universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

Quantencomputer in der Schule

angestrebter akademischer Grad

Magister der Naturwissenschaften (Mag. rer.nat.)

Verfasser:	Stefan Greindl
Matrikel-Nummer:	0601835
Studienrichtung:	Lehramtsstudium UF Physik UF Mathematik
Betreuerin:	Privatdoz. Mag. Dr. Beatrix Hiesmayr

Wien, am 5. Mai 2011

Zusammenfassung

Was ist eigentlich ein Quantencomputer und wie kann man ihn in der Schule unterrichten?
Diese Diplomarbeit beschäftigt sich mit diesem Thema und stellt ein Unterrichtskonzept vor, das zunächst eine Einführung in die Quantenphysik beinhaltet und anschließend die Funktionsweise der Quantencomputer skizziert.
Es werden zu Beginn die wichtigsten Personen und Experimente der Quantenphysik vorgestellt und anschließend die beiden bekanntesten Quantenalgorithmen, in einer schülerInnen-gerechten