Solve HSP quantumly

- Step 1: Prepare uniform superposition

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle$$

- Step 2: Load "data" F:

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |F(x)\rangle$$

- Step 3: Measure answer qubits, and get some label C^*.
  - State collapses to …?

- Get a random coset state $|gH\rangle$ = …?
- Recall: a probability distribution over quantum states is called a mixed state
- ρ_H := uniform distribution over all coset states $|gH\rangle$
- Question: can we learn H from ρ_H?
- Idea:
  - Apply the appropriate Fourier transform for G and measure
  - Obtain a “clue” about H
  - Deduce H (hopefully) from the clues

- Fact 1: When G is finite commutative, that is $G = \mathbb{Z}/N_1\mathbb{Z} \times \ldots \times \mathbb{Z}/N_k\mathbb{Z}$, the appropriate Fourier transform is $\mathrm{DFT}_{N_1} \otimes \ldots \otimes \mathrm{DFT}_{N_k}$, which can be implemented efficiently by a quantum circuit.

- Application: $G = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, Shor's discrete log algorithm, which breaks Diffie–Hellman

- Fact 2: When G is not commutative, the appropriate Fourier transform can be implemented efficiently in most cases, but don't know how to deduce H from clues efficiently.

- Application 1: G is the dihedral group D_n, which solves approximate shortest vector in a lattice.

- Application 2: G is the symmetric group S_n, which solves graph isomorphism

Grover's algorithm

- Task: Given N bits, find a 1. Think of truth table of Boolean function $F\colon \{0,1\}^n \to \{0,1\}$, where $N = 2^n$
- In "black-box query" model
  - Deterministic / probabilistic algorithm needs about N queries
  - Quantum algorithm uses $\sqrt{N}$ queries
- Theorem [BBBV '94] In the "black box query" model, at least $c\sqrt{N}$ queries of Q_F are needed. (Grover's algorithm is the best one can hope for.)

- Given description of circuit F, this is precisely SAT problem:
  - NP-complete. P != NP means no poly(n)-time classical algorithm
  - SETH (strong exponential time hypothesis) means no 1.999^n-time classical algorithm

Grover's algorithm

- Given quantum circuit Q_F implementing $F\colon \{0,1\}^n \to \{0,1\}$, want to find $x \in \{0,1\}^n$ such that $F(x) = 1$ or become confident none exists
- Key difference from Bernstein–Vazirani / Simon / Shor
  - F is not promised to have any special structure / pattern
- Assume hardest case $F(x) = 1$ for exactly one string $x^* \in \{0,1\}^n$
- Sign-implementation trick

$$\begin{bmatrix} \alpha_{00\cdots0} \\ \alpha_{00\cdots1} \\ \vdots \\ \\ \alpha_{11\cdots1} \end{bmatrix} \xrightarrow{Q_F^{\pm}} \begin{bmatrix} \alpha_{00\cdots0} \\ \alpha_{00\cdots1} \\ \vdots \\ -\alpha_{x^*} \\ \vdots \\ \alpha_{11\cdots1} \end{bmatrix}$$