Einleitung

Solange man eine Wahrheit als tief empfindet,
solange hat man sie noch nicht richtig verdaut.

Über dieses Buch

Es ist ein faszinierender Zug unseres Universums, dass es sich als berechenbar erweist und dadurch uns gleichzeitig Werkzeuge schaffen lässt, das Universum – sagen wir besser: kleine Teile davon – berechnen zu können. Unter Benutzung der mechanischen Gesetzmäßigkeiten wurden schon früh »Kalkulatoren« konstruiert, zum Beispiel von Gottfried Leibnitz, Blaise Pascal und anderen.

Manche der Naturgesetze wirkten im Verborgenen. Erst mit dem Eindringen in die Mikrowelt zeigten sie sich. Dabei wurden nicht einfach nur neue Regeln sichtbar, sondern es wurde ein ganz neues »Paradigma« der Naturbeschreibung geboten. Diese neuen Gesetzmäßigkeiten lassen sich zum Bau neuer (Quanten-)Kalkulatoren nutzen, was an sich vor dem Hintergrund früher gemachter Erfahrungen nicht so überraschend sein musste. Relevant ist, dass man unter Ausnutzung der neuen Gesetzmäßigkeiten um vieles schneller rechnen kann. Man rechnet geradezu in einer neuen Liga. Hinzu kommt, dass eine effiziente Berechnung mikrophysikalischer Prozesse erst mit den neuen Quantenkalkulatoren möglich wird. Es gilt gleichsam: »Die effiziente Berechnung von Quantenprozessen erfordert den gezielten Einsatz von Quantenprozessen«.

In diesem Sinne ist es ein Ziel dieses Buchs, sowohl die dem Quantencomputing zugrunde liegenden Prinzipien zu beschreiben als auch die darauf beruhenden innovativen Algorithmen.

Törichte Annahmen über die Leser

Das Buch ist hervorgegangen aus einer Reihe von Seminaren, die an unserer Hochschule und in Schloss Dagstuhl, zum Teil in Kooperation mit der Universität des Saarlands, durchgeführt wurden. Viel Feedback unserer Studenten ist eingegangen, und so ist das Buch vor allem für Studenten gedacht, die sich mit dem relativ neuen und sich dynamisch entwickelnden Gebiet auseinandersetzen möchten. Mit einem gewissen Basiswissen aus der linearen Algebra und Wahrscheinlichkeitstheorie wird ihnen – so unsere Hoffnung – hier eine gute Handreichung geboten. In diesem Kontext können wir uns natürlich auch vorstellen, dass auch der eine oder andere Kollege einen Blick hinein wagen möchte. Vielleicht findet er den einen oder anderen Abschnitt dabei sogar etwas »süffig«.

Ein paar subtile Hintergedanken, was weitere Kreise unserer potenziellen Leserschaft anbetrifft, hatten wir darüber hinaus. Wir nehmen hierzu eine kleine »literarische Anleihe« beim ehemaligen Forschungsminister Volker Hauff, der zur Neuerscheinung der deutschen Ausgabe des Scientific American ein Geleitwort schrieb:

»Wissenschaft, Forschung und Technologie sind heute entscheidende Einflußfaktoren unserer gesamtgesellschaftlichen Entwicklung. […] Der Dialog zwischen Wissenschaft und Öffentlichkeit setzt die laufende Information über wissenschaftliche, technologische und ökonomische Entwicklungen, ihre Alternativen und Konsequnezen voraus: Information aller am Innovationsprozeß interessierten Unternehmen, Verbände, Wissenschaftler und natürlich der staatlichen Institutionen; Information der Bürger, weil demokratische Beteiligung davon abhängt, daß neue Entwicklungen rechtzeitig gesehen, verstanden und bewertet werden.«

Und bereits 15 Jahre vorher schrieb der seinerzeitige Forschungsminister Hans Lenz zur Gründung der Zeitschrift »Bild der Wissenschaft«:

»…die Öffentlichkeit wird nur dann auf eine großzügige Förderung der Wissenschaft drängen, wenn sie sich der steigenden Bedeutung der Wissenschaft bewußt ist. «

Nun hat man durchaus den Eindruck, dass die »Öffentlichkeit sich der Bedeutung der Wissenschaft bewußt ist«, wo man hingegen Zweifel hegen mag, ist, ob »neue Entwicklungen wirklich verstanden werden«, um sie selbst angemessen bewerten zu können. Man verlässt sich auf Experten und gerät unversehens in ein Fahrwasser der – pardon – »Wahrheitsfindung per Zitatologie«.

