Felix Gemeinhardt
Johannes Kepler University Linz
Institute for Business Informatics –
Software Engineering

Quantum Computing

From Fundamentals to first Quantum Algorithms

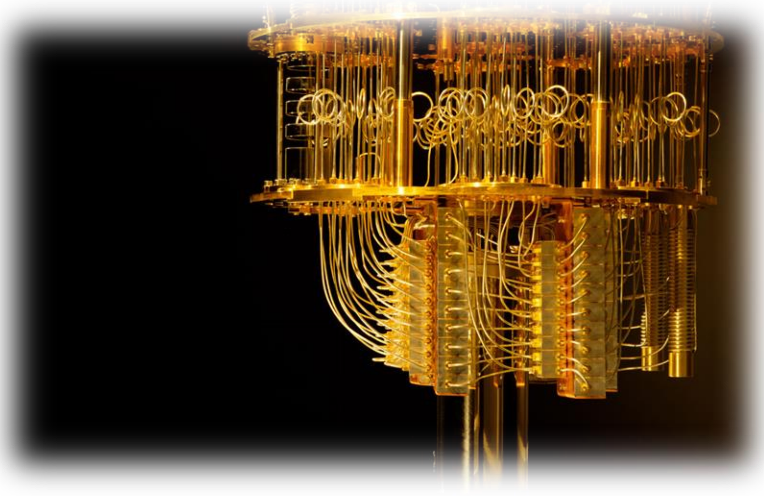
Disclaimer

- **This material, no matter whether in printed or electronic form, may be used for personal and non-commercial educational use only. Any reproduction of this material, no matter whether as a whole or in parts, no matter whether in printed or in electronic form, requires explicit prior acceptance of the authors.**

Agenda

Goal: Overview and basic understanding of working principles

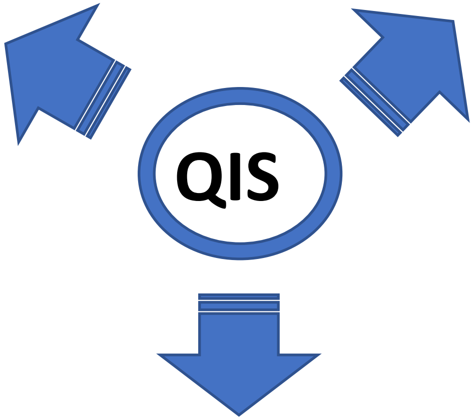
1. **Motivation** and Overview
2. Basic **Working Principles**
3. **Near-term** Applications
4. Simple Quantum **Algorithms**
5. **Challenges** and Limitations
6. Quantum **Software** Engineering



Overview and Motivation

Quantum Information Science (QIS)

Computer Science

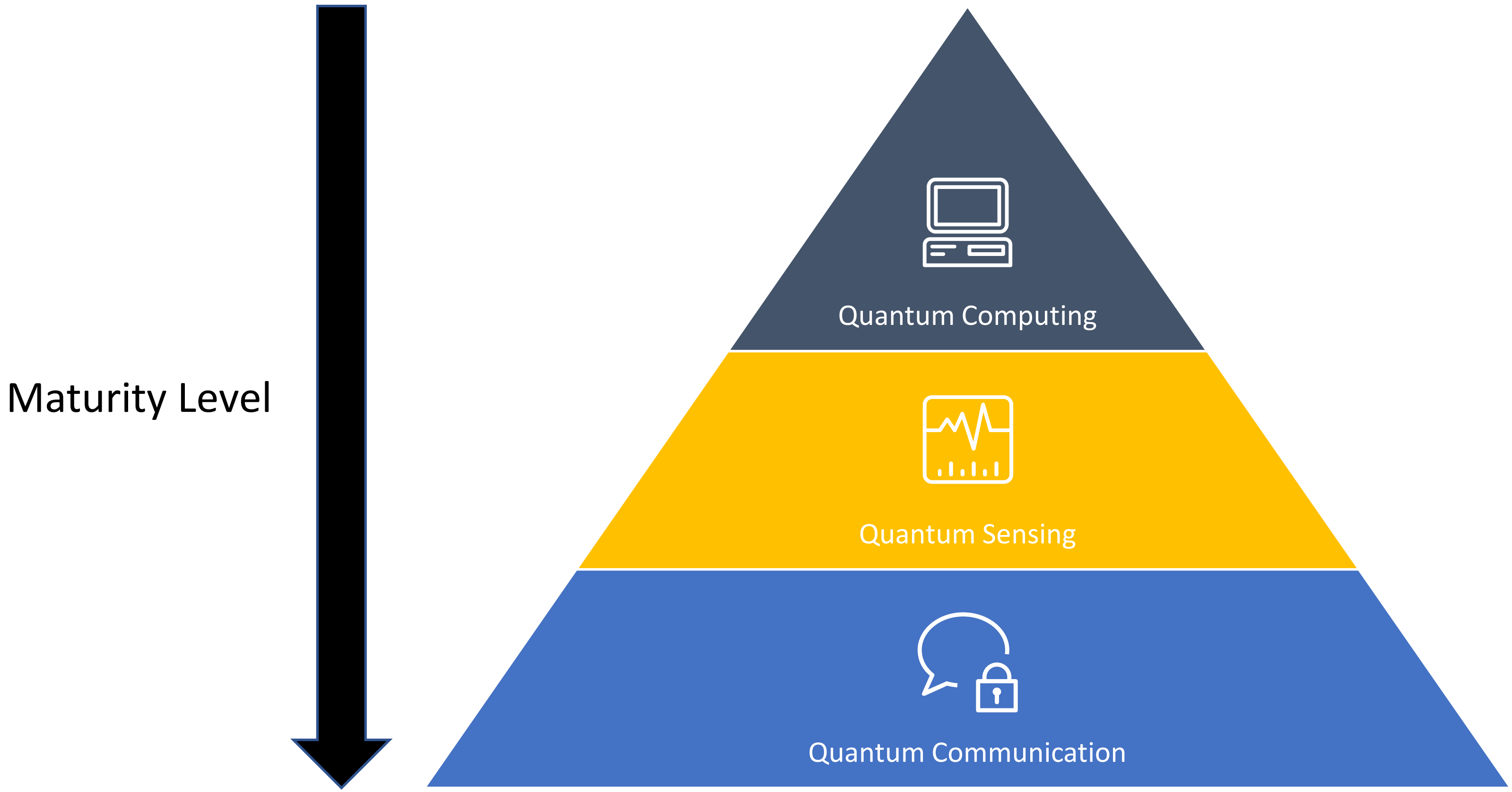


Information Theory

Quantum Mechanics

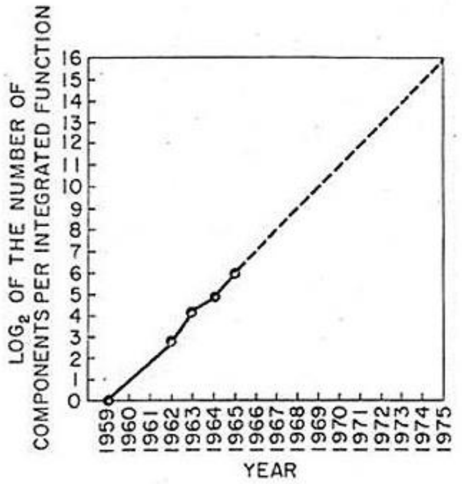
- Emerged in the 1920s
- Inventions like: Transistors, Lasers and GPS

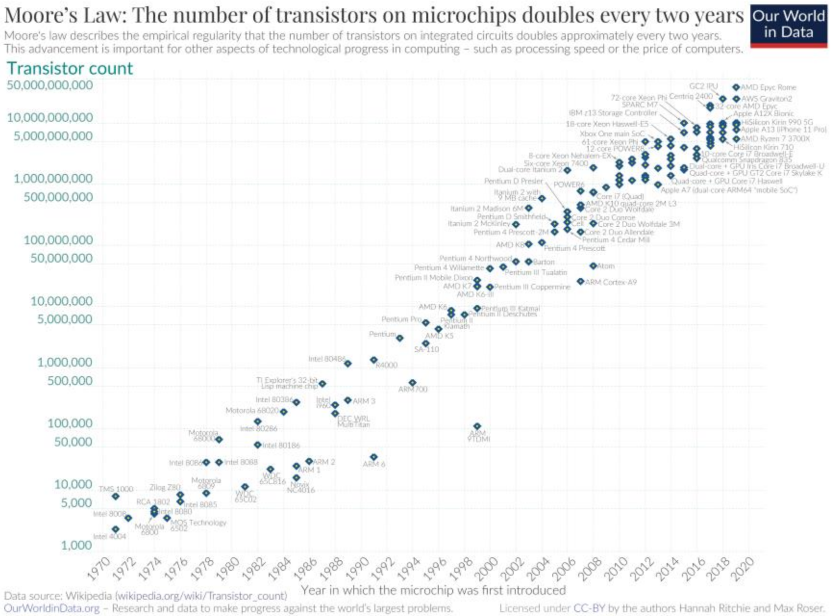
Quantum Technologies



Classical Computing: Limitations - Hardware

- **Limits of Moore´s law**
  - ➢ Doubling of transistor counts on microchips every 12-24 months
  - ➢ Physical limitations



