Lecture

Quantum Computing

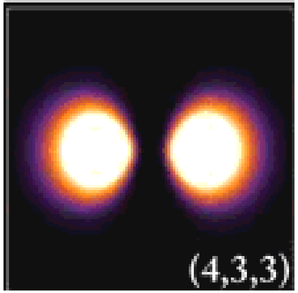
(CS5070)

Introduction to Quantum Computing

Professor Dr. rer. nat. habil. Sven Groppe
https://www.ifis.uni-luebeck.de/~groppe

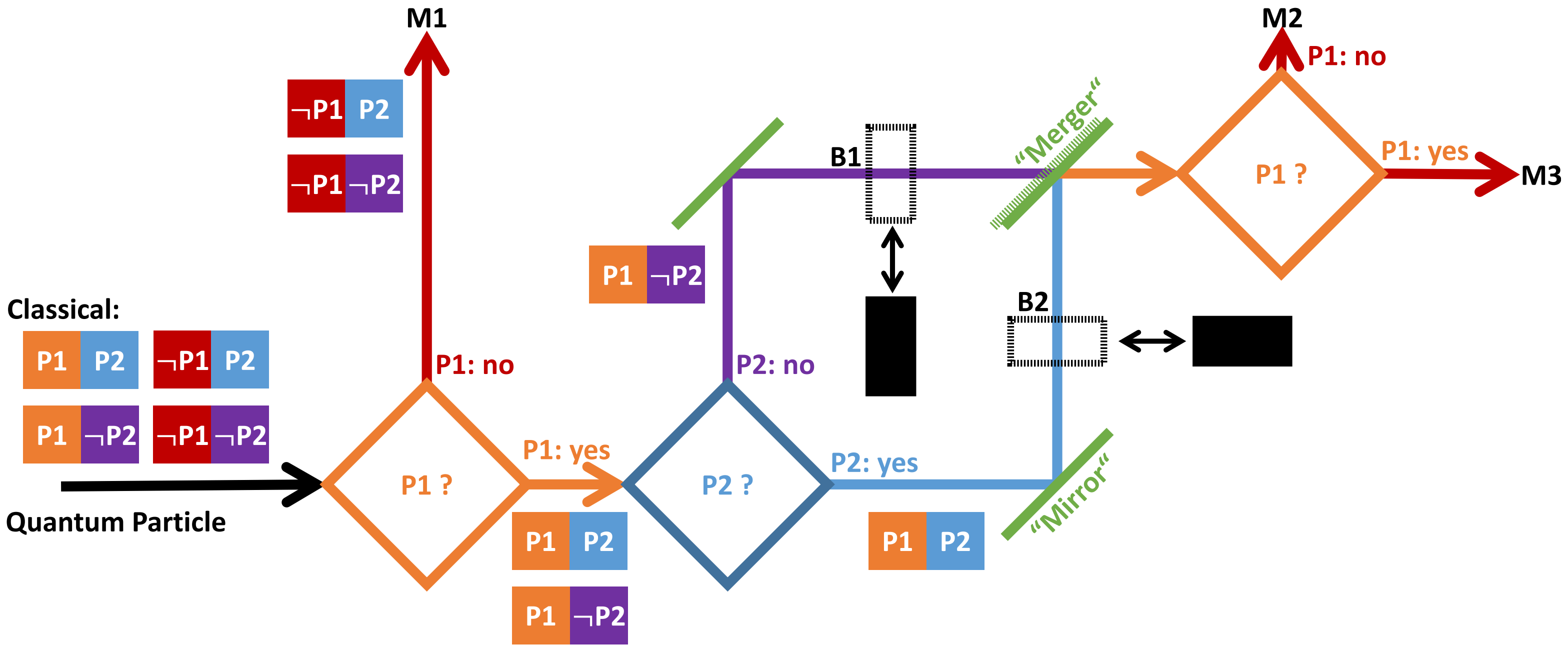
Quantum Mechanics

- Very small particles and light behave differently from objects in normal life
- Mechanics of light and matter at the atomic and subatomic scale are described by quantum theory
  - forming the underlying principles of chemistry and most of physics
- Quantum theory has brought us the information age with its disruptive technologies of
  - transistors,
  - lasers,
  - nuclear power, and
  - superconductivity...
  - **...and now also quantum computers!**



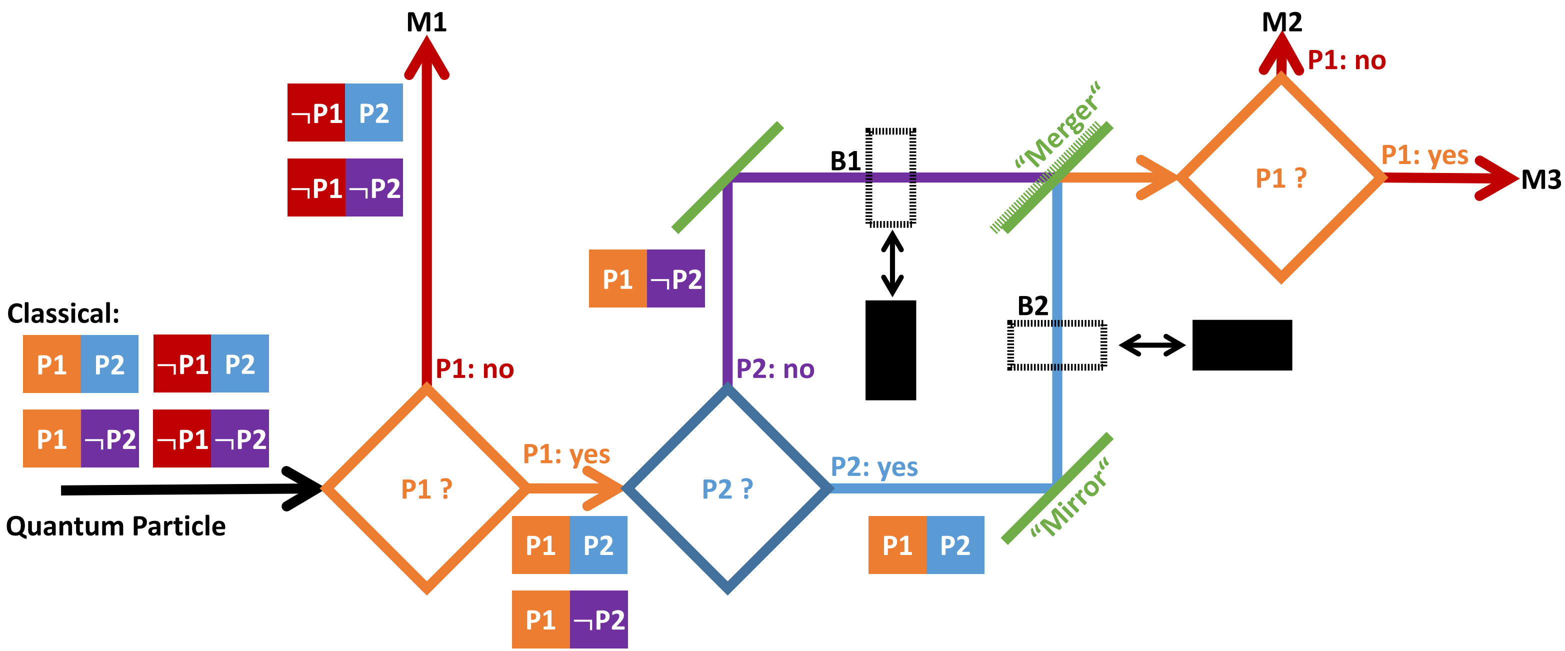
Wavefunctions of the electron in a hydrogen atom at different energy levels. Brighter areas represent a higher probability of finding the electron.

