

# 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  $|gH\rangle = \dots?$
- Recall: a probability distribution over quantum states is called a mixed state
- $\rho_H :=$  uniform distribution over all coset states  $|gH\rangle$
- Question: can we learn  $H$  from  $\rho_H$ ?
- 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  $G = \mathbb{Z}/N_1\mathbb{Z} \times \dots \times \mathbb{Z}/N_k\mathbb{Z}$ , the appropriate Fourier transform is  $\text{DFT}_{N_1} \otimes \dots \otimes \text{DFT}_{N_k}$ , 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

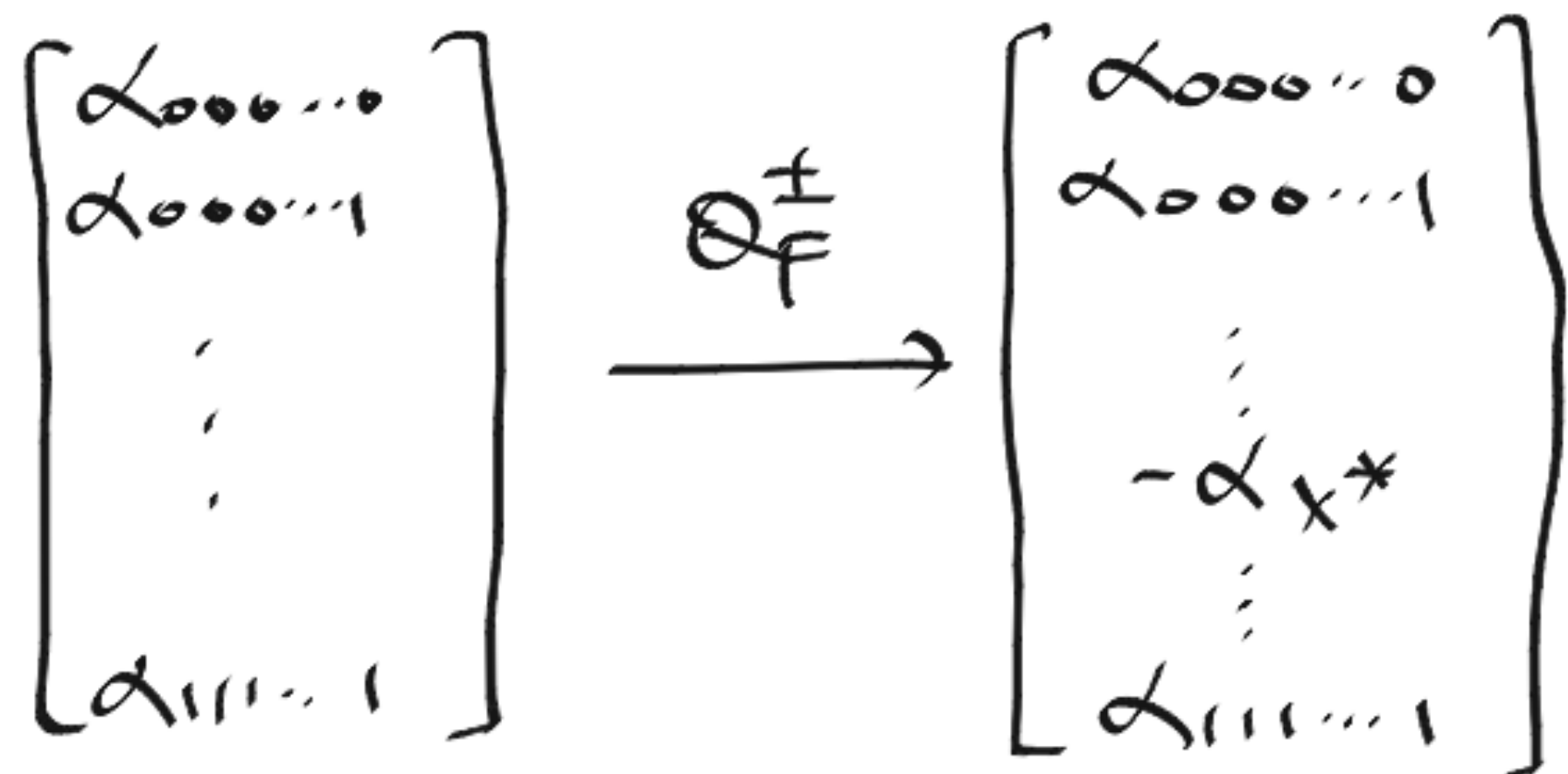
# Grover's algorithm

- Task: Given  $N$  bits, find a 1. Think of truth table of Boolean function  $F: \{0,1\}^n \rightarrow \{0,1\}$ , 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.  $P \neq NP$  means no  $\text{poly}(n)$ -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  $F: \{0,1\}^n \rightarrow \{0,1\}$ , 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
 

The diagram illustrates the sign-implementation trick. It shows a transformation of a vector of amplitudes. On the left, a column vector is enclosed in large square brackets. It contains several entries: the top two are  $\alpha_{000\dots 0}$  and  $\alpha_{000\dots 1}$ , followed by three vertical dots, and the bottom entry is  $\alpha_{111\dots 1}$ . An arrow points from this vector to the right. Above the arrow is the label  $Q_F^\pm$ . On the right, another column vector is enclosed in large square brackets. Its top two entries are the same as the first vector:  $\alpha_{000\dots 0}$  and  $\alpha_{000\dots 1}$ . It also has three vertical dots in the middle. The entry corresponding to  $x^*$  is  $-\alpha_{x^*}$ , with a minus sign in front. The bottom entry is  $\alpha_{111\dots 1}$ .