Universal Quantum Algorithm

Avatar Tulsi

Department of Physics, IIT Bombay, Mumbai - 400 076, India

tulsi9@gmail.com

August 27, 2018

Abstract

Quantum amplitude amplification and quantum phase estimation are two fundamental quantum algorithms. All known quantum algorithms are derived from these two algorithms. Even the adiabatic quantum algorithms can also be efficiently simulated using quantum phase estimation. We present a universal quantum algorithm which explains these two algorithms as special cases. An interesting result is that we do not need quantum fourier transform to do quantum phase estimation.

We present a universal quantum algorithm. We show that quantum phase estimation (see Section 5.2 of [1]) and quantum amplitude amplification [2, 3, 4] are special cases of our universal algorithm. As these two quantum algorithms are known as fundamental quantum algorithms, all other quantum algorithms (including adiabatic quantum algorithms) can be constructed using them. Thus our universal algorithm explains all known quantum algorithms as its special cases. This may help us in finding new quantum algorithms.

We consider an N-dimensional quantum system and denote its computational basis states by $|i\rangle$ where $i \in \{0, \ldots, N-1\}$. The initial state $|s\rangle$ can be expanded as $\sum_i s_i |i\rangle$ where s_i are chosen to be real. The universal algorithm is multiple iterations of the operator U on $|s\rangle$ where U is $I_s G$. Here I_s is the selective phase inversion of $|s\rangle$ given by $\mathbb{1} - 2|s\rangle\langle s|$ where $\mathbb{1}$ is the identity operator. The diagonal operator G is defined by its diagonal elements $\langle i|G|i\rangle$ which are $e^{i\theta_i}$. Up to an ignorable global phase factor, θ_i can be chosen to be zero for a unique basis state which we refer here as the *target* state $|t\rangle$. We desire evolution of quantum system to $|t\rangle$. Thus

$$|\theta_{i \neq t}| \geq \theta_{\min}, \quad \theta_{i=t} = 0. \tag{1}$$

Here $\theta_{\min}$ is the spectral gap of G.

The dynamics of universal algorithm can be understood by analyzing the eigenspectrum of U. Suppose $U|\lambda\rangle$ is $e^{i\lambda}|\lambda\rangle$. Left multiplication by I_s implies that $G|\lambda\rangle$ is $e^{i\lambda}I_s|\lambda\rangle$ as U is I_sG and I_sI_s is $\mathbb{1}$. Another left multiplication by $\langle i|$ gives us

$$e^{i(\theta_i - \lambda)}\langle i|\lambda\rangle = \langle i|\lambda\rangle - 2s_i\langle s|\lambda\rangle. \tag{2}$$

A simple rearrangement of the terms gives us

$$\langle i|\lambda\rangle = \frac{2s_i\langle s|\lambda\rangle}{1 - e^{i(\theta_i - \lambda)}} = i\frac{s_i\langle s|\lambda\rangle e^{-i(\theta_i - \lambda)/2}}{\sin\frac{\theta_i - \lambda}{2}}. \tag{3}$$

Multiplying by s_i and then summing over i, we get

$$\sum_i s_i^2 \cot\frac{\lambda - \theta_i}{2} = 0. \tag{4}$$

which must be satisfied by λ for $e^{i\lambda}$ to be an eigenvalue of U. Generally it is hard to solve but it is simple if we assume $|\lambda| \ll \theta_{\min}$ and $s_t \ll 1$. Then using the Laurent series expansions for $\cot\frac{\lambda - \theta_i}{2}$ and ignoring $O(s_t^2, \lambda^2)$ terms, above equation becomes

$$(1 + \Lambda_2)\lambda^2 + 2\Lambda_1\lambda - 4s_t^2 = 0, \tag{5}$$

where

$$\Lambda_p = \sum_{i \neq t} s_i^2 \cot^p\frac{\theta_i}{2}, \quad p \in \{1, 2\}. \tag{6}$$

The product and sum of the two solutions $\lambda_\pm$ of Eq. (5) are $-4s_t^2/B^2$ and $-2\Lambda_1/B^2$ respectively. So

$$\lambda_\pm = \pm\frac{2s_t}{B}(\tan\eta)^{\pm 1}, \quad \cot 2\eta = \frac{\Lambda_1}{2s_tB}, \tag{7}$$

where B is $\sqrt{1 + \Lambda_2}$.