Superposition Experiments



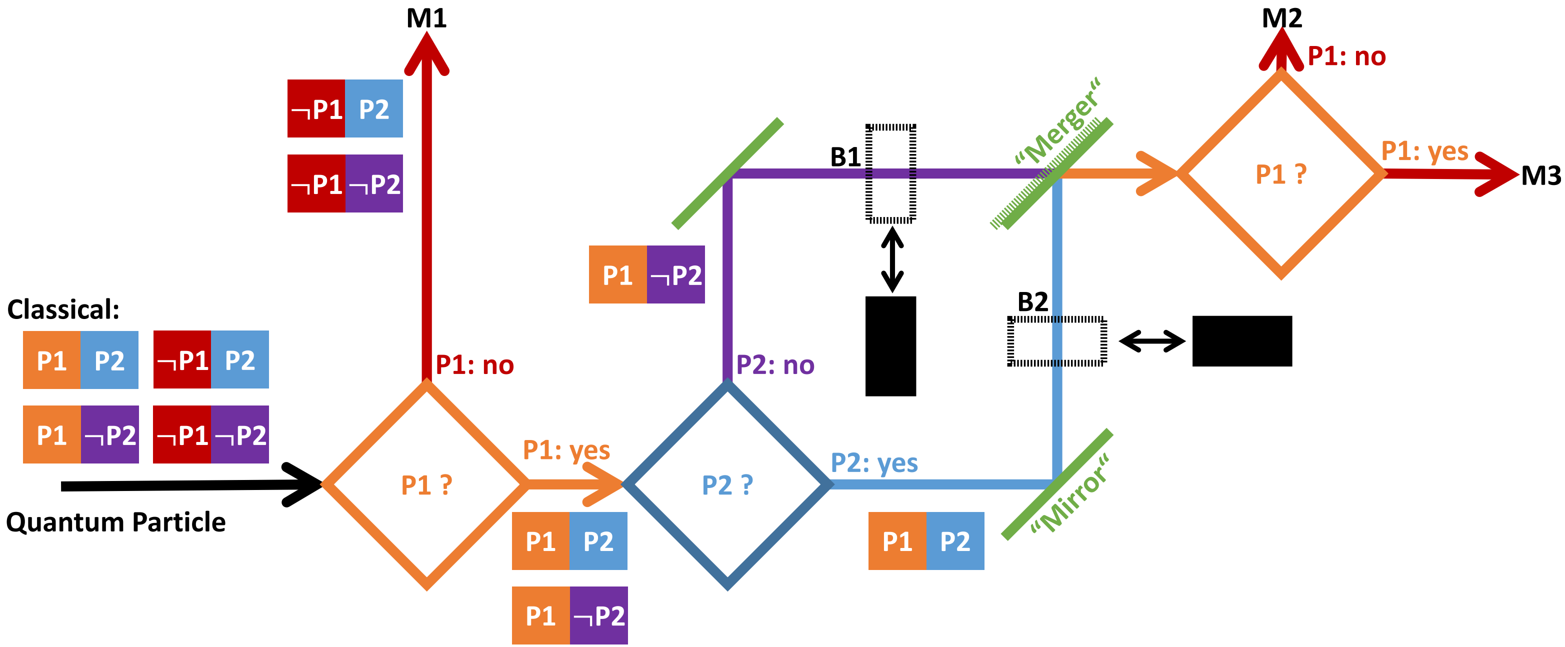
B1	Not Blocking		Not Blocking		Blocking		Blocking	
B2	Not Blocking		Blocking		Not Blocking		Blocking	
Type	Classical	Quantum	Classical	Quantum	Classical	Quantum	Classical	Quantum
M1	???	...	???	...	???	...	???	...
M2	???	...	???	...	???	...	???	...
M3	???	...	???	...	???	...	???	...

Superposition Experiments



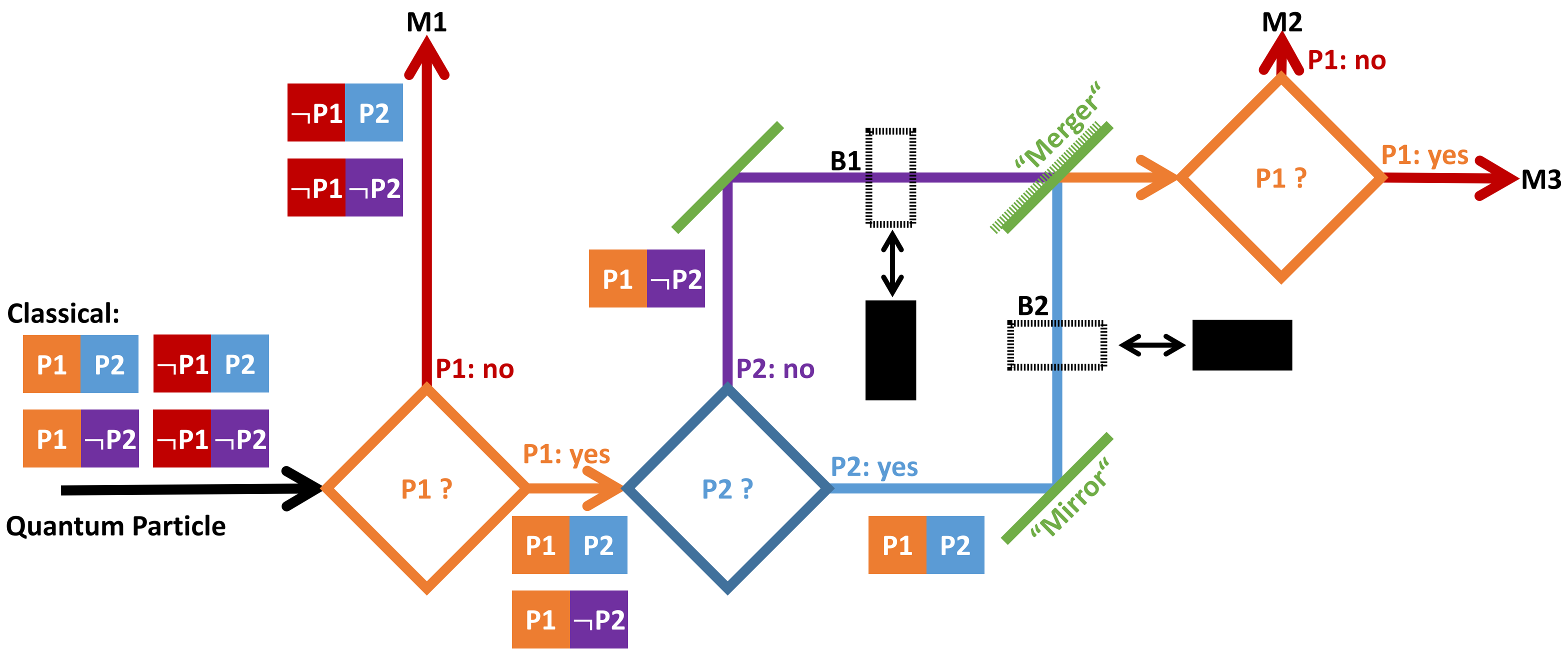
B1	Not Blocking		Not Blocking		Blocking		Blocking	
B2	Not Blocking		Blocking		Not Blocking		Blocking	
Type	Classical	Quantum	Classical	Quantum	Classical	Quantum	Classical	Quantum
M1	50%	50%	50%	50%	50%	50%	50%	50%
M2	0%	0%	0%	12.5%	0%	12.5%	0%	0%
M3	50%	50%	25%	12.5%	25%	12.5%	0%	0%