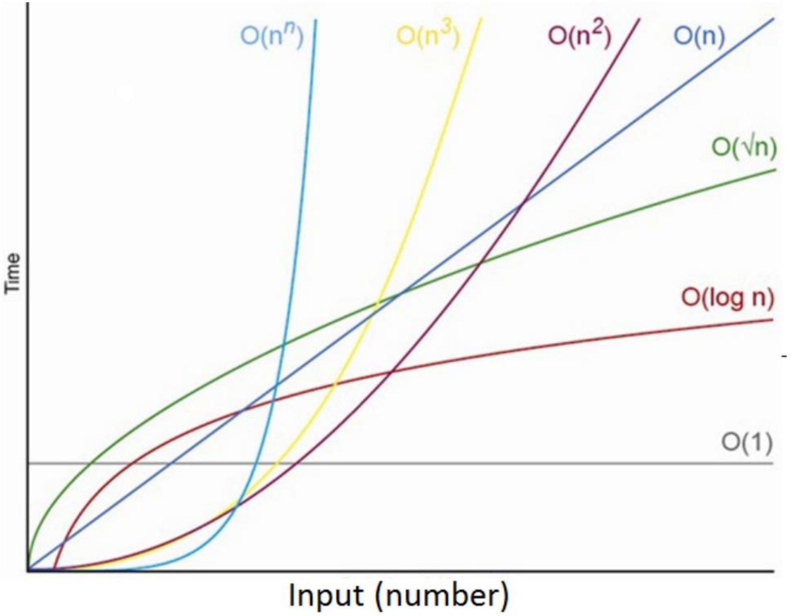


Source: https://web.archive.org/web/20211221191600/https://www.intel.com/pressroom/kits/events/moores_law_40th/index.htm?iid=tech_mooreslaw+body_presskit

Source: https://ourworldindata.org/technological-progress

Classical Computing: Limitations – Algorithms

- **Many complex problems are intractable for classical computing, e.g.:**
  - ➢ Exponentially growing search spaces
  - ➢ Simulation of quantum processes



Source: Hidary (2019). Quantum Computing: An Applied Approach

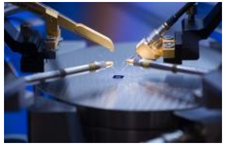
- **Best case:**
  - From O(n^n) to O(n)

Applications – from research to operations

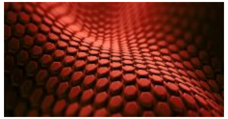
Research applications

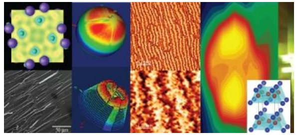

Batteries

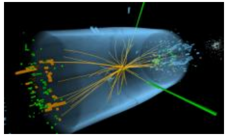

Drug discovery

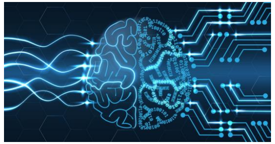

Semiconductors


Fertilizer production


Materials design


Condensed matter physics


High-energy
particle physics


Machine Learning

Operations applications


Transportation


Finance


Energy utilities


Telecoms


Manufacturing


Marketing

Current Limitations of Quantum Computing

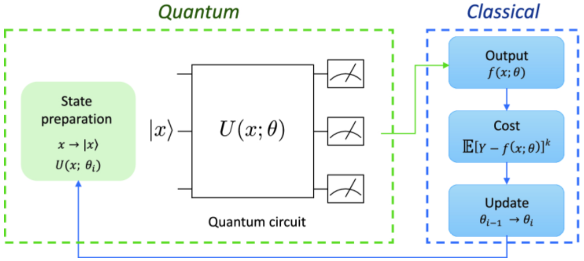
JOHANNES KEPLER UNIVERSITY LINZ

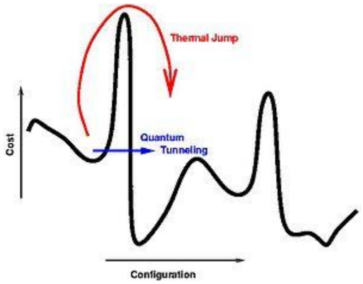
- **Technical Challenges:**
  - Error prone (coherence time)
  - Sensitivity to environment and to each other (noise)
  - Accuracy of Quantum Operations
  - …
- **Regimes**
  - Noisy Intermediate Scale Quantum (NISQ-era)
  - Fault-tolerant Quantum Computing

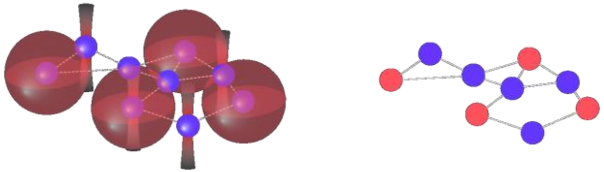
Preskill, J., 2018. Quantum computing in the NISQ era and beyond. *Quantum, 2,* p.79.

NISQ-Era

- **Variational Quantum Algorithms**
  - ➢ Similar to neural nets in ML
  - ➢ VQE, QAOA
  - ➢ Gate-based → sequencial programming
- **Quantum Annealing**
  - ➢ Encode optimization problem into energy of quantum system
  - ➢ System “wants” to stay in minimum
- **Quantum Simulators**
  - ➢ Encode problem into energy of quantum system
  - ➢ Different quantum phenomena

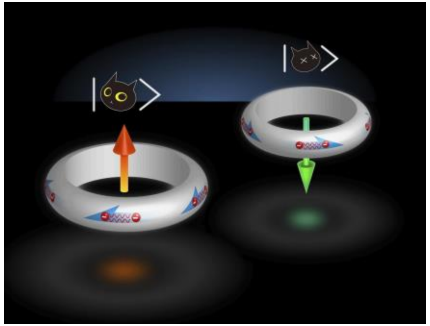






Quantum Computer – Hardware Architectures (1)

- **Photonics**
  - Photons are information carrier
  - Optical elements (mirrors, phase shifters) for manipulation
- **Superconductors**
  - Google, IBM, Rigetti,…
  - Electric current produces magnetic moment (spin)
  - Temperatures: mK
  - Microwave pulses for manipulation



Source: Johnston et. al (2019). Programming Quantum Computers

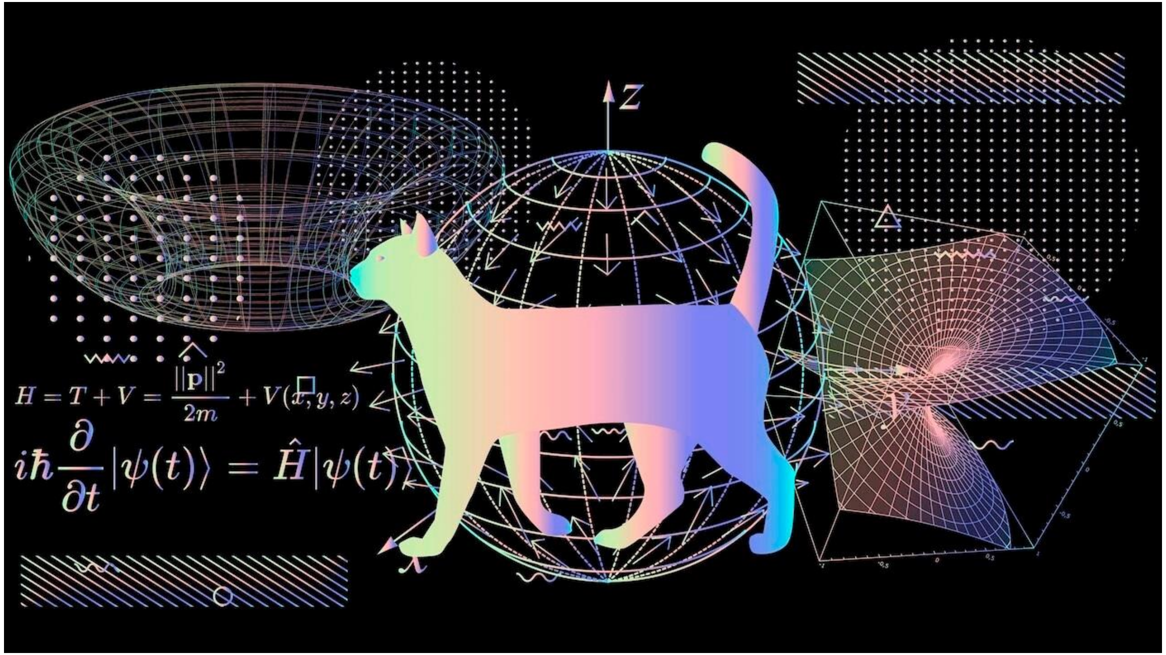
Quantum Computer – Hardware Architectures (2)

