IFIP 60 Virtual Event Series

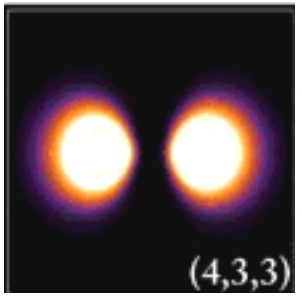
Quantum Computing for DB

Future Trends in Databases: from Data Science through Artificial Intelligence to Quantum Computing

Professor Dr. rer. nat. habil. Sven Groppe
https://www.ifis.uni-luebeck.de/index.php?id=groppe

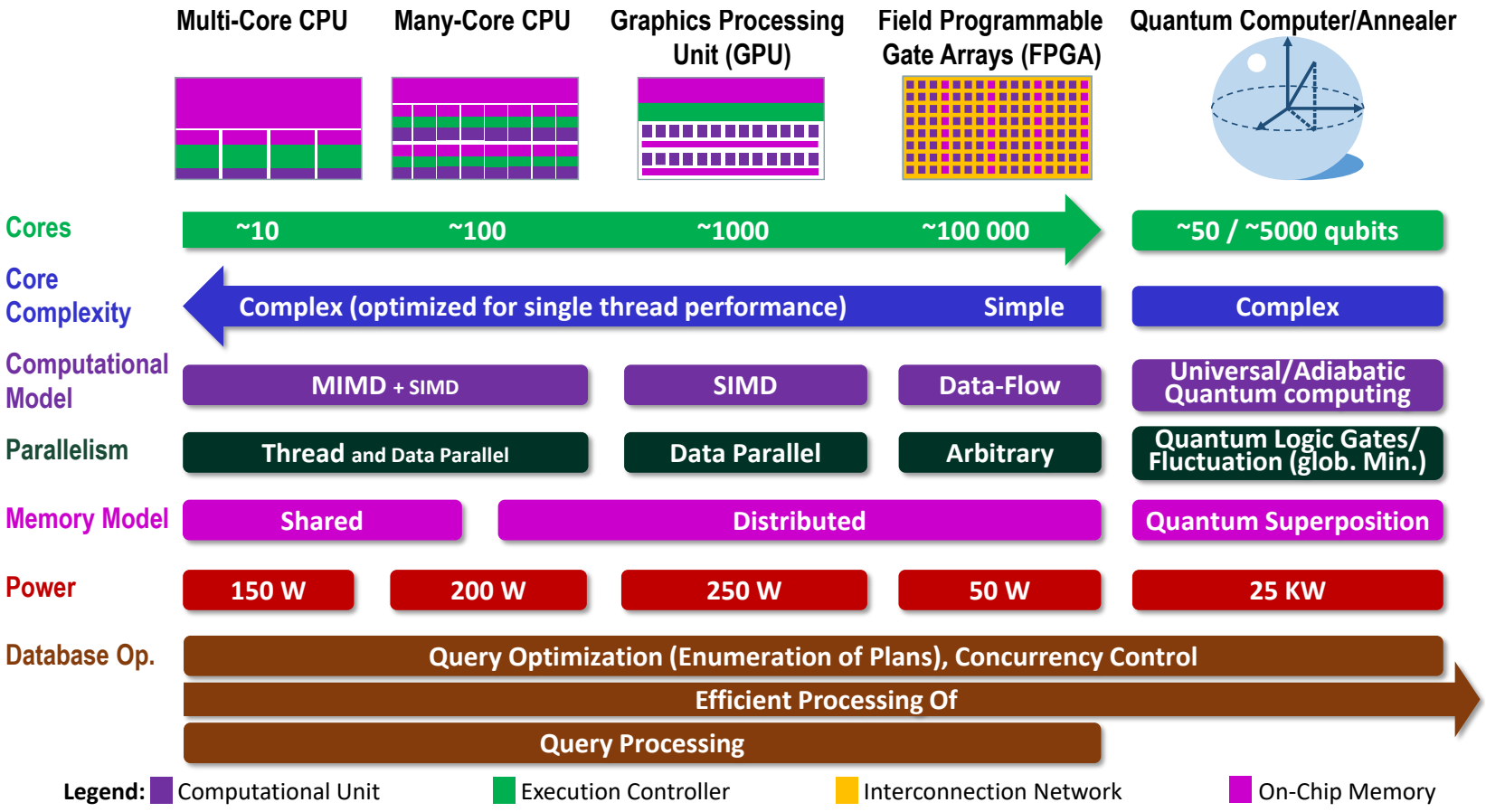
Quantum Mechanics

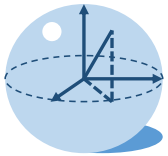
- Very small particles and light behave differently from objects in normal life
- Mechanics of light and matter at the atomic and subatomic scale are described by quantum theory
  - forming the underlying principles of chemistry and most of physics
- Quantum theory has brought us the information age 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.