Superposition Experiments



- Which route one single quantum particle (reaching either M2 or M3) takes?
  - Does it take the route of B1?
  - Does it take the route of B2?
  - Does it take the routes of B1 and B2 together?
  - Does it take neither the route of B1 nor of B2?

Superposition Experiments

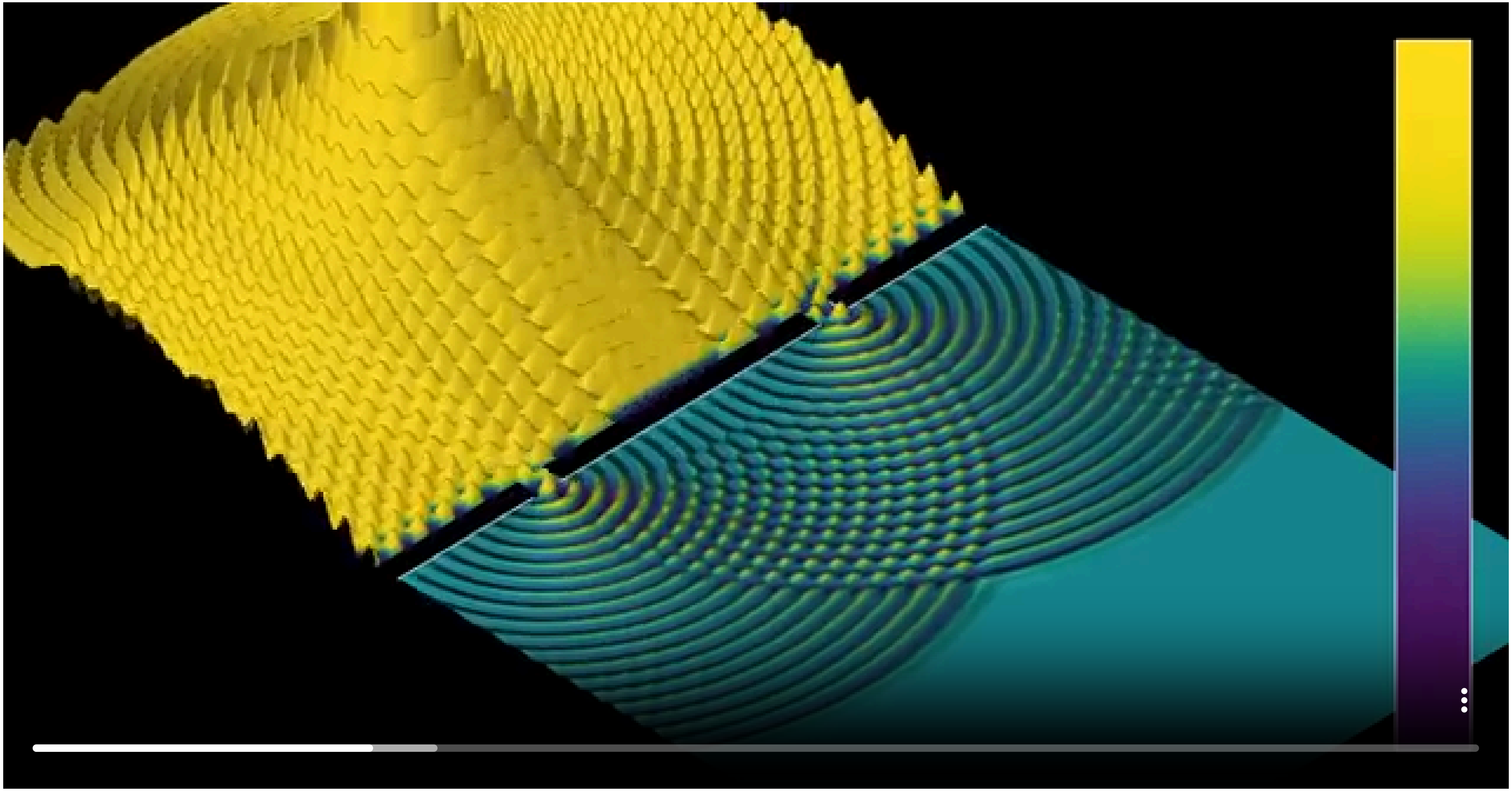


- Which route one single quantum particle (reaching either M2 or M3) takes?
  - Does it take the route of B1? **No:** Blocking B2 ⇒ Observation at M2/M3 changes!
  - Does it take the route of B2? **No:** Blocking B1 ⇒ Observation at M2/M3 changes!
  - Does it take the routes of B1 and B2 together? **No:** Another experiment: Always 1 (full) quantum particle is observed either at B1 or at B2 when measuring at B1/B2!
  - Does it take neither the route of B1 nor B2? **No:** Block.B1&B2⇒Nothing@M2/M3!

