Week 6 work: Oct. 18 — Oct. 25
9-hour week
Obligatory problems are marked with [**]
1. [Fourier Analysis of Boolean Functions.] Watch these two videos. If you really want to go crazy, you can watch this playlist.
2. [A simple Boolean Fourier formula.] [**] Let $f : \{0, 1\}^n \to \mathbb{C}$. In class we saw the following nice fact:

$$s = 000 \cdots 0 \implies \hat{f}(s) = \mathbb{E}_{x \sim \{0, 1\}^n}[f(x)],$$

where $\mathbb{E}_{x \sim \{0, 1\}^n}[]$ denotes “the expected value, when $x$ is chosen uniformly at random from $\{0, 1\}^n$”. (We wrote this as $\text{avg}_x[\cdot]$, but same difference.)

Prove also the following formula:

$$s \neq 000 \cdots 0 \implies \hat{f}(s) = \frac{1}{2} \left( \mathbb{E}_{x \sim \{0, 1\}^n}[f(x) \mid \chi_s(x) = +1] - \mathbb{E}_{x \sim \{0, 1\}^n}[f(x) \mid \chi_s(x) = -1] \right),$$

where the $\mid$ notation denotes “conditional expectation”.
3. [Hands-on XOR-pattern practice.]

(a) [**] Let $AND : \{0,1\}^2 \rightarrow \{0,1\}$ be the logical-AND function on two bits.
i. Write the full truth-table of $AND$.
ii. Let $and : \{0,1\}^2 \rightarrow \{\pm 1\}$ be defined by $and(x) = (-1)^{AND(x)}$. Write the full
   "truth-table" (table of function values) for $and$.
iii. Write the quantum state $|and\rangle$ in standard bra-ket notation.
iv. It’s too annoying to keep including the “$\frac{1}{\sqrt{N}}$ factors” everywhere. So for this
   problem, if $g : \{0,1\}^n \rightarrow \mathbb{C}$ is a function, let $[g]$ denote the column vector in
   $\mathbb{C}^N$ of $g$’s values ($N = 2^n$). Write the four length-4 column vectors $[\chi_s]$, where
   $\chi_s : \{0,1\}^2 \rightarrow \{\pm 1\}$ are the XOR functions corresponding to the 2-bit Boolean
   Fourier transform.
v. Compute $and(s)$ for each $s \in \{0,1\}^2$.
vi. Using your solutions to (ii), (iv), and (v), write down the explicit vector form of the
   true equation

   \[ [\text{and}] = \widehat{\text{and}}(00)[\chi_{00}] + \widehat{\text{and}}(01)[\chi_{01}] + \widehat{\text{and}}(01)[\chi_{10}] + \widehat{\text{and}}(11)[\chi_{11}] ; \]

   then write, “Yep.”

(b) [**] Repeat parts (ii), (v), (vi) for the function $MAJ : \{0,1\}^3 \rightarrow \{0,1\}$, defined by
$MAJ(x_1, x_2, x_3) =$ the majority bit-value among $x_1, x_2, x_3$. (Hint for doing (v) somewhat
efficiently: you might perhaps want to use the result in Problem 2.)

(c) Repeat parts (ii), (v), (vi) for the function $SORT : \{0,1\}^4 \rightarrow \{0,1\}$, defined as follows:
$SORT(x_1, x_2, x_3, x_4) = 1$ if and only if $x_1 \leq x_2 \leq x_3 \leq x_4$ or $x_1 \geq x_2 \geq x_3 \geq x_4$.
(Honestly, you might want to get a computer to help you with this.)
4. [Deutsch–Jozsa.] David and Richard enjoy the fact that one can easily take a classical circuit computing a Boolean function $F$, and convert it into a quantum circuit which implements the same Boolean function when given “classical inputs” — but which also can accept quantum superpositions of classical inputs. David and Richard did this for a bunch of Boolean functions, including:

- The constantly-0 function $F : \{0,1\}^n \rightarrow \{0,1\}$, satisfying $F(x) = 0$ for all $x$.
- Various balanced functions, meaning $F$ having $F(x) = 0$ for 50% of inputs $x$ and $F(x) = 1$ for 50% of inputs $x$.

