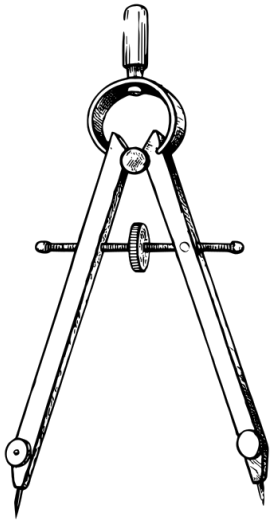

ARTELLICO

Quantencomputing

Grundlagen, Herausforderungen und strategische Implikationen

Informationsdossier

Mag. Alexander Pokorny
Geschäftsführer, Unternehmer, Lektor

https://artellico.com

Version 1.0 • März 2026

Das ist keine Policy — das ist Mathematik.

Jenseits binärer Gewissheiten

Paradigmenwechsel

Die klassische Informatik operiert seit über sieben Jahrzehnten auf einer eleganten Grundlage: dem Bit. Jede Berechnung, jede Entscheidung, jede Verschlüsselung lässt sich auf eine Sequenz von Nullen und Einsen zurückführen. Diese Architektur hat Zivilisationen transformiert — und stößt nun an fundamentale Grenzen. Quantencomputing bricht nicht mit dieser Tradition; es erweitert sie in eine Dimension, die unsere Intuition herausfordert.

Ein klassischer Computer verarbeitet Informationen sequentiell oder parallel, aber stets deterministisch: Jedes Bit befindet sich zu jedem Zeitpunkt in einem definierten Zustand. Ein Quantencomputer hingegen nutzt die Gesetze der Quantenmechanik, um Informationen in Zuständen zu kodieren, die erst durch Messung kollabieren. Dies ist kein technisches Detail — es ist ein ontologischer Bruch.

Das Qubit: Anatomie einer Quanteninformation

Qubit = Superposition zweier Basiszustände $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Während ein klassisches Bit exakt einen von zwei Zuständen annimmt (0 oder 1), existiert ein Qubit in einer Superposition beider Zustände gleichzeitig. Mathematisch wird dies durch einen Zustandsvektor in einem zweidimensionalen Hilbertraum beschrieben: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, wobei α und β komplexe Amplituden sind, deren Betragsquadrate sich zu 1 summieren.

Entscheidend ist: Die Superposition ist kein Ausdruck von Unwissen. Das Qubit befindet sich nicht „entweder in 0 oder 1, und wir wissen es nur nicht“. Es befindet sich nachweisbar in beiden Zuständen simultan. Erst die Messung erzwingt den Kollaps in einen der Basiszustände. Dieses Phänomen, zusammen mit Verschränkung (*Entanglement*) und Interferenz, bildet die physikalische Grundlage für die Überlegenheit von Quantenalgorithmen.

Verschränkung bedeutet, dass der Zustand eines Qubits instantan mit dem Zustand eines anderen korreliert — unabhängig von der räumlichen Distanz. Einstein nannte dies „spukhafte Fernwirkung“, doch mittlerweile ist es experimentell vieltausendfach bestätigt und bildet das Rückgrat von Quantenprotokollen.

Klassisches und Quantencomputing im Vergleich

Exponentielle vs. polynomiale Komplexität

Der fundamentale Unterschied liegt nicht in der Geschwindigkeit, sondern in der Komplexitätsklasse lösbarer Probleme. Ein klassischer Computer mit n Bits kann genau einen von 2^n Zuständen repräsentieren. Ein Quantencomputer mit n Qubits kann eine Superposition aller 2^n Zustände gleichzeitig manipulieren. Dies ermöglicht algorithmische Abkürzungen, die klassisch unmöglich sind.

Shors Algorithmus zerlegt große Zahlen in ihre Primfaktoren in polynomialer Zeit — ein Problem, das klassisch als exponentiell schwer gilt und die Grundlage der RSA-Verschlüsselung bildet. Grovers Algorithmus durchsucht unsortierte Datenbanken mit quadratischer Beschleunigung. Diese Algorithmen sind keine theoretischen Kuriositaten; sie definieren die Grenzen dessen, was berechenbar ist, neu.

Gleichwohl ist Quantencomputing kein universeller Ersatz. Für die überwiegende Mehrheit alltäglicher Rechenaufgaben — Textverarbeitung, Datenbankabfragen, Web-Applikationen — bieten Quantencomputer keinen Vorteil. Ihre Stärke liegt in spezifischen Problemklassen: Optimierung, Simulation quantenmechanischer Systeme, kryptographische Operationen und bestimmte Formen maschinellen Lernens.

Herausforderungen: Kühlung, Kohärenz, Fehlerkorrektur

10–15 Millikelvin: kälter als der Weltraum

Die größte technische Hürde des Quantencomputings ist die Dekohärenz: die Tendenz von Qubits, ihre Quanteneigenschaften durch Wechselwirkung mit der Umgebung zu verlieren. Supraleitende Qubits — die derzeit dominante Technologie, eingesetzt von IBM, Google und Rigetti — müssen auf Temperaturen nahe dem absoluten Nullpunkt gekühlt werden: typischerweise 10 bis 15 Millikelvin, realisiert durch mehrstufige Dilutionskühlsysteme.

Diese Kühlung ist energieintensiv und mechanisch komplex. Ein einzelner Quantencomputer benötigt Infrastruktur, die eher einem physikalischen Großlabor als einem Rechenzentrum gleicht. Die Kohärenzzeiten — die Zeitspanne, in der ein Qubit seine Quanteninformation behält — liegen bei supraleitenden Systemen im Bereich von Mikrosekunden bis Millisekunden. Jede Berechnung muss innerhalb dieses Fensters abgeschlossen sein.

Quantenfehlerkorrektur adressiert dieses Problem durch Redundanz: Hunderte physischer Qubits werden zu einem einzigen logischen Qubit zusammengefasst, das Fehler tolerieren kann. Dies bedeutet jedoch, dass ein praxistauglicher Quantencomputer mit tausend logischen Qubits physisch

Millionen von Qubits benötigen könnte — eine Größenordnung, die derzeit noch außer Reichweite liegt.

Neutral-Atom-Quantencomputer: Eine alternative Architektur

Optische Pinzetten halten einzelne Atome

Neben supraleitenden Systemen haben sich Neutral-Atom-Quantencomputer als vielversprechende Alternative etabliert. Unternehmen wie QuEra, Pasqal und Atom Computing nutzen einzelne neutrale Atome — typischerweise Rubidium oder Cäsium —, die durch hochfokussierte Laserstrahlen (optische Pinzetten) in zweidimensionalen oder dreidimensionalen Gittern gefangen und manipuliert werden.

Der entscheidende Vorteil dieser Architektur liegt in der Skalierbarkeit. Während supraleitende Qubits individuell auf Chips gefertigt werden müssen, können Neutral-Atom-Systeme hunderte bis tausende identischer Qubits gleichzeitig erzeugen. Die Atome sind von Natur aus identisch — ein Rubidium-Atom ist physikalisch ununterscheidbar von jedem anderen —, was Herstellungsvariabilität eliminiert.

Zudem erlauben *Rydberg-Wechselwirkungen* — langreichweitige Kopplungen zwischen hoch angeregten Atomzuständen — eine flexible Verbindungsstruktur zwischen Qubits, die nicht auf physisch benachbarte Qubits beschränkt ist. Dies ist ein signifikanter Vorteil gegenüber supraleitenden Architekturen, deren Konnektivität durch die physische Chip-Topologie limitiert wird.

Topologische Supraleiter: Der Traum fehlerresistenter Qubits

Majorana-Fermionen als fehlerresistente Qubits

Die eleganteste, aber auch ambitionierteste Strategie zur Überwindung der Dekohärenz stammt aus der topologischen Quantenmechanik. Topologische Supraleiter — Materialien, deren quantenmechanische Zustände durch globale geometrische Eigenschaften statt lokaler Parameter geschützt sind — versprechen inhärent fehlerresistente Qubits.

Das Schlüsselkonzept sind Majorana-Fermionen: exotische Quasiteilchen, die an den Enden topologischer Supraleiterdrähte entstehen und deren Quanteninformation nicht lokal gespeichert, sondern über die gesamte Struktur delokalisiert ist. Störungen, die nur lokal wirken, können diese Information nicht zerstören — ein natürlicher Schutz gegen Dekohärenz.

Microsoft verfolgt diesen Ansatz mit seinem Majorana-1-Programm, das im Februar 2025 einen funktionalen topologischen Qubit demonstrierte. Gleichwohl bleibt die Technologie in einem frühen Stadium. Die experimentelle Herstellung zuverlässiger Majorana-Zustände ist außerordentlich anspruchsvoll, und der Weg von einzelnen topologischen Qubits zu skalierbaren Systemen ist noch weit. Dennoch: Sollte dieser Ansatz gelingen, würde er die Fehlerkorrektur-Overhead drastisch reduzieren und Quantencomputing fundamental verändern.

Anwendungsfelder: Wo Quantencomputing Wirkung entfaltet

Von Pharma bis Finanzmärkte

Die vielversprechendsten Anwendungsgebiete liegen dort, wo klassische Computer an kombinatorischer Explosion scheitern. In der Pharmaforschung ermöglicht die Quantensimulation von Molekülinteraktionen die Beschleunigung der Wirkstoffentwicklung: Proteinstrukturen, Bindungsenergien und Reaktionspfade lassen sich direkt auf Quantenebene modellieren, statt sie klassisch zu approximieren.

In der Materialwissenschaft eröffnen Quantensimulatoren die Möglichkeit, neuartige Materialien — Hochtemperatursupraleiter, effizientere Katalysatoren, leistungsfähigere Batteriechemien — vorherzusagen, bevor sie synthetisiert werden. In der Finanzwirtschaft versprechen Quantenalgorithmen Vorteile bei der Portfoliooptimierung, Risikomodellierung und der Bepreisung komplexer Derivate.

Optimierungsprobleme in Logistik und Lieferkettenmanagement, Verkehrsflusssteuerung und Netzwerkdesign gehören ebenfalls zu den Kandidaten für Quantum Advantage. Doch Vorsicht ist geboten: Der Nachweis eines genuinen Quantenvorteils — also einer Überlegenheit gegenüber den besten klassischen Algorithmen auf realen, wirtschaftlich relevanten Probleminstanzen — steht für die meisten dieser Anwendungsfelder noch aus.

Energetische Implikationen: Ein zweischneidiges Schwert

Energieparadox: weniger Operationen, mehr Kühlung

Die Energiebilanz von Quantencomputern ist paradox. Einerseits versprechen Quantenalgorithmen, bestimmte Berechnungen mit exponentiell weniger Operationen durchzuführen als klassische Verfahren — was theoretisch einen

dramatischen Effizienzgewinn bedeutet. Andererseits ist der Betrieb aktueller Quantencomputer extrem energieintensiv.

Ein Dilutionskühlsystem für supraleitende Qubits verbraucht typischerweise 15 bis 25 Kilowatt kontinuierlich — allein für die Kühlung. Hinzu kommen die Steuerungselektronik, die Signalverarbeitung und die klassischen Coprozessoren, die den Quantenchip kontrollieren. Der Gesamtenergieverbrauch eines Quantencomputing-Systems übersteigt den eines vergleichbaren klassischen HPC-Knotens um ein Vielfaches.

Langfristig könnten Quantencomputer jedoch einen indirekten, aber tiefgreifenden Beitrag zur Energieeffizienz leisten: durch die Simulation und Optimierung von Materialien für effizientere Solarzellen, Batterien und Katalysatoren; durch die Optimierung von Energienetzen und Logistikketten; und durch die Beschleunigung der Forschung an Fusionsreaktoren. Die Frage ist nicht, ob Quantencomputer selbst wenig Energie verbrauchen, sondern ob die durch sie ermöglichten Erkenntnisse den Energieverbrauch ganzer Industrien transformieren können.

Quantencomputing und Kryptographie: Die Erosion klassischer Sicherheit

Harvest now, decrypt later

Die kryptographischen Implikationen des Quantencomputings sind vielleicht die unmittelbarsten. Shors Algorithmus bedroht die Sicherheit asymmetrischer Verschlüsselungsverfahren wie RSA, DSA und ECC — Verfahren, die das gesamte digitale Vertrauenssystem des Internets tragen: TLS-Zertifikate, digitale Signaturen, sichere Kommunikation.

Die Bedrohung ist nicht abstrakt. Geheimdienstorganisationen betreiben mutmaßlich bereits sogenannte „Harvest now, decrypt later"-Strategien: das Abfangen und Speichern verschlüsselter Kommunikation in der Erwartung, sie mit zukünftigen Quantencomputern entschlüsseln zu können. Für Daten mit langen Geheimhaltungsfristen — diplomatische Kommunikation, medizinische Daten, Geschäftsgeheimnisse — ist dies eine reale, gegenwärtige Bedrohung.

Die Antwort der Kryptographie ist zweigeteilt. Erstens: Post-Quanten-Kryptographie (PQC), also Algorithmen, die auch auf klassischen Computern laufen, aber gegen Quantenangriffe resistent sind. Das NIST hat 2024 die ersten PQC-Standards finalisiert (FIPS 203–205). Zweitens: Quantum Key Distribution (QKD), die quantenmechanische Prinzipien nutzt,

um physikalisch sichere Schlüsselverteilung zu ermöglichen. Beide Ansätze sind komplementär, nicht alternativ.

Quantencomputing und Künstliche Intelligenz

Quantum Machine Learning: Potenzial und Skepsis

Die Schnittstelle von Quantencomputing und Künstlicher Intelligenz ist Gegenstand intensiver Forschung — und ebenso intensiver Übertreibung. Theoretisch könnten Quantencomputer bestimmte Teilprobleme des maschinellen Lernens beschleunigen: die Lösung linearer Gleichungssysteme (HHL-Algorithmus), die Optimierung von Verlustfunktionen, die Suche in hochdimensionalen Parameterräumen.

Quantum Machine Learning (QML) erforscht Variationsschaltkreise als parametrisierte Modelle — sogenannte Quantum Neural Networks —, die durch klassische Optimierer trainiert werden. Erste Ergebnisse zeigen Vorteile bei kleinskaligen Problemen, doch die Skalierbarkeit auf industrierelevante Datensätze ist ungeklärt. Das fundamentale Problem bleibt die Daten-Ein- und -Ausgabe: Klassische Daten müssen in Quantenzustände kodiert und die Ergebnisse wieder klassisch ausgelesen werden — ein Flaschenhals, der potenzielle Quantenvorteile konterkarieren kann.

Realistischer ist der Einsatz von Quantencomputern für spezifische Optimierungsprobleme innerhalb von KI-Pipelines: die Optimierung von Molekülkandidaten im Drug Discovery, die Lösung kombinatorischer Allokationsprobleme oder die effiziente Suche in graphbasierten Strukturen. Die Revolution liegt nicht darin, dass Quantencomputer LLMs trainieren werden — das werden sie absehbar nicht —, sondern darin, dass sie Probleme lösen, die klassische KI als Eingabe oder Kontext benötigt.

Ausblick: Zwischen Hype und Physik

NISQ → FT-QC: ein Jahrzehnt?

Quantencomputing befindet sich in der sogenannten NISQ-Ära (*Noisy Intermediate-Scale Quantum*): Geräte mit dutzenden bis wenigen tausend verrauschten Qubits, die für spezifische Aufgaben nützlich sein könnten, aber noch nicht fehlerkorrigiert arbeiten. Der Übergang zur fehlertoleranten Quantenberechnung (FT-QC) wird voraussichtlich noch ein Jahrzehnt oder länger dauern.

Die strategische Implikation für Unternehmen und Institutionen ist klar: Quantencomputing erfordert keine sofortige Investition in Hardware, aber es erfordert sofortige Aufmerksamkeit in drei Bereichen. Erstens,

kryptographische Vorbereitung: Die Migration zu quantenresistenten Algorithmen sollte jetzt beginnen, nicht wenn Quantencomputer verfügbar sind. Zweitens, algorithmische Kompetenz: Organisationen sollten verstehen, welche ihrer Probleme quantengeeignet sind. Drittens, souveräne Infrastruktur: In einer Zukunft, in der Quantencomputer klassische Verschlüsselung brechen können, wird die Kontrolle über die eigene Datenarchitektur nicht mehr optional, sondern existenziell.

Quantencomputing ist kein Allheilmittel und kein unmittelbarer Disruptor. Es ist eine fundamentale Erweiterung des Berechenbaren — und damit eine Einladung, die Grenzen unseres Denkens ebenso zu erweitern wie die Grenzen unserer Maschinen.

Literaturverzeichnis

Arute, F. et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505–510.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings 28th ACM Symposium on Theory of Computing, 212–219.

Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. Quantum, 2, 79.

National Institute of Standards and Technology (2024). FIPS 203–205: Post-Quantum Cryptography Standards. NIST.

Bluvstein, D. et al. (2024). Logical quantum processor based on reconfigurable atom arrays. Nature, 626(7997), 58–65.

Nayak, C. et al. (2008). Non-Abelian anyons and topological quantum computation. Reviews of Modern Physics, 80(3), 1083–1159.

Kitaev, A. Y. (2003). Fault-tolerant quantum computation by anyons. Annals of Physics, 303(1), 2–30.

Microsoft Research (2025). Majorana 1: A topological qubit chip. Microsoft Technical Report.

Cerezo, M. et al. (2021). Variational quantum algorithms. Nature Reviews Physics, 3(9), 625–644.

Bauer, B. et al. (2020). Quantum algorithms for quantum chemistry and quantum materials science. Chemical Reviews, 120(22), 12685–12717.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41.

Bernstein, D. J. & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194.

Fellous-Asiani, M. et al. (2022). Limitations in quantum computing from resource constraints. PRX Quantum, 3, 020319.

Alexeev, Y. et al. (2021). Quantum computer systems for scientific discovery. PRX Quantum, 2, 017001.