Quantum Algorithms
Homework 11

Patrick Canny

Due: 2019-04-23

Carefully read through the description of Simon's algorithm on pages 118 and 119.

Let $\mathbb{G} = (\mathbb{Z}_2)^k$. Regarding elements of $\mathbb{G}$ as k-dimensional vectors, we define

$$g \cdot h = \sum_{i=1}^{k} g_i h_i \bmod 2$$

to be the dot product modulo 2. Furthermore, for a subgroup $\mathbb{H} \leq \mathbb{G}$ define

$$\mathbb{H}^{\partial} = \big\{ g \in G \mid g \cdot h = 0 \text{ for all } h \in H \big\}.$$

1. Explain each step in this calculation:

$$\sum_{\substack{x,y \in G \\ x-y \in D}} (-1)^{a \cdot x - b \cdot y} = \sum_{d \in D} \sum_{x \in G} (-1)^{a \cdot d} (-1)^{(a-b) \cdot (x -_2 d)} = \sum_{d \in D} \sum_{z \in G} (-1)^{a \cdot d} (-1)^{(a-b) \cdot z}$$
$$= \left(\sum_{d \in D} (-1)^{a \cdot d} \right) \left(\sum_{z \in G} (-1)^{(a-b) \cdot z} \right)$$

[NB: the addition/subtraction in the exponent is the usual kind (not modulo 2) except for the "$-_2$".]

Solution: I will break each step into a sub-calculation as follows:

(i)

$$\begin{aligned}
\sum_{\substack{x,y \in G \\ x-y \in D}} (-1)^{a \cdot x - b \cdot y} &= \sum_{\substack{x,y \in G \\ x-y \in D}} (-1)^{a \cdot x - b \cdot y + 0} \\
&= \sum_{\substack{x,y \in G \\ x-y \in D}} (-1)^{a \cdot x - b \cdot y + (a \cdot y - a \cdot y)} \\
&= \sum_{\substack{x,y \in G \\ x-y \in D}} (-1)^{a \cdot x - a \cdot y + (a \cdot y - b \cdot y)} \\
&= \sum_{\substack{x,y \in G \\ x-y \in D}} (-1)^{a \cdot (x-y) + (a \cdot y - b \cdot y)} \\
&= \sum_{\substack{x,y \in G \\ x-y \in D}} (-1)^{a \cdot (x-y) + (a-b) \cdot y}
\end{aligned}$$

Then, since $x - y = d, y = x - d$. So:

$$\sum_{\substack{x,y\in G\\ x-y\in D}} (-1)^{a\cdot(x-y)+(a-b)\cdot y} = \sum_{\substack{x,y\in G\\ d\in D}} (-1)^{a\cdot(x-y)+(a-b)\cdot(x-d)}$$
$$= \sum_{d\in D}\sum_{x\in G} (-1)^{a\cdot d+(a-b)\cdot(x-d)}$$

Doing the subtraction $\mod 2$ ensures that the resulting vector will be in $\mathbb{G}$. This is because $\mathbb{G}$ is only defined over $\{0,1\}^k$, and doing the subtraction normally could result in negative components.

(ii) z must be in $\mathbb{G}$, so it is possible to re-write the sum in terms of $\mathbb{G}$.

(iii) By properties of summations, the double summation of a product can be re-written as a product of two single summations.

2. (i) Prove that $\sum_{d\in D}(-1)^{a\cdot d} \neq 0$ if and only if $a \cdot d = 0$ for all $d \in D$.

Solution:

Proof. Towards a contradiction, assume that $\sum_{d\in D}(-1)^{a\cdot d} \neq 0$ if and only if $a\cdot d \neq 0$ for all $d \in D$.

Then, it holds that $a \cdot d = 1$ for some d.

