SummerSoC 2019

Quantum Computing: A Brief Introduction

Frank Leymann
Institute of Architecture of Application Systems (IAAS)
University of Stuttgart

Agenda

Basics in Quantum Physics

The Qbit

Quantum Register

Operators on Quantum Registers

Exponential Speedup

Search & Complexity

Cracking Keys

Encryption

Error Correction

NISQ

Conclusion

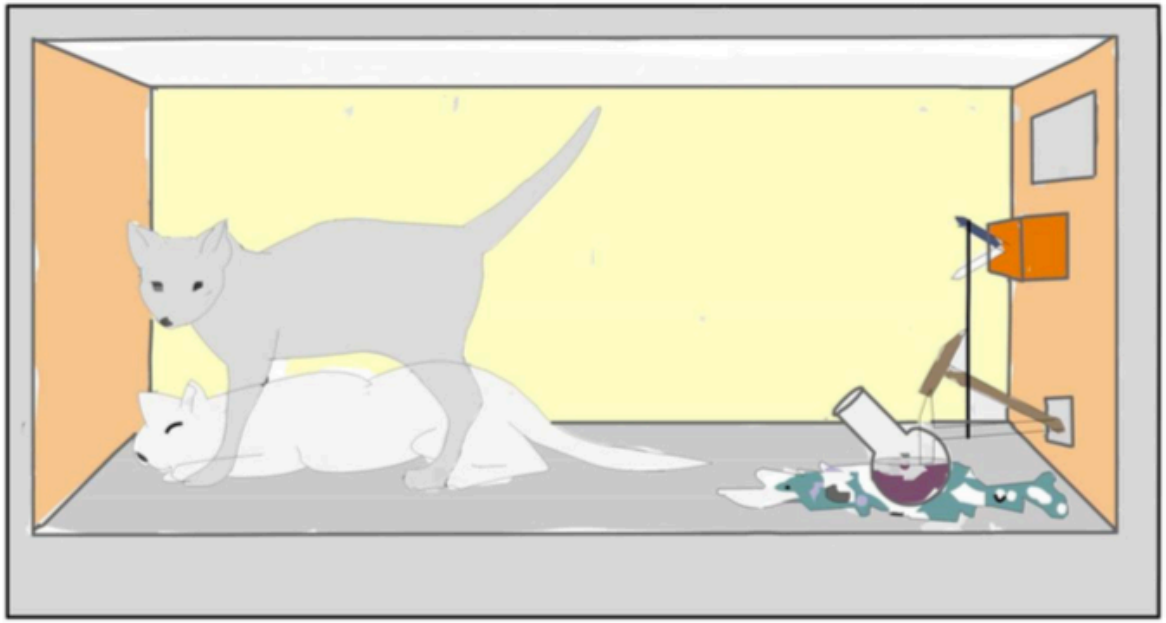
Agenda

- Basics in Quantum Physics
- The Qbit
- Quantum Register
- Operators on Quantum Registers
- Exponential Speedup
- Search & Complexity
- Cracking Keys
- Encryption
- Error Correction
- NISQ
- Conclusion

Heisenberg's Uncertainty Principle

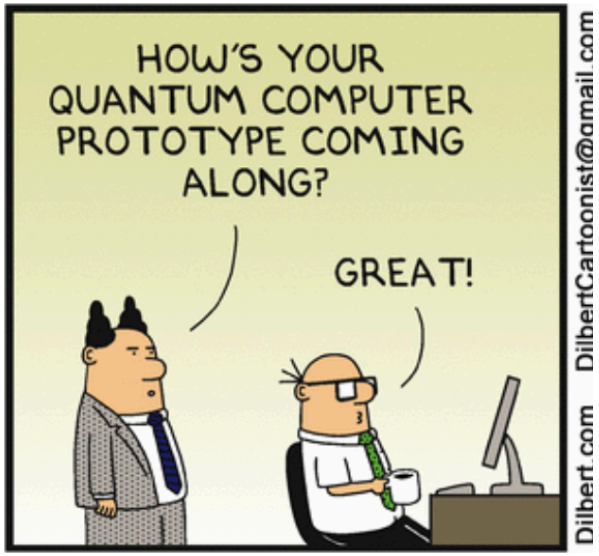
$$\Delta x \cdot \Delta p \geq \frac{h}{4\pi}$$

Schrödinger's Cat



Measuring delivers the result - it destroys superposition

Dilbert Version



http://dilbert.com/strip/2012-04-17

Agenda

- Basics in Quantum Physics
- The Qbit
- Quantum Register
- Operators on Quantum Registers
- Exponential Speedup
- Search & Complexity
- Cracking Keys
- Encryption
- Error Correction
- NISQ
- Conclusion

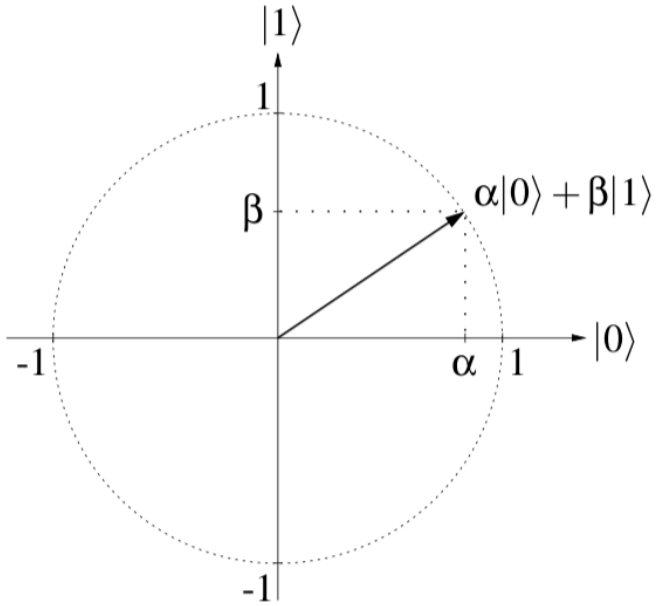
Qbit

Quantum bit (***Qbit***) is in the two classical states $|0\rangle$ or $|1\rangle$ <u>at the same time</u> (!): ***Superposition***
→ not quite right: see refinement a bit later

State of a qbit is

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

ie a linear combination of $|0\rangle$ and $|1\rangle$
$\alpha, \beta \in \mathbb{C}$ and $\mathbf{|\alpha|^2 + |\beta|^2 = 1}$.
Ie a quantum state is a vector
on the unit circle S^1.
$\{|0\rangle, |1\rangle\}$ is a basis of the state space



$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Spherical Coordinates

For each Qbit $|\psi\rangle$ there is a $\theta \in [0, \pi]$ and a $\varrho \in [0, 2\pi]$, such that

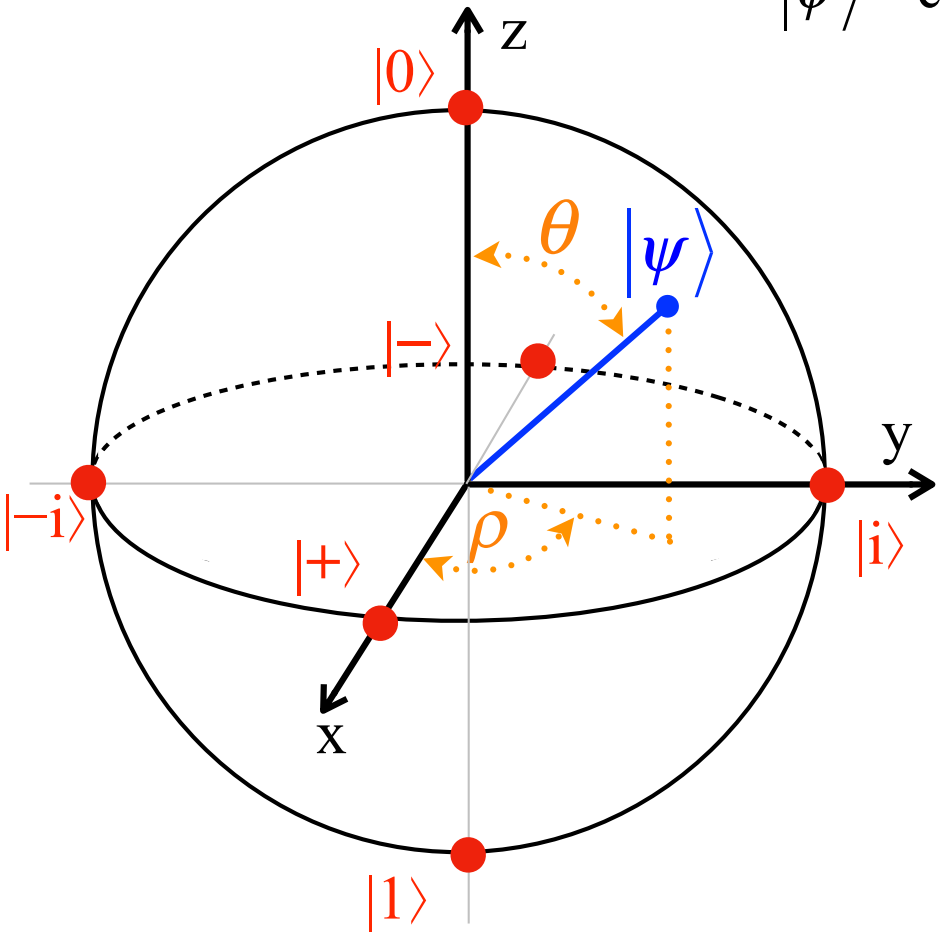
$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\rho}\sin\frac{\theta}{2}|1\rangle$$

This is a bijective map of S^3
(subset of 4-dimensional space)
onto S^2 (subset of 3-dimensional space):

$$\mathbb{C}^2 = \mathbb{R}^4 \supset S^3 \mapsto \mathbb{R}^2 \mapsto S^2 \subset \mathbb{R}^3$$

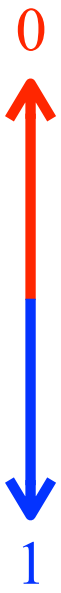
Bloch Sphere

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\rho}\sin\frac{\theta}{2}|1\rangle \;\mapsto\; (\theta,\rho)$$



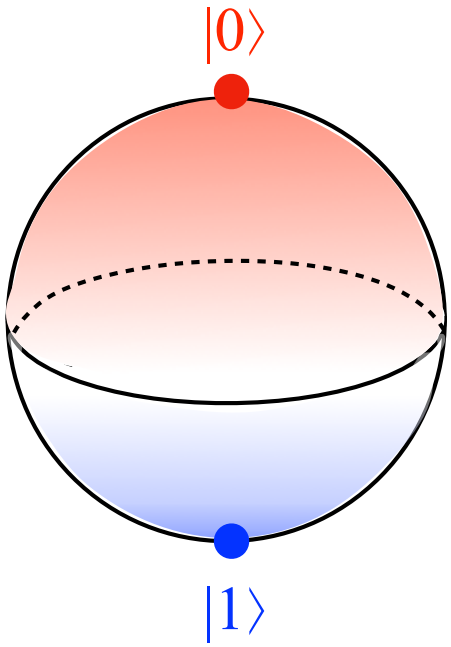
- $\theta = 0 \Rightarrow \psi = |0\rangle$
- $\theta = \pi \Rightarrow \psi = |1\rangle$
- $\theta = \pi/2 \wedge \varrho = 0 \Rightarrow$
  $\psi = 1/\sqrt{2} \cdot (|0\rangle + |1\rangle) =: |+\rangle$
- $\theta = \pi/2 \wedge \varrho = \pi \Rightarrow$
  $\psi = 1/\sqrt{2} \cdot (|0\rangle - |1\rangle) =: |-\rangle$
- $\theta = \pi/2 \wedge \varrho = \pi/2 \Rightarrow$
  $\psi = 1/\sqrt{2} \cdot (|0\rangle + i \cdot |1\rangle) =: |i\rangle$
- $\theta = \pi/2 \wedge \varrho = 3\pi/2 \Rightarrow$
  $\psi = 1/\sqrt{2} \cdot (|0\rangle - i \cdot |1\rangle) =: |-i\rangle$

Intuition of a Qbit



Bit

A bit is either "0" or "1"
→ Two possible values



Qbit

A qbit is an arbitrary point on the Bloch Sphere
→ Uncountably infinit possible values

Measurement

Classical bits can be read
⇒ You can find out <u>the **exact** state</u> (value 0 or 1) of the bit

Can't be done for qbits, their state is the superposition $\alpha|0\rangle + \beta|1\rangle$

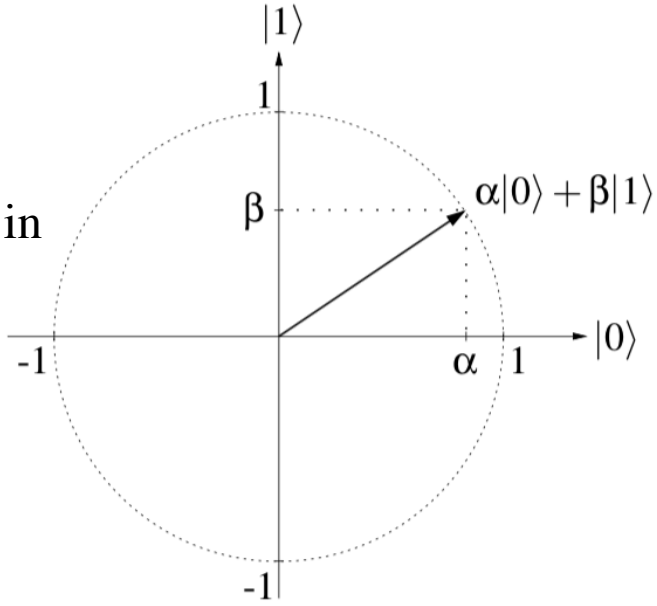
Reading a qbit means measurement, and measuring **destroys** superposition!

