[P6] (Chernoff bound). A language L is in BPP if there is a poly-time randomized Turing machine T such that for every input x we have

$$\Pr[T(x) = L(x)] > \frac{2}{3}.$$

Here, we will prove that the success probability 2/3 can be replaced by any fixed probability without changing the set of languages in BPP.

Suppose we run the Turing machine m times on the same input string x. For $i = 1, \ldots, m$, let $X_i \in \{0, 1\}$ be the random variable describing the outcome of the ith computation. We employ a "majority voting" strategy and accept x if more than half the X_i are equal to 1 (i.e. if $\sum_{i=1}^m X_i > \frac{m}{2}$) and reject x otherwise (for simplicity, assume that m is even).

We'll analyze the situation where x is in fact in L. Let $\epsilon = \frac{2}{3} - \frac{1}{2} = \frac{1}{6}$ the "bias towards the right answer of a single run". The *Chernoff-Hoeffding* bound (to be proven) says that

$$\Pr\left[\sum_{i=1}^m X_i \leq \frac{m}{2}\right] \leq e^{-2m\epsilon^2},$$

i.e. that the probability of not accepting x after m runs goes down exponentially in m.

(1) Let $x = (x_1, \ldots, x_m) \in \{0, 1\}^m$ be a string of possible outcomes. What is the probability $\Pr[X_1 = x_1, \ldots, X_m = x_m]$ of obtaining x? Show that if x contains at most $\frac{m}{2}$ ones, then

$$\Pr[X_1 = x_1, \ldots, X_m = x_m] \leq \frac{1}{2^m} \left(1 - 4\epsilon^2\right)^{m/2}.$$

(2) Verify (by a computer plot if necessary) that $1 - t \leq e^{-t}$ for all $t \geq 0$. Use this bound and the previous result to show that the probability of obtaining at most $\frac{m}{2}$ ones in m runs is smaller than $e^{-2m\epsilon^2}$.

(4) How large does one have to take m in order to obtain a probability of failure below 10^{-20}? Compare this to the probability that in the popular German "draw six balls from 49" lottery the same result will be obtained for three weeks in a row. (5 P.)

[P7] (Bloch sphere). State vectors of qubits can easily be visualized as points on a sphere. The technique allows us to gain intuition for their properties as well as the ones of single-qubit operations.

(1) The *Pauli operators*

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

play an important role in quantum mechanics and computing. Find their eigenvectors and eigenvalues.

(2) Up to an important global phase factor, any state vector $|\psi\rangle \in \mathbb{C}^2$ can be written as $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$ for suitable parameters θ, ϕ. A state vector is uniquely determined (why?) by the *density matrix* $\rho = |\psi\rangle\langle\psi|$. Show that the vector

$$(\mathrm{tr}\rho\sigma_x, \mathrm{tr}\rho\sigma_y, \mathrm{tr}\rho\sigma_z) \in \mathbb{R}^3$$

corresponds to the Cartesian coordinates of a point on the unit sphere with polar angle θ and azimuth angle ϕ (in this context, the unit sphere is referred to as *Bloch sphere*). Explain how this suggests a physical way of determining $|\psi\rangle$ given access to many copies. Where on the Bloch sphere do the eigenvectors of the Pauli matrices lie?

(3) One can check that the Pauli matrices anti-commute: $\sigma_i\sigma_j = -\sigma_j\sigma_i$ for $i, j \in x, y, z$, $i \neq j$. They also square to the identity matrix. Use these facts to compute $\sigma_x\sigma_x\sigma_x^\dagger, \sigma_x\sigma_y\sigma_x^\dagger, \sigma_x\sigma_z\sigma_x^\dagger$ and show that the action of the NOT gate is to rotate the Bloch sphere by 180 degrees about the x-axis (recall the Heisenberg picture!). The Hadamard gate also corresponds to a rotation. About which axis and by which angle? (5 P.)

[P8] (No cloning). It has been claimed in the lecture that there is no physical process which can take a qubit in an unknown state and produce two exact copies. We can actually prove a stronger result: namely that no theory that is compatible with experimental observations can have this property. Indeed, assume a theory would allow for a *copying process*, i.e. a method by which one system A is converted into two systems B, C with the property that any measurement performed on either B or C behaves in exactly the same way it would have, had it been performed on A.

Argue that such a theory can never predict Bell inequality violations. (2 P.)