Now we show that the eigenphases $\lambda_\pm$ are the only relevant eigenphases for our purpose as the desired target state $|t\rangle$ is completely spanned by the corresponding eigenstates $|\lambda_\pm\rangle$. First, we find $\langle s|\lambda_\pm\rangle$ choosen to be real and positive. Putting Eq. (3) in the normalization condition $\sum_i |\langle i|\lambda_\pm\rangle|^2 = 1$ implies that

$$\langle s|\lambda_\pm\rangle^{-2} = \sum_i s_i^2 \csc^2\frac{\lambda_\pm - \theta_i}{2}. \tag{8}$$

2

The assumption $|\lambda_\pm| \ll \theta_{\min} < 1$ implies that in the sum over i, the $i = t$ term contributes $4s_t^2/\lambda_\pm^2$ which is $B^2(\tan\eta)^{\mp 2}$ as per Eq. (7). Also, using the Laurent series expansions for $\csc\frac{\lambda_\pm - \theta_i}{2}$, we find that all other $i \neq t$ terms contribute B^2 if we ignore small $O(\lambda_\pm/\theta_{\min})$ terms. Thus

$$\langle s|\lambda_\pm\rangle = B^{-1}f_\pm(\eta), \quad f_\pm(\eta) = \left(1 + \tan^{\mp 2}\eta\right)^{-1/2}. \tag{9}$$

It is easy to show that $f_+(\eta)$ is $\sin\eta$ whereas $f_-(\eta)$ is $\cos\eta$. As $\langle s|\lambda_\pm\rangle$ are chosen to be real and positive, η satisfies $\eta \in [0, \pi/2]$.

To find $\langle t|\lambda_\pm\rangle$, we note that θ_t is zero. Thus, putting Eqs. (9), (7) and the assumption $|\lambda_\pm| \ll \theta_{\min}$ in Eq. (3), we get

$$\langle t|\lambda_\pm\rangle = \pm \imath e^{\imath\lambda_\pm/2}\frac{f_\pm(\eta)}{\tan^{\pm 1}\eta} = \pm \imath e^{\imath\lambda_\pm/2}f_\mp(\eta). \tag{10}$$

As $f_+(\eta)^2 + f_-(\eta)^2$ is 1, the desired target state $|t\rangle$ is completely spanned by the eigenstates $|\lambda_\pm\rangle$ making them the only relevant eigenstates for our purpose.

We wish to compute $\alpha(q)$ which is $\langle t|U^q|s\rangle$. This can be expanded as $\sum_j \langle t|\lambda_j\rangle\langle\lambda_j|s\rangle e^{\imath q\lambda_j}$. As $\langle t|\lambda_j\rangle$ is zero for $j \neq \pm$, Eqs. (9) and (10) alongwith the identity $2f_\pm(\eta)f_\mp(\eta) = \sin 2\eta$ imply that

$$|\alpha(q)| = \frac{\sin 2\eta}{2B}\left|e^{\imath q'\lambda_+} - e^{\imath q'\lambda_-}\right| = \frac{\sin 2\eta}{B}\sin\frac{2q's_t}{B\sin 2\eta}, \tag{11}$$

where q' is $q + \frac{1}{2}$. To get above equation, we have used the fact that $|e^{\imath a} - e^{\imath b}|$ is $2\sin\frac{a-b}{2}$ and $\lambda_+ - \lambda_-$ is $\frac{4s_t}{B\sin 2\eta}$ as per Eq. (7).

