Quantum Complexity Theory, UPB
Winter 2020, Assignment 3

To be completed by: Tuesday, December 1, start of tutorial

1 Exercises

1. **BPP versus BQP.**
   (a) Is BPP $\subseteq$ PromiseBPP? Is PromiseBPP $\subseteq$ BPP?
   (b) A fact that is believed to separate BPP from BQP is the Sipser-Gács-Lautemann theorem, which states that BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$. Here, Σ_2^p is the second level of the Polynomial-Time Hierarchy (PH), defined roughly as NP with a second, universally quantified poly-size witness. Slightly more formally, the YES and NO cases of Σ_2^p are:
   - If $x \in L$, $\exists$ poly-size proof y, such that $\forall$ poly-size proofs z, the verifier accepts (x, y, z).
   - If $x \notin L$, then $\forall$ poly-size proofs y, $\exists$ a poly-size proof z, such that the verifier rejects (x, y, z).

   In contrast, it is believed that BQP is *not* contained in *any* level of PH. (If you have never seen PH before, this would be an excellent excuse to procrastinate via a visit to Wikipedia.) In this exercise, you will prove the Sipser-Gács-Lautemann theorem. For this, you will use the *probabilistic method* and the *union bound*, two useful techniques in basic probability theory.

   Setup. Let M be a BPP machine for language L. Without loss of generality, assume we have applied standard error reduction so that the completeness and soundness parameters for M are $1 - 2^{-n}$ and 2^n, for $n = |x|$ for $x \in \{0,1\}^*$ the input. Also, M takes in m random bits. Define $R_x \subseteq \{0,1\}^m$ to be set of all random strings r such that M accepts (x, r). Define a *translation* for R_x by string $t \in \{0,1\}^m$ as

   $$R_x \oplus t = \{y \oplus t \mid y \in R_x\},$$

   for $\oplus$ the bit-wise XOR. Given strings $y_1, \ldots, y_m \in \{0,1\}^m$, define $M(y_1, \ldots, y_m)$ to be a modification of M which accepts if its random string r appears in *at least one* translation of R_x, i.e.

   $$r \in R_x \oplus y_i \text{ for some } i \in [m].$$

   Questions.
   i. Prove that if $x \in L$, there exist $y_1, \ldots, y_m \in \{0,1\}^m$ such that for all $r \in \{0,1\}^m$, $M(y_1, \ldots, y_m)$ accepts (x, r). (Hint: Use the probabilistic method — pick $y_1, \ldots, y_m$ uniformly at random, and show that there is non-zero probability the claim holds. For this, first upper bound the probability that r is not in one of the translations defined by the y_i. Then look up the union bound/Boole's inequality.)
   ii. If $x \notin L$, for all $y_1, \ldots, y_m \in \{0,1\}^m$, there exists $r \in \{0,1\}^m$, such that $M(y_1, \ldots, y_m)$ rejects (x, r). (Hint: A straightforward bound will work here, thanks to the fact that you assumed an exponentially small soundness parameter.)
   iii. Why do the previous two exercises together show BPP $\subseteq \Sigma_2^p$?

2. **Perturbations to quantum gate sequences.** Prove Lemma 19 of the Lecture 3 notes.

3. **Quantum eigenvalue surgery.** Assume $A \in \mathrm{Pos}\left(\mathbb{C}^N\right)$ is a positive semidefinite, s-sparse matrix satisfying $\| A \|_\infty \leq 1$, and that you have a black box preparing state $|b\rangle \in \mathbb{C}^N$. Assume further that all eigenvalues λ_j of A require at most n bits to represent, for some integer $n > 0$. Show how to use quantum eigenvalue surgery to probabilistically simulate operation $\sqrt{A}|b\rangle$. You may assume all operations are error-free (other than the fact that postselection can fail, as in the course notes). Give a bound on success probability (in terms of $\lambda_{\min}(A)$) and runtime. (Bonus: What if A is unitary instead?)