▲ Hochschule Harz
Hochschule für angewandte Wissenschaften

DAV/DGVFM
Herbsttagung
2022

DAV-Herbsttagung 2022, 15.11. Rheingoldhalle Mainz

Quantum Computing: Hype oder Heilsbringer?

Bildquelle: Pixabay

▲ Hochschule Harz
Hochschule für angewandte Wissenschaften

Datum: 15.11.2022
Prof. Dr. F. Transchel
Fachbereich AI

Prof. Dr. Fabian Transchel

Zur Person

An der HS Harz seit 2020

- Stiftungsprofessur „Data Science“ der E+S Rückversicherung AG
- Studiengangskoordinator M.Sc. Data Science (alle Varianten)

Berufspraxis: Senior Data Scientist in der Versicherungsbranche

- Kfz-Telematik / Fahrassistenzsysteme / Autonomes Fahren

Forschungsschwerpunkte

- Actuarial Data Science
- Kfz-Versicherung / Mobility
- Erklärbarkeit / Regulatorik von KI-Modellen

Bildquelle: Hochschule Harz

Quantum Computing in den Aktuarswissenschaften

Agenda

- Was ist Quantum Computing und (warum) ist das wichtig?
- Was sind denkbare Auswirkungen auf die Aktuarswissenschaften bzw. Actuarial Data Science?
- Was kann und sollte aktuell konkret unternommen werden?

Quantum Computing in den Aktuarswissenschaften

Was zum #*/% ist Quantum Computing?

- Einige Effekte der Quantenmechanik erlauben „interessante“ Konzepte, die für abstrakte Berechnungen verwendet werden können
  - Inhärente komplex-wertige Beschreibung der physikalischen Realität
  - „Echter“ Zufall
  - „Verschränkung“
  - „Quantensuperposition“
  - „Quantenparallelismus“
  - „Quantum Supremacy“
- Anwendungen
  - Optimierungsprobleme (Finance, Logistik, Energie)
  - Simulation (Chemie, Biotech, Materialwissenschaften)
  - Kryptographie (→ Nobelpreis 2022)

Quantum Computing in den Aktuarswissenschaften

Was zum #*/% ist Quantum Computing?

Allgemein wird vermutet, dass Quantum Computing die **Church-Turing-These** erfüllt:

- *Ein Funktional auf den Natürlichen Zahlen kann von einer Methode genau dann effektiv berechnet werden, wenn sie von einer Turingmaschine berechnet werden kann.*

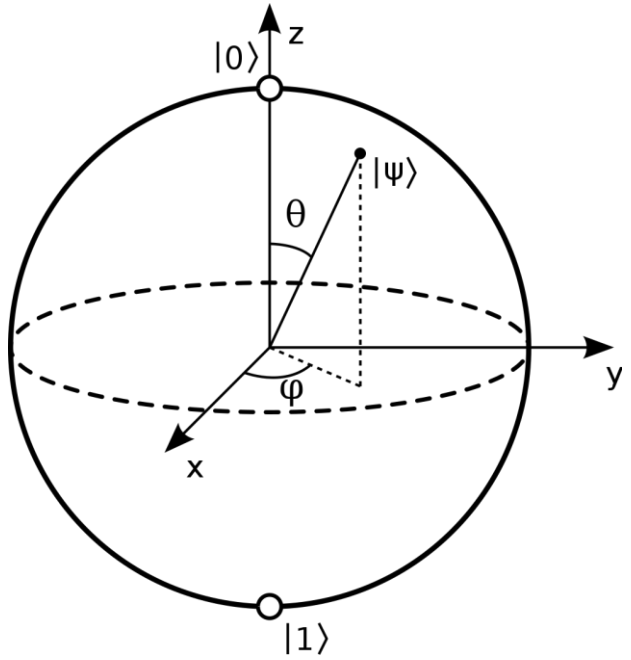
- Dies ist zutreffend in mindestens der Hinsicht, dass **Quantenmechanik von Turingmaschinen simuliert werden kann**, wenngleich mit exponentiellem Overhead: 2^N Zahlen werden benötigt, um ein N-Quanten-Problem zu beschreiben.

- Daher ergibt sich die Frage: *Kann irgendein Quantenfunktional effizient simuliert werden*?

  → ***Auf jeden Fall von Quantencomputern!***

- Die sog. „**Quantum Supremacy“**: Quantum computers sind darin überlegen, *einige spezifische Probleme zu lösen*, aber in jedem Fall **mindestens so effizient wie klassische Computer**, wenn klassische Probleme gelöst werden.

Quantum Computing
Wie funktioniert QC?



