QUANTUM ALGORITHMS
HOMEWORK 10 SELECTED SOLUTIONS

PROF. MATTHEW MOORE

2. Using the previous question, prove the assertion on page 119 that

$$\sum_{\substack{a,b \\ x-y\in D}} (-1)^{a\cdot x - b\cdot y} \neq 0$$

if and only if $a = b \in D^{\perp}$ (the book uses E^{*}).

Solution:

Proof. Define

$$F = \{(x,y) \in (\mathbb{Z}_2^n)^2 \mid x - y \in D\}.$$

Observe that F is a subgroup of $(\mathbb{Z}_2^n)^2$: if $(x_1, y_1), (x_2, y_2) \in F$ then $(x_1 + x_2, y_1 + y_2) \in F$ since

$$(x_1 + x_1) - (y_1 + y_2) = (x_1 - y_1) + (x_2 - y_2) = 0 + 0 = 0.$$

It follows that

$$\sum_{\substack{a,b \\ x-y\in D}} (-1)^{a\cdot x - b\cdot y} = \sum_{a,b} \sum_{(x,y)\in F} (-1)^{a\cdot x - b\cdot y} = \sum_{(a,b)\in(\mathbb{Z}_2^n)^2} \sum_{(x,y)\in F} (-1)^{(a,b)\cdot(x,y)}.$$

Using the result of Additional Problem 1 with $(\mathbb{Z}_2^n)^2$ in place of $\mathbb{Z}_2^n$ and $\mathbb{F}$ in place of $\mathbb{A}$, we obtain the claimed result. □

3. We say that a subgroup $\mathbb{A} \leq \mathbb{Z}_2^n$ is *maximal* if

- $A \neq \mathbb{Z}_2^n$ and
- if $\mathbb{A} \leq \mathbb{X} \leq \mathbb{Z}_2^n$ then $\mathbb{A} = \mathbb{X}$ or $\mathbb{X} = \mathbb{Z}_2^n$.

Similarly, $\mathbb{A} \leq \mathbb{Z}_2^n$ is *minimal* if

- $\{0\} \neq A$ and
- if $\{0\} \leq \mathbb{X} \leq \mathbb{A}$ then $\{0\} = \mathbb{X}$ or $\mathbb{X} = \mathbb{A}$.

Prove that $\mathbb{A}$ is maximal if and only if $\mathbb{A}^{\perp}$ is minimal (use this in your solution to 13.1).

Solution:

Proof. We begin with a claim.

Claim. *The operator $(\cdot)^{\perp}$ is order reversing. That is, $\mathbb{A} \leq \mathbb{B}$ if and only if $\mathbb{B}^{\perp} \leq \mathbb{A}^{\perp}$.*

Proof of claim. Implicit to this claim is that $\mathbb{A}^{\perp}$ is a subgroup. This is easy to verify: if $\alpha_1, \alpha_2 \in \mathbb{A}^{\perp}$ then $\alpha_1 \cdot a = 0 = \alpha_2 \cdot a$ for all $a \in A$. Therefore

$$0 = \alpha_1 \cdot a + \alpha_2 \cdot a = (\alpha_1 + \alpha_2) \cdot a$$

for all $a \in A$, so $\alpha_1 + \alpha_2 \in \mathbb{A}^{\perp}$.

Date: April 21, 2021.

Suppose that $\mathbb{A} \leq \mathbb{B}$ and let $\beta \in \mathbb{B}^\perp$. It follows that $\beta \cdot b = 0$ for all $b \in B$. Since $A \subseteq B$, we therefore have that $\beta \cdot a = 0$ for all $a \in A$. Hence $\beta \in \mathbb{A}^\perp$ and so $\mathbb{B}^\perp \leq \mathbb{A}^\perp$. In turn, this implies that $\mathbb{A} \leq \mathbb{B}$ since $(\mathbb{A}^\perp)^\perp = \mathbb{A}$. ∘

