Assignment 3

DUE: Tuesday, beginning of lecture 3/14/2023 (FIRM!!!), work individually.

1. Some generalizations of our study of the Bloch sphere:

   (a) As we saw, modulo overall phase[1], we can write any qubit as $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle$, where $0 \leq \theta \leq \pi$ and $0 \leq \varphi \leq 2\pi$. Determine, again modulo overall phase, the unique qubit $|\psi^\perp\rangle$ that is orthogonal to $|\psi\rangle$ (i.e., such that $\langle\psi^\perp|\psi^\perp\rangle = 1$ and $\langle\psi^\perp|\psi\rangle = 0$), written in terms of θ and φ.

   (b) Using your answer of part (a), show that $|\psi\rangle$ and $|\psi^\perp\rangle$ are antipodal[2] points on the Bloch sphere.

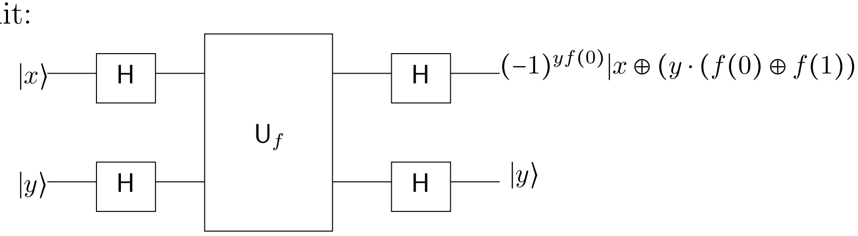
   (c) Prove, conversely, that any two antipodal points on the Bloch sphere correspond to orthogonal qubits.

   (d) Recall from linear algebra that two orthonormal vectors span a 2D vector space (of which the space of qubits is one example, in which we have been using $|0\rangle$ and $|1\rangle$ as a basis). Thus we ought to be able to write any qubit as $\gamma|\psi\rangle + \delta|\psi^\perp\rangle$ where $|\gamma|^2 + |\delta|^2 = 1$. Indeed, one may speak of "measuring in the $|\psi\rangle, |\psi^\perp\rangle$ basis[3]," which essentially means a $|\gamma|^2$ probability of winding up in the state $|\psi\rangle$ and a $|\delta|^2$ probability of winding up in the state $|\psi^\perp\rangle$. Recall the geometric picture we had for these probabilities for qubits in the computational basis (where $|\psi\rangle = |0\rangle$ and $|\psi^\perp\rangle = |1\rangle$). Show that the same geometric prescription works for probabilities when measuring in the $|\psi\rangle, |\psi^\perp\rangle$ basis.

2. One can generalize the Deutsch Algorithm to accept arbitrary two-bit inputs (rather than just 0 in the first bit and 1 in the second). The generalized relation is,

$$(\mathsf{H} \otimes \mathsf{H})\mathsf{U}_f(\mathsf{H} \otimes \mathsf{H})|x, y\rangle = (-1)^{yf(0)}|x \oplus (y \cdot (f(0) \oplus f(1))), y\rangle. \tag{1}$$

   Or, written as a circuit:



   Of course, if you plug in $x = 0$ and $y = 1$, you obtain the relation proved in class, namely, $(\mathsf{H} \otimes \mathsf{H})\mathsf{U}_f(\mathsf{H} \otimes \mathsf{H})|0, 1\rangle = (-1)^{f(0)}|f(0) \oplus f(1), 1\rangle$.

   By carefully tracing through the proof of the latter as given in class, but now including the Boolean variables x, y, prove Eq. (1) as given above.

---

[1] Which is to say, *ignoring* the overall phase, treating any such factor as though it were 1.

[2] I.e., on opposite sides of the sphere, similar to the north and south pole. E.g., Augusta, Australia is the closest city to the antipodal point of Boston.

[3] A technique often used in quantum computing, although we likely will not encounter it this semester.

3. In the Deutsch-Jozsa algorithm, we are promised that the function $f : \{0,1\}^n \to \{0,1\}$ is either balanced or constant. Explain what happens to the algorithm if f is neither balanced nor constant.

4. In Deutsch/Josza and elsewhere we're dealing a lot with $\mathsf{H}^{\otimes n}$ and have, perhaps, lost track of the fact that it can be represented as a $2^n \times 2^n$ matrix of ± 1's (and it is these that are generally known as Hadamard matrices, not just the 2×2 version). Let us index each row and column by n bits, i.e., a row is determined by r where r is a string of n bits, and similarly for column c. Prove, by induction on n, that the (r, c) element of $\mathsf{H}^{\otimes n}$ is $\frac{1}{2^{n/2}}(-1)^{r \cdot c}$, where the "$\cdot$" denotes inner product (that is, $\sum_{i=0}^{n-1} r_i c_i$). Use this to prove that any two rows and any two columns of $\mathsf{H}^{\otimes n}$ are orthonormal.

5. Here are a couple of exercises to better acquaint yourself with the arguments regarding how the tail end of Simon's algorithm works.

   (a) Use Gaussian elimination (over $\mathbb{Z}_2$) to find the unique solution of the set of equations $a \cdot y^{(i)} \equiv 0 \pmod 2$, such that $a \neq 0$, given by the following set of bit vectors $y^{(i)}$:

$$
\begin{aligned}
y^{(1)} &= 1\,0\,1\,0\,1\,1\,0 \\
y^{(2)} &= 0\,0\,1\,0\,0\,0\,1 \\
y^{(3)} &= 1\,1\,0\,0\,1\,0\,1 \\
y^{(4)} &= 0\,0\,1\,1\,0\,1\,1 \\
y^{(5)} &= 0\,1\,0\,1\,0\,0\,1 \\
y^{(6)} &= 0\,1\,1\,0\,1\,1\,1
\end{aligned}
$$

   (HINT: Regard this as a matrix equation $Ya = 0$, where the rows of Y are the $y^{(i)}$. You can reduce the matrix to row echelon form by adding rows, remembering that over $\mathbb{Z}_2$, we have $1 + 1 = 0$.)

   (b) Note in part (a) there were 6 equations in 7 unknowns, yielding a unique solution for a. Generally, in Simon's algorithm, we are content with $n - 1$ linearly independent bit vectors y obeying $y \cdot a \equiv 0 \pmod 2$ to determine all n bits of a. But we may tend to think that n equations are required to uniquely determine n values. Why, in this circumstance, do $n - 1$ equations suffice? Explain as precisely as you can. (You are welcome and encouraged to use any notions from linear algebra. If your answer relies on a particular theorem, state (no need to prove!) what theorem you are using.)