Math 280: Quantum Probability
Homework 4

This problem set is due Thursday, December 13, by 8pm in my mailbox.

All of the problems on this problem set concern the standard or "computational" basis for n qubits. The idea is that $|0\rangle$ and $|1\rangle$ is a standard orthonormal basis for the qubit Hilbert space $\mathbb{C}^2$, and then the space $(\mathbb{C}^2)^{\otimes n}$ for n qubits should have the tensor basis. The tensor products of these basis vectors are typically abbreviated by bit strings inside a single "ket", *e.g.*:

$$|10010\rangle = |1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle.$$

Also: A real or complex vector subspace of $M_n = M_n(\mathbb{C})$ is a *Lie algebra* when it is closed under the commutator operation $[A,B] = AB - BA$. In particular M_n itself is a Lie algebra under the new name $\mathfrak{gl}(n)$. Meanwhile a Lie group $G \subseteq M_n$ has a Lie algebra $\mathfrak{g}$, by definition its tangent space at the identity element $I \in G$. The Lie algebra of the unitary group $\mathrm{U}(n)$ is $\mathfrak{u}(n)$. Finally $\mathfrak{gl}(n)$ is a complexification of $\mathfrak{u}(n)$:

$$\mathfrak{gl}(n) = \mathfrak{u}(n) \oplus i\mathfrak{u}(n) \cong \mathfrak{u}(n) \otimes_{\mathbb{R}} \mathbb{C}.$$

4.1. One of the important facts about quantum gates is that 2-qubit gates are universal in a group-theoretic sense: Unitary gates in $\mathrm{U}(4)$ that act on pairs of qubits generate the Lie group $\mathrm{U}(2^n)$ acting on all n qubits. The aim of this exercise is to prove this by induction.

(a) Show that if you have $n \geq 3$ qubits and $\mathfrak{gl}(2^{n-1}) \otimes I$ acts on the left $n-1$ of them while $I \otimes \mathfrak{gl}(2^{n-1})$ acts on the right $n-1$ of them, then together these two Lie algebras generate $\mathfrak{gl}(2^n)$ (by taking repeated commutators). To get started with this exercise, you should look for elementary matrices A and B (matrices with a single non-zero entry) in $\mathfrak{gl}(2^{n-1})$ such that

$$C = [A \otimes I, I \otimes B]$$

is an elementary matrix in $\mathfrak{gl}(2^n)$. For instance, if $n = 3$

$$A|00\rangle = |11\rangle \qquad B|00\rangle = |01\rangle,$$

where A and B each annihilate the other 3 standard basis vectors, then

$$C|000\rangle = |111\rangle$$

and C also annihilates the other 7 standard basis vectors, so C is elementary. After making some elementary matrices in this way, you can take further commutators to eventually make all off-diagonal elementary matrices. Diagonal matrices can be recovered in a similar but slightly different way.

If this exercise seems too complicated for all n, try the case $n = 3$ for partial credit. (Or try that case first!)

***(b)** Prove that if $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are two real Lie algebras in $\mathfrak{u}(n)$, then they generate $\mathfrak{g}_3$ if and only if their complexifications $\mathfrak{g}_1 \otimes \mathbb{C}$ and $\mathfrak{g}_2 \otimes \mathbb{C}$ generate $\mathfrak{g}_3 \otimes \mathbb{C}$ in $\mathfrak{gl}(n)$.

***(c)** Prove that two connected Lie groups $G_1, G_2 \subseteq M_n$ generate a (necessarily connected) Lie group $G_3 \subseteq M_n$ if and only if the Lie algebras $\mathfrak{g}_1$ and $\mathfrak{g}_2$ generate $\mathfrak{g}_3$, where in each case $\mathfrak{g}_k$ is the Lie algebra of G_k.

(d) Combine (a), (b), and (c) to prove the assertion of the problem.

4.2. If $\mathbb{C}[S]$ is a Hilbert space with a finite standard basis S (maybe the Hilbert space of n qubits) and $T \subseteq S$ is a subset, then we can define the constant pure state

$$|T\rangle = \frac{1}{\sqrt{|T|}} \sum_{s \in T} |s\rangle \in \mathbb{C}[S].$$

Now let $f : S \to X$ be a function to another finite set X, and define the unitary embedding

$$U_f : \mathbb{C}[S] \to \mathbb{C}[S] \otimes \mathbb{C}[X] \cong \mathbb{C}[S \times X]$$

by

$$U_f|s\rangle = |s, f(s)\rangle.$$

Starting with $|S\rangle$, form the state $U_f|S\rangle$ and then discard the $\mathbb{C}[X]$ factor to obtain a certain mixed state $\rho \in \mathscr{L}(\mathbb{C}[S])^\Delta$. Show that

$$\rho = \sum_{x \in X} \frac{|f^{-1}(x)|}{|S|} \, |f^{-1}(x)\rangle\langle f^{-1}(x)|.$$

In other words, ρ is a weighted mixture of the constant states $|f^{-1}(x)\rangle$, weighted by the size of the inverse image $f^{-1}(x)$. (Hint: One way to get this formula is to imagine that someone else the system with Hilbert space $\mathbb{C}[X]$ out of the trash and measures it.)

4.3. This exercise describes Simon's algorithm, which is an important, simplified precursor to Shor's algorithm. Let

$$f : (\mathbb{Z}/2)^n \to X$$

be a function which is periodic with respect to an unknown vector v, and otherwise injective. *I.e.*, $f(x) = f(y)$ if and only if $x = y + v$. We suppose that there is a polynomial-time classical algorithm to compute f, which thus means a polynomial-sized quantum circuit to compute the unitary embedding

$$U_f|x\rangle = |x, f(x)\rangle$$

as in problem 4.2.

(a) Assume n qubits that are each initialized to the state $|+\rangle$. Show that all n qubits are then in the state $|(\mathbb{Z}/2)^n\rangle$. Apply U_f to this state and discard the output, to obtain a state ρ. Using problem 4.2, show that this state is

$$\rho = 2^{-n} \sum_{x \in (\mathbb{Z}/2)^n} |\{x, x+v\}\rangle\langle\{x, x+v\}|.$$

Argue that if you are given the state ρ on n qubits, it is equivalent to being given the state $|\{x, x+v\}\rangle$ for a randomly chosen value of $x \in (\mathbb{Z}/2)^n$.

(b) Given a state $|\{x, x+v\}\rangle$ as in part (a), measure each qubit in the basis $|+\rangle$ and $|-\rangle$, and then replace each measured "+" by 0 and each "−" by 1 to obtain a vector $y \in (\mathbb{Z}/2)^n$. Show that

$$v \cdot y = \sum_k v_k y_k = 0 \in \mathbb{Z}/2,$$

and that y is randomly chosen with this property.

***(c)** The set of y such that $v \cdot y$ is a certain vector space $Y \subseteq (\mathbb{Z}/2)^n$ of dimension $n-1$. Prove that $n-1$ randomly chosen vectors in Y span Y with probability greater than

$$\prod_{k=1}^{\infty} (1 - 2^{-k}) > \frac{1}{4},$$

and that when this happens it is easy to recover v with linear algebra over $\mathbb{Z}/2$. (Note: Although you don't have to prove this, if you use moderately more than $n-1$ vectors, the probability that they span Y converges to 1 at an exponential rate.)

(d) Conclude that the hidden vector v can be computed in quantum polynomial time.