Damit kommen wir aber zu einem systemischen Problem: Der vermittelnde Wissenschaftler *hat* die Zeit, sein Thema aufzubereiten, der Adressat muss sie sich in Konkurrenz zu anderen Interessen und Verpflichtungen *nehmen*. Dies betrifft insbesondere politische und sonstige Meinungsführer, die keine Zeit haben. Sie haben einfach nie Zeit. Sogar die jungen Leute an unseren Hochschulen, denen man noch eine gewisse Zeitsouveränität zubilligen würde, sind – das ist so schnell wohl nicht zu ändern – sehr von ihren Smartphones und YouTube absorbiert. Für die früheren Generationen der Karl-May-Leser war das Lesen gedruckter Bücher noch selbstverständlicher. Heute muss man dafür werben. Und wir denken, dass es exzellente Gründe gibt, zu einem Buch zu greifen. Wir sehen ein gutes Buch als »Haupttriebwerk« und die YouTube-Videos als »Booster«.

Wenn wir mit unseren Hintergedanken über unsere Studenten und Kollegen hinaus an Entscheider oder andere Multiplikatoren wie Fachjournalisten denken, stellt sich die ganz praktische Frage, wie man potenzielle Leser animieren kann, im Buch zu schmökern. Nicht aus unangenehmer Pflicht, sondern lustvoll.

Wie also kann man potenzielle Leser animieren, zu einem/diesem Buch zu greifen? Man sollte es zum einen bebildern, und zwar mit Grafiken, die überraschende Botschaften beinhalten. Dies haben wir in den ersten Kapiteln versucht, etwa mit dem Bild eines neugierigen Menschen, der hinter den Monitor zu blicken versucht. Einen Schuss »Zauberei« haben wir dazugegeben, zum Beispiel beim Bombentest-Experiment mittels einer »Nullmessung« vor dem Hintergrund des Doppelspaltexperiments. Dabei haben wir den Stoff in möglichst kleine Häppchen aufgeteilt mit vielen verschiedenen »Einsprungstellen«. Der Preis hierfür besteht in einer gewissen Redundanz, in Wiederholungen von zum Teil schon vorher Gesagtem. (Allerdings hat eine maßvolle Redundanz in den Lehrveranstaltungen unsere Studenten nie so wirklich gestört …)

Insofern haben wir die Hoffnung, den einen oder anderen aus den genannten Personengruppen zunächst zum Blättern und dann doch zum Lesen zu verführen.

Vor welchen speziellen Herausforderungen standen wir?

Ein Buch über »Quantencomputing« erfordert wie schon angedeutet einen Spagat zwischen Anschaulichkeit – das sind die klassischen Anforderungen einer breiteren Leserschaft – und einer Beschreibung der eigentlich unanschaulichen Prozesse in der Mikrowelt – das sind die nicht verhandelbaren Anforderungen der Natur selbst. Man ist in solchen Fällen geneigt, mit Metaphern zu arbeiten, die im Grenzfall dann eben doch eine falsche Anschaulichkeit vorspiegeln.

Geht es auch anders? In einer Rezension zu »The road to reality« von Roger Penrose lesen wir:

»Die übliche Weise moderne Physik einem größeren Auditorium zu vermitteln, sind Sachbücher, wie die von S. Hawking, P. Davis, J. Barrow oder B. Green nur um einige zu nennen, die sich wohl verdienter Weise großer Beliebtheit und Verbreitung erfreuen, leider weichen diese Darstellung - mit unter im entscheidenden Moment - in Metaphern aus, zum Beispiel wird das oft zitierte Gummituch als Gleichnis für die gekrümmte Raumzeit der Relativitätstheorie bemüht.«

Kenner dieses Buchs wissen, dass Penrose *nicht* in Metaphern ausweicht und dabei Stephen Hawking in dessen Ansicht, dass jede Formel in einem Buch die Anzahl der Leser halbiere, doch widerlegt. Ob das auch mit dem vorliegenden Buch gelingt, ist natürlich ein Experiment mit ungewissem Ausgang.

