

Quanteninformatik als Thema und Aufgabengebiet informatischer Bildung

Tilman Michaeli¹, Stefan Seegerer², Ralf Romeike³

Abstract: Quantentechnologien gehören derzeit zu den vielversprechendsten technologischen Entwicklungen, wobei insbesondere der Quanteninformatik eine entscheidende Bedeutung zukommt. Damit einher gehen vielversprechende Möglichkeiten, aber auch neue Herausforderungen für unsere Gesellschaft. Allerdings steht die Quanteninformatik als Gegenstand informatischer Bildung noch in den Anfängen. Ziel dieses Beitrags ist es, Quanteninformatik als Thema und Aufgabengebiet der informatischen Bildung zur Diskussion zu stellen und eine erste Annäherung an zentrale Begriffe und Ideen sowie deren Erklärungsansätze vorzunehmen. Mithilfe eines explorativen Fokusgruppen-Interviews mit Expertinnen und Experten werden in der vorliegenden Untersuchung fünf wesentliche Ideen der Quanteninformatik identifiziert. Anhand einer Literaturanalyse werden anschließend verschiedene Erklärungsansätze für diese Ideen herausgearbeitet, kategorisiert und kontrastiert. Die Ergebnisse tragen damit zur Erschließung der Quanteninformatik für die informatische Bildung bei und werfen weitere Fragestellungen für die informatikdidaktische Forschung auf.

Keywords: Quanteninformatik; Quantencomputing; Ideen; Erklärungsansätze; Fokusgruppen

1 Einleitung

Mit der digitalen Transformation haben Computertechnologien Einzug in nahezu alle Lebensbereiche gehalten und begegnen den Bürgerinnen und Bürgern in Form von immer weiteren informationstechnischen Innovationen, wie bspw. eingebetteten ubiquitären Systemen, Big Data oder Künstlicher Intelligenz. Ein wesentlicher Treiber dieser Entwicklungen ist die Wissenschaft Informatik. Gegenstand der informatischen Bildung ist es, die korrespondierenden Grundlagen, Anwendungsmöglichkeiten und Implikationen dieser Technologien jungen wie älteren Menschen näherzubringen und begreifbar zu machen. Hierzu sollten im Sinne der fundamentalen Ideen der Informatik langfristig bedeutsame Entwicklungen aufgegriffen werden, ohne kurzfristigen „Moden“ zu folgen.

Eine zunehmend präzise Entwicklung an der Schnittstelle zwischen Physik, Mathematik und Informatik stellen Quantentechnologien dar, welche in Form des Quantencomputing als neues Paradigma bedeutende Fortschritte und Herausforderungen für die Informatik bedeutet, die im Rahmen der Quanteninformatik betrachtet werden. Auch wenn heutige informatische

¹ FU Berlin, Didaktik der Informatik, Königin-Luise-Str. 24-26, 14195 Berlin, tilman.michaeli@fu-berlin.de

² FU Berlin, Didaktik der Informatik, Königin-Luise-Str. 24-26, 14195 Berlin, stefan.seegerer@fu-berlin.de

³ FU Berlin, Didaktik der Informatik, Königin-Luise-Str. 24-26, 14195 Berlin, ralf.romeike@fu-berlin.de

Systeme bereits auf quantenphysikalischen Prozessen aufbauen, ergeben sich erst aus den jüngeren Entwicklungen der sogenannten „zweiten Quantenrevolution“ potenziell gesellschaftsverändernde Möglichkeiten und Herausforderungen. Eine in der Quanteninformatik verortete Frage ist bspw., wie sich neue Quantentechnologien auf die informationstechnische Sicherheit (Security) und Privatheit (Privacy) von Bürgerinnen und Bürgern, aber auch von staatlichen und wirtschaftlichen Akteuren auswirken. So können bereits heute schon sensible Daten ohne quantenresistente Verschlüsselung aus Netzwerken abgegriffen, gespeichert und zu einem späteren Zeitpunkt durch Quantencomputer entschlüsselt werden. Gleichzeitig schafft die Quantenkommunikation neue Möglichkeiten abhörsicherer Übertragungen. Ein weiterer wichtiger Anwendungsbereich des Quantencomputing ist die Simulation. Hier versprechen Quantencomputer bspw. in der Arzneimittelforschung oder der Meteorologie enorme Effizienzgewinne. Damit bringen Quantentechnologien sowohl große zivilgesellschaftliche Chancen als auch Risiken mit sich, die eine informierte öffentliche Debatte verlangen. Quantencomputer und Quanteninformatik (regelmäßig auch subsumiert unter *Quantencomputing*) haben hierbei einen besonderen Stellenwert.

