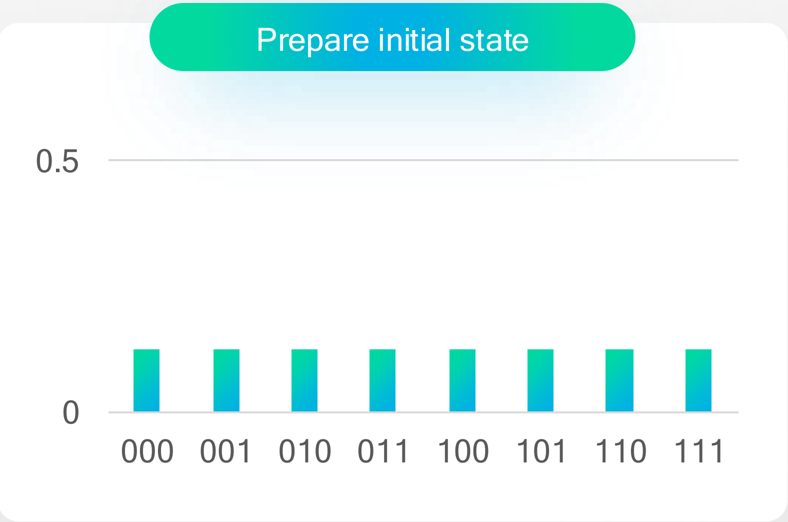
Introduction to Quantum Algorithms

A lecture series by IQM and HS RM

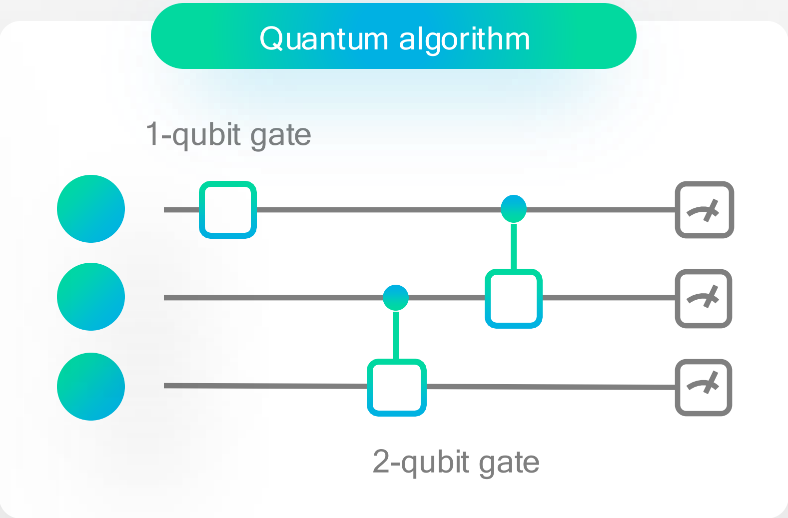
Authors: Stefan Seegerer

Last Updated 06/2025

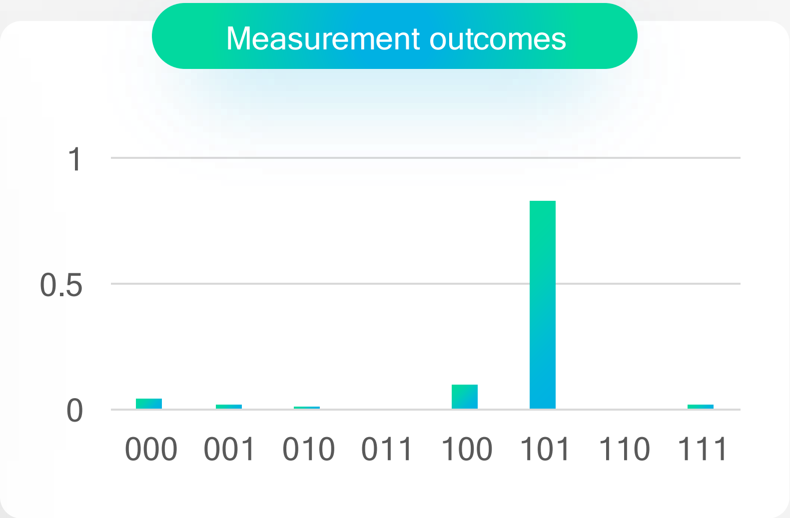
Quantum computing: algorithms



Prepare initial quantum state



Use interference to make wanted outcomes more likely

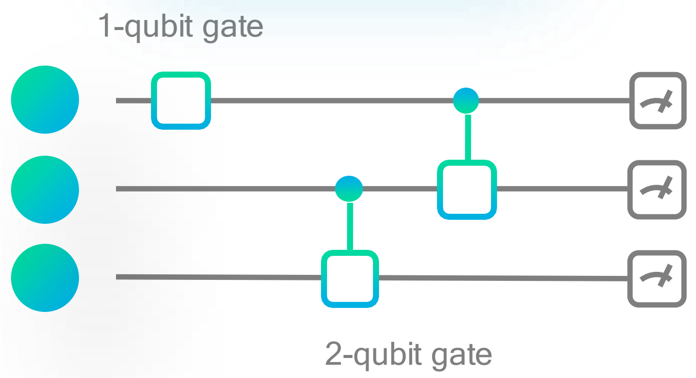


Measure multiple times

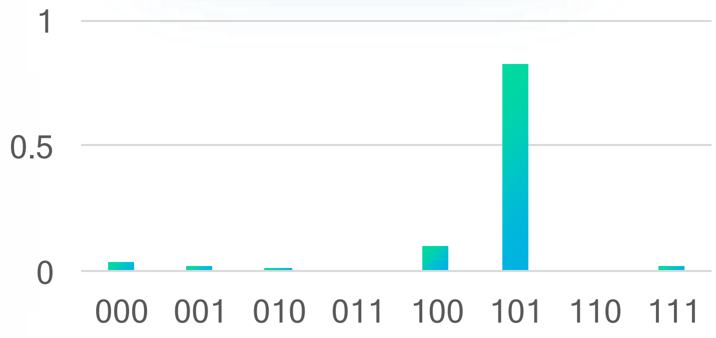
Quantum computing: algorithms

- Quantum algorithms leverage superposition and entanglement to enable new algorithms and manipulate qubits via quantum operations (or gates).