Unfortunately, David and Richard forgot to label their quantum circuits, and now they forget which ones compute what! David and Richard run across an old circuit $Q^\pm$ they built which evidently “sign-implements” some $F : \{0,1\}^n \rightarrow \{0,1\}$, but they’re not sure if $F$ is all-0, or if it’s balanced.

(a) [**] Show that it is possible for David and Richard to tell whether $F$ is all-0 or balanced by just using $Q^\pm$ once. (Hint: The good old Fourier sampling paradigm. Which outcome $s$ tells you about the balancedness of $F$?)

(b) [**] Suppose now you only have access to a classical circuit $C$ computing a Boolean function $F$, promised to be either all-0 or else balanced. Show that if you act deterministically, there is no way you can tell the difference unless you apply $C$ to more than $2^{n-1}$ inputs.

(c) [**] On the other hand, suppose that you have the classical $C$ but you may use randomness. Show that by applying $C$ to only $T$ classical inputs, you can tell the difference between all-0 $F$ and balanced $F$ with one-sided error $2^{-T}$.
5. **Translated Fourier coefficients.** [**] Let $f : \{0,1\}^n \to \mathbb{C}$. Now for $y \in \{0,1\}^n$, define the function $f^+ y : \{0,1\}^n \to \mathbb{C}$ by $f^+ y(x) = f(x + y)$. (Here the addition is in $\mathbb{F}_2^n$; i.e., coordinate-wise mod 2.) Compute $\hat{f^+ y}(s)$ in terms of $\hat{f}(s)$. How does performing Fourier sampling of $f^+ y$ compare to performing Fourier sampling on $f$?
6. [Complex roots of unity.]

(a) Review, if necessary, Problem 2 on Weekly Work 2.

(b) [★★] Let $M$ be a positive integer and let $\omega_M \in \mathbb{C}$ be the primitive $M$th root of unity. Let $0 \leq t < M$ be an integer. Compute

$$\operatorname{avg}_{u \in \{0,1,2,\ldots,M-1\}} \{\omega^{tu}\}.$$

There should be two possible outcomes, depending on $t$. (Hint.)
7. [Subspaces and Fourier transforms.] Recall our discussion from the last homework about the vector space \( \mathbb{F}_2^n \), the \( n \)-dimensional vector space over the field \( \mathbb{F}_2 = \{0, 1\} \).

(a) Suppose \( A \subseteq \mathbb{F}_2^n \) is a linear subspace of dimension \( k \); that is, \( A \) is the span of \( k \) linearly independent vectors. Let \( A^\perp \) denote the set \( \{s \in \mathbb{F}_2^n : s \cdot x = 0 \ \forall x \in A\} \), where \( s \cdot x \) denotes the dot product. Show that \( A^\perp \) is a subspace; specifically, a subspace of dimension \( n - k \).

(b) Just so you don’t get too comfortable thinking that things are exactly the same as in \( \mathbb{R}^n \) or \( \mathbb{C}^n \): give an example, when \( n = 2 \), of a subspace \( A \) of dimension \( k = 1 \) such that \( A^\perp = A \).

(c) Show that \( (A^\perp)^\perp = A \).

(d) [**] Given subspace \( A \) of dimension \( k \) (and hence cardinality \( 2^k \)), define the function

\[
g : \{0, 1\}^n \to \mathbb{C}, \quad f(x) = \begin{cases} \sqrt{\frac{N}{2^n}} & \text{if } x \in A, \\ 0 & \text{if } x \not\in A, \end{cases}
\]

where \( N = 2^n \) as usual. (The constant \( \sqrt{\frac{N}{2^n}} \) is chosen so that \( \text{avg}_x \{|g(x)|^2\} = 1 \) and hence \( |f\rangle \) is a quantum state.)

Compute \( H^{\otimes n} |g\rangle \); equivalently, compute \( \hat{g}(s) \) for each \( s \in \{0, 1\}^n \).