We choose q to be

$$q = Q = \frac{\pi B}{4s_t} - \frac{1}{2}. \tag{12}$$

Then Eq. (11) implies that the success probability of getting the desired target state $|t\rangle$ is

$$P = |\alpha(Q)|^2 = \frac{\sin^2 2\eta}{B^2}\sin^2\left(\frac{\pi}{2\sin 2\eta}\right). \tag{13}$$

As $B \geq 1$, P is very small if $\sin 2\eta \ll 1$ which happens when $\cot 2\eta \gg 1$. To keep P large enough, we assume that $\cot 2\eta$ is small. When $\cot 2\eta$ is zero then η is $\frac{\pi}{4}$. So, for small values of $\cot 2\eta$, η is close to $\frac{\pi}{4}$ or Δ is small where Δ is defined as $\eta = \frac{\pi}{4} + \Delta$. Thus $\cot 2\eta$ is $-\tan 2\Delta \approx -2\Delta$ for small Δ. Eq. (7) is rewritten as

$$\Delta = -\Lambda_1/(4s_t B) \ll 1. \tag{14}$$

3

Also, $\sin^2 2\eta$ is $1 - 4\Delta^2$ and $\sin^2\left(\frac{\pi}{2\sin 2\eta}\right)$ is $1 - \pi^2\Delta^4$ so that P is $\Theta(1/B)$. Thus $\Theta(B^2)$ times preparations of $|\alpha(Q)\rangle$ state are needed to get the target state $|t\rangle$. Each preparation of $|\alpha(Q)\rangle$ needs $Q = \Theta(B/s_t)$ applications of the operator U so a total of

$$\Theta(B^3/s_t) \tag{15}$$

applications of U are needed for the success of our algorithm. Also, for small Δ, $\tan \eta$ is $\tan\left(\frac{\pi}{4} + \Delta\right)$ or $1 + 2\Delta$ so Eq. (7) implies that the assumption $|\lambda_\pm| \ll \theta_{\min}$ for the validity of our analysis is equivalent to

$$(2s_t/B)(1 \pm \Delta) \ll \theta_{\min}. \tag{16}$$

This completes the analysis of the universal algorithm.

The eigenvalues of U are evaluated with an error of $O(s_t^2, \lambda_\pm^2)$. So the analysis holds for $q_{\max}$ iterations of U with an error of $q_{\max}O(s_t^2, \lambda_\pm^2)$. Typically $\lambda_\pm$ is $\Theta(s_t)$ so that $q_{\max}$ is $\Theta(s_t^{-1})$. Thus the total error is $\Theta(s_t)$ which is very small. The eigenstates of U are evaluated with an error of $O(\lambda_\pm/\theta_{\min})$ which is small due to the assumption $|\lambda_\pm| \ll \theta_{\min}$.

Quantum Amplitude Amplification: Consider the special case when G is $-I_t$ where I_t is the selective phase inversion of the target state $|t\rangle$. Thus G is $2|t\rangle\langle t| - \mathbb{1}$ and $\theta_{i\neq t}$ is π for all $i \neq t$. The moments Λ_1 and Λ_2 are zero so that η is $\frac{\pi}{4}$ and B is 1. Thus $P_{\max}$ is 1 and $q_{\max}$ is $\pi/4s_t$. This performance of the quantum amplitude amplification is also known to be the best possible performance. In Grover's search algorithm $|s\rangle$ is chosen to be a uniform superposition of all N basis states. Thus $|s\rangle$ is $\sum_i |i\rangle/\sqrt{N}$ and s_t is $1/\sqrt{N}$. So the Grover's algorithm finds the target state in $O(\sqrt{N})$ time steps which is quadratically faster than classical algorithms which take $O(N)$ time steps.

Quantum Phase estimation: Suppose we are given a copy of an eigenstate $|\phi\rangle$ corresponding to an eigenvalue $e^{i2\pi\phi}$ of a unitary operator V. In the phase estimation, the goal is to estimate ϕ. Let M be 2^m for an integer m. We estimate ϕ by finding an integer $b \in \{0, M-1\}$ such that $\frac{b}{M} = 0.b_1 \ldots b_m$ is the nearest m-bit approximation to ϕ. Here b_k $(k \in \{1, \ldots, m\})$ denote the bit values of the binary expression of b. So b is $\sum_{k=1}^m 2^{m-k}b_k$. We define δ as

$$\delta = \phi - (b/M), \quad |\delta| \leq (1/2M). \tag{17}$$

The inequality follows from the definition of b.