Wo liegen die verstandesmäßigen Knackpunkte?

In der evolutionären Auseinandersetzung mit der Natur haben wir einen Objektbegriff entwickelt und kalibriert, der sich bei kleinen Kindern innerhalb des ersten Lebensjahres konsolidiert. Die dabei gemachten Erfahrungen beziehen sich auf den Umgang mit Gegenständen, die aus vielen, vielen Elementarteilchen zusammengesetzt sind. Sie bestehen in der Regel aus 10^{20} oder mehr Atomen. Die Situation ist – um hier eine Metapher auf der »Metaebene« zu gebrauchen – vielleicht vergleichbar dem Blick auf einen Monitor oder Fernsehbildschirm aus der Ferne. Die Helligkeits- und Farbverteilungen der Pixels auf der Bildschirmoberfläche lässt uns reflexhaft Objekte und ihre Dynamik »sehen«. Nähert man sich dem Bildschirm, womöglich noch mit einer Lupe versehen, dann »verschwinden« die Objekte. Was bleibt, ist eine räumliche und zeitliche Verteilung von elementaren Einzelereignissen, eben das Aufleuchten einzelner Pixelpunkte. Erst in deren Aggregation und aus der Ferne betrachtet »entstehen« die Objekte.

Verlust der Anschaulichkeit

So haben wir es in der Mikrophysik, dem Geburtsort der Quantenmechanik, mit ganz andersartigen Teilchen (besser: Entitäten) zu tun, die man sich eben nicht mehr als kleine Billardbälle vorstellen sollte. Man spricht in solchen Fällen gerne davon, dass solche Objekte sowohl Wellen-als auch Teilcheneigenschaften besitzen, und nennt dies den »Welle-Teilchen-Dualismus«. Dies kann man tun. Ausgeblendet wird bei dieser Sprechweise, dass

solche Teilchen durchaus in einer einheitlichen Datenstruktur codiert werden können, die beides automatisch enthält: Teilchen- und Wellencharakter. Hierzu, und das kann als ein Sprung in den »Abgrund« empfunden werden, wird als Rahmen im Allgemeinen ein unendlich dimensionaler Vektorraum mit darüber hinaus komplexwertigen Skalaren benötigt. Hier sind wir bei den sogenannten *Hilberträumen.* Eine mikrophysikalische Entität »ist« ein Element eines Hilbertraums.

Bekanntlich besitzt jeder Vektorraum ganz unterschiedliche Basen, die man sich als unterschiedliche Koordinatensysteme vorstellen kann. Jede Entität im Hilbertraum kann dann als geeignete Linearkombination – oder Überlagerung – von Basisvektoren beschrieben werden. Es sind zwei Basen, die hier eine prominente Rolle spielen. Diese Basen unterscheiden sich darin, dass die eine Basis den Teilchencharakter widerspiegelt oder »implementiert« und die andere den Wellencharakter. Welche der beiden Basen zur Anwendung kommt, hängt vom Messgerät ab. Der Messapparat »inkarniert« sozusagen die Basis, sodass es Messungen gibt, die den Teilchencharakter hervortreten lassen, und solche, bei denen die Welleneigenschaften manifest werden.

Nullmessungen

Eine gerne benutzte Sprechweise lautet auch, dass die zutage getretene Unfassbarkeit der Mikrowelt darauf beruhe, dass mit jedem Messvorgang eine unkontrollierbare Störung beim Messprozess auftrete. Das ist nicht (ganz) falsch, und findet in den Beschreibungen des Messprozesses seine Entsprechung. Dennoch kennt man auch hier das Phänomen der »Nullmessung«, bei der eben nichts »gestört« wird. Einzig die Tatsache, dass etwas gemessen werden könnte, dass also ein Messapparat »scharf gestellt« wurde, führt hier zu einem Effekt, der klassisch nicht zu erklären ist.