<u>Corollary</u>: A qbit can be read only once.

Measuring $|x\rangle = \alpha|0\rangle + \beta|1\rangle$ destroys superposition and results in

state $|0\rangle$ with probability $|\alpha|^2$

state $|1\rangle$ with probability $|\beta|^2$

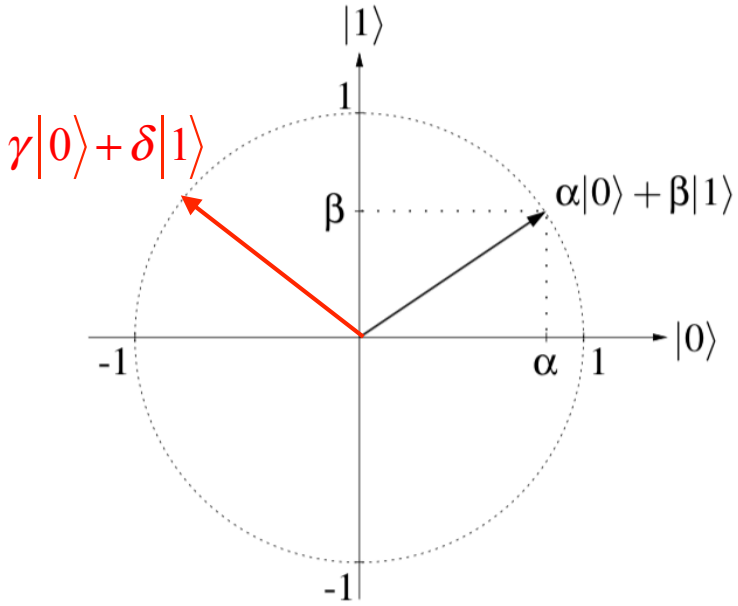


Measurement ≡ Random Experiment

Single Computation Steps

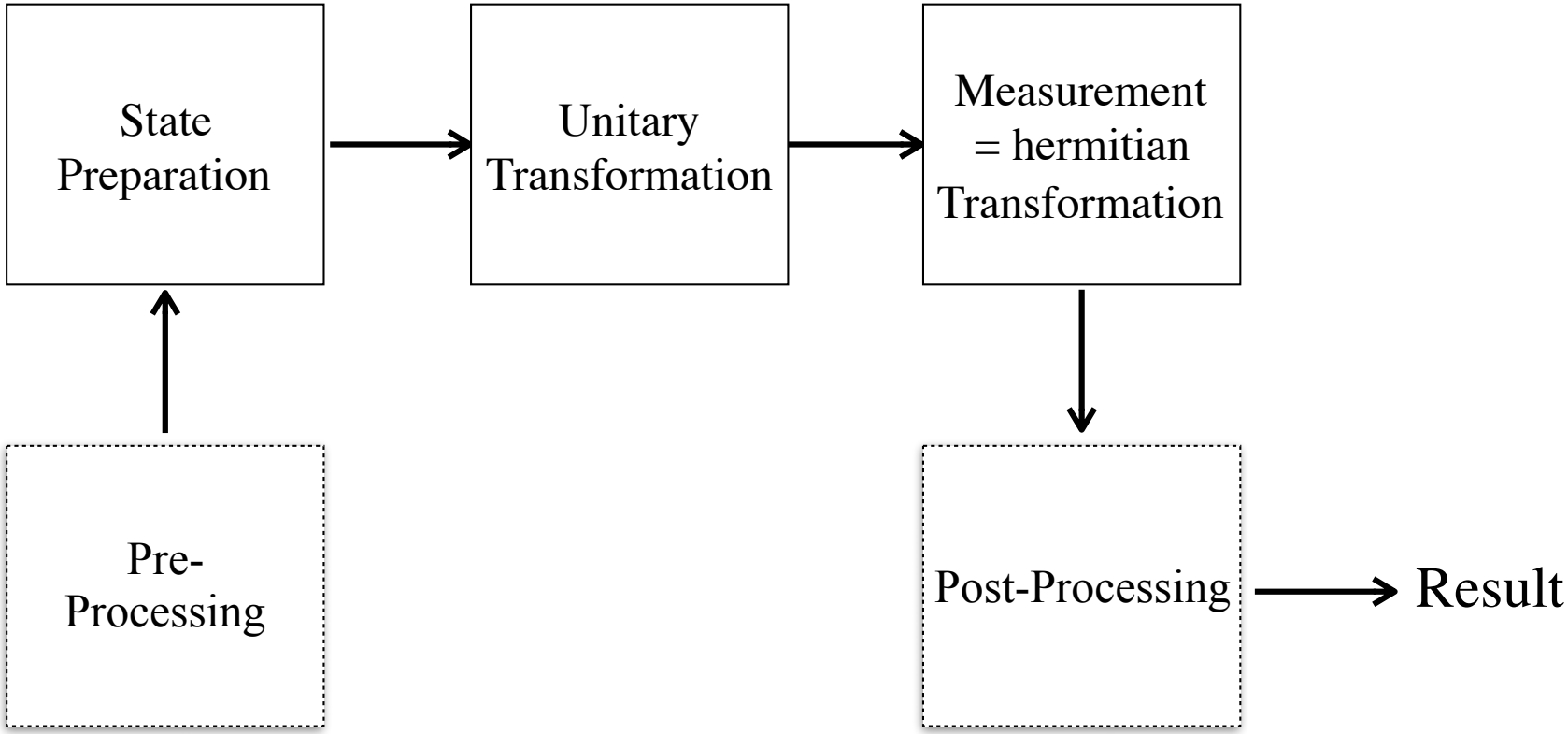
A *computation step* creates from a state (a vector of length "1") a new state (again a vector of length "1").

A computation step is a linear map preserving lengths, thus, a unitary map.



A computation step is represented by a unitary linear map

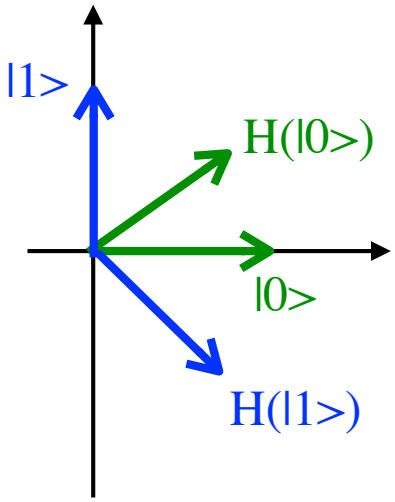
Principle of a Quantum Algorithm



Example: Coin Flipping

We want an algorithm, that results in $|0\rangle$ with probability 1/2,

and that results in $|1\rangle$ with probability 1/2



1. $|x\rangle \leftarrow |0\rangle$
2. $|x\rangle \leftarrow H|x\rangle$
3. Measure $|x\rangle$

Step 1: Qbit $|x\rangle$ is initialized in state $|0\rangle$

Step 2: Hadamard transformation H is applied to $|x\rangle$
thus, $|x\rangle$ transitions into state $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$

Step 3: Measuring gives the desired result

The algorithm produces a completely random bit, i.e. a random number:
Classical algorithms can only produce pseudo random numbers!

Impossible Algorithm: No-Cloning Theorem

There can be no algorithm,
which can copy each arbitrary state of a system.

Formalization:

There exists no unitary transformation $U : H \to H$

such that for a chosen $|c\rangle \in H$ (the state receiving the copy)

and an arbitrary state $|\psi\rangle \in H$ holds: $(id \otimes U)(|\psi\rangle \otimes |c\rangle) = |\psi\rangle \otimes |\psi\rangle$

Agenda

Basics in Quantum Physics

The Qbit

Quantum Register

Operators on Quantum Registers

Exponential Speedup

Search & Complexity

Cracking Keys

Encryption

Error Correction

NISQ

Conclusion

Quantum Register: Informally

Quantum ***register*** is a series of n qbits

Classical register is a series of n bits

Quantum register with n qbits is the superposition of the corresponding 2^n states

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

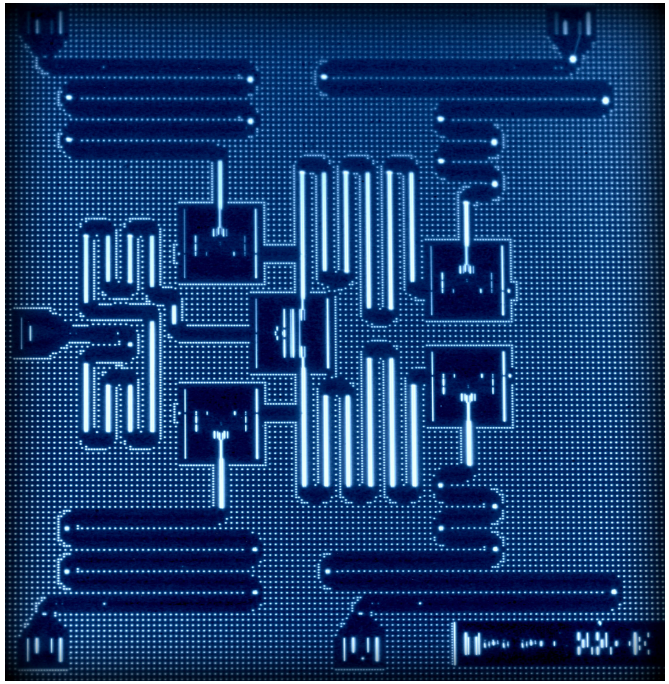
Classical register with n bit $\rightarrow$ 1 value at a time

Quantum register with n bit $\rightarrow$ 2^n value at the **same** time

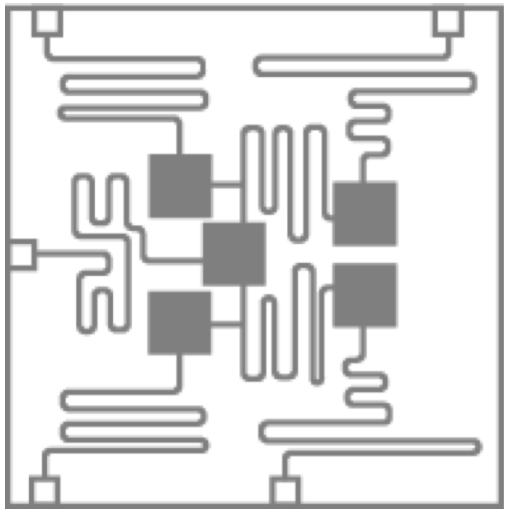
E.g.. $2^{50} = (2^{10})^5 > (10^3)^5 = 10^{15}$ ($\triangleq$Peta…)

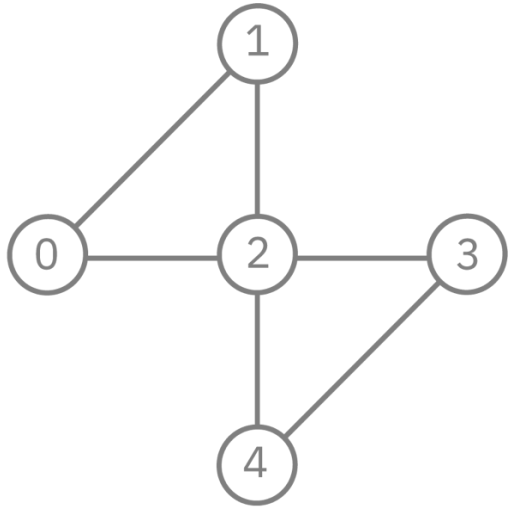
Quantum computer manipulates 2^n values at the same time (*Quantum Parallelism*)

