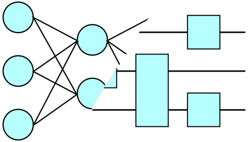
Quantum Algorithms

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

...

Quantum algorithms

NISQ

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

...

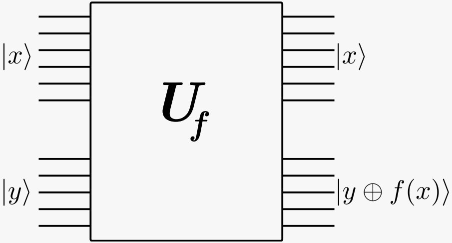
Fault-tolerant

- *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

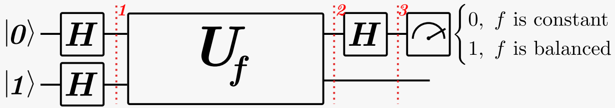
Solutions

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

The Deutsch Algorithm

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

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



Analysis

1

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

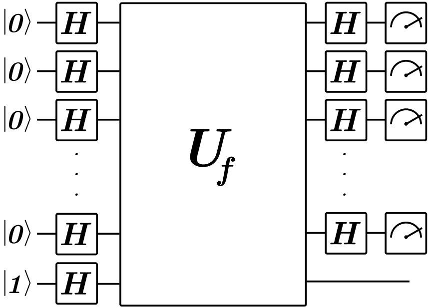
2

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

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

3 (ignoring the second qubit)

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

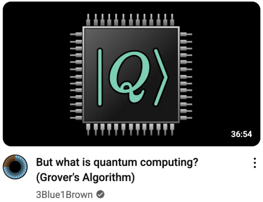


- Extend the same circuit to bigger input (2^n states)
- The probability $\Pr[|00...0\rangle]$

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

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



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:

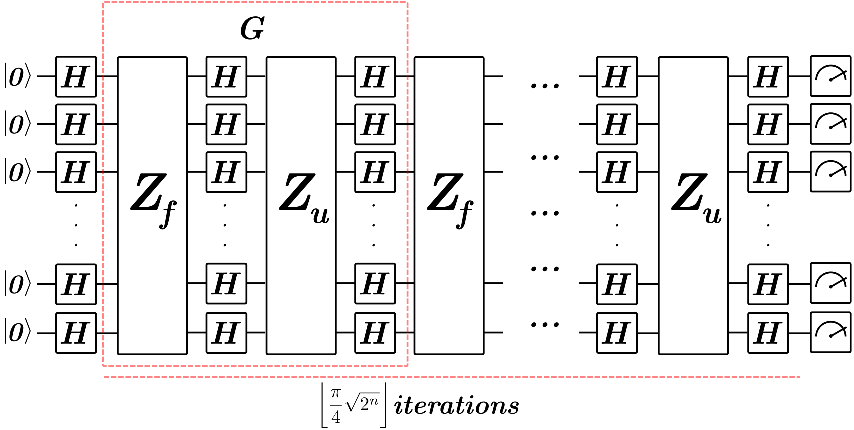
$$Z_f$$

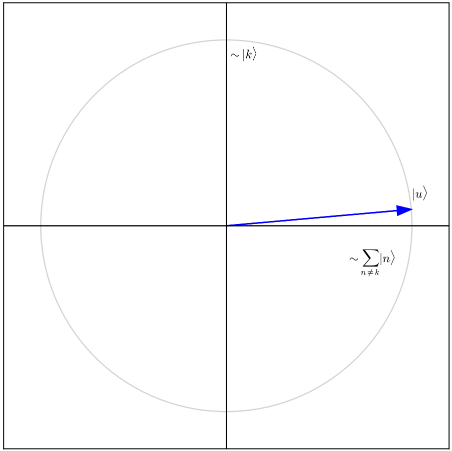
Reflection around the uniform superposition of states which are not solutions.
$|k\rangle$ - solution, reflection around $\sim \sum_{n \neq k} |n\rangle$.