Superposition Experiments

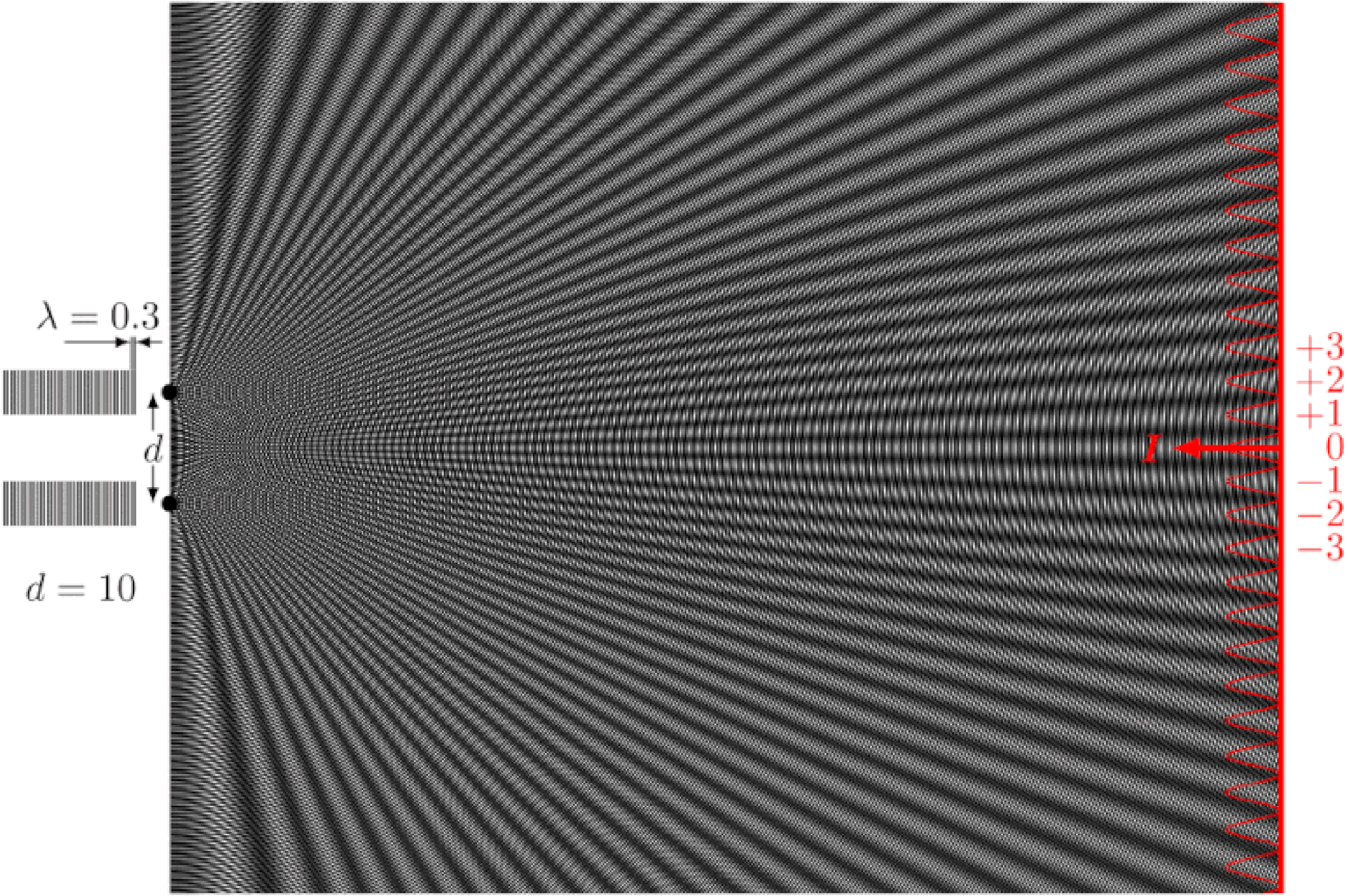
Allan Adams: "*Apparantly, empirically, [quantum particles like] electrons have a way of moving, electrons have a way of being which is unlike anything that we are used to thinking about. And so do molecules. And so do bacteria. So does chalk. It's just harder to detect in those objects. So physicists have a name for this new mode of being. And we call it superposition. ... So to build a better definition of superposition than I have no idea what is going on is going to require a new language. And that language is quantum mechanics.*"

Double-Slit Experiment with Classical Waves (e.g., Water)

