Quantencomputer und Komplexität

thosch

Alles was ich sage beruht auf meinen aktuellen Kentnisstand (07.02.2014) und kann morgen bereits überholt sein!

Quantencomputer

- Superpositionsprinzip
- Quantenverschränkung
- No-Cloning

Qubit

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

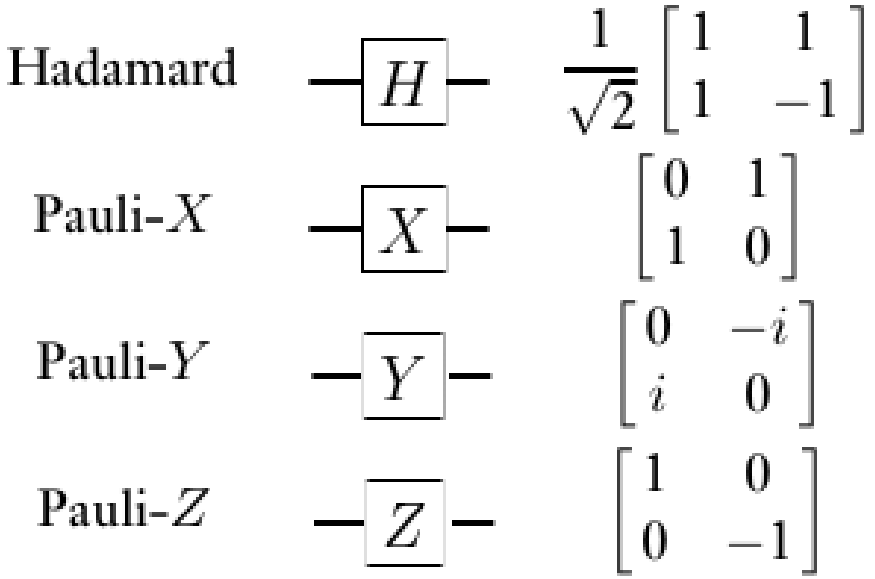
$$|a|^2 + |b|^2 = 1$$

Mehrere Qubits setzen sich als Tensorprodukt der einzelnen Hilberträume zusammen.