Quantum Register: Hardware



https://www.theregister.co.uk/2017/03/06/ibm_has_cloud_access_to_quantum_computer_400_times_smaller_than_dwave_system/





https://www.research.ibm.com/ibm-q/technology/devices/images/5qubit.png

2-Qbit Quantum Register: Formally

$$R = |x_1\rangle \otimes |x_0\rangle$$

This is a product!
("tensor product")

$$|x_0\rangle = \gamma_0|0\rangle + \gamma_1|1\rangle$$

$$|x_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

$$\begin{aligned} R &= |x_1\rangle \otimes |x_0\rangle \\ &= \left(\beta_0|0\rangle + \beta_1|1\rangle\right) \cdot \left(\gamma_0|0\rangle + \gamma_1|1\rangle\right) \\ &= \beta_0\gamma_0|0\rangle|0\rangle + \beta_0\gamma_1|0\rangle|1\rangle + \beta_1\gamma_0|1\rangle|0\rangle + \beta_1\gamma_1|1\rangle|1\rangle \end{aligned}$$

With $\alpha_{ij} = \beta_i\gamma_j$

$$\begin{aligned} R &= \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle \\ &= \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \end{aligned}$$

Quantum Register

Let ${}_2\mathrm{H}$ be the $\mathbb{C}$-vector space spanned by $\left\{\left|0\right\rangle,\left|1\right\rangle\right\}$

Then, $\left|\phi\right\rangle \in {}_2H^{\otimes n} := \underbrace{{}_2H \otimes \cdots \otimes {}_2H}_{n-times}$ with $\left|\left|\left|\phi\right\rangle\right|\right| = 1$ is called *state* of the n-qbit-*quantum register* $\left|x_{n-1}\right\rangle \otimes \cdots \otimes \left|x_0\right\rangle$

$$\mathbb{C}^{2^n} = {}_2H^{\otimes n}$$

Separable & Entangled States

$$\left|\phi\right\rangle \in H_1 \otimes \cdots \otimes H_n \quad \text{is called} \quad \textit{separable} :\Leftrightarrow$$

$$\left|\phi\right\rangle = \left|\psi_1\right\rangle \otimes \cdots \otimes \left|\psi_n\right\rangle \quad \text{with} \quad \left|\psi_i\right\rangle \in H_i,\ 1 \leq \mathrm{i} \leq \mathrm{n}$$

$$\left|\phi\right\rangle \quad \text{is called } \textit{entangled} :\Leftrightarrow \left|\phi\right\rangle \text{ is not separable}$$

Entanglement

$$\frac{1}{\sqrt{2}}\left(|00\rangle+|01\rangle\right)=\frac{1}{\sqrt{2}}|0\rangle\otimes\left(|0\rangle+|1\rangle\right)$$

A state that is not separable is called *entangled*

(separable)

$$\frac{1}{\sqrt{2}}\left(|00\rangle+|01\rangle\right)$$

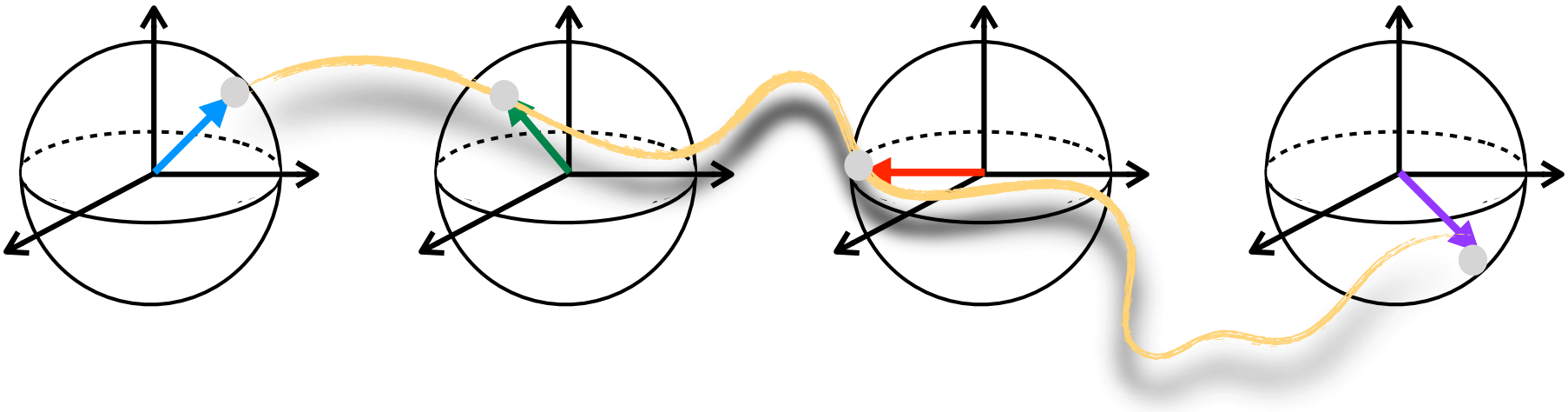
Measuring the first qbit results in $|0\rangle$ with probability 1.
The second qbit will be measured as $|0\rangle$ or $|1\rangle$ with probability 1/2

$$\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)$$

Measuring the first qbit results in $|0\rangle$ or $|1\rangle$ with equal probability.
After that the value of the second qbit is already determined!

Einstein–Podolsky–Rosen Paradox
(EPR Paradox)

Intuition:
Entanglement as Global Phenomenon



Manipulation of a single Qbit $|x_i\rangle$ of a quantum register $|x_1\rangle \otimes \ldots \otimes |x_n\rangle$

has impact on all qbits of the quantum register

Entanglement: Importance

Entanglement is unique for quantum computing!

Every computation that is not involving entangled qbits,
can be performed with the same efficiency with classical computations.

Every quantum algorithm showing exponential speedup
compared to classical algorithms, must exploit entanglement.

(Jozsa / Linden, 2003)

Agenda

Basics in Quantum Physics

The Qbit

Quantum Register

Operators on Quantum Registers

Exponential Speedup

Search & Complexity

Cracking Keys

Encryption

Error Correction

NISQ

Conclusion

1-Qbit Operators

A unitary map f : ${}_2H \to {}_2H$ is called *1-qbit operator* (…*Gate*)

Quantum NOT, Bit Flip

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Phase Flip

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

X, Y, Z are called *Pauli-Matrices*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Hadamard Matrix

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

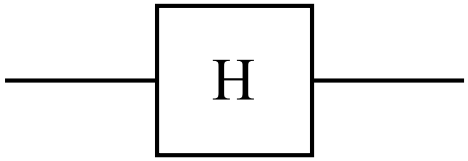
Phase Matrix

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

π/8 Matrix
(yeah, strange: π/8 vs π/4;
pure historical reasons!)

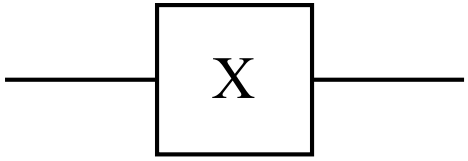
1-Qbit Gates

Hadamard



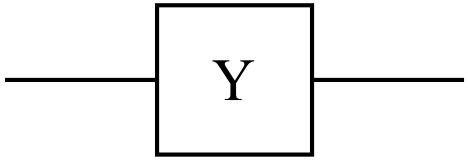
$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Pauli-X



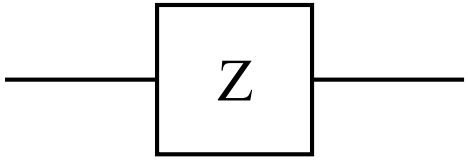
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Pauli-Y



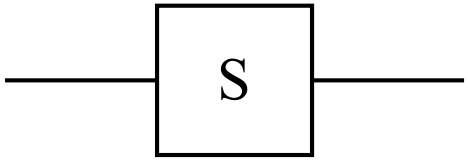
$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Pauli-Z



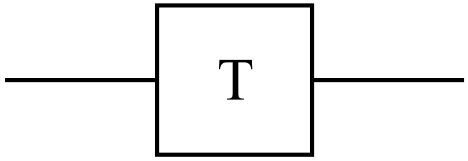
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Phase



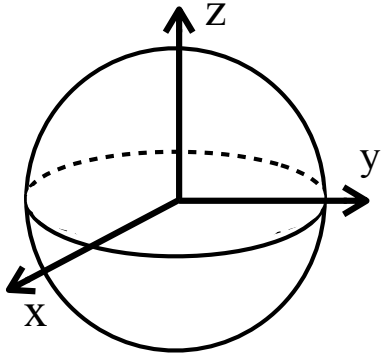
$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

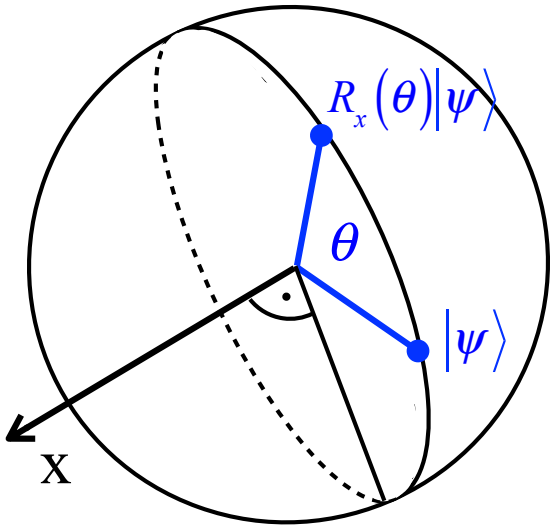
$\pi/8$



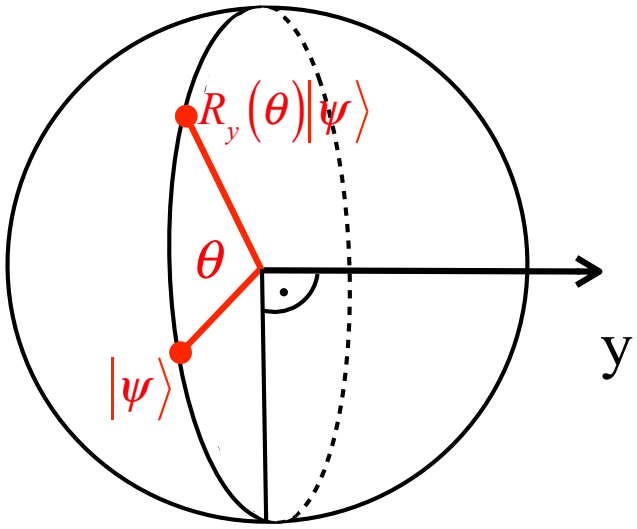
$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

Geometry of Exponential Pauli Operators

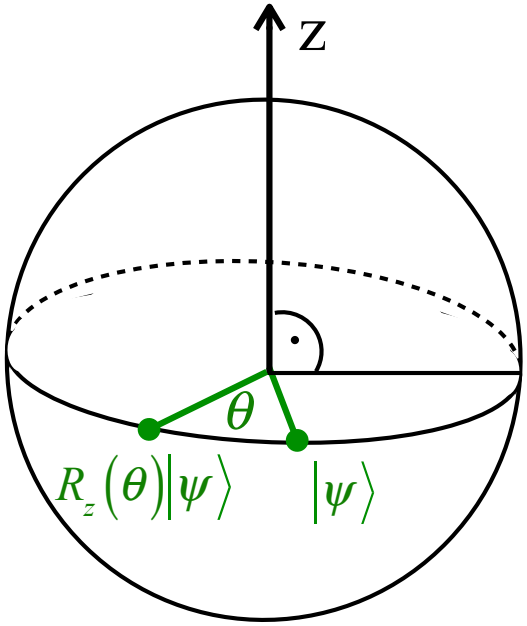




$R_x(\theta)$ is rotation by θ around x-axis

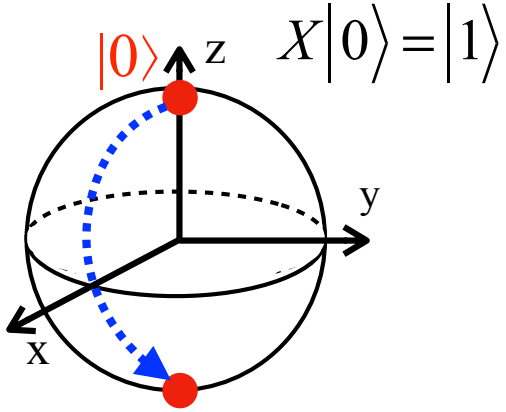


$R_y(\theta)$ is rotation by θ around y-axis



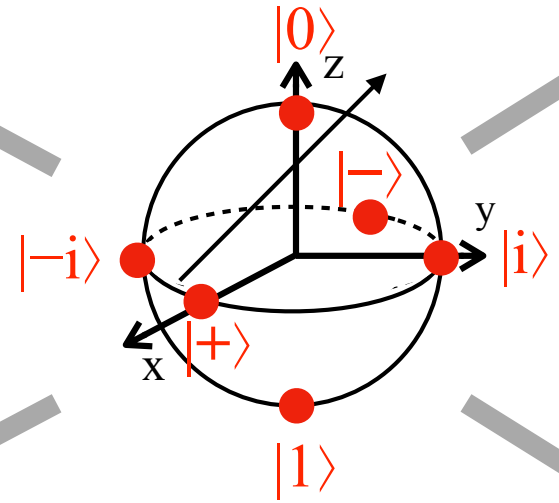
$R_z(\theta)$ i is rotation by θ around z-axis

