

Quantum Computing – The Grover Algorithm for 2 Qbits

Bill Celmaster

June 6, 2026

Problem setup

- ▶ Consider a 2-qubit system with computational basis states:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

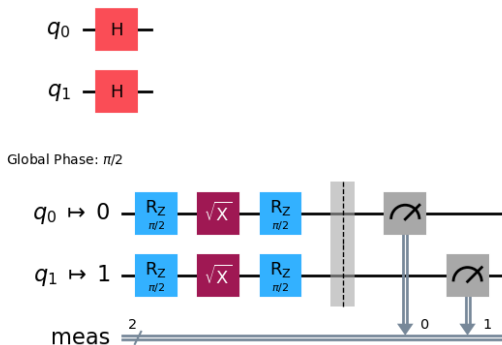
- ▶ Choose a target (“password”) – we’ll use the following:

$$z = 10$$

- ▶ Our goal is to identify the state $|10\rangle$.

Superposition

- ▶ Apply a Hadamard gate to both qubits and run 10000 times
- ▶ The effect is $|00\rangle \rightarrow \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$



Job ID: d8evnqo7jphs7391f5m0

Probabilities: {'11': 0.2632, '10': 0.2482, '00': 0.2392, '01': 0.2494}

Oracle

- ▶ We want an operator with:
 - ▶ $|10\rangle \rightarrow -|10\rangle$
 - ▶ $|ij\rangle \rightarrow |ij\rangle$ when $|ij\rangle \neq |10\rangle$
- ▶ Use the built-in gate *controlled-z* (\mathbf{U}_{CZ}) with:
 - ▶ $|11\rangle \rightarrow -|11\rangle$
 - ▶ $|ij\rangle \rightarrow |ij\rangle$ when $|ij\rangle \neq |11\rangle$
- ▶ So first convert $|i0\rangle$ to $|i1\rangle$ and $|i1\rangle$ to $|i0\rangle$
 - ▶ Accomplish this by applying the X gate to qbit 1
- ▶ Then apply the *controlled-z* gate, so
 - ▶ $|10\rangle \rightarrow |11\rangle \rightarrow -|11\rangle$
 - ▶ $|11\rangle \rightarrow |10\rangle \rightarrow |10\rangle$; $|01\rangle \rightarrow |00\rangle \rightarrow |00\rangle$; $|00\rangle \rightarrow |01\rangle \rightarrow |01\rangle$
- ▶ Finally, again use the X gate to convert $|i0\rangle$ to $|i1\rangle$ and $|i1\rangle$ to $|i0\rangle$
 - ▶ $|10\rangle \rightarrow |11\rangle \rightarrow -|11\rangle \rightarrow -|10\rangle$
 - ▶ $|11\rangle \rightarrow |10\rangle \rightarrow |10\rangle \rightarrow |11\rangle$
 - ▶ $|01\rangle \rightarrow |00\rangle \rightarrow |00\rangle \rightarrow |01\rangle$
 - ▶ $|00\rangle \rightarrow |01\rangle \rightarrow |01\rangle \rightarrow |00\rangle$

Diffusion

- ▶ For $|\psi\rangle = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle$
 - ▶ $\mu = \frac{1}{4} \sum_i \alpha_i$
 - ▶ $\mathbf{D} : |\psi\rangle \rightarrow 2\mu(|00\rangle + |01\rangle + |10\rangle + |11\rangle) - |\psi\rangle$
 - ▶ $\implies \mathbf{D} = \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$
 - ▶ \mathbf{D} is unitary (so can be a gate)
- ▶ Example 1: $\alpha_i = \frac{1}{2}$
 - ▶ $\mu = \frac{1}{2}$
 - ▶ $\mathbf{D} : |\psi\rangle \rightarrow |\psi\rangle$
- ▶ Example 2: $\alpha_3 = -\frac{1}{2}; \alpha_1 = \alpha_2 = \alpha_4 = \frac{1}{2}$
 - ▶ $\mu = \frac{1}{4}$
 - ▶ $\mathbf{D} : |\psi\rangle \rightarrow |10\rangle$

Grover (with a diffusion gate)

The “password” 10 is identified with $|10\rangle$ and confirmed by the oracle for 10.

- ▶ Superposition: $\mathbf{U}_{\mathbf{H}\otimes\mathbf{H}} : |00\rangle \rightarrow |\mathbf{S}\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
- ▶ Oracle is $\mathbf{O}_{10} = \mathbf{U}_{\mathbf{I}_1\otimes\mathbf{X}}\mathbf{U}_{\mathbf{CZ}}\mathbf{U}_{\mathbf{I}_1\otimes\mathbf{X}}$
 $\mathbf{O}_{10}|\mathbf{S}\rangle = \frac{1}{2} (|00\rangle + |01\rangle - |10\rangle + |11\rangle)$
- ▶ Diffusion: $\mathbf{D}\mathbf{O}_{10}|\mathbf{S}\rangle = |10\rangle$
- ▶ Measurement: result is $|10\rangle$

Another password, 01

- ▶ Its oracle \mathbf{O}_{01} is $\mathbf{U}_{\mathbf{X}\otimes\mathbf{I}_2}\mathbf{U}_{\mathbf{CZ}}\mathbf{U}_{\mathbf{X}\otimes\mathbf{I}_2}$
- ▶ $\mathbf{O}_{01}|\mathbf{S}\rangle = \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle + |11\rangle)$
- ▶ $\mathbf{D}\mathbf{O}_{01}|\mathbf{S}\rangle = |01\rangle$

Generalize – change the password (oracle) and the procedure selects it.

Implementation of the diffusion gate

- ▶ We'll build the diffusion gate out of "standard" gates.

$$\begin{aligned} \text{▶ } \mathbf{U}_{\mathbf{H} \otimes \mathbf{H}} &= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \quad \mathbf{U}_{\mathbf{I}_1 \otimes \mathbf{H}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}, \\ \mathbf{U}_{\mathbf{X} \otimes \mathbf{X}} &= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \mathbf{U}_{\mathbf{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{aligned}$$

- ▶ We can show that $\mathbf{D} = \mathbf{U}_{\mathbf{H} \otimes \mathbf{H}} \mathbf{U}_{\mathbf{X} \otimes \mathbf{X}} \mathbf{U}_{\mathbf{I}_1 \otimes \mathbf{H}} \mathbf{U}_{\mathbf{CNOT}} \mathbf{U}_{\mathbf{I}_1 \otimes \mathbf{H}} \mathbf{U}_{\mathbf{X} \otimes \mathbf{X}} \mathbf{U}_{\mathbf{H} \otimes \mathbf{H}}$.