Trotz zunehmender Präsenz in den Medien und wachsender Bedarfe in Wissenschaft, Wirtschaft und Gesellschaft steht die Quanteninformatik als Themengebiet der informatischen Bildung – im Gegensatz bspw. zum Stellenwert im Unterrichtsfach Physik – noch am Anfang. Ziel dieses Beitrags ist es, Quanteninformatik als Thema und Aufgabe der informatischen Bildung zur Diskussion stellen und auf Basis einer Expertenbefragung eine erste Annäherung an zentrale Begriffe, Ideen und geeignete Erklärungsansätze bereitzustellen.

2 Hintergrund und Forschungsstand

Informationsverarbeitung auf Grundlage der Quantenphysik unterscheidet sich in vielerlei Hinsicht von der herkömmlichen Art der Informationsverarbeitung: Während ein klassischer Computer Informationen mit Bits darstellt, die entweder den Wert 0 oder den Wert 1 annehmen können, nutzt ein Quantencomputer sogenannte *Qubits*. Ein Qubit kann ebenso den Wert 0 bzw. den Wert 1 annehmen oder in einer sogenannten *Superposition* sein. In diesem Fall hat es eine bestimmte Wahrscheinlichkeit, als 0 oder als 1 gemessen zu werden. Eine Messung zerstört allerdings die Superposition. Außerdem können Qubits miteinander *verschränkt* – d. h. zueinander in Abhängigkeit gebracht – werden, was es erst ermöglicht, beliebige Quantenzustände herzustellen und damit Quantenüberlegenheit zu erreichen. Unter Ausnutzung von Superposition und Verschränkung versuchen *Quantenalgorithmen*, bestimmte Probleme wie die Primfaktorzerlegung [Sh99], die Suche in Datenbanken [Gr96] oder Simulationen [Za98] deutlich schneller zu lösen als klassische Supercomputer: Während n klassische Bits nur in einem der 2^n möglichen Zustände sein können, können mit n Qubits 2^n Zustände gleichzeitig repräsentiert werden, wobei jedem Zustand eine bestimmte Wahrscheinlichkeit zugeordnet ist. Quantenalgorithmen manipulieren die Qubits durch Anwendung spezieller *Quantengatter* so, dass am Ende mit hoher Wahrscheinlichkeit ein richtiges Ergebnis gemessen wird.

Zum Verständnis von Quantentechnologien können die drei direkt beteiligten Wissenschaften Physik, Mathematik und Informatik beitragen und jeweils als Perspektive und Einstieg in den Themenbereich dienen. So existieren verschiedene physikdidaktische Vorschläge, Grundlagen der Quantenphysik in der Schule zu adressieren, bspw. mit Lichtexperimenten [Er12a], im physikdidaktischen Schülerlabor [Er12b] oder über das Doppelspaltexperiment, um hieran exemplarisch zentrale Inhalte und Fragen der Quantenphysik zu verdeutlichen [Le99]. Ein physikdidaktischer Zugang zum Quantencomputing existiert bspw. für Schülerinnen und Schüler der Sekundarstufe II [Ru19], der allerdings vertiefte Mathematikkenntnisse erfordert. Auch wenn Quantencomputing als Thema der informatischen Bildung bisher allenfalls in Nischen auftritt, findet es sich inzwischen in einzelnen universitären Lehrveranstaltungen in Bachelor- (bspw. [La17]) oder Masterinformatikstudiengängen (bspw. [LM18; Un19]). Billig [Bi18] adressiert Quantencomputing für die Sekundarstufe mit entsprechend einfachen Mathematikkenntnissen, bspw. durch didaktische Vereinfachung der zentralen Begriffe und Vermeidung komplexer Zahlen. Zur Verdeutlichung der Potenziale des Quantencomputing werden hierbei zunächst klassische Computersysteme und kryptografische Verfahren beschrieben, um darauf aufbauend die Besonderheiten, Stärken und Herausforderungen der Quantentechnologie herauszustellen. Einen ersten Vorschlag für Schlüsselkonzepte des Quantencomputing legen QISLearners [Al20] vor. Weitere Curricula für die Sekundarschule berücksichtigen den MINT-Kontext [Sa18], verwenden problemorientiertes Lernen und den IBM Quantum Circuit Designer [Pe19] oder schlagen Quantencomputing-Aktivitäten in Ergänzung zum regulären Unterricht vor [Su19]. Wootton [Wo18] beschreibt einen Ansatz zum Einstieg mittels einer Denkspiel-App, mit der interessierte Personen ab fünf Jahren spielerisch mit Qubits und Quantengattern umgehen lernen können. Darüber hinaus vermitteln eine Reihe an Erklärvideos auf Videoplattformen die Grundlagen von Quantentechnologien auf unterschiedlichen Niveaus. Wissenschaftliche Untersuchungen bzw. informatikdidaktische Forschungserkenntnisse liegen zu den o. g. Ansätzen, die sich vor allem der inhaltlichen Aufbereitung widmen, noch nicht vor.