Damit stehen wir vor der folgenden Aufgabe

Will man es nicht bei phänomenologischen Situationsbeschreibungen begleitet von ungefähren Handbewegungen bewenden lassen, was einem gewissen Obskurantismus Vorschub leisten würde, dann hat man auch in einem »Dummy«-Buch eigentlich keine Wahl. Die Andersartigkeit der Mikrowelt ist in eine rationale Form zu bringen, und diese Form macht sich die schon erwähnten komplexen Vektorräume zunutze.

Man kann sich dabei auf den optimistischen Standpunkt stellen, dass dadurch wieder etwas »Anschaulichkeit« zurückkehrt. Denn zumindest niedrigdimensionale Vektorräume lassen sich leicht visualisieren. Den Übergang zu höherdimensionalen Räumen wird man dann nicht mehr als Übergang von der Quantität in eine neue Qualität empfinden.

Hat man damit die Quantenmechanik verstanden? Nicht ganz. Es bleiben die zufälligen Übergänge, die, da sie keinem Algorithmus gehorchen, genau deshalb nicht rational zu erfassen und zu »verstehen« sind.

Umgang mit der Komplexität

Auch hier ist ein Spagat vorzunehmen, den man schon vom Software Engineering und vom Programmverstehen her kennt. Große Programmpakete bestehen aus Millionen und aber

Millionen Zeilen von Code. Auf der Code-Ebene einzusteigen, um auf diese Weise ein Programmverständnis zu erwerben, ist nur etwas für Temperamente, »die ausziehen wollen, das Fürchten zu lernen«. Und so gibt es auch in der Mathematik Theoreme, deren Beweise eigentlich nur »top down« zu verstehen sind, ausgehend von Beweisideen und der Beschreibung einer »Beweisarchitektur«. Die benutzten Hilfssätze, die Lemmata, kann man dann, sofern sie einem hinreichend plausibel erscheinen, überspringen. Will man es genau wissen, steigt man auch in deren Beweise ein.

In Originalaufsätzen wird dabei oft ein gerüttelt Maß an Vorwissen vorausgesetzt. Man schreibt für seinesgleichen auf der Peer-Ebene. Das ist, wenn man auf Augenhöhe kommunizieren kann, ein probates Mittel, die Komplexität auf ein erträgliches Maß zu reduzieren.

Für ein »Dummy«-Buch ist das natürlich kein gangbarer Weg. Der Kompromiss muss also darin bestehen, dass dort, wo wir das Herz der Quantenmechanik berühren, die Prozesse möglichst exakt – also ohne »suggestive Handbewegungen« – beschreiben. Dabei nehmen wir den Leser, wenn er sich denn führen lassen will, »eng an die Hand«. Das heißt, wir führen ihn in kleinen Schritten durch unwegsam erscheinendes Gelände. Wenn er geneigt ist, gewisse Sachverhalte zu glauben, kann er Abschnitte überspringen. Sollte er sich jedoch dazu entscheiden, wichtige Rechenschritte im Detail nachzuvollziehen, wird er feststellen, dass er es kann! Und sollte er sich im unwegsamen Gelände tasächlich verstiegen haben, rufe er die »Bergwacht« an: `hans-juergen.steffens@hs-kl.de`. Wir holen Sie raus.

Was muten wir zu?

Man könnte befürchten, dass es von den Seiten abhängt, die man zufällig aufschlägt, ob weitergelesen wird oder nicht. Ob es also ein interessantes Bild oder eine Seite voller Formeln ist, die einem entgegenblickt. Nun muss ein Buch über Quantencomputing, wenn es ernstgenommen werden soll, Formeln und Herleitungen enthalten, auch wenn es sich als eine Einführung versteht. Wir haben darauf geachtet, die Herleitungen so ausführlich wie nur irgend möglich zu beschreiben. Das, von dem wir annehmen, dass es nicht zum Vorwissen gehört, wird in den laufenden Kapiteln und in separaten Anhängen beschrieben. Es sollte nach unseren Standards nachvollziehbar sein. Die Frage stellt sich natürlich, ob die ganzen Formeln nötig sind. In Artikeln der Tagespresse verzichtet man darauf und argumentiert mit Metaphern, wir hatten diesen Aspekt bereits angesprochen. Das kann durchaus hilfreich sein. Ein wirkliches Verständnis erhält man dadurch leider nicht.