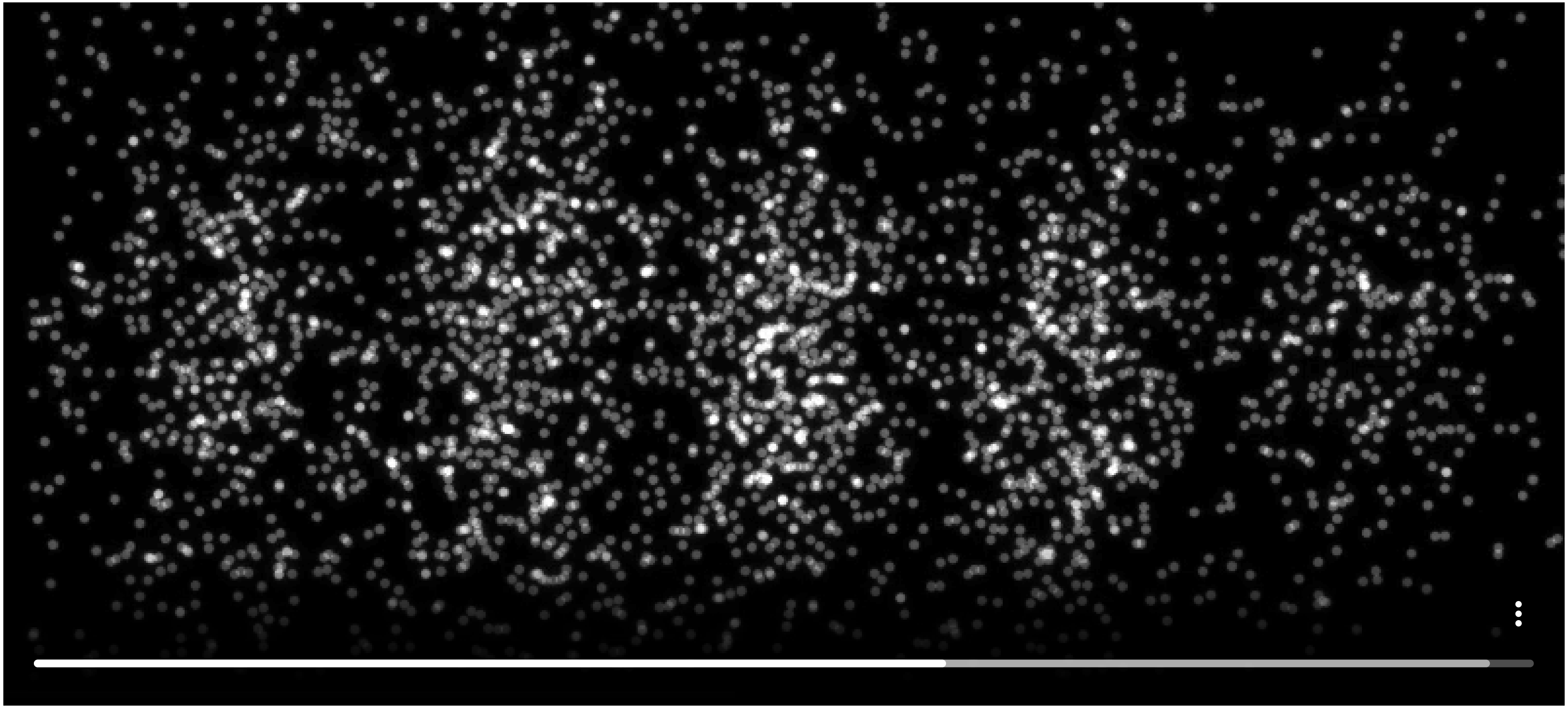


Video: Nils Berglund, "Young's double-slit experiment with waves, in 3D" Music: "Seductress" by Francis Preve@francispreve

Double-Slit Experiment (e.g., Light/Laser)

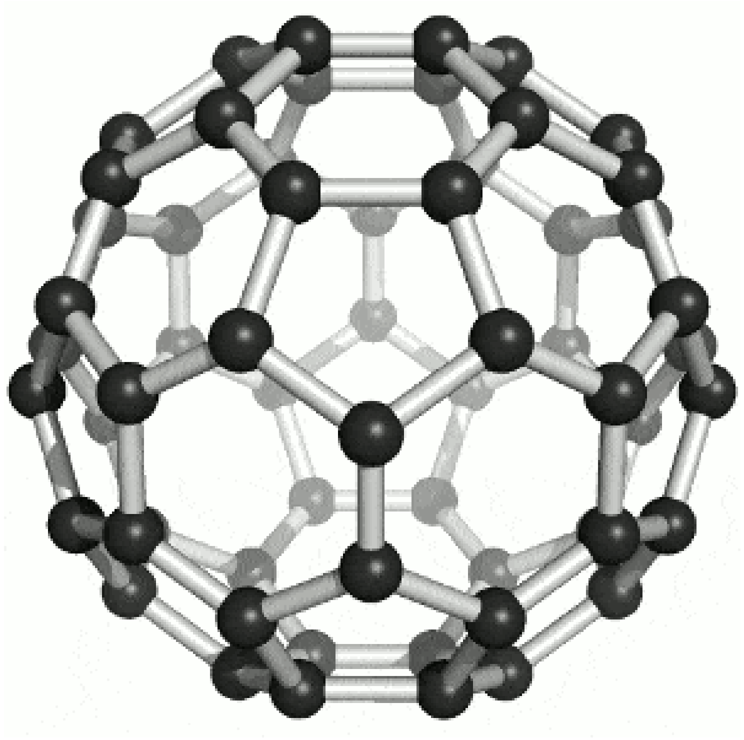


Double-Slit Experiment with Electrons

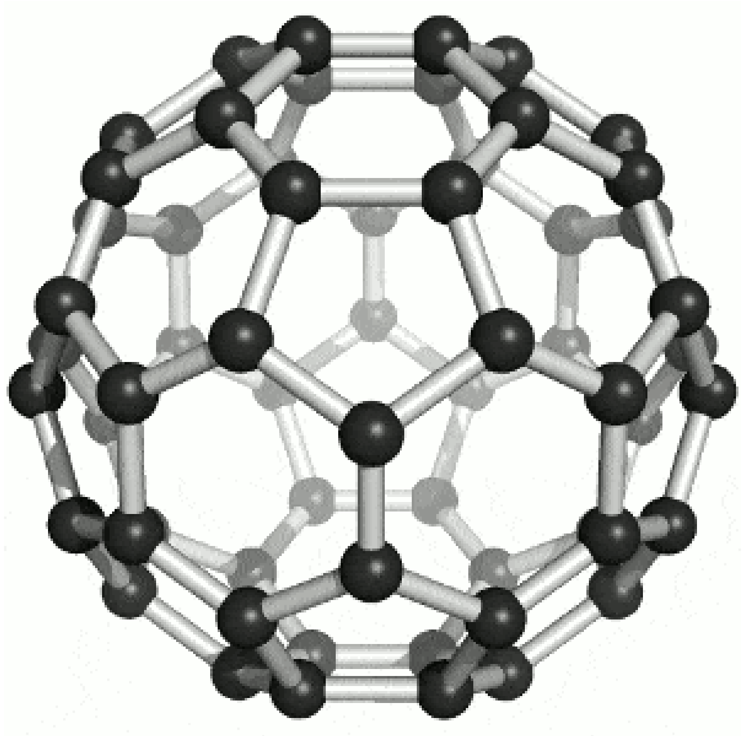


R. Bach, D. Pope, S.-H. Liou, H. Batelaan: Controlled double-slit electron diffraction, New J. Phys. 15, 2013, DOI 10.1088/1367-2630/15/3/033018

Double-Slit Experiment with "Soccer Balls"