JOHANNES KEPLER UNIVERSITY LINZ

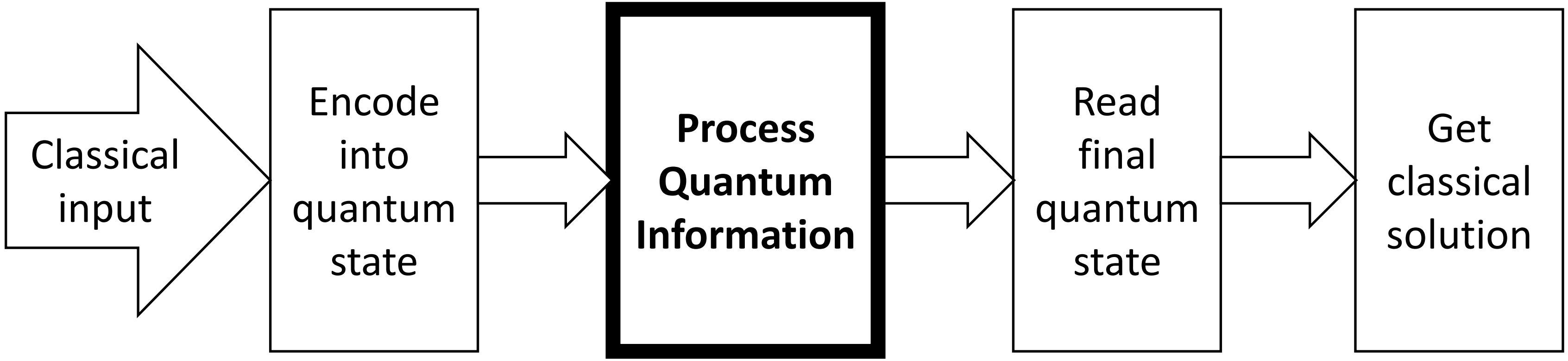
- **Trapped Ion**
  - Ions in electromagnetic field
  - Lasers for manipulation
- **And many more:**
  - Topological Quantum Computation
  - Silicon-based
  - …

All these approaches seek to make the jump to the next regime. To do this, they try to better model a Qubit.

Basic Working Principles



Quantum Information Processing – Pipeline

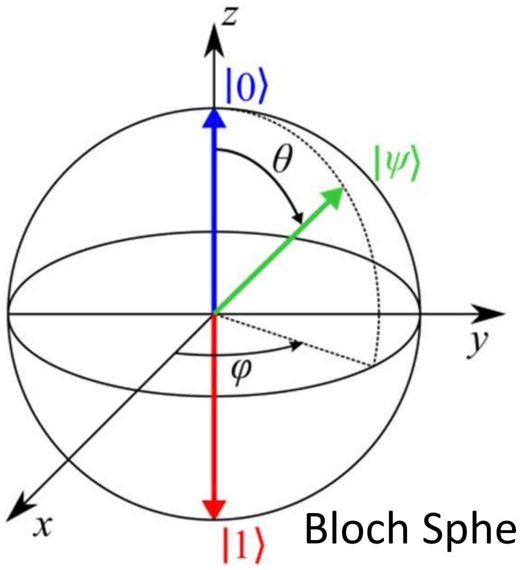


Basic Concepts – From Bits to Qubits

- A qubit is a **two-level** quantum mechanical system
- The **state** of the qubit at any given time can be represented by a **vector**

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

- Similar to classical bit 0,1 → $|0\rangle, |1\rangle$
- Can also be a mixture → **superposition**

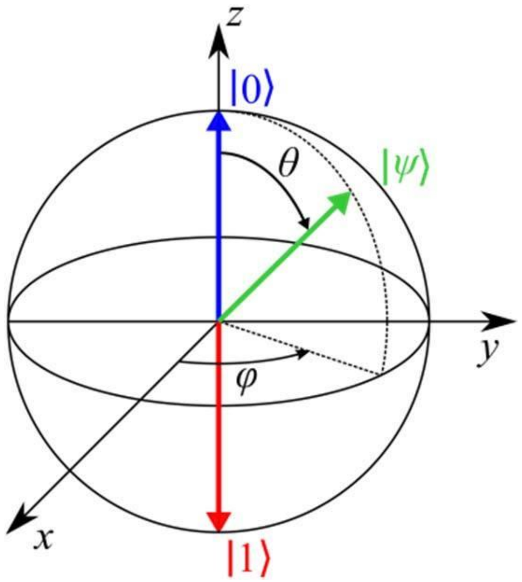


Bloch Sphere

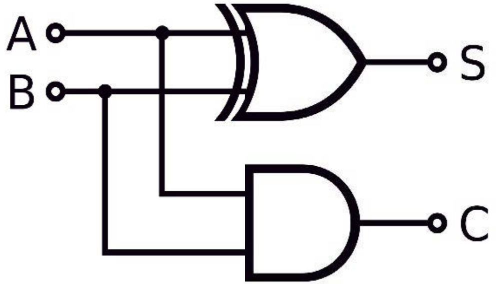
Phase

- Additional **degree of freedom** in quantum systems
- Often useful to **encode information** in the phase
- Can then be **transformed to amplitudes via QFT** → see later

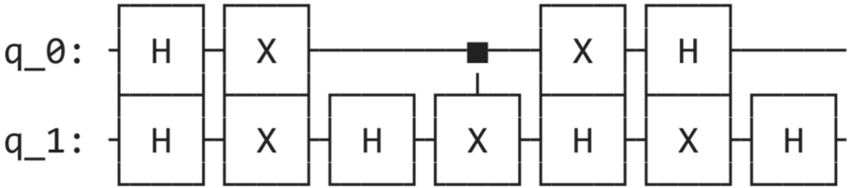
  → intuitively: transformation from φ to θ



- **Classical Computing Circuit**

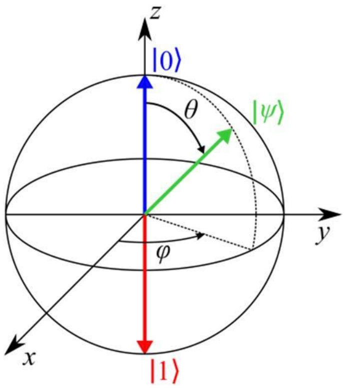


- **Quantum Computing Circuit**
  - Construct and read these diagrams from left to right
  - Input and output space are the same



Quantum Operator - Reversibility

- **Isolated quantum system**
  - Every quantum operation is reversible
  - Every quantum operation is unitary
    → describes rotation but no change in vector length



- **Reversibility**
  - $\boldsymbol{U}^{-\mathbf{1}}\boldsymbol{U}|\Psi\rangle = \boldsymbol{U}^{\dagger}\boldsymbol{U}|\Psi\rangle = |\Psi\rangle$
  - $\boldsymbol{U}^{\dagger}$ is U transposed and complex conjugated

Basic Concepts – From Classical to Quantum Operations

Properties	Classical Operations	Quantum Operations
Reversibility	✗ Only NOT operation	✓
Universality	1. Set{AND, NOT, OR, NAND, XOR, FANOUT} 2. Set{NAND}	1. Set {Toffoli, basis-changing unary operator with real coefficients (such as H)} 2. Set{CNOT, T, Hg} 3. Set{RX,RY,RZ,P,CNOT}

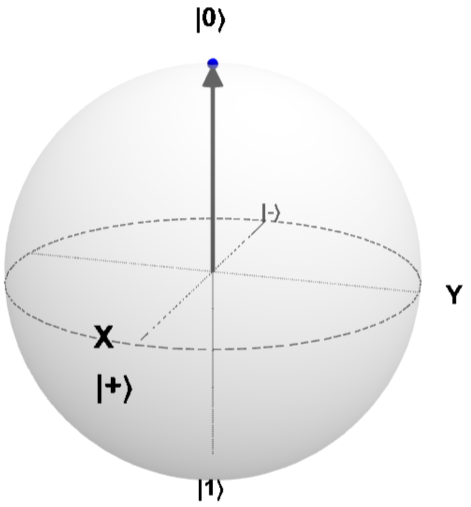
Basic Concepts – Quantum Operations

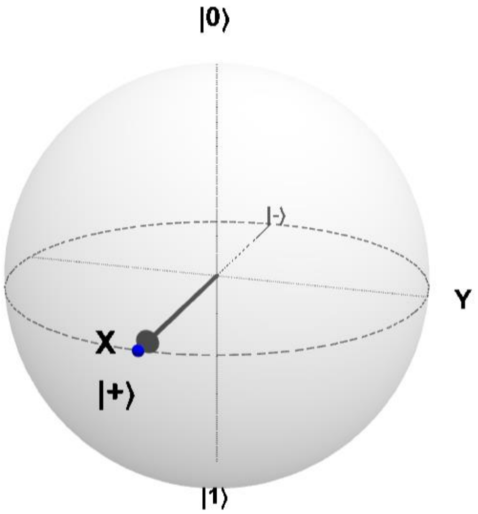
- Quantum Operations **manipulate the *state*** of the qubit
- Mathematically they are defined as a ***matrix***
- Unary Operators
  - One-qubit
- Binary Operators
  - Two qubit
- Ternary Operators
  - 3-qubit operators
- ...