Qubits und die Hilbert-Algebra

- Grundlegende Informationseinheit: Das **Qubit**

- Qubits folgen den spezifischen Regeln der **Hilbert-Algebra**:
  - Quanten-Zustände sind Vektoren beschrieben als sog. **Kets**: $|0\rangle$ und $|1\rangle$
  - Jedes Qubit kann sich in **Superposition** von $|0\rangle$ und $|1\rangle$ befinden,
    daher ergibt sich $|\Psi\rangle = \alpha\,|0\rangle + \beta|1\rangle$ mit $|\alpha^2|+|\beta^2| = 1$.

- **Born'sche Regel**[1]: Bei Messung von $|\Psi\rangle$, erhält man $|0\rangle$ mit W-Keit $|\alpha^2|$ und $|1\rangle$ mit W-Keit $|\beta^2|$.
  - Kohärente Kombination (d.h. „Verschränkung") von Qubits erlaubt die Konstruktion von **Gemischten Zuständen**,
    d.h. $|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ und man erhält entweder genau $|0\rangle|0\rangle$ oder genau $|1\rangle|1\rangle$ durch Messung, jeweils mit W-Keit 0.5.

[1]Auch: „Kopenhagener Deutung der Quantenmechanik", heute sog. Standardinterpretation

Quantum Computing
Wie funktioniert QC?

Berechnungsparadigma: Durch die Born‘sche Regel ergibt sich die Notwendigkeit probabilistischer Berechnungen

- **Quantum Gate Model[1]**
  - Logische Quantengatter ähnlich jenen aus der klass. Informatik, aber komplexwertige Hilbert-Operatoren
- **One-way Quantum Computer (Briegel-Paradigma)[2]**
  - Superpositionen von kohärenten Quantenzuständen sind die „Berechnungsressource“
    → Das zu lösende Problem wird als problemspezifischer Quantenoperator kodiert
- **Adiabatische Quantencomputer (→ *KEINE universale QC*)[3]**
  - Quantenversion von *Simulated Annealing*, anwendbar auf Optimierungsprobleme wie frustrierte Spin-Gitter

[1] Vatan, Farrokh and Colin P. Williams. “Optimal quantum circuits for general two-qubit gates (5 pages).” Physical Review A 69 (2004): 32315.
[2] Robert Raussendorf, Daniel E. Browne, Hans J. Briegel The one-way quantum computer – a non-network model of quantum computation, Journal of Modern Optics, Band 49, 2002, S. 1299, arxiv:quant-ph/0108118
[3] Apolloni, Bruno; Cesa-Bianchi, Nicolo; De Falco, Diego (July 1988). "A numerical implementation of quantum annealing". Stochastic Processes, Physics and Geometry,

Quantum Computing
Wie funktioniert QC?

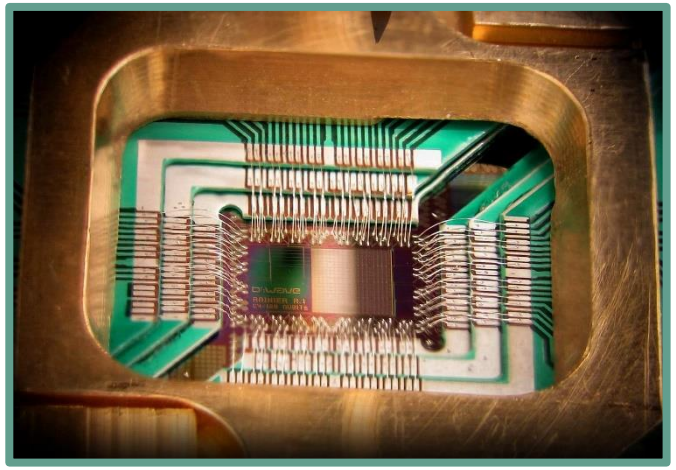
Berechnungsparadigma: Durch die Born‘sche Regel ergibt sich die Notwendigkeit probabilistischer Berechnungen

All diesen Modellen ist gemein, dass für die Kodierung eines Problems eine Kombination eines Quantenzustands und eines Messoperators bestimmt werden muss, gefolgt von einer Messung des Systemzustands oder eines Annealings.

[1] Vatan, Farrokh and Colin P. Williams. “Optimal quantum circuits for general two-qubit gates (5 pages).” Physical Review A 69 (2004): 32315.
[2] Robert Raussendorf, Daniel E. Browne, Hans J. Briegel The one-way quantum computer – a non-network model of quantum computation, Journal of Modern Optics, Band 49, 2002, S. 1299, arxiv:quant-ph/0108118
[3] Apolloni, Bruno; Cesa-Bianchi, Nicolo; De Falco, Diego (July 1988). "A numerical implementation of quantum annealing". Stochastic Processes, Physics and Geometry,

Quantum Computing
Wie funktioniert QC hardwareseitig?

