Freie Universität Berlin

Tutorials on Quantum Information Theory

Winter term 2020/21

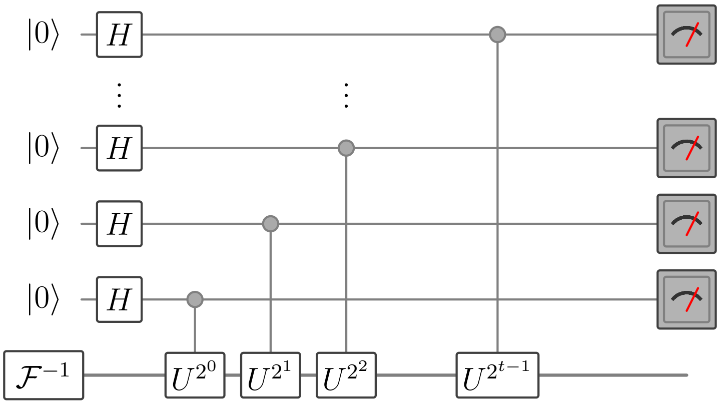
Problem Sheet 10
Aspects of quantum algorithms and circuits

J. Eisert, J. Haferkamp, J. C. Magdalena De La Fuente

1. **Phase estimation.** 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 $\mathrm{e}^{2\pi \mathrm{i}\phi}$, the phase estimation problem is to 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 tranform is a unitary operator and draw the circuit implementing the inverse of the Fourier transform.

   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 $|u\rangle$. For simplicity we assume that ϕ can be written with exactly t bits, i.e. $\phi = \sum_{k=1}^{t} \phi_k 2^{-k}$ with $\phi_k \in \{0, 1\}$.

   b) Show that the algorithm works.

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

   d) What is the computational complexity of a classical solution to the phase estimation problem?

   e) Sketch why phase estimation constitutes the core of Shor's algorithm.

2. **Control gates.**

   a) Show that the control-Z gate is invariant under swapping the two inputs with each other and the two outputs.

   b) The roles of the two inputs to the cNOT gate can be exchanged by applying the gate in another basis 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.

3. **Probabilistic algorithm for Deutsch-Josza.**

   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 $p > 1/2$. How does the best classical algorithm for this problem perform?