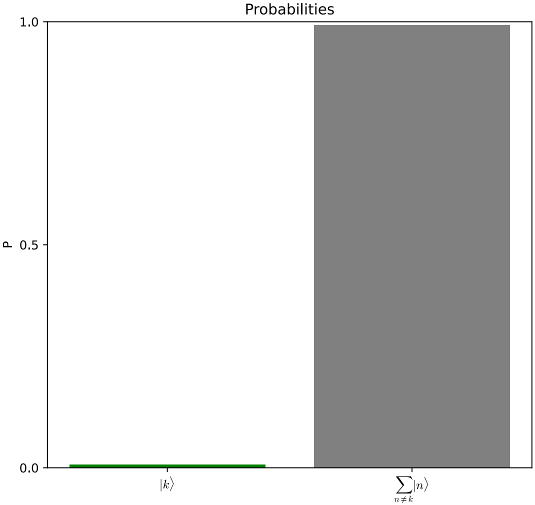
$$H^{\otimes n} Z_u H^{\otimes n}$$

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

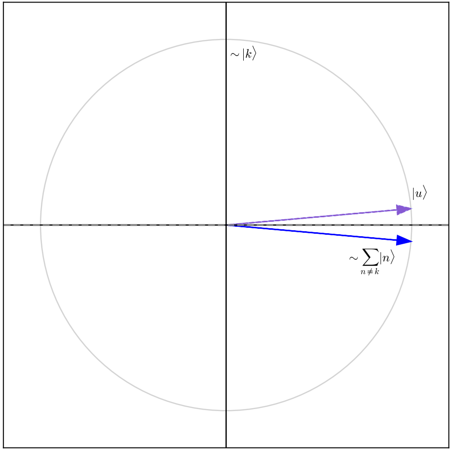
The Grover Algorithm - circuit

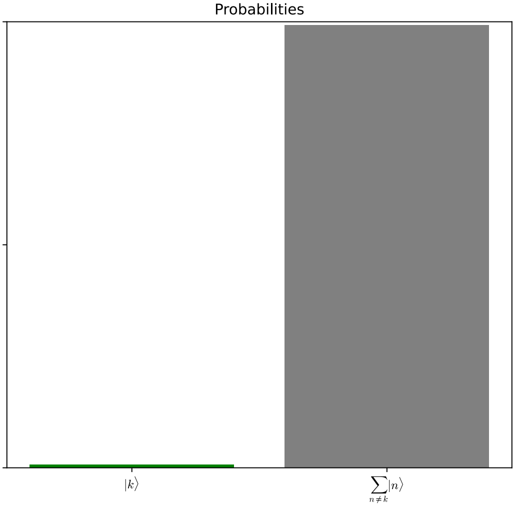


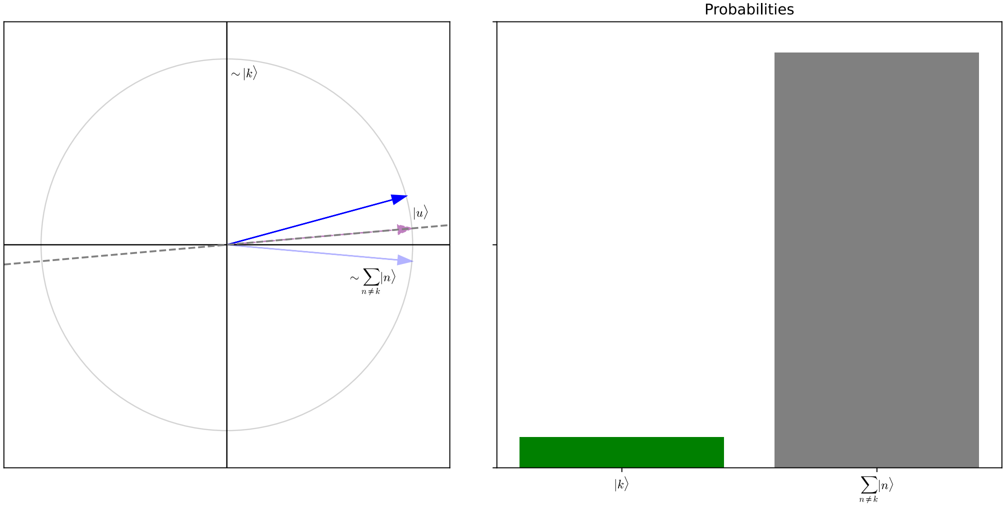

$\sim |k\rangle$
$|u\rangle$
$\sim \sum_{n \neq k} |n\rangle$


Probabilities
1.0
0.5
0.0
P
$|k\rangle$
$\sum_{n \neq k} |n\rangle$

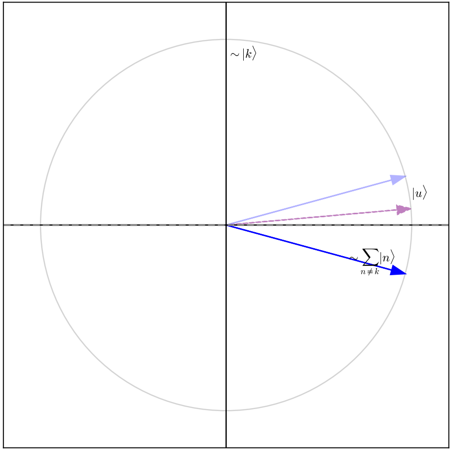
The Grover Algorithm - geometric picture