- Dekohärenz erfordert für aktuelle Hardware die Operation bei ~0 Kelvin
- State of the art: ~128 Qubits – „Quantum Moore‘s Law“ noch nicht etabliert
- Marktreife Systeme verwenden supraleitende Halbleiter, aber optronische Quantencomputer scheinen langfristig vielversprechender
- Der D-Wave® Quantum Annealing Processor verwendet begrenzte Verbindungen zwischen seinen Qubits für einen Kompromiss zwischen Dekohärenz und Effizienz
- Wie bei den ersten klass. Computern auch werden Quantensysteme aktuell vorrangig von Konzernen und Research Labs betrieben: NASA, DLR bzw. Google, IBM, Lockheed Martin



Quantum Computing
Wie funktioniert QC softwareseitig?

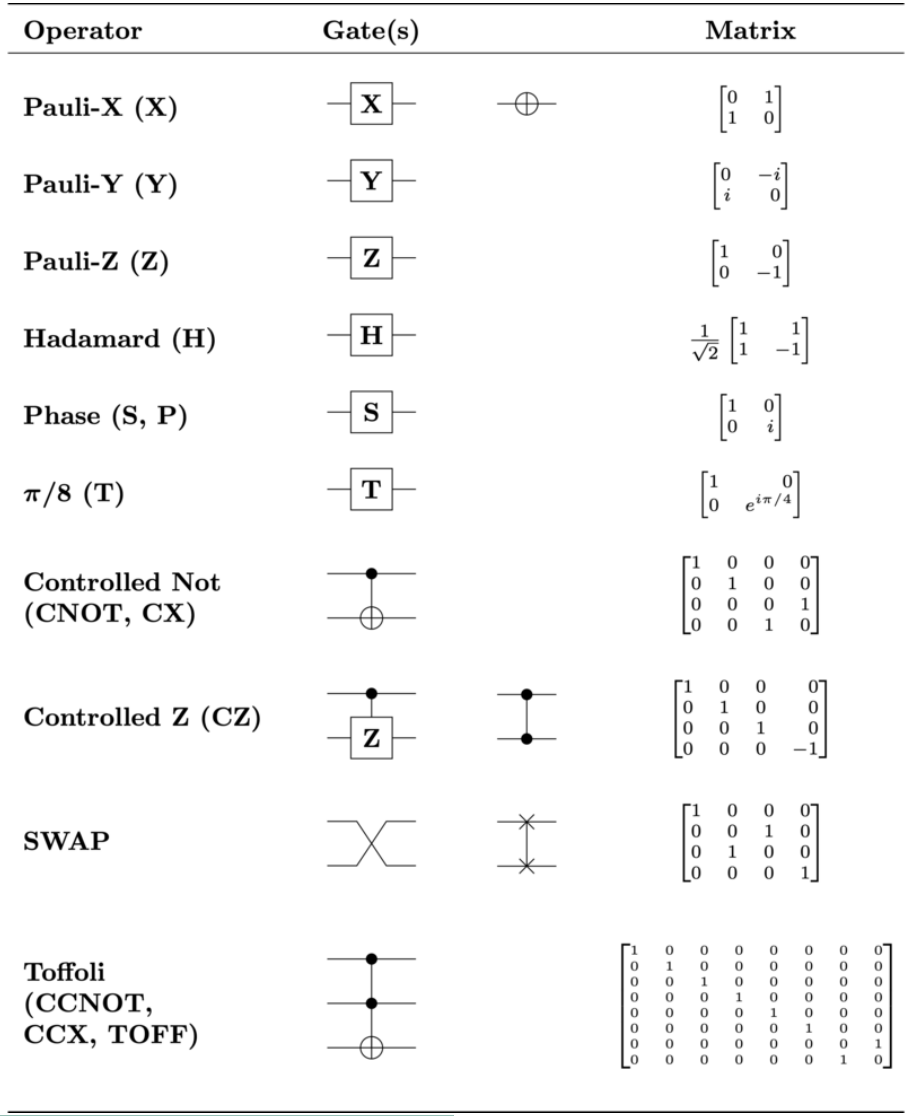
Quantum Gate-Paradigma

Idee:
Eine Menge von unverschränkten („reinen“) Qubits verwenden, um einen problemspezifischen Zustabnd herzustellen, der mit eingrenzbarer Genauigkeit gemessen werden kann (d.h. > 50%
W-Keit in endlicher Zeit)

Universalität:

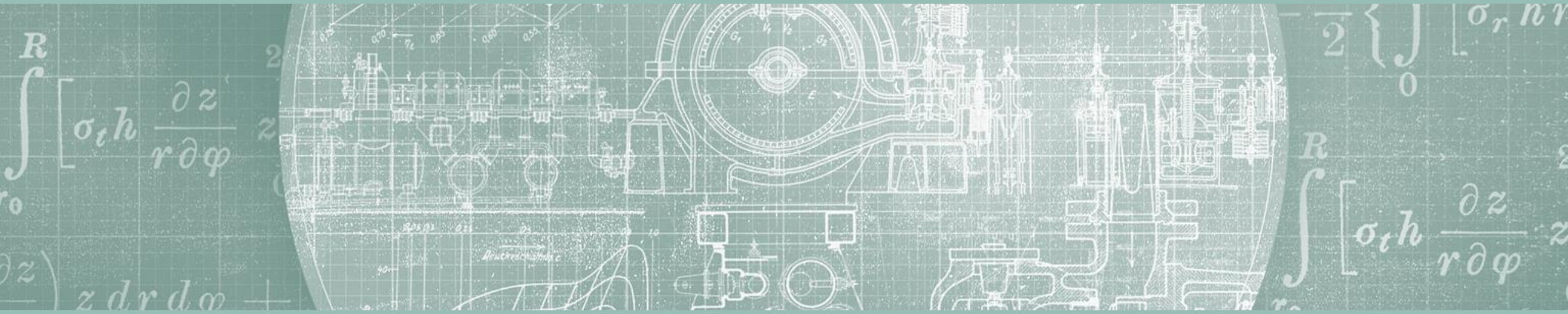
Bei klass. Computern gilt De Morgan‘s Regel, die besagt, dass das NAND-Gate (oder das NOR-Gate m.m.) funktional vollständig ist
→ Es gibt kein einzelnes Q-Gate, das funktional vollständig ist:

Nur $\{X, Y, Z, S, CX\}$, $\{CX, H, S, T\}$, $\{TOFF, H\}$ und ein paar exotischere Kombinationen sind jeweils universal.



Bildquelle: https://en.wikipedia.org/wiki/Quantum_logic_gate#/media/File:Quantum_Logic_Gates.png, CC BY-SA 4.0

Quantenalgorithmen



▲ Hochschule Harz
Hochschule für angewandte Wissenschaften

Datum: 15.11.2022
Prof. Dr. F. Transchel
Fachbereich AI

Quantum Computing
Grover-Algorithmus

- Der Grover-Algorithmus findet einen Wert in einer (Quanten-)Datenbank in $\mathcal{O}(\sqrt{N})$ Schritten.
- Klassische Suche (ohne Optimierung) hat die Komplexität $\mathcal{O}(N)$ Schritte.

  → War der erste Quantenalgorithmus, der einen quadratischen ***Quantum Speedup*** demonstriert hat.

  → Weil Suchen komplexitätstheoretisch verhältnismäßig trivial ist, ergeben sich keine Implikationen im Hinblick auf Quantum Supremacy.

- Problem: Um Quantensuchen durchzuführen muss die gesamte Datenbank als Quantenzustand vorliegen.

Quantum Computing
Shor-Algorithmus

- Der Shor-Algortihmus faktorisiert natürlich Zahlen in $\mathcal{O}((\log n)^3)$. Der Algorithmus ist in **BQP**.

- Bester klassischer Algorithmus: $\mathcal{O}(1+\varepsilon)^b)$. Es wird vermutet, dass Faktorisierung in **NP**, aber nicht in **P ist**, aber es gibt keinen Beweis dafür.

- Note: Es wird zudem vermutet, dass Faktorisierung ***nicht*** NP-vollständig ist.
  → Das würde bedeuten, dass auch Quantencomputer wahrscheinlich NP-vollständige Problems ***nicht*** in polynomieller Zeitkomplexität lösen könnten.

- Praktische Relevanz: Komplexität von Faktorisierung ist in der Kryptographie lebensnotwendig für Shared-Key-Verschlüsselungen, denn ihre **Sicherheit hängt von der Schwierigkeit der Faktorisierungsaufgabe ab**.

Quantum Computing
Toolkit für Quantencomputing

- Ein Toolkit übernimmt idealerweise Error Correction und low-level-Encodings für uns

  (→ Natürlich kann man das auch selbst erledigen, wenn man unbedingt möchte…)

- **Pennylane**  **(OpenQASM: Quantum Assembly Language)**
  - Nahtlose Integration von quantenmechanischer und klassischer Berechnungen via „**device coupling**“
  - Vollständig kompatibel zu Tensorflow, Pytorch, Numpy, …

- **QISKIT (IBM, QASM-kompatibel)**
  - Cloud-Zugriff auf IBM Quantum Computing Service via Notebook interface (Julia, Python)

Quantum Computing
Toolkit für Quantencomputing

Wie funktioniert das?