Multi-Qubit Operations: involve more than 1-qubit

Quantum Operations – Unary Operator – Hadamard

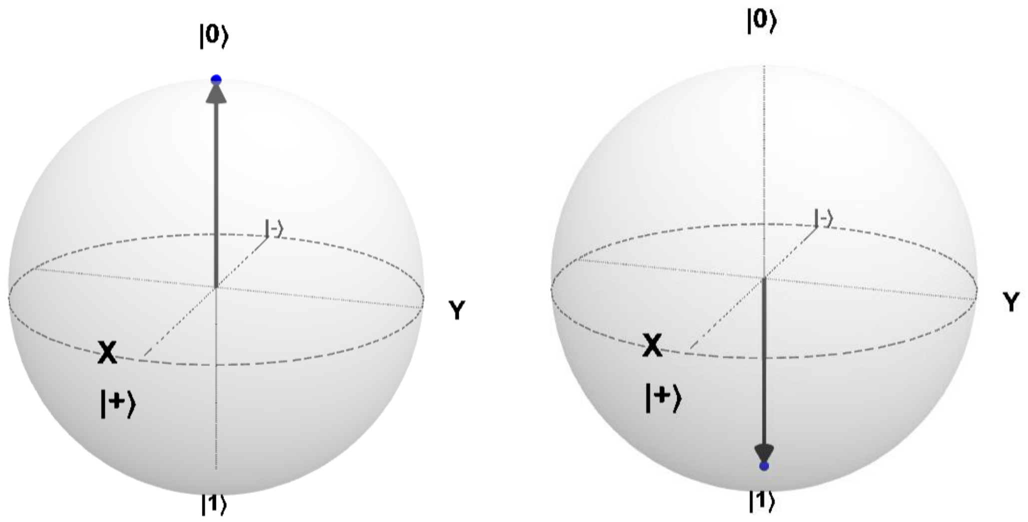
- Hadamard operator is *crucial* in quantum computing
- Takes a qubit into a superposition of two states
- Bloch Sphere:





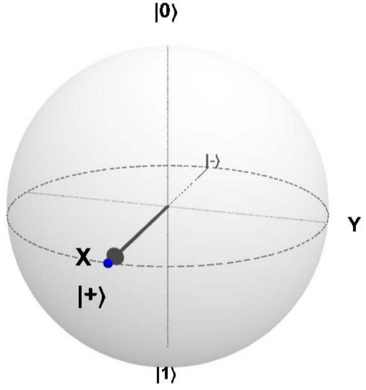
Quantum Operations – Unary Operations – Pauli X

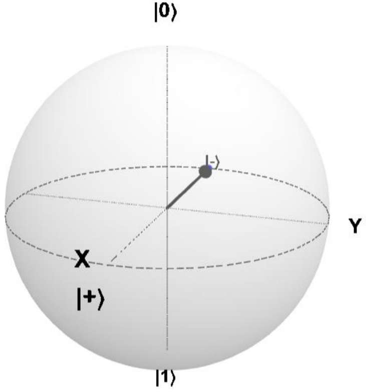
- Similar behavior like *Not* in classical computing
- Also known as *Not Gate*



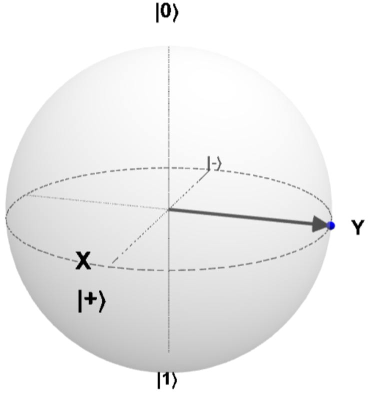
Quantum Operations – Unary Operations – Pauli Y & Z

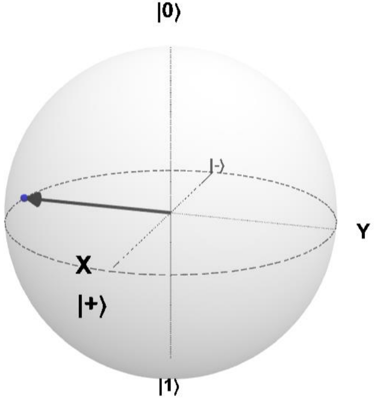
- Pauli Y





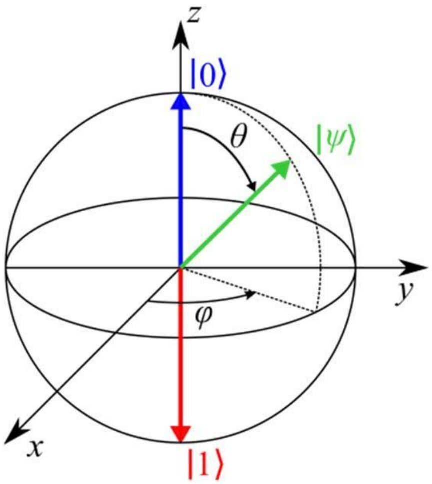
- Pauli Z





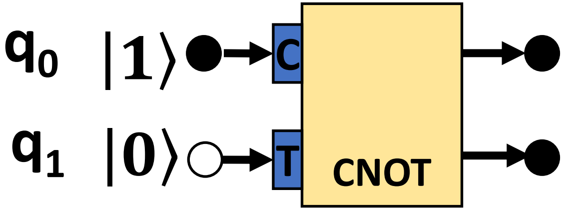
Single Qubit Gates – Parameterized Gates

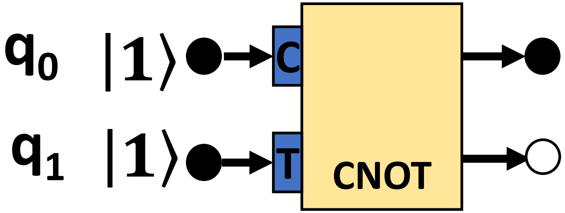
- **Bloch sphere rotations can be parametrized**
  - E.g., rotation of φ around z-axis
- **3 angles for any arbitrary rotation**
  - Euler’s rotation theorem
- **Examples:**
  - RX, RY, RZ



Quantum Operations – Binary Operator – CNOT

- Controlled-NOT (CNOT)
- First Qubit is the *control qubit*
- Second Qubit is the *target* qubit
- Examples





Mathematical Notation – Bra-ket Notation (1)

- Also known as: Dirac Notation

$$\langle \mathbf{0}| = \begin{pmatrix}\mathbf{1} & \mathbf{0}\end{pmatrix}, \ |\mathbf{0}\rangle = \begin{pmatrix}\mathbf{1}\\ \mathbf{0}\end{pmatrix} \qquad \langle \mathbf{1}| = \begin{pmatrix}\mathbf{0} & \mathbf{1}\end{pmatrix}, \quad |\mathbf{1}\rangle = \begin{pmatrix}\mathbf{0}\\ \mathbf{1}\end{pmatrix}$$

- Multi-qubit state representation

$$|\mathbf{00}\rangle = \begin{pmatrix}\mathbf{1}\\ \mathbf{0}\\ \mathbf{0}\\ \mathbf{0}\end{pmatrix} \ |\mathbf{01}\rangle = \begin{pmatrix}\mathbf{0}\\ \mathbf{1}\\ \mathbf{0}\\ \mathbf{0}\end{pmatrix} \ |\mathbf{10}\rangle = \begin{pmatrix}\mathbf{0}\\ \mathbf{0}\\ \mathbf{1}\\ \mathbf{0}\end{pmatrix} \ |\mathbf{11}\rangle = \begin{pmatrix}\mathbf{0}\\ \mathbf{0}\\ \mathbf{0}\\ \mathbf{1}\end{pmatrix}$$