We continue now with the main proof. Suppose that $\mathbb{A}$ is maximal and consider $\mathbb{A}^\perp$. If $\mathbb{A}^\perp = \{0\}$ then $\mathbb{A} = \{0\}^\perp = \mathbb{Z}_2^n$, contradicting $\mathbb{A}$ being maximal. If $\{0\} \leq \mathbb{X} \leq \mathbb{A}^\perp$ then

$$\mathbb{Z}_2^n \geq \mathbb{X}^\perp \geq \mathbb{A}^\perp.$$

Since $\mathbb{A}$ is maximal, this implies that $\mathbb{X}^\perp = \mathbb{Z}_2^n$ or $\mathbb{X}^\perp = \mathbb{A}^\perp$. This is equivalent to $\mathbb{X} = \{0\}$ or $\mathbb{X} = \mathbb{A}^\perp$. Hence $\mathbb{A}^\perp$ is minimal. The proof that if $\mathbb{A}$ is minimal then $\mathbb{A}^\perp$ is maximal is quite similar. □

4. In Simon's algorithm, what would happen if instead of measuring the first block of qubits, we measured the second block of qubits? Calculate the density matrix and describe what distribution it represents.

Solution: Simon's algorithm *without any measurement* is given by

$$(H^{\otimes n} \otimes I_m) \circ \hat{f} \circ (H^{\otimes n} \otimes I_m) \left|0^{n+m}\right\rangle$$

where $\hat{f}$ is the unitary operator defined on basis vector $|x, y\rangle$ by $\hat{f}\,|x, y\rangle = |x, y + f(x)\rangle$. Evaluating it in stages, we have

$$\begin{aligned}
|\psi_1\rangle &= (H^{\otimes n} \otimes I_m) \left|0^{n+m}\right\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x, 0^m\rangle\,, \\
|\psi_2\rangle &= \hat{f}\,|\psi_1\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x, f(x)\rangle\,, \\
|\psi_3\rangle &= (H^{\otimes n} \otimes I_m) |\psi_2\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} H^{\otimes n} |x\rangle \otimes |f(x)\rangle\,.
\end{aligned}$$

The density matrix for the last state $|\psi_3\rangle$ is

$$\begin{aligned}
\rho = |\psi_3\rangle\langle\psi_3| &= \frac{1}{2^n} \Big(\sum_{x \in \{0,1\}^n} H^{\otimes n} |x\rangle \otimes |f(x)\rangle \Big) \Big(\sum_{y \in \{0,1\}^n} \langle y| H^{\otimes n} \otimes \langle f(y)| \Big) \\
&= \frac{1}{2^n} \sum_{x,y \in \{0,1\}^n} H^{\otimes n} |x\rangle\langle y| H^{\otimes n} \otimes |f(x)\rangle\langle f(y)|
\end{aligned}$$

(recall that $H^\dagger = H$). Applying the partial trace on the first register yields

$$\mathrm{Tr}_1(\rho) = \frac{1}{2^n} \sum_{x,y \in \{0,1\}^n} \mathrm{Tr}\left(H^{\otimes n} |x\rangle\langle y| H^{\otimes n}\right) |f(x)\rangle\langle f(y)|\,.$$

We have

$$\mathrm{Tr}\left(H^{\otimes n} |x\rangle\langle y| H^{\otimes n}\right) = \mathrm{Tr}\left(H^{\otimes n} H^{\otimes n} |x\rangle\langle y|\right) = \mathrm{Tr}\left(|x\rangle\langle y|\right) = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{otherwise,} \end{cases}$$

so

$$\mathrm{Tr}_1(\rho) = \frac{1}{2^n} \sum_{x\{0,1\}^n} |f(x)\rangle\langle f(x)| = \frac{1}{2^n} \sum_{z\{0,1\}^m} F_z |z\rangle\langle z|\,,$$

where $F_z = \left|\{x \in \{0,1\}^n \mid f(x) = z\}\right|$. Since $f(x) = f(y)$ if and only if $x + D = y + D$, each F_z is just the size of the coset $x + D$ for $f(x) = z$. All cosets are of size $|D|$, so

$$\frac{1}{2^n} \sum_{z\{0,1\}^m} F_z |z\rangle\langle z| = \frac{|D|}{2^n} \sum_{z\{0,1\}^m} |z\rangle\langle z| = \frac{1}{2^m} \sum_{z\{0,1\}^m} |z\rangle\langle z|$$

(we use the fact that $[G : D] = |G|/|D| = |f(G)| = 2^m$). This corresponds to the uniform distribution over the *output* space of f.