3 Vorgehen

Im Folgenden soll eine erste informatikdidaktische Annäherung an das Thema Quanteninformatik explorativ unter Einbeziehung von Expertinnen und Experten erfolgen. Dazu werden (1) zunächst literaturbasiert zentrale Begriffe und Konzepte sowie relevante Fragen und Klärungsbedarfe identifiziert, die im Sinne einer *fachlichen Klärung* essentiell für die Erschließung des Themengebiets sind [HNR07], (2) expertenbasiert erste Einschätzungen vorgenommen und Kandidaten für zentrale Ideen der Quanteninformatik bestimmt sowie (3) zur Fundierung der didaktischen Bestandsaufnahme existierende Erklärungsansätze für die resultierenden Ideen analysiert und kontrastiert. Zur Diskussion und Bewertung der im ersten Schritt identifizierten Begriffe und Fragestellungen wurde im zweiten Schritt eine Expertenbefragung in Form eines Fokusgruppen-Interviews durchgeführt. Diese teilstandardisierte Erhebungsmethode eignet sich vor allem wegen ihres explorativen Charakters und aufgrund des diskursiven Austauschs, der zu einer Konsensfindung beiträgt [BD06]. Die

Expertinnen und Experten wurden dazu über den Arbeitskreis „Quantencomputing“ der Gesellschaft für Informatik angesprochen und zeichnen sich sowohl durch fachliche Expertise im Forschungsgebiet der Quanteninformatik als auch durch eine korrespondierende fachliche Lehrerfahrung aus. Für den online durchgeführten Workshop konnten neun Personen gewonnen werden. Die Expertinnen und Experten wurden vorab zunächst mithilfe eines teilstandardisierten Fragebogens zu der Bezeichnung des Fachgebiets, zentralen Begriffen, Anwendungsmöglichkeiten und gesellschaftlichen Auswirkungen der Quanteninformatik befragt. Die Ergebnisse dieser schriftlichen Befragung wurden für die Gruppendiskussion aufbereitet und zusammengefasst. Damit diente der Aufbau des Fragebogens auch als Leitfaden für die Fokusgruppe, in der eine Diskussion der Ergebnisse sowie eine Strukturierung zentraler Begrifflichkeiten hin zu Ideen der Quanteninformatik und deren Priorisierung erfolgte. Darüber hinaus wurden Follow-up-Interviews mit ausgewählten Teilnehmenden durchgeführt. Im dritten Schritt wurden mithilfe einer Literaturanalyse Erklärungsansätze für die identifizierten Ideen herausgearbeitet, kategorisiert und kontrastiert. Dazu wurde der insgesamt 17 Dokumente umfassende Literaturkorpus (Kinderbücher, Lehrbücher, Schulcurricula und populärwissenschaftliche Bücher, die sich mit dem Thema Quanteninformatik auseinandersetzen) herangezogen und mithilfe einer strukturierenden qualitativen Inhaltsanalyse nach Mayring [Ma10] hinsichtlich wiederkehrender Muster in den Erklärungsansätzen für die entsprechenden Ideen untersucht.

