# Introduction to Quantum Computation

**Artur Miroszewski**

Quantum Cosmos Lab, Jagiellonian University

High Performance and Disruptive Computing in Remote Sensing School 2025

JAGIELLONIAN UNIVERSITY IN KRAKÓW

Quantum Cosmos Lab

## QUEST Technical Committee


Gabriele Cavallaro


Upendra N. Singh


Artur Miroszewski

## QS4EO WG


Aaron Strangfeld


Jan Rudolph

## QC4EO WG


Alessandro Sebastianelli


Francesco Mauro


Amer Delilbasic

Join QUEST!

# Course material

09:30 - 11:00 **Introduction to Quantum Computation**

11:00 - 11:30 Break

11:30 - 12:00 Quantum Algorithms

12:00 - 13:00 Hands-on Session 1

13:00 - 14:30 Lunch

14:30 - 15:30 Quantum machine learning

15:30 - 16:00 Break

16:00 - 17:00 Hands-on Session 2

# Course material

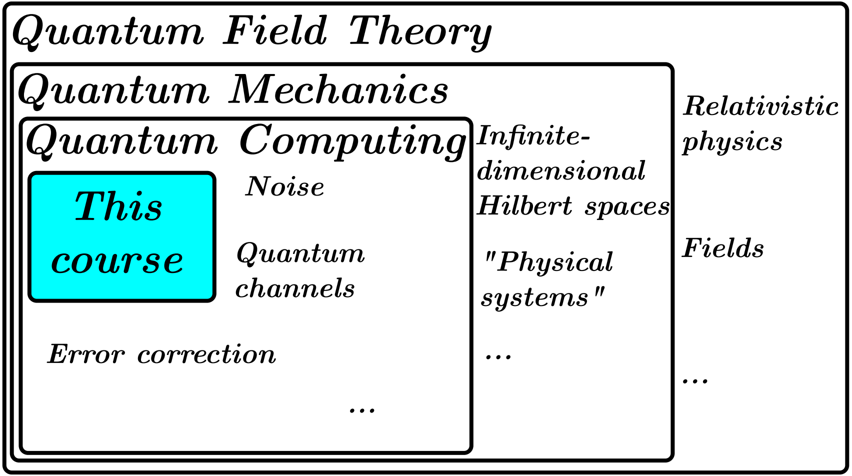
| | |
|---|---|
| 09:30 - 11:00 | **Introduction to Quantum Computation** |
| 11:00 - 11:30 | Break |
| 11:30 - 12:00 | Quantum Algorithms |
| 12:00 - 13:00 | Hands-on Session 1 |
| 13:00 - 14:30 | Lunch |
| 14:30 - 15:30 | Quantum machine learning |
| 15:30 - 16:00 | Break |
| 16:00 - 17:00 | Hands-on Session 2 |

**Introduction to Quantum Computation**

- Basic notions and postulates of quantum mechanics
- Measurement
- Introduction of quantum gates and circuits
- Computational paradigms and quantum computing hardware technologies

**Quantum Algorithms**

- Logic behind quantum algorithms
- Advanced circuits
- Review of main algorithms


Quantum Field Theory
Quantum Mechanics
Quantum Computing
This course
Noise
Quantum channels
Error correction
...
Infinite-dimensional Hilbert spaces
"Physical systems"
...
Relativistic physics
Fields
...

# Math reminder - Complex numbers

## Basic definition

$$z = \underbrace{a}_{\text{real part}} + i \underbrace{b}_{\text{imaginary part}}$$

$$Re[z] = a, \;\; Im[z] = b$$

$$i^2 = -1 \rightarrow \sqrt{-1} = i$$

## Complex conjugation

$$z^* = a - ib$$

$$Re[z] = \frac{1}{2}(z + z^*)$$

$$Im[z] = \frac{1}{2}(z - z^*)$$

## Basic operations

Addition

$$z_1 + z_2 = (a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2)$$

Multiplication

$$z_1 \cdot z_2 = (a_1 + ib_1) \cdot (a_2 + ib_2) = (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1)$$

Modulus

$$|z| = \sqrt{z \cdot z^*} = \sqrt{a^2 + b^2}$$

## Example

$$z = 2 - 3i$$

$$Re[z] = 2, \;\; Im[z] = -3$$

$$z^* = 2 + 3i, |z| = \sqrt{4 + 9} = \sqrt{13}$$

## Basic definition

$$z = \underbrace{r}_{modulus} \cdot e^{i \overbrace{\varphi}^{argument}}$$

$$Re[z] = r \cdot cos\varphi, \;\; Im[z] = r \cdot sin\varphi$$

$$z^* = r \cdot e^{-i\varphi}$$

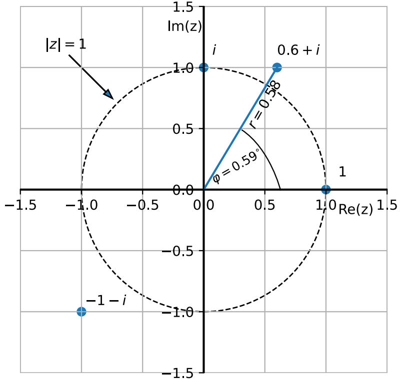
## Basic operations

Multiplication

$$z_1 \cdot z_2 = r_1 \cdot r_2 \cdot e^{i(\varphi_1+\varphi_2)}$$

Modulus

$$|z| = r$$



# Math reminder - Complex matrices

## Basic definitions

$$a, b, c, d \in \mathbb{C}, M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$M^T = \begin{bmatrix} a & c \\ b & d \end{bmatrix}, M^* = \begin{bmatrix} a^* & b^* \\ c^* & d^* \end{bmatrix},$$

$$M^\dagger = (M^T)^* = (M^*)^T = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix},$$

$$(M_1 \cdot M_2)_{ij} = \sum_k (M_1)_{ik} \cdot (M_1)_{kj}$$

In general

$$M_1 \cdot M_2 \neq M_2 \cdot M_1$$

$$[M_1, M_2] = M_1 \cdot M_2 - M_2 \cdot M_1$$

## Hermitian matrix

- $H = H^\dagger$
- Generalization of symmetric matrices
- All eigenvalues real

## Unitary matrix

- $U \cdot U^\dagger = \mathbb{I}$
- $U^{-1} = U^\dagger$
- Generalization of orthogonal matrices
- $|det(U)| = 1, \; det(U) = e^{i\varphi}$

# Postulates of quantum mechanics: Postulate I

## Postulate I

In quantum mechanics the state of a physical system is represented by a vector in a Hilbert space $\mathcal{H}$: a complex vector space with an inner product.

(This course - only finite dimensional Hilbert spaces)

## Dirac notation

Vector: 'ket' $|\psi\rangle$ Dual vector: 'bra' $\langle\varphi|$
Customarily, for $d = dim(\mathcal{H})$:

$$|0\rangle = \left.\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}\right\} d,\ |1\rangle = \begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix}, \ldots, |d-1\rangle = \begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix}$$

$\langle 0| = [1\ 0\ \ldots\ 0]$, $\langle\psi| = (|\psi\rangle)^\dagger$

### Hilbert space

A Hilbert space $\mathcal{H}$ is a complex inner product space.

- Linear combination (superposition):

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle, \; |\varphi\rangle = \sum_{i=0}^{d-1} \beta_i |i\rangle,$$

- Inner product (bra-ket):

$$\langle i|j\rangle = \delta_{ij}$$

$$\langle \psi|\varphi\rangle = \sum_{ij} \alpha_i^* \beta_j \langle i|j\rangle = \sum_i \alpha_i^* \beta_i$$

- Assumption of normalization:

$$||\psi||^2 = \langle \psi|\psi\rangle = 1$$

### State examples

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d-1} \end{bmatrix}$$

$$|\varphi_1\rangle = \frac{1}{\sqrt{30}} \left(|0\rangle + 2i|1\rangle + 3|2\rangle + 4i|3\rangle\right)$$

$$|\varphi_2\rangle = \frac{1}{2} \left((1+i)|0\rangle + i|1\rangle + |2\rangle\right)$$

$$|\varphi_1\rangle = \tfrac{1}{\sqrt{30}} \begin{bmatrix} 1 \\ 2i \\ 3 \\ 4i \end{bmatrix}, \; |\varphi_2\rangle = \tfrac{1}{2} \begin{bmatrix} 1+i \\ i \\ 1 \\ 0 \end{bmatrix}$$

$$\langle \varphi_1|\varphi_2\rangle = \frac{1}{2\sqrt{30}} \left((1-i) + 2 + 3 + 0\right) = \frac{6-i}{2\sqrt{30}}$$

# Postulate I - State examples

**‘Matrix’ multiplication**

$$\langle \varphi_1 | \varphi_2 \rangle = (|\varphi_1\rangle)^\dagger |\varphi_2\rangle =$$

$$= \frac{1}{\sqrt{30}}[1, -2i, 3, -4i] \cdot \frac{1}{2}\begin{bmatrix} 1+i \\ i \\ 1 \\ 0 \end{bmatrix} = \frac{6+i}{2\sqrt{30}}$$

**Exercise 1**

1. Find $N$, such that the state

$$|\varphi\rangle = \frac{1}{N}(|0\rangle + 5i|1\rangle)$$

is normalized, $||\varphi||^2 = \langle \varphi | \varphi \rangle = 1$.

2. Is $N$ unique?

**Exercise 1 part 1**

1. Find $N$, such that the state

$$|\varphi\rangle = \frac{1}{N}\left(|0\rangle + 5i|1\rangle\right)$$

is normalized, $||\varphi||^2 = \langle\varphi|\varphi\rangle = 1$.
**Answers:** $a)\sqrt{26}$, $b)17i$, $c)6$, $d)36$

$$\langle\varphi|\varphi\rangle = \frac{1}{N^*}(\langle 0| - 5i\langle 1|)\cdot\frac{1}{N}(|0\rangle + 5i|1\rangle) = \frac{26}{|N|^2} = 1 \Rightarrow |N| = \sqrt{26}$$

**Exercise 1 part 2**

2. Is $N$ unique?
**Answers:** $a)$ *Yes*, $b)$ *No*

No, we only know the modulus of $N$, but the phase is arbitrary, $N = \sqrt{26}e^{i\alpha}$.
Customarily, we choose $N$ real, $N = \sqrt{26}$.

