The HHL Algorithm

Danial Dervovic

March 21, 2017

These notes are an exposition of the most well-known quantum algorithm for solving linear systems problems. In Section 1 we define the Classical and Quantum Linear Systems problems (QLSP) explicitly. In Section 2 we look at the 2009 algorithm of Harrow, Hassidim and Lloyd [HHL09] (HHL) to solve QLSP.

1 Problem Definition

The general definition of the Linear Systems Problem (LSP) is given below.

Definition 1. LSP: Given a matrix A and a vector **b**, find the vector **x** such that A**x** = **b**.

The QLSP is defined as follows [CKS15]:

Definition 2. QLSP: Let A be an $N \times N$ Hermitian matrix with unit determinant¹. Let **b** and **x** be N-dimensional vectors such that $\mathbf{x} := A^{-1}\mathbf{b}$. Now define the quantum states

$$|b\rangle := \frac{\sum_{i} b_{i} |i\rangle}{\|\sum_{i} b_{i} |i\rangle\|} \quad \text{and} \quad |x\rangle := \frac{\sum_{i} x_{i} |i\rangle}{\|\sum_{i} x_{i} |i\rangle\|}.$$
 (1)

Given A (whose elements are accessed by an oracle) and $|b\rangle$, output a state $|\widetilde{x}\rangle$ such that $||\widetilde{x}\rangle - |x\rangle|| \le \epsilon$ with some probability larger than $\frac{1}{2}$, with a flag indicating success.

Note that QLSP is a different and less general problem than LSP. As such, one should be careful when comparing the performance of algorithms solving the two problems separately.

2 The HHL Algorithm

2.1 Summary

A schematic for the algorithm shown in Figure 1. Let us first understand the main idea of the algorithm. The main technique used here is phase estimation, where given some unitary U with eigenstates $|u_j\rangle$ and corresponding eigenvalues $e^{i\varphi_j}$, the algorithm enacts

$$|0\rangle |u_j\rangle \mapsto |\widetilde{\varphi}\rangle |u_j\rangle,$$
 (2)

These restrictions can be slightly relaxed by noting that the matrix $\begin{bmatrix} 0 & A^{\dagger} \\ A & 0 \end{bmatrix}$ is Hermitian (and therefore also square), and any matrix with non-zero determinant can be scaled appropriately.

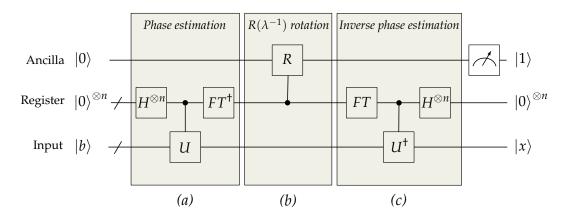


Figure 1: *HHL Algorithm Schematic:* Broadly, there are three main steps. (a) Phase estimation is used to estimate the eigenvalues of A, using $U = \sum_{k=0}^{T-1} |k\rangle\langle k| \otimes \mathrm{e}^{\mathrm{i}Akt_0/T}$, where $T = 2^t$, with t the number of qubits in the computational register and $t_0 = 2\pi$. After this stage the state of the computation is $(\sum_{j=1}^N \beta_j |u_j\rangle_R |\lambda_j\rangle_I) \otimes |0\rangle_A$, where the $|u_j\rangle$ are the eigenvectors of A, the β_j are $|b\rangle$'s representation in this basis and the $|\lambda_j\rangle$ are the binary representations of the eigenvalues of A. (b) The controlled $R(\lambda^{-1})$ rotation extracts the eigenvalues of A^{-1} and executes a σ_y rotation, conditioned on λ_j , leaving the state as $\sum_{j=1}^N \beta_j |u_j\rangle_I |\lambda_j\rangle_R ((1-C^2/\lambda_j^2)^{1/2} |0\rangle + C/\lambda_j |1\rangle)_A$, where C is a normalising constant. (c) The inverse phase estimation subroutine sets the register to $|0\rangle_R^{\otimes n}$ and leaves the remaining state as $\sum_{j=1}^N \beta_j |u_j\rangle_I ((1-C^2/\lambda_j^2)^{1/2} |0\rangle + C/\lambda_j |1\rangle)_A$, so post-selecting on $|1\rangle_A$ gives the state $\sum_{j=1}^N C(\beta_j/\lambda_j) |u_j\rangle_I$, which is $|x\rangle_I$, up to the constant C.

