Lecture 15

Lemma 6. *Let $x \in \{0,1\}^k$ and $|x\rangle = |x_1\rangle \dots |x_k\rangle$ be a k-qubit state. Then*

$$H^{\otimes k} |x\rangle = \frac{1}{\sqrt{2^k}} \sum_{y \in \{0,1\}^k} (-1)^{x \cdot y} |y\rangle , \tag{98}$$

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

Proof. We have

$$\begin{aligned}
H^{\otimes k} |x\rangle =& H |x_1\rangle \otimes \dots \otimes H |x_n\rangle \\
=& \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1} |1\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1} |1\rangle) && \text{Eq. (39) (Phase kickback)} \\
=& \frac{1}{\sqrt{2^k}} \sum_{y_1,\dots,y_k \in \{0,1\}} (-1)^{x_1 y_1 + \dots + x_k y_k} |y_1\rangle |y_2\rangle \dots |y_k\rangle && \text{think about phase for fixed } y \\
=& \frac{1}{\sqrt{2^k}} \sum_{y \in \{0,1\}^k} (-1)^{x \cdot y} |y\rangle ,
\end{aligned}$$

as required. □

Lemma 7. *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*

$$V := \{a_1 z_1 + \dots + a_K z_K \mid a_1, \dots, a_K \in \mathbb{F}_2\} \leq \mathbb{F}_2^k \tag{99}$$

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

Based on [StackExchange post].

Proof. Let $A \in \mathbb{F}_2^{K \times k}$ denote the matrix whose rows are the z_is. The dimension of V is the same as the row-rank (dimension of the span of the rows) of A, which is equal to the column-rank of A by a standard fact in linear algebra. Now, the column-rank of A is k if and only if the kernel of A is $\{0\}$ by the rank-nullity theorem, where the kernel of A is defined by

$$\ker(A) := \{x \in \mathbb{F}_2^k \mid Ax = 0\}. \tag{100}$$

Since the z_is are chosen uniformly from $\mathbb{F}_2^k$, A is a uniformly random matrix in $\mathbb{F}_2^{K \times k}$. In the following, the probability is over $A \leftarrow \mathbb{F}_2^{K \times k}$.

$$\begin{aligned}
\Pr[\ker(A) \neq \{0\}] =& \Pr[\exists x \in \mathbb{F}_2^k, x \neq 0, Ax = 0] && \text{definition} \\
\leq& \sum_{x \in \mathbb{F}_2^k, x \neq 0} \Pr[Ax = 0] && \text{union bound} \\
=& (2^k - 1) \frac{1}{2^K} && Ax \text{ is unif. random in } \mathbb{F}_2^K \text{, e.g., suppose } x_k = 1 \\
\leq& \frac{2^k}{2^K}.
\end{aligned}$$

Therefore $\Pr[\dim(V) = k] = \Pr[\ker(A) = \{0\}] \geq 1 - 2^{k-K}$. □

Lemma 8. *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 $k - 1$.*

Proof. It suffices to prove that the dimension of the following subspace is $k - 1$:

$$U := \{z \in \mathbb{F}_2^k \mid a \cdot z = 0\}. \tag{101}$$

Note that U is the kernel of the $1 \times k$ matrix $A := (a_1, \dots, a_k)$. Now, the column-rank of A is 1 since $a \neq 0$. Therefore, by the rank-nullity theorem, $\dim(U) = k - 1$. □

Remark 8. In the case $x \in D_1$, a slight modification of the algorithm above can also recover a: choose K large enough (how large?) such that in the case $x \in D_1$, we have $d = k-1$ whp; collect the $k-1$ linearly independent vectors $z^{(1)}, \dots z^{(k-1)} \in \mathbb{F}_2^k$ into the rows of a matrix $A \in \mathbb{F}_2^{(k-1) \times k}$ and compute the kernel of A, which will have size 2. a is the non-zero element. Moreover, note that, since $n = 2^k$, we can identify $\{0, 1, \dots, n-1\}^n$ with $\{0, 1, \dots, n-1\}^{\mathbb{F}_2^k}$.

Therefore, we also have an $O(\log(n))$ quantum algorithm for the following query problem:

$$\mathrm{Simon}'_n \colon D' \subseteq \{0,1,\ldots,n-1\}^{\mathbb{F}_2^k} \to \mathbb{F}_2^k \tag{102}$$

where $x \in D'$ if and only if there exists an $a \in \mathbb{F}_2^k - \{0^k\}$ such that $\forall s,t \in \mathbb{F}_2^k$, $x(s) = x(t) \iff s \in \{t, t+a\}$ (addition as defined in the group $\mathbb{Z}_2^k$, i.e., component-wise addition), and $\mathrm{Simon}'_n(x)$ outputs the a (period) associated with x. (Writing it this way is to allow for direct comparison with the order finding problem at the heart of Shor's algorithm later.)

Proposition 8. $Q(\mathrm{Simon}_n) = \Theta(\sqrt{n})$

Proof. **Upper bound.** Randomized query algorithm for finding a collision. Note that the following description can be formally phrased in terms of a distribution over decision trees (how?).

Given input $x \in \{0,1,\ldots,n-1\}^n$

> Sample a uniformly random subset $\{i_1,\ldots,i_m\} \subseteq [n]$ of size m. Query $x_{i_1},\ldots,x_{i_m}$, if there is a collision, i.e., $i_a \neq i_b$ with $a,b \in [m]$, such that $x_{i_a} = x_{i_b}$, then output 1, else output 0.

How large of a $m \leq n/2$ do we need to pick? (Note if $m > n/2$, guaranteed to find a collision.) If x is a permutation, then will never observe a collision, so always correct in this case. So the probability of error is the probability that no collision is observed if x is two-to-one. Comment: first expression: for visual aid, consider a complete bipartite graph with $n/2$ vertices in each part.

$$\begin{aligned}\frac{n(n-2)(n-4)\ldots(n-2(m-1))/m!}{\binom{n}{m}} =& 1 \cdot \Big(1 - \frac{1}{n-1}\Big) \cdot \Big(1 - \frac{2}{n-2}\Big) \ldots \Big(1 - \frac{m-1}{n-m+1}\Big) \\ &\leq \exp\Big(-\sum_{i=1}^{m-1} \frac{i}{n-i}\Big) \leq \exp\Big(-\sum_{i=1}^{m-1} \frac{i}{n}\Big) = \exp\Big(-\frac{m(m-1)}{2n}\Big) \leq \exp\Big(-\frac{(m-1)^2}{2n}\Big).\end{aligned}$$

Therefore the probability of error is $\leq \epsilon$ if

$$\exp\Big(-\frac{(m-1)^2}{2n}\Big) \leq \epsilon \iff m \geq \sqrt{2n\ln(1/\epsilon)} + 1. \tag{103}$$

Therefore, $R_\epsilon(\mathrm{Simon}_n) \leq \min(\sqrt{2n\ln(1/\epsilon)} + 1, n/2)$. So $R(\mathrm{Simon}_n) \leq O(\sqrt{n})$. (Note that the algorithm only used the fact that x is either a permutation or two-to-one. It did not use the *additional* fact that in the two-to-one case, x is also periodic.) $\square$