## Qubit

Two state system:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

From normalization condition $|\alpha|^2+|\beta|^2 = 1$
Examples:

$$|0\rangle, \ \alpha = 1, \beta = 0$$

$$|1\rangle, \ \alpha = 0, \beta = 1$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

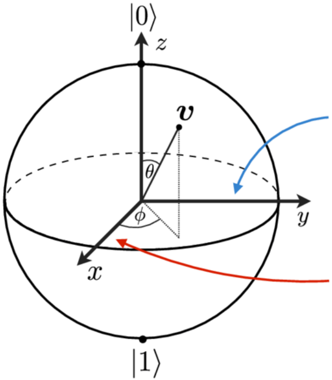
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|i+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$

$$|i-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

**State on the Bloch sphere**

$$|\psi\rangle = cos(\theta/2)|0\rangle + e^{i\varphi} sin(\theta/2)|1\rangle$$




**Pole states:**

$$|i+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$
$$|i-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

**Tensor product**

Hilbert space of a composite system is the tensor product of the Hilbert spaces for the subsystems.

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2, \; dim(\mathcal{H}) = \dim(\mathcal{H}_1) \cdot \dim(\mathcal{H}_2)$$

Customarily:

$$|i\rangle \otimes |j\rangle = |i\rangle|j\rangle = |i\,j\rangle$$

For qubits:

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle, |\varphi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

$$|\psi\rangle \otimes |\varphi\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$$

$$|\psi\rangle \otimes |\varphi\rangle = \begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix} \otimes \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix} = \begin{bmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{bmatrix}$$

### Entangled states

States of the form $|\psi\rangle \otimes |\varphi\rangle$ are product states, all others are entangled states.

Consider:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Interpretation:
A product state $|\psi\rangle \otimes |\varphi\rangle$ has the meaning that system $\psi$ has the property $|\psi\rangle$ and system $\varphi$ the property $|\varphi\rangle$. For an entangled state one typically cannot assign definite properties to the individual systems $\psi$ and $\varphi$.

**Exercise 2**

Which of the following states is entangled?

$$|\psi\rangle = |00\rangle - |01\rangle - |10\rangle + |11\rangle, \ |\phi\rangle = |00\rangle + |01\rangle - |10\rangle + |11\rangle$$

a) Both are entangled,
b) Only $|\psi\rangle$,
c) Only $|\phi\rangle$,
d) None.

## Exercise 2

Which of the following states is entangled?

$$|\psi\rangle = |00\rangle - |01\rangle - |10\rangle + |11\rangle, \ |\phi\rangle = |00\rangle + |01\rangle - |10\rangle + |11\rangle$$

a) Both are entangled,
b) Only $|\psi\rangle$,
c) Only $|\phi\rangle$,
d) None.

## Solution

Remember the formula $(a-b)^2 = a^2 - ab - ba + b^2$? Mixed terms are negative, hence $|\psi\rangle = (|0\rangle - |1\rangle) \otimes ((|0\rangle - |1\rangle))$ - not entangled.
We would expect that there will be even negative terms if all basis states are present.
$|\phi\rangle = |00\rangle + |01\rangle - |10\rangle + |11\rangle$ - entangled.
Changing the relative phase leads to different states. Only global phase does not matter!

# Postulates of quantum mechanics: Postulate II

## Postulate IIa

Every measurable physical quantity $\mathcal{A}$ is described by a Hermitian matrix $A$ acting in the state space $\mathcal{H}$.
The result of measuring a physical quantity $\mathcal{A}$ must be one of the eigenvalues of the corresponding matrix $A$.

## Postulate IIb

When the physical quantity $\mathcal{A}$ is measured on a system in a normalized state $|\psi\rangle$, the probability of obtaining an eigenvalue (denoted $a_n$) of the corresponding observable $A$ is given by the amplitude squared of the appropriate state (projection onto corresponding eigenvector).

$$Pr[a_n] = |\langle a_n|\psi\rangle|^2,$$

where $A|a_n\rangle = a_n|a_n\rangle$.

# Postulates of quantum mechanics: Postulate II

$$\text{Mathematical modeling} \xrightarrow{\text{measurement}} \text{Real world}$$

# Postulate II in quantum computation

In quantum computing, we typically work in the computational basis, which consists of the orthonormal states:

$$|\underbrace{0\dots00}_{n}\rangle, |0\dots01\rangle, |0\dots10\rangle, \dots, |1\dots11\rangle$$

for an $n$-qubit system.
A measurement in the computational basis is a projective measurement where the projectors are:

$$P_k = |k\rangle\langle k|, \quad \text{for } k \in \{0\dots00, 0\dots01, \dots, 1\dots11\}$$

Immediately after the measurement, the system collapses (with probability $\langle\psi|P_k|\psi\rangle = |\langle k|\psi\rangle|^2$) into the (normalized) post-measurement state:

$$|\psi_k\rangle = \frac{P_k|\psi\rangle}{\sqrt{\langle\psi|P_k|\psi\rangle}}.$$

**Hermitian matrices as observables**

Hermitian matrices have real eigenvalues. Although we work with complex numbers, the measurement outcome is real, like in classical physics.

**Pauli matrices and the computational basis**

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

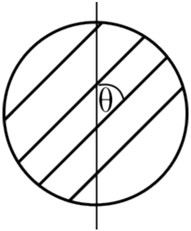
$$Z|0\rangle = 1|0\rangle, \; Z|1\rangle = -1|1\rangle$$

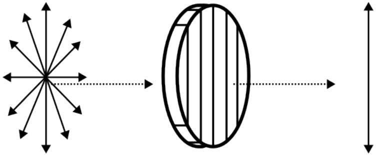
$$X|0\rangle = |1\rangle, \; X|1\rangle = |0\rangle$$

$$X|+\rangle = 1|+\rangle, \; X|-\rangle = -1|-\rangle$$

$$Y|i+\rangle = 1|i+\rangle, \; Y|i-\rangle = -1|i-\rangle$$

# Postulate I+II - Experiment pt. 1



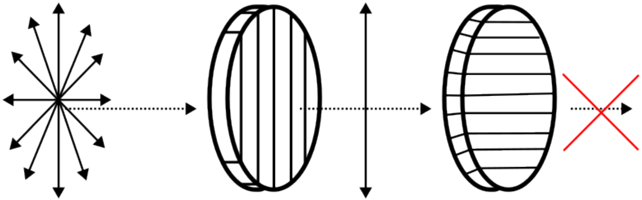



- Two orthogonal polarizations of light, vertical and horizontal, introduce a basis: $|v\rangle, |h\rangle$
- Two dimensional Hilbert space: $\mathcal{H} = span(|v\rangle, |h\rangle)$, $\langle v|h\rangle = 0$
- Any polarization photon state: $|\theta\rangle = cos(\theta)|v\rangle + sin(\theta)|h\rangle$
- The action of the polarizer:
  - ◇ The intensity of light after a polarizer is proportional to the probability that the photon had a correct polarization

$$Pr[v] = |\langle v|\theta\rangle|^2, Pr[h] = |\langle h|\theta\rangle|^2$$

  For unpolarized light (Malus' law 1809)
  - ◇ $Pr[v|unpolarized] = \int |\langle v|\theta\rangle|^2 d\theta = \int cos^2(\theta) d\theta = \frac{1}{2}$

# Postulate I+II - Experiment pt. 2

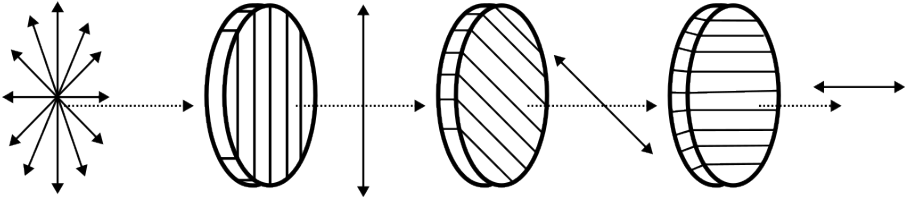


1. Checking the polarization filters: apply two filters orthogonally.
2. After the first polarizer the light is in state $|v\rangle$
3. The second polarizer projects the state on the horizontal orientation eigenvector $|h\rangle$,

$$Pr[h|v] = |\langle h|v\rangle|^2 = 0$$

The light vanishes in this setup.

# Postulate I+II - Experiment pt. 3



1. Insert tilted polarizer ($\theta = 45^\circ$),
$$|45^\circ\rangle = \frac{1}{\sqrt{2}}|v\rangle + \frac{1}{\sqrt{2}}|h\rangle$$
$$+ \quad |-45^\circ\rangle = \frac{1}{\sqrt{2}}|v\rangle - \frac{1}{\sqrt{2}}|h\rangle$$
$$|v\rangle = \frac{1}{\sqrt{2}}|45^\circ\rangle + \frac{1}{\sqrt{2}}|-45^\circ\rangle$$
2. After the first polarizer we have state $|v\rangle$, after the second
$$Pr[45^\circ|v] = |\langle 45^\circ|v\rangle|^2 = |\frac{1}{\sqrt{2}}|^2$$
3. After the final polarizer
$$Pr[h|45^\circ] = |\langle h|45^\circ\rangle|^2 = |\frac{1}{\sqrt{2}}|^2$$
4. The intensity in the whole process
$$Pr[v|unpolarized]Pr[45^\circ|v]Pr[h|45^\circ] = \frac{1}{8}$$

### Postulate III

The time evolution of a closed system is described by a unitary transformation on the initial state.

$$|\psi(t)\rangle = U(t; t_0)|\psi(t_0)\rangle$$

### High-level evolution in QC

In quantum computing, unitary operations will be called gates.
Time evolution is discretized - single time step is the execution of a single (layer) of gate(s).

## Exercise 3

Assume that we have a unitary $U_{cl}$ such that it is able to copy an arbitrary one-qubit state to the second register

$$U_{cl}\left(|\psi\rangle \otimes |0\rangle\right) = |\psi\rangle \otimes |\psi\rangle$$

What is the result of the action of $U_{cl}$ on the state $(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle$?
Answers:
a) $\alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$
b) $\alpha|00\rangle + \beta|11\rangle$

**Solution?**

Both answers seem to be correct...

- First apply $U_{cl}$, then multiply
  $U_{cl}\left((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle\right) = (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$
- First multiply, then apply $U_{cl}$
  $U_{cl}\left((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle\right) = U_{cl}\left(\alpha|00\rangle + \beta|10\rangle\right) = U_{cl}\left(\alpha|00\rangle\right) + U_{cl}\left(\beta|01\rangle\right) = \alpha|00\rangle + \beta|11\rangle$

**Solution?**

Both answers seem to be correct...

- First apply $U_{cl}$, then multiply
  $U_{cl}\left((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle\right) = (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$
- First multiply, then apply $U_{cl}$
  $U_{cl}\left((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle\right) = U_{cl}\left(\alpha|00\rangle + \beta|10\rangle\right) = U_{cl}\left(\alpha|00\rangle\right) + U_{cl}\left(\beta|01\rangle\right) = \alpha|00\rangle + \beta|11\rangle$

**No-cloning theorem**

There is no unitary operator U on $\mathcal{H} \otimes \mathcal{H}$ such that for all normalized states $|\phi\rangle_A$ and $|e\rangle_B$ in $\mathcal{H}$

$$U(|\phi\rangle_A|e\rangle_B) = e^{i\alpha(\phi,e)}|\phi\rangle_A|\phi\rangle_B$$

for some real number $\alpha$ depending on $\phi$ and $e$.