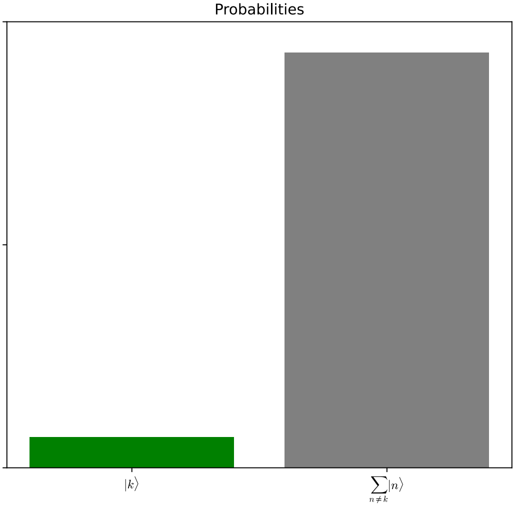




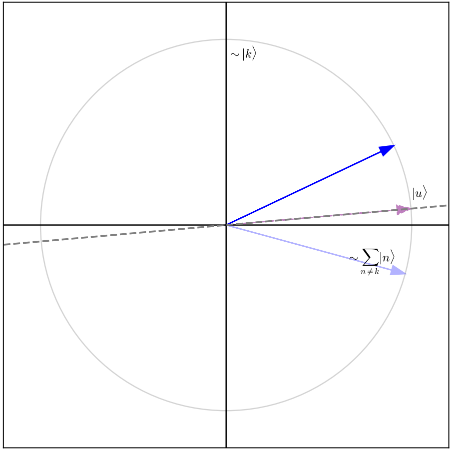

$\sim|k\rangle$
$|u\rangle$
$\sim\sum_{n\neq k}|n\rangle$
Probabilities
$|k\rangle$
$\sum_{n\neq k}|n\rangle$

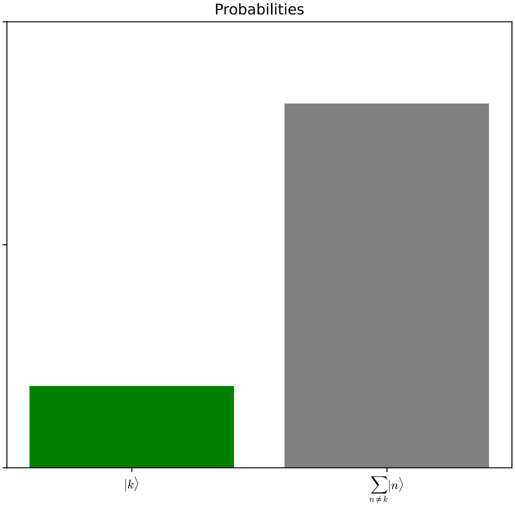
The Grover Algorithm - geometric picture



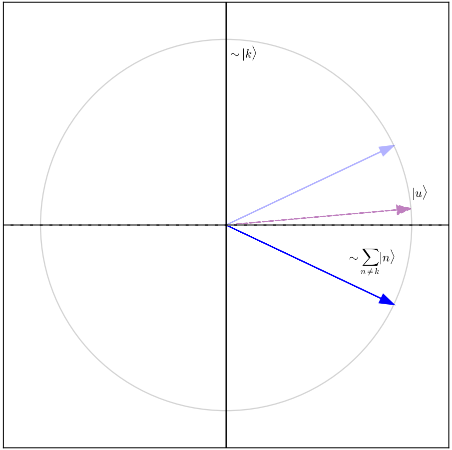


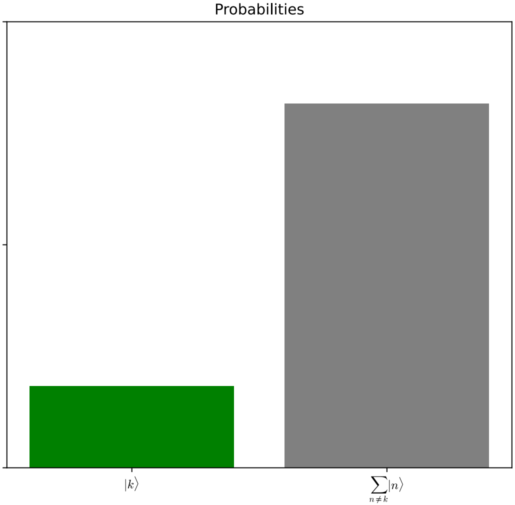
The Grover Algorithm - geometric picture



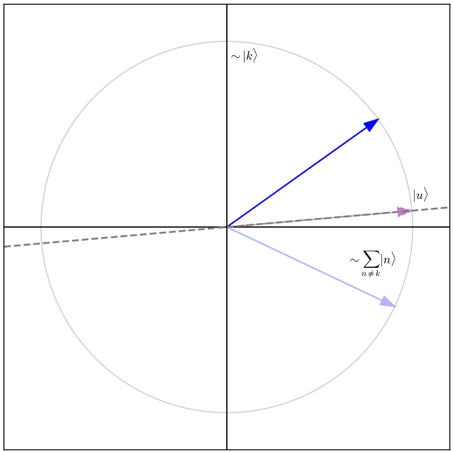


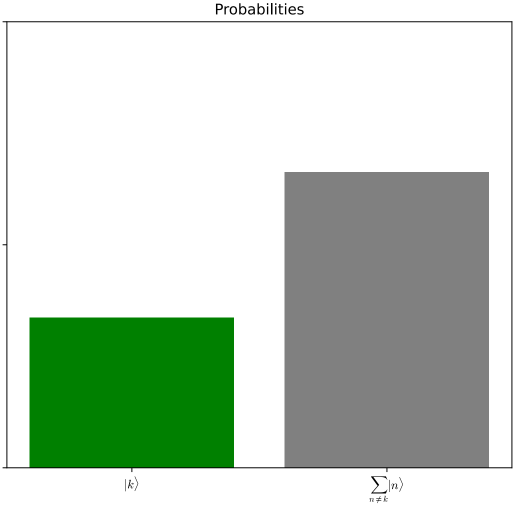
The Grover Algorithm - geometric picture