where $\widetilde{\varphi}$ is the binary representation of φ . For the Hermitian matrix A, with eigenstates $|u_j\rangle$ and corresponding eigenvalues λ_j , the matrix $\exp(iAt)$ is unitary, with eigenvalues $i\lambda_j t$ and eigenstates $|u_j\rangle$. Thus, phase estimation can be used with the matrix $\exp(iAt)$ and some arithmetic gates to get

$$|0\rangle |u_j\rangle \mapsto |\widetilde{\lambda}_j\rangle |u_j\rangle.$$
 (3)

Then, adjoining an ancilla qubit and carrying out a controlled rotation conditioned on $\tilde{\lambda}_j$ gives a state of the form

$$\sqrt{\frac{1}{\lambda_j}} |\widetilde{\lambda}_j\rangle |u_j\rangle |1\rangle + \sqrt{1 - \frac{1}{\lambda_j}} |\widetilde{\lambda}_j\rangle |u_j\rangle |0\rangle.$$
 (4)

Measuring the ancilla in the state $|1\rangle$ occurs with probability $\frac{1}{\lambda_j}$. Since $A^{-1} = \sum_j \frac{1}{\lambda_j} |u_j\rangle\langle u_j|$, we can see the intuition for how the state $A^{-1}|b\rangle$ is constructed, when we bear in mind that $|b\rangle$ can be expressed as a convex sum of the $|u_j\rangle$. There are more details in Figure 1 and Section 2.2.

Table 1 compares the runtime of HHL with the best general purpose classical matrix-inversion algorithm, the conjugate-gradient method [She94]. We see that HHL scales exponentially faster in

Problem	Algorithm	Runtime Complexity
LSP	Conjugate Gradient	$O(Ns\kappa \log(1/\epsilon))$
QLSP	HHL	$O(\log(N)s^2\kappa^2/\epsilon)$

Table 1: Runtime comparison between HHL and the best general-purpose classical algorithm.

N, but linearly slower in sparsity s and condition number κ . The sparsity of A is the maximum

number of non-zero entries in any row or column. The *condition number* of A is the ratio of largest to smallest eigenvalue. It also scales exponentially slower in the precision ϵ , which Childs *et al.* have rectified, with an algorithm eliminating the exponential slowdown in ϵ [CKS15]. We won't discuss their algorithm here.

In [HHL09], it is also established that a substantial improvement to the classical algorithm is highly unlikely, as they demonstrate that matrix inversion is a BQP-complete problem. More precisely, they show that a classical poly(log $N, \kappa, 1/\epsilon$) algorithm would be able to simulate a poly(n)-gate quantum circuit in poly(n) time, a scenario which is generally understood to not be possible.

It is also assumed that an efficient construction for $|b\rangle$ exists. If the b_i and $|b_i|^2$ are efficiently computable, then $|b\rangle$ can be built efficiently [GR02]. This admits a rather large class of superpositions, but it is worth bearing in mind that the exponential speedup gained disappears if this isn't satisfied.

2.2 Algorithm Details

The first step of the algorithm is to prepare the state $|b\rangle$. The authors simply assume that there exist a unitary B and a state $|\text{initial}\rangle$ such that $B|\text{initial}\rangle = |b\rangle$ to perfect accuracy, requiring T_B gates to implement.

Then, the state

$$|\Psi_0\rangle = \sqrt{\frac{2}{T}} \sum_{\tau=0}^{T-1} \sin \frac{\pi(\tau + \frac{1}{2})}{T} |\tau\rangle$$
 (5)

is prepared using a T chosen later. The state $|\Psi_0\rangle$ can be prepared up to error ϵ_{Ψ} in time poly $\log(T/\epsilon_{\Psi})$ [GR02].

