Shor's Algorithm as a Violation of the Time-Energy Uncertainty (non) Principle
Draft, NOT FOR CIRCULATION

Dorit Aharonov, Yosi Atia

School of Computer Science and Engineering, Hebrew University, Jerusalem, Israel

November 25, 2014

Abstract

In the early days of quantum mechanics, the time energy uncertainty principle, $\Delta E \Delta t \geq \frac{\hbar}{2}$ was misinterpreted as a lower bound for the duration (Δt) required for measuring the energy of a state with accuracy ΔE. Though many systems obey this lower bound, Y. Aharonov and Bohm (1961) were the first to give a counter example using a measurement Hamiltonian, which is infeasible: they can reach an exponentially small accuracy ΔE in time $\Delta t = 1$ by increasing the norm of their Hamiltonian by a factor inverse to the accuracy, namely by investing an exponential amount of energy. In this work we claim that Shor's algorithm is the first example for measuring an energy with accuracy of n bits (i.e. exponentially good accuracy), in complexity that is polynomial in n. This is due to an effect which we define of acceleration of Hamiltonians - the ability to simulate an evolution of a system under Hamiltonian for time t using significantly less than t computational steps. This raises the question: What other interesting Hamiltonians can be accelerated?

1 Background

Using the Fourier transform it is well known that one can prove the position-momentum uncertainty principle (PMUP).

PMUP *Given two identical ensembles of quantum particles, if we measure the position of one ensemble and the momentum the other, the variances are subject to the following relation:*

$$\Delta x \Delta p \geq \frac{\hbar}{2}. \tag{1}$$

Like position and momentum, frequency and time are also conjugate variables, and since frequency represents energy in quantum theory, a natural question is whether a time and energy also obey an uncertainty principle. Several obstacles arise immediately - time is not an operator but a scalar, hence it commutes with all quantum operators; the "time" quantity of a particle is not well defined; time doesn't evolve, and can't be a constant of motion. A common misconception of the time energy uncertainty principle (TEUP) is the following:

TEUP Misconception *The duration Δt of an energy measurement with accuracy ΔE is bounded from below by*

$$\Delta E \Delta t \geq \frac{\hbar}{2}. \tag{2}$$

This interpretation was rebutted by Y. Aharonov and Bohm [1]. By increasing the coupling between the system measured and the measurement device, the measurement duration can be reduced indefinitely. Adapting their argument, one can describe an energy measurement scheme of an eigenstate $|\Psi_E\rangle$ of a

Hamiltonian H with energy E in the Hilbert space $\mathcal{H}_{system}$, as a unitary operator U operating on $\mathcal{H}_{system} \otimes \mathcal{H}_{output}$ defined by

$$U|\Psi_E, x\rangle = e^{-iH \otimes H_{output} \Delta t} |\Psi_E, E' \oplus x\rangle, \tag{3}$$

with Δt annotating the measurement duration, and E' annotating the outcome of the measurement (an approximation of the energy). Knowing H, the measurement duration Δt can be decreased by an arbitrary factor c, at the cost of multiplying the interaction Hamiltonian $H \otimes H_{output}$ by c.

2 Our Contribution

One might suspect that the violation of the TEUP presented in [1] is due to the usage of unphysical measurements, namely, unbounded norms. It is natural to speculate that confining ourselves to physically realistic situations, an appropriate TEUP can be defined and shown to hold. A first attempt might read:

Conjecture 1 (TEUP bounded norm version)**.** If the norm of the interaction Hamiltonian is $O(1)$, then the energy measurement duration is inversely proportional to the accuracy.

Claim: Conjecture 1 is false, since any unitary matrix has eigenvalues on the complex unit circuit, and hence can be generated using a Hamiltonian and time satisfying $||Ht|| = O(1)$. □

However, the time complexity for computing as well as applying the Hamiltonian might be exponentially high. Therefore, a natural modification of Conjecture 1 would be to require that not only that the norm of the Hamiltonian is bounded, but also that it can be applied efficiently by a quantum circuit. Hence, we identify "physically realistic" with "efficiently applicable by a quantum circuit":

Conjecture 2 (TEUP bounded complexity version)**.** An energy measurement of a state under a Hamiltonian H with accuracy ΔE satisfies

$$\Delta E \cdot (\texttt{measurement circuit depth}) \geq 1. \tag{4}$$

We define the measurement circuit depth to be the minimal depth of a quantum circuit performing the measurement, namely the time required to apply the measurement. In a Hamiltonian language, we replace the universal set of gates used in quantum circuits by a list of Hamiltonians with constant norms applied for a single time unit. Since the example adapted from [1] requires increasing the norm of the measurement Hamiltonian by a factor c, it is equivalent to increasing the depth of the quantum circuit simulating the Hamiltonian evolution by the same factor.