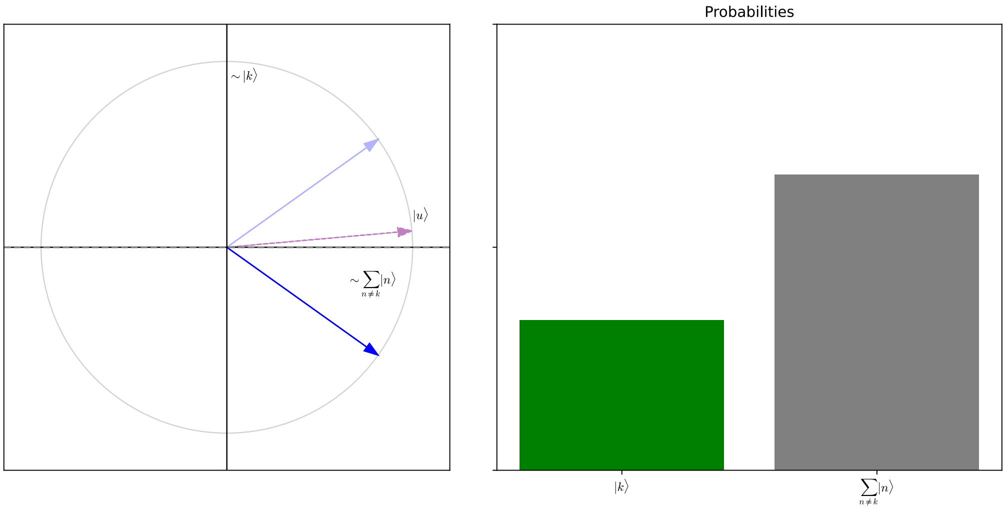


The Grover Algorithm - geometric picture

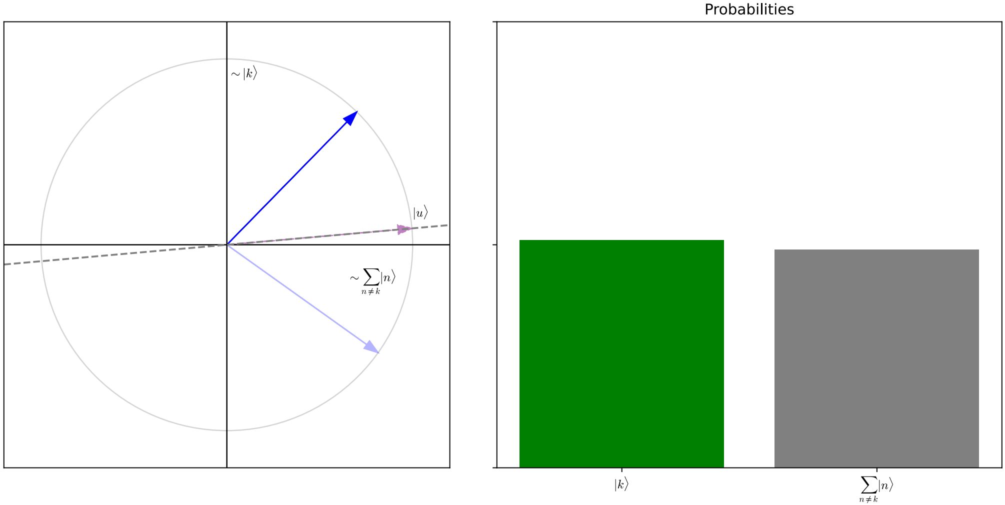




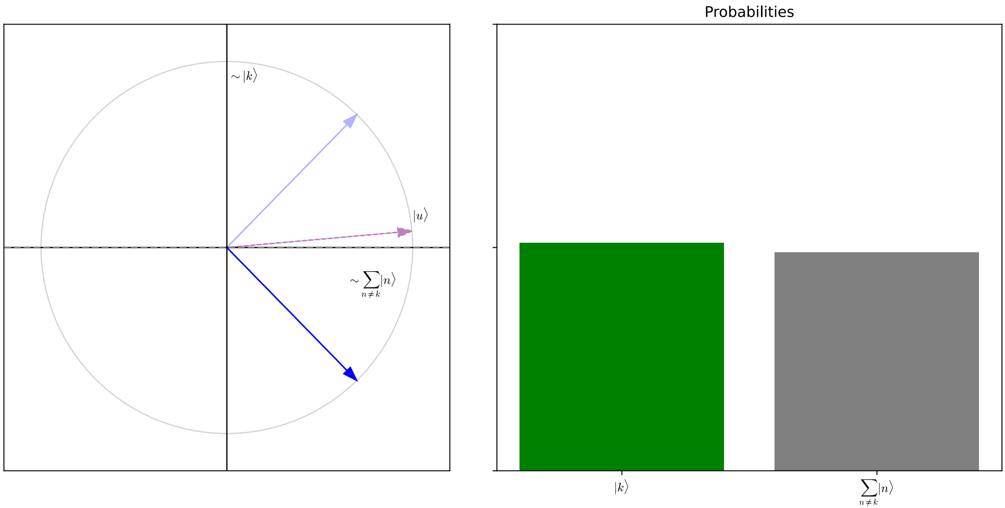
The Grover Algorithm - geometric picture