4 Ergebnisse

4.1 Fachliche Klärung

Mit dem Ziel, längerfristig und übergreifend als wichtig erachtete Ideen der Quanteninformatik zu identifizieren, wurde zunächst mithilfe einer explorativen Analyse einschlägiger Fachliteratur und Lehrwerke für unterschiedliche Zielgruppen (siehe oben) ein erster Überblick über die relevanten Begriffe und damit Schwerpunkte und Dimensionen des Themenfeldes gewonnen. Hierbei zeigte sich, dass offenbar ein gewisser Konsens hinsichtlich für das Fachgebiet relevanter Themen und Begriffe vorliegt, der sich in einem Kern wiederkehrender und in allen analysierten Dokumenten ähnlich gebrauchter Begriffe widerspiegelt (vgl. auch Begriffe in Tab. 1) – weitgehend unabhängig von der Zielgruppe der Literatur. Aufgrund ihres Stellenwerts in der Literatur kann angenommen werden, dass die Begriffe auch aus Perspektive der informatischen Bildung und damit für das Verständnis der Quanteninformatik zentral sind und als Ansatz für das Bestimmen zentraler Ideen herangezogen werden können.

Darüber hinaus ergaben sich eine Reihe weiterer Fragen. So werden in der entsprechenden Literatur mit *Quantencomputing*, *Quanteninformatik* oder seltener auch *Quanteninformatiktheorie* unterschiedliche Termini zur Bezeichnung des Fachgebiets als solches verwendet. Es stellt sich hier die Frage, welche Begrifflichkeit aus Perspektive der informatischen Bildung am geeignetsten erscheint. Weiterhin hat es sich als zielführend erwiesen, neben

Begriff	#	Begriff	#	Begriff	#
Qubit	8	Zustand	2	Quanteninformatio- nverarbeitung	1
Verschränkung	8	Messung	2	Quantenkommunikation	1
Quantenschaltkreis / -gatter	5	Quantensimulation	2	Quanten- beschleunigung	1
Superposition	5	Dekohärenz	2	Bloch-Sphäre	1
Quantenkryptographie	5	Teleportation	2	Supremacy	1
Quantencomputer	4	Quanteninternet	2	Quantum Advantage	1
Quantenalgorithmus	2	Fehleranfälligkeit	2	Photon	1
Quantenparallelismus	2	Quanteninformatio- n	1		

Tab. 1: Zentrale Begriffe und Anzahl der Nennungen.

der technologischen Perspektive (vgl. Dagstuhl-Dreieck) auch die Nutzungsmöglichkeiten und gesellschaftlichen Auswirkungen in den Blick zu nehmen. In der analysierten Literatur finden sich allerdings fast ausschließlich Ausführungen zur technologischen Perspektive. Anwendungsmöglichkeiten und auch gesellschaftliche Auswirkungen der Quanteninformatik werden lediglich angedeutet, sodass diese Frage ebenso in die Expertenrunde getragen wurde.

4.2 Ergebnisse des Fokusgruppen-Interviews

Quantencomputing oder Quanteninformatik? Mit der informatikdidaktischen Erschließung des neuen Fachgebiets stellt sich die Frage der adäquaten Bezeichnung. Das auf Basis des Fragebogens noch zunächst sehr uneindeutige Stimmungsbild wurde im Verlauf des Diskurses in der Fokusgruppe zugunsten des Begriffs *Quanteninformatik* aufgelöst: Obgleich Quantencomputing bekannter und damit öffentlichkeitswirksamer sei, stimmten die Expertinnen und Experten dem Ergebnis unserer fachlichen Klärung zu, dass der Begriff Quanteninformatik weiter gefasst sei und auch alle aktuellen Forschungsfelder wie z. B. Quantenkryptographie und Quanteninternet mit einbeziehe. Aus Perspektive der informatischen Bildung ist daher der Begriff Quanteninformatik zu wählen.

Zentrale Begriffe. Begriffe können bei der Bestimmung, Präzisierung und Priorisierung eines Fachgebiets helfen. Mit diesem Ziel wurden die Teilnehmerinnen und Teilnehmer im Rahmen des Fragebogens gebeten, die aus ihrer Sicht sieben wichtigsten Begriffe zum Thema, die jede bzw. jeder kennen sollte, zu nennen (vgl. Tab. 1). Im Fokusgruppen-Interview wurden diese Begriffe zunächst gemeinsam gruppiert bzw. kombiniert. So wurden beispielsweise die Begriffe Quantenparallelismus, Quantenbeschleunigung und Quantum Advantage zusammengefasst. Dabei wurde insbesondere auf ein ähnliches Abstraktionsniveau geachtet. Darüber hinaus wurden die Begriffe gemeinsam priorisiert und diejenigen ausgewählt, die

zu einem grundlegenden Verständnis beitragen und somit einen Zugang zum Fachgebiet eröffnen – auch vor dem Hintergrund der gesellschaftlichen Perspektive. So wurden etwa Quanteninternet bzw. -kommunikation oder Quantensimulation, die sich vor allem auf spezielle Anwendungen konzentrieren, als weniger relevant eingestuft.

