Lecture 15

Comment: Draw two colored cubes on $n = 3$ bits, one for D_0 and one for D_1. Do the first step below using the examples.

1. Measure the second register (i.e., last n qubits), suppose outcome is $f(z)$ for some $z \in \{0,1\}^n$.

   If $f \in D_0$, then the state of the first register collapses to $|z\rangle$.

   If $f \in D_1$ and the period of f is s, then the state of the first register collapses to

$$\frac{1}{\sqrt{2}} \left(|z\rangle + |z \oplus s\rangle \right). \tag{82}$$

2. Apply $H^{\otimes n}$ to the first register and measure all n qubits.

   If $f \in D_1$:

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \{0,1\}^n} \left((-1)^{z \cdot y} + (-1)^{(z \oplus s) \cdot y} \right) |y\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{\substack{y \in \{0,1\}^n \\ y \cdot s = 0}} (-1)^{z \cdot y} |y\rangle, \tag{83}$$

   the output y is uniformly random subject to $y \cdot s = 0$ (dot product mod 2).

   If $f \in D_0$:

$$\frac{1}{\sqrt{2^n}} (-1)^{y \cdot z} |y\rangle \tag{84}$$

   the output y is uniformly random without constraints.

3. Repeat these steps $K = O(n)$ (the precise setting of K depends on the desired success probability, see later) times and collect the ys into the rows of a $K \times n$ matrix $A \in \{0,1\}_2^{K \times n}$. Output D_0 if A has rank n and D_1 if A has rank less than n, where the rank is defined over $\mathbb{F}_2$. (Note that the rank of A is at most n.)

Comment: rank of a zero-one matrix A over $\mathbb{F}_2$ is the dimension of the span of the rows of A over $\mathbb{F}_2$, which may be different from the rank of A over $\mathbb{R}$: for example, the matrix $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$ has rank 2 over $\mathbb{F}_2$ but rank 3 over $\mathbb{R}$. But almost all other standard facts in linear algebra still hold over $\mathbb{F}_2$, for example, row-rank=column-rank, the rank-nullity theorem, full-rank implies invertible, etc.

Query complexity is $K = O(n)$ since each repeat uses only 1 query.

For correctness, first note that if $f \in D_1$ then A must have rank less than n since the rows of A are all orthogonal to s. Alternatively, note that $As = 0$ and $s \neq 0$ so $n(A) > 0$, so the rank-nullity theorem, i.e., $\mathrm{rk}(A) + n(A) = n$, implies $\mathrm{rk}(A) < n$. Therefore, it suffices to lower bound the probability that the rank of A is equal to n as a function of K, which is done by the following lemma.

Lemma 2. *Let $K \in \mathbb{N}$. Suppose $y_1, \ldots, y_K \leftarrow \mathbb{F}_2^n$. Then*

$$\Pr[\mathrm{rk}(A) = n] \geq 1 - 2^{n-K}. \tag{85}$$

Based on [StackExchange post].

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

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

Therefore, $\Pr[\mathrm{rk}(A) = n] = \Pr[\ker(A) = \{0\}] \geq 1 - 2^{n-K}$, where the first equality follows from the rank-nullity theorem. □

Comment: proof of implication: assume wlog that $x_1 = 1$ so Ax is the first column of A plus another length-K vector: it does not matter what the other vector is, the sum will be uniformly random in $\mathbb{F}_2^K$.

Therefore, by choosing $K = n + 100$, say, the probability that the rank of A is equal to n is at least $1 - 2^{n-K} \geq 1 - 2^{-100}$, which is very close to 1.