„Ziemlich gut!“

```
include "qelib1.inc"
qreg q[5];                // allocate 5 qubits (set automatically to |00000>)
creg c[5];                // allocate 5 classical bits

h q[0];                   // Hadamard-transform qubit 0
cx q[0], q[1];            // conditional pauli X-transform (ie. "CNOT") of qubits 0 and 1
                          // At this point we have a 2-qubit Bell state (|00> + |11>)/sqrt(2)

cx q[1], q[2];            // this expands entanglement to the 3rd qubit

measure q[0] -> c[0];     // this measurement collapses the entire 3-qubit state
measure q[1] -> c[1];     // therefore qubit 1 and 2 read the same value as qubit 0
measure q[2] -> c[2];
```

Preparation

Manipulation

Messung

Source code: https://en.wikipedia.org/wiki/IBM_Quantum_Experience

Und jetzt zur dunklen Seite

Bildquelle: Pixabay

▲ Hochschule Harz
Hochschule für angewandte Wissenschaften

Datum: 15.11.2022
Prof. Dr. F. Transchel
Fachbereich AI

Quantum Computing
Theoretische Limitierungen

Die No-Gos

Der Berechnung mit Qubits liegen quantenmachanisch einige seltsame Regeln zugrunde:

- **No-cloning-Theorem**

  „It is impossible to create an independent and identical copy of an arbitrary unknown quantum state.“[1]

- **No-deletion-Theorem**

  „In general, given two copies of some arbitrary quantum state, it is impossible to delete one of the copies.“[2]

- **No-broadcasting-Theorem**

  „Given a pair of quantum states which do not commute, there is no method capable of taking a single copy of either state and succeeding, no matter which state was supplied.“[3]

[1] Wootters, William; Zurek, Wojciech (1982). "A Single Quantum Cannot be Cloned". *Nature*. **299**
[2] Pati, A. K., Braunstein, S. L. (2000), "Impossibility of Deleting an Unknown Quantum State", *Nature* **404**
[3] Barnum, H., Caves, C.M., Fuchs, C.A., Jozsa, R., Schumacher, B. (1996), "Noncommuting Mixed States Cannot Be Broadcast". Physical Review Letters. 76 (15)

Quantum Computing
Praktische Limitierungen (1)

- Wie man bei den Algorithmen von Grover und Shor sieht, **muss stets ein Startzustand präpariert werden.**
  → Der Aufwand steigt *schneller als linear* mit der Inputgröße. → Sogenannte **Dekohärenz**.

- **Dekohärenz**: Gradueller Verlust von Quantenverschränkung durch thermisch-physikalische Störungen.

  → „Spontaner Kollaps der Wellenfunktion“ (→ Schrödingers Katzenbox wird zufällig geöffnet.)

- Umgang mit Dekohärenz: **Quantum Error Correction**[1]

  - Um Quantenzustände für Berechnungen intakt zu halten, werden in der Praxis **viele physische Qubits pro logischem Qubit gebraucht**.

  - **Beispiel**: Im Shot-Algorithmus erfordern fehlertolerante Berechnungen insgesamt **neun physische Qubits pro verwendetem logischem Qubit**[2]

1. *Devitt, Simon J; Munro, William J; Nemoto, Kae (2013-06-20). "Quantum error correction for beginners". Reports on Progress in Physics. **76** (7): 076001. arXiv:0905.2794.*
2. *W.Shor, Peter (1995). "Scheme for reducing decoherence in quantum computer memory". Physical Review A. **52** (4): R2493–R2496.*

Quantum Computing
Praktische Limitierungen (2)

Es gibt auch in der Quantenwelt ein **No-Free-Lunch-Theorem**[1]:

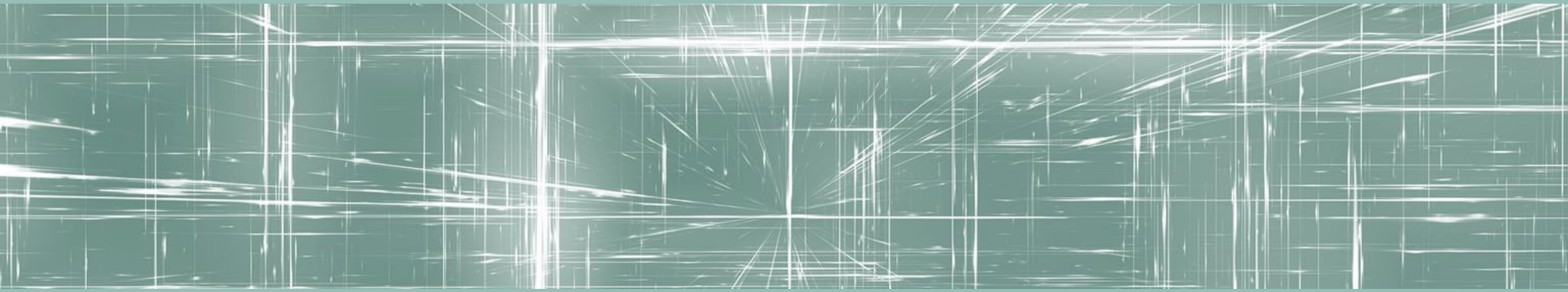
„Über alle Klassen von Problemen gemittelt performen alle Quanten-Optimierungsalgorithmen asymptotisch identisch.“

→ Es ist immer ein **Tradeoff** nötig zwischen möglichem **Effizienzvorteil** durch Quantum Computing und dem **gegenüberstehenden Mehraufwand** für Encoding, Kühlung, Betrieb andererseits.