The conditional Hamiltonian $\sum_{\tau=0}^{T-1} |\tau\rangle\langle\tau|^C \otimes e^{iA\tau t_0/T}$ is then applied to $|\Psi_0\rangle^C \otimes |b\rangle$, for $t_0 = O(\kappa/\epsilon)$. The resulting state is

$$\sqrt{\frac{2}{T}} \sum_{j=1}^{N} \beta_j \left(\sum_{\tau=0}^{T-1} e^{\frac{i\lambda_j t_0 \tau}{T}} \sin \frac{\pi(\tau + \frac{1}{2})}{T} |\tau\rangle \right) |u_j\rangle, \tag{6}$$

where λ_j , $|u_j\rangle$ are the j^{th} eigenvalue and eigenvector of A respectively. Now expressing the bracketed part of Eq. 6 in the Fourier basis $|k\rangle$ (by taking an inner product with $\frac{1}{\sqrt{T}}\sum_{\tau=0}^{T-1}\mathrm{e}^{\frac{2\pi\mathrm{i}k\tau}{T}}|\tau\rangle$), we are left with

$$\sum_{j=1}^{N} \beta_{j} \sum_{k=0}^{T-1} \left(\frac{\sqrt{2}}{T} \sum_{\tau=0}^{T-1} e^{\frac{i\tau}{T} (\lambda_{j} t_{0} - 2\pi k)} \sin \frac{\pi(\tau + \frac{1}{2})}{T} \right) |k\rangle |u_{j}\rangle := \sum_{j=1}^{N} \beta_{j} \sum_{k=0}^{T-1} \alpha_{k|j} |k\rangle |u_{j}\rangle.$$
 (7)

It can be shown that $\left|\alpha_{k|j}\right|^2 \leq 64\pi^2/\delta^2$ whenever $|k-\lambda_j t_0/2\pi| \geq 1$, where $\delta := \lambda_j t_0 - 2\pi k$. This means that $\left|\alpha_{k|j}\right|$ is large if and only if $\lambda_j \approx \frac{2\pi k}{t_0}$. We can now relabel the $|k\rangle$ basis states by defining $\widetilde{\lambda}_k := 2\pi k/t_0$, giving us

$$\sum_{j=1}^{N} \beta_j \sum_{k=0}^{T-1} \alpha_{k|j} |\widetilde{\lambda}_k\rangle |u_j\rangle. \tag{8}$$

Now an additional three-dimensional register S is adjoined in the state

$$|h(\widetilde{\lambda}_k)\rangle^S := \sqrt{1 - f(\widetilde{\lambda}_k)^2 - g(\widetilde{\lambda}_k)^2} |\text{nothing}\rangle^S + f(\widetilde{\lambda}_k) |\text{well}\rangle^S + g(\widetilde{\lambda}_k) |\text{ill}\rangle^S,$$
 (9)

for functions $f(\lambda)$, $g(\lambda)$ we define below in Eq. 10. The flag 'nothing' corresponds to no inversion taking place, 'well' means it has, and 'ill' indicates the part of $|b\rangle$ in the ill-conditioned subspace of A

The functions $f(\lambda), g(\lambda)$ are known as filter functions, and act to invert A only on its well-conditioned subspace, where we mean the subspace spanned by eigenvectors corresponding to $\lambda \geq 1/\kappa$. We also have intermediary eigenvalues, characterised by $1/\kappa' \leq \lambda \leq 1/\kappa$ for some κ' , say $\kappa' = 2\kappa$, where interpolating behaviour is chosen for the filter functions, which are defined below.

$$f(\lambda) = \begin{cases} \frac{1}{2\kappa\lambda}, & \lambda \ge 1/\kappa; \\ \frac{1}{2}\sin\left(\frac{\pi}{2} \cdot \frac{\lambda - \frac{1}{\kappa'}}{\frac{1}{\kappa} - \frac{1}{\kappa'}}\right), & \frac{1}{\kappa} > \lambda > \frac{1}{\kappa'}; & \text{and} \quad g(\lambda) = \begin{cases} 0, & \lambda \ge 1/\kappa; \\ \frac{1}{2}\cos\left(\frac{\pi}{2} \cdot \frac{\lambda - \frac{1}{\kappa'}}{\frac{1}{\kappa} - \frac{1}{\kappa'}}\right), & \frac{1}{\kappa} > \lambda > \frac{1}{\kappa'}; \\ \frac{1}{2}, & \frac{1}{\kappa'} > \lambda. \end{cases}$$
(10)

The authors of [HHL09] don't explicitly provide a scheme for implementing the controlled rotations required to implement for $f(\tilde{\lambda})$ and $g(\tilde{\lambda})$. However, a circuit representation (at least for $f(\lambda)$) is given in [CDFK12].