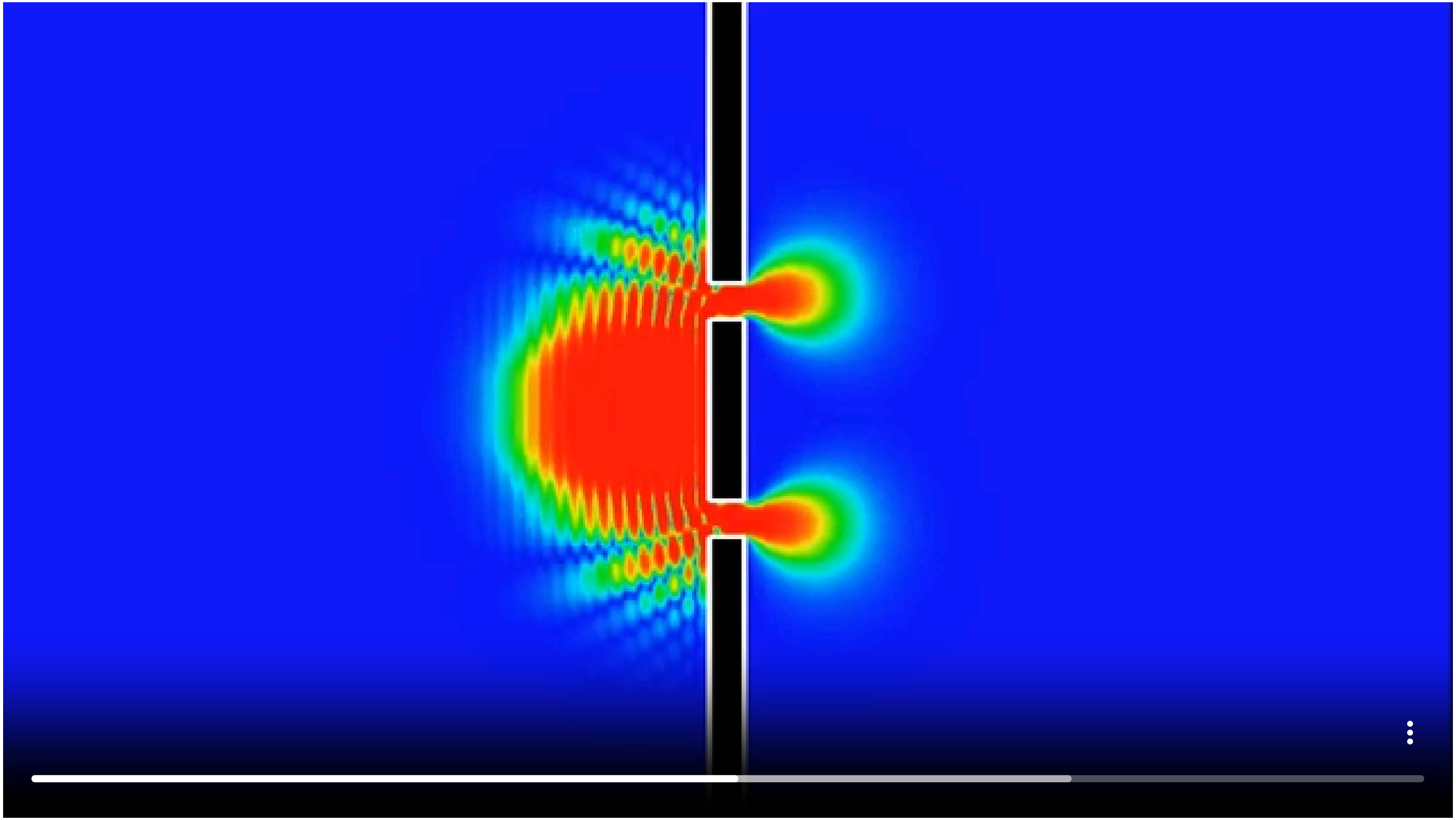


Double-Slit Experiment with "Soccer Balls"



- Interference pattern also visible for huge molecules like C_{60} (i.e., consisting of 60 Carbon atoms) [A+99]

Quantum Particle (Schrödinger Equation)

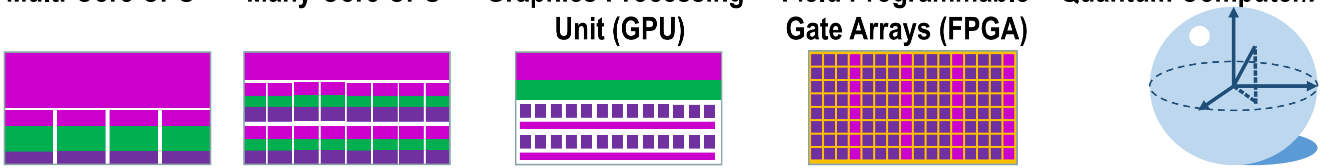


Video: Nils Berglund, "Young's double-slit experiment with a quantum particle" Music: "Consort for Brass - Classical Rousing" by Kevin MacLeod

Timeline of important events

- **1982**: Feynman proposes the concept of quantum computers [F'82]
- **2019**: Google announces "Quantum Supremacy" by its 53-qubits chip "Sycamore" [A+'19]
  - 200 seconds on Sycamore versus 10,000 years on the world's fastest supercomputer IBM Summit
  - IBM [P+'19]: only 2.5 days on classical supercomputer after deduction of the problem (i.e., using a better classical algorithm)
  - Pan et al. [PCZ'21]: only 15 hours on 512 GPU-cluster using another classical algorithm for obtaining a large number of uncorrelated samples
    - Estimation: a few dozens of seconds on ExaFLOPS supercomputer
  - Discussion intensified the excessive hype about quantum technology
- **2023**: Next try: Google runs Random Circuit Sampling experiments on its 70-qubits improved "Sycamore" in seconds instead of 47 years (estimation for #1 classical supercomputer in 2023) [G+'23]
- **2025**: DWave solves magnetic materials simulation problems in 20 min instead of 1 million years [K+25] (others disagree [W'25])

Architectures of Emergent Hardware



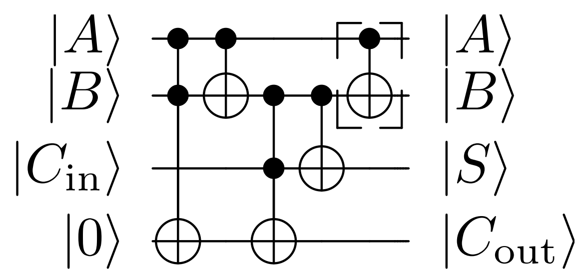
	Multi-Core CPU	Many-Core CPU	Graphics Processing Unit (GPU)	Field Programmable Gate Arrays (FPGA)	Quantum Computer/Annealer
Cores	~10	~100	~1000	~100 000	~100 / ~5000 qubits
Core Complexity	Complex (optimized for single thread performance)			Simple	Complex
Computational Model	MIMD + SIMD		SIMD	Data-Flow	Universal/Adiabatic Quantum computing
Parallelism	Thread and Data Parallel		Data Parallel	Arbitrary	Quantum Logic Gates/ Fluctuation (glob.Min.): Interference
Memory Model	Shared	Distributed			Quantum Superposition
Power	150 W	200 W	250 W	50 W	25 KW
Database Op.	Query Optimization (Enumeration of Plans), Concurrency Control				
	Efficient Processing Of				
	Query Processing				

Legend: Computational Unit, Execution Controller, Interconnection Network, On-Chip Memory

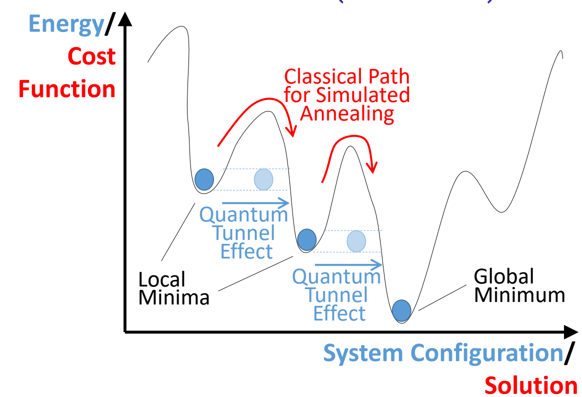
Extended from C. Plessl, Accelerating Scientific Computing with Massively Parallel Computer Architectures, IMPRS Winter School, Wroclaw, 2012

