Quanto Vadis?

A Computer Science Perspective on Quantum Computing

Thomas Gabor

LMU Munich

Tag der Informatiklehrerinnen und -lehrer 2025, 2025-07-04

The Legend of Quantum Computing

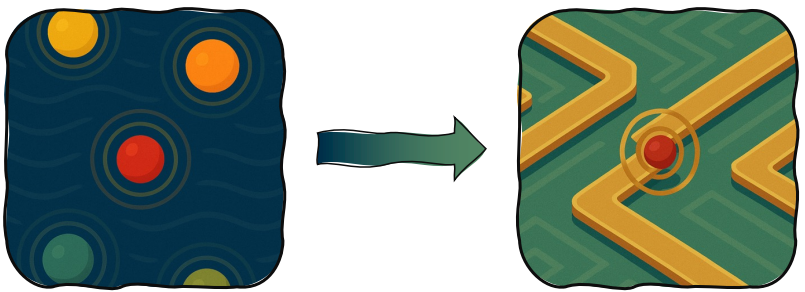
classical
discrete
computing

image by chatgpt.com

The Legend of Quantum Computing

quantum
real world

classical
discrete
computing



The Legend of Quantum Computing

quantum
real world

classical
discrete
computing

quantum
computations

Richard
Feynman

images by chatgpt.com

The Legend of Quantum Computing

quantum
real world

quantum
computing

quantum
computations

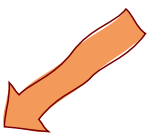
Richard
Feynman

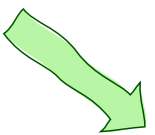
images by chatgpt.com

Are quantum computers useful
for computing something else?

Yes, if we can use their quantum effects.