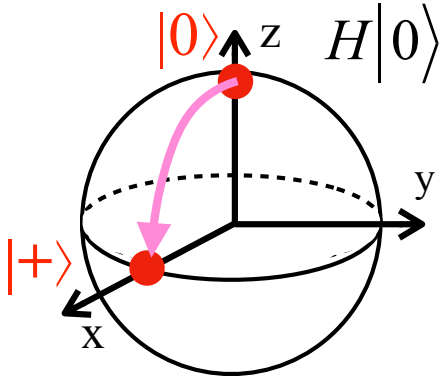
Examples



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

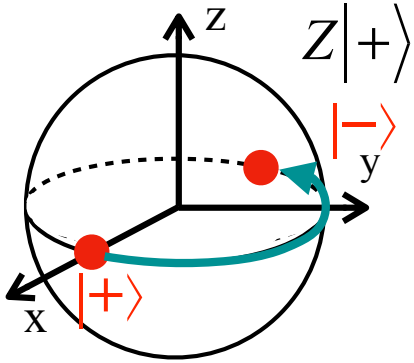
$$R_x(\pi)|0\rangle = |1\rangle$$





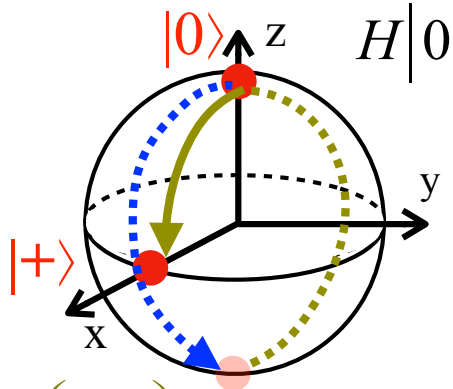
$$H|0\rangle = |+\rangle$$

$$R_x\left(\frac{\pi}{2}\right)|0\rangle = |+\rangle$$



$$Z|+\rangle = |-\rangle$$

$$R_z(\pi)|+\rangle = |-\rangle$$



$$H|0\rangle = |+\rangle$$

$$R_y\left(\frac{3\pi}{2}\right)R_x(\pi)|0\rangle = |+\rangle$$

1-Qbit Operators: Decomposition

A set $\mathcal{U}$ of 1-qbit operators is called *universal* :$\Leftrightarrow$
Each 1-qbit operator is a finite combination of operators from $\mathcal{U}$

Let U be a 1-qbit operator. Then:

Z-Y Decomposition

$$\exists\ \alpha,\beta,\gamma,\delta \in \mathbb{R}:\ U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

X-Y Decomposition

$$\exists\ \alpha,\beta,\gamma,\delta \in \mathbb{R}:\ U = e^{i\alpha} R_x(\beta) R_y(\gamma) R_x(\delta)$$

Every 1-qbit operator is a composition of rotations on the Bloch Sphere

The set of Pauli-Operators are universal for 1-qbit operators

Operators on Quantum Registers

Let n>1, ${}_2H^{\otimes n} = {}_2H \otimes \cdots \otimes {}_2H$

A unitary map f : ${}_2H^{\otimes n} \rightarrow {}_2H^{\otimes n}$ is called
n-qbit operator (or *quantum-register-operator* oder *quantum gate*)

A set $\mathcal{U}$ of quantum-register-operators is called *universal* :$\Leftrightarrow$
Every quantum-register-operator is a finite combination of operators from $\mathcal{U}$

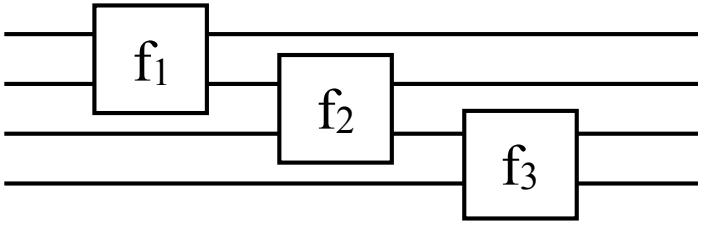
Two-Level Operators

Let $f : V \to V$ be a unitary map

f is called *two-level* $:\Leftrightarrow \exists\, U \in \mathbb{C}^{2\times 2} :$ M(f) = and U is unitary

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & U & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$$

A two-level operator modifies
at most two adjacent qbits of a quantum register



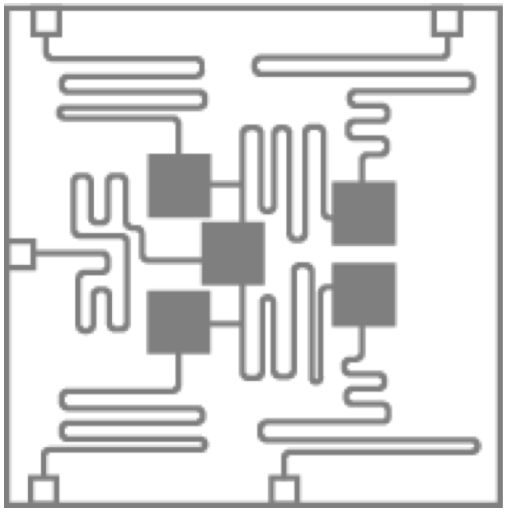
Decomposition into Two-Level Operators

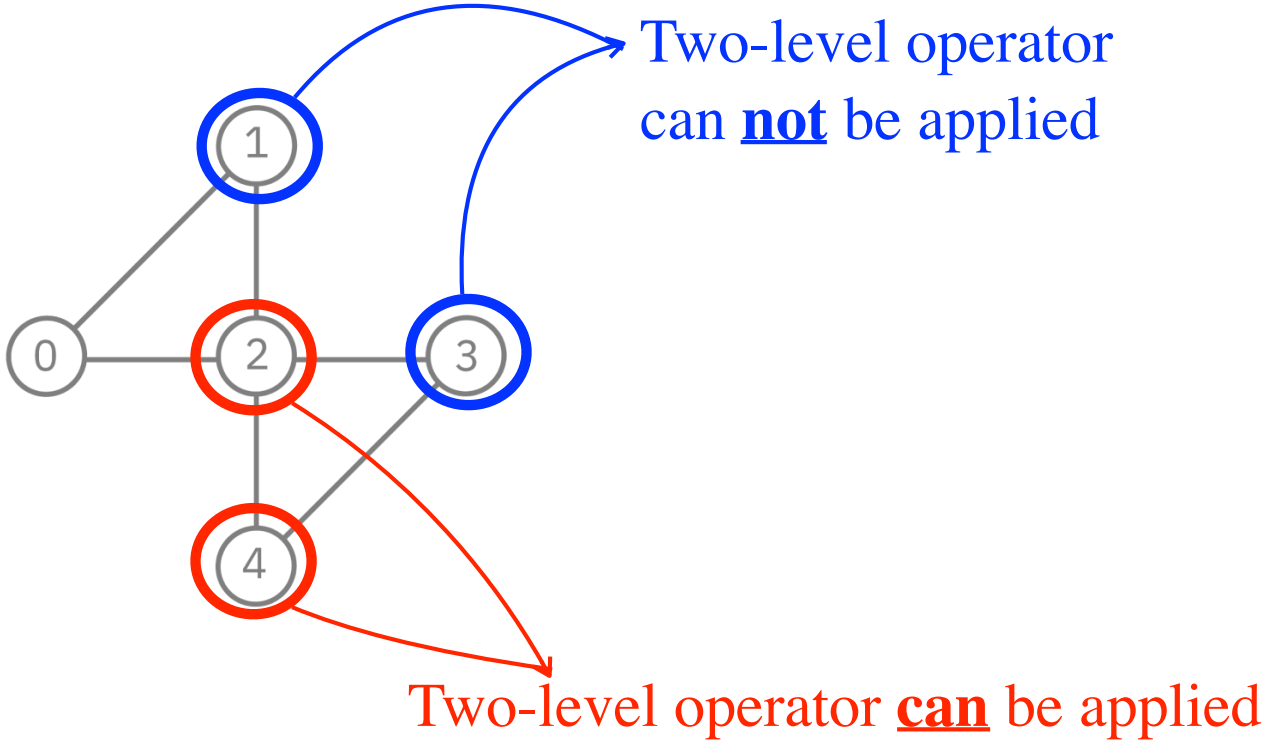
The set of all two-level operators on quantum registers
is universal.

Problem: There is an infinite number of two-level operators.
But the set of universal operators should be "small"!

Two-Level Operators: Hardware

Two-level operator requires connection between the two qbits





CNOT (Controlled Not)

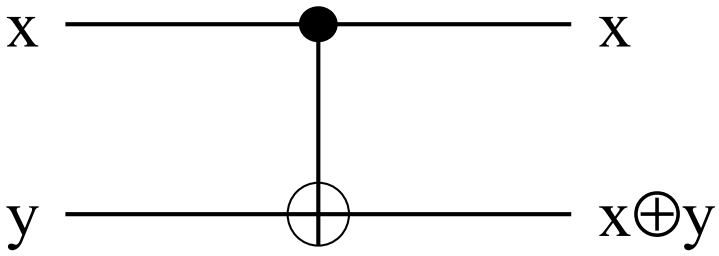
$$\text{CNOT} : {}_2H \otimes {}_2H \to {}_2H \otimes {}_2H$$
$$|x,y\rangle \mapsto |x, x \oplus y\rangle$$

$\oplus$	0	1
0	0	1
1	1	0

$\oplus : \{0,1\} \to \{0,1\}$ with $x \oplus y \mapsto x+y \bmod 2$

I.e. if x=1 then y will be negated; otherwise, y is not changed at all
(x is called *control*-qbit, y is called *target*-qbit)

CNOT is unitary



CNOT Gate

CNOT and Entanglement

$$\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\otimes|0\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle+|10\rangle\right)$$ is separable

$$CNOT\left(\frac{1}{\sqrt{2}}\left(|00\rangle+|10\rangle\right)\right)=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)$$ is entangled

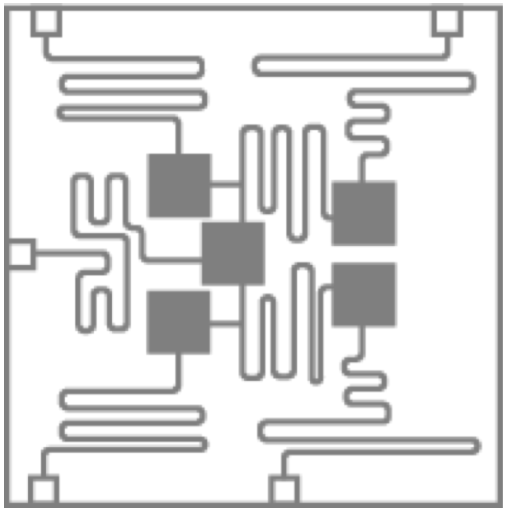
CNOT can transform separable states into entangled states