Mathematical Notation – Bra-ket Notation (2)

- Quantum State: Bra-ket Notation

Amplitudes

$$|\psi\rangle = \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle \xrightarrow{\text{Normalization}} |\alpha|^2 + |\beta|^2 = \mathbf{1}$$

Ket

$$\langle\psi| = \alpha^*\langle\mathbf{0}| + \beta^*\langle\mathbf{1}|$$

Bra

- Superposition $\quad \boldsymbol{if} \begin{cases} \alpha \neq \mathbf{0} \\ \beta \neq \mathbf{0} \end{cases}$

Tensor Product

- Description of space for 2 (or multiple) qubits
- Notation $\bigotimes$
- 2-qubit-state example

Product state: $$\begin{pmatrix} \boldsymbol{a_1} \\ \boldsymbol{b_1} \end{pmatrix} \bigotimes \begin{pmatrix} \boldsymbol{a_2} \\ \boldsymbol{b_2} \end{pmatrix} = \begin{pmatrix} \boldsymbol{a_1} * \begin{pmatrix} \boldsymbol{a_2} \\ \boldsymbol{b_2} \end{pmatrix} \\ \boldsymbol{b_1} * \begin{pmatrix} \boldsymbol{a_2} \\ \boldsymbol{b_2} \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \boldsymbol{a_1 a_2} \\ \boldsymbol{a_1 b_2} \\ \boldsymbol{b_1 a_2} \\ \boldsymbol{b_1 b_2} \end{pmatrix} = \begin{pmatrix} \boldsymbol{a} \\ \boldsymbol{b} \\ \boldsymbol{c} \\ \boldsymbol{d} \end{pmatrix}$$

In general : $|\psi\rangle = \boldsymbol{a}|\mathbf{00}\rangle + \boldsymbol{b}|\mathbf{01}\rangle + \boldsymbol{c}|\mathbf{10}\rangle + \boldsymbol{d}|\mathbf{11}\rangle$

Condition for separability: $\frac{a}{b} = \frac{c}{d}$, otherwise: „**entangled**“

n qubits → length of vector: 2^n

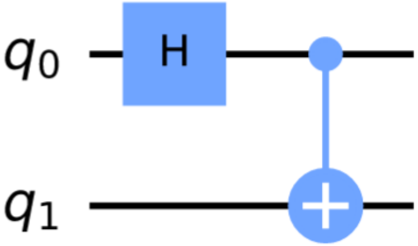
Basic Concepts – Entanglement

JOHANNES KEPLER UNIVERSITY LINZ

- **Correlation between states of qubits**
  - One can gain information about a qubits state by knowing the states of the other qubits
  - Non-entangled states can be simulated efficiently by classical computers → power of QC comes from entanglement
- **E.g.,: Bell States (completely entangled):**
  - $|\Psi_+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
  - $|\Psi_-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$
  - $|\Phi_+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$
  - $|\Phi_-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$

Multi-qubit gates – Entangled states

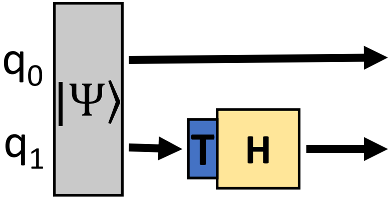
- **Consider the following example:**



- **H** $|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0+\rangle$
- **CNOT** $|0+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ → **Bell-state**

Multi-qubit gates – Mathematics

- **Example:**



- **Why not just H** $\begin{pmatrix} \boldsymbol{a_1} \\ \boldsymbol{b_1} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{pmatrix} \boldsymbol{a_1} \\ \boldsymbol{b_1} \end{pmatrix}$**? (→ Entanglement)**

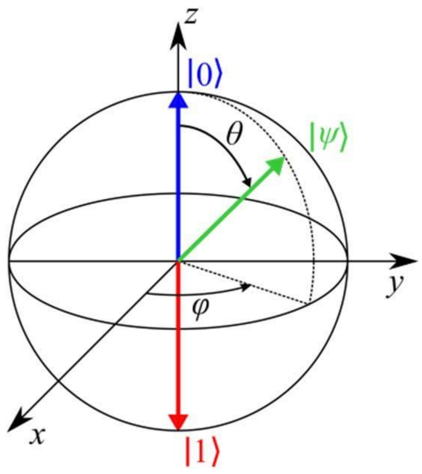
- **Tensor product: H ⊗ I** $= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & -1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix} =$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & -\mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & -\mathbf{1} \end{bmatrix}$$

Basic Concepts - Measurement

- **Measurement destroys superposition**
  - ➢ Non-reversible quantum operation
  - ➢ What was state before measurement?
- Probability distribution → Quantum state
- No-cloning theorem

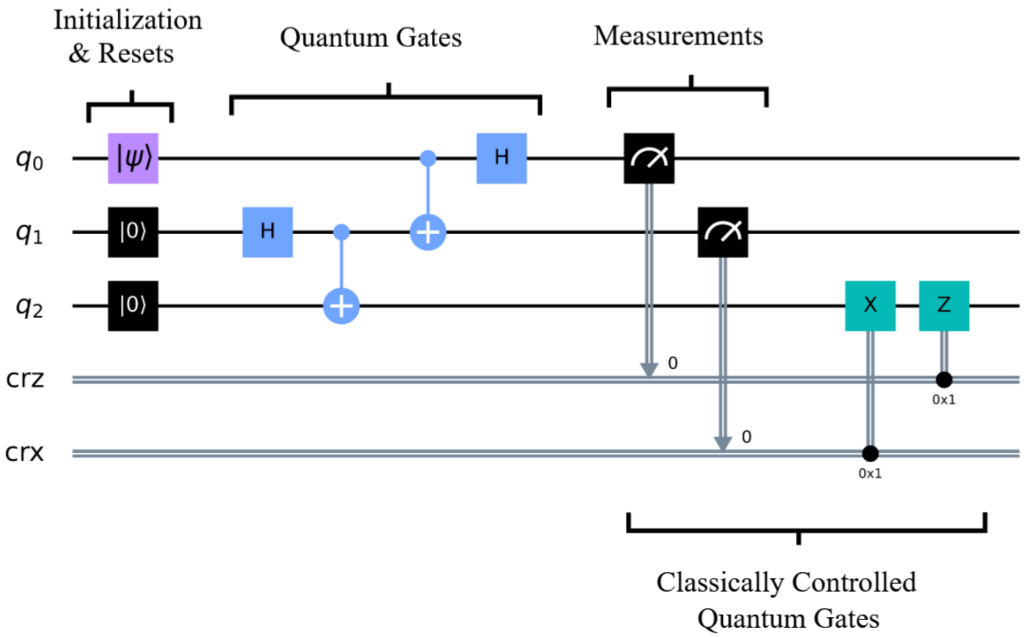
  → Repeated computation and measurement
- **Intermediate states** of the quantum system are **not accessible**



Quantum Circuits

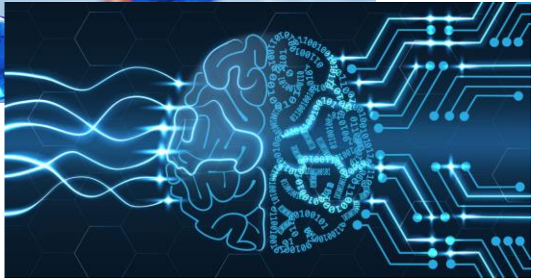
- **Qiskit definition:**

*„A **quantum circuit** is a computational routine consisting of coherent **quantum operations** on **quantum data**, such as qubits. It is an **ordered sequence** of quantum gates, measurements and resets, which may be conditioned on real-time classical computation.”*