Quantengatter

unitäre Transformation auf Qubit

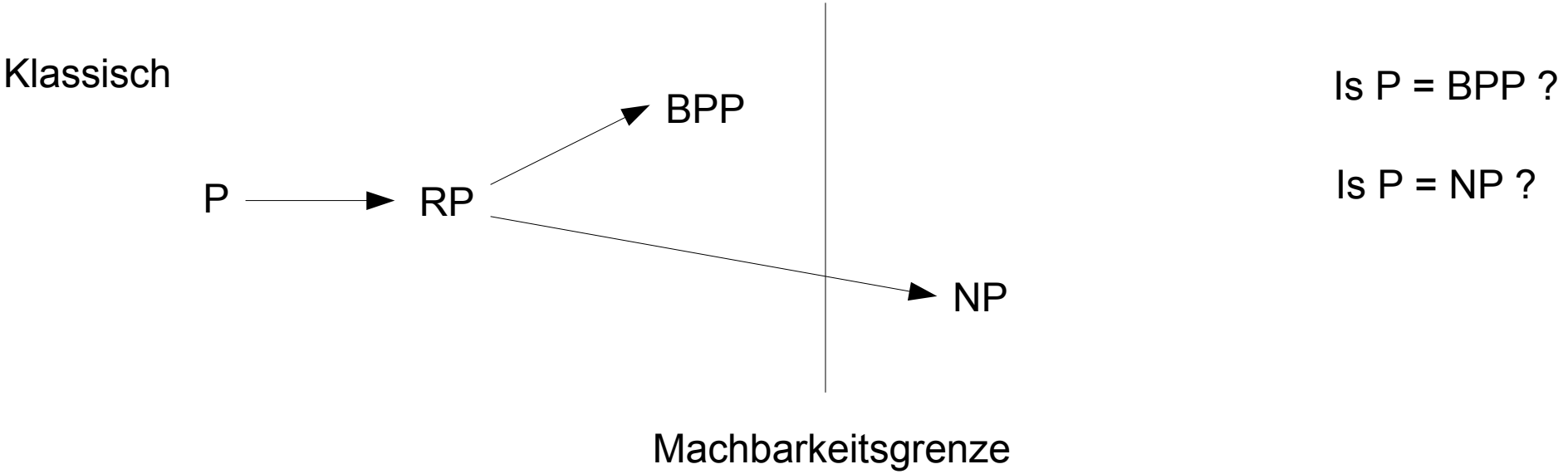
reversible Transformation



Algorithmen Quantencomputer

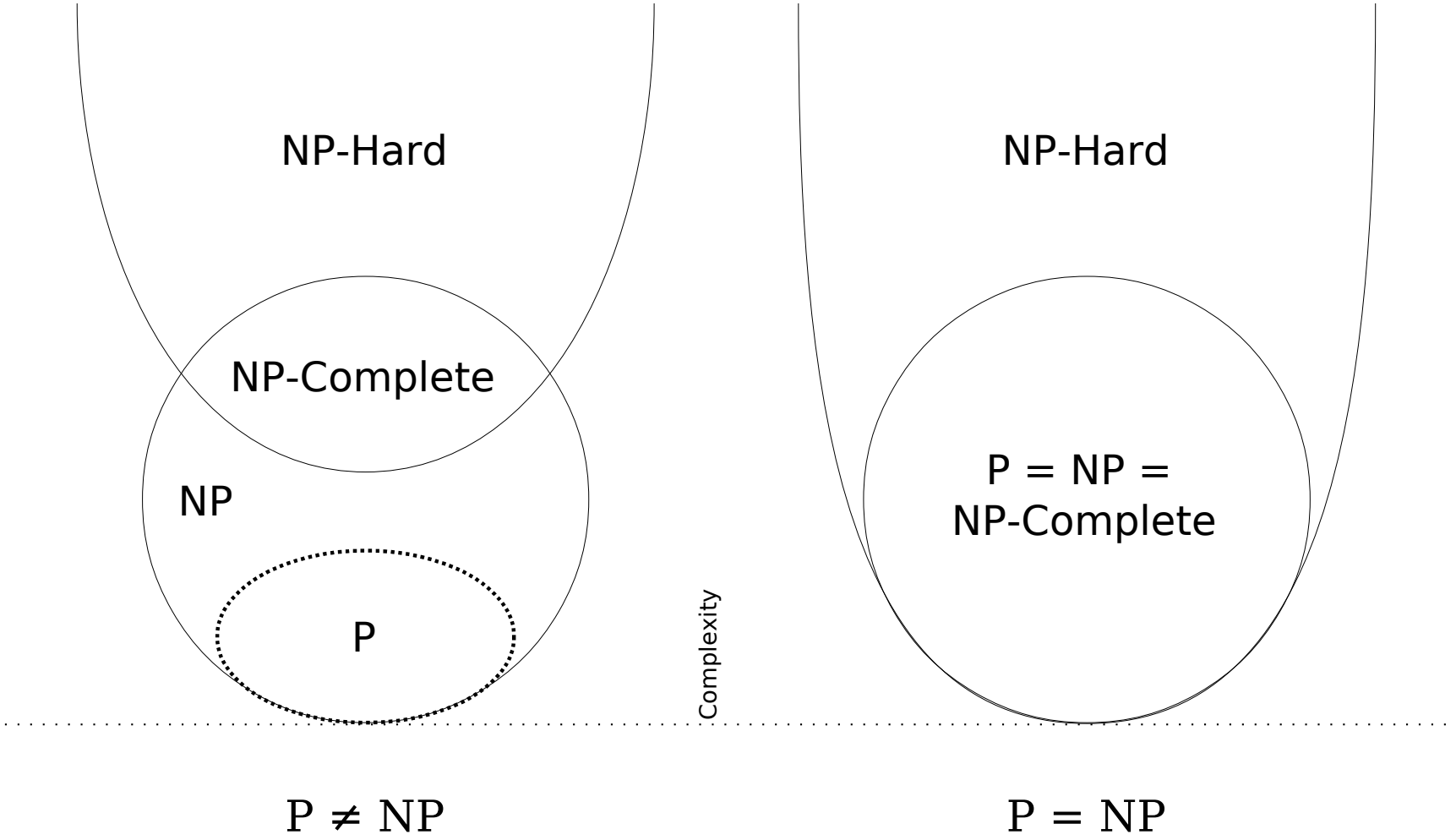
- Quanten-Fouriertransformation (Shor-Algoritmus)
- Quanten-Suchalgorithmen (Grover-Algorithmus)
- Quanten-Simulation

Komplexitätsklassen



- P polynomial time
- RP randomized polynomial time
- BPP bounded-error probabilistic polynomial time (decision problems)
- NP nondeterministic polynomial time (decision problems)

P/NP



http://de.wikipedia.org/w/index.php?title=NP-Vollst%C3%A4ndigkeit&oldid=125038815