- Quantum algorithms explore a superposition of solution paths simultaneously.
- Quantum algorithms use interference to enhance the likelihood of measuring correct solutions.

Quantum operations

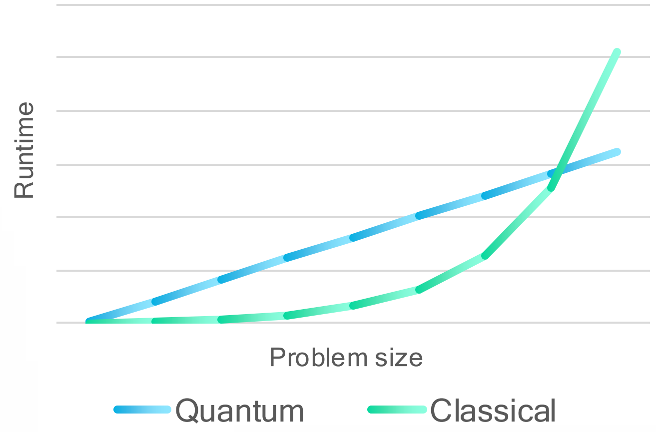


Measurement outcomes



Quantum algorithms vs. Classical algorithms

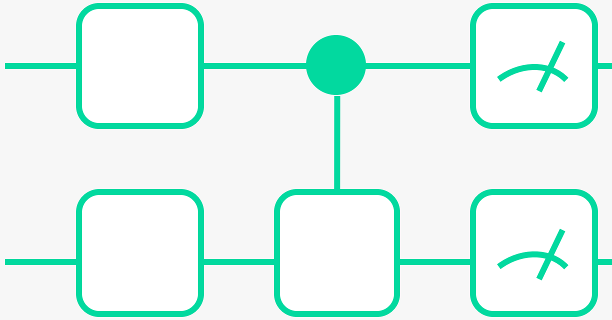
Quantum algorithms can provide up to exponential speedup for certain tasks in domains like simulation, optimization, or machine learning.



Quantum computers do not speed up existing algorithms but allow new types of algorithms