# One-qubit unitary gates

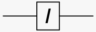
## Matrix representation in a basis

Operation from $|i\rangle$ to $|j\rangle$

$$U_{ji} = |j\rangle\langle i|$$

## Identity gate

| Before | After |
|---|---|
| $\|0\rangle$ | $\|0\rangle$ |
| $\|1\rangle$ | $\|1\rangle$ |




$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| =$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

# One-qubit unitary gates

## Matrix representation in a basis

Operation from $|i\rangle$ to $|j\rangle$

$$U_{ji} = |j\rangle\langle i|$$

## NOT gate

| Before | After |
|---|---|
| $\|0\rangle$ | $\|1\rangle$ |
| $\|1\rangle$ | $\|0\rangle$ |


$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$X = |1\rangle\langle 0| + |0\rangle\langle 1| =$$

$$= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

# One-qubit unitary gates

## Hadamard gate

| Before | After |
|---|---|
| $\|0\rangle$ | $\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ |
| $\|1\rangle$ | $\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$ |


$$H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1| = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- Hermitian and Unitary

$$H \cdot H^{\dagger} = H \cdot H = \mathbb{I}$$

- Changes basis

$$HXH = Z$$

- Hadamard transform

$$H^{\otimes n}(|0\rangle)^{\otimes n} = H \otimes \cdots \otimes H|0 \ldots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$$

### Matrix representation in a basis

Operation from $|i\rangle$ to $|j\rangle$

$$U_{ji} = |j\rangle\langle i|$$

### Phase gate - Exercise 4

| Before | After |
|---|---|
| $\|0\rangle$ | $\|0\rangle$ |
| $\|1\rangle$ | $i\|1\rangle$ |


What is the matrix representation of $S$?

$$a) \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, b) \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, c) \begin{bmatrix} 2 & 0 \\ 2 & 0 \end{bmatrix}, d) \begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix}$$

# One-qubit unitary gates

## Matrix representation in a basis

Operation from $|i\rangle$ to $|j\rangle$

$$U_{ji} = |j\rangle\langle i|$$

## Phase gate - Exercise

| Before | After |
|---|---|
| $\|0\rangle$ | $\|0\rangle$ |
| $\|1\rangle$ | $i\|1\rangle$ |


What is the matrix representation of $S$?

$$b) \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

# Parameterized gates

**Gates as an exponentiation of gates**

We (theoretically) can perform arbitrary continuously parameterized gates

$$R_X(\theta) = e^{-iX\frac{\theta}{2}}$$

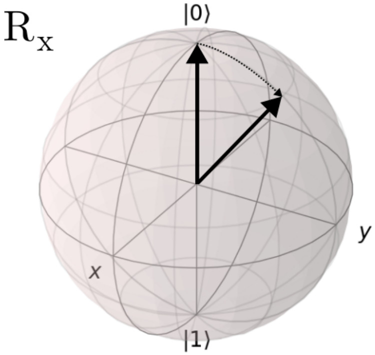
$$R_X(\theta) = \begin{bmatrix} cos(\theta/2) & -i\ sin(\theta/2) \\ -i\ sin(\theta/2) & cos(\theta/2) \end{bmatrix}$$

$$R_Y(\theta) = e^{-iY\frac{\theta}{2}}$$

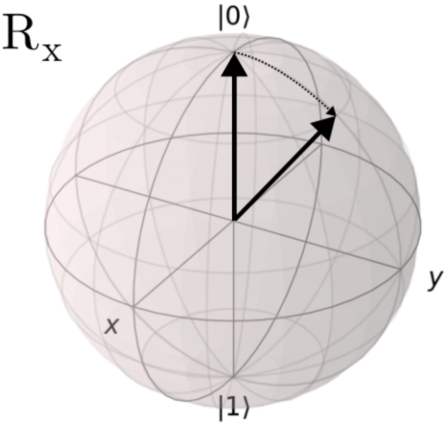
$$R_Y(\theta) = \begin{bmatrix} cos(\theta/2) & -sin(\theta/2) \\ sin(\theta/2) & cos(\theta/2) \end{bmatrix}$$

$$R_Z(\theta) = e^{-iZ\frac{\theta}{2}}$$

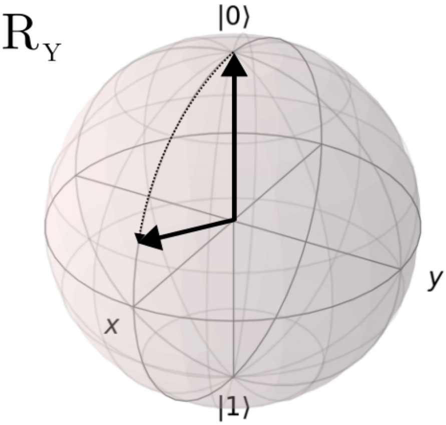
$$R_Z(\theta) = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$



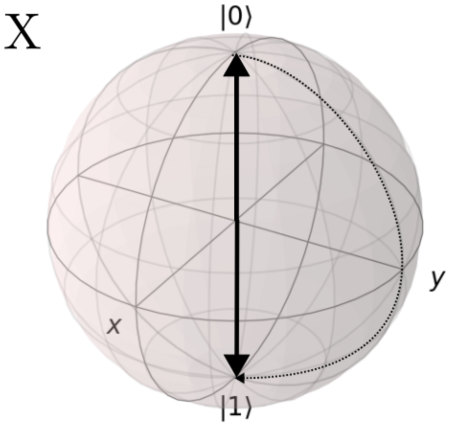
## Quantum computing as unitary rotations



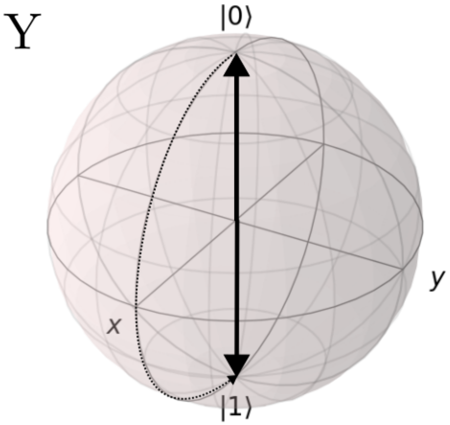
# Quantum computing as unitary rotations

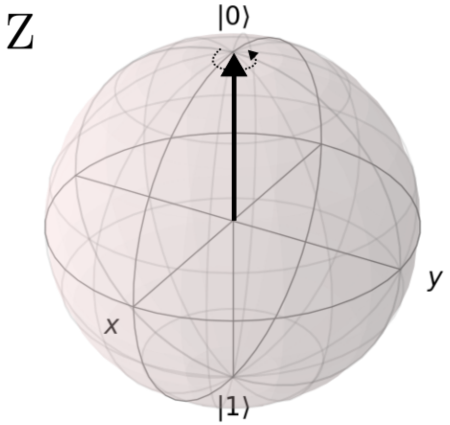


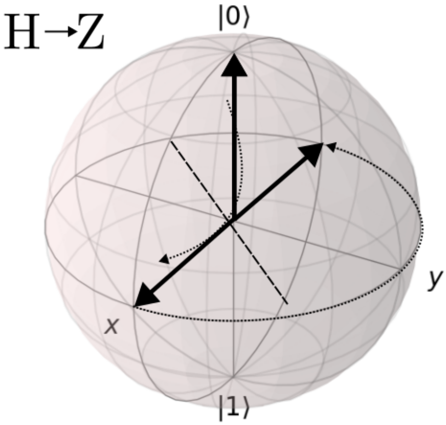
# Quantum computing as unitary rotations



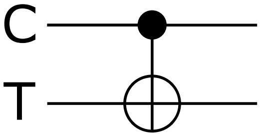
# Quantum computing as unitary rotations




Z
|0⟩
x
y
|1⟩


H→Z
|0⟩
x
y
|1⟩

# Controlled NOT gate




### CNOT truth table

| Before | | After | |
|---|---|---|---|
| C | T | C | T |
| $\|0\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|0\rangle$ |
| $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ |
| $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|1\rangle$ |
| $\|1\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ |

### Matrix representation

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

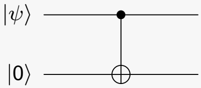
$$CNOT = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| =$$

$$= \begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}$$

# CNOT gate - action on an arbitrary quantum state

## Arbitrary state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$




$$CNOT\,[(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle] =$$

$$= CNOT(\alpha|00\rangle + \beta|10\rangle) =$$

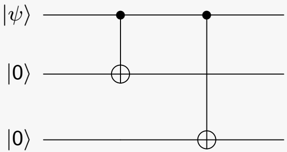
$$= \alpha|00\rangle + \beta|11\rangle$$

For $\alpha = \frac{1}{\sqrt{2}}, \beta = \frac{1}{\sqrt{2}}$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

## Even more qubits

$$|\psi\rangle \otimes |0\rangle \otimes |0\rangle$$

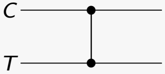



$$\alpha|000\rangle + \beta|111\rangle$$

Error correction - repetition codes

# Controlled Z gate

### diagram




### CNOT truth table

| Before | | After | |
|---|---|---|---|
| C | T | C | T |
| $\|0\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|0\rangle$ |
| $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ |
| $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ |
| $\|1\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $-\|1\rangle$ |

### Matrix representation

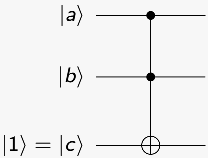
$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

$$CZ = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 11| - |11\rangle\langle 11| =$$

$$= \begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 1 & 0\\0 & 0 & 0 & -1\end{bmatrix}$$

# Quantum simulation of Classical Logic

## Toffoli gate and ancilla

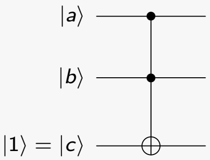



## Truth table

| Before | | | After | | |
|---|---|---|---|---|---|
| $\|a\rangle$ | $\|b\rangle$ | $\|c\rangle$ | $\|a\rangle$ | $\|b\rangle$ | $\|c\rangle$ |
| $\|0\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|1\rangle$ |
| $\|0\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|1\rangle$ |
| $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|1\rangle$ |
| $\|1\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|1\rangle$ | $\|0\rangle$ |

# Quantum simulation of Classical Logic

## Toffoli gate and ancilla




## Truth table

| Before | | | After |
|---|---|---|---|
| $\|a\rangle$ | $\|b\rangle$ | [redacted] | $\|c\rangle$ |
| $\|0\rangle$ | $\|0\rangle$ | [redacted] | $\|1\rangle$ |
| $\|0\rangle$ | $\|1\rangle$ | [redacted] | $\|1\rangle$ |
| $\|1\rangle$ | $\|0\rangle$ | [redacted] | $\|1\rangle$ |
| $\|1\rangle$ | $\|1\rangle$ | [redacted] | $\|0\rangle$ |

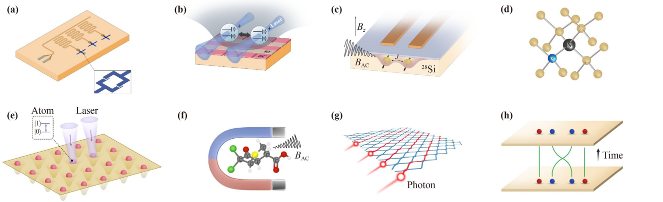
## Universality argument $Q \to C$

- Quantum computations are inherently reversible.
- The classical NAND gate is irreversible but universal for classical computation.
- To simulate NAND, we introduce additional qubit(s) called *ancilla*.
- We apply a reversible quantum circuit (e.g., the Toffoli gate) to perform the computation.
- The overall quantum operation is reversible.
- By discarding (ignoring) some qubits, we obtain an effective irreversible operation on a subsystem.
- This allows us to simulate a NAND gate within a reversible quantum system.
- Since NAND is universal, quantum computers can simulate any classical computation.