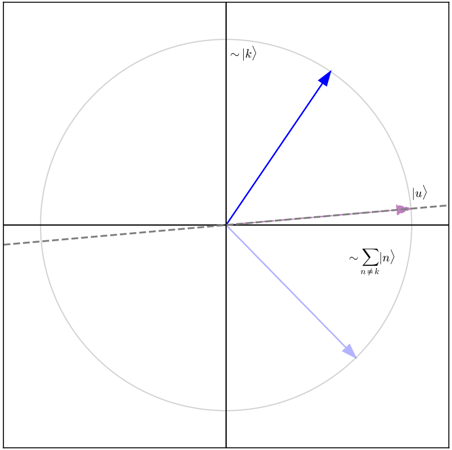
The Grover Algorithm - geometric picture

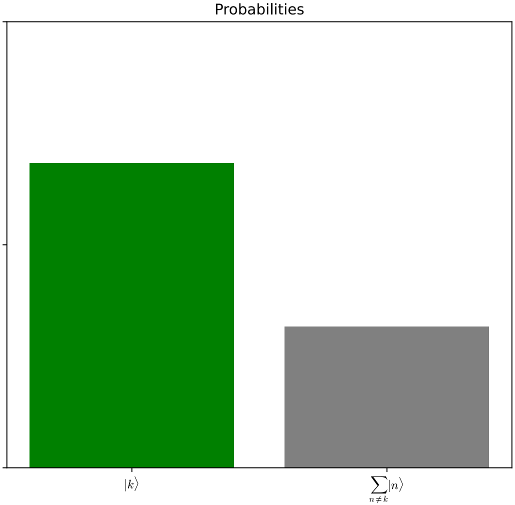


The Grover Algorithm - geometric picture

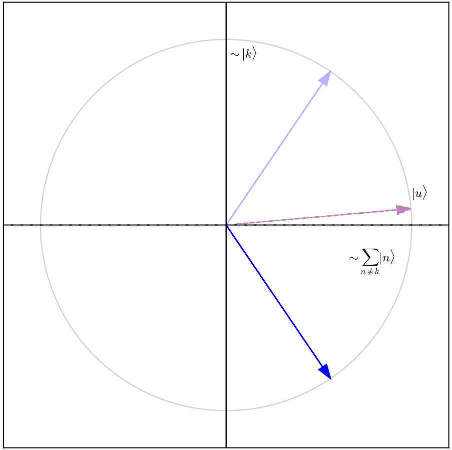


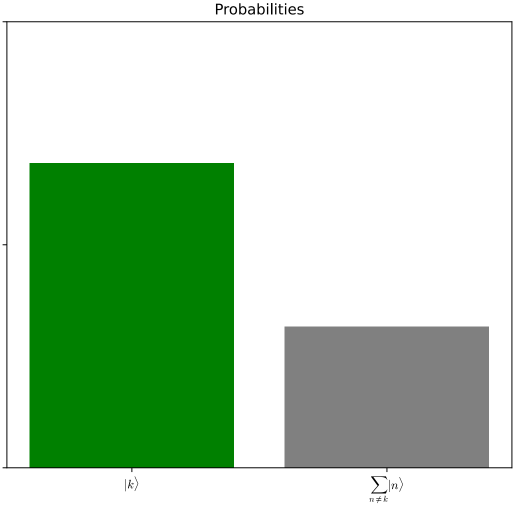
The Grover Algorithm - geometric picture



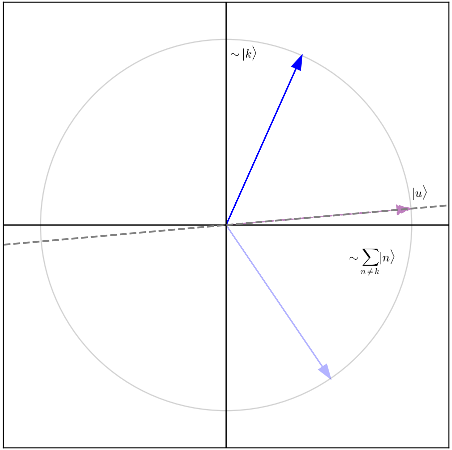


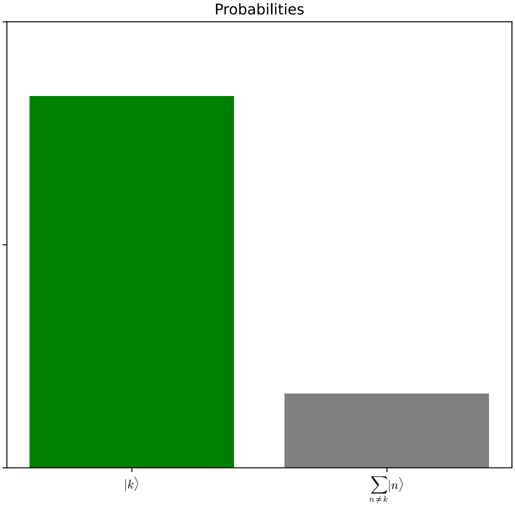
The Grover Algorithm - geometric picture