IQM

Near-term quantum computing applications compass three main areas



Quantum simulation

Material science, pharmacy, biology, chemistry, high energy physics

Optimization

Logistics, processes, portfolios, risks

Artificial intelligence / machine learning

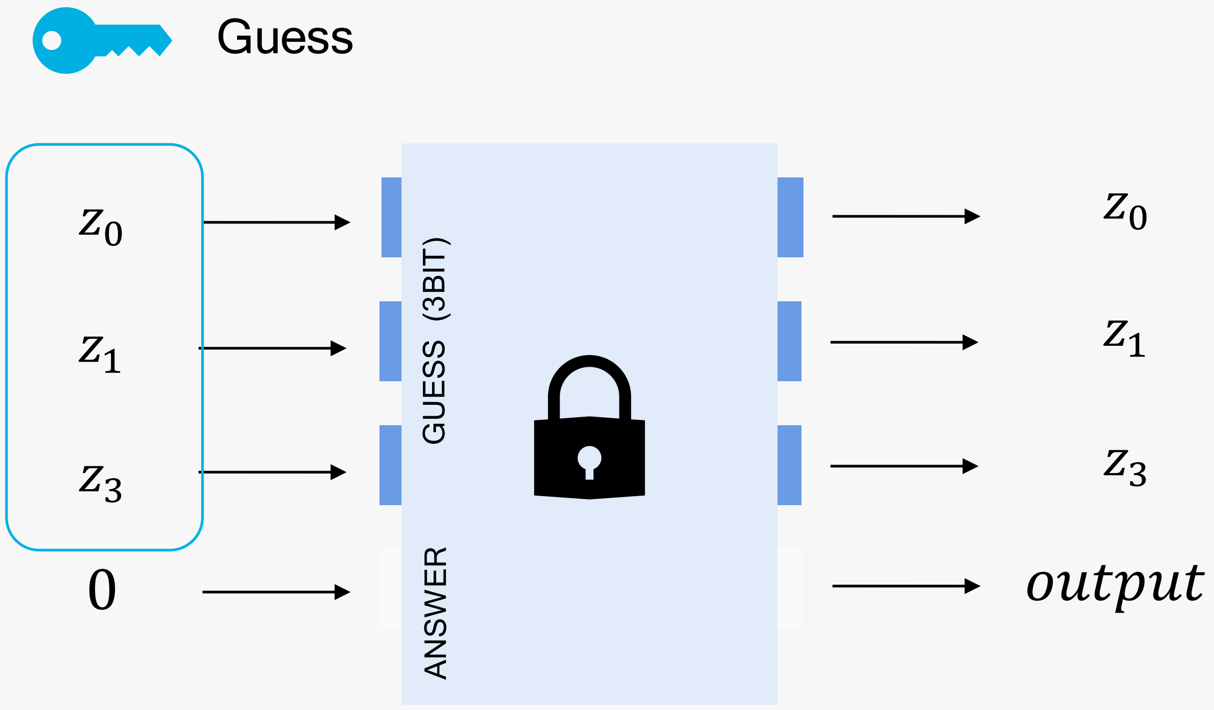
Model training, pattern recognition

Simple Quantum Algorithms: Bernstein Vazirani

Problem

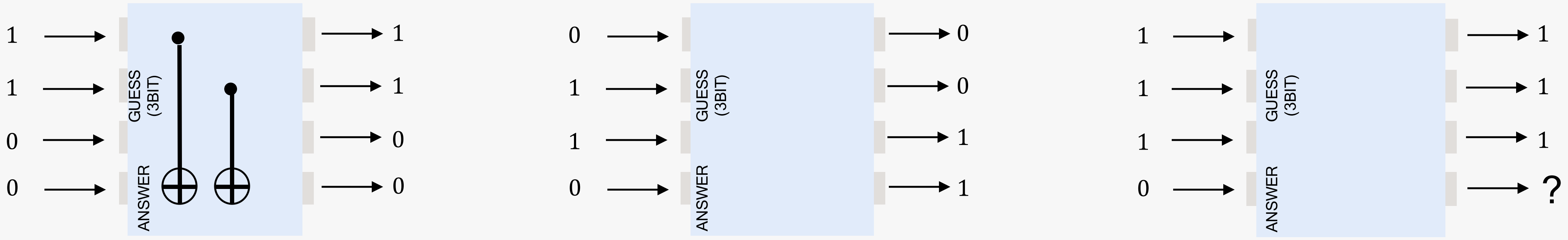
- Given: A secret (but unknown) code
- Given: A black box, that changes the answer for every 1 in the secret code (0 → 1, 1 → 0)

- **Goal**: identify secret code



Example

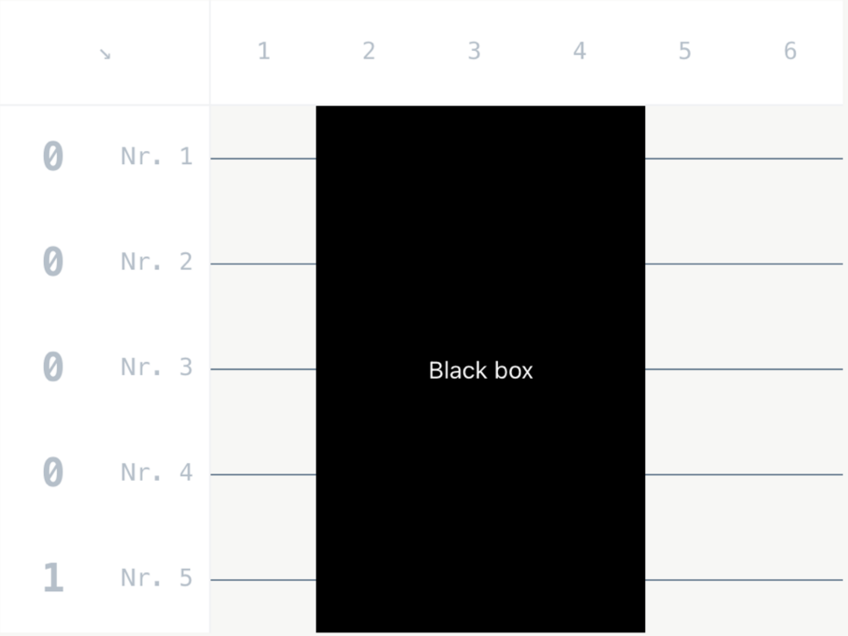
secret code = 110



IQM

QUIZ TIME!