After this, the phase estimation procedure is reversed, uncomputing garbage qubits in the process. The procedure we have described up until now we denote U_{invert} . Applying U_{invert} to $|b\rangle$, then measuring S with the outcome 'well', returns the state $|\widetilde{x}\rangle$ with probability $\widetilde{p} := \mathbb{E}_{j,k} \left[f(\widetilde{\lambda}_k)^2 + g(\widetilde{\lambda}_k)^2 \right]$, where $\mathbb{E}_{j,k}[\cdot] := \sum_{j,k} |\beta_j|^2 |\alpha_{j|k}|^2 (\cdot)$ and $||\widetilde{x}\rangle - |x\rangle|| \le \epsilon$ for $\epsilon = O(\kappa/t_0)$. Typically, one would need to repeat this procedure $1/\widetilde{p}$ times, but the authors use amplitude

Typically, one would need to repeat this procedure $1/\tilde{p}$ times, but the authors use amplitude amplification [BHMT00] to obtain the same results with $O(1/\sqrt{\tilde{p}})$. This achieved by the following: Introduce operators

$$R_{\text{succ}} := I^S - 2 |\text{well}\rangle \langle \text{well}|^S, \tag{11}$$

which acts only on the S register and

$$R_{\text{init}} := I - 2 |\text{initial}\rangle\langle \text{initial}|.$$
 (12)

We then proceed using the amplitude amplification procedure. Start with $U_{\text{invert}}B |\text{initial}\rangle$, then repeatedly apply $U_{\text{invert}}BR_{\text{init}}B^{\dagger}U_{\text{invert}}^{\dagger}R_{\text{succ}}$. The ideal number of repetitions would be $\frac{\pi}{4\sqrt{p}}$, which is $O(\kappa)$. Although \tilde{p} is initially unknown, the procedure has constant success probability if the number of repetitions is a constant fraction of $\pi/4\tilde{p}$. Thus, taking note from [BHMT00] we repeat the entire process with a geometrically increasing number of repetitions each time: 1,2,4,8,..., until a power of two is reached which is $\geq \kappa$. This yields constant success probability using $\leq 4\kappa$ repetitions.

The runtime of this algorithm is thus $\widetilde{O}(\kappa(T_B + t_0 s^2 \log N))$, where the first term comes from preparing $|b\rangle$ and the second from the quantum simulation. We also have that $t_0 = O(\kappa/\epsilon)$ so the runtime can be written as $\widetilde{O}(\kappa T_B + \kappa^2 s^2 \log(N)/\epsilon)$.

2.3 Reduction of a Quantum Circuit to Matrix Inversion

The optimality of HHL is shown for a specific definition of the matrix inversion problem, which is defined as follows.

Definition 3. (Quantum) Matrix Inversion: An algorithm solves matrix inversion if it has:

• **Input:** An O(1)-sparse matrix A specified using an oracle or via a poly $\log(N)$ -time algorithm that returns the non-zero elements of a row.

• Output: A bit that equals one with probability $\langle x|M|x\rangle \pm \epsilon$, where $M=|0\rangle\langle 0|\otimes I_{N/2}$ corresponds to measuring the first qubit and $|x\rangle$ is a normalised state proportional to $A^{-1}|b\rangle$ for $|b\rangle = |0\rangle$.

We also demand that A be Hermitian and $\kappa^{-1}I \leq A \leq I$.

A relativising algorithm is one in which A is specified by an oracle. Despite this very weak definition for matrix inversion, this task is still classically hard.

The authors of [HHL09] show that a quantum circuit using n qubits and T gates can be simulated by inverting an O(1)-sparse matrix A of dimension $N = O(2^n \kappa)$. If we need A to be positive definite, $\kappa = O(T^2)$ and is O(T) otherwise. The reduction proceeds as follows: Let \mathcal{C} be a quantum circuit acting on $n = \log N$ qubits applying T two-qubit gates $U_T \cdots U_1$. The initial state is $|0\rangle^{\otimes n}$ with the answer being the result of measuring the first qubit.