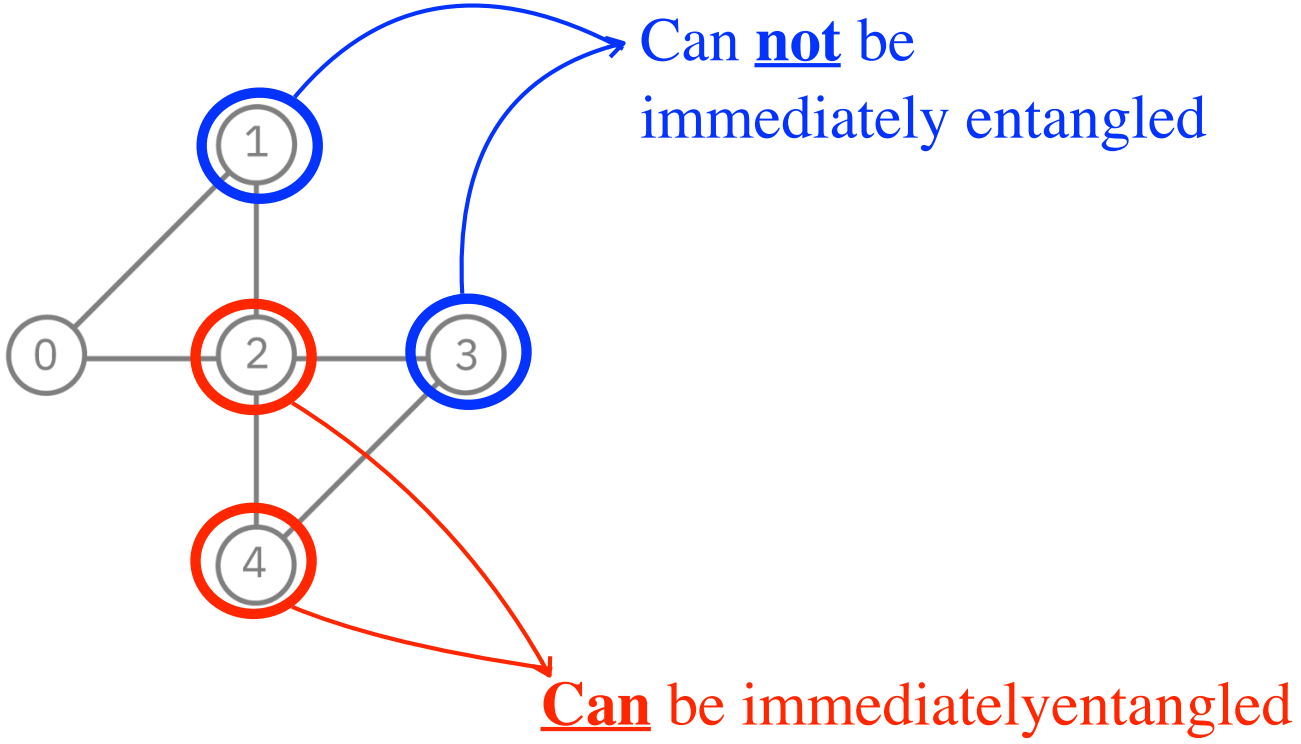
$$CNOT\left(\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)\right)=\frac{1}{\sqrt{2}}\left(|00\rangle+|10\rangle\right)$$

CNOT can transform entangled states into separable states

Entanglement: Hardware

Immediate entanglement of two qbits requires connection between them





⇒ Connectivity of a quantum chip is important

Decomposition into CNOT and 1-Qbit Operators

The set of 1-qbit Operators and CNOT is universal.

Reminder: The Pauli-Matrices is a set of universal 1-qbit operators

For an n qbit quantum register it is $d=2^n$.
The number of required 1-qbit operators and CNOTs is $O(n^2 \cdot 4^n)$

Problem: This is not an efficient implementation of quantum register operators

Approximation

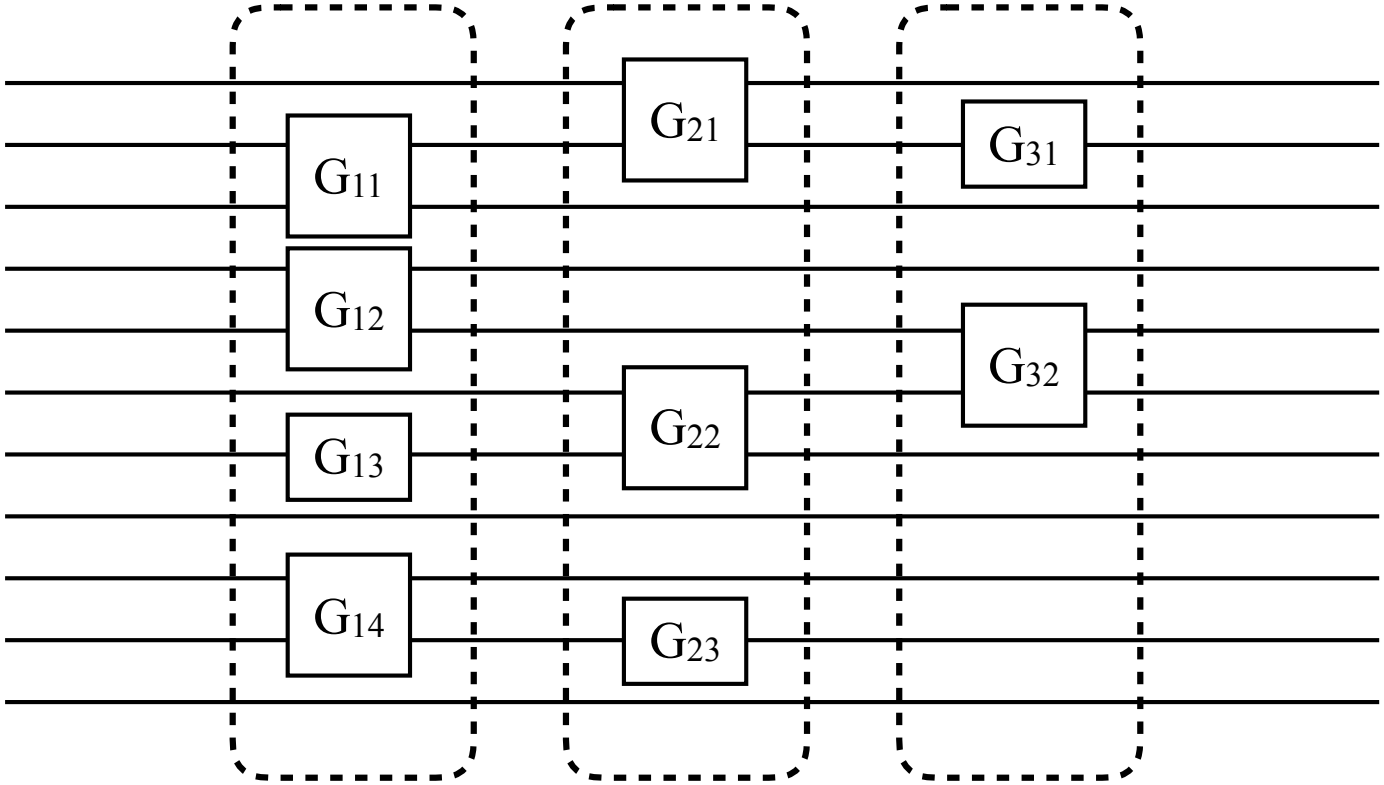
Using {H, S, T, CNOT},
each operator U on a quantum register
can be approximated with arbitrary precision.

Solovay-Kitaev Theorem (1997)

Assumption: This implementation is acceptable.

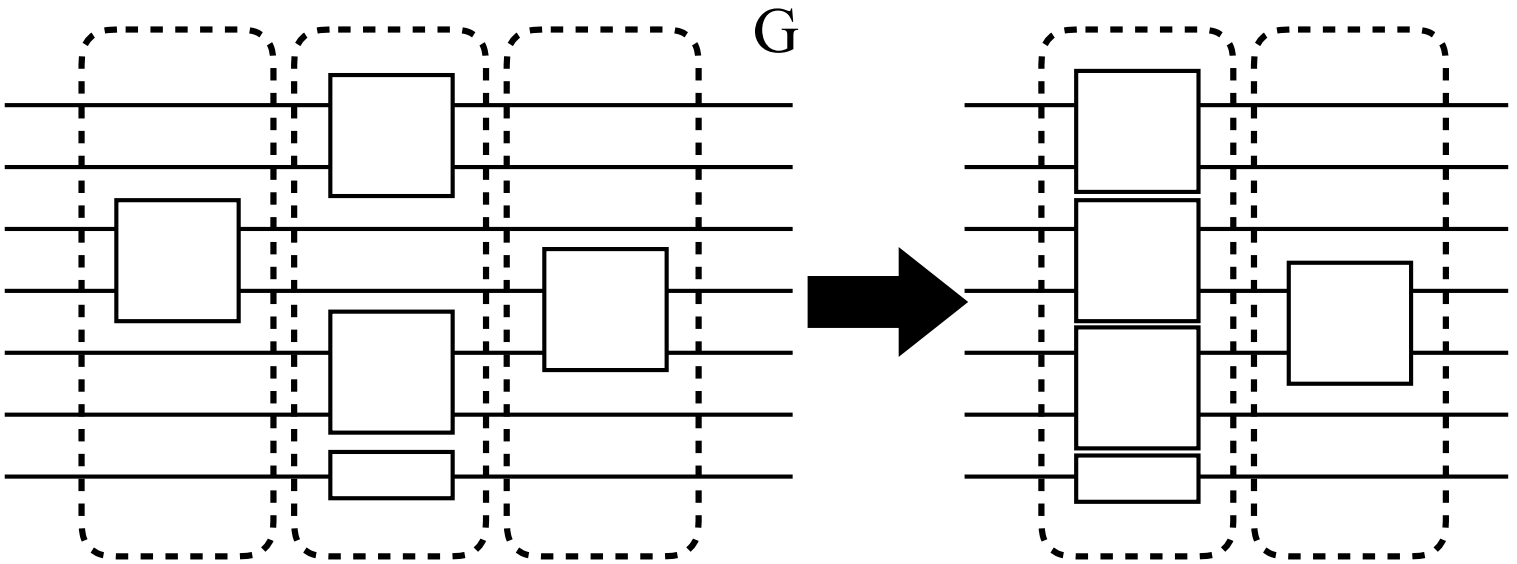
Depth of an Algorithm (a.k.a. Quantum Circuit)

The *depth* of a quantum circuit is the number of layers of 1- or 2-qbit gates that operate in parallel on disjoint qbits.



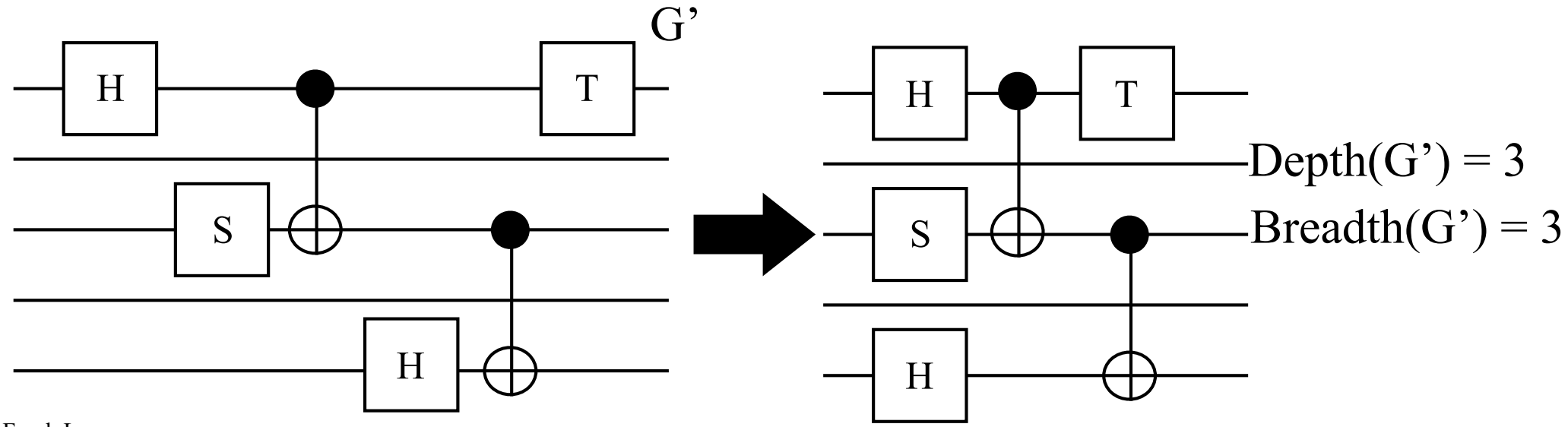
The *breadth* of a quantum circuit is the number of manipulated qbits.