Develop a strategy for the given problem. How many attempts do you need? Describe your approach.

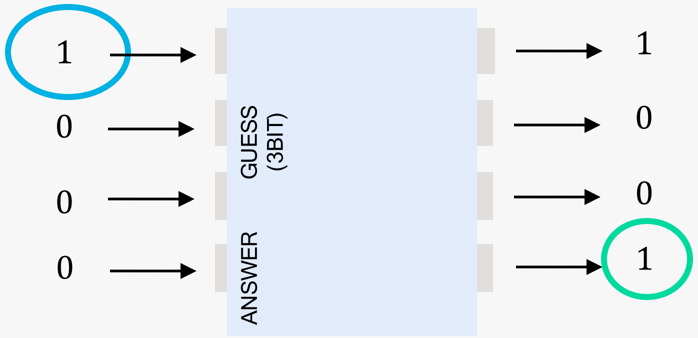


Easy solution

- Set all inputs except one to 0

Easy solution

- Set all inputs except one to 0
- The last qubit indicates if there is a 0 or 1 on this position



Easy solution

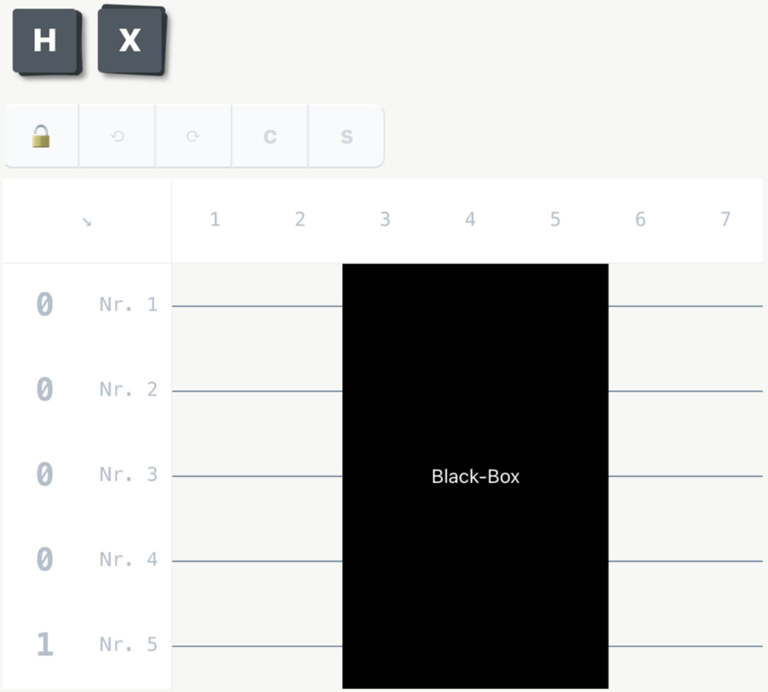
- Set all inputs except one to 0
- The last qubit indicates if there is a 0 or 1 on this position
- Repeat for every digit in the secret code

Secret code is: 101 !

QUIZ TIME!

To find out the secret 4-digit code of this black box, prepare an equal superposition of all 5 qubits. Apply a set of H also after the black box.

Afterward, open the black box and check how you can retrieve the secret code from the measurement outcomes.