Zentrale Ideen. Im Nachgang an die Interviews wurden die begriffsbezogenen wichtigsten nichttrivialen Konzepte in Form von Ideen ausformuliert und mit Follow-up-Interviews abgesichert. Die finalen 5 Kandidaten für diese Ideen lauten wie folgt:

1. Superposition: Qubits in einer Superposition aus 0 und 1 haben eine bestimmte Wahrscheinlichkeit als 0 bzw. als 1 gemessen zu werden.
2. Verschränkung: Der Zustand von mehreren verschränkten Qubits lässt sich nicht durch die Angabe eines individuellen Quantenzustands für jedes Qubit beschreiben.
3. Quantencomputer: Quantencomputer können bestimmte – aber nicht alle – Probleme effizienter lösen als klassische Computer.
4. Quantenalgorithmus: Bei einem Quantenalgorithmus wird mithilfe von Quantengattern der Zustand der Qubits so beeinflusst, dass die Wahrscheinlichkeit steigt, eine richtige Lösung zu messen.
5. Quantenkryptographie: Quantenkryptographie nutzt die Fragilität der Qubits, um abhörsichere Kommunikation zu ermöglichen.

Anwendungs- und gesellschaftliche Perspektive. Aus den Antworten der Expertinnen und Experten gehen drei zentrale Anwendungsmöglichkeiten bzw. gesellschaftliche Implikationen hervor. Im Bereich der *Kryptographie* ergibt sich einerseits eine Gefahr für traditionelle Verfahren wie RSA, andererseits eröffnen sich aber auch Chancen für neue, sichere Verfahren. Gleichzeitig versprechen sich die Expertinnen und Experten gesellschaftliche Implikationen bei *Optimierungsproblemen*, etwa im Bereich der künstlichen Intelligenz, die zukünftig besser bzw. schneller gelöst werden könnten. Schließlich versprechen *Quantensimulationen* gesellschaftliche Fortschritte in der biologischen, chemischen oder physikalischen Forschung und können so bspw. helfen, neue Impfstoffe zu entwickeln. Nichtsdestotrotz finden sich quanteninformatische Anwendungen bis auf wenige Ausnahmen, etwa zur Erzeugung von Zufallszahlen auf Smartphones, bisher eben kaum in Lebenswelt und Alltag wieder.

4.3 Erklärungsansätze

Im Folgenden wird nun das Ergebnis der Literaturanalyse zu Erklärungsansätzen für die identifizierten Ideen dargestellt. Dabei treten die einzelnen Erklärungsansätze nicht notwendigerweise isoliert auf: Innerhalb eines Dokuments wurden mitunter unterschiedliche Erklärungsansätze für eine Idee verwendet.

Superposition: Qubits in einer Superposition aus 0 und 1 haben eine bestimmte Wahrscheinlichkeit als 0 bzw. als 1 gemessen zu werden. Ein beliebter Erklärungsansatz für diese Idee ist die Verwendung von *Analogien* wie dem Münzwurf (oder dem Drehen einer Münze), bei dem die Münze in der Luft (oder im Spin) als Superposition aus Kopf und Zahl interpretiert wird (vgl. Abb. 1). Eine andere Herangehensweise stellt ein *physikalischer Erklärungsansatz* dar, bei dem konkrete Realisierungen von Qubits durch Photonen oder Elektronenspin sowie Experimente wie Stern-Gerlach herangezogen werden. Weiterhin werden Qubits im Korpus auch *mathematisch-symbolisch* erklärt: Der Zustand eines oder mehrerer Qubits wird dann durch einen Vektor repräsentiert. Zur Erklärung werden außerdem *grafische Darstellungen* verwendet, etwa geometrisch über die Bloch-Sphäre oder den Einheitskreis sowie schematisch über teilweise gefüllte Kreise oder Quadrate für jeden Zustand eines Qubit-Systems. Zudem werden Qubits auf Basis des Bit-Begriffs mithilfe von probabilistischen Bits eingeführt und anschließend zu Qubits verallgemeinert, also aufbauend auf *klassischen Themen informatischer Bildung*.