Quantum Computer

- use of quantum-mechanical phenomena such as superposition and entanglement to perform computation
- Different types of quantum computer, e.g.
  - Universal Quantum Computer
    - uses quantum logic gates arranged in a circuit to do computation
    - measurement (sometimes called observation) assigns the observed variable to a single value
  - Quantum Annealing
    - metaheuristic for finding the global minimum of a given objective function over a given set of candidate solutions
    - i.e., some way to solve a special type of mathematical optimization problem



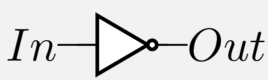
Quantum Circuit (Full Adder)



Simulated versus Quantum Annealing

Classical versus Quantum Computing

	Classical	Quantum
Information Unit	**Bi**nary Digi**t** (Bit): • basis of a 2-level system • can be in state 0 or 1	**Qu**antum **Bit** (Qubit): • basis of a 2-level quantum system • can be in state $\|0\rangle$, $\|1\rangle$ or in a linear combination of both states
Operation	Logic Gate: • performs on 1 or more bits to produce a single bit output	Quantum Logic Gate: • performs on 1 or more qubits to change the quantum state of a single qubit
Example Operation	NOT/Inverter: Digital Circuit:	NOT/Pauli$_x$-Gate: Quantum Circuit: $\|In\rangle \oplus \|Out\rangle$ Alternatively: $\|In\rangle$ $\boxed{X}$ $\|Out\rangle$



In	Out
0	1
1	0

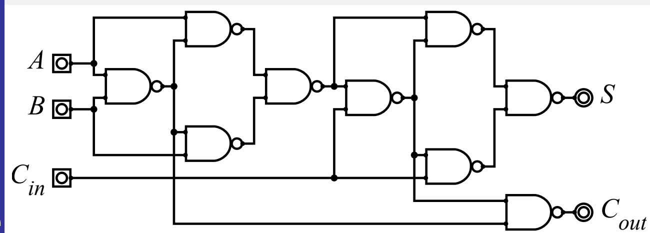
In	Out
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$
$\frac{3\cdot i}{5}\|0\rangle + \frac{4}{5}\|1\rangle$	$\frac{4}{5}\|0\rangle + \frac{3\cdot i}{5}\|1\rangle$

Digital versus Quantum Circuits

	Digital Circuit	Quantum Circuit
Building Blocks	Logic Gates	Quantum Logic Gates

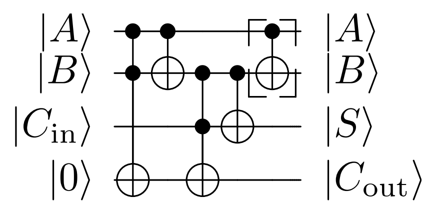
Full Adder Example

Digital Circuit:



consists of NAND gates

Quantum Circuit:



consists of Toffoli and CNOT gates[1]

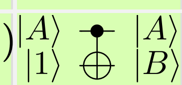
In- and Output Full Adder

Digital Circuit:

Inputs			Outputs	
A	**B**	**C_{in}**	**C_{out}**	**S**
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Quantum Circuit:

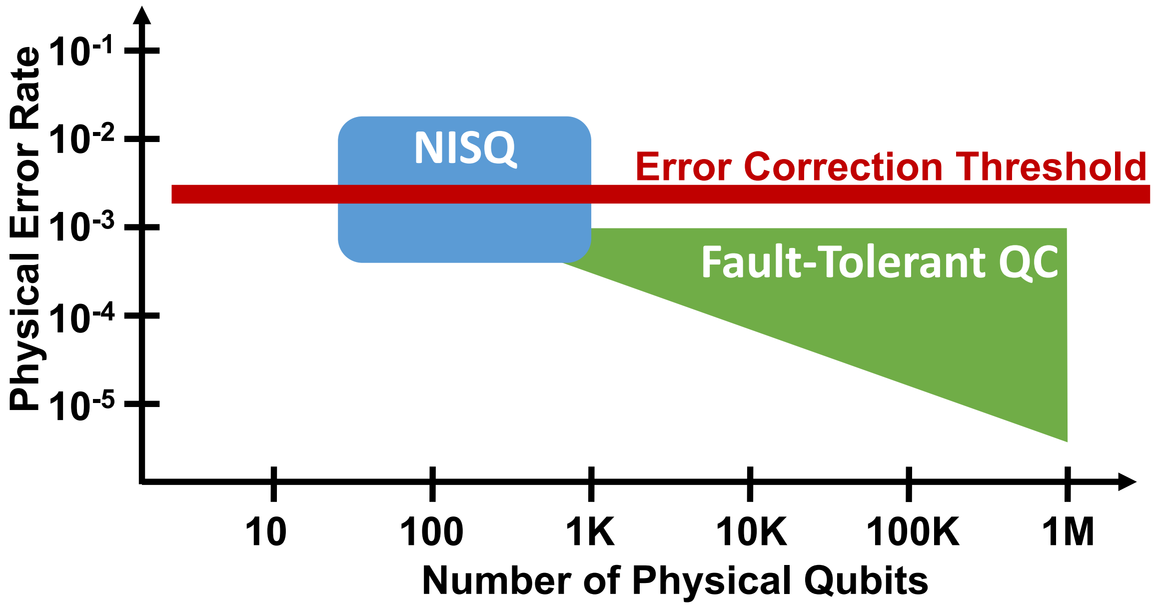
$|0\rangle$ **and** $|1\rangle$ **as input:** Output is $|0\rangle$ and $|1\rangle$ analogous to digital circuit.
Superpositions as input: Superpositions as output with corresponding probabilities for basic quantum states, e.g.:

A	B	C_{in}	C_{out}	S
$\frac{1}{\sqrt{2}}(\lvert 0\rangle + \lvert 1\rangle)$	$\lvert 0\rangle$	$\lvert 0\rangle$	**$ABC_{out}S$:** $\frac{1}{\sqrt{2}}(\lvert 0000\rangle + \lvert 1001\rangle)$	
$\frac{1}{\sqrt{2}}(\lvert 0\rangle + \lvert 1\rangle)$		$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$

[1] The dotted square marks a superfluous gate if uncomputation to restore the B output is not required. **[Feynman, 1986]**

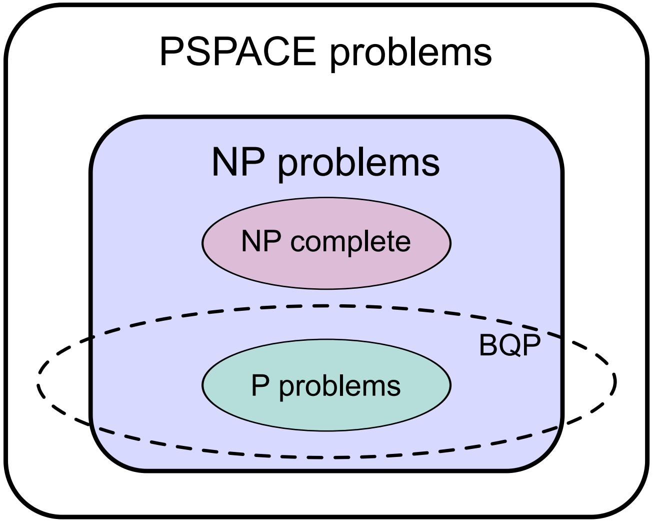
Timeline of Quantum Computers

Noisy Intermediate-Scale Quantum (NISQ)



