Lecture & Proseminar 250078/250042
"Quantum Information, Quantum Computation, and Quantum Algorithms" WS 2024/25

— Exercise Sheet #9 —

Problem 1: Phase estimation

Consider a unitary U with an eigenvector $U|\phi\rangle = e^{2\pi i\phi}|\phi\rangle$. Assume that

$$\phi = 0.\phi_1\phi_2\dots\phi_n = \tfrac{1}{2}\phi_1 + \tfrac{1}{4}\phi_2 + \dots + \tfrac{1}{2^n}\phi_n \ ,$$

i.e. ϕ can be exactly specified with n binary digits. Our goal will be to study ways to determine ϕ as accurately as possible, given that we can implement U (and are given the state $|\phi\rangle$).

1. First, consider that we use controlled-U operations $CU|0\rangle|\phi\rangle = |0\rangle|\phi\rangle$, $CU|1\rangle|\phi\rangle = |1\rangle e^{2\pi i\phi}|\phi\rangle$. Describe a protocol where we apply CU to $|+\rangle|\phi\rangle$, followed by a measurement in the $|\pm\rangle$ basis, to infer information about ϕ. Which information, and to which accuracy, can we obtain with N iterations? (*Bonus question:* Could this scheme be refined by changing the measurement?)

2. Now consider a refined scheme. To this end, assume we can also apply controlled-$U^{(2^k)} \equiv CU_k$ operations for integer k efficiently.

   a) We start by applying CU_{n-1} to $|+\rangle|\phi\rangle$. On what property of ϕ does the resulting state depend? Which information can we thus infer? What measurement do we have to make to obtain this information with a single measurement?

   b) In the next step, we apply CU_{n-2}, *knowing* the result of step a). What information can we infer, given that we know the result of the previous measurement and can use it to adapt the measurement? What measurement do we have to make? Rephrase the measurement as a unitary rotation followed by a measurement in the $|\pm\rangle$ basis.

   c) Iterating the preceding steps, describe a procedure (circuit) to obtain $|\phi\rangle$ exactly. How many times do we have to evaluate controlled-$U^{(2^k)}$'s?

3. An alternative way to determine ϕ is to use the quantum Fourier transform. To this end, we apply a transformation $\sum_x |x\rangle|\phi\rangle \mapsto \sum_x |x\rangle U^x|\phi\rangle$, followed by a quantum Fourier transform and a measurement in the computational basis. Show that this protocol also yields the desired outcome, by expressing the state $\sum_x |x\rangle U^x|\phi\rangle$ using $U|\phi\rangle = e^{2\pi i\phi}|\phi\rangle$, and the properties of the quantum Fourier transform. How many $U^{(2^k)}$'s are required?

4. Compare the two protocols derived in step 2 and 3, using the fact that we can commute measurements in the computational basis and controlled operations (cf. Sheet 7, Problem 3).

(*Note:* This procedure, which allows to estimate the eigenvalue of a unitary, given a corresponding eigenvector, is known as *quantum phase estimation.*)

Problem 2: Fast Fourier transform.

In this problem, we will use the expression

$$\hat{\mathcal{F}} : |j_1,\dots,j_n\rangle \mapsto \tfrac{1}{2^{n/2}}\big(|0\rangle + e^{2\pi i\, 0.j_n}|1\rangle\big) \otimes \big(|0\rangle + e^{2\pi i\, 0.j_{n-1}j_n}|1\rangle\big) \otimes \dots \otimes \big(|0\rangle + e^{2\pi i\, 0.j_1 j_2\dots j_n}|1\rangle\big) \quad (1)$$

for the quantum Fourier transform $\hat{\mathcal{F}}$ derived in the lecture to construct an algorithm for the classical Fourier transformation on vectors of length $N = 2^n$ which scales as $O(2^n n) = O(N\log N)$ – the fast Fourier transformation (FFT) – as opposed to the naive $O(N^2)$ scaling.
Recall that the classical Fourier transformation $\mathcal{F} : \mathbb{C}^N \to \mathbb{C}^N$ acts as $\mathcal{F} : (x_0,\dots,x_{N-1}) \mapsto (y_0,\dots,y_{N-1})$, where

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i\, jk/N} x_j \ . \quad (2)$$

1. Show that performing the classical Fourier transformation by directly carrying out the sum in Eq. (2) requires $O(N^2)$ elementary operations.

2. As shown in the lecture, $\hat{\mathcal{F}}$ maps $\sum_j x_j|j\rangle$ to $\sum_k y_k|k\rangle$. Use this, combined with Eq. (1), to derive an explicit expression for y_k in terms of the x_j in the spirit of Eq. (1).

3. The resulting expression for y_k as a function of the x_j should contain a sum over $j_1, \ldots, j_n$. Show that this sum can be carried out bit by bit. (What should happen is that in each step, the "input" x_j is transformed to a vector where one j_i disappears due to the sum, and instead a dependency on one of the k_ℓ appears.)

4. What is the number of elementary operations required for each of these transformations? What is the total computational cost of the algorithm?

Problem 3: Factoring 15

Verify the factoring algorithm (i.e., the reduction to period finding described in the lecture – subsection 3.c) for $N = 15$ – i.e., consider all $a = 2, \ldots, N-1$, check wether $\gcd(a, N) = 1$, find r s.th. $a^r \bmod N = 1$ (you don't have to use a quantum computer), and check if this can be used to compute a non-trivial factor of N. How many different cases do you find? What possible periods r appear?