→ Es gibt informationstheoretisch aktuell nicht viel Grund zur Annahme, die Existenz von **Quantum Supremacy** für eine breite Klasse von Algorithmen zu vermuten.

[1] Poland, Kyle Lewis et al. “No Free Lunch for Quantum Machine Learning.” arXiv: Quantum Physics (2020)

Quantum Machine Learning



Bildquelle: Pixabay

▲ Hochschule Harz
Hochschule für angewandte Wissenschaften

Datum: 15.11.2022
Prof. Dr. F. Transchel
Fachbereich AI

Quantum Computing
Quantum Machine Learning: Ein Überblick

- Mit der praktischen Verfügbarkeit von marktreifen Quantencomputern (wenngleich mit niedriger Anzahl Qubits), wurde eine ganze Reihe von neuen Algorithmen im Bereich Quantum Machine Learning vorgeschlagen:
  - Quantum Support Vector Machines
  - Quantum Gradient Boosting
  - Quantum Neural Nets
  - Quantum (Simulated) Annealing
  - u.v.m.

Quantum Computing
Quantum Machine Learning: Ein Überblick

- Mit der praktischen Verfügbarkeit von marktreifen Quantencomputern (wenngleich mit niedriger Anzahl Qubits), wurde eine ganze Reihe von neuen Algorithmen im Bereich Quantum Machine Learning vorgeschlagen:
  - Quantum Support Vector Machines
  - Qu
  - Qu
  - Qu
  - u.v.m.

Wichtige Praxisunterscheidung

→ *Ist das Modell oder der Algorithmus quantenmechanisch?* ←

Falls es sich um das Modell handelt, ergeben sich profunde Probleme im Hinblick auf die Reproduzierbarkeit und nur Monte Carlo-basierte Ensemble-Ansätze scheinen zweckmäßig:

Quantenmodelle können bis dato nicht gespeichert werden.

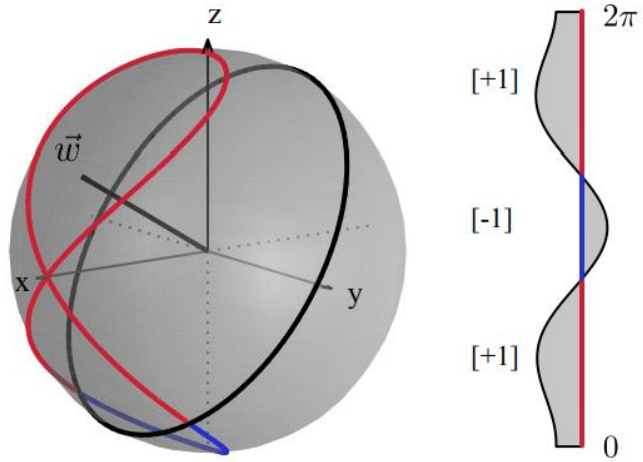
Quantum Computing

Quantum Machine Learning: Quantum SVM[1]

- Wie bei klassischen Support Vector Machines auch, werden für eine Vorhersage die Beobachtungen auf die konvexe Hülle der jeweiligen Klassen abgebildet.

- Wichtiger Unterschied: Das sog. Quantum feature muss nicht den Kernel-Trick verwenden – das Encoding wird ***direkt*** auf den Dualraum des problems abgebildet.
  → Das Encoding ***ist*** der Schätzer.

- Die Quantenversion ist effektiv überlegen, wenn die Lösung des Problems einen ***sehr großen*** Kernraum erfordert.



- Prinzipiell sollte dies beliebige Präzision erlauben, aber es gibt zwei Herausforderungen:
  - Entweder müssen mehrere Messungen durchgeführt werden (d.h. lineare Aufwandssteigerung für wurzel-wertige Präzisionsgewinn) *oder*
  - Alternativ wird der Zustandsraum weiter vergrößert – d.h. man muss mehr Error Correction betreiben, die die Anzahl der logischen Qubits effektiv begrenzt.

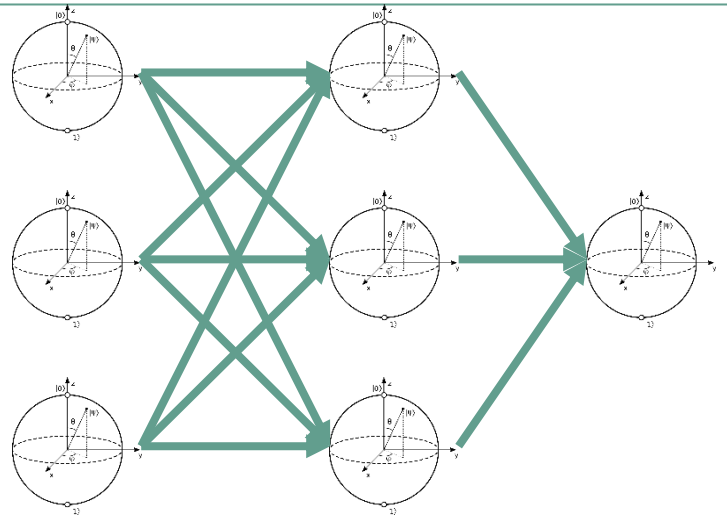
1. Havlíček, Vojtěch et al. "Supervised learning with quantum-enhanced feature spaces." *Nature* 567 (2019): 209-212.