Quantum solution

- Initialize GUESS Qubits with 0, answer qubit with 1

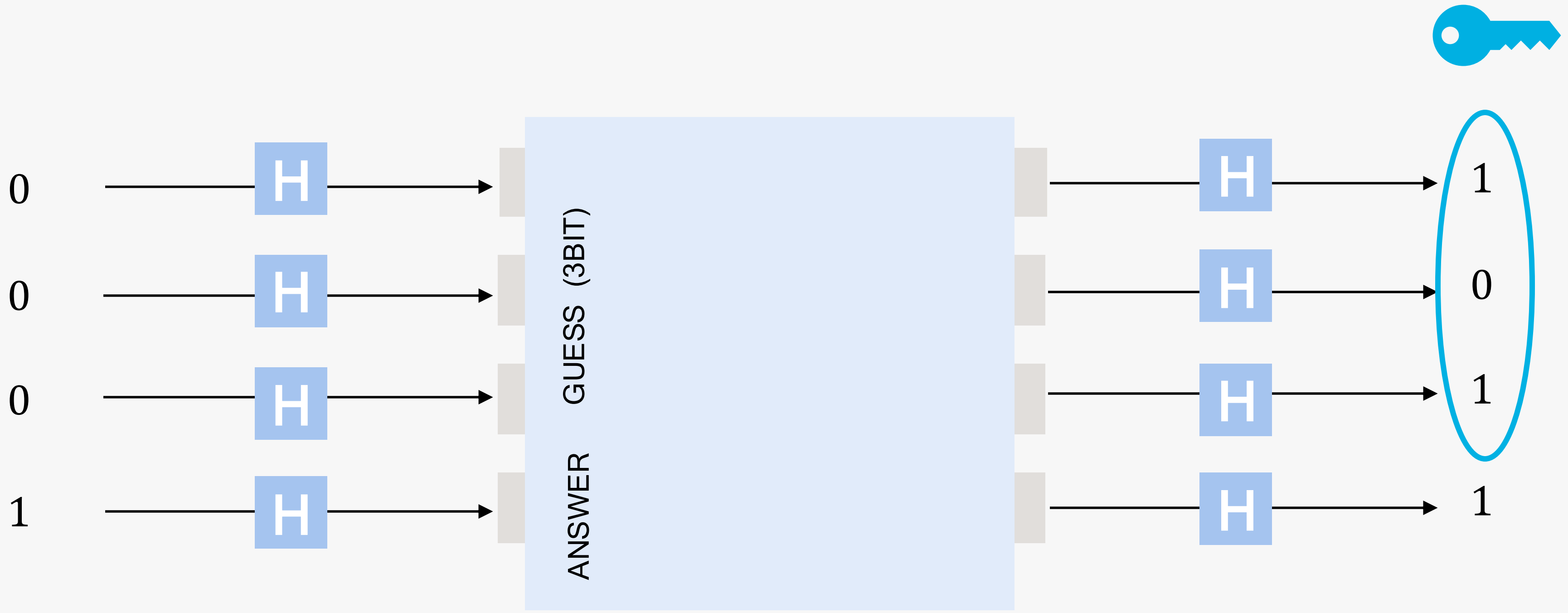
Quantum solution

- Initialize GUESS Qubits with 0, answer qubit with 1
- Apply H gates before and after the black box

IQM

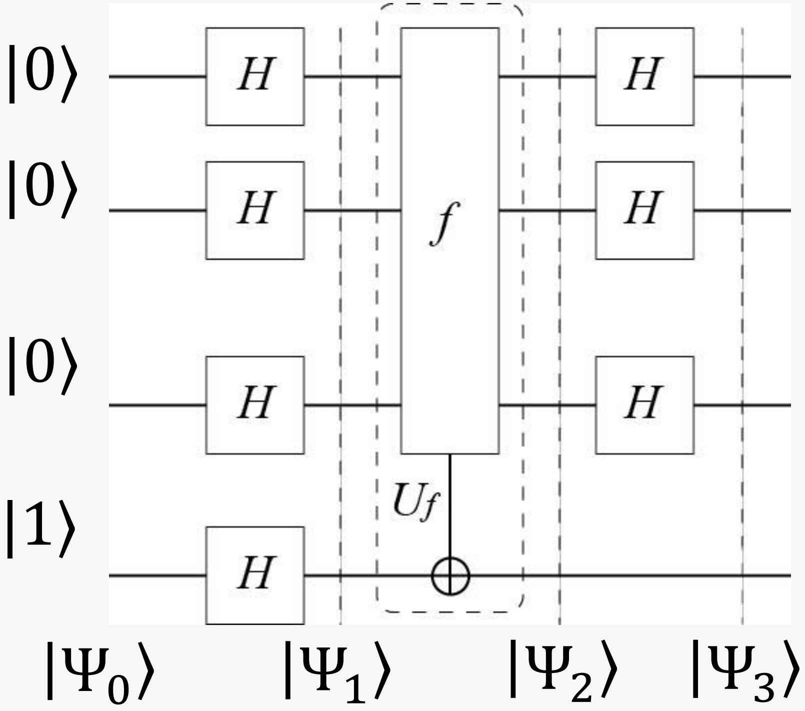
Quantum solution

- Initialize GUESS Qubits with 0, answer qubit with 1
- Apply H gates before and after the black box
- Output of GUESS qubits is the secret code 🤩