Examples



Depth(G) = 2

Breadth(G) = 7



Depth(G') = 3

Breadth(G') = 3

Noise

Quantum operators are typically implemented by rotation operators

$$\text{E.g.:} \quad H = i \cdot R_z(\pi) \cdot R_y\left(-\frac{\pi}{2}\right) \cdot R_z(0)$$

Typically, these are rotations by non-rational angels

Such rotations cannot be performed precisely

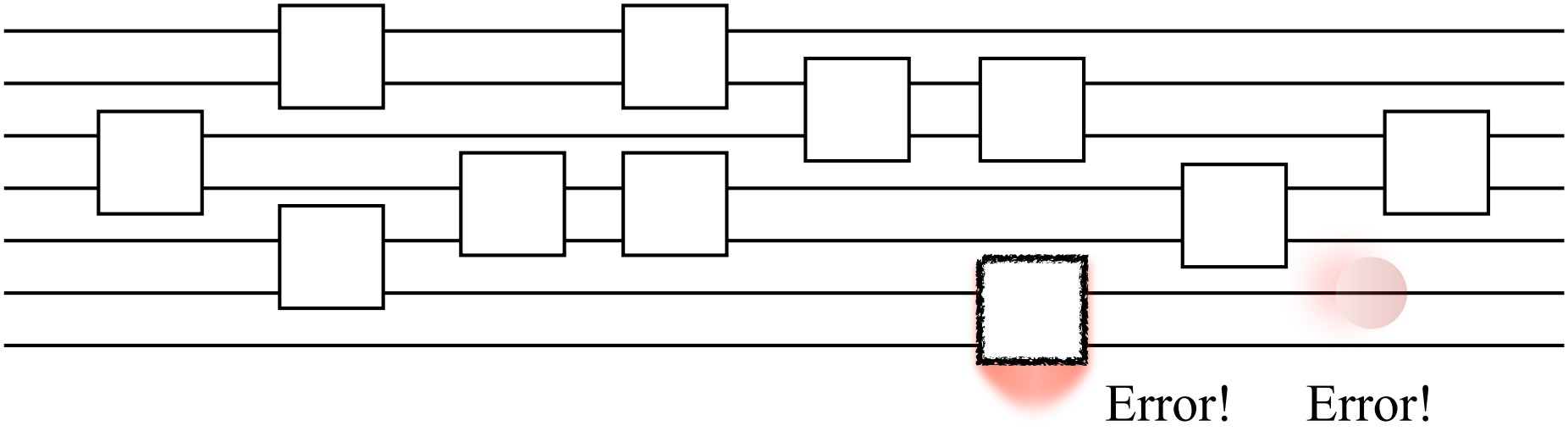
$\Rightarrow$ Quantum operators are typically *noisy* (i.e. erroneous)

Qbits are typically interacting with their environment, i.e. they are unstable

$\Rightarrow$ Qbits "decay" over time (*decoherence*)

$\Rightarrow$ A quantum algorithm cannot per performed for an arbitrary long time, i.e. it cannot contain arbitrary many steps

Noisy Algorithms



Rough estimation of the "size" of a quantum algorithm
that can be performed without errors:

$$wd \ll \frac{1}{\varepsilon}$$

w: width
d: depth
ε: error rate

<u>But</u>: See "Error Correction" later!

Consequences

$$wd \ll \frac{1}{\varepsilon}$$

Deep quantum algorithms $\Rightarrow$ few qbits
$\Rightarrow$ efficient classical simulation possible

Shallow quantum algorithms $\Rightarrow$ many qbits
$\Rightarrow$ potential for *quantum advantage*

See **NISQ** (Noisy Intermediate Scale Quantencomputing) later

Agenda

Basics in Quantum Physics

The Qbit

Quantum Register

Operators on Quantum Registers

Exponential Speedup

Search & Complexity

Cracking Keys

Encryption

Error Correction

NISQ

Conclusion

Problem

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

f *constant* $:\Leftrightarrow \quad \forall\, x, y \in \{0,1\}^n : f(x) = f(y)$

f *balanced* $:\Leftrightarrow \quad \operatorname{card} f^{-1}(0) = 2^{n-1} = \operatorname{card} f^{-1}(1)$

(f maps half of the domain to 0, the other half to 1)

Problem:
Determine with a minimum number of evaluations of f whether f is constant or balanced!

Classical Case

In the classical case, even after having read half (i.e. 2^{n-1}) values it's not clear whether f is constant or balanced

Example:
All values read are 0, but the next value
(i.e. the $(2^{n-1}+1)$-th value) is $1 \Rightarrow$ f balanciert;
or the next value is $0 \Rightarrow$ f konstant.

I.e. a classical (deterministic) algorithm requires (worst case) $2^{n-1}+1$ evaluations of f

"Oracle"

$$U_f : {}_2H^{\otimes n} \otimes {}_2H \rightarrow {}_2H^{\otimes n} \otimes {}_2H$$

$$|x, y> \ \mapsto \ |x, y \oplus f(x)>$$

($|x\rangle$ is an n-Qbit-Quatum Register)

U_f is unitary

Algorithm of Deutsch-Jozsa

Step 1: Initialize the register

$$|x\rangle|y\rangle \leftarrow |0\rangle^{\otimes n}|1\rangle$$

Step 2: Apply the Hadamard Transformation

$$|x\rangle|y\rangle \leftarrow H^{\otimes(n+1)}\left(|0\rangle^{\otimes n}|1\rangle\right)$$

Step 3: Evaluate f

$$|x\rangle|y\rangle \leftarrow U_f\left(|x\rangle|y\rangle\right)$$

U_f will be executed exactly once!

Step 4: Apply the Hadamard Transformation

$$|x\rangle \leftarrow H^{\otimes n}|x\rangle$$

Step 5: Measure

$$|x\rangle = |0\cdots0\rangle \Rightarrow \text{ f is constant}$$

$$|x\rangle \neq |0\cdots0\rangle \Rightarrow \text{ f is balanced}$$

Meaning

The algorithm evaluates f exactly once!

In the classical case, f has to be evaluated
(worst case) $2^{n-1}+1$ times!

The quantum algorithm of Deutsch-Jozsa
results in an exponential speedup!

Quantum Parallelism

$$U_f\left(H\left(\left|0\right\rangle^{\otimes n}\right)\left|0\right\rangle\right)=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\left|x\right\rangle\left|f(x)\right\rangle$$

This is "quantum parallelism"

Agenda

Basics in Quantum Physics

The Qbit

Quantum Register

Operators on Quantum Registers

Exponential Speedup

Search & Complexity

Cracking Keys

Encryption

Error Correction

NISQ

Conclusion

Algorithm of Grover

We want to find out to whom a certain phone number belongs.
Alphabetic order of phone book doesn't help!

Classical unstructured search is O(N)

There is a quantum algorithm that solves the problem in

$$G(N) = \frac{\pi}{4}\sqrt{N} = O\left(\sqrt{N}\right)$$

$\Rightarrow$ Quantum search results in quadratic speedup!

Application

Quantum search can speed-up (selective*) NP-problems

"Just" list all possible solutions and build a "database" out of them

Then use Grover algorithm to determine in $O(\sqrt{N})$ the solution

(*) You can define an oracle function for the problem
(which can be done for cracking keys, traveling salesman,…)

Bounded Error Quantum Polynomial Time (BQP)

A problem is *Bounded Error Quantum Polynomial time* (BQP) if it can be solved on a quantum computer with error probability $\leq \frac{1}{2} - \varepsilon$

BQP is for quantum computing what P is for classical computing!

- Let A be a BQP algorithm
- Let A' be the following algorithm:
  - A is repeated N times
  - The result with highest frequency will be output

Chernoff Bound

The probability to output the correct result increases exponentially with the number N of repetitions

$$P\left(\text{wrong majority}\right) \leq e^{-2N\varepsilon^2}$$

(Chernoff Bound)

Success Amplification

Let ω be the maximal probability to accept a wrong result.

After $N \geq \frac{1}{2\varepsilon^2} \ln \frac{1}{\omega}$ repetitions of a BQP algorithm
the result is correct with probability $1 - \omega$

Example: ε=1/4, ω=1/1000 ⇒ N=56
⇒ After 56 repetitions the result is correct with probability 99.99%

Agenda

Basics in Quantum Physics

The Qbit

Quantum Register

Operators on Quantum Registers

Exponential Speedup

Search & Complexity

Cracking Keys

Encryption

Error Correction

NISQ

Conclusion

Prime Factorization

Every number $n \in \mathbb{N}$ can be uniquely written as product of prime numbers:

$$\forall\, n \in \mathbb{N}\ \exists\, p_1,...,p_{k(n)} \in \mathbf{P}\ \exists\, i_1,...,i_{k(n)} \in \mathbb{N} : n = p_1^{i_1} \cdot ... \cdot p_{k(n)}^{i_{k(n)}}$$

with $i_1,\ldots,i_{k(n)} > 0$, $p_i \neq p_j$ for $i \neq j$ and **P** is set of all prime numbers

If you need m bits to represent $n \in \mathbb{N}$ as binar number, then the best classical algorithm for factorization of n requires the runtime

$$\Omega\left(2^{\sqrt[3]{m}}\right)$$

Periodic Functions

$f : \mathbb{N}_0 \to \mathbb{N}_0$ is called *periodic* $:\Leftrightarrow \exists\, k \in \mathbb{N}\ \forall\, x \in \mathbb{N}_0 : f(x) = f(x+k)$

$k \in \mathbb{N}$ is called *period* of f $:\Leftrightarrow$ k is minimal

I.e. if f(x+k') = f(x) for k' then k'>k

Example: Define $f(x) = 2^x \bmod 5$

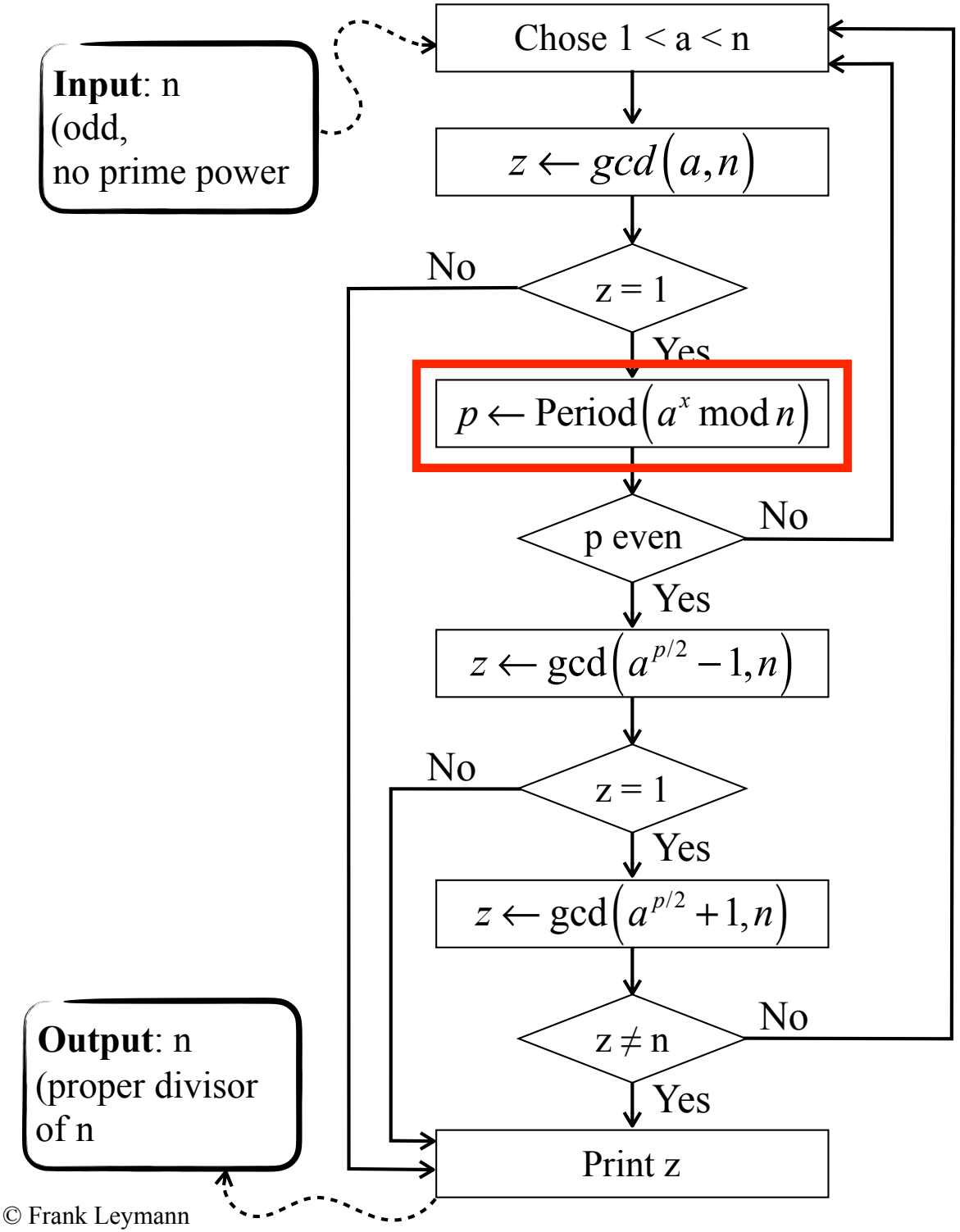
x	0	1	2	3	4	5	6	7	…
f(x)	1	2	4	3	1	2	4	3	…