We now adjoin an ancilla register of dimension 3T and define the unitary:

$$U = \sum_{t=1}^{T} |t+1\rangle\langle t| \otimes U_t + |t+T+1\rangle\langle t+T| \otimes I + |t+2T+1 \bmod 3T\rangle\langle t+2T| \otimes U_{3T+1-t}^{\dagger}.$$
 (13)

The unitary U has been chosen such that for $T+1 \le t \le 2T$, applying U^t to $|1\rangle |\psi\rangle$ yields $|t+1\rangle \otimes U_T \cdots U_1 |\psi\rangle$. We can see this as the first T+1 applications of U return $|T+2\rangle \otimes U_T \cdots U_1 |\psi\rangle$ (first term of Eq. 13). We see from the second term of (13) that for the next $t' \le T-1$ applications the action on the $|\psi\rangle$ register remains unchanged, while the ancilla variable is merely being incremented.

We can now define $A = I - Ue^{-1/T}$, which gives $\kappa(A) = O(T)$. This expands as

$$A^{-1} = \sum_{k \ge 0} U^k e^{-k/T}.$$
 (14)

We can see Eq. 14 holds by multiplying by A, then observing all terms in the series apart from k=0 cancel. We can also interpret this as applying U^t for t a geometrically distributed random variable. As $U^{3T}=I$, we can assume $1 \le t \le 3T$. Measuring the first register and obtaining $T+1 \le t \le 2T$ occurs with probability $e^{-2}/(1+e^{-2}+e^{-4}) \ge 1/10$ (taking amplitude(t) = $e^{-t/T}$ modulo normalisation). If we obtain this result, the second register is left in the state $U_T \cdots U_1 |\psi\rangle$. By drawing t from a geometric distribution and applying t many times to t0 and post-selecting on t1 and t2 are t3. Sampling the resulting state is equivalent to sampling t3.

Since for any quantum circuit \mathcal{C} there is an associated matrix $A_{\mathcal{C}}$ which, when inverted then sampled from, will in a fixed fraction of instances give the same results as sampling from the output of \mathcal{C} , Matrix Inversion (as defined in Definition 3) is BQP-complete.

2.4 Optimality of HHL

In order to simulate a quantum circuit up to some pre-determined accuracy ϵ , the simulations need to be iterated. That is, at iteration i, one uses the technique above to simulate the circuit at iteration i-1. The authors show that if one can solve matrix inversion in time $\kappa^{1-\delta}(\log(N)/\epsilon)^{c_1}$ for constants $c_1 \geq 2, \delta > 0$, then a computation with $T \leq 2^{2n}/18$ gates can be simulated with a polynomial number of qubits and gates. The TQBF (totally quantified Boolean formula satisfiability) problem requires time $T \leq 2^{2n}/18$ by exhaustive enumeration and is PSPACE-complete. Thus a quantum algorithm for matrix inversion running in time $\kappa^{1-\delta}$ poly $\log N$ could efficiently solve TQBF, thus implying PSPACE = BQP.

2.5 Non-Hermitian Matrices

We now consider the case where A is neither square nor Hermitian. Let us now suppose that we have $A \in \mathbb{C}^{m \times n}$, $\mathbf{b} \in \mathbb{C}^m$ and $\mathbf{x} \in \mathbb{C}^n$ with $m \leq n$. Generically the linear system $A\mathbf{x} = \mathbf{b}$ is underconstrained. The singular value decomposition of A is

$$A = \sum_{j=1}^{m} \sigma_j |u_j\rangle\langle v_j|, \qquad (15)$$

where $|u_j\rangle \in \mathbb{C}^m$, $|v_j\rangle \in \mathbb{C}^n$ and $\sigma_1 \geq \cdots \geq \sigma_n \geq 0$. Now define

$$H := \sum_{j=1}^{m} \sigma_j(|0\rangle\langle 1| \otimes |u_j\rangle\langle v_j| + |1\rangle\langle 0| \otimes |v_j\rangle\langle u_j|) \equiv \begin{pmatrix} 0 & A \\ A^{\dagger} & 0 \end{pmatrix}.$$
 (16)

The matrix H is Hermitian with eigenvalues $\pm \sigma_1, \ldots, \pm \sigma_m$, corresponding to eigenvectors $\left| w_j^{\pm} \right\rangle := \frac{1}{\sqrt{2}} (|0\rangle |u_j\rangle \pm |1\rangle |v_j\rangle$). This can be verified by direct substitution into Eq. 16. It also has n-m zero eigenvalues, with eigenspace V^{\perp} , where $V := \operatorname{span}(|v_1\rangle, \ldots, |v_m\rangle)$.