"Strange" Quantum Effects
used in Quantum Computing





Superposition

Entanglement

Superposition

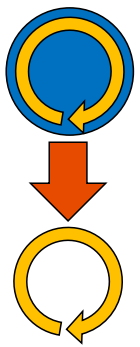
classical physics

particle

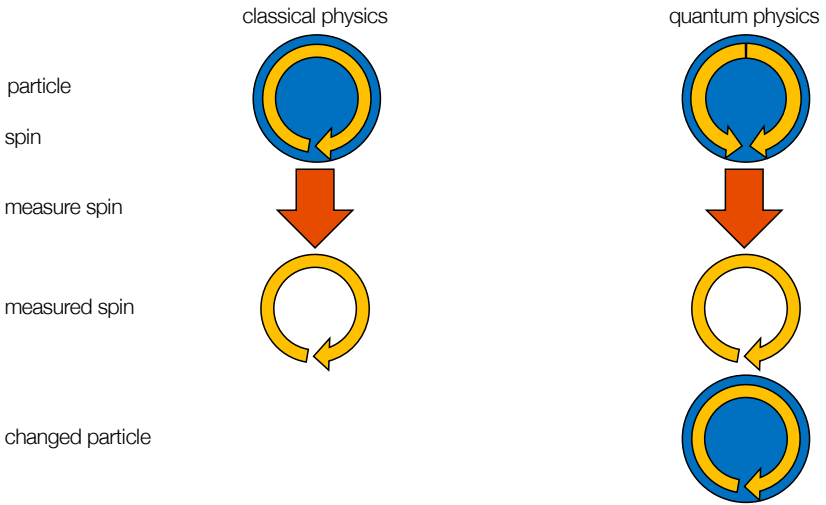
spin

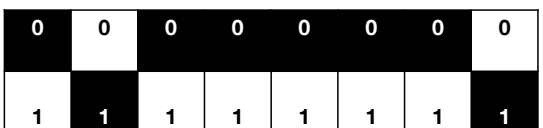
measure spin

measured spin

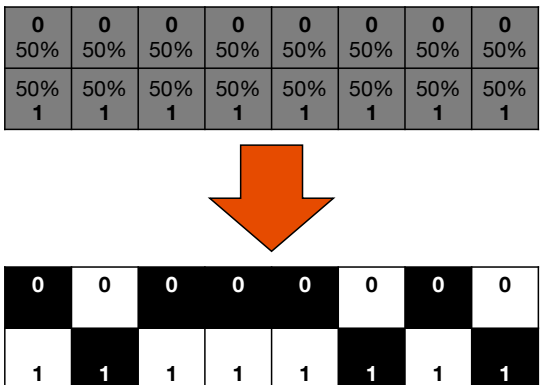


Superposition





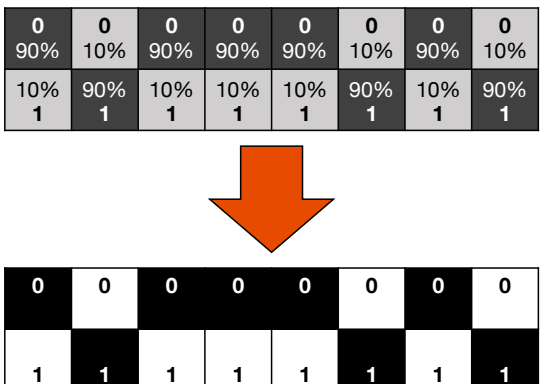
ASCII letter A



all ASCII chars
in superposition

measuring

ASCII char E with
probability 1/256

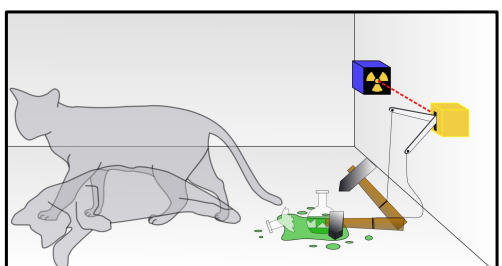


all ASCII chars
in superposition
(but probably E)

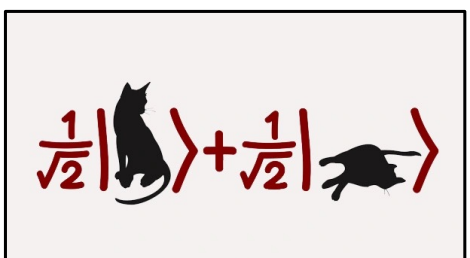
measuring

ASCII char E with
probability 0.43

Schrödinger's Cat



en.wikipedia.org/wiki/Schrödinger%27s_cat



www.motherjones.com/kevin-drum/2018/09/schrodingers-cat-is-alive-one-twelfth-of-the-time/