Kommen wir damit nochmals zu unseren Politikern und sonstigen Entscheidern. Wir halten es für wichtig, dass auch hier (und auch bei anderen Fragen) ein tieferes Verständnis entwickelt wird. Um hier einen bekannten Satz abzuwandeln: »Vertrauen ist gut – selbst rechnen ist besser«. Man sollte wegkommen von blindem Vertrauen auf Experten, und ähnlich wie beim Umgang mit Zahlen sollte man Plausibilitätsbetrachtungen und Überschlagsrechnungen selbst durchführen können. Nichts ist schlimmer, als eine Antwort zu hören der Art: »Aber der Computer hat's doch gesagt.«

Worin also bestehen die nützlichen Voraussetzungen: Da sind zum einen die Vektorrechnung und der Umgang mit Matrizen, kurz ein Stück linearer Algebra. Von ihr lebt die Quantentheorie ebenso wie von der Wahrscheinlichkeitsrechnung. Wir denken, dass der bereitgestellte working set im Anhang die Hemmungen beseitigt, sich mit dem Quantencomputing ernsthaft auseinanderzusetzen.

Wie dieses Buch aufgebaut ist

So wie die Interessen der verschiedenen Lesergruppen unterschiedlich ausgeprägt sind, so werden unterschiedliche Einstiege in die Fragen und die Methodik des Quantencomputing als sinnvoll empfunden. Ein Blick aus der »Vogelperspektive« auf das Konzept »Computer« und »Berechenbarkeit« allgemein schien uns für ein **einleitendes Kapitel** unverzichtbar.

Teil I: Neue Phänomene und neue Betrachtungsweisen

Neue Perspektiven sollen also im ersten Teil vermittelt werden, ausgehend von dem, was die klassische Physik an Vorstellungen mitbrachte, ergänzt um das, was die Quantenphysik später dazugab. Der Kontrast zwischen klassischer und Quantenphysik sollte hier schon sichtbar anklingen. Auch denen, die einen besonderen Blick auf die Anwendungen haben, sollte hier eine erste Antwort gegeben werden.

Um die interessierten Leser nicht zu lange auf die Folter zu spannen, ist es wünschenswert, so früh wie möglich einen Einblick in die besonderen Fähigkeiten beim Quantencomputing zu erhalten. Hier biss sich die Katze ein wenig in den eigenen Schwanz. Für eine vernünftige Beschreibung benötigt es einiges an mathematischem Rüstzeug. Ein guter Kompromiss erschien uns, im **zweiten Kapitel** das sogenannte »dense coding« kombiniert mit einem ersten noch etwas oberflächlicheren Durchlauf durch die Qubits zu behandeln. Das dense coding ist zwar noch kein Quantenalgorithmus im engeren Sinne, die dabei benutzten Qubit-Manipulationen sind aber so grundlegend für die eigentlichen Quantenalgorithmen, dass sie einen ersten wichtigen Eindruck auf das Wesen des Quantencomputing vermitteln.

Das **dritte Kapitel** führt den Matrizenkalkül ein und nutzt ihn zu einer zweiten tiefergehenden Behandlung der Qubits. Das Konzept der Tensorprodukte wird übertragen auf Matrizen (allgemein Operatoren). Damit kann das dense coding prägnanter und nach unserem Empfinden auch eleganter beschrieben werden.

Mit diesem Rüstzeug versehen kommen wir im **vierten Kapitel** zum zweiten Beispiel, der Quantenteleportation, einem Klassiker im Kontext des Quantencomputing. Sie wird in zwei Sichtweisen präsentiert: rein mathematisch im Matrizenkalkül ohne eine physikalische Interpretation und einmal unter expliziter Benutzung des Tensorkalküls, in dem sich die physikalische Sichtweise widerspiegelt.

