MPRI 2.34.2: Quantum Information and Cryptography **2024 - 2025**

Lecture 3: Quantum linear algebra

Lecturer: Simon Apers (apers@irif.fr)

In this lecture we touch on the topic of "quantum linear algebra". Broadly construed, this is the use of quantum algorithms to do linear algebraic operations such as matrix powering or linear system solving.

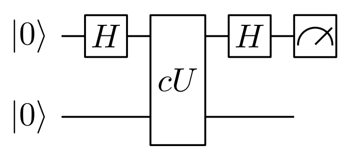
1 Quantum Hadamard test

Consider a situation where we have access to some "black-box unitaries" U_0 and U_1. Let $U_0 |0\rangle = |\psi_0\rangle$ and $U_1 |0\rangle = |\psi_1\rangle$. If we are promised that either $|\psi_0\rangle = |\psi_1\rangle$ or $|\psi_0\rangle \perp |\psi_1\rangle$, can we efficiently decide which is the case?

The answer turns out to be "yes", and the solution is a simple quantum algorithm called the quantum Hadamard test. If we define the controlled unitary

$$cU = |0\rangle \langle 0| \otimes U_0 + |1\rangle \langle 1| \otimes U_1,$$

then the quantum Hadamard test corresponds to the following circuit:



Exercise 1.

- *Show that from the output of this circuit we can distinguish whether $|\psi_0\rangle = |\psi_1\rangle$ or $|\psi_0\rangle \perp |\psi_1\rangle$.*
- *Show that you can build up cU from calls to $cU_i = |0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes U_i$ for $i = 1, 2$.*

This a very remarkable fact about quantum algorithms, and strongly contrasts with randomized algorithms. If we were given two *randomized* circuits that return n-bit probability distributions p_0 and p_1, then distinguishing $p_0 = p_1$ from p_0 and p_1 having disjoint supports would generally require $\Omega(2^{n/2})$ calls to the circuits!

A nice application of the quantum Hadamard test is the *graph isomorphism problem*. We are given two n-vertex graphs G_0 and G_1, and we are asked whether they are isomorphic. I.e., given their respective adjacency matrices A_0 and A_1, does there exist a permutation σ of the indices such that $A_1 = \sigma(A_0)$?

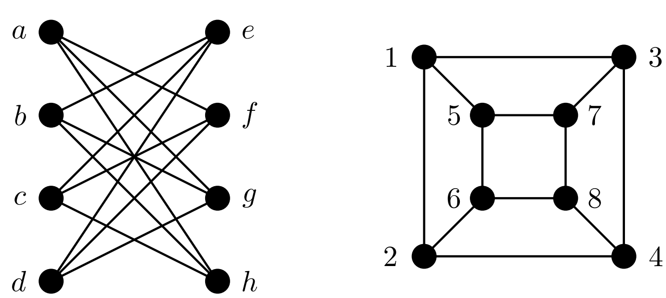


Figure 1: Isomorphic graphs.

Exercise 2. *Assume access to unitaries U_0 and U_1 such that $U_i |0\rangle = |\psi_i\rangle$ with $|\psi_i\rangle$ the uniform superposition over all possible permutations of G_i's adjacency matrix A_i. I.e.,*

$$|\psi_i\rangle \propto \sum_{\sigma \in S_n} |\sigma(A_i)\rangle .$$

Argue that the quantum Hadamard test solves the graph isomorphism problem with a single call to U_0 and U_1.