Schrödinger's Cat

i.redd.it/9w2ifbjagtm41.jpg

i.redd.it/gq3ehlg8nfx71.jpg

tvtropes.org/pmwiki/pmwiki.php/UsefulNotes/SchrodingersCat

xkcd.com/45

i.redd.it/aky5jzorxu661.jpg

Entanglement

multiple quantum particles

measure single spin

measured spin

changed particles

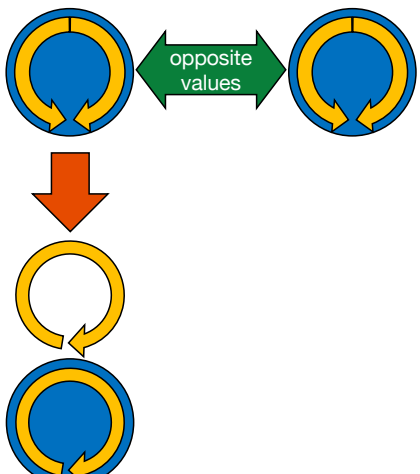
Entanglement

multiple quantum particles

measure single spin

measured spin

changed particles



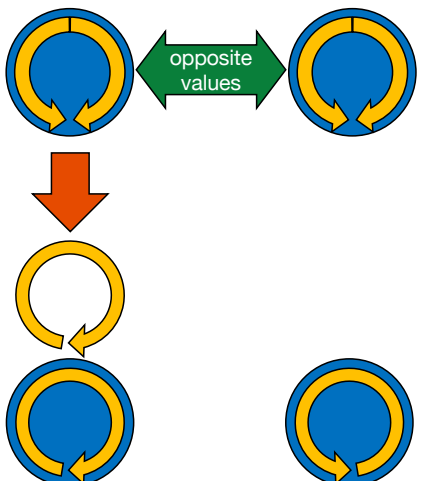
Entanglement

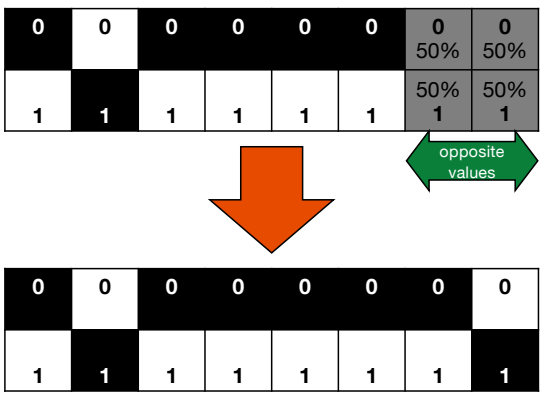
multiple quantum particles

measure single spin

measured spin

changed particles





ASCII chars A B at the same time

measuring

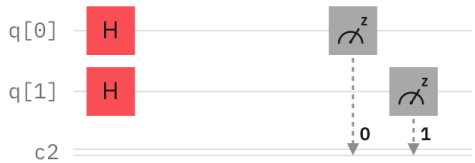
ASCII char A with probability 1/2

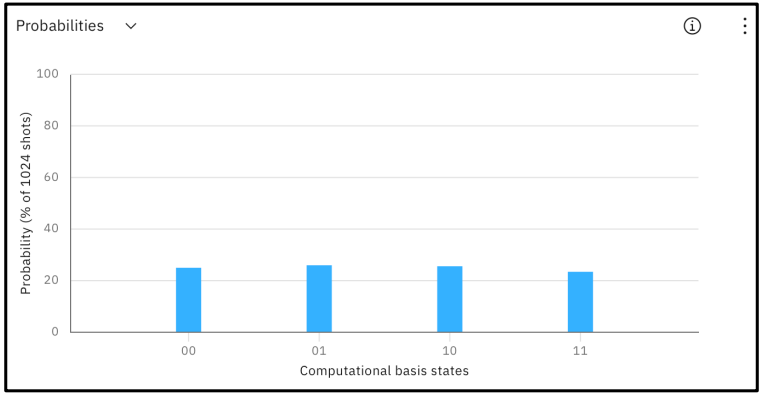
Einstein’s “Spukhafte Fernwirkung”

image by chatgpt.com

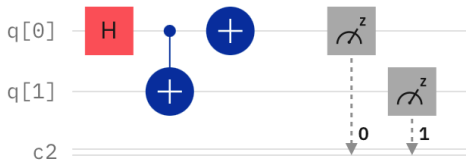
Let’s try

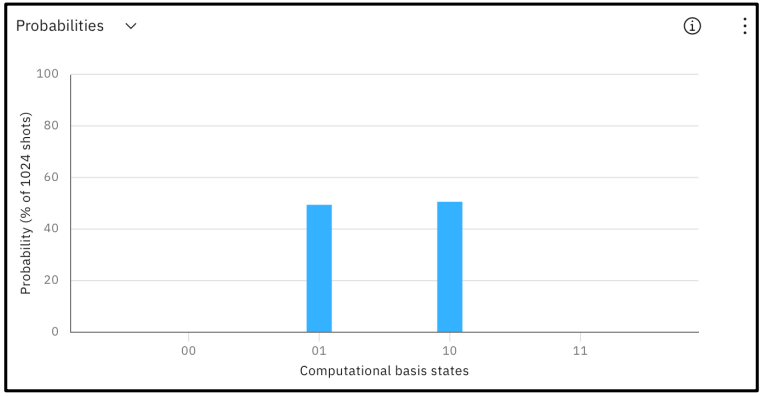
quantum-computing.ibm.com/composer





generated with quantum-computing.ibm.com/composer





generated with quantum-computing.ibm.com/composer

This looks very different from classical programming...

A little excursion:

Why do computers get hot
when they compute?

Deleted information needs to go somewhere.

Quantum algorithms are reversible up to measuring.

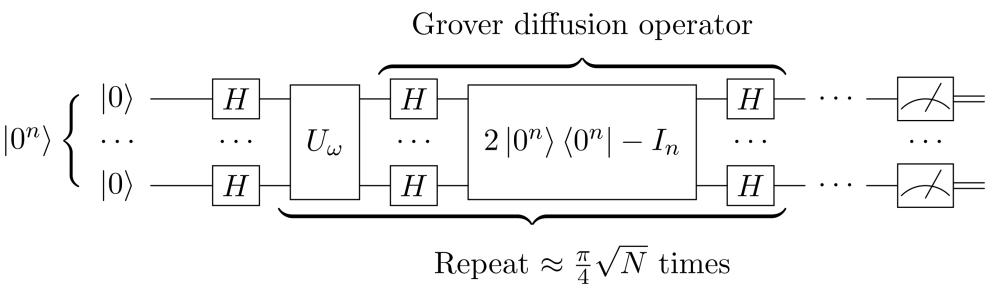
Are quantum computers useful
for computing something else?