From here, one of two things will happen:

- $a \cdot d = 1$ for all $d \in D$.
  This cannot be true, since the identity operator in D is $|0\rangle$, and $a \cdot |0\rangle = 0$ for all a, so this is a contradiction.
- $a \cdot d = 1$ for some $d \in D$.
  Take a partition of D s.t the partitions are of equal size. This can be done, since the subgroup D could be selected in a way where the following property holds for its partitions:

$$D_0 = \{d \in D \quad | \quad a \cdot d = 0 \text{ for all } d \in D\}$$
$$D_1 = \{d \in D \quad | \quad a \cdot d = 1 \text{ for all } d \in D\}$$

  Then, we can represent the original sum as the following:

$$\sum_{d\in D}(-1)^{a\cdot d} = \sum_{g\in D_0}(-1)^{a\cdot g} + \sum_{e\in D_1}(-1)^{a\cdot e}$$
$$= \sum_{g\in D_0}(-1)^0 + \sum_{e\in D_1}(-1)^1$$
$$= |D_0| - |D_1| = 0$$

  Because D_0, D_1 have equal size. This is a contradiction, so the claim holds.

□

(ii) Prove that $\sum_{z \in G} (-1)^{(a-b)\cdot z} \neq 0$ if and only if $a = b$.

Solution:

Proof. Towards a contradiction:

$$\begin{aligned}\sum_{z \in G} (-1)^{(a-b)\cdot z} &= \sum_{z \in G} (-1)^{a\cdot z - b\cdot z} \\ &= \sum_{z \in G} (-1)^{a\cdot z} (-1)^{-b\cdot z}\end{aligned}$$

Now we can select $|a\rangle, |b\rangle$ to aid in producing a contradiction. Pick $a = |0\rangle, b = |1\rangle$. Note that $-b$ and b produce the same result when -1 is raised to their power. Then:

$$\sum_{z \in G} (-1)^{a\cdot z} (-1)^{-b\cdot z}$$

$$\sum_{z \in G} (-1)^{1\cdot z}$$

Now if we take G to be $0, 1^3$, the eight vectors in G can be used to show a contradiction:

$$(-1)^{1\cdot|000\rangle} + (-1)^{1\cdot|001\rangle} + \ldots + (-1)^{1\cdot|111\rangle} = 0$$

This is because there are an equal number of times where the term being added is 1 and -1. Since $a \neq b$ and $\sum_{z \in G} (-1)^{(a-b)\cdot z} = 0$ this is a contradiction. □

3. Prove the assertion on page 119 that $\sum_{\substack{x,y \in G \\ x-y \in D}} (-1)^{a\cdot x - b\cdot y} \neq 0$ if and only if $a = b \in D^\partial$ (the book uses E^*).

Solution:

Proof. This equation is comprised of the calculations shown in problem 2. By the previous problem, we can make a few observations:

- $a \in D^\partial$ by 2.(i) since $a \cdot d = 0$ for all $d \in D$.
- Similarly, $b \in D^\partial$ since by 2.(ii) $a = b$
- If either of the two summations in problem 2 equals 0, the whole equation will evaluate to 0. Therefore, it is essential that both summations do no equal 0, as shown in the previous problem.
- The only way that this is possible is if $a = b \in D^\partial$ as shown by item (i) and the previous problem.

□

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

Solution: By the form described in the text and lecture, ρ can be represented as follows:

$$\begin{aligned}
\rho &= \mathrm{Tr}_1(U(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|)U^\dagger) \\
&= \mathrm{Tr}_1(U(2^{-k/2}\sum_{x\in G}|x\rangle\, 2^{-k/2}\sum_{x\in G}\langle x| \otimes |0\rangle\langle 0|)U^\dagger) \\
&= 2^{-k}\,\mathrm{Tr}_1(U\big(\sum_{x\in G}|x\rangle \otimes |0\rangle \sum_{x\in G}\langle x| \otimes \langle 0|\,\big)U^\dagger) \\
&= 2^{-k}\,\mathrm{Tr}_1((\big(\sum_{x\in G}|x\rangle \otimes |f(x)\rangle \sum_{x\in G}\langle x| \otimes \langle f(x)|\,\big)) \\
&= 2^{-k}\,\mathrm{Tr}_1\big(\sum_{x,y\in G}|x\rangle\langle y| \otimes |f(x)\rangle\langle f(y)|\,\big) \\
&= 2^{-k}\big(\sum_{x,y\in G}|f(x)\rangle\langle f(y)|\,\mathrm{Tr}_1(|x\rangle\langle y|)\big) \\
&= 2^{-k}\big(\sum_{x=y\in G}|f(x)\rangle\langle f(y)|
\end{aligned}$$