Teil II: Neue Spielregeln in der Physik

Eine neue Physik das Thema des zweiten Teils. Im Bemühen, möglichst früh charakteristische Beispiele zu bringen, die als Bausteine des Quantencomputing illustriert werden können, ist die Beschreibung quantentheoretischer Aspekte in den zweiten Teil gerückt. Der Übergang von der klassischen Physik zur Quantenmechanik beruht auf einer Remodellierung der Mikrowelt, wie sie im **fünften Kapitel** skizziert wird. Dort liegt die eigentliche Revolution.

Hierzu steigen wir im **sechsten Kapitel** bildlich in die »Unterwelt« ein. In der Mikrowelt findet eine Neubewertung des Konzepts zufälliger Ereignisse statt. Viel Raum und Zeit wird dafür verwendet, diesen Aspekt anhand des berühmten »Doppelspaltexperiments« in der Gegenüberstellung makroskopischer und mikroskopischer Prozesse zu illustrieren. Hier

befindet sich das Einfallstor des nackten Zufalls, eines Zufalls, der nicht auf »zufälliger« Unwissenheit beruht. Dies ist der Punkt, an dem der berühmte Physiker Richard Feynman bemerkt: »Niemand versteht die Quantenmechanik«. Der reine Zufall ist eben algorithmisch nicht zu fassen und in genau diesem Sinne nicht zu verstehen. Wir sähen es als Lücke, würde der Leser eines Buches über Quantencomputing hierfür nicht sensibilisiert.

Teil III: Qubits und ihre Operatoren

Hiermit beginnt der Hauptteil des Buchs. Der mathematisch etwas versiertere Leser kann hier direkt einsteigen (und so finden wir hier zum Beispiel – wie oben erwähnt – gewisse Überlappungen zu vorangegangenen Kapiteln).

Zum Zweck einer sanften mathematischen Überleitung des klassischen Bit-Begriffs zum Qubit wird das Bit im **siebten Kapitel** voll in den mathematischen Rahmen der Qubits überführt. Aus Sicht der Informatik ist das zunächst ein Overkill: Es ändert sich am operationellen Verhalten der Bits nichts, aber der benutzte Formalismus ist komplexer. Aufgrund der Vorteile einer direkteren Vergleichbarkeit zwischen Bit und Qubit erschien es uns das aber wert. Als »Return on Invest« hat man dann im **achten Kapitel** bereits die passenden »unitären« Operatoren für die Handhabung von Qubits.

Das Quantencomputing wäre nur eine »Schönwetterveranstaltung«, wenn keine sinnvollen Maßnahmen zur Fehlerkorrektur vorlägen. Denn die physikalischen Bausteine zur Implementierung von Qubits sind »empfindlicher als ein Schmetterlingsflügel«. Die Beschreibung von Fehlerkorrekturen geschieht im **neunten Kapitel**.

Teil IV: Quantenfouriertransformationen und mehr

Quantenalgorithmen in Aktion sind das Thema des vierten Teils. Dreh- und Angelpunkt zentraler Algorithmen ist die Quantenfouriertransformation. Und wir nehmen uns viel Zeit, im **zehnten Kapitel** auch die Einzelheiten zu erklären.

Aufbauend auf der Quantenfouriertransformation werden im **elften Kapitel** die berühmten »Killerapplikationen«, der Shor-Algorithmus, als Anwendung besprochen. Auch dort bemühen wir uns, die Herleitungen möglichst genau und nachvollziehbar zu beschreiben.

Teil V: Weitere Anwendungen

Breit gestreutere Anwendungen finden sich abschließend im fünften Teil. Für die Gefahr, die das Quantencomputing für bis heute starke Verschlüsselungsverfahren bedeutet, bietet sie faszinierenderweise gleichzeitig eine Lösung, wie sie im **zwölften Kapitel** erläutert wird. Diese innovativen quantenmechanischen Verschlüsselungsverfahren beruhen in einem wichtigen Sinne nicht mehr auf einem Algorithmus, sondern auf den nicht algorithmisierbaren Zufallsprozessen. Diese Verfahren sind heute in der Quantentechnologie am meisten fortgeschritten. Sie haben gleichsam »Production Quality«-Status.