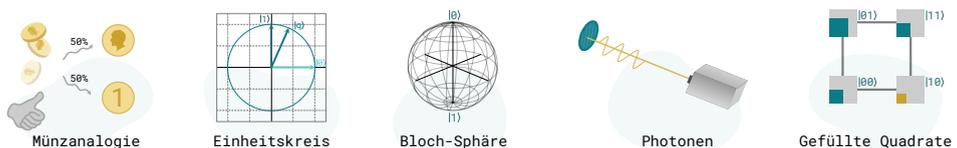


Abb. 1: Beispiele für Erklärungsansätze

Verschränkung: Der Zustand von mehreren verschränkten Qubits lässt sich nicht durch die Angabe individueller Quantenzustände für jedes Qubit beschreiben. Analog zur ersten Idee wird Verschränkung häufig über *Analogien* erklärt. So landen bspw. zwei verschränkte Münzen stets beide auf Kopf bzw. stets beide auf Zahl. In einer anderen Analogie werden zwei farbige Bälle in unterschiedliche Boxen verpackt: Auch wenn nicht bekannt ist, welche Farbe in den Boxen ist, werden beide Bälle dieselbe Farbe haben. Daneben wird oftmals ein *mathematisch-symbolischer* Erklärungsansatz gewählt, bei dem rechnerisch nachgewiesen wird, dass ein verschränkter Zwei-Qubit-Zustand nicht als zwei einzelne Ein-Qubit-Zustände dargestellt werden kann. Darüber hinaus wird Verschränkung auch über das *Messen von Quantenschaltkreisen* erklärt, wenn Hadamard- und CNOT-Gatter kombiniert werden oder erneut ausgehend von *klassischen Themen informatischer Bildung* über das Einführen probabilistischer Bits als Zwischenschritt.

Quantenalgorithmus: Bei einem Quantenalgorithmus wird mithilfe von Quantengattern der Zustand der Qubits so beeinflusst, dass die Wahrscheinlichkeit steigt, eine richtige Lösung zu messen. Für dieses Konzept wird einerseits ein *physikalischer Erklärungsansatz* herangezogen, der eine konkrete Realisierung und Manipulation von Qubits (z. B. Photonen) beschreibt. Um den Effekt der verschiedenen Gatter auf den Zustand eines (oder mehrerer Qubits) zu erläutern, wird mitunter auch eine *grafische Darstellung* gewählt. Dabei wird bspw. eine Rotation an der Bloch-Sphäre vorgenommen oder ein Vektor an einer bestimmten Achse am Einheitskreis gespiegelt. Beim *experimentellen Erklärungsansatz* werden die Effekte der Gatter durch Messung untersucht – hierfür wird üblicherweise

direkt mit entsprechenden Werkzeugen (meist Simulatoren für Quantencomputer) gearbeitet. Zuletzt werden bei einem *mathematisch-symbolischen Erklärungsansatz* die Quantengatter in ihrer Matrixdarstellung herangezogen, wobei das Anwenden eines Gatters dann einer Multiplikation der Matrix mit einem Vektor entspricht.

Quantencomputer: Quantencomputer können bestimmte aber nicht alle Probleme effizienter lösen als klassische Computer. Auch hier wird häufig der Ansatz einer *Analogie* gewählt, bei der Quantencomputer als hochgradig parallel arbeitend beschrieben werden. Ein weiterer Erklärungsansatz nutzt die *Menge an darstellbaren Zuständen* – oft anhand konkreter Beispiele und Größenordnungen: So können bspw. 300 Qubits bereits mehr Zustände (ca. 10^{90}) abbilden als Teilchen im Universum existieren. Ein weiterer beliebter Erklärungsansatz arbeitet mit einem *konkreten Beispiel* wie dem Deutsch-Josza-Algorithmus, anhand dem die Anzahl notwendiger Schritte bei Lösung mit einem klassischen Computer und einem Quantencomputer verglichen werden.