2 Linear Combination of Unitaries

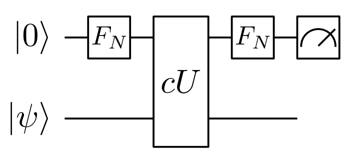
If we "postselect" on measurement outcome "0" in the quantum SWAP test circuit, then the output is proportional to

$$|0\rangle (U_0 + U_1) |0\rangle .$$

Effectively one could argue that the circuit takes the sum of two unitaries (which might no longer be a unitary). We can generalize this to more unitaries U_0, U_1, ..., U_{N-1} for $N = 2^n$ by defining the controlled unitary

$$cU = \sum_{k=0}^{N-1} |k\rangle \langle k| \otimes U_k$$

and invoking the following circuit (where F_N is the N-dimensional Fourier transform):



Exercise 3.
- *What is the output of this circuit if we postselect on measurement outcome "0"?*
- *What is the probability of obtaining outcome "0"?*
- *What is the output of the quantum phase estimation circuit from Lecture 1 if we postselect on measurement outcome "0"?*

Generalizing this even further, consider a set of nonnegative coefficients $c_1, c_2, \ldots, c_N$ satisfying $\sum_k c_k = 1$ and define the "select unitary" U_{sel} as any unitary satisfying

$$U_{\text{sel}} |0\rangle = \sum_{k=0}^{N-1} \sqrt{c_k} |k\rangle .$$

Now consider the following circuit, which implements the so-called "linear combination of unitaries" (LCU) technique:

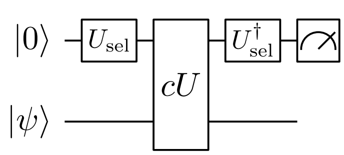


Figure 2: LCU circuit.

Exercise 4. *What is the output of this circuit if we postselect on measurement outcome "0"?*

3 Quantum linear system solving

Consider a linear system $Ax = b$ for some invertible matrix $A \in \mathbb{C}^{N \times N}$. Given appropriate query access to A and b, we wish to compute the solution $x = A^{-1}b$. In a famous work, Harrow, Hassidim and Lloyd [HHL09] proposed a quantum algorithm that returns a *quantum state* $|x\rangle$ encoding the solution in time $\mathrm{poly}(\kappa) \cdot \mathrm{polylog}(N)$. Here κ is the condition number of A, defined by the ratio of the largest over the smallest eigenvalue of A in magnitude. If $\kappa \in O(\mathrm{polylog}(N))$ (i.e., A is "well-conditioned") then this is exponentially faster than the usual classical algorithms for matrix inversion, which take time $\mathrm{poly}(N)$.

Exercise 5. *We can argue that, without loss of generality, we may assume that A is Hermitian. To prove this, show that for a general invertible A we can always find a solution of the linear system $Ax = b$ by solving the alternative Hermitian linear system*

$$\begin{bmatrix} 0 & A \\ A^\dagger & 0 \end{bmatrix} y = \begin{bmatrix} b \\ 0 \end{bmatrix}.$$

While there are different versions of the HHL algorithm, we will describe the algorithm from [CKS17] that combines Hamiltonian simulation with the LCU technique. At its core is the existence of an (approximate) Fourier expansion of the inverse function $1/x$ (valid for the range $1/\kappa \leq |x| \leq 1$) of the form

$$\frac{1}{x} \approx \kappa \sum_{k=0}^{O(\kappa)} c_k e^{ikx}, \tag{1}$$

where for simplicity we assume that $c_k \geq 0$ and $\sum_k c_k = 1$. This implies that we can also rewrite the matrix inverse

$$A^{-1} \approx \kappa \sum_{k=0}^{O(\kappa)} c_k e^{ikA},$$

and so A^{-1} can be approximated by a linear combination of (unitary!) matrix exponentials. This leads to an algorithm by defining the c_k's in U_{sel} to be those in (1), and picking the unitaries

$$U_k = e^{ikA}.$$

Notice that we can implement these unitaries using a quantum algorithm for Hamiltonian simulation. The algorithm is then given by the LCU circuit from Fig. 2.

Exercise 6.
- *What is the output of the circuit, when applied to the state $|0\rangle\,|b\rangle$, and postselected on outcome "0"?*
- *Argue about the complexity of the resulting algorithm.*

References

[CKS17] Andrew M. Childs, Robin Kothari, and Rolando D. Somma. Quantum algorithm for systems of linear equations with exponentially improved dependence on precision. *SIAM Journal on Computing*, 46(6):1920–1950, 2017.

[HHL09] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical review letters*, 103(15):150502, 2009.