Ein weiterer Klassiker im Quantencomputing, der Grover-Algorithmus, wird im **dreizehnten Kapitel** vorgestellt. Als innovatives Suchverfahren beschleunigt er zwar »nur« quadratisch, hat damit aber bei Datenbanken mit Milliarden von Einträgen einen durchaus attraktiven Vorteil.

Das Thema des **vierzehnten Kapitels**, adiabatisches Quantencomputing und zeitliche Simulation der sogenannten Schrödingergleichung, erforderte streng genommen ein eigenes Buch. Hier begegnen sich Quantencomputer und Analogcomputer am engsten. Die ursprüngliche Idee von Richard Feynman, quantenmechanische Prozesse für die Simulation quantenmechanischer Prozesse zu benutzen, findet hier ihre stärkste Ausprägung. Das bedeutet aber auch, dass es hierbei sehr viel mehr noch als in der physikalischen Implementierung einzelner Qubits um »harte« Quantenphysik geht. Das aber wollten wir dem Leser nicht mehr so ganz zumuten. Ganz außen vor lassen wollten wir es aber auch nicht. Einen Teil davon haben wir in die Anhänge ausgelagert.

Teil VI: Top Ten Teil

Im **fünfzehnten und letzten Kapitel** streifen wir die geschichtlichen Entwicklungen, die zu unseren heutigen Vorstellungen geführt haben. Mit Geschichte beschäftigt man sich dann, wenn die Probleme der Gegenwart gelöst sind – oder sollte es faktisch umgekehrt sein? Übertragen auf dieses Buch möchte man sagen: Wer bis zum fünfzehnten Kapitel durchgehalten hat und feststellt, dass er mehr verstanden hat, als er ursprünglich zu hoffen wagte, wird den Rückblick auf die Geschichte als lustvolles Dessert empfinden.

Eingestreute »two cents«

Wir haben der Versuchung nicht widerstehen können, einige einfache Vorschläge zu kontrovers diskutierten Fragen im Rahmen der Quantenmechanik einzubauen. Dies betrifft zum Beispiel das berühmte Messproblem in der Quantenmechanik, das Einstein-Podolsky-Rosen-Paradox und einen Beitrag zu einem hybriden Verschlüsselungsverfahren, wie wir es in der Literatur bisher nicht gefunden haben. Ob es sich dabei, um »Schmankerl« handelt, das müssen andere entscheiden ...

Was wir draußen ließen

Nimmt man ein enzyklopädisches Lehrbuch (mit Kultcharakter) wie das Buch von Nielsen und Chuang »Quantum Computation and Quantum Information« zur Hand, stellt man schnell fest, dass das Quantencomputing sehr viel mehr umfasst als das, was wir in unserem Buch behandeln. Das liegt ein wenig in der Natur eines Buchs, wie wir es uns vorgestellt haben. Nielson und Chuang führen mit ihren »Übungsaufgaben« bis an die heutigen Forschungsgrenzen heran (sie haben sie unauffällig mit »Research« gekennzeichnet). Damit können, wollen und dürfen wir uns nicht messen.

Folgende Aspekte und Fragestellungen haben wir weggelassen oder nur gestreift:

- ✔ Die theoretische Komplexitätstheorie, also die exakte Beschreibung der Klassen, die als polynomial, nichtdeterministisch polynomial, NP-vollständig und so weiter klassifiziert werden. Dies sind Themen für gestandene Theoretiker. Für eine Einführung in das Quantencomputing soll es genügen, an Beispielen, etwa beim Shor-Algorithmus, zu sehen, dass hier ein qualitativ großer Performanzgewinn liegt.
- ✔ Die verschiedenen sich anbietenden physikalischen Implementierungen von Qubits. Ähnlich den klassischen Bits ist dies eine Frage für den Physikingenieur. So haben wir

uns in diesem Buch auf eine kurze Beschreibung einer Implementierung mittels polarisierter Photonen beschränkt, gewissermaßen als »proof of concept«. Damit kommen wir der Sichtweise eines Informatikers entgegen: Ein Qubit ist ein Qubit ist ein Qubit.

