1145/2090236.2090261.
- [Poi90] H. Poincaré. Sur les equations aux dérivées partielles de la physique mathématique. *American Journal of Mathematics*, 12(3):211–294, 1890. URL: <http://www.jstor.org/stable/2369620>.
- [QA07] P. C. García Quijas and L. M. Arévalo Aguilar. Factorizing the time evolution operator. *Phys. Scr.*, 75(2):185–194, 2007. doi:10.1088/0031-8949/75/2/012.
- [Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):Art. 34, 40, 2009. doi:10.1145/1568318.1568324.
- [RT22] Ran Raz and Avishay Tal. Oracle separation of BQP and PH. *J. ACM*, 69(4):Art. 30, 21, 2022.
- [Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. doi:10.1137/S0097539795293172.
- [Sim97] Daniel R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997. [arXiv:https://doi.org/10.1137/S0097539796298637](https://arxiv.org/abs/https://doi.org/10.1137/S0097539796298637), doi:10.1137/S0097539796298637.
- [SLSB19] Yuval R. Sanders, Guang Hao Low, Artur Scherer, and Dominic W. Berry. Black-box quantum state preparation without arithmetic. *Physical review letters*, 122(2):020502, 2019.
- [Som16] Rolando D. Somma. Quantum simulations of one dimensional quantum systems, 2016. URL: <https://arxiv.org/abs/1503.06319>, [arXiv:1503.06319](https://arxiv.org/abs/1503.06319).
- [Som19] Rolando D. Somma. Quantum eigenvalue estimation via time series analysis. *New Journal of Physics*, 21(12):123025, 2019.

- [Sze39] Gabor Szegő. *Orthogonal polynomials*, volume 23. American Mathematical Soc., 1939.
- [TCW14] Lloyd N. Trefethen, J. A. C., and Weideman. The exponentially convergent trapezoidal rule. *SIAM Review*, 56(3):385–458, 2014. [arXiv:https://doi.org/10.1137/130932132](https://arxiv.org/abs/https://doi.org/10.1137/130932132), doi:10.1137/130932132.
- [Wu20] Xinyu Wu. A stochastic calculus approach to the oracle separation of BQP and PH, 2020. URL: <https://arxiv.org/abs/2007.02431>, [arXiv:2007.02431](https://arxiv.org/abs/2007.02431).
- [YLC14] Theodore J. Yoder, Guang Hao Low, and Isaac L. Chuang. Fixed-point quantum search with an optimal number of queries. *Phys. Rev. Lett.*, 113:210501, Nov 2014. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.113.210501>, doi:10.1103/PhysRevLett.113.210501.
- [YZ24] Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. *J. ACM*, 71(3):Art. 20, 50, 2024.
- [Zal98] Christof Zalka. Simulating quantum systems on a quantum computer. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 454(1969):313–322, 1998. [arXiv:quant-ph/9603026](https://arxiv.org/abs/quant-ph/9603026).