Yes, if know the right algorithm.

Grover's Search

Problem: Search in unsorted data structure with N elements
Classical Complexity: $\mathcal{O}(N)$
Quantum Complexity: $\mathcal{O}(\sqrt{N})$

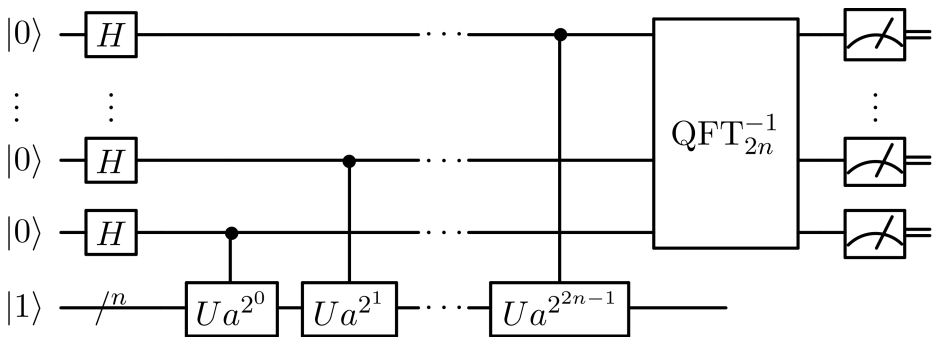
en.wikipedia.org/wiki/Grover%27s_algorithm



Shor's Algorithm

Problem: Prime factorization of integer N
Classical Complexity: best-known exponential in $\log N$
Quantum Complexity: polynomial in $\log N$

en.wikipedia.org/wiki/Shor%27s_algorithm

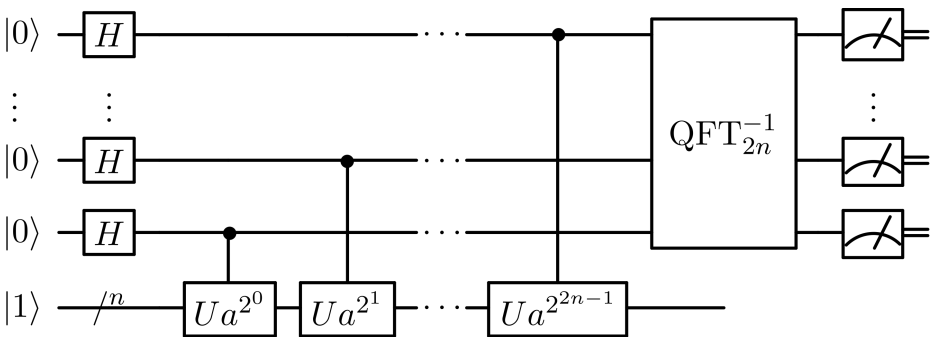


Shor's Algorithm

Problem: Prime factorization of integer N
Classical Complexity: best-known exponential in $\log N$
Quantum Complexity: polynomial in $\log N$