✔ Letztlich verzichten wir auf eine Behandlung der Fragen zu Entropie und zum Quantenrauschen. Auch dies ist mehr etwas für den ausgewiesenen Spezialisten.

Konventionen und Symbole in diesem Buch

Sie finden in diesem Buch einige Icons mit besonderer Bedeutung, die kurz beschrieben werden sollen:

Hier finden Sie Ergänzungen und vertiefende Informationen. Dies kann beim ersten Lesen übersprungen werden, um später noch einmal darauf zurückzukommen.

Die hiermit gekennzeichneten Teile dienen der Auflockerung. Es sind zum Teil Episoden aus der Geschichte und ein Blick über die fachlichen Grenzen hinaus.

Dort finden sich wchtige Zusammenfassungen des Gesagten, Fakten, an die man sich erinnern sollte.

Danksagungen

An einem Buchprojekt sind regelmäßig nicht nur die genannten Autoren beteiligt. Viele haben mittel- oder unmittelbar beigetragen und haben es verdient, hier namentlich erwähnt zu werden. Beginnen möchte ich mit unseren Studenten, die in den Seminaren über Quantencomputing ein bemerkenswertes Engagement gezeigt hatten. Sie legten – mit einer intakten Skepsis sozusagen – stets den Daumen auf Unklarheiten und Ungenauigkeiten. Kurzum: Sie wollten es wirklich *wissen*. Ihr Feedback floss in geeigneter Weise in die Gestaltung und die Inhalte unseres Buchs ein.

Genannt werden sollen hier also zunächst:

Armin Beckmann, Dennis Buttel, Sebastian Dauenhauer, Maik Denisenko, Kim Enders, Julian Frenzel, Patrick Geerds, Manuel Golz, Luca Hartmut, Julia Hartwich, Benjamin Hütz, Andreas Jost, Kevin Klein, Marcel Krebs, Xaver Lutz, Emira Mansour, Felix Mayer, Dominik Müller, Daniel Mutz, Adrian Risch, Christian Roth, Benedict Särota, Kai Uwe Sauther, Mario Schertan, Lucas Schopp, Tristan Theiß, Felix Trautmann, Leon Veith.

Ein besonderer Dank geht an die Kollegen Prof. Becher und Prof. Eschner von der Universität des Saarlands sowie Prof. Hettel an unserer eigenen Hochschule Kaiserslautern. Die früheren gemeinsamen Seminare im Schloss Dagstuhl in Kooperation mit den Saarbrücker

Kollegen waren ein Highlight. Ihre Präsentationen der physikalischen Grundlagen für die Implementierungen von Qubits waren für Informatiker immer erhellend. In jedem Fall »erdeten« sie uns Informatiker. In diesem Kontext auch nochmals ein spezieller Dank an Jörg Hettel, der es mir dankenswerterweise überließ, in der Zeit der Arbeiten an diesem Buch das Seminar über Quantencomputing durchzuführen.

Unsere beiden studentischen High Potentials Lorena Mayer und Sagani Naguleswaran ließen sich nie entmutigen, wenn sich die Anforderungen und Wünsche hinsichtlich textueller Verbesserungen und grafischer Gestaltung manchmal (sehr) schnell änderten. Sie haben sich mit viel Herzblut eingebracht.

Die Betreuung durch unseren Lektor Herrn Ferner vom Wiley-Verlag empfanden wir – wie auch schon bei unserem ersten Buch – als vorbildlich. Es war in Anbetracht der Corona-Pandemie ja keine leichte Zeit, und es entlastete uns doch sehr, wenn uns an der einen oder anderen Stelle etwas mehr Zeit zugebilligt wurde.

Widmungen

Gewidmet meiner lieben Frau Petra sowie unseren Kindern Stella Isabel, Victor André und Sophie Madeleine, die einmal den Staffelstab von uns übernehmen werden.
(Hans-Jürgen Steffens)

Für Patricia, weil das Leben mit dir »bunt und granatenstark« ist.
(Christian Zöllner)

Gewidmet meinem Mann André und unserem Sohn Lennard in der Hoffnung, dass die Quanteninformatiker ihm eine chancenreiche Zukunft bieten.
(Kathrin Schäfer)