This comes from that $|x\rangle\langle y|$ will produce a matrix with a singular 1 on the diagonal when x=y. Then:

$$\begin{aligned}
\rho = 2^{-k}\sum_{x=y\in G}|f(x)\rangle\langle f(y)| &= 2^{-k}\sum_{x\in G}|f(x)\rangle\langle f(x)| \\
&= 2^{-k}\sum_{x\in G}(-1)^{a\cdot f(x)-b\cdot f(y)} \\
&= 2^{-k}\sum_{x\in G}(-1)^{(a-b)\cdot f(x)}
\end{aligned}$$

The final ρ is then some matrix with mostly ones, but some places where larger values are found. This distribution seems to represent the distribution of the predicted values for $f(x)$.

5. We say that a subgroup $\mathbb{H} \leq \mathbb{G}$ is *maximal* if

   - $H \neq G$ and
   - if $\mathbb{H} \leq \mathbb{X} \leq \mathbb{G}$ then $\mathbb{H} = \mathbb{X}$ or $\mathbb{X} = \mathbb{G}$.

   Similarly, $\mathbb{H} \leq \mathbb{G}$ is *minimal* if

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

   Prove that $\mathbb{H}$ is maximal if and only if $\mathbb{H}^\partial$ is minimal.

Solution:

Proof. Take $\mathbb{H}^\partial$ to be minimal. The most simple minimal subgroup is composed of $\{0\}$ and one other singleton. Call this additional element a. Then, $\mathbb{H}^\partial$ is $\{0, a\}$. Then, the corresponding group $\mathbb{H}$ can be created by finding $(\mathbb{H}^\partial)^\partial = \mathbb{H}$.

This means that H is defined by all the elements $g \in G$ where $g \cdot h = 0 \quad \forall h \in H^{\partial}$. For $\{0\}$ this is simply all elements, so the size of the group gets limited by a. If we take a to be a simple element of G, say that it's the vector $|10\ldots0\rangle$. From here, we can see that all of the elements that make $a \cdot h = 0$ can be expressed as vectors starting with 0 and followed by $k-1$ many elements which may be either 1 or 0, it doesn't matter. If we take $\mathbb{H}$ to be all of these elements, the final group will be maximal with size $|G|/2$.

Now take $\mathbb{H}$ to be maximal. This means that H^{∂} is made of $g \in G$ where $g \cdot h = 0 \quad \forall h \in H$. Clearly, this $\mathbb{H}^{\partial}$ must contain 0, as $0 \cdot h = 0$ for all $h \in H$. Now, what are the other elements in this subgroup? If we have a maximal subgroup, we know that it does not have every element of the group. This maximal subgroup must also be closed under addition. This implies that there is a maximal size of a maximal subgroup, because with the addition of any single element, the rest of the group must be included in order to retain the group properties.

When we consider the minimal subgroup as above, we can imagine the addition of elements to this group to form a maximal subgroup. Whenever we add a new element to the group, the sum of that new element and every other element in the group must be added. This implies that each time a new element is added to the group, the total number of elements in the group increases by $|H| - 1$ (since $0 + a = a$). This means that the size of any maximal subgroup is $|G|/2$

From here if it is possible to assume that if the elements of this maximal subgroup were selected in a particular way, it holds that there exists some singleton d such that $a \cdot d = 0$ for all a in $\mathbb{H}$. Since this new group has only one element, it is minimal. □