Consider a $2M$-dimensional quantum system of $1 + m$ qubits. The first qubit controls the crucial operators and we call this the *control*-qubit whose basis states are denoted by $\{|0'\rangle, |1'\rangle\}$. The remaining m qubits provide

4

estimate of ϕ and we call them the *estimate*-qubits labelled by an index $k \in \{1, \ldots, m\}$. The joint Hilbert space of all m estimate-qubits has $M = 2^m$ basis states. Each basis state $|\ell\rangle$ encodes an integer ℓ which is $\sum_{k=1}^{m} 2^{m-k}\ell_k$ where $\ell_k \in \{0, 1\}$ denote the bit values of the binary expression of ℓ. Thus $|\ell\rangle$ is $\prod_{k=1}^{m} |\ell_k\rangle$ where $|\ell_k\rangle$ denote the basis state of kth estimate-qubit which is $|0\rangle$ or $|1\rangle$ depending upon the value of ℓ_k.

The initial state $|s\rangle$ is chosen to be $|\sigma\rangle|+\rangle^{\otimes m}$ or $(1/\sqrt{M})|\sigma\rangle\sum_\ell |\ell\rangle$. Thus the control-qubit state is $|\sigma\rangle$ where $\langle\sigma|0'\rangle$ is $1/(2\sqrt{M})$ and all m estimate-qubits are in $|+\rangle$ states where $|+\rangle$ is $(|0\rangle + |1\rangle)/\sqrt{2}$. The operator G is chosen to be $Z'(c_1 V)(c_0 R)$. Here Z' acts on the control-qubit to multiply the $|1'\rangle$ state by a phase of $e^{\imath\pi}$. The controlled operator $c_1 V$ applies V on its eigenstate $|\phi\rangle$ if and only if the control qubit is in $|1'\rangle$ state. This multiplies the $|1'\rangle$ state by a phase of $e^{\imath 2\pi\phi}$. Another controlled operation $(c_0 R)$ applies the operator R on m estimate-qubits if and only if the control qubit is in $|0'\rangle$ state. The operator R is such that $R|\ell\rangle$ is $e^{\imath 2\pi\ell/M}|\ell\rangle$ or $\prod_{k=1}^{m} e^{\imath 2\pi 2^{-k}\ell_k}|\ell_k\rangle$. Thus R is a product of m single qubit gates R_k where each R_k acts only on k^{th} estimate-qubit to multiply its $|1\rangle$ state by a phase of $e^{\imath 2\pi/2^k}$. Hence $c_0 R$ is a product of m two-qubit gates.

Multiplying G by an ignorable global phase factor of $e^{-\imath 2\pi b/M}$, we can write it as

$$G|0\ell\rangle = e^{\imath 2\pi(\ell-b)/M}|0\ell\rangle, \quad G|1\ell\rangle = -e^{\imath 2\pi(\phi-(b/M))}|1\ell\rangle = e^{\imath\pi(1+2\delta)}|1\ell\rangle. \quad (18)$$

Here $|0\ell\rangle$ and $|1\ell\rangle$ denote the $|0'\rangle|\ell\rangle$ and $|1'\rangle|\ell\rangle$ states respectively. As $G|i\rangle$ is $e^{\imath\theta_i}|i\rangle$, we get

$$\theta_{0\ell} = 2\pi(\ell-b)/M, \quad \theta_{1\ell} = \pi(1+2\delta), \quad \theta_{\min} = 2\pi/M. \quad (19)$$

The eigenphase θ_i is zero if and only if $|i\rangle$ is $|0b\rangle$. Thus $|0b\rangle$ is the target state $|t\rangle$ which provides an estimate of ϕ in terms of b.

