Assignment 2

1. Show how to find $a \in \mathbb{Z}_2^n$ given one application of a black-box that maps $|x\rangle|b\rangle \to |x\rangle|b \oplus \langle x, a\rangle\rangle$ for some $b \in \{0,1\}$.

   Here, $\langle x, a\rangle = \sum_{i=1}^{n} x_i a_i$

2. For $x, y \in \{0,1\}^n$ and $s = x \oplus y$,

   Prove that $H^{\otimes n}\left(\frac{|x\rangle + |y\rangle}{\sqrt{2}}\right) = \frac{1}{2^{\frac{n-1}{2}}} \sum_{z \in \{s\}^{\perp}} (-1)^{\langle x, z\rangle} |z\rangle$

~~3. Let $S = \langle 0, s\rangle$ is a 0-dimens subspace of $\mathbb{Z}_2^n$ spanned by s. Define $|S\rangle = \sum_{s \in S}$~~

3. Let S be a subspace of $\mathbb{Z}_2^n$ of dimension $= m$.

   Define $|S\rangle = \sum_{s \in S} \frac{1}{2^{m/2}} |s\rangle$. Prove that

   $H^{\otimes n} |S\rangle = \sum_{w \in S^{\perp}} \frac{1}{2^{n-m}} |w\rangle$.

   For any $y \in \mathbb{Z}_2^n$, define $|y + S\rangle = \sum_{s \in S} \frac{1}{2^{m/2}} |y + s\rangle$. Compute $H^{\otimes n} |y + S\rangle$.

Let $W \leq \{0,1\}^n$ be a subspace of dimension m. Let $w_1, w_2, w_3, \ldots$ be a sequence of elements of W selected u.a.r.

Let $V_i = \langle w_1, w_2, \ldots, w_i \rangle$ be the subspace generated by $\{w_1, \ldots, w_i\}$. Define X_j to be the random variable denoting the lowest index i such that V_i has dimension j. Show an upper bound on the expected value of X_m.