Source: https://qiskit.org/documentation/apidoc/circuit.html

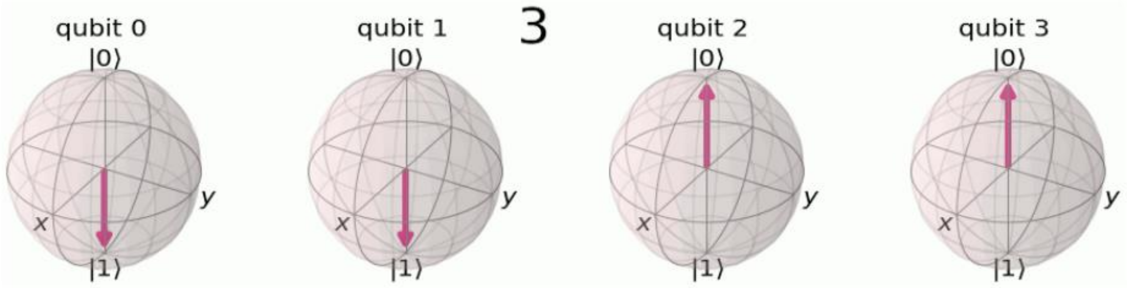
Algorithms & Application Areas



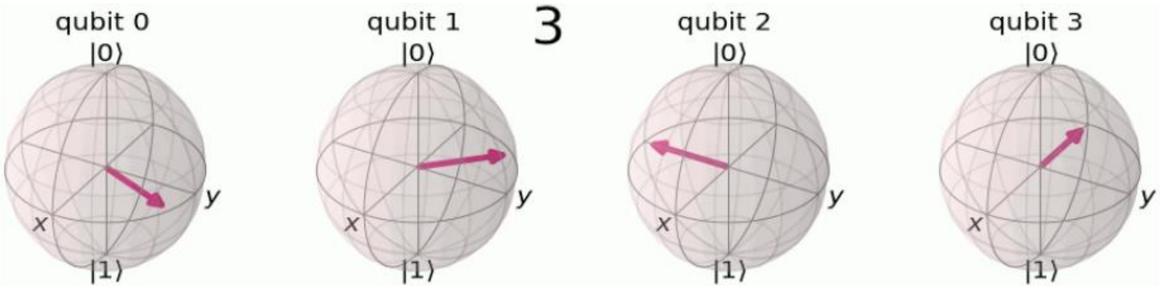
Quantum Fourier Transform

- **Quantum** implementation of **discrete Fourier transform**
- **Part** of many **quantum algorithms** (Shor,…)

Computational basis

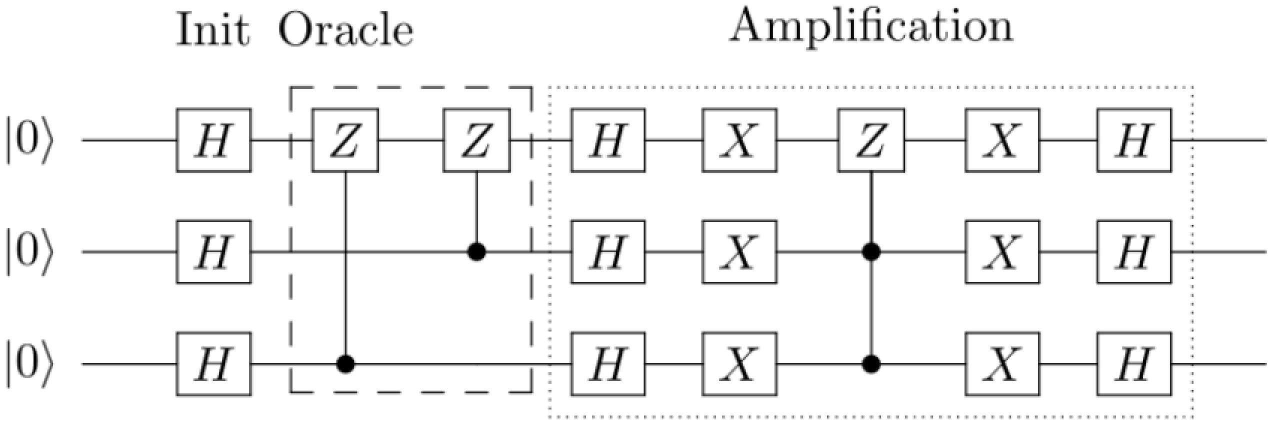


Fourier basis



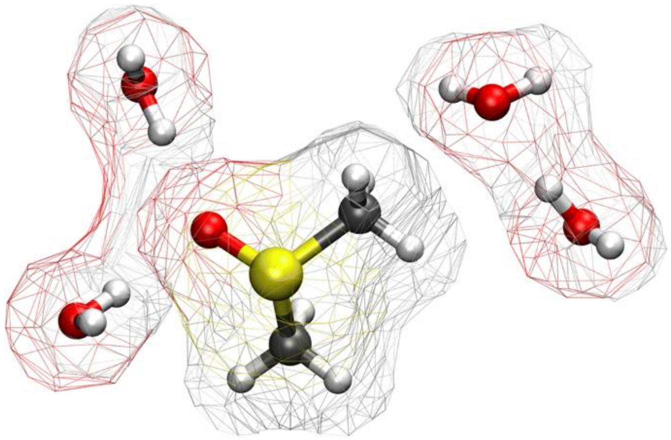
Grover-search algorithm

- **Database searches**, subroutine in other algorithms,…
- **Quadratic** speed-up



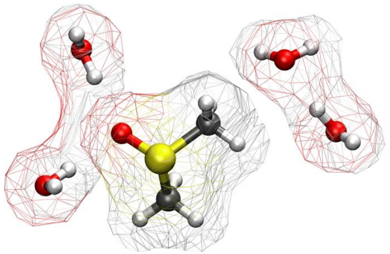
Application Areas – Quantum Chemistry

- **Closest to idea of Feynman 1981:**
  - Simulate quantum systems (molecules) with quantum systems (QC)



- **Scientific insights**
  - Quantum mechanical properties of molecular systems
  - Physiological processes (e.g., photosynthesis, DNA mutation)

Application Areas – Quantum Chemistry

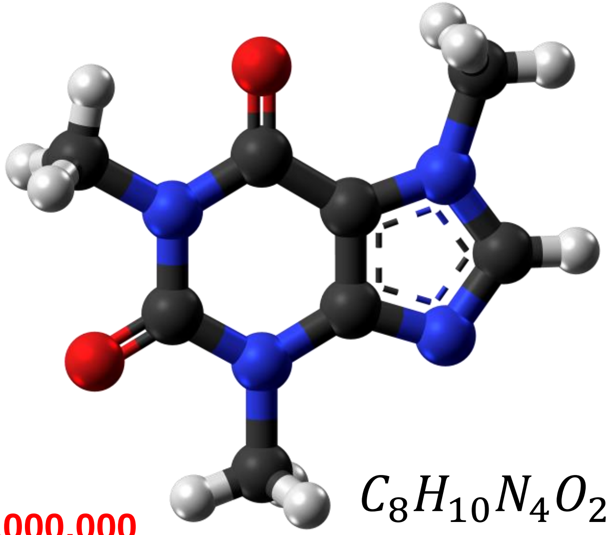


- **Classical approach:**
  - Calculations based on simplified model of molecule
  - Check a posteriori validity of the model

- **Simulation of molecular behaviour at quantum level:**
  - Drug design
  - Materials design
  - Development of new chemicals (e.g. catalyst in agriculture)

Quantum Chemistry- Example

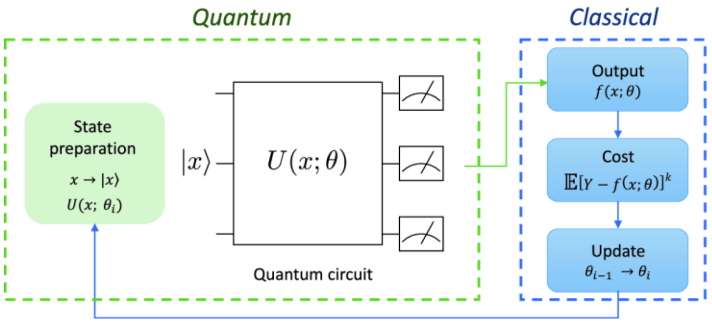
- **Molecule as quantum object:**
  - ➢ Many particles (e.g., nuclei, electrons)
  - ➢ Many-body problem
  - ➢ Highly interacting
- **Caffeine: 24 atoms**
- **Classical computation: 10^{48} bits**
  - ➢ **10,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000**
- **Quantum computation: 160 qubits**



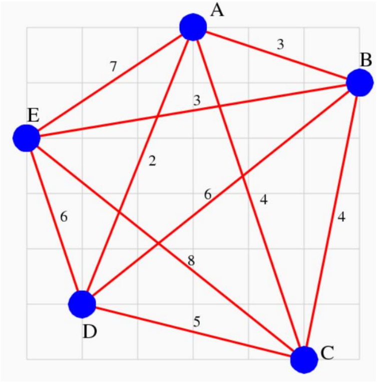
$C_8H_{10}N_4O_2$

Variational Quantum Eigensolver – VQE

- Originally used for **quantum chemistry**
  → e.g., **ground state energy**
- Makes use of **parameterized gates (VQA)**
- **Procedure:**
  - Generate trial state with U(θ)
  - Measure in computational basis
  - Calculate cost function: energy
  - Update parameters classically (e.g. gradient descent)