HHL now runs with the input $|0\rangle |b\rangle$. If $|b\rangle = \sum_{j=1}^{m} \beta_j |u_j\rangle$ then

$$\sum_{j=1}^{m} \beta_j \frac{1}{\sqrt{2}} \left(\left| w_j^+ \right\rangle + \left| w_j^- \right\rangle \right) \tag{17}$$

and upon running of the algorithm we get

$$H^{-1} |0\rangle |b\rangle = \sum_{j=1}^{m} \beta_{j} \sigma_{1}^{-1} \frac{1}{\sqrt{2}} \left(\left| w_{j}^{+} \right\rangle - \left| w_{j}^{-} \right\rangle \right) = \sum_{j=1}^{m} \beta_{j} \sigma_{j}^{-1} |1\rangle |v_{j}\rangle. \tag{18}$$

If we discard the $|1\rangle$, we can recognise this expression as the Moore-Penrose pseudoinverse of A applied to $|b\rangle$. The definition of the Moore-Penrose pseudoinverse is provided in Definition 4. Thus, on non-square, non-Hermitian A, HHL outputs a state $|x\rangle := A^+ |b\rangle$.

Now in the overconstrained case where $m \geq n$, the equation $A|x\rangle = |b\rangle$ is only satisfiable if $|b\rangle \in U$, where $U = \operatorname{span}(|u_1\rangle, \dots, |u_n\rangle)$. In this case, applying H to $|0\rangle |b\rangle$ will return a valid solution. Otherwise the state $|x^*\rangle$ is returned, which minimises the squared error loss, i.e. $|x^*\rangle := \arg\min_{|x\rangle \in \mathbb{R}^n} ||A|x\rangle - |b\rangle||_2^2$, which is again the Moore-Penrose pseudoinverse.

Definition 4. Let $A \in \mathbb{C}^{m \times n}$ have singular value decomposition given by $A = U\Sigma V^{\dagger}$ and be of rank r, with U and V unitary matrices. The *Moore-Penrose pseudoinverse* of A is given by

$$A^{+} = V \Sigma^{+} U^{\dagger}, \tag{19}$$

where $\Sigma^+ = \operatorname{diag}(\frac{1}{\sigma_1}, \dots, \frac{1}{\sigma_r}, 0, \dots, 0)$ for the singular values $\sigma_i, i \in [r]$. Further to this,

$$A^{+} = \begin{cases} \left(A^{\dagger}A\right)^{-1}A^{\dagger}, & \text{if } m \ge n; \\ A^{\dagger}\left(AA^{\dagger}\right)^{-1}, & \text{if } m \le n. \end{cases}$$
 (20)

References

- [BHMT00] G. Brassard, P. Høyer, M. Mosca and A. Tapp. Quantum Amplitude Amplification and Estimation (2000). arXiv:quant-ph/0005055.
- [CDFK12] Y. Cao, A. Daskin, S. Frankel and S. Kais. Quantum circuit design for solving linear systems of equations. Mol. Phys. An Int. J. Interface Between Chem. Phys., 110, 1675 (2012).
- [CKS15] A. M. Childs, R. Kothari and R. D. Somma. Quantum linear systems algorithm with exponentially improved dependence on precision (2015). arXiv:1511.02306.
- [GR02] L. Grover and T. Rudolph. Creating superpositions that correspond to efficiently integrable probability distributions (2002). arXiv:quant-ph/0208112v1.
- [HHL09] A. W. Harrow, A. Hassidim and S. Lloyd. Quantum algorithm for linear systems of equations. *Phys. Rev. Lett.*, **103**, 150502 (2009).
- [She94] J. R. Shewchuk. An Introduction to the Conjugate Gradient Method Without the Agonizing Pain. Tech. rep., Carnegie Mellon University (1994).