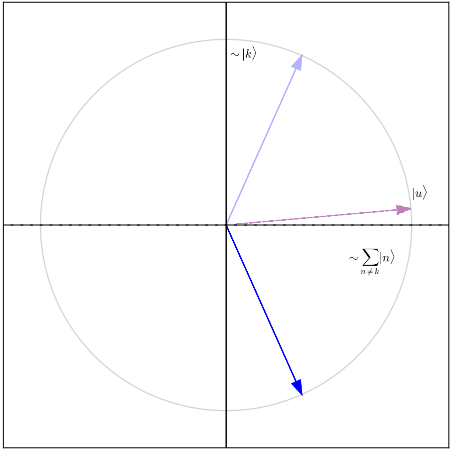


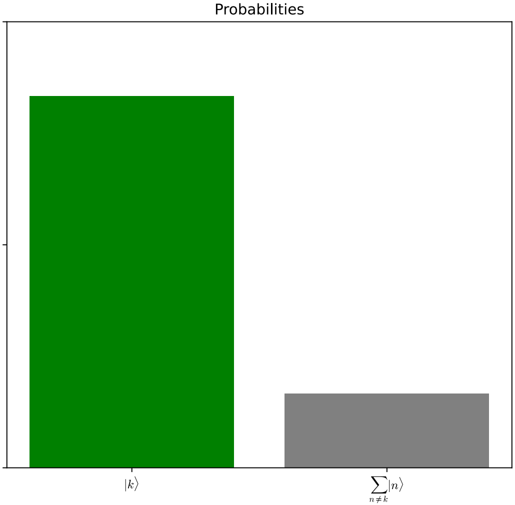
The Grover Algorithm - geometric picture