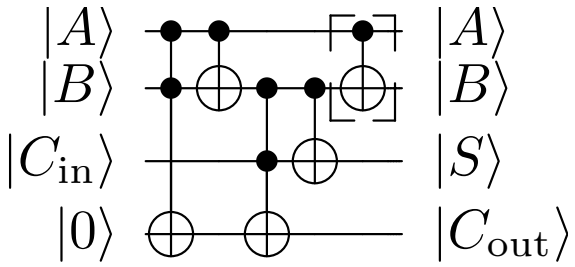
Architectures of Emergent Hardware



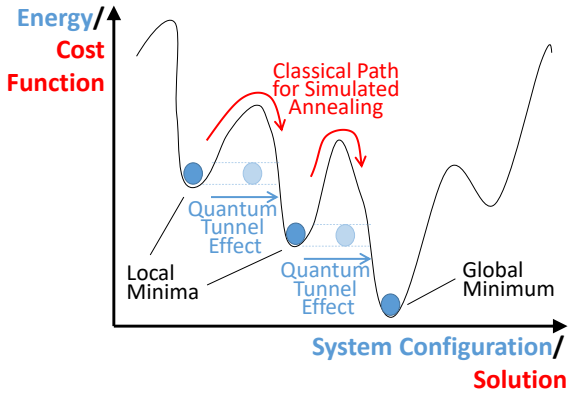


Quantum Computer

- 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

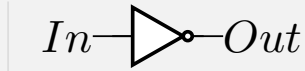
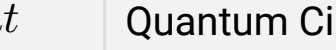
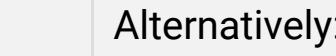


Quantum Circuit (Full Adder)

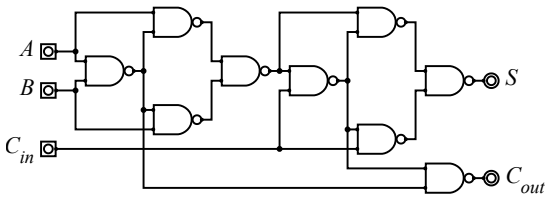
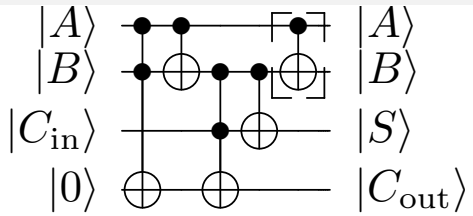