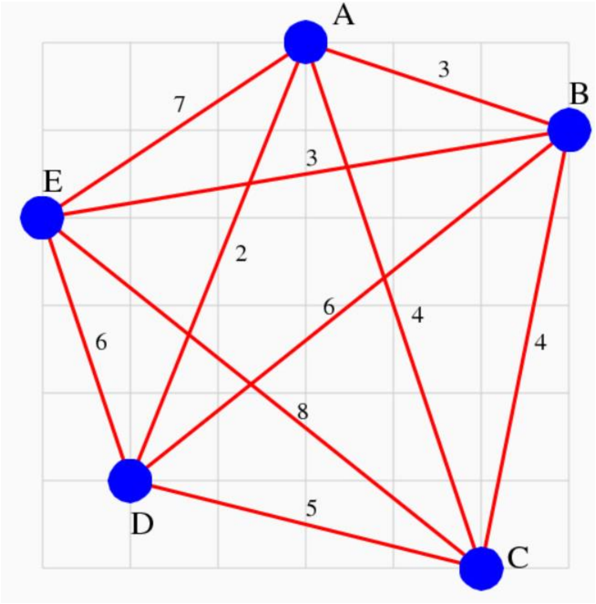
Application Areas – Quantum Optimization



- **Industrial relevance**
  - Logistics,
  - Manufacturing,
  - …
- **Optimizing operational metrics** (e.g., time, energy, fuel, cost)
- **Examples:** graph optimization, routing, scheduling
  - Usually exponentially growing search space
- **Classical computation**
  - Expensive algorithms (e.g., Brute force algorithms)
  - Use of approximative heuristics (e.g., Genetic Programming)

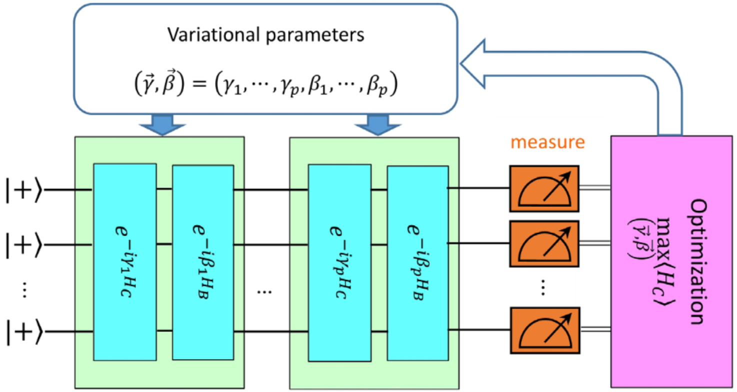
Quantum Optimization – Example

- **Travelling Salesman Problem**
  - Visit all cities → shortest route?
  - E.g., 20 cities: 20x19x18x..x2x1= 2,430,000,000,000,000,000 combinations
- **Quantum Computation**
  - Iteratively increase probability of getting optimal result
  - Usual form: Quadratic Unconstrained Binary Optimization (QUBO): $f(x) = x^T Q x$



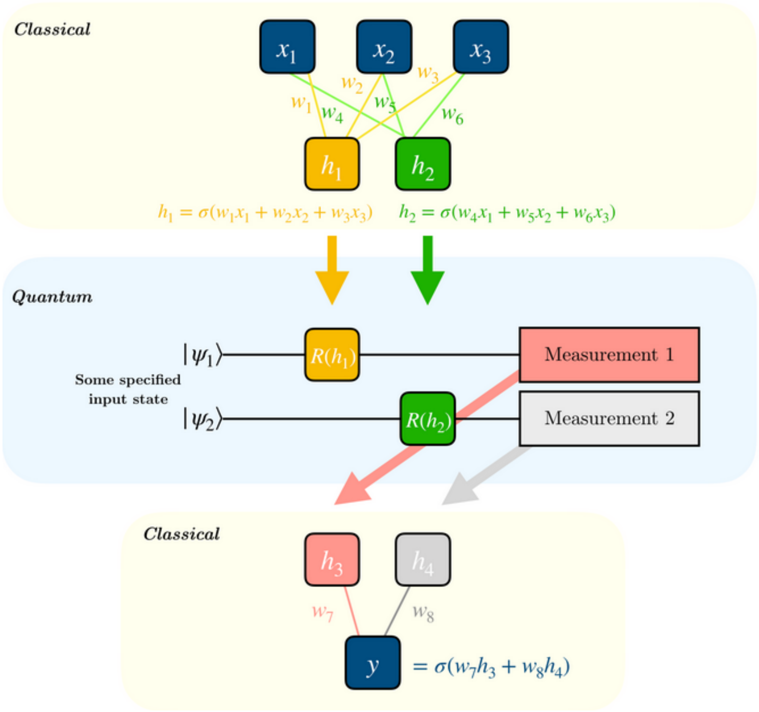
Quantum Approximate Optimization Algorithm – QAOA

- Algorithm for **combinatorial optimization** problems
- Very **similar to VQE** but with a defined ansatz
- **Procedure:**
  - Generate trial state with $U_C(\gamma), U_B(\beta)$
    - $U_C(\gamma)$: problem unitary
    - $U_B(\beta)$: mixing unitary
  - Measure in computational basis
  - Calculate cost function
  - Update parameters classically



Application Areas – Quantum Machine Learning

- **Mostly quantum-enhanced ML**
  - ➢ Hybrid nature
  - ➢ Difficult subroutines outsourced to QC
  - ➢ E.g., Quantum GAN
- **Quantum Neural Networks**
  - ➢ Variational Quantum Algorithms
- **Quantum Topology Analysis**
- And many more…

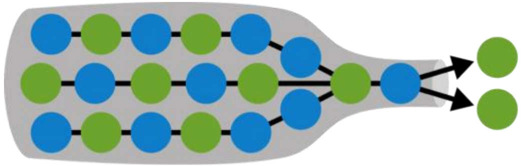


Quantum Algorithms – Requirements

JOHANNES KEPLER UNIVERSITY LINZ

Solve useful problem

Speed-up or other advantage



Relatively small data

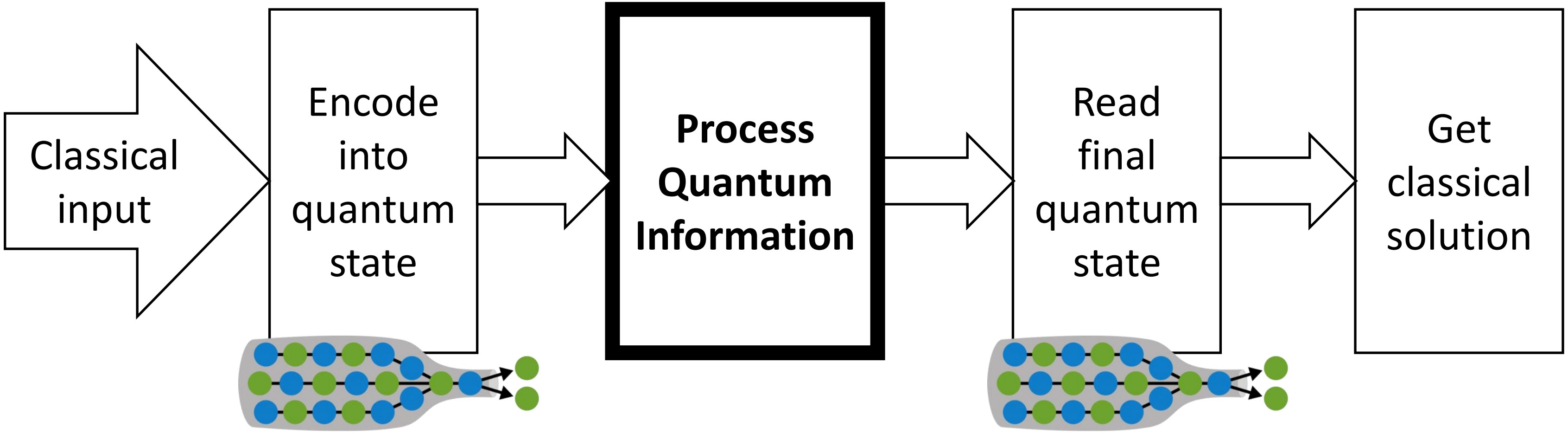
Correctness guarantees

Resources can be estimated

→ goal today: find promising problem where hybrid algorithm is better heuristic than purely classical approach