$$f(4+x) = 2^4 \cdot 2^x \bmod 5 = 1 \cdot 2^x \bmod 5 = f(x)$$

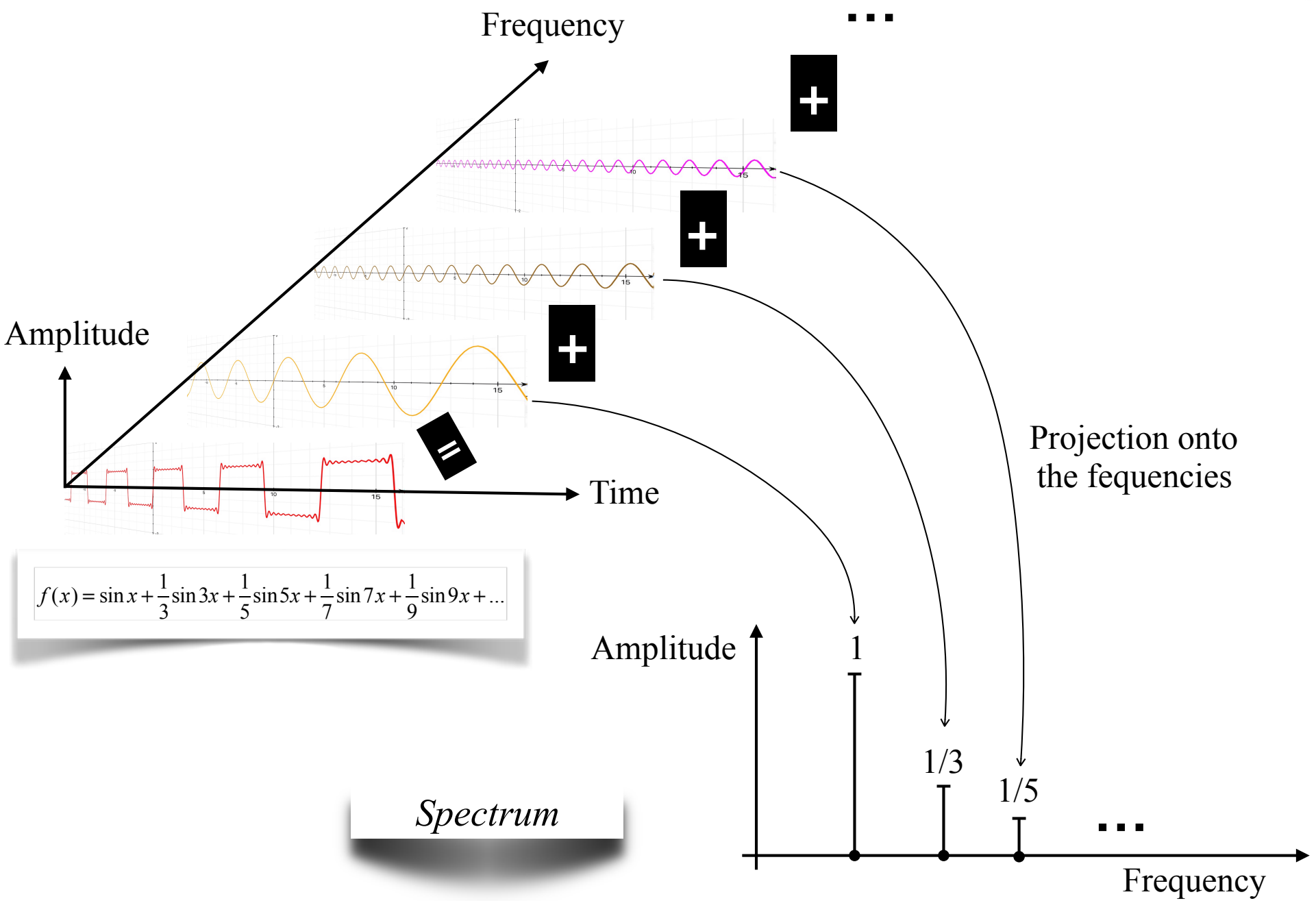
$\Rightarrow$ f has period 4

Now: chose $0 < a < n$ and define **$f(x) := a^x \bmod n$**

Shor's Algorithm



- If you know the period…
  - …you'll find a proper divisor within k runs with probability $\geq(1 - 1/2^k)$
- Overall runtime is $O((\log n)^4)$



Determining the spectrum of a function is called *Fourier-Transformation*

Discrete Fourier-Transformation

Often, the closed-form expression of a function f is not known, but only its values $f(t_0),\ldots,f(t_{N-1})$ at sampling points $t_0,\ldots,t_{N-1}$

Then, the Fourier-coefficients $c_k \approx \frac{1}{N}\sum_{n=0}^{N-1} f_n \cdot \omega_N^{k\cdot n}$

with equidistant sampling point $t_n = \frac{2\pi n}{N}$, $0 \le n \le N-1$,

with $\omega_N^k = e^{\frac{2\pi i}{N}\cdot k}$ (*complex N-th root of unity*) and $f(t_n)=f_n$

Quantum Fourier Transformation

$$QFT_N = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^{2\cdot 2} & \cdots & \omega_N^{2\cdot(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2\cdot(N-1)} & \cdots & \omega_N^{(N-1)\cdot(N-1)} \end{pmatrix}$$

$$c_k = \frac{1}{N}\sum_{n=0}^{N-1} f_n \cdot \omega_N^{k\cdot n}$$

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{N-1} \end{pmatrix} = \frac{1}{N} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^{2\cdot 2} & \cdots & \omega_N^{2\cdot(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2\cdot(N-1)} & \cdots & \omega_N^{(N-1)\cdot(N-1)} \end{pmatrix} \cdot \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ \vdots \\ f_{N-1} \end{pmatrix}$$

$\Rightarrow$ Fourier-Transformation becomes matrix multiplication!

Shor Algorithm: Details

Step 1: Initialize Qbit-Register

$$R = |a\rangle|b\rangle \leftarrow |0...0\rangle|0...0\rangle$$

Step 2: Apply Hadamard Transformation to |a>

$$R \leftarrow H^{\otimes n} \otimes I\left(|0\rangle|0\rangle\right) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle$$

Step 3: Apply Oracle Function

$$R \leftarrow U_f\left(R\right) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle$$

Step 4: Apply Quanten Fourier Transformation to |a>

$$|a\rangle \leftarrow \mathrm{QFT}_N\left(|a\rangle\right)$$

Step 5: y ← Measure |a>

Quantum Part

Step 6: Expand y as "Continued Fraction" $[y_0;y_1,\ldots,y_n]$

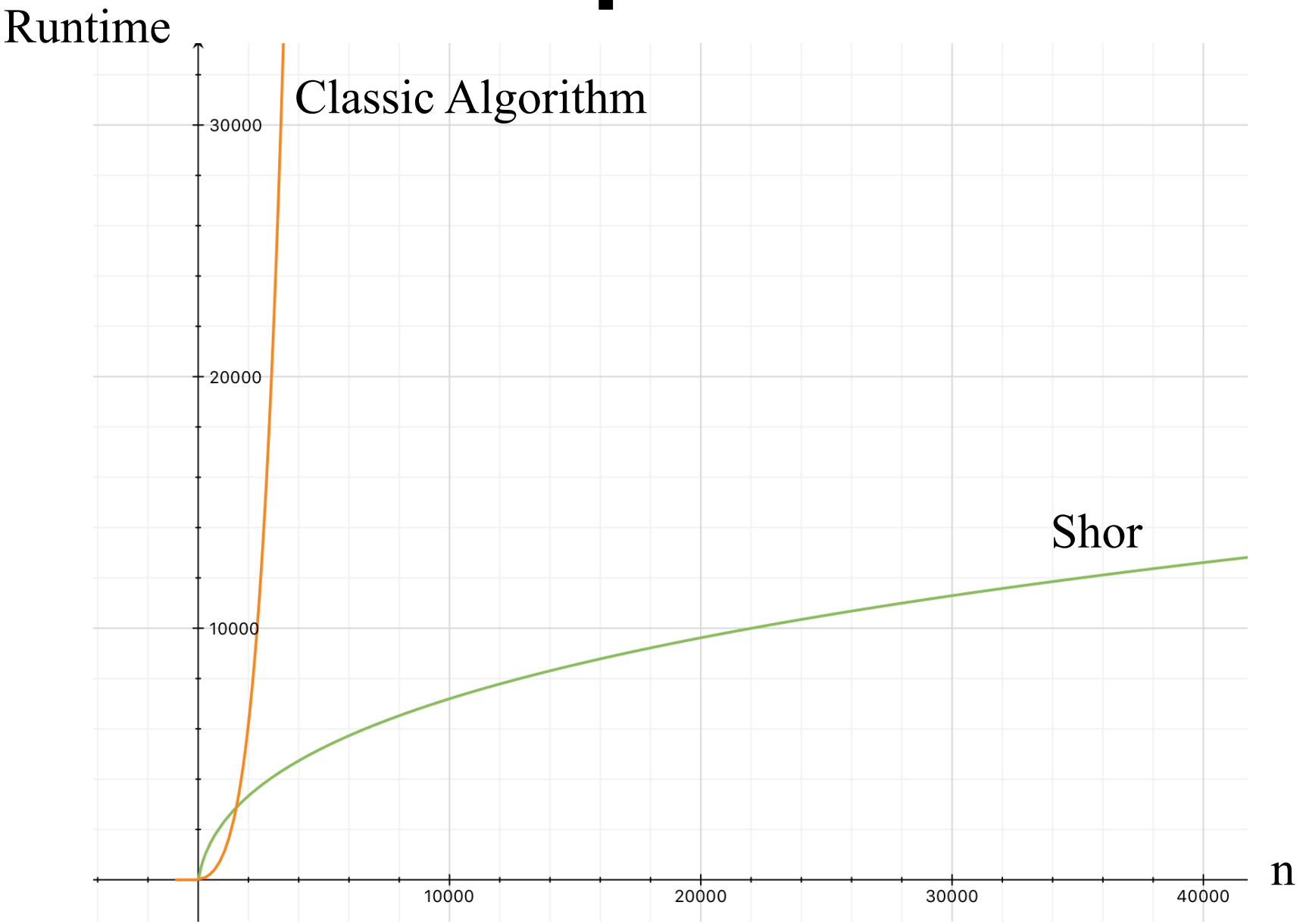
Step 7: p ← Determine p from convergents(*) $[y_0;y_1,\ldots,y_k]$, $k \leq n$

Step 8: Output of p

Classical Part

(*) initial segments

Comparison



Agenda

Basics in Quantum Physics

The Qbit

Quantum Register

Operators on Quantum Registers

Exponential Speedup

Search & Complexity

Cracking Keys

Encryption

Error Correction

NISQ

Conclusion

One-Time-Pad

- Let $m = a_1 \ldots a_m$ be the message to be exchanged as bit-string (*clear text*)

→ **Key generation**

- $k = k_1 \ldots k_m$ be a random bit string (*key*) of same size

→ **Encryption**

- $c = a_1 \oplus k_1 \ldots a_m \oplus k_m = c_1 \ldots c_m$ is the encrypted message (*crypto text*)

→ **Decryption**

- $m = c_1 \oplus k_1 \ldots c_m \oplus k_m = a_1 \ldots a_m$ is the original clear text

  because: $c_i \oplus k_i = a_i \oplus k_i \oplus k_i = a_i$

Mechanics

Attacker cannot copy the qbit ("no cloning")!

- Sender generates a sequence of random bits
- Each such bit is encoded as qbit in a randomly selected quantum basis
- Recipient decodes qbit by measuring it in a randomly selected quantum basis
- Sender and recipient exchange for each qbit in which basis it was en-/decoded
- Qbits treated by same basis result in bits of the key - other bits are destroyed
- Sender and recipient exchange subset of identified key bits to detect attacks

→ Too many attacks, i.e. too many differently identified key bits
⇒ Destroy complete key

→ Otherwise: use the key

Result

- Attack on a single qbit can be detected with probability 1/4
- Attack on many qbits can be detected with nearly 100% probability

$\Rightarrow$ Generation of long keys by means of quantum channels is secure!