# Summary - Theoretical part

- Quantum computation is described using the formalism of quantum mechanics: states are vectors in a Hilbert space and transformations are unitary operators.
- The outcome of a quantum computation is obtained by measurement; intermediate quantum states are not directly observable.
- Measurement collapses a quantum state probabilistically according to the Born rule, giving classical outcomes based on the quantum amplitudes.
- Quantum systems evolve in exponentially large Hilbert spaces due to the tensor product structure of qubits, enabling potentially more expressive computation.
- Quantum computations proceed via unitary transformations (quantum gates) applied to qubits.
- Unitarity of quantum gates implies that all quantum computations are inherently reversible.
- Any classical (irreversible) computation can be implemented reversibly on a quantum computer by using additional ancilla qubits and reversible gate constructions.

# Quantum technologies




**(a) Superconducting quantum processor:**
An array of artificial atoms made of Josephson junctions and capacitors, fabricated with lithography, controlled with microwave electronics
**Number of qubits with individual control:**
~100
**Gate fidelities:**
Systems with 53 qubits: $F_1 > 99\%$; $F_2 > 99\%$
**Pros:**
Fast gate speed, tailored qubits, high controllability and scalability
**Cons:**
Crosstalk between qubits, low temperature, supporting technology for scaling up

**(b) Trapped ion quantum computing:**
Laser-cooled atomic ions held by radio-frequency electric fields in ultra-high vacuum environment
**Number of qubits with individual control:**
20−30
**Gate fidelities:**
Systems with dozens of ions
$F_1 > 99.9\%$; $F_2 > 99\%$
**Pros:**
Extremely long coherence time and excellent gate operations on few ions;
Reconfigurable connectivity between ion qubits
**Cons:**
Technically challenging in integration

**(c) Semiconductor spin-based quantum computing:**
Electron or hole spins in semiconductor (silicon) quantum dot
**Number of qubits with individual control:** 6
**Gate fidelities:**
Donor spin qubit: $F_1 \sim 99.99\%$; $F_2 \sim 99.5\%$
Gate-defined qubit: $F_1 \sim 99.9\%$; $F_2 \sim 99.51\%$
**Pros:**
Semiconductor fabrication
Long coherence and fast high-fidelity gate
Work at temperature > 1 K
Small footprint
**Cons:**
Challenge of nanoscale fabrication

**(d) NV center quantum computing:**
Point defects in diamond; electron and nuclear spins with long coherence time; atom-like properties and solid-state host environment
**Number of qubits with individual control:**
10 (one electron + nine $^{13}$C nuclear spins)
**Gate fidelities:**
$F_1 \sim 99.995\%$; $F_2 \sim 99.2\%$
**Pros:**
Work at room temperature
Excellent quantum sensor
Handy in quantum network
**Cons:**
Hard to scale up

**(e) Neutral atom array quantum computing:**
Neutral atom arrays trapped in optical tweezers with controlled interactions based on the Rydberg interactions
**Number of qubits in digital quantum processors:** 24
**Number of qubits in analog quantum simulators:** 289
**Pros:**
Both digital and analog quantum simulations
Scaling up beyond 100 qubits in programmable geometries
**Cons:**
Improving fidelities of two-qubit gates

**(f) NMR quantum computing:**
Nuclear spins in molecule
**Number of qubits with individual control:**
12
**Gate fidelities:**
$F_1 \sim 99.98\%$; $F_2 \sim 99.3\%$
**Pros:**
Work at room temperature
Long coherence time
Digital quantum simulator
**Cons:**
Hard to scale up

**(g) Photonic quantum computing:**
Coherently manipulating a large number of single photons or canonically conjugate pair of variables for electromagnetic modes to process quantum information
**Number of qubits with individual control:**
18
**Number of photons with coherent control**:
255 (Jiuzhang 3.0 (to be published))
**Gate fidelities:**
$F_1 \sim 99.84\%$; $F_2 \sim 99.69\%$
**Pros:** robust against decoherence, working at room temperature, compatible with CMOS fabrications, natural interface for distributed quantum computing
**Cons:** Big challenge to realize deterministic photon-photon gate

**(h) Topological quantum computing:**
Fault-tolerant quantum computation based on non-abelian braiding of anyons
**Number of qubits with individual control:**
N/A
**Gate fidelities:**
N/A
**Pros:**
Intrinsic topological protection
Few physical qubits to construct a logic qubit
Promising to achieve large-scale, error-corrected computation
**Cons:**
The ideal materials or systems not found yet.
Zero topological qubit so far

# Technical details of different technologies

| Parameters | SC | T.ions | Photonic | N.atoms | S.spin | NV | CPUs |
|---|---|---|---|---|---|---|---|
| Clock cycle | 1MHz | 1KHz | 10Hz | 1MHz | 0.76MHz | 1MHz | 3GHz |
| Measurement | $660ns$ | $300\mu s$ | x | $200ms$ | $1.3\mu s$ | x | x |
| 2-qubit gate | $34ns$ | $200\mu s$ | x | $< 100\mu s$ | x | $700ns$ | x |
| 1-qubit gate | $25ns$ | $15\mu s$ | x | x | x | $9ns$ | x |
| Readout fidelity | 99.4% | 97.3% | 50.0% | 99.1% | 99% | 98% | x |
| 1Q fidelity | 99.99% | 99.99% | 99.84% | 99.83% | 99.99% | 99.99% | x |
| 2Q fidelity | 99.97% | 99.9% | 99.69% | 99.4% | 99.5% | 99.2% | x |

# Adiabatic quantum computing

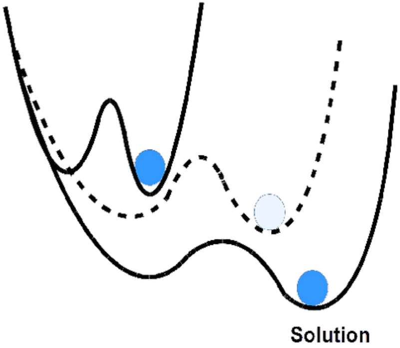
**Adiabatic theorem**

A physical system remains in its instantaneous eigenstate if a given perturbation is acting on it slowly enough and if there is a gap between the eigenvalue and the rest of the Hamiltonian's spectrum.

$$H(t) = \left(1 - \frac{t}{T}\right) H_0 + \frac{t}{T} H_1,\ T = \mathcal{O}\left(\frac{1}{\Delta^2_{min}}\right)$$

$$H(t) = -\sum_{i,j} J_{ij}\sigma_i\sigma_j - \mu\sum_i h_i\sigma_i,\ \sigma_i = \{-1, 1\}$$

Easy implementation for Quadratic unconstrained binary optimization (QUBO) problems.




Adiabatic evolution

# How to access quantum computing devices?

aws

JÜLICH Forschungszentrum

IBM

CESGA GALICIA SUPERCOMPUTING CENTER

Google AI Quantum

D-Wave The Quantum Computing Company™

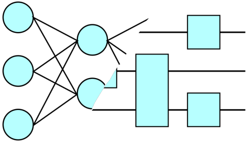
Azure

# Quantum Algorithms

**Artur Miroszewski**

Quantum Cosmos Lab, Jagiellonian University

High Performance and Disruptive Computing in Remote Sensing School 2025



Jagiellonian University in Kraków

Quantum Cosmos Lab

# Quantum algorithms

## NISQ

- Variational Quantum Eigensolver
- Quantum Approximate Optimization Algorithm
- Quantum Machine Learning
- Quantum Simulation
- Quantum Sampling

...

## Fault-tolerant

- Shor's Algorithm
- Grover's Algorithm
- Quantum Phase Estimation
- Deutsch-Jozsa Algorithm
- Quantum Simulation
- Harrow-Hassidim-Lloyd Algorithm

...

# Algorithms zoo

**Quantum algorithms**

**NISQ**

- Variational Quantum Eigensolver
- Quantum Approximate Optimization Algorithm
- Quantum Machine Learning
- Quantum Simulation
- Quantum Sampling

...

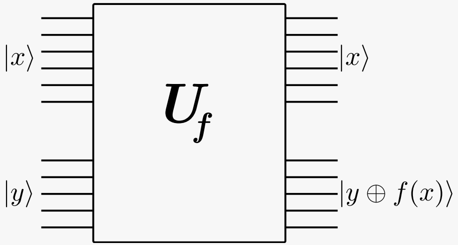
**Fault-tolerant**

- Shor's Algorithm
- Grover's Algorithm
- Quantum Phase Estimation
- Deutsch-Jozsa Algorithm
- Quantum Simulation
- Harrow-Hassidim-Lloyd Algorithm

...

# The Deutsch-Jozsa Algorithm

## Query gates




## The problem statement

Given a function a boolean function $f : \{0,1\}^n \mapsto \{0,1\}$ determine whether it is constant or balanced.

## Balanced functions

A function $f : \{0,1\}^n \mapsto \{0,1\}$ is:

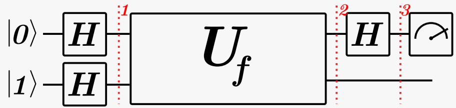
- Balanced
  when exactly half of it outputs is 0 and half is 1,
- Constant
  when all the outputs are either 0 or 1

## Solutions

- Classical
  Worst-case: $2^{n-1} + 1$ querries
- Quantum Single query!

