Introduction to Quantum Computation, UPB
Winter 2022, Assignment 6

Due: Thursday, December 1, at start of tutorial

Exercises

1. Let X_p be a random variable denoting a coin flip with bias $p \in [0,1]$, i.e. a coin flip which lands HEADS with probability p. In class, we claimed the maximum entropy $H(X_p) = 1$ is achieved when $p = 1/2$, i.e. when we have a fair coin.

   (a) Convince yourself of this fact visually by plotting $H(X_p)$ as p ranges from 0 to 1. You may use a mathematics package such as Mathematica (available for download free at UPB), Matlab, GNU Octave (like Mathematica, but free for everyone), or anything that produces a plot. My hope is you will use this exercise as an excuse to download Mathematica or Octave and start tinkering with them, as they are very useful packages. (Matlab is excellent as well, but is not free at UPB.)

   (b) Now prove rigorously that in the range $p \in [0,1]$, $H(X_p)$ is maximized for $p = 1/2$. Hint: A simple and elegant proof can be given by first computing $2^{H(X_p)}$, and then applying the weighted Arithmetic-Geometric Mean inequality, which states in our setting that for $x_1, x_2, w_1, w_2 \geq 0$

   $$\frac{w_1 x_1 + w_2 x_2}{w_1 + w_2} \geq \sqrt[w_1+w_2]{x_1^{w_1} x_2^{w_2}}.$$

   (c) Use Part (b) to argue that among two-qubit pure states $|\psi_{AB}\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, the only states which are "maximally entangled" (i.e. maximizing the quantity $E(|\psi_{AB}\rangle)$ from class) are those whose reduced state is $\rho_A = I/2$.

   (d) Finally, prove that it does not matter whether we take ρ_A or ρ_B in Part (c) — namely, prove that for any $|\psi_{AB}\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$,

   $$S(\rho_A) = S(\rho_B).$$

   Observe that this is true even if $\rho_A \neq \rho_B$.

2. This question asks you to practice working with operator functions, as they play a fundamental role in quantum computation. In particular, you will show that an operator U is unitary if and only if there exists a Hermitian operator H such that $U = e^{iH}$ for complex number i. This ties back to one of the most important equations in quantum mechanics, the *Schrödinger* equation, which roughly says that quantum systems evolve in time according to some "Hamiltonian" H, whose action on the system is given by e^{iH}; this is how the notion of unitary evolution actually comes about.

   (a) Let $H \in \mathrm{Herm}(\mathbb{C}^n)$ and $c \in \mathbb{C}$. Using the Taylor series definition of e^{cH}, what does the spectral decomposition of e^{cH} look like?

   (b) Prove that for any $H \in \mathrm{Herm}\left(\mathbb{C}^d\right)$, e^{iH} is unitary.

   (c) Next, characterize the set of possible eigenvalues for a unitary matrix.

   (d) Now prove that for any unitary $U \in \mathrm{U}(\mathbb{C}^n)$, there exists an $H \in \mathrm{Herm}(\mathbb{C}^n)$ such that $U = e^{iH}$.

3. In stark contrast to the complex numbers, for which $e^{x+y} = e^x e^y$ for all $x, y \in \mathbb{C}$, the matrix analogue of this identity does *not* hold in general.

(a) Prove that for normal X, Y, if $[X, Y] = XY - YX = 0$, then $e^{X+Y} = e^X e^Y$. (Hint: Use the fact that commuting normal operators simultaneously diagonalize in a common eigenbasis.)

(b) Although $e^{X+Y} = e^X e^Y$ does not hold for all normal X and Y, the operator e^{X+Y} can nevertheless be approximated via the Lie Product Formula, which says that for any normal X and Y:

$$e^{X+Y} = \lim_{m \to \infty} \left(e^{\frac{X}{m}} e^{\frac{Y}{m}} \right)^m .$$

In words, to approximate e^{X+Y}, we can repeatedly switch back and forth between applying small slices of $e^{X/m}$ and $e^{Y/m}$ instead. (Think of m as a very large number.)

Prove the Lie Product formula. (Hints: Your goal is to argue that

$$e^{\frac{X}{m}} e^{\frac{Y}{m}} = e^{\frac{X}{m} + \frac{Y}{m} + O\left(\frac{1}{m^2}\right)}.$$

Once you have this, you can use the continuity of the exponential to take the limit as $m \to \infty$. To get the equation above, start by using Taylor series expansions to write $e^{\frac{X}{m}} e^{\frac{Y}{m}}$ up to first order terms. Then use the fact that there is a constant c which, for all $n \times n$ matrices B with $\| B \|_\infty < 1/2$, satisfies $\| \log(I + B) - B \|_\infty \leq c \| B \|_\infty^2$. Here, $\| X \|_\infty$ denotes the spectral or operator norm of matrix X, which can formally be defined equivalently as either the largest singular value of X, or the largest eigenvalue of $\sqrt{X^\dagger X}$. In the special case where X is diagonalizable, $\| X \|_\infty$ equals the largest absolute value of any eigenvalue of X, i.e. $\max_{\lambda(X)} |\lambda(X)|$.)