Quantenkryptographie: Quantenkryptographie nutzt die Fragilität der Qubits, um abhörsichere Kommunikation zu ermöglichen. Für die Funktionweise der Quantenkryptographie wird als Erklärungsansatz in Form des BB84-Schlüsseltausch-Protokolls häufig ein *konkretes Beispiel* gewählt, da dieses keine verschränkten Zustände benötigt und insgesamt als leicht zu verstehen gilt. Um die Vorteile eines Quantenschlüsseltauschprotokolls zu verdeutlichen, wird weiterhin auch der Bezug zu *klassischen Themen informatischer Bildung* wie der symmetrischen Verschlüsselung und dem One-Time-Pad hergestellt.

5 Diskussion und Fazit

Sowohl die literaturbasierte fachliche Klärung als auch die Expertenbefragung zeigen, dass Quanteninformatik über einen überschaubaren Kern zentraler Ideen zugänglich gemacht werden kann. Vergleichbar mit den Anfängen der Informatik, liegen mathematische Grundlagen, physikalische Realisierung und informatische Nutzung von Quantencomputern noch sehr nah beieinander, was sich auf die existierenden Schwerpunkte und Vermittlungsansätze auswirkt. Darüber, dass eine quanteninformatische Perspektive existiert und sinnvoll ist, bestand in der Expertengruppe Einigkeit. Eine besondere Herausforderung für die informatische Bildung stellt der Umstand dar, dass bisher noch kaum konkrete Anwendungsmöglichkeiten der Quanteninformatik existieren und sich Handlungsorientierung im Unterricht bspw. auf Simulation und Zukunftsszenarien beschränken muss. Gleiches gilt für die gesellschaftlich-kulturelle Perspektive: Die potenziellen Auswirkungen der Quantentechnologien motivieren zwar bereits eine Reihe an Forschungsrichtungen, wie bspw. die (Post-)Quantenkryptographie, sind aber in der Lebenswelt derzeit noch nicht spürbar. Da ihnen aber gesellschaftsveränderndes Potenzial zugeschrieben wird, sind im Sinne eines informierten öffentlichen Diskurses Bildungszugänge notwendig, die für die breite Bevölkerung verständlich sind.

Betrachtet man die analysierten Erklärungsansätze, ist festzustellen, dass bisher die mathematischen und physikalischen Sichtweisen und Zugänge zu Quantentechnologien dominieren. So wurden im untersuchten Korpus oft auch im Rahmen von Einführungen in die Quanteninformatik physikalische Experimente beschrieben oder komplexe Zahlen und Matrizen zur Beschreibung von Zuständen und Gattern eingeführt. Der Korpus zeigt aber, dass Erklärungen der Ideen auch ohne entsprechende physikalische Grundlagen oder elaborierte Mathematikkenntnisse möglich sind. Weiterhin ist festzustellen, dass im Korpus quanteninformatische Ideen oftmals von klassischen Konzepten ausgehend erklärt bzw. dazu kontrastiert werden. Damit stellen traditionelle Inhalte der informatischen Bildung, wie die Repräsentation von Informationen durch Bits oder die Realisierung der Informationsverarbeitung durch Computer mithilfe von Logikgattern, eine wichtige Grundlage für die Vermittlung von Quanteninformatik dar. Darüber hinaus zeigt sich, dass häufig Analogien eingesetzt werden. Analogien können helfen, einem konstruktivistischen Lernverständnis entsprechend, Sachverhalte anschaulich zu verdeutlichen, reduzieren aber zumeist die Idee auf einen einzelnen Teilaspekt, woraus sich hier besondere Herausforderungen in Bezug auf Fehlvorstellungen ergeben. So ist die Analogie des Münzwurfs für Qubits in Superposition nur eingeschränkt tragfähig, da sich Objekte wie Münzen eben nicht nach quantenmechanischen Gesetzen verhalten, sondern sich das Ergebnis eines Wurfes bei genauer Kenntnis aller Parameter durchaus berechnen ließe. Ein vergleichbares Problem zeigt sich bei der Analogie, dass Quantencomputer – ähnlich wie klassische Multiprozessorsysteme – hochgradig parallel arbeiten würden. Tatsächlich verändern Quantencomputer die Wahrscheinlichkeiten einer Vielzahl von potenziellen Lösungen so, dass sehr wahrscheinlich eine korrekte Lösung gemessen wird. Entsprechend kann es als Aufgabe der Informatikdidaktik angesehen werden, zu erforschen, welche Zugänge und Analogien geeignet sind, hilfreiche Vorstellungen zu entwickeln, welche Fehlvorstellungen vermieden werden sollten und welche altersgerechten Kompetenzen Schülerinnen und Schüler im Bezug auf Quanteninformatik erwerben können und sollten.