Four possible functions $f:\{0,1\}\mapsto\{0,1\}$:

- $f_1(0)=0, f_1(1)=0$
- $f_2(0)=0, f_1(1)=1$
- $f_3(0)=1, f_1(1)=0$
- $f_4(0)=1, f_1(1)=1$




$$\begin{cases} 0, & f \text{ is constant} \\ 1, & f \text{ is balanced} \end{cases}$$

## Analysis

1

$\frac{1}{2}\left(|0\rangle+|1\rangle\right)\left(|0\rangle-|1\rangle\right)$

2

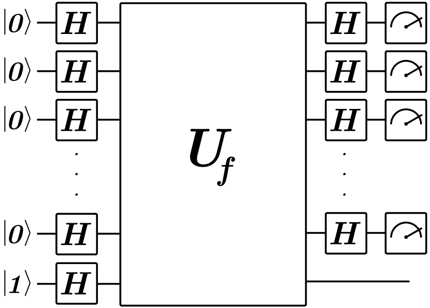
$\frac{1}{2}\left(|0\rangle|0\oplus f(0)\rangle-|0\rangle|1\oplus f(0)\rangle+|1\rangle|0\oplus f(1)\rangle-|1\rangle|1\oplus f(0)\rangle\right)=$

$\frac{1}{\sqrt{2}}\left(|0\rangle+(-1)^{f(0)\oplus f(1)}|1\rangle\right)\otimes\frac{(-1)^{f(0)}}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$

3 (ignoring the second qubit)

$\frac{1}{2}\left(\left(1+(-1)^{f(0)\oplus f(1)}\right)|0\rangle+\left(1-(-1)^{f(0)\oplus f(1)}\right)|1\rangle\right)$

# The Deutsch-Jozsa Algorithm



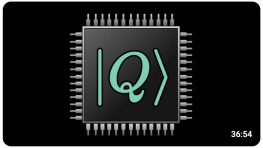

- Extend the same circuit to bigger input ($2^n$ states)
- The probability $\Pr[|00 \ldots 0\rangle]$

$$\left| \frac{1}{2^n} \sum_{x_{n-1} \cdots x_0 \in \Sigma^n} (-1)^{f(x_{n-1} \cdots x_0)} \right|^2 = \begin{cases} 1 & \text{if } f \text{ is constant} \\ 0 & \text{if } f \text{ is balanced} \end{cases}$$

# The Deutsch-Jozsa Algorithm - summary

- Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, promised to be either constant or balanced, the Deutsch-Jozsa Algorithm determine which one it is.
- Distinguishing constant vs. balanced functions in not widely useful. Especially with the promise that the function $f$ has to belong to one of the classes.
- Need to construct $U_f$ query gate - efficient if we have 'blueprint' of $f$
- Exponential speedup: quantum - $\mathcal{O}(1)$, classical - $\mathcal{O}(2^n)$.
- However, classical probabilistic - in $k$ querries with probability $p = 1 - 2^{-k+1}$
- Quantum parallelism - 'compute' the function on all inputs
- Extremely rare case, of being able to use parallelism - problem structure $\to$ constructive/destructive interference

# The Grover Algorithm




But what is quantum computing? (Grover's Algorithm)
3Blue1Brown

## Unstructured search

A function

$$f : \{0,1\}^n \mapsto \{0,1\}$$

Strings $x \in \{0,1\}^n$ for which $f(x) = 1$ are called solutions.
The problem of finding solutions is called *unstructured search*.

Classical solution: worst case - $\mathcal{O}(2^n)$
Grover algorithm: $\mathcal{O}(\sqrt{2^n})$ - quadratic speedup

## Grover algorithm

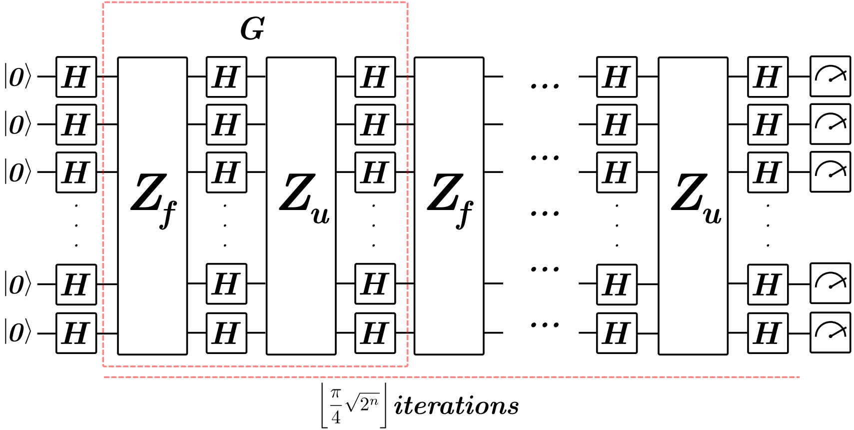
Creation of the uniform superposition and iterative application of two operations:

$$Z_f$$

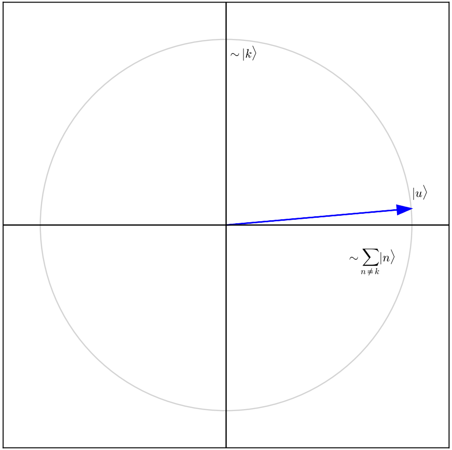
Reflection around the uniform superposition of states which are not solutions.
$|k\rangle$ - solution, reflection around $\sim \sum_{n \neq k} |n\rangle$.

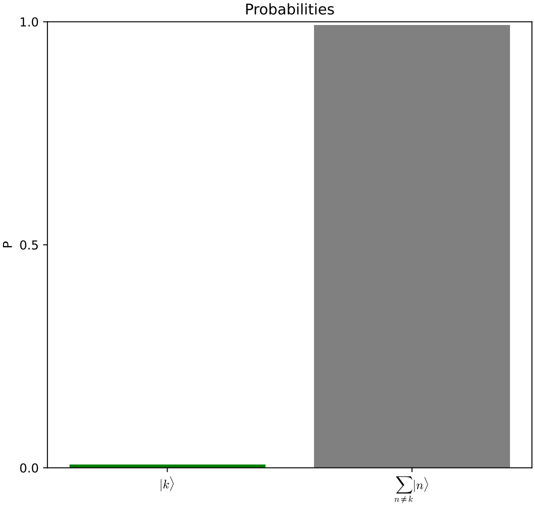
$$H^{\otimes n} Z_u H^{\otimes n}$$

Reflection around the uniform superposition of all states, $|u\rangle = \frac{1}{\sqrt{2^n}} \sum_n |n\rangle$.

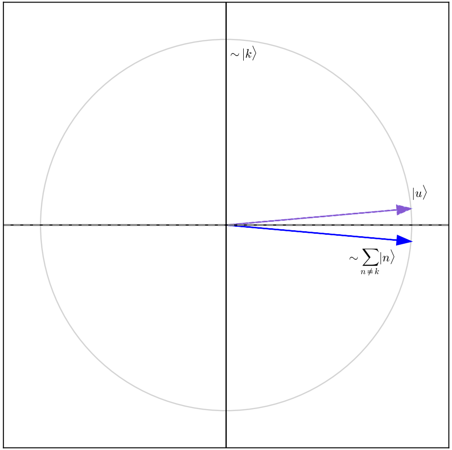

G
|0⟩
H
Zf
Zu
...
$\left\lfloor \frac{\pi}{4}\sqrt{2^n} \right\rfloor$ iterations

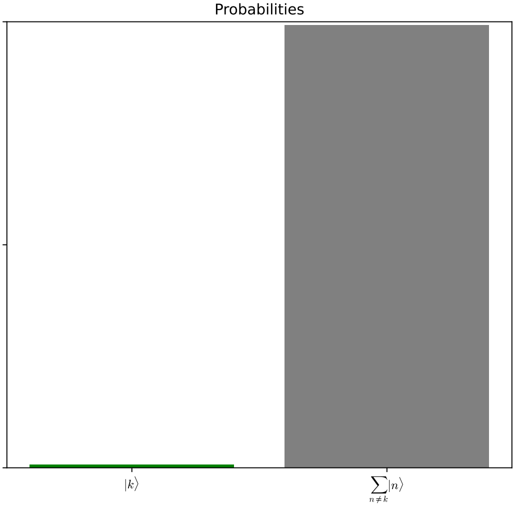
# The Grover Algorithm - geometric picture