Bernstein-Vazirani algorithm expressed mathematically

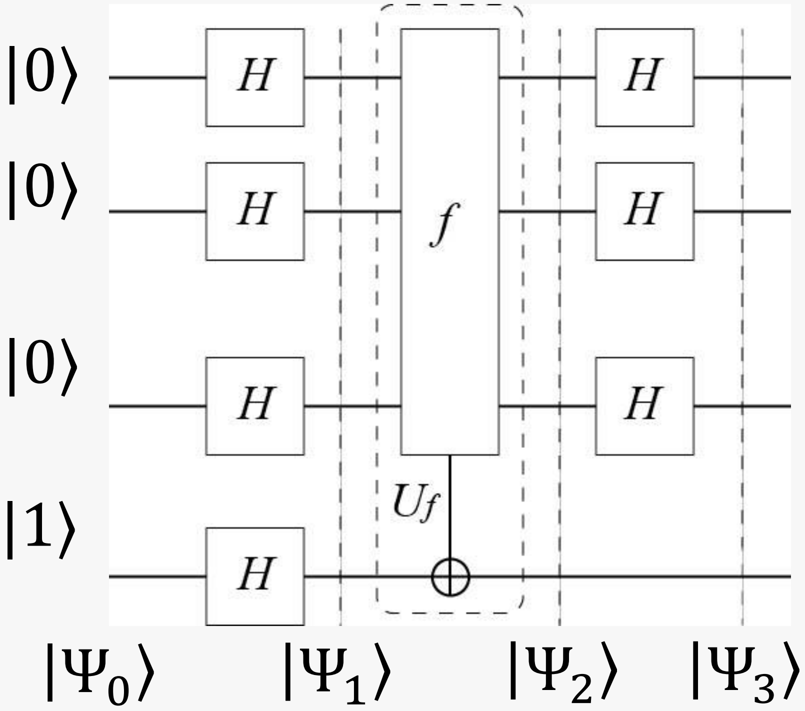
- Let $f = c \cdot x = c_{n-1}x_{n-1} \oplus \cdots \oplus c_0x_0$: $S_n \equiv \{0,1,\dots,2^n-1\} \rightarrow \{0,1\}$. $c = c_{n-1} \dots c_1c_0$.
- We need to evaluate f n times for n different x to find c classically.
  $x = (100 \dots 0)$ is used to find c_{n-1}, for example.
- The Bernstein-Vazirani algorithm finds c with a single query of f.



- $|\Psi_0\rangle = |1\rangle|00\dots0\rangle$.
- $|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)^{\otimes n}$
  $= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$
- $|\Psi_2\rangle = U_f|\Psi_1\rangle$
  $= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle(|c \cdot x\rangle - |\neg c \cdot x\rangle)|x\rangle$
  $= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{c \cdot x}|x\rangle$

$U_f|y,x\rangle = |y \oplus (c \cdot x), x\rangle$

Bernstein-Vazirani algorithm

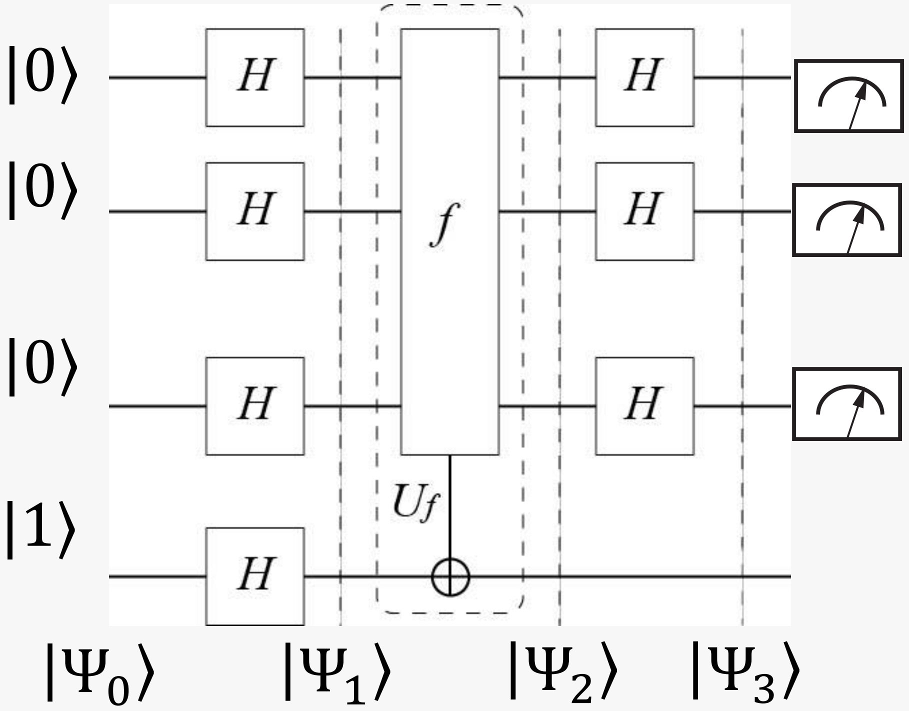


- $|\Psi_3\rangle = (I \otimes H^{\otimes n})|\Psi_2\rangle$
  $= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{c\cdot x} H^{\otimes n}|x\rangle$.
- Recall that

$$H|x_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_k}|1\rangle)$$
$$= \frac{1}{\sqrt{2}}\sum_{y_k\in\{0,1\}}(-1)^{x_k y_k}\,|y_k\rangle.$$ Then
$$H^{\otimes n}|x\rangle = (H|x_{n-1}\rangle)(H|x_{n-2}\rangle)\dots(H|x_0\rangle)$$
$$= \frac{1}{\sqrt{2^n}}\sum_{y_k\in\{0,1\}}(-1)^{x_{n-1}y_{n-1}+\cdots+x_0y_0}|y_{n-1}\dots y_0\rangle$$
$$= \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle.$$

- $|\Psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,\frac{1}{2^n}\sum_{x_k,y_k\in\{0,1\}}(-1)^{c\cdot x+\,x\cdot y}|y\rangle$.
- Let $y = c$. Then the phase is 1 independently of x and $\sum_{x_k\in\{0,1\}} 1 = 2^n$.
- If $y \neq c$, a half of x gives $(-1)^{c\cdot x+\,x\cdot y} = +1$ and the rest $(-1)^{c\cdot x+\,x\cdot y} = -1$.