Quantum Computing

Quantum Machine Learning: Quantum Neural Nets[1]

- Drei strukturell unterschiedliche Typen von **quantum neural nets**:

	Input-Typ	
Netzwerk-Typ	C-C	C-Q
	Q-C	Q-Q



- **Quanten-Perceptron**: Neuronen mit „**Quoronen**“ ersetzen

  → **Quoronen können in Superposition von „aktivieren“ und „nicht aktivieren“ sein.**

- Netzwerkstrukturen ohne dichte Schichten können von sog. „Finitely Correlated States“ (d.h. Quantensystemen mitZuständen)

1 Kak, S. (1995). "On quantum neural computing". *Advances in Imaging and Electron Physics*. **94**: 259–313.
2 da Silva, Adenilton J.; Ludermir, Teresa B.; de Oliveira, Wilson R. (2016). "Quantum perceptron over a field and neural network architecture selection in a quantum computer". *Neural Networks*. **76**: 55–64
3 Beer, Kerstin; Bondarenko, Dmytro; Farrelly, Terry; Osborne, Tobias J.; Salzmann, Robert; Scheiermann, Daniel; Wolf, Ramona (2020). "Training deep quantum neural networks". *Nature Communications*. **11** (1): 808.

Quantum Computing
Quantum Machine Learning: Quantum Boosting

- „Quantum Boosting“ erfährt in folgender Hinsicht eine mehrdeutige Verwendung:
  - Alle BQP-Algorithmen sind „geboosted“, weil Messung-basierte Quantenalgorithmen per definitionem schwache Lerner darstellen.

    → *Viele Schriften verwenden den Begriff „Quantum Boost“ – keinerlei Verknüpfung mit Boosting im ML-Sinne!*

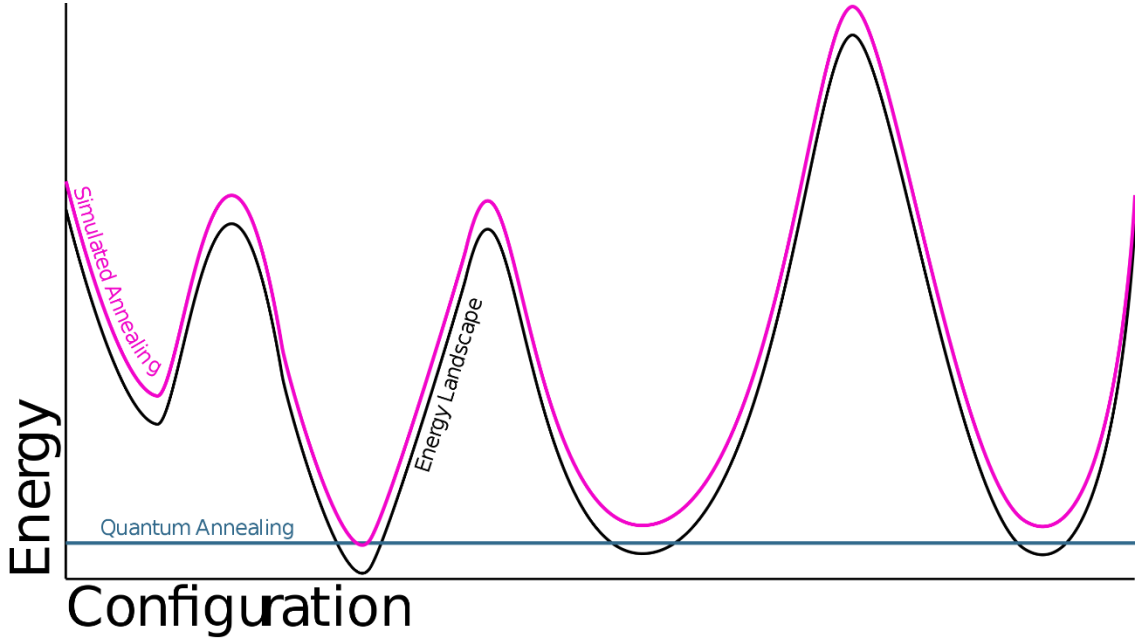
  - Quantum Boosting als „Quantenalgorithmus von Gradient Boosting“ ist am ehesten kompatibel mit dem Paradigma des Adiabatischen Quantencomputers, weil der geboostete Gradient der optimale Operator ist, in einem Quantenzustand den Grundzustand (d.h. kleinsten Eigenwert der Zustandssumme) zu finden.