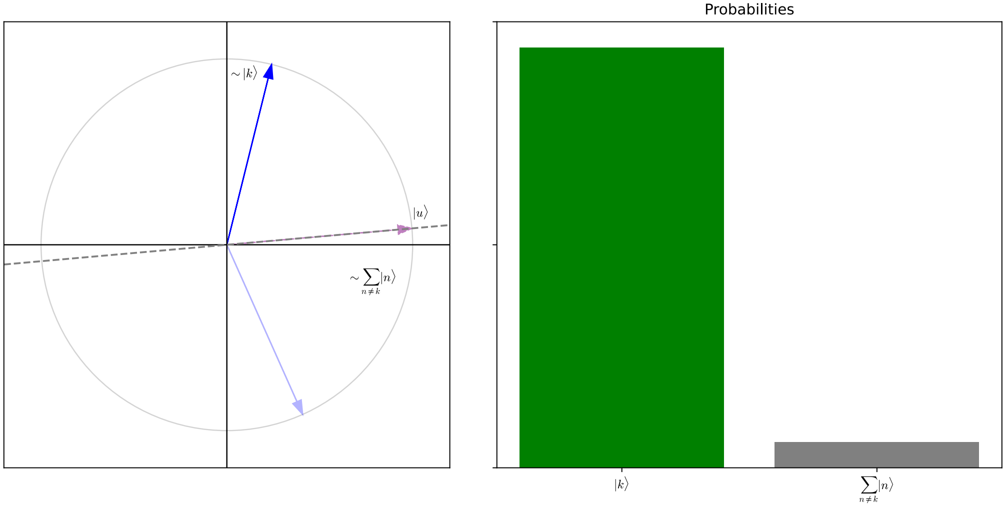


The Grover Algorithm - geometric picture

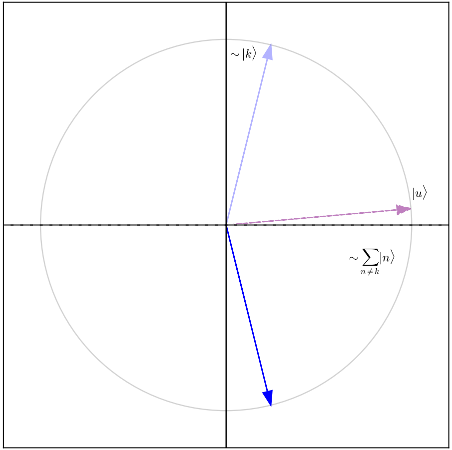


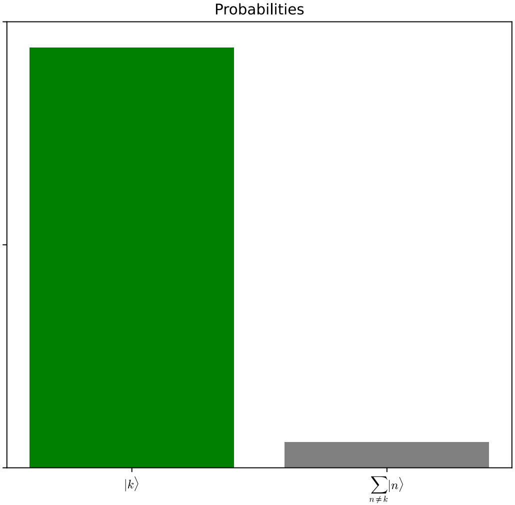


The Grover Algorithm - geometric picture

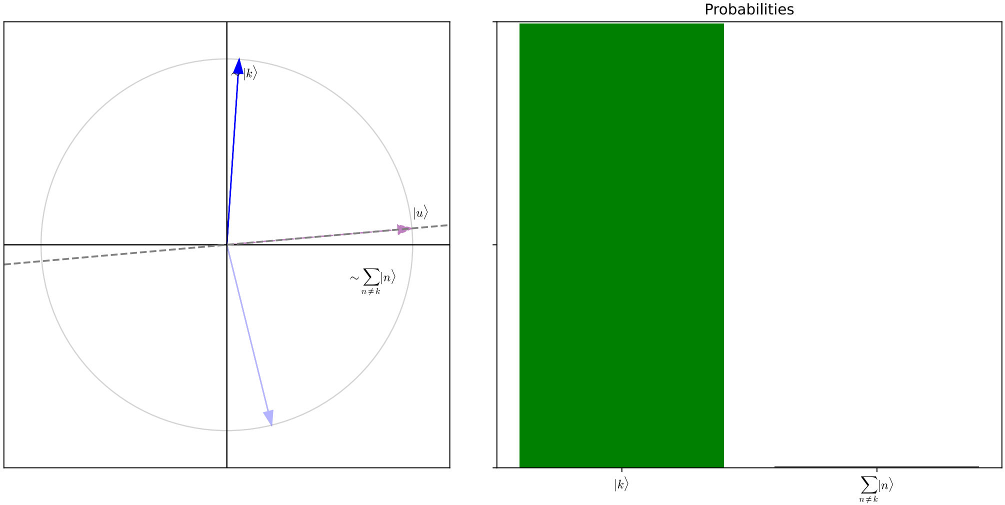


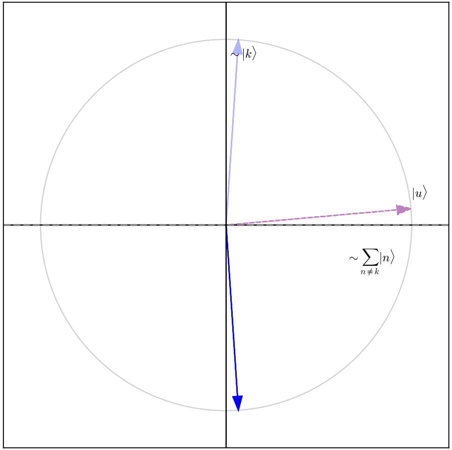
The Grover Algorithm - geometric picture

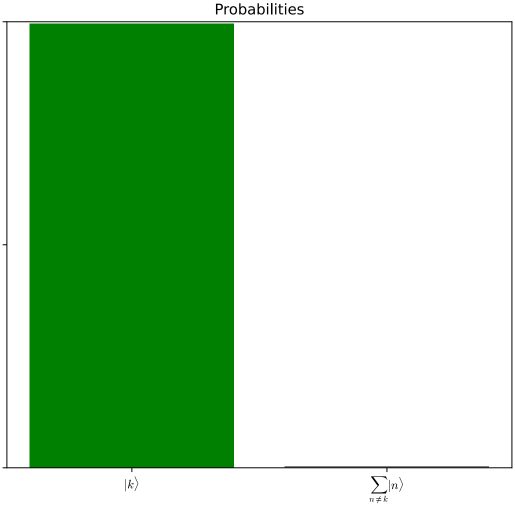




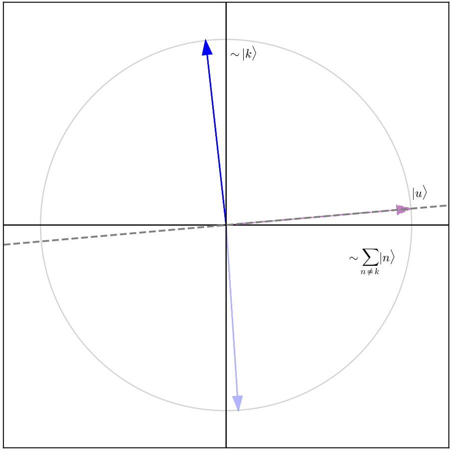
The Grover Algorithm - geometric picture

