33-658 Quantum Computing and Quantum Information Homework 8

1. (i) prove $\mathbf{C}_{ij} = \tilde{\mathbf{n}}_i + \mathbf{n}_i\mathbf{X}_j$. (ii) Apply algebraic manipulations (i.e. do not use matrix arithmetic) to prove: $\mathbf{S}_{ij} = (1/2)(\mathbf{1} + \mathbf{X}_i\mathbf{X}_j + \mathbf{Y}_i\mathbf{Y}_j + \mathbf{Z}_i\mathbf{Z}_j) = (1/2)(1 + \vec{\sigma}_i \cdot \vec{\sigma}_j)$.

Answer:

(i) If $\mathbf{n}_i = 0$ then $\mathbf{C}_{ij} = \tilde{\mathbf{n}}_i = \mathbf{1}$, as required, while if $\mathbf{n}_i = 1$, then $\mathbf{C}_{ij}$ acts as a `NOT` on j, as required.

(ii) Expressing $\mathbf{C}_{ij}$ as in (i), noting the identities $\mathbf{n}\mathbf{X} = \mathbf{X}\tilde{\boldsymbol{n}}$ and $\tilde{\boldsymbol{n}}\mathbf{X} = \mathbf{X}\mathbf{n}$, and invoking an identity for $\mathbf{S}_{ij}$ proved in class, we can show

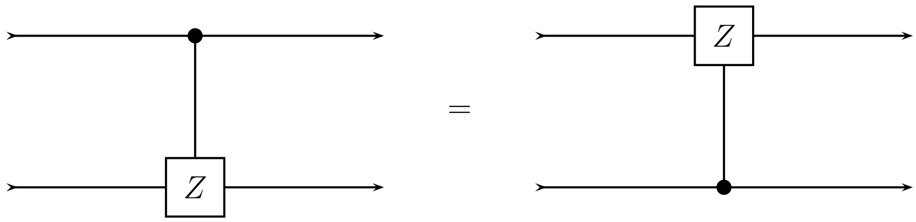
$$\mathbf{S}_{ij} = \mathbf{C}_{01}\mathbf{C}_{10}\mathbf{C}_{01} = \mathbf{n}_i\mathbf{n}_j + \tilde{\boldsymbol{n}}_i\tilde{\boldsymbol{n}}_j + (\mathbf{X}_i\mathbf{X}_j)(\mathbf{n}_i\tilde{\boldsymbol{n}}_j + \tilde{\boldsymbol{n}}_i\mathbf{n}_j).$$

Then, substituting $\mathbf{n} = (1 - \mathbf{Z})/2$ and $\mathbf{n} = (1 + \mathbf{Z})/2$ (also shown in class) and defining $\mathbf{Y} = i\mathbf{X}\mathbf{Z}$) yields

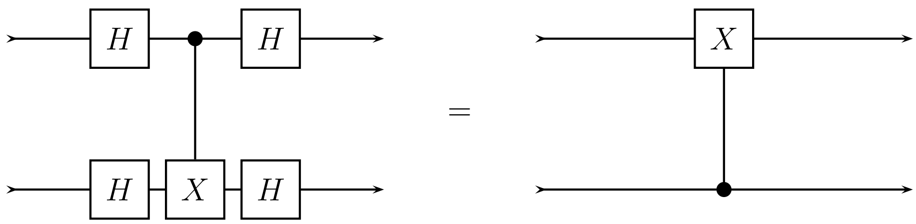
$$\mathbf{S}_{ij} = (1/2)(\mathbf{1} + \mathbf{X}_i\mathbf{X}_j + \mathbf{Y}_i\mathbf{Y}_j + \mathbf{Z}_i\mathbf{Z}_j) = (1/2)(1 + \vec{\sigma}_i \cdot \vec{\sigma}_j)$$

where the final equality expresses the definition of the dot product of the vector of Pauli operators.

2. Prove the identities



and



Answer: The top identity follows because each operation leaves the basis states $|00\rangle$, $|01\rangle$, and $|10\rangle$ invariant while reversing the sign of $|11\rangle$. The bottom identity then follows because we may apply the top identity to move $\mathbf{HXH} = \mathbf{Z}$ from the second qubit to the first, and then identify $\mathbf{HZH} = \mathbf{H}^2\mathbf{XH}^2 = \mathbf{X}$ on the first qubit.

3. In the Bernstein-Vazirani problem we are told that function $f(x) = a \cdot x$, where a and x are n-bit integers and the dot product

$$a \cdot x = a_0 x_0 \oplus a_1 x_1 \oplus \cdots \oplus a_{n-1} x_{n-1}$$

is the modulo 2 sum of products of bits. Suppose that we are given a quantum circuit that evaluates $f(x)$ for any input x but that we do not know the value of a. To determine a on a classical computer would require n evaluations of f. This exercise, which is based on the analysis in Mermin, shows how to determine a with a *single* evaluation of f on a quantum computer.

(i) Let $\mathbf{U}_f$ be an f-controlled unitary transformation on the tensor product of the n-bit input register initially in state $|x\rangle_n$ and a 1-bit output register initially in state $|y\rangle_1 = \mathbf{HX}|0\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Show that

$$\mathbf{U}_f |x\rangle_n |y\rangle_1 = (-1)^{f(x)} |x\rangle_n |y\rangle_1.$$

Answer: If $f(x) = 0$ then U_f acts as the identity. If $f(x) = 1$ then U_f flips the states of the second bit. Since $|y\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, flipping the bits reverses the sign of $|y\rangle$.

(ii) Show that

$$\mathbf{H}^{\otimes n} |x\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n - 1} (-1)^{x \cdot y} |y\rangle_n.$$

Answer: First note that

$$\mathbf{H}|x\rangle_1 = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^x |1\rangle\right) = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{xy} |y\rangle$$

Now multiplying the sums for an n-bit ket, we obtain the required result where the dot product

$$x \cdot y = \sum_j x_j y_j.$$

(iii) Show that

$$(\mathbf{H}^{\otimes n} \otimes \mathbf{H})\mathbf{U}_f(\mathbf{H}^{\otimes n} \otimes \mathbf{H})|0\rangle_n|1\rangle_1 = |a\rangle_n|1\rangle_1.$$

Note that the unknown value of a appears in the *input* register!

Answer: Applying the given sequence of operations and inserting the results of parts (i) and (ii), we obtain

$$(\mathbf{H}^{\otimes n} \otimes \mathbf{H})\mathbf{U}_f(\mathbf{H}^{\otimes n} \otimes \mathbf{H})|0\rangle_n|1\rangle_1 = \frac{1}{2^n}\sum_{xy}(-1)^{f(x)+x\cdot y}|y\rangle_n\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Now set $f(\vec{x}) = \vec{a}\cdot\vec{x}$ and consider the sum over $\vec{x}$,

$$\sum_x(-1)^{(a\cdot x)}(-1)^{(y\cdot x)} = \prod_{j=1}^{n}\sum_{x_j=0}^{1}(-a)^{(a_j+y_j)x_j}$$

The sum over x_j vanishes unless $a_j + y_j = 0\text{mod}2$ ($i.\ e.a_j = y_j$) so the product vanishes unless $\vec{y} = \vec{a}$, and the sum over y above contains only $y = a$.