As $|s\rangle$ is $(1/\sqrt{M})|\sigma\rangle\sum_\ell |\ell\rangle$ and $\langle\sigma|0'\rangle$ is $1/2\sqrt{M}$, we find that the co-efficients $s_{0\ell}$ are $1/2M$ whereas $s_{1\ell}$ are $(1/\sqrt{M})(1 - \Theta(1/M))$. Thus the moments Λ_p as per Eq. (6) are found to be, ignoring $O(M^{-3/2})$ terms,

$$\Lambda_p = (-\pi\delta)^p + (4M^2)^{-1}\sum_\ell{}' h_\ell^p, \quad h_\ell = \cot\frac{\pi}{M}(\ell-b). \quad (20)$$

The prime notation indicates that the sum excludes $\ell = b$ term. To evaluate this sum, we note that h_ℓ is zero when ℓ is $b + \frac{M}{2}$. Other integers $\ell \neq \{b, b + (M/2)\}$ come in pairs $\{\ell, \ell'\}$ where ℓ' is $(2b - \ell)\mathrm{mod}M$ so that h_ℓ is $-h_{\ell'}$. Thus $\sum_\ell' h_{ell}$ is zero and $\sum_\ell' h_{ell}^2$ is $2\sum_\ell'' h_\ell^2$ where the double prime

5

indicates that the sum is over all ℓ from $(b+1)\bmod M$ to $(b+\frac{M}{2})\bmod M$. The significant contributions to this sum is due to the terms for which $\pi(\ell-b)/M$ is small and h_ℓ is $\frac{M}{\pi(\ell-b)}$. Thus this sum is approximately $2\sum_{r=1}^{M/2}\frac{1}{r^2}$ which converges to $\frac{\pi^2}{3}$ for large M. Thus Λ_2 is $\frac{1}{12}$ and $B=\sqrt{1+\Lambda_2}$ is 1.04 or $\Theta(1)$.

As $|t\rangle$ is $|0b\rangle$, s_t is $1/2M$ and Eq. (15) implies that b can be found using $\Theta(M)$ applications of U which is $I_s G$ provided the assumption of small Δ is correct. As $|\delta|\leq 1/2M$, δ lies in the interval $\{\frac{-1}{2M},\frac{1}{2M}\}$ or $\{\frac{-4}{8M},\frac{4}{8M}\}$. We can always write δ as $\frac{g}{8M}+\delta'$ where $|\delta'|\leq\frac{1}{8M}$ and $g\in\{\pm1,\pm3\}$. We run our universal algorithm 4 times where each running correspond to a unique value of g. In each running, we use the operator $V'=e^{-\imath 2\pi g/8M}V$ in place of V to construct the operator G. The $|\psi\rangle$ is an eigenstate of V' with the eigenvalue $e^{\imath 2\pi\phi'}$ where ϕ' is $\phi-\frac{g}{8M}$ or $\frac{b}{M}-\frac{g}{8M}+\delta$ or $\frac{b}{M}+\delta'$. Thus our analysis can be used if we put δ' in place of δ. Then Eq. (20) implies that Λ_1 is $-\pi\delta'$. Putting this in Eq. (14), we find that Δ is $1.51\delta'M$ as s_t is $1/2M$ and B is 1.04. Then $|\delta'|\leq\frac{1}{8M}$ implies that $|\Delta|\leq 0.19$ and thus Δ is small enough for our analysis to hold. Note that 4 runnings of the algorithm also improve the accuracy of estimation of ϕ by a factor of 4 from $\pm\frac{1}{2M}$ to $\pm\frac{1}{8M}$.

It is easy to check that Δ is small only if we choose the *ignored* global phase factor in Eq. (18) to be $e^{-\imath 2\pi b/M}$. Suppose we choose this phase to be $e^{-\imath 2\pi b'/M}$ where b' is an integer far from b. Then Λ_1 is such that $|\cot 2\eta|=\Lambda_1/2s_t B$ is too large making $\sin 2\eta$ too small so that the success probability also becomes very small. The condition $\Lambda_1\ll 2s_t B$ for the success of our algorithm is quite similar to the phase-matching condition of Grover's algorithm and it is due to resonance phenomena. This plays a crucial part in estimating ϕ.

References

[1] M. Nielsen and I. Chuang (2010), Quantum Computation and Quantum Information, Cambridge University Press.

[2] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[3] L.K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).

[4] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, SIAM J. Computing **26**, 1510 (1997) [arXiv.org:quant-ph/9701001].