Bernstein-Vazirani algorithm



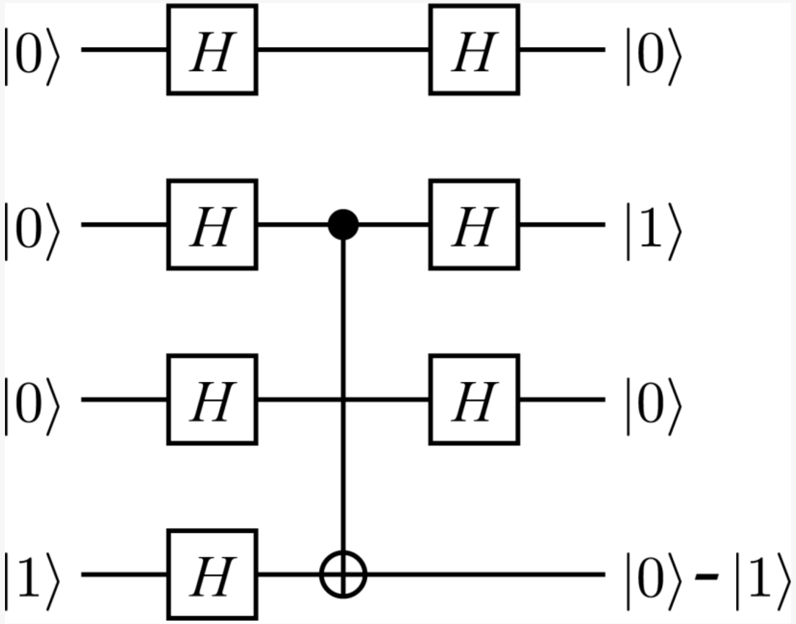
- $|\Psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|c\rangle$.
- A single measurement of the n qubits reveals $c = c_{n-1}c_{n-2} \dots c_1 c_0$.

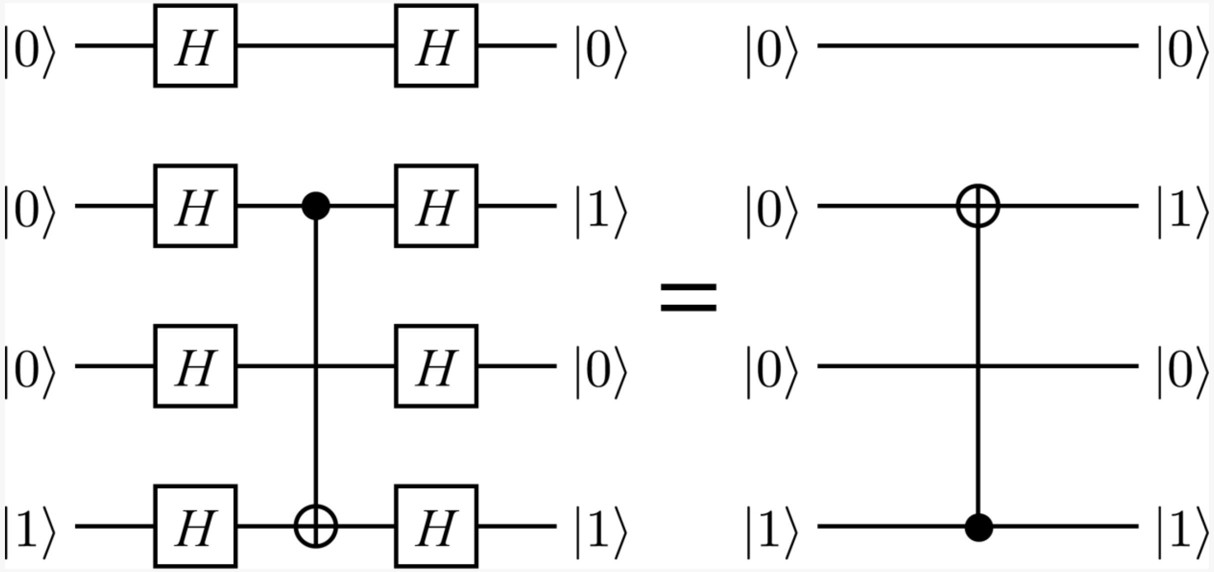
IQM

Bernstein-Vazirani algorithm

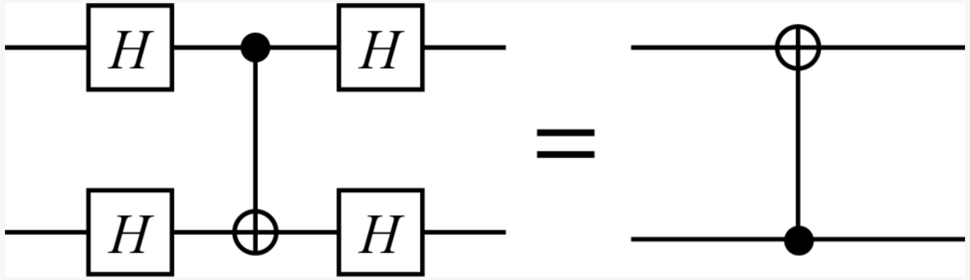
Another example:

- Let us consider U_f for $c = 010$ for example.

