The Hidden Subgroup Problem

Clayton W. Seitz

April 28, 2023

The Hidden Subgroup Problem

Let G be a group and X a finite set and $f : G \to X$ a function that *hides* a subgroup $H \leq G$. The problem is to determine H. A nice example for the Abelian version is Simon's problem.

Simon's problem. Given a 2-1 function $f : \{0,1\}^n \to \{0,1\}^n$ such that there is a secret string $s \in \{0,1\}^n$ where $f(x) = f(y)$ if and only if $x \oplus y = s$.

The function f is a black box. Clasically you would solve the problem by drawing pairs x, y and checking if $f(x) = f(y)$. If they match, you can obviously retrieve $s = x \oplus y$

Clasically the problem scales as $\mathcal{O}(2^{n/2})$ but Simon designed a quantum algorithm that scales as $\mathcal{O}(n)$.

Solution to Simon's problem

Solution is very similar to the common solution to the HSP

In the first register, we prepare a uniform superposition over all possible input strings x

In the second register we use ancillary bits that will store $f(x)$

$$|\psi\rangle = H^{\otimes n} |0^n\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$$

We assume we have some oracle function U_f which will compute and store $f(x)$ in register 2

$$O_f(|\psi\rangle |0^n\rangle) = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

Solution to Simon's problem

Then we measure the second register

This collapses the system to a superposition of the two inputs that map to our measured output $|f(a)\rangle$

$$\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle\,|f(x)\rangle \rightarrow (|a\rangle + |a \oplus s\rangle) \otimes |f(a)\rangle$$

Then, we can Fourier transform the first register

$$\sum_{\gamma} \gamma\,|\gamma\rangle \otimes |f(a)\rangle$$

If we measure the first register we get γ with probability $|\gamma|^2$.