Lecture 14

Simon's problem. Let $n, k \in \mathbb{N}$ be such that $n = 2^k$. So that $\{0,1,\dots,n-1\}^n$ bijects with $\{0,1,\dots,n-1\}^{\{0,1\}^k}$ and be identified under a fixed bijection. In the following, we will switch between these two notations.

$$\text{Simon}_n \colon D := D_0 \dot{\cup} D_1 \subseteq \{0,1,\dots,n-1\}^n \to \{0,1\}, \tag{87}$$

where

$$D_0 := \{x \in \{0,1,\dots,n-1\}^{\{0,1\}^k} \mid \forall s,t \in \{0,1\}^k, s \neq t \implies x(s) \neq x(t)\}, \tag{88}$$

$$D_1 := \{x \in \{0,1,\dots,n-1\}^{\{0,1\}^k} \mid \exists a \in \{0,1\}^k - \{0^k\}, \forall s,t \in \{0,1\}^k, x(s) = x(t) \iff s \in \{t, t \oplus a\}\}, \tag{89}$$

and $\text{Simon}_n(x) = 0 \iff x \in D_0$.

Proposition 7. $Q(\text{Simon}_n) = O(\log(n))$.

We need some lemmas.

Lemma 3. *Let $x \in \{0,1\}^k$ and $|x\rangle = |x_1\rangle \dots |x_k\rangle$ be a k-qubit state. Then*

$$H^{\otimes k} |x\rangle = \frac{1}{\sqrt{2^k}} \sum_{y \in \{0,1\}^k} (-1)^{x \cdot y} |y\rangle, \tag{90}$$

where $H^{\otimes k} := H \otimes \dots \otimes H$ (k times) and $x \cdot y := \sum_{i=1}^k x_i y_i$.

Lemma 4. *Let $K \in \mathbb{N}$. Suppose $z_1, \dots, z_K \leftarrow \mathbb{F}_2^k$. Then the probability that the dimension of the span of the z_is, i.e., the dimension of the subspace*

$$V := \{a_1 z_1 + \dots + a_K z_K \mid a_1, \dots, a_K \in \mathbb{F}_2\} \leq \mathbb{F}_2^k \tag{91}$$

is k is at least $1 - 2^{k-K}$.

Lemma 5. *Let $K \in \mathbb{N}$ and $0 \neq a \in \mathbb{F}_2^k$. Let $z_1, \dots, z_K \in \mathbb{F}_2^k$ (arbitrary) be such that $\forall i \in [K]$, $a \cdot z_i = 0 \mod 2$. Then the dimension of the span of the z_is is at most $k-1$.*

With the lemmas in place, we can now prove Proposition 7.

Proof of Proposition 7. Create the state using 1 query to $x \in D$:

$$\frac{1}{\sqrt{2^k}} \sum_{s \in \{0,1\}^k} |s\rangle |x(s)\rangle. \tag{92}$$

Measure the second register in the computational basis. There are two cases depending on whether $x \in D_0$ or $x \in D_1$.

1. $x \in D_0$. Obtain a value $y_0 \in \{0,1,\dots,n-1\}$ (with probability $1/n$ but the precise value doesn't matter for the later analysis) and the state becomes

$$|s_0\rangle |y_0\rangle, \tag{93}$$

   where $x(s_0) = y_0$.

2. $x \in D_1$. Obtain a value $y_0 \in x(\{0,1\}^k)$ (with probability $2/n$ – note $|x(\{0,1\}^k)| = n/2$) and the state becomes

$$\frac{1}{\sqrt{2}}(|s_0\rangle + |s_0 \oplus a\rangle) |y_0\rangle, \tag{94}$$

   where $x(s_0) = y_0$.

Now apply $H^{\otimes k}$ to the first register. Then measure the first register in the computational basis. (Will ignore the second register for notational convenience since it just stays $|y_0\rangle$.) Analyze two cases $x \in D_0$ and $x \in D_1$ separately:

1. $x \in D_0$. After applying $H^{\otimes k}$:

$$\frac{1}{\sqrt{2^k}} \sum_{z \in \{0,1\}^k} (-1)^{s_0 \cdot z} |z\rangle. \tag{95}$$

   After measurement in the computational basis: obtain $z \in \{0,1\}^k$ uniformly at random.

2. $x \in D_1$. After applying $H^{\otimes k}$:

$$\frac{1}{\sqrt{2^k}} \sum_{z \in \{0,1\}^k} ((-1)^{s_0 \cdot z} + (-1)^{(s_0 \oplus a) \cdot z}) |z\rangle = \frac{1}{\sqrt{2^k}} \sum_{z \in \{0,1\}^k} (-1)^{s_0 \cdot z} (1 + (-1)^{a \cdot z}) |z\rangle \,. \tag{96}$$

After measurement in the computational basis: obtain $z \in \{0,1\}^k$ such that $a \cdot z = 0 \mod 2$ with probability $2/2^k$. (Note that there are 2^{k-1} zs satisfying $a \cdot z = 0$.)

Repeat the entirety of the above K times and output 0 if and only if

$$d := (\text{dimension of the span of the } K \; z\text{s obtained viewed as vectors in } \mathbb{F}_2^k) = k. \tag{97}$$

Analyze two cases $x \in D_0$ and $x \in D_1$ separately:

1. $x \in D_0$. By Lemma 4: with probability at least $1 - 2^{k-K}$, $d = k$. Therefore the probability of the output being correct, i.e., 0, is at least $1 - 2^{k-K}$.

2. $x \in D_1$. By Lemma 5: $d \leq k - 1$. Therefore, the output is always correct, i.e., equal to 1.

So if we take $K \geq k + 2$, then, for all $x \in D$, the probability of being correct is at least $2/3$.
Since each repeat costs only 1 query. The overall query complexity is $K = k + 2 = O(\log(n))$, as required. □