Quantum Computing

Instructor: Alexander Razborov, University of Chicago.
razborov@cs.uchicago.edu
Course Homepage: www.cs.uchicago.edu/~ razborov/teaching/winter18.html

Winter Quarter, 2018

Homework 1, due February 8 at the beginning of the class. LaTeX submissions are strongly encouraged and accepted until Friday morning.

1. (a) Describe all permutations $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ that can be realized by a reversible circuit with reversible gates on ≤ 2 bits.

   (b) Using the description, prove the following: if a permutation $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ can be in principle computed by a circuit of this kind then it can be computed by such a circuit of polynomial size.

2. Let $\mathsf{PP}(\log)$ be the class of languages $L \subseteq \{0,1\}^*$ that can be recognized by a probabilistic Turing machine with unbounded error (that is, we only require that $\mathbf{P}[x \in L \equiv M(x) \text{ accepts}] > 1/2$, without specifying the margin) that is allowed to roll $O(\log n)$ cubic dice during its execution on any input x of length n.

   Prove that $\mathsf{PP}(\log) = \mathsf{P}$.

3. Let, as usual, $\mathcal{H} = \mathbb{C}^{\{0,1\}^n}$, define the bi-linear mapping $* : \mathcal{H} \times \mathcal{H} \longrightarrow \mathcal{H}$ on basic states by the formula

$$|x\rangle * |y\rangle \stackrel{\text{def}}{=} |x \oplus y\rangle$$

   and extend it by (Hermitian) linearity so that it satisfies $(\alpha v) * w = \alpha^*(v * w), v * (\alpha w) = \alpha(v * w)$ $(\alpha \in \mathbb{C})$, $(v_1 + v_2) * w = v_1 * w + v_2 * w$, $v * (w_1 + w_2) = v * w_1 + v * w_2$.

   (a) Give an explicit description of the operator $\widehat{*} : (v, w) \mapsto H^{\otimes n} (H^{\otimes n}(v) * H^{\otimes n}(w))$.

(b) For $S \subseteq \{0,1\}^n$, let $|S\rangle \stackrel{\text{def}}{=} \frac{1}{|S|^{1/2}} \sum_{x \in S} |x\rangle$. Describe all pairs of sets S, T for which $\widehat{*}(|S\rangle, |T\rangle) = 0$.

4. Prove that for any (regardless of its size) quantum circuit C that uses oracle access to the operator $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$ for finding w such that $f(w) = 1$ there exists a non-zero function $f : \{0,1\}^n \longrightarrow \{0,1\}$ on which C errs with probability $\geq 1/2$.

5. Prove that for any unitary operator U and $\epsilon > 0$ there exists r such that U^r is ϵ-close to the identity operator.