Die Beschäftigung mit Quanteninformatik als junge Teildisziplin der Informatik macht deutlich, dass sowohl die fachliche Ausgestaltung als auch die informatikdidaktische Diskussion noch ganz am Anfang stehen. Vor dem Hintergrund der anzunehmenden enormen Fortschritte im Feld der Quanteninformatik und dem daraus resultierenden wachsenden Einfluss auf unsere Lebenswelt ist zu erwarten, dass Quanteninformatik sich vermehrt auch als Aufgaben- und Forschungsgebiet der Informatikdidaktik entwickeln wird. So deuten bspw. das Rahmenprogramm der Bundesregierung zu Quantentechnologien und das steigende Interesse der Informatiklehrinnen und -lehrer bereits darauf hin. Auch wenn Quanteninformatik nicht in naher Zukunft Eingang in die Lehrpläne findet, so sollte doch den Schülerinnen und Schülern die Möglichkeit gegeben werden, im Rahmen extracurricularer Vertiefungen oder Wahlthemen diese spannenden Entwicklungen nachzuvollziehen, Interesse zu entwickeln und vielleicht später selbst Zukunft mitzugestalten.

Literatur

- [Al20] Alpert, C. L.; Edwards, E.; Franklin, D.; Freericks, J.: Key Concepts for Future QIS Learners, 2020, URL: <https://qis-learners.research.illinois.edu/>.
- [BD06] Bortz, J.; Döring, N.: Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler. Springer, Berlin Heidelberg, 2006.
- [Bi18] Billig, Y.: Quantum Computing for High School Students. Qubit Publishing, Ottawa, Ontario, Canada, 2018.
- [Er12a] Erb, R.: Einführung in die Quantenphysik mit Licht, 2012, URL: https://www.uni-frankfurt.de/52729717/12_Quantenphysik_mit_Licht1.pdf.
- [Er12b] Erler, G.; Strunz, A.; Vetter, A.; Bronner, P.: QuantumLab - Schülerlabor zur Quantenoptik, 2012, URL: <https://www.quantumlab.nat.fau.de/>.
- [Gr96] Grover, L. K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. S. 212–219, 1996.
- [HNR07] Hartmann, W.; Näf, M.; Reichert, R.: Informatikunterricht planen und durchführen. Springer-Verlag, 2007.
- [La17] LaRose, R.: Teaching quantum computing through programming, 2017, URL: https://medium.com/@rlarose_26759/teaching-quantum-computing-through-programming-799283c9769a.
- [Le99] Leisen, J.: Quantenphysik-Mikroobjekte: Handreichung zum neuen Lehrplan Physik in der Sekundarstufe II, 1999.
- [LM18] LMU: Introduction to Quantum Computing, 2018, URL: <http://www.nm.ifi.lmu.de/teaching/Vorlesungen/2018ws/QuantumComputing/>.
- [Ma10] Mayring, P.: Qualitative Inhaltsanalyse. In: Handbuch qualitative Forschung in der Psychologie. Springer, S. 601–613, 2010.
- [Pe19] Perry, A.; Sun, R.; Hughes, C.; Isaacson, J.; Turner, J.: Quantum Computing as a High School Module. arXiv preprint arXiv:1905.00282/, 2019.
- [Ru19] Rubin, H.: Vom Doppelspalt zum Quantencomputer, 2019, URL: <https://educ.ethz.ch>.
- [Sa18] Satanassi, S.: Quantum computers for high school: design of activities for an I SEE teaching module./, 2018.
- [Sh99] Shor, P. W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review 41/2, S. 303–332, 1999.
- [Su19] Sun, J.: Teaching High School Quantum Computing Scenarios. In: Proceedings of Student-Faculty Research Day CSIS. 2019.
- [Un19] University of Oxford: Quantum Computer Science: 2019-2020, 2019, URL: <https://www.cs.ox.ac.uk/teach-%20ing/courses/2019-2020/quantum/>.
- [Wo18] Wootton, J.: Hello Quantum: Taking your first steps into quantum computation, 2018, URL: <https://medium.com/qiskit/hello-quantum-2c1c00fe830c>.
- [Za98] Zalka, C.: Simulating quantum systems on a quantum computer. Proceedings of the Royal Society: Mathematical, Physical and Engineering Sciences 454/1969, S. 313–322, 1998.