    → *Siehe Quantum Annealing*

Quantum Computing

Quantum Machine Learning: Quantum Annealing[1]

- Quanten-Analogon von Simulated Annealing
- Verwendet den „Tunnel-Effekt“
- Man kann den Grundzustand eines komplexen Zustandsraumes effizient finden
- Trade-off: Difficult to find appropriate feature mapping to the Hamiltonian (i.e. the operator governing system behaviour)
- NP-harte Probleme erfordern trotzdem exponentiell lange Berechnungszeiten



[1] Apolloni, Bruno; Cesa-Bianchi, Nicolo; De Falco, Diego (July 1988). "A numerical implementation of quantum annealing". Stochastic Processes, Physics and Geometry, Proceedings of the Ascona-Locarno Conference.
Image source: https://en.wikipedia.org/wiki/Quantum_annealing#/media/File:Quantum_Annealing_Analogy.svg, Brian Lechthaler, CC BY-SA 4.0

Quantum Computing
Und die Aktuarswissenschaften?

Wo gibt es Potential für den Einsatz von Quantum Computing in Actuarial (Data) Science?

- **Optimierung (Annealing, Variationelle Thermalisierung)**

  → Cases wie Benchmarking können interessant sein, wenn die Berechnung des Optimums nicht explizit erfordert ist.

- **Support Vector Machines bzw. Support Vector Regression**

  → Lohnt ggf. wenn die Trennungsmannigfaltigkeit hochdimensional ist, das Problem sehr komplex ist.

- **Problemfälle**

  → Stresstesting, Validierung, individuelles Pricing → Weil *Erklärbarkeit* und *Konfidenz* schwierig zu bestimmen sind.

Quantum Computing
Herausforderungen für Quantum Actuarial Data Science

- Die Anforderungen an Quantum Error Correction bedeuten, dass Real-Life-Probleme noch **mehrere Größenordnungen zu umfangreich** für skalierende Quantenalgorithmen sind.

- Es wird noch viel Forschung nötig sein, um ein umfassendes Verständnis für die **Kodierung von klassischer Information** für Quantenalgorithmen zu erreichen. Viele vorgeschlagene Umsetzungen scheitern bisher an ineffizientem Encoding.

- Es gibt aktuell wenig Hinweise dafür, dass echter **Quantenzufall** den Aufwand für stochastische Modellierung rechtfertigen würde – spezifische Quantenzufallsquellen könnten dies aber ändern

- **Umwelt- und Nachhaltigkeitsziele** dürften den Energiebedarf von Quantencomputern mittelfristig in Frage stellen. Trotz großer Fortschritte ist die **Nettoenergiebilanz** bei gleicher Rechenleistung deutlich aufseiten der klassischen Rechneransätze.

Quantum Computing in den Aktuarswissenschaften
Fazit und Ausblick

- Quantum Computing zeigt einiges Potenzial für *Kryptographie*, *Optimierung* und (teilweise) *Machine Learning*.

  → Einschränkung: Es wird einen **sanften Paradigmenwechsel statt einer Disruption geben**.
- Müssen Versicherer und Aktuare schnell handeln?

  → **Nein**.
- Müssen Versicherer und Aktuare sich auf das Quanten Cpmputing vorbereiten?

  → Natürlich. **Aber die Herausforderung ist zunächst, überhaupt Anwendungsfälle zu identifizieren**.

Gesamtfazit

Es wird (*wie immer von den typischen Anbietern*) viel Quatsch erzählt,

um unfertige Technologie zu verkaufen und beim Kunden reifen zu lassen!

Vielen Dank!

Prof. Dr. Fabian Transchel

Stiftungsprofessur Data Science der E+S Rückversicherung AG

Telefon +49 3943 – 305

Telefax +49 3943 – 5305

E-Mail ftranschel@hs-harz.de

Friedrichstraße 57 – 59

38855 Wernigerode

Bildquelle: Pixabay

Shor-Algorithmus
Quantenmechanischer Teil („Hidden Subgroup Problem“)

- Klassischer Algorithmus reduziert eine Ganzzahl q zu einer Potenz von $n^2 \leq q \leq 2n^2$

  → q ist der klassisch irreduzible Teil und (effizienter) zugänglich mittels der Quantum Fourier Transformation.

- Quantum Fourier Transformation ist eine verschränkende Version der klassischen Fourier Transformation:

  → Die QFT transformiert einen reinen Zustand auf einen maximal-verschränkten Quantenzustand ab.

-

  → Verschränkung ist eine der zentralen „Ressourcen“ eines Quantencomputers.

- Unter Verwendung des maximal-verschränkten Zustandskann das System (mit W-Keit $\mathrm{p} > 0.5$) auf einen Zustand abgebildet werden, wo q in genau zwei nicht-triviale Faktoren zerfällt.

  → Man wiederholt diesen Schritt, bis die Zahl vollständig zerlegt ist.