- quantum computers with 50-100 qubits: noise in quantum gates limits the size of quantum circuits that can be executed reliably
- Such NISQ devices may be able to perform tasks which surpass the capabilities of today's classical digital computers with application areas like quantum chemistry, optimization & machine learning
- 100-qubit quantum computers are (only) intermediate technologies

Suspected Shape of BQP



- PSPACE is the set of all decision problems that can be solved by a Turing machine using a polynomial amount of space
- NP: nondeterministic polynomial time is the set of problems that can be solved in polynomial time by a nondeterministic Turing machine
- A problem is said to be NP-hard if everything in NP can be transformed in polynomial time into it even though it may not be in NP
- A problem is NP-complete if it is both in NP and NP-hard
- P: PTIME contains all decision problems that can be solved by a deterministic Turing machine in polynomial time
- BQP: bounded-error quantum polynomial time is the class of decision problems solvable by a quantum computer in polynomial time, with an error probability of at most 1/3 for all instances
- Note: Neither P≠NP nor P≠PSPACE has been proven, and if either of these are equal, the shape of BQP would be different

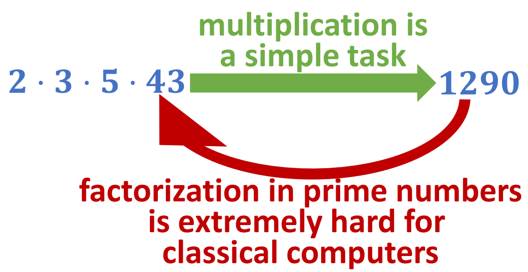
Potential of Quantum Algorithms

- **Quantum Algorithm Zoo** as example of collection of *important* quantum algorithms

Covered Years	1974-today
#Investigated References	430 (visited on October 2021)
#Algorithms	**64**
Speedups	**Superpolynomial: 31**, Polynomial: 27, Constant factor: 1, Varies: 3, Various: 1, Unknown: 1

Terminology:
α: positive constant
$C(n)$: runtime of the best known classical algorithm
$Q(n)$: runtime of the quantum algorithm
Superpolynomial Speedup: $C = 2^{\Omega(Q^\alpha)}$
Polynomial Speedup: otherwise

Very Important Quantum Algorithms 1/2: Shor's Algorithm[1]



- factoring integers in polynomial time
  - Depth of quantum circuit[2] to factor integer N: $O((log\ N)^2(log\ log\ N)(log\ log\ log\ N))$
  - superpolynomial speedup, i.e., almost exponentially faster than the most efficient known classical factoring algorithm (general number field sieve): $O(e^{1.9(log\ N)^{\frac{1}{3}}(log\ log\ N)^{\frac{2}{3}}})$
- Important for cryptography $\longrightarrow$ Post-Quantum Cryptography
- Most quantum algorithms with superpolynomial speedup like Shor's algorithm are based on quantum Fourier transforms (quantum analogue of inverse discrete Fourier transform)

[1] [Shor, 1994] [2] [Beckman et al., 1996]

Very Important Quantum Algorithms 2/2: Grover's Search Algorithm

- Black box function (oracle) $f\ :\{0, ..., 2^b - 1\} \mapsto \{true, false\}$
- Grover's search algorithm finds one $x\ \in\{0, ..., 2^b - 1\}$, such that $f(x) = true$
  - if there is only one solution: $\frac{\pi}{4} \cdot \sqrt{2^b}$ basic steps each of which calls f
    Let $f'(b)$ be runtime complexity of f for testing x to be true:
    $\Rightarrow O(\sqrt{2^b} \cdot f'(b))$
  - if there are k possible solutions: $O(\sqrt{\frac{2^b}{k}} \cdot f'(b))$
- Basis of many other quantum algorithms and applications

Lov K. Grover. A fast quantum mechanical algorithm for database search. *STOC'96*, 1996

Algorithms (used e.g. in Query Optimization) and their Quantum Counterparts

Query Optimization Approach	Basic Algorithm	Quantum Computing Counterpart
[S+79]	Dynamic Programming [E04]	[R19] [A+19]
[IW87], QA: [TK16]	Simulated Annealing [KGV83]	[J+11]
[MP18] [Y+20] [W+19] [O+19]	Reinforcement Learning [BSB81]	[S+21] [DCC05]
[GPK94]	Random Walk [BN70]	[ADZ93] [A+01]
[BFI91]	Genetic Algorithm [H92]	[W+13]
[TC19]	Ant Colony Optimization [CDM91] [DBS06]	[WNF07] [G+20]

This list is not complete...

Open Challenges for QC for Databases

- Are QC counterparts of basic algorithms used in query optimizations suitable for speeding up databases?
- What should be the properties of a quantum computer (e.g. #qubits, latencies of gates) to achieve certain speedups?
- How to combine classical and quantum computing algorithms to achieve good speedups with few qubits?
  (...for running database optimizations on current available quantum computers...)
- What other database domains besides query optimization benefit from quantum computers?
  (In short: those based on mathematical optimization problems, but also other...?)

QC4DB: Accelerating Relational Database Management Systems via Quantum Computing

- **Project Website@Quantentechnologien**
- Project funded by BMBF
  - Duration 3 years, 1.8M Euros
- Topics
  - Query Optimization
  - Optimizing Transaction Schedules

  of an open source relational database management system
- Partners
  - University of Lübeck (Coordinator Sven Groppe)
    - Hardware-Acceleration of Databases
    - Website: https://www.ifis.uni-luebeck.de/~groppe/
  - Quantum Brilliance GmbH
    - Room Temperature Diamond Quantum Accelerators
    - Website: https://quantumbrilliance.com/

Topics of this Lecture

Summary and Conclusions

- Quantum Mechanics $\Rightarrow$ Quantum Computers
  - Universal Quantum Computing versus Quantum Annealing
- Quantum Computing as Hardware Accelerator
- Classical versus Quantum Computing
  - Bits versus Qubits
  - (Quantum) Logic Gate
  - Digital Circuits versus Quantum Circuits
- Timeline of Quantum Computers
- Noisy Intermediate-Scale Quantum (NISQ) technologies
- Bounded-error quantum polynomial time problems
- Potential of Quantum Algorithms
  - Shor (superpolynomial speedup)
  - Grover (quadratic speedup)
- Quantum Computing for databases