QUANTUM ALGORITHMS
HOMEWORK 10 ADDITIONAL PROBLEMS

PROF. MATTHEW MOORE

Due: 2021-04-20

For a subgroup $\mathbb{A} \leq \mathbb{Z}_2^n$ define

$$\mathbb{A}^{\perp} = \{g \in \mathbb{Z}_2^n \mid g \cdot a = 0 \text{ for all } a \in A\},$$

where $a \cdot g$ is the dot product modulo 2 of g and g (regarded as $\mathbb{Z}_2$-vectors).

1. Let $\mathbb{A} \leq \mathbb{Z}_2^n$ and $g \in \mathbb{Z}_2^n$. Define

$$A_0 = \{a \in A \mid a \cdot g = 0\} \qquad \text{and} \qquad A_1 = \{a \in A \mid a \cdot g = 1\}.$$

(i) Prove that $A = A_0 \cup A_1$ and $\emptyset = A_0 \cap A_1$.

(ii) Suppose that $a \in A_1$. Prove that $a + A_0 = A_1$ and $a + A_1 = A_0$. Explain why this implies $|A_0| = |A_1|$ if $A_1 \neq \emptyset$.

(iii) Prove that

$$\sum_{a \in A} (-1)^{a \cdot g} = \begin{cases} |A| & \text{if } a \cdot g = 0 \text{ for all } a \in A, \\ 0 & \text{otherwise.} \end{cases}$$

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^*).

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).

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.