many variants of asymmetric cryptography rely on that

en.wikipedia.org/wiki/Shor%27s_algorithm

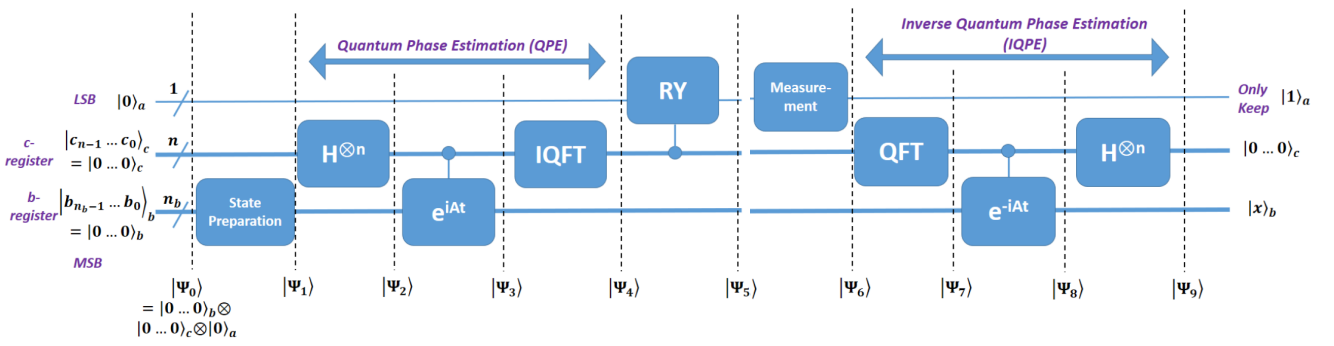


HHL Algorithm

Harrow, Hassidim, Lloyd

Problem: Solving linear systems of N equations with condition number κ
Classical Complexity: $\mathcal{O}(\sqrt{\kappa}N)$ for a scalar value computed from solution
Quantum Complexity: $\mathcal{O}(\kappa^2 \log N)$ for a scalar value computed from solution

adapted from arxiv.org/pdf/2108.09004.pdf

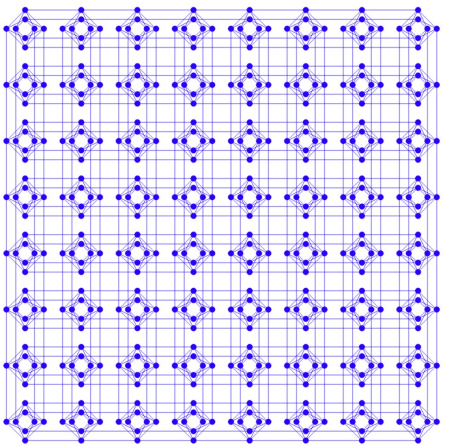


Quantum Annealing

Kadowaki, Nishimori

Problem: Solving (quadratic unconstrained binary) optimization problems
Classical Complexity: best-known exponential for exact solution
Quantum Complexity: probably exponential as well?

arxiv.org/pdf/1406.2741.pdf



The Question of Quantum Advantage

Is there any task for which
a quantum computer is
better than
any classical computer?

image by chatgpt.com

The Question of Quantum Advantage

Is there any task for which
a quantum computer is
better than
any classical computer?

Theorem 1 (Church-Turing thesis). Any computable function can be computed by a Turing machine.

Theorem 2 (extended Church-Turing thesis). Any computable function can be computed by a Turing machine *with at most polynomial overhead.*

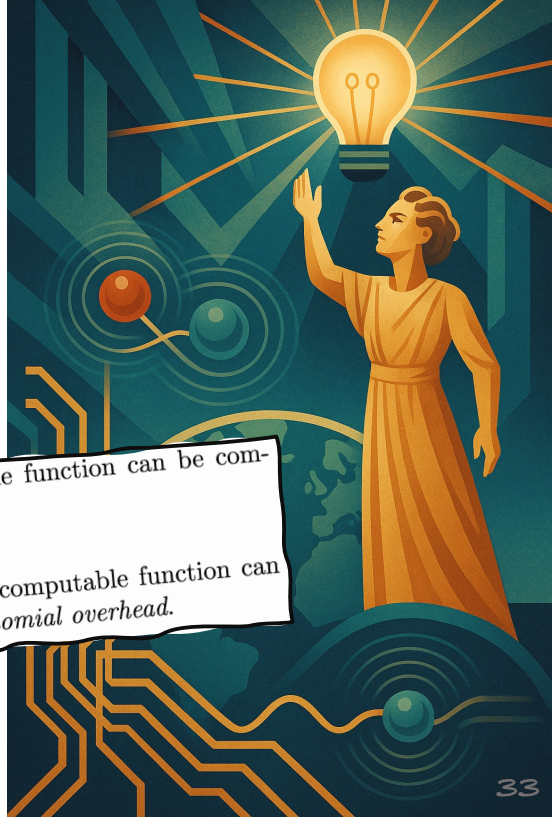


image by chatgpt.com

A Note on Quantum Communication

quantum-secure channels

blind quantum computing

image by chatgpt.com

physics

complexity theory

reversible computing

quantum computing

optimization & learning

communication & security

languages & theory

image by chatgpt.com

Quanto Vadis?

A Computer Science Perspective on Quantum Computing

Thank you!

Thomas Gabor

LMU Munich

Tag der Informatiklehrerinnen und -lehrer 2025, 2025-07-04