Theorem 1 (main)**.** *Shor's algorithm can be associated with a Hamiltonian whose energy measurement satisfies*

$$\Delta E \cdot (\texttt{measurement circuit depth}) \approx 1/exp(n), \tag{5}$$

and therefore the complexity version of the TEUP is exponentially violated.

Proof. Phase estimation is a common procedure in quantum computing, which estimates the phase of an eigenvalue of a unitary operator (see section 5.2 in [3]). Since each unitary operator $U = e^{-iH}$ is generated by applying an non-unique effective Hamiltonian H for a single time unit, it is natural to see the phase estimation as an energy measurement (modulo 2π) of a state under the Hamiltonian H.

In Shor's algorithm, the order r of $a \in \mathbb{Z}_M^*$ is found with $O(1)$ probability by phase estimating a randomly chosen eigenstate of the unitary operator

$$U_a|x\rangle = |ax \ \texttt{Mod}\ M\rangle, \tag{6}$$

i.e. by estimating the energy of that state under the effective Hamiltonian H_a

$$\langle m|H_a|l\rangle = \frac{2\pi}{r\left(e^{\frac{2\pi i}{r}\log_a(m/l)} - 1\right)} \tag{7}$$

The spectrum of H_a is in the form $\frac{2\pi k}{r}$ with $k \in [0...r-1]$. Once an energy is measured with accuracy of n bits (n is the number of bits required to represent M), and the value k of the energy found is co-prime[1]

[1] if they are not co-prime, we'll find r_1, a factor of r. Repeating the process, we can find r_2, and with probability ≥ 0.607, r equals $\texttt{lcm}(r_1, r_2)$. For details see chapter 6 of [5]

to r, the continued fraction algorithm can extract r. Since $\Delta E = 1/r$ is exponentially small, and the time complexity of the algorithm is $O(n^3)$, their product is exponentially small. □

3 Discussion and Implications

An energy measurement with an accuracy exponential in n is feasible due to the ability to apply $U_a^{exp(n)}$ efficiently, or equivalently, by efficiently simulating the evolution of the system under H_a for time that is exponential in n. We define this notion more generally:

Definition 1 (Acceleration of Hamiltonian)**.** The time evolution under a Hamiltonian H applied on a system of n qubits for duration t can be accelerated to time $t' \triangleq f(H, H', t) \ll t$ if there exists an efficiently computable Hamiltonian H' s.t.

$$e^{-iHt} = e^{-iH't'} + O(1/poly(n)). \tag{8}$$

Note that since the eigenvalues of e^{-iHt} are complex, infinite number of matrices V satisfies

$$V = \ln(e^{-iHt}). \tag{9}$$

Only a portion of these matrices have a poly(n) norm, and deciding whether any of them represent an easy to simulate Hamiltonian is not trivial. A simple example for acceleration is the Hamiltonian $H = \frac{1}{2}\sigma_x$. Applying the Hamiltonian for time $t \gg 1$ is equivalent to applying it for time $t' = t \bmod 2\pi$. However the acceleration is possible since we *already know* the eigenvalues. In the light of these observations, the Shor's algorithm is special by hiding the solution to factoring in a spectrum of a Hamiltonian that can be efficiently accelerated *without knowing its spectrum.*

Note that a version of TEUP *can* in fact be proven ($\Delta E \Delta t > 1/4$) if one assume the Hamiltonian is unknown - however, here we are interested in the case in which at least partial information is known about the Hamiltonian [2].

To summarize: A new perspective to Shor's algorithm was presented - as a special counterexample for the time energy uncertainty principle misconception. In the light of this observation, we are interested to find what other Hamiltonians can be accelerated (exactly or approximately) without knowing their spectrum; whether the solution to other interesting problems hides in the spectrum of Hamiltonians that can be accelerated efficiently; and do other quantum algorithms relate to energy measurement? Finally, Hamiltonian acceleration may be important to other fields - it may reduce the run time of an adiabatic computation by effectively increasing the spectral gap, and improve the runtime of continuous time quantum walks.

References

[1] Y. Aharonov and D. Bohm. Time in the quantum theory and the uncertainty relation for time and energy. *Physical Review*, 122(5):1649–1658, 1961.

[2] Y. Aharonov, S. Massar, and S. Popescu. Measuring energy, estimating hamiltonians, and the time-energy uncertainty relation. *Phys. Rev. A: At., Mol., Opt. Phys.*, 66:052107, 2002.

[3] Michael A. Nielsen and Isaac L. Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[4] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.*, 26(5):1484–1509, 1997.

[5] John Preskill. Lecture notes for Physics 229: Quantum information and computation. http://www.theory.caltech.edu/people/preskill/ph229/notes/book.ps, 1998.