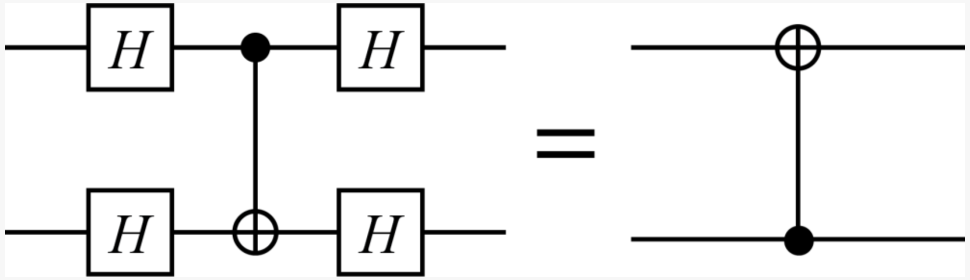




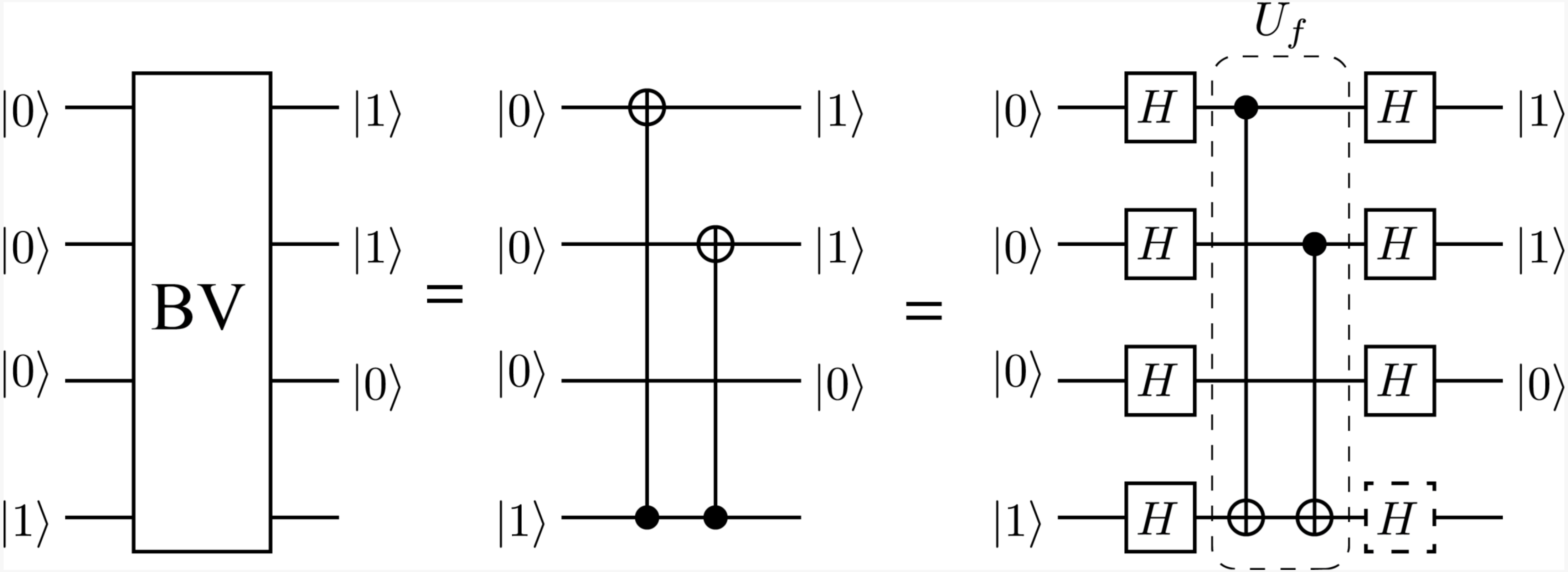
<u>**Exercise**</u>: Show that



Exercise



- Find the oracle U_f for $c = 110$.



Conclusion: Quantum algorithms

- Quantum algorithms use hybrid manner, utilizing both quantum and classical computing resources
- Quantum algorithms are adaptable to a range of problems. Developing a deeper understanding of suitable problems and how they are mapped is essential
- Achieving early quantum advantage requires the strategic alignment of purpose-built algorithms with targeted problems and the compatible hardware