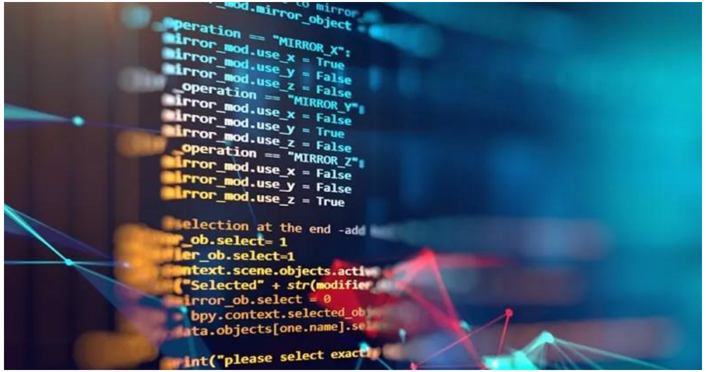
Challenges & Limitations

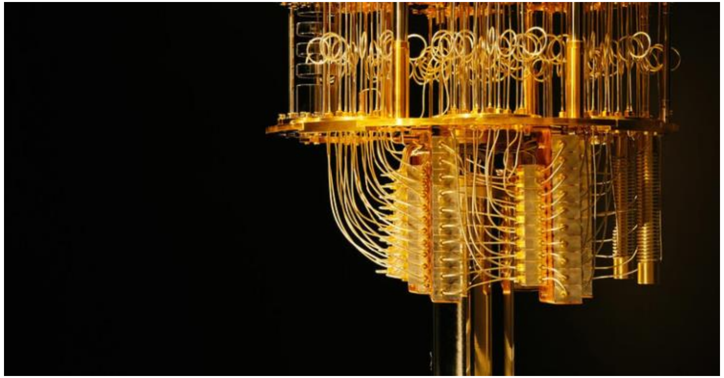
Quantum Information Processing – Bottlenecks




Ewin Tang
Quantum Recommendation Systems
arXiv:1807.04271
Ewin Tang
arXiv:1811.00414
Quantum PCA
Ewin Tang
arXiv:1811.04909
Low rank HHL

Challenges and Limitations





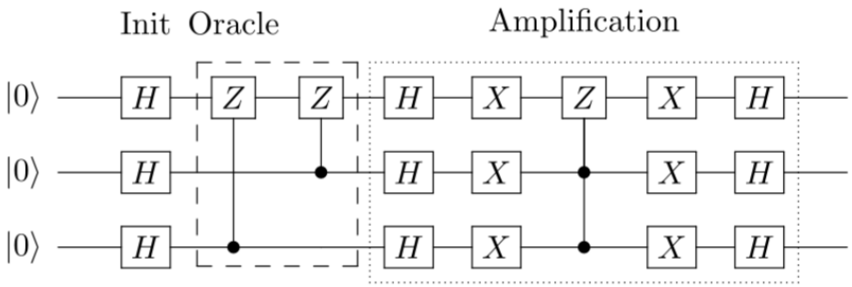
Algorithms & Software

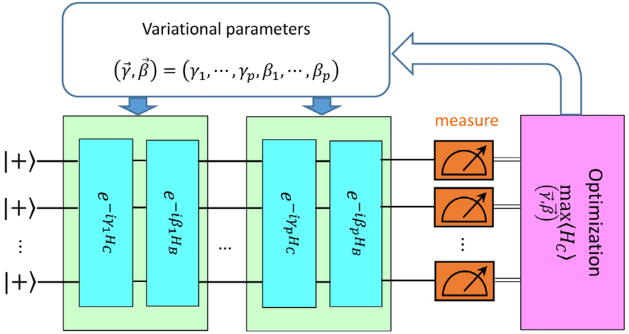
- Dequantization
- Error correction
- Programming languages
- Compilers
- Interface to classical regime
- Standards & Protocols

Hardware

- Fidelity
- Error correction
- Scalability
- Interface to classical regime

Challenges and Limitations





Fundamental

- No copies
- No assessment of intermediate states
- Decoherence
- Analog machines: $F = f^n$
- …

Variational Quantum Algorithms

- Exponentially small gradients
- Optimization of Parameters is NP-hard
- Requires a LOT of runs
- …

Summary of Challenges

Fault-tolerant Quantum Computing:

- Provable improvement for some applications
- Requires a lot of research

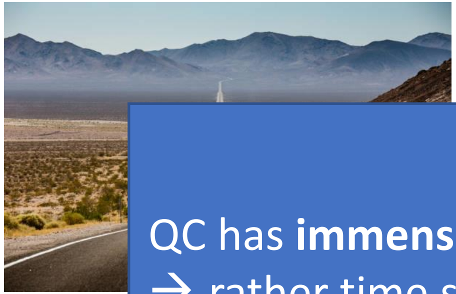
NISQ-era:

- No provable improvement
- Maybe still better heuristic especially in combination with classical computing

---

- **Fidelity** has to improve drastically
- QCs will **NEVER replace** classical ones!!!

Summary of Challenges



BUT:

QC has **immense transformative potential**

→ rather time scale is questionable

→ topics still requires

- a lot of fundamental and applied research
- strong connection between levels of abstraction
  - Fundamental & applied
  - Hardware & algorithms/software

Fault-tolerant Qu

- Provable impro
  some applicati ... in
- Requires a lot

- **Fidelity** has to improve drastically
- QCs will **NEVER replace** classical ones!!!

Quantum Software Engineering

Quantum Software Engineering

Emerging Field:

Goal: apply lessons learned from classical software engineering

Problem:

- Fundamentally different working principles
  - →Requires to raise abstraction levels

Review-Article:

De Stefano, M., Pecorelli, F., Di Nucci, D., Palomba, F., & De Lucia, A. (2022). Software engineering for quantum programming: How far are we?. *Journal of Systems and Software*, *190*, 111326.

Coding abstraction level

Classical

“No-Code”: whatever

Python + Frameworks: objects

Java,…: objects

C++: objects

C: arrays, strings

Assembly: byte

Machine language: bit

Quantum

Application spec. env.

Python + appl. Frameworks (qubits)

Gate-code before transpilation (qubits)

Gate-code after transpilation (qubits)

Electronics (control elec. instr.)

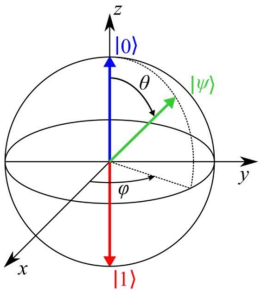
→ same abstraction level with qubit gates

Development Libraries

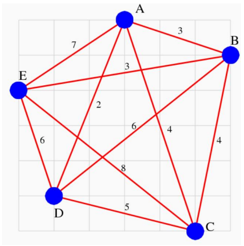
- **Dedicated tools**
  - from assembly languages to software development kits
- **Vendor-specific or vendor-agnostic**
  - E.g., IBM (Qiskit), Google (Cirq), D-Wave (Ocean), AWS (Braket), Microsoft (Q#)
- **Mostly based on Python & open-source**
  - Flexible,
  - High-level language
- **Focus on high-level**
  - Often domain-specific: e.g.,: ML→ PennyLane, TensorFlow Quantum
  - Graphical Quantum Circuit Designer mainly for education
- **Simulator vs. real quantum computer as backend**

Wrap-Up

1. Motivation and Overview
- Classical computing faces severe scaling issues
- QC is applicable to a variety of computational problems
- There are diverse approaches to quantum computing



2. Basic Working Principles
- QC harnesses quantum mechanical phenomena
- Mathematically its linear algebra

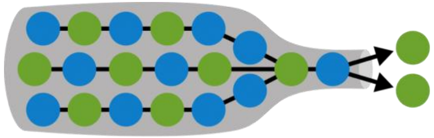


3. Near-term Applications are
- Quantum chemistry
- Quantum optimization
- Quantum machine learning

Wrap-Up

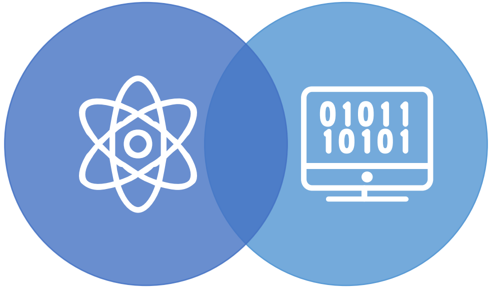
4. Challenges and Limitations

- Interesting challenges remain regarding quantum hardware, software, and their interaction
- Quantum computers will always be special purpose machines
- The potential is worth the effort



5. Quantum Software Engineering

- Which concepts from classical SE can be applied to QC?
- What are sound SE principles for engineering quantum software?
- What are quantum-specific challenges and how to consider them?




HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
Dilbert.com DilbertCartoonist@gmail.com
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
4-17-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.