Grover-Algorithmus

Suche in einer unsortierten Datenbank
mit N Einträgen in

$$\mathcal{O}(\sqrt{N})$$

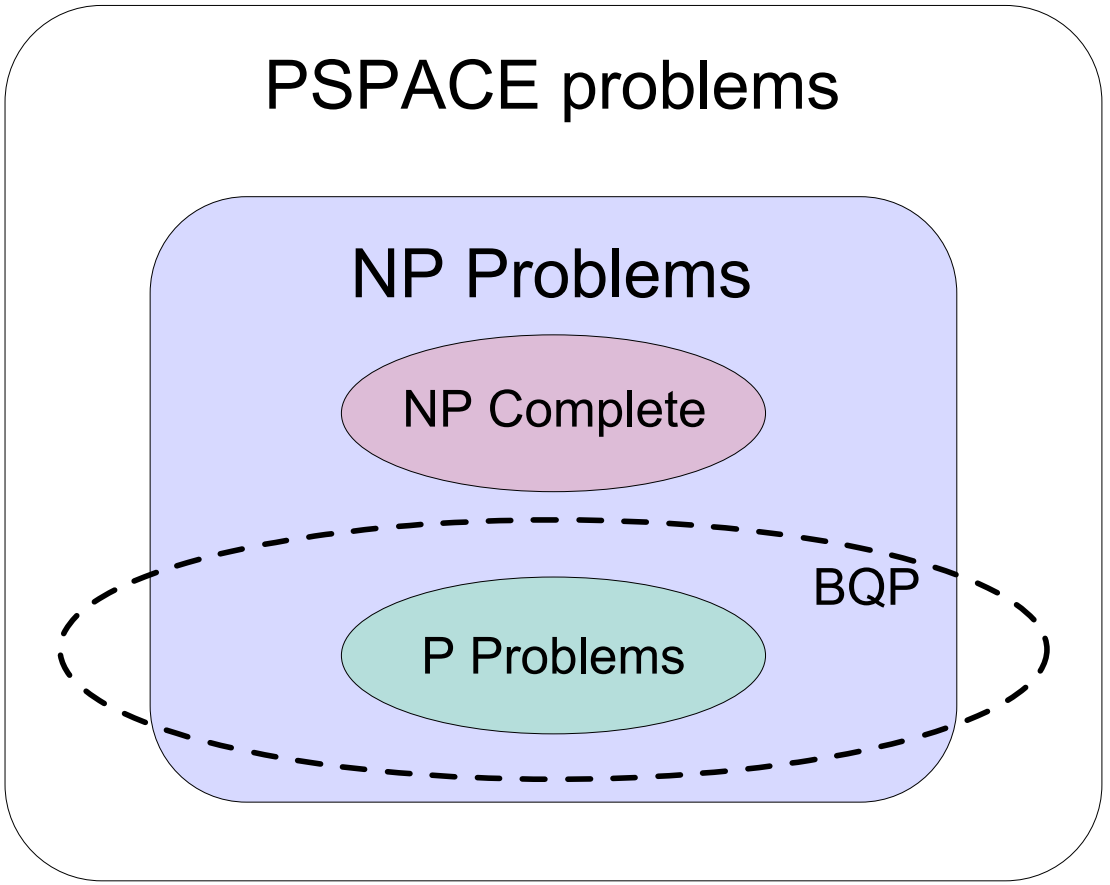
probabilistischer Algorithmus

Grover-Algorithmus ist optimal, kein schnellerer Quantenalgorithmus möglich

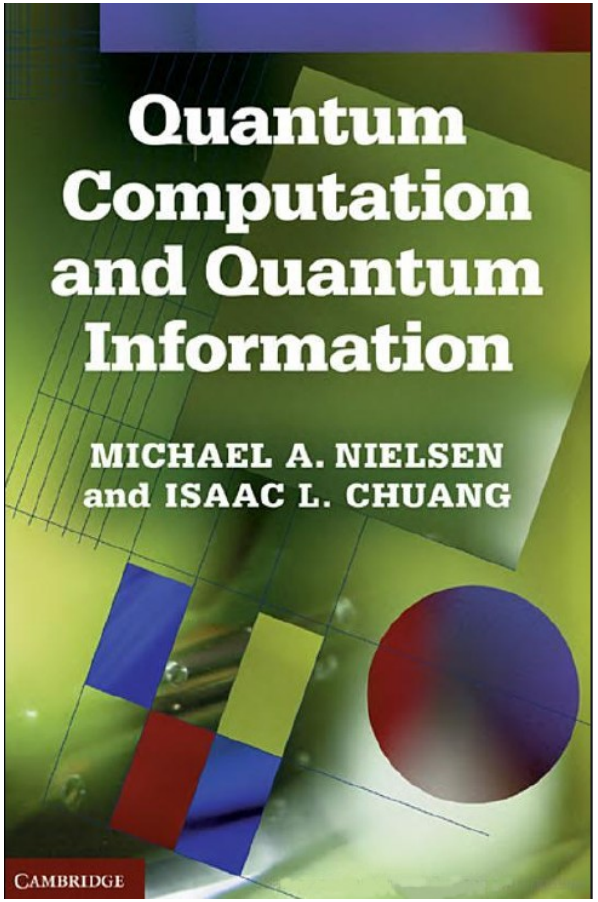
→ kein exponentieller Geschwindigkeitsvorteil

Komplexitätsklassen

BQP (bounded error quantum polynomial time)



http://de.wikipedia.org/w/index.php?title=BQP&oldid=116224717


Quantum Computation and Quantum Information
MICHAEL A. NIELSEN and ISAAC L. CHUANG
CAMBRIDGE