Freie Universität Berlin

Tutorials on Quantum Information Theory

Winter term 2021/22

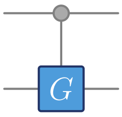
Problem Sheet 11
Aspects of quantum algorithms and circuits

J. Eisert, A. Nietner, F. Arzani, C. Bertoni, R. Suzuki

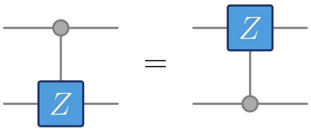
1. **Control gates.** (5 points: 3+2) Control gates are among the most ubiquitous 2-qubits gates found in quantum computation. Given a gate G, control-G is given by

$$\mathrm{c}G = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes G \tag{1}$$

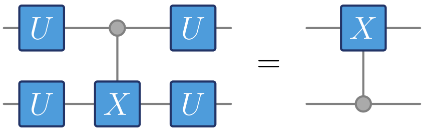
that is, the gate G is applied to the second qubit if the first one is in the state 0, and otherwise nothing is done. This is usually denoted as



a) Show that



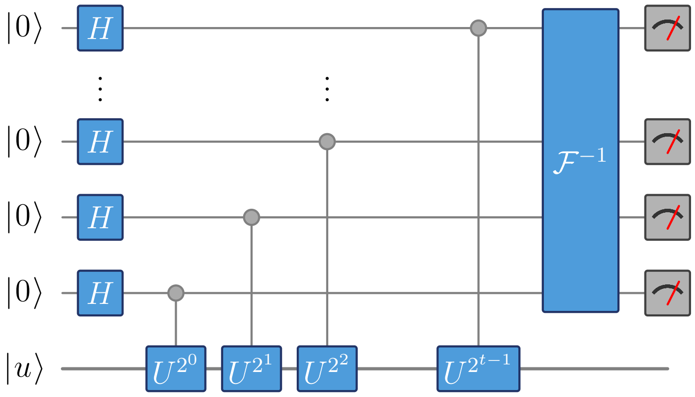
b) The control-X gate is usually called cNOT. The roles of the two inputs to the cNOT gate can be exchanged by applying the gate in a basis other than the computational basis. Find a local unitary that applied to all inputs and outputs and turns a cNOT gate controlled by the first register into one controlled by the second register., i.e. U such that



2. **Phase estimation.** (11 points: 1+1+2+1+1+2+2+1) Perhaps at the heart of the majority of modern quantum algorithms lies the *phase estimation algorithm.* The problem of phase estimation is the following: Given a unitary operator U and one of its eigenvectors $|u\rangle$ with eigenvalue $\mathrm{e}^{2\pi\mathrm{i}\phi}$, output the phase ϕ.

a) On the last sheet the definition and the circuit of the quantum Fourier transform was given. Show that the Quantum Fourier transform is invertible and give its inverse.

The phase estimation algorithm is implemented via the following quantum circuit:



The circuit constists of H, the Hadamard gate, controlled-U^{2^k}-gates, that apply the unitary operator U for 2^k times if the control qubit is $|1\rangle$, the inverse of the quantum Fourier transform $\mathcal{F}^{-1}$ and a measurement in the computational basis at the very end. At the beginning, the first register comprising t qubits is initialised as $|0\rangle^{\otimes t}$ and the second register is prepared in the state $|u\rangle$.

b) Express the state of the t-qubits in the first register before the inverse Fourier transform is applied in the computational basis $\{|x\rangle\}_{x\in\{0,1\}^t}$.

c) Assume that ϕ can be written with exactly t bits, i.e. $\phi = \sum_{k=1}^{t} 2^{-k}\phi_k$. Show that the measurement result at the end is $|\phi_1 \dots \phi_t\rangle$ with probability 1.

If the phase does not happen to have a t-bits representation, it is possible to show that a measurement outcome close to ϕ occurs with high probability. From now on we will assume all phases mentioned have t-bits representations.

d) Suppose now that instead of applying the unitaries to an eigenstate we apply them to some superposition $|\psi\rangle = \sum_i c_i|u_i\rangle$, where $|u\rangle_i$ is an eigenvector of U with eigenvalue $e^{2\pi \mathrm{i}\phi_i}$. What does the algorithm output?

e) How many calls of the unitary operator are required in the algorithms?

In the lecture, you saw how the problem of finding prime factors of an integer N can be reduced to finding the period of a certain function defined as

$$f(x) = a^x \mod N. \tag{2}$$

If $f(x+r) = f(x)$ where r is even and $a^{r/2} \not\equiv -1 \mod N$, then $a^r - 1 = (a^{r/2}+1)(a^{r/2}-1) = 0 \mod N$, this implies that $a^{r/2} \pm 1$ and N have nontrivial common divisors, which can be found using Euclid's algorithm, hence finding a non trivial factor of N. An a such that r has the right properties can be guessed with high probability.

r, the smallest integer such that $a^r \mod N = 1$, is called the *order* of a in $\mathbb{Z}_N$.

The crucial point of Shor's algorithm is then to find the period of f, we want to elaborate how this can be done through period finding. Consider the operator

$$U|x\rangle = \begin{cases} |xa \mod N\rangle & \text{if } x < N \\ |x\rangle \text{ otherwise} & \end{cases} \tag{3}$$

f) Using that a and N are coprimes, show that U is a unitary.

g) Show that U has eigenvalues of the form $e^{2\pi \mathrm{i}k/r}$ for integers $0 \leq k < r$. Find the corresponding eigenvectors, knowing that they are of the form

$$|v_s\rangle = \sum_{k=0}^{r-1} \alpha_{k,s}|a^k \mod N\rangle \tag{4}$$

Now we are able to get $q = k/r$ for $k \in \mathbb{N}$, we could use this to find a guess of r by simply finding a fraction representation of q, but if k and r have a common divisor d, this will yield $r' = r/d$, as $q = k'/r' = (k/d)/(r/d)$. This can be easily dealt with by running the algorithm multiple times for different eigenvectors and get $k_1/r = k_1'/r_1', k_2/r = k_2'/r_2', \ldots$. With high probability, r is the least common multiple of the r_i'.

We are almost done, the only element we're missing is that in general we do not know how to prepare the eigenvectors of U.

h) What is the output of the phase estimation algorithm for the unitary U if we input the vector $|1\rangle$? Why does this solve the problem?

3. **Probabilistic algorithm for Deutsch-Josza.** (4 points)

The Deutsch-Josza algorithm can determine whether a function $f : \{0,1\}^n \to \{0,1\}$ is balanced or constant by invoking the function (or more precisely a quantum implementation of the function) only a single time. In contrast, a deterministic classical algorithm needs to invoke the function exponentially $\mathcal{O}(2^n)$ often (at least in a worst-case scenario).

Assume instead that the goal is not to distinghuish these two cases with certainty, but only with a probability $p > 1/2$. Find a classical algorithm that performs better than the previously mentioned brute force approach. How does it perform?