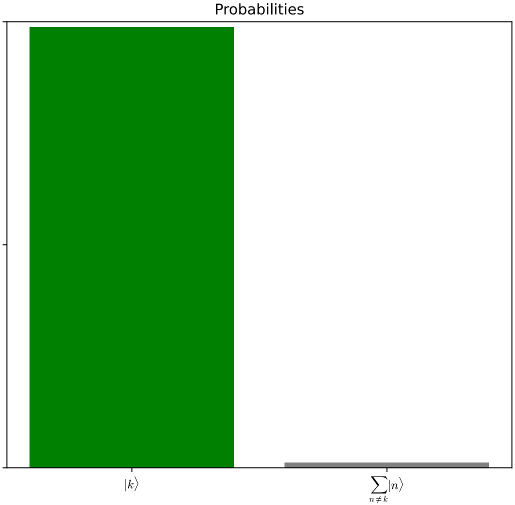



$\sim |k\rangle$
$|u\rangle$
$\sim \sum_{n \neq k} |n\rangle$

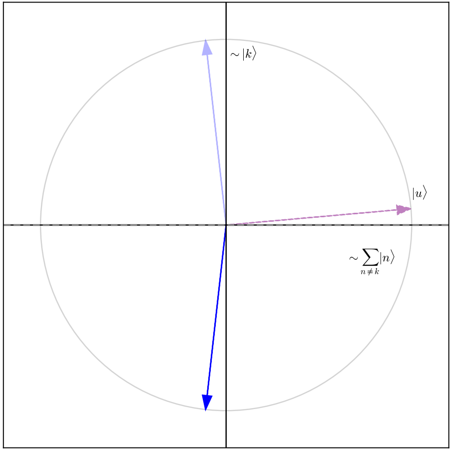

Probabilities
$|k\rangle$
$\sum_{n \neq k} |n\rangle$

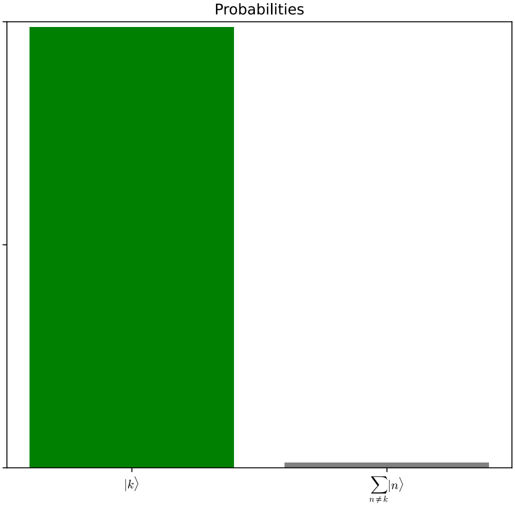
The Grover Algorithm - geometric picture

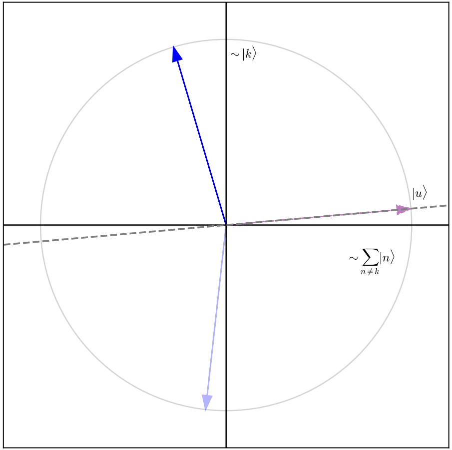


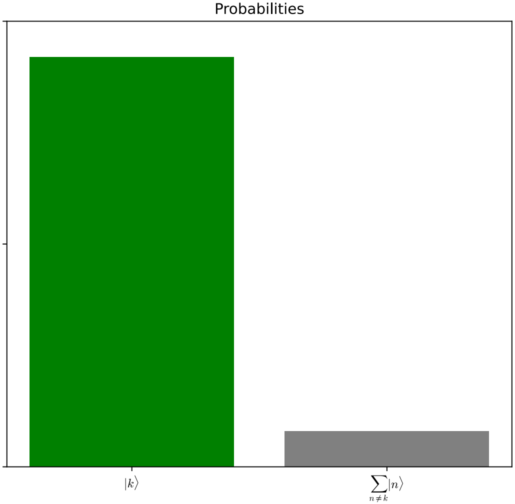


The Grover Algorithm - geometric picture






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


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

The Grover Algorithm - summary

- Given a function $f : \{0,1\}^n \to \{0,1\}$ 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.

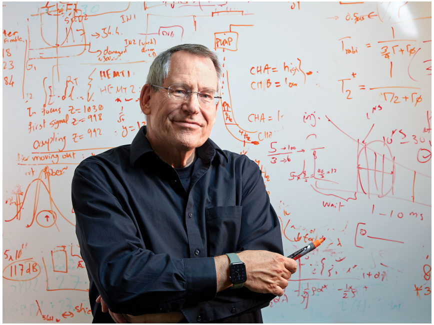
Noisy Intermediate-Scale Quantum (NISQ) devices

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