This property of quantum cryptography has no classical correspondence

Because of the possibility of a secure distribution of keys, one-time-pad becomes practicable

Agenda

Basics in Quantum Physics

The Qbit

Quantum Register

Operators on Quantum Registers

Exponential Speedup

Search & Complexity

Cracking Keys

Encryption

Error Correction

NISQ

Conclusion

Non-Applicability of Classical Error Correction

Redundant codes (copies of qbits) cannot be created: **No-Cloning**!

A qbit will not change in a discrete manner (0 to 1, 1 to 0), but the amplitudes of superposition can be changed arbitrarily: **Continuous Errors**!

Reading means measurement, but this destroys the state, i.e. recovery of the original state is impossible: **Destructive Reads**!

Physical/Logical Qbits

Bit-Flip Error:

Qbit in state ψ is changed into $X\psi$ (Pauli Matrix X): X(a|0>+b|1>) = b|0>+a|1>

Phase-Flip Error:

Qbit in state ψ is changed into $Z\psi$ (Pauli Matrix Z): Z(a|0>+b|1>) = a|0> - b|1>

…etc …

Encoding ***1*** qbit by ***9*** qbits allows to detect and correct any (bit single) error!

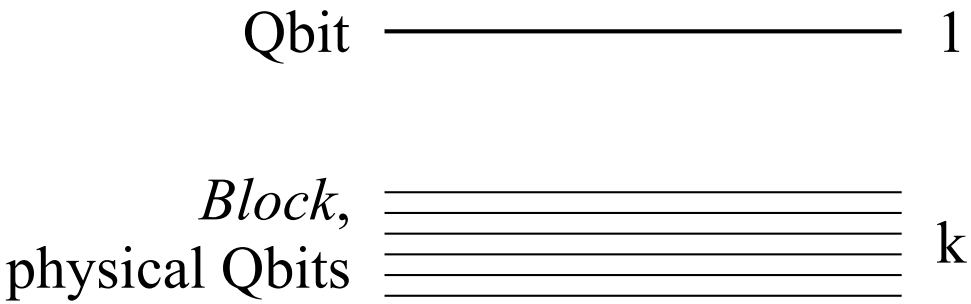
$$|0\rangle \mapsto \frac{(|000\rangle+|111\rangle)\cdot(|000\rangle+|111\rangle)\cdot(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \mapsto \frac{(|000\rangle-|111\rangle)\cdot(|000\rangle-|111\rangle)\cdot(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

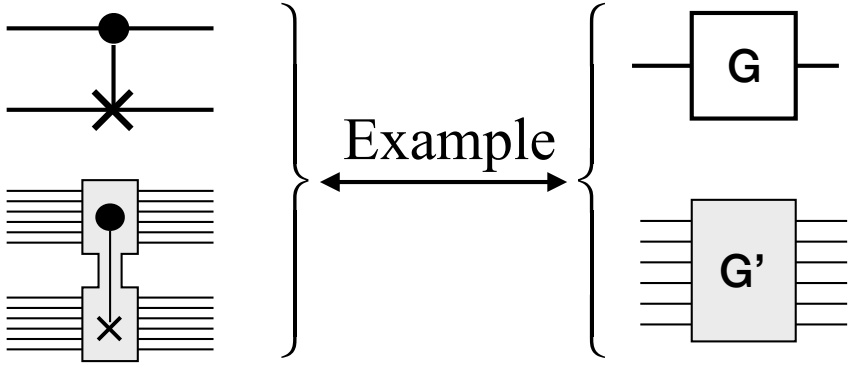
…and other encodings are possible. But:

N noisy "physical" qbits are needed to realize 1 stable "logical" qbit!

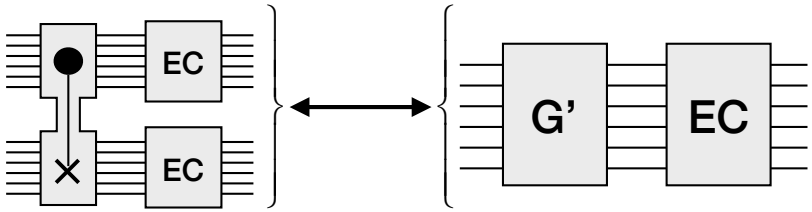
But Gates May Fail Too



1 Qbit is encoded by
k error-correcting Qbits



Universal gate G is substituted
by a *coded gate* G'
(coded gate G' ist quantum subroutine
implementing the functionality of G)



After executing a coded gate, error
correction on affected blocks are run

Agenda

Basics in Quantum Physics

The Qbit

Quantum Register

Operators on Quantum Registers

Exponential Speedup

Search & Complexity

Cracking Keys

Encryption

Error Correction

NISQ

Conclusion

Technological Problems

Decoherence : Qbits are unstable

⇒ State of a qbit decays over time (often fast!)

→ Implementations of qbits even results in disturbances

⇒ Increasing number of qbits is difficult

Gate Fidelity : individual operations are (a bit) imprecise

⇒ Error of an algorithm increases with number of operations

⇒ Only algorithms with "a few" operations can be correctly performed

Readout Error: Measuring a qbit is imprecise

⇒ Results are distorted

Qbit Connectivity : Not all qbits have a physical connection

⇒ 2-qbit operations cannot be performed on arbitrary pairs of qbits

→ Reminder: 2-qbit operations are key for universal sets of operations

⇒ Additional SWAP operations needed

⇒ Number of operations to implement an algorithm increases

What is NISQ?

…attempt to do meaningful quantum computing in such a noisy situation!

NISQ (noisy intermediate-scale quantum) **Technology** uses these…

- 50..100 Qbits
- with a limited number of operations in algorithms

…to provide significant proof of quantum supremacy

Problem: Classical computer get more powerful over time, i.e. the number of qbits and number of reliably performed gates must be adapted to proof quantum supremacy

Quanten Computer vs Super Computer

Quanten Computer are significantly more energy-efficient
than super computers

Hardware of Quanten Computer is significantly cheaper
than a super computer

- One hour compute time on a QC can be offered for about 200€

⇒ Even for problems that a classical super computer may solve faster,
a QC may be more appropriate

Entanglement Threshold

Quantum states that are thus complex (because of entanglement) that they cannot be simulated on a digital computer

Indicators for *quantum advantage*:

1. There are problems that are hard to solve on a classical computer, but easy to solve on a quantum computer (e.g. factorization).
2. Even on the largest classical computer, a general quantum computer cannot be simulated (while a quantum computer can easily do everything that a classical computer can do)
3. There are problems that can only be solved on a quantum computer

50 Qbit Threshold

Even with todays(*) most powerful classical computers, a quantum computer with 50 qbit can not be simulated

A 50 Qbit quantum computer is already available to selected user groups ("intermediate-scale")

But: these qbits are noisy, i.e. there usability is limited (precision of operations, number of sequentially executed operations,…)

⇒ No practical use of quantum error correction yet

"*Error Proneness*": No more than about 1000 basic 2-qbit operations can be performed in sequence

⇒ Limitation of NISQ Technology

(*) 2019

Hybrid Architecture

For the next foreseeable time, Quantum Computer will be "special computers" offered in the cloud

$\Rightarrow$ Software Architecture is "hybrid"
(*Quantum Variational*)

Example:

General paradigm for optimization problems:

- Compute a quantum state on a QC
- Measure the qbits
- Process the measured results on a classical computer
- Derive indicators for improving the quantum state

Iterate this cycle until quantum state converges, and derive approximate solution from this

QAOA : Quantum Approximate Optimization Algorithm

Promising NISQ Applications

- Deep learning
- Matrix inversion
- Recommender
- Semidefinite programming (e.g. SVM)
- Simulation
- …

Agenda

Basics in Quantum Physics

The Qbit

Quantum Register

Operators on Quantum Registers

Exponential Speedup

Search & Complexity

Cracking Keys

Encryption

Error Correction

NISQ

Conclusion

PlanQK

Plattform und Ökosystem für Quantenunterstütze Künstliche Intelligenz

(Platform and Ecosystem for quantum supported Artificial Intelligence)

stone one
The Web Service Factory

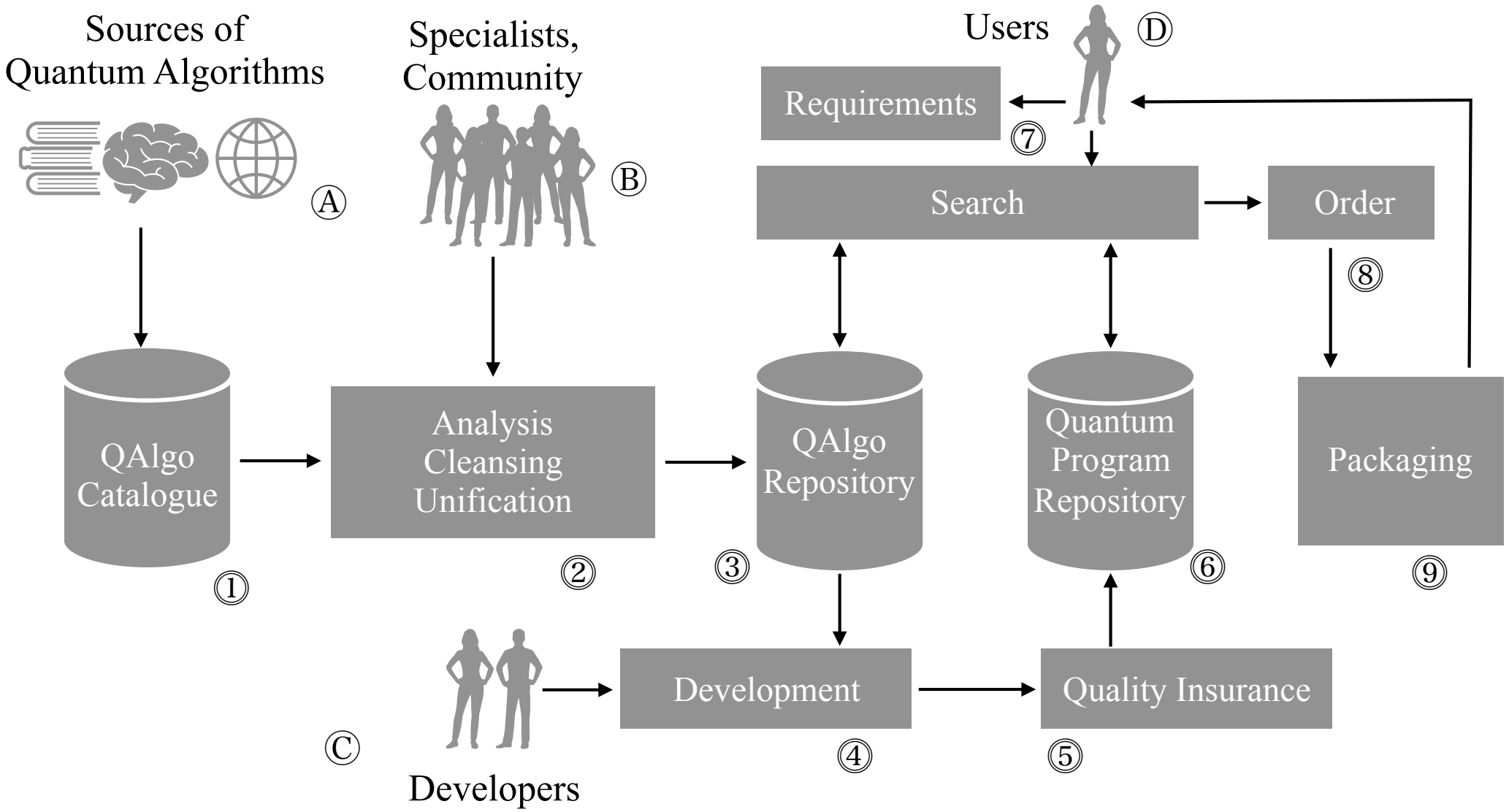
HQS QUANTUM SIMULATIONS

Universität Stuttgart

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Federal Ministry
for Economic Affairs
and Energy

Goals



Summary

- Quantum algorithms are very different from classical algorithms
  $\Rightarrow$ Very different skills are needed to solve problems with a QC
- The current state of the art of software for implementing quantum computing is at the assembler level
- Hardware of quantum computers is rapidly evolving $\Rightarrow$ In the next few years deep problems will very likely become solvable
- NISQ (and QC-implied skills) suggest to start now becoming acquainted with quantum technology

Quote by Enrico Fermi

I am still confused…

…but at a higher level!

End