Quantum Computing

Instructor: Alexander Razborov, University of Chicago.
razborov@uchicago.edu
Course Homepage: www.cs.uchicago.edu/~ razborov/teaching/winter25.html

Winter Quarter, 2025

You may work together on solving homework problems, but put all the names of your collaborators clearly at the top of the assignment. Everyone must turn in their own independently written solutions. Shopping for solutions on the Internet (or asking ChatGPT and such) is strongly discouraged but if you do it anyway, you must completely understand the proof, explain it in your own words and include the URL. On the contrary, shopping for useful facts is encouraged.

Prove all your answers with ‘‘reasonable’’ degree of rigor.

PDF file **prepared from a TeX source** is the preferred format. In that case you will get back your feedback in a neat annotated form.

Homework 1, due February 7

1. Prove that the basis $\{\mathrm{CNOT}, \mathrm{TOFFOLI}, \mathrm{FREDKIN}\}$ is not complete for reversible computation even in the presence of ancilla bits. In other words, show the existence of a permutation $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ such that there does not exist any reversible circuit C in this basis with the property $C(x, 0^L) = (f(x), 0^L)$ for all $x \in \{0,1\}^n$ (L is arbitrary).

2. Prove that any real square matrix that is both stochastic and orthogonal is necessarily double stochastic.

3. Consider the following modification of the Deutch-Josza problem.

   Input. A function $f : \{0,1\}^n \longrightarrow \{0,1\}$ with the promise that f is imbalanced, i.e. $|f^{-1}(1)| \neq 2^{n-1}$.

   Goal. Determine whether f is balanced towards 0 or 1.

Prove that no quantum circuits using arbitrarily many qubits and arbitrarily many phase-flipping oracle gates $U_f^* |x\rangle \stackrel{\text{def}}{=} (-1)^{f(x)} |x\rangle$ (as well as unitaries not depending on f) can solve this problem in the worst case with probability $> 1/2$.

4. Which of the following statements are always true (prove your answer):

   (a) if A and B are normal operators then AB is normal;

   (b) if A and B are normal operators then $A + B$ is normal;

   (c) if A is normal and U is unitary then $U^\dagger AU$ is normal;

   (d) if A is normal and H is Hermitian then HAH is normal.

5. Prove the uniqueness theorem for continued fractions: if $[a_0; a_1, \ldots, a_n] = [b_0; b_1, \ldots, b_m]$ and, say, $m \geq n$ then either $m = n$ and $a_i = b_i$ $(0 \leq i \leq n)$ or $m = n+1,\ a_i = b_i\ (0 \leq i \leq n-1),\ a_n \geq 2,\ b_n = a_n - 1,\ b_{n+1} = 1$.