Simulated versus Quantum Annealing

Classical versus Quantum Computing

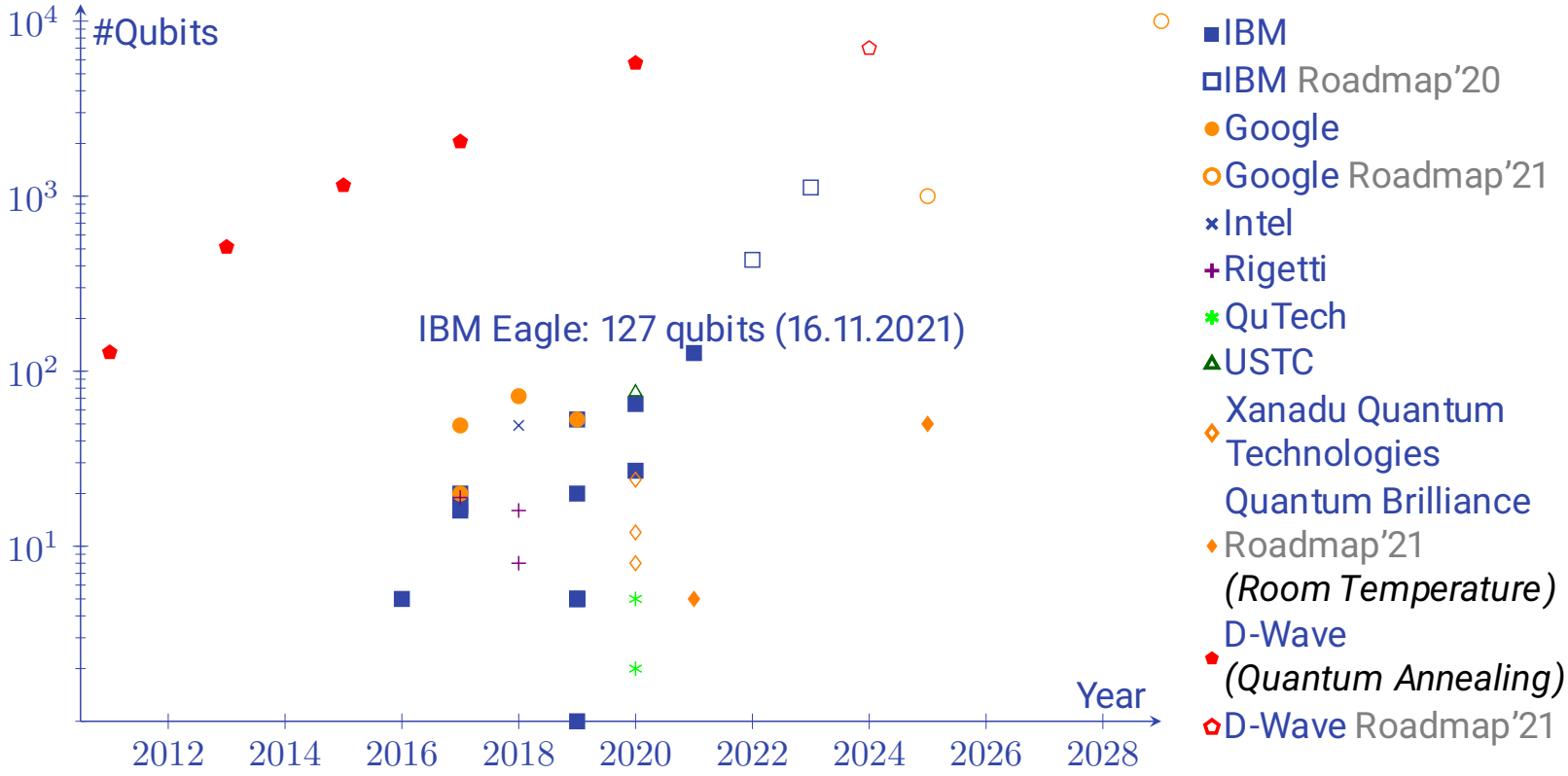
	Classical	Quantum
Information Unit	**Bi**nary Digi**t** (Bit): • basis of a 2-level system • can be in state 0 or 1	**Qu**antum **Bit** (Qubit): • basis of a 2-level quantum system • can be in state $\|0>$, $\|1>$ or in a linear combination of both states
Operation	Logic Gate: • performs on 1 or more 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:  In | Out 0 | 1 1 | 0	NOT/Pauli$_x$-Gate: Quantum Circuit:  Alternatively:  In | Out $\|0>$ | $\|1>$ $\|1>$ | $\|0>$ $\frac{1}{\sqrt{2}}(\|0>+\|1>)$ | $\frac{1}{\sqrt{2}}(\|0>+\|1>)$ $\frac{3\cdot i}{5}\|0>+\frac{4}{5}\|1>$ | $\frac{4}{5}\|0>+\frac{3\cdot i}{5}\|1>$

Digital versus Quantum Circuits

	Digital Circuit	Quantum Circuit
Building Blocks	Logic Gates	Quantum Logic Gates
Full Adder Example	 consists of NAND gates	 consists of Toffoli and CNOT gates[1]
In- and Output Full Adder	**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	$\|0>$ **and** $\|1>$ **as input:** Output is $\|0>$ and $\|1>$ 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** $\frac{1}{\sqrt{2}}(\|0>+\|1>)$ 0 0 **ABC$_{out}$S:** $\frac{1}{\sqrt{2}}(\|0000>+\|1001>)$ $\frac{1}{\sqrt{2}}(\|0>+\|1>)$ $\|A\rangle$ $\|1\rangle$ $\|A\rangle$ $\|B\rangle$ 0 0 1

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

Timeline of Quantum Computers



Main Data Source IBM Eagle Roadmaps: IBM Google Quantum Brilliance D-Wave

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 $\rightarrow$ 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

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...?)

Please contact me for collaborations: groppe@ifis.uni-luebeck.de