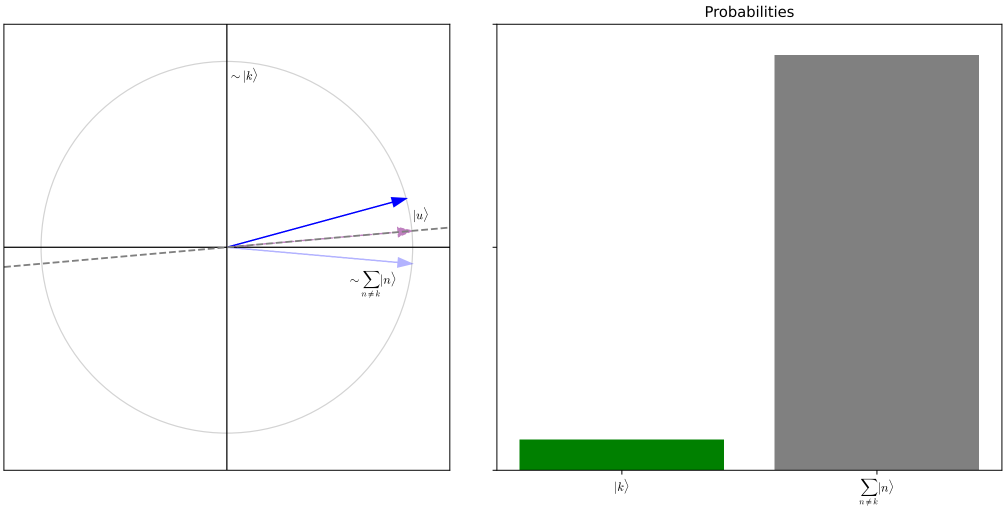



# The Grover Algorithm - geometric picture

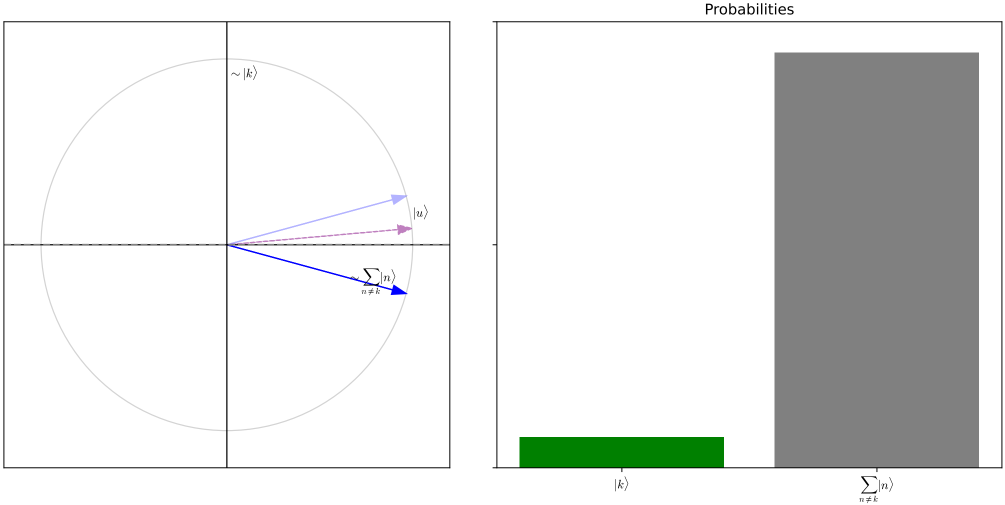


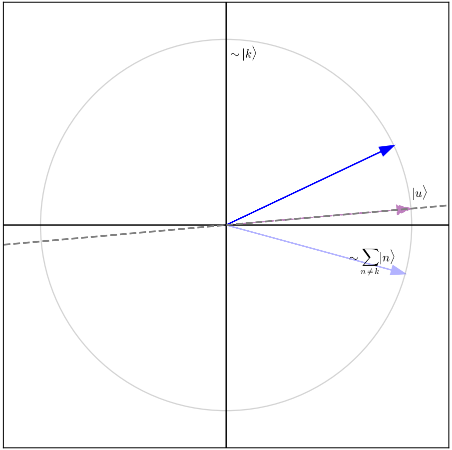



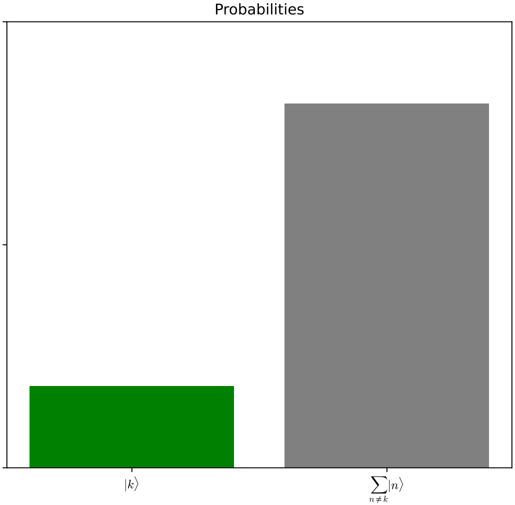
# The Grover Algorithm - geometric picture



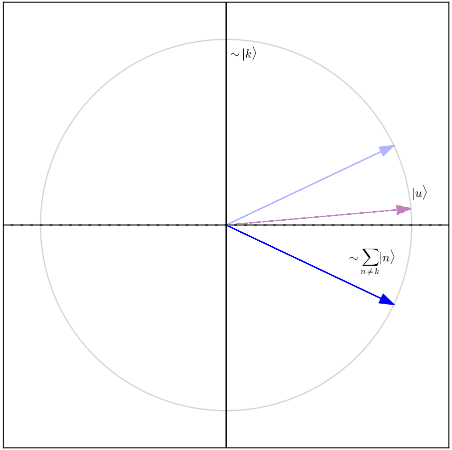
# The Grover Algorithm - geometric picture

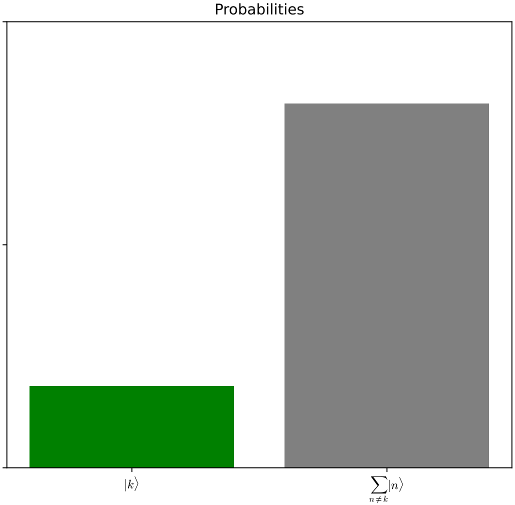


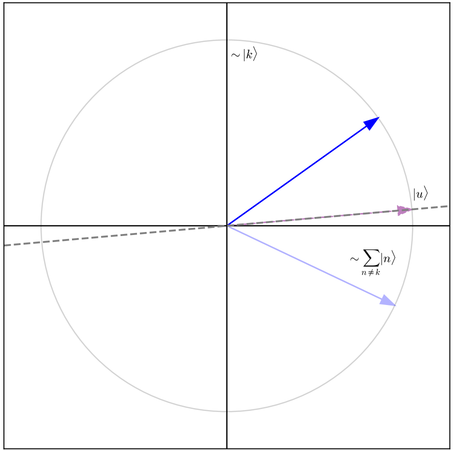

$\sim |k\rangle$
$|u\rangle$
$\sim \sum_{n \neq k} |n\rangle$

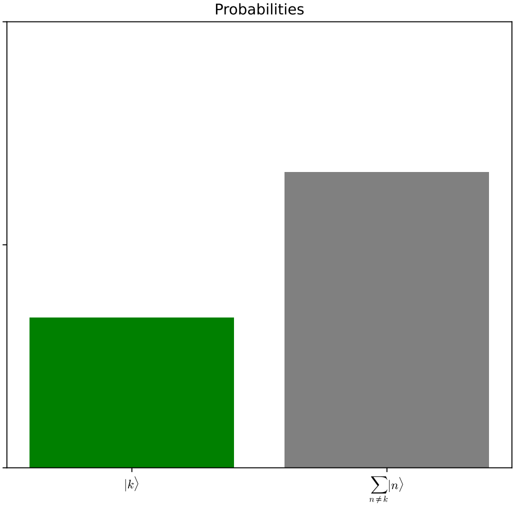

Probabilities
$|k\rangle$
$\sum_{n \neq k} |n\rangle$

# The Grover Algorithm - geometric picture

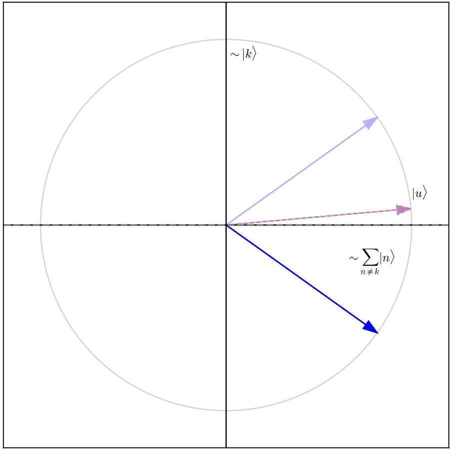


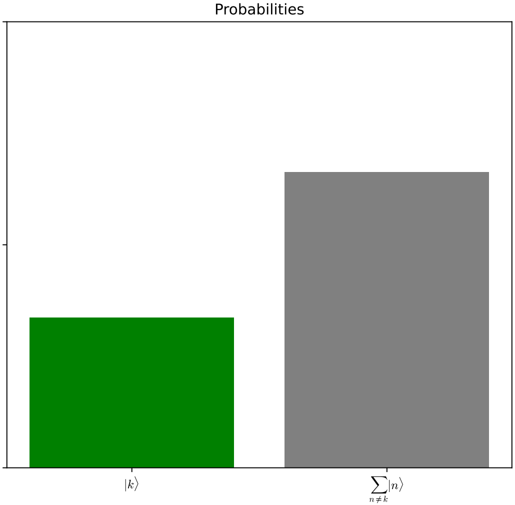



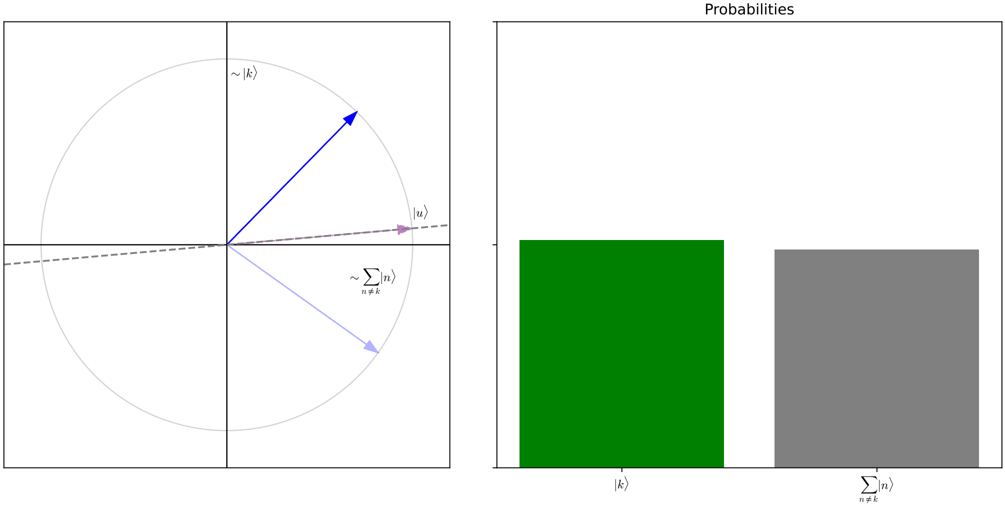

$\sim |k\rangle$
$|u\rangle$
$\sim \sum_{n\neq k} |n\rangle$


Probabilities
$|k\rangle$
$\sum_{n\neq k} |n\rangle$

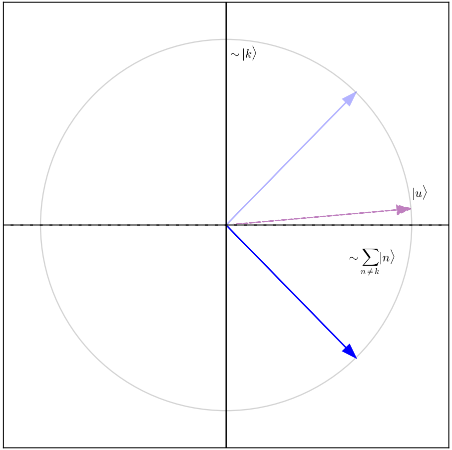
# The Grover Algorithm - geometric picture

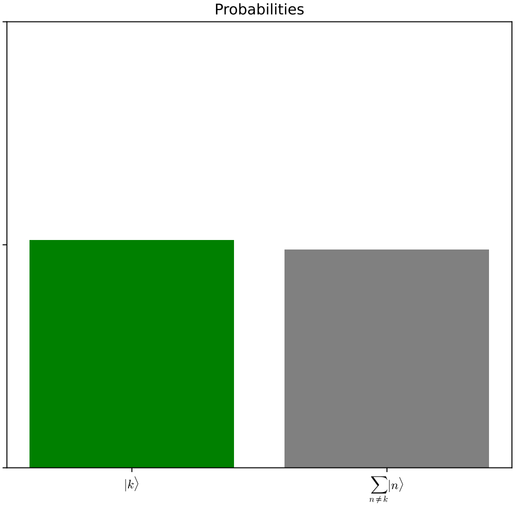


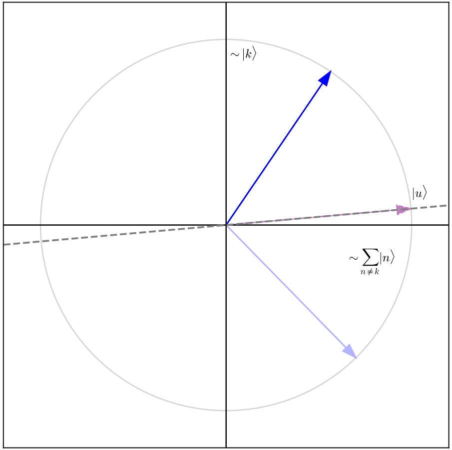

$\sim |k\rangle$
$|u\rangle$
$\sim \sum_{n \neq k} |n\rangle$
Probabilities
$|k\rangle$
$\sum_{n \neq k} |n\rangle$

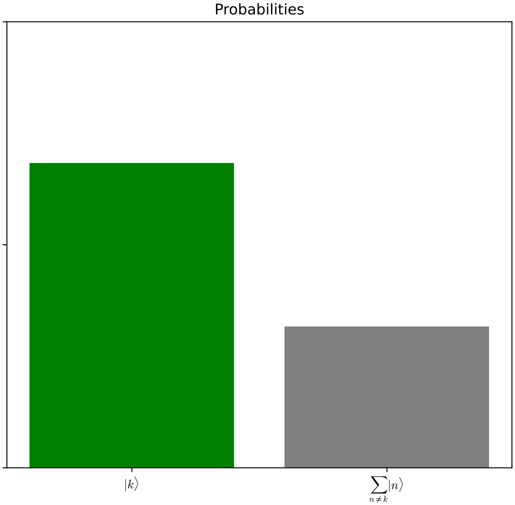
# The Grover Algorithm - geometric picture



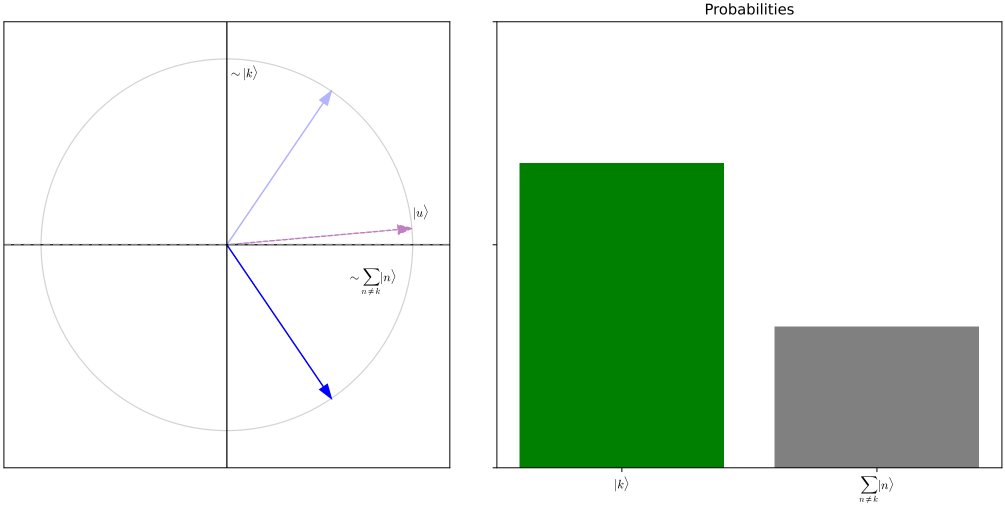



# The Grover Algorithm - geometric picture

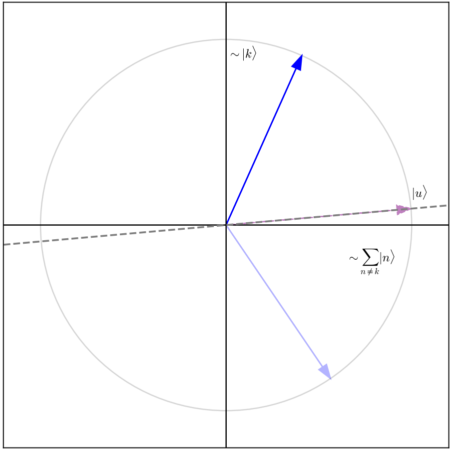


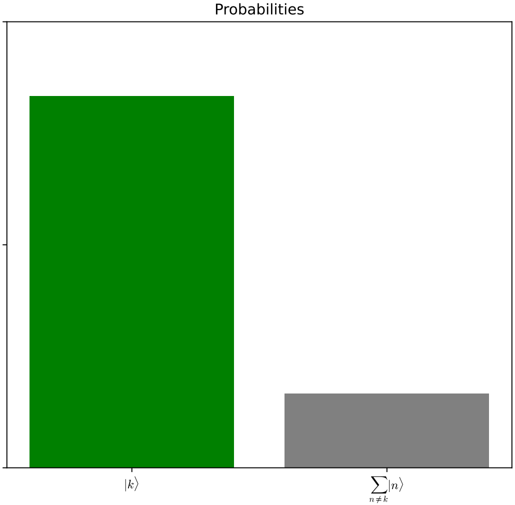



# The Grover Algorithm - geometric picture

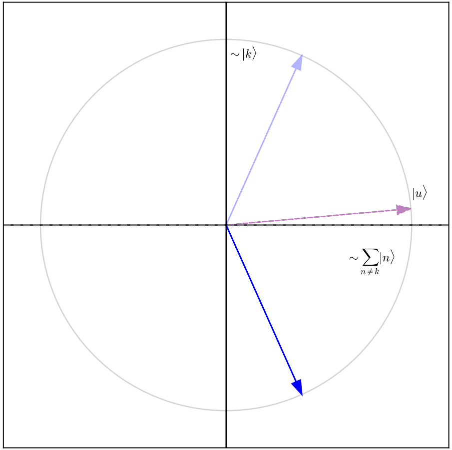


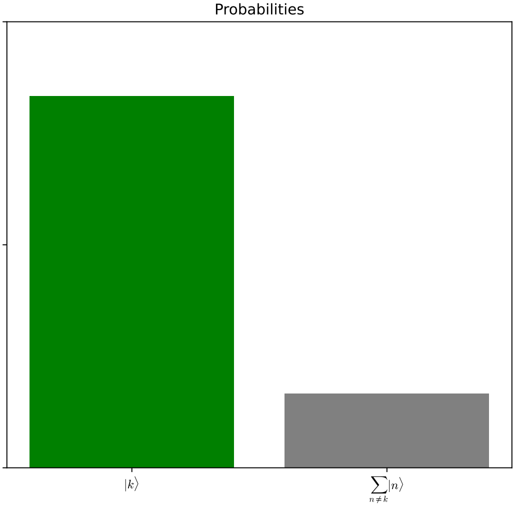
# The Grover Algorithm - geometric picture



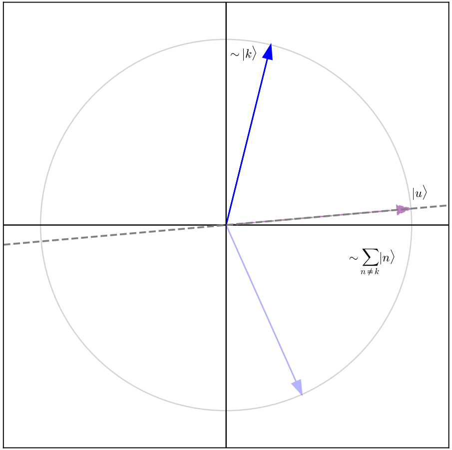



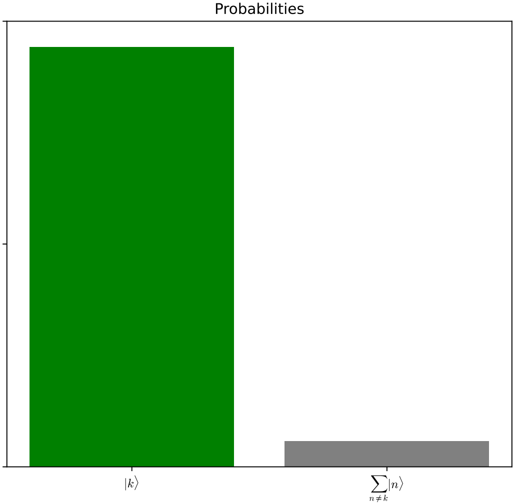
# The Grover Algorithm - geometric picture



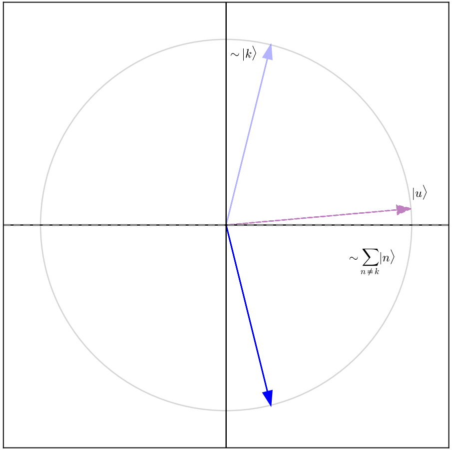



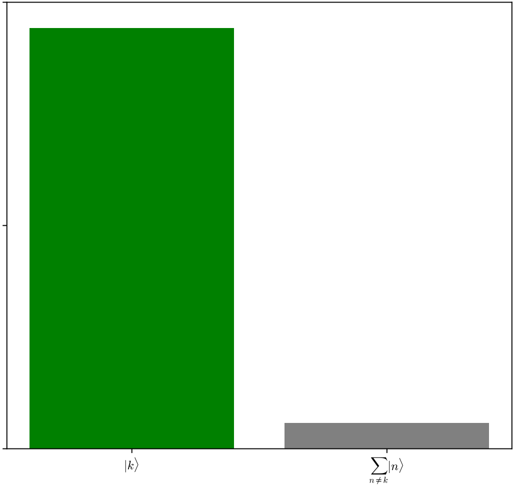
# The Grover Algorithm - geometric picture



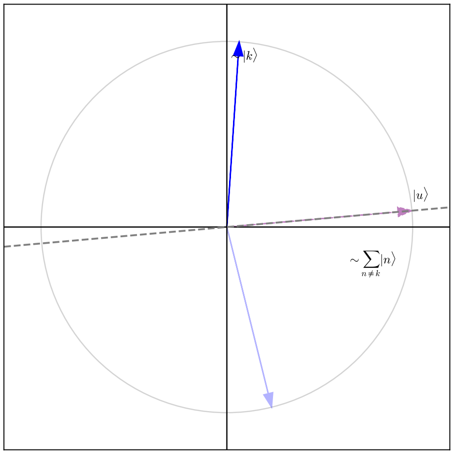



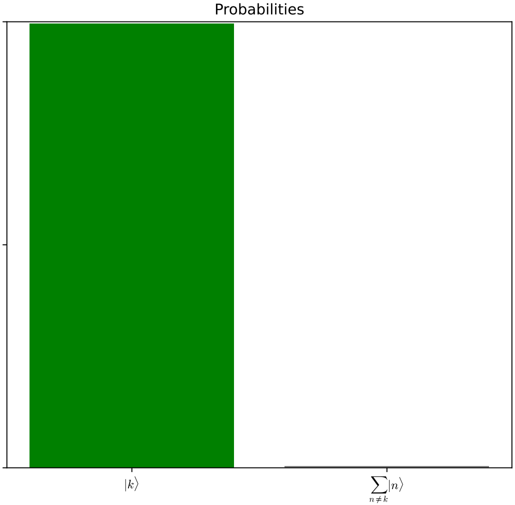
# The Grover Algorithm - geometric picture



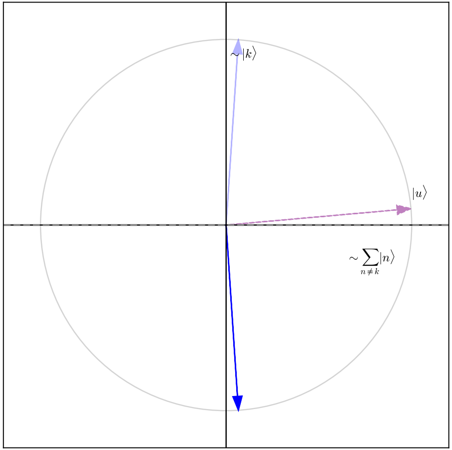



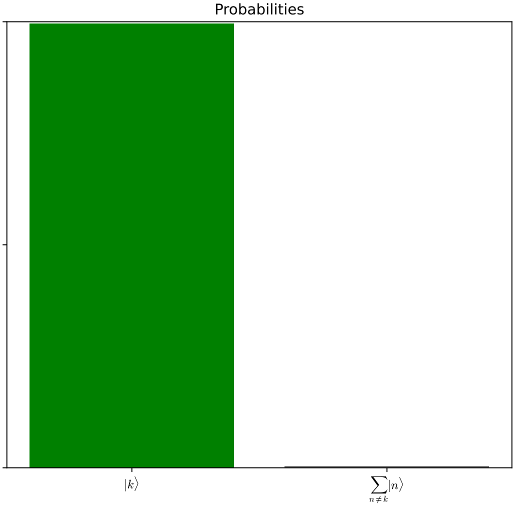
# The Grover Algorithm - geometric picture



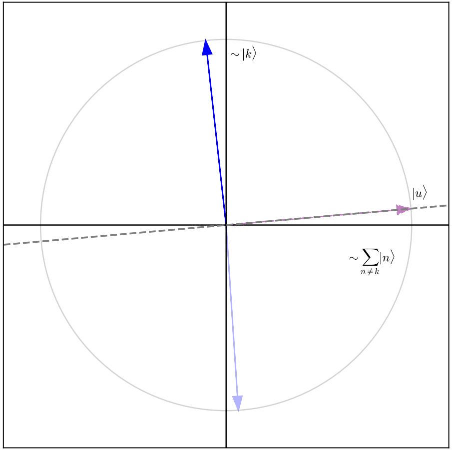



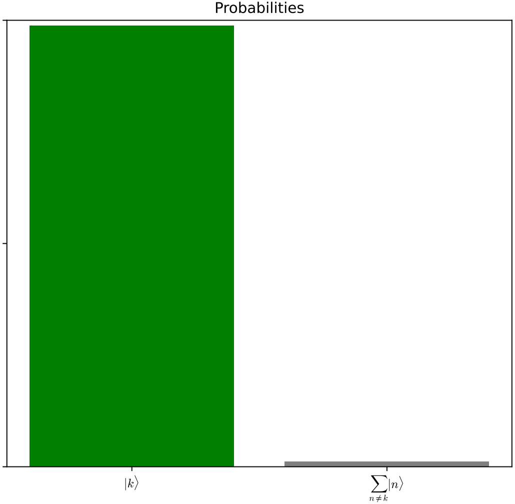
# The Grover Algorithm - geometric picture



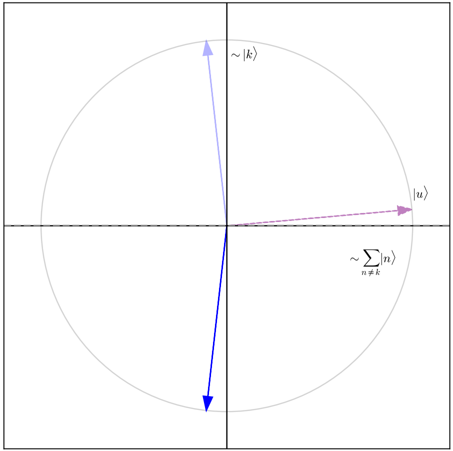



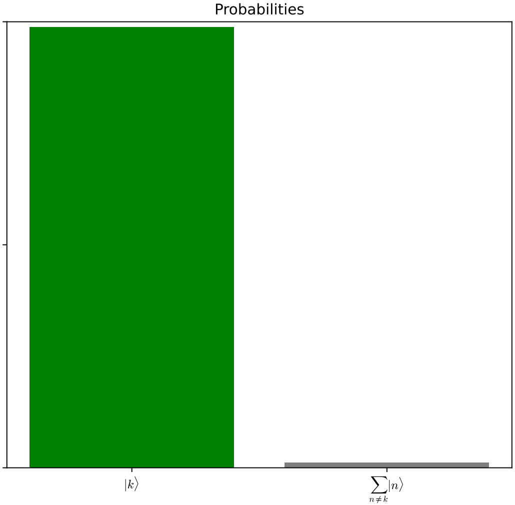
# The Grover Algorithm - geometric picture



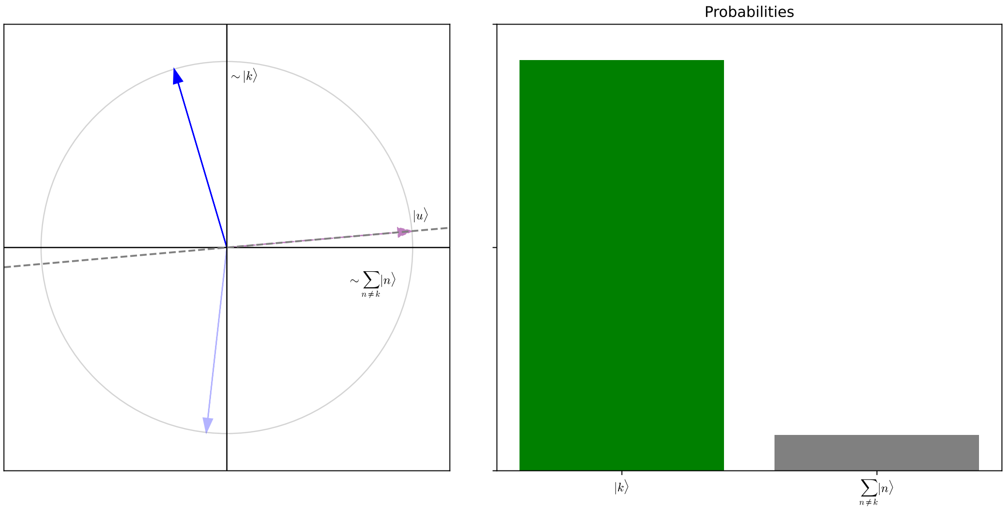



# The Grover Algorithm - geometric picture



# The Grover Algorithm - geometric picture



# The Grover Algorithm - summary

- Given a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ such that $f(x) = 1$ for $x = x^*$, and $f(x) = 0$ otherwise, find $x^*$.
- Unstructured search problems—like finding a needle in a haystack—where no information is known about the solution's location.
- Quadratic speedup. A classical complexity $\mathcal{O}(2^n)$, Grover $\mathcal{O}(\sqrt{2^n})$.
- Iteratively amplifies the amplitude of the solution state using two steps: the oracle and the diffusion operator
- The algorithm is probabilistic but achieves success probability close to 1 after approximately $\frac{\pi}{4}\sqrt{N}$ iterations
- Works also if there are M solutions—requiring $\mathcal{O}(\sqrt{2^n/M})$ queries
- Grover's algorithm is provably optimal—no quantum algorithm can solve unstructured search with fewer queries.
- Like Deutsch-Jozsa, Grover assumes a black-box oracle model. In practice, implementing $U_f$ can be difficult unless f has a known efficient structure.

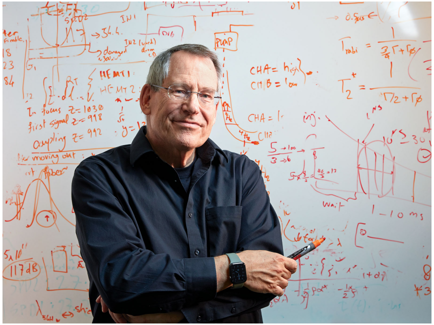
# Noisy Intermediate-Scale Quantum (NISQ) devices

## Noisy

- Quantum devices are exposed to noise (thermal fluctuations, environment, imperfections of gates ...), error rate $\sim 10^{-3} - 10^{-5}$.
- This limits the complexity and accuracy of the computations they can perform.
- No error-correction.

## Intermediate-Scale

- Tens to a few hundred physical qubit
- 50 qubits milestone, $2^{50} \approx 10^{15}$
- Beyond what can be simulated by brute force using the most powerful existing digital supercomputers.



## Limitations

- Only 'short' quantum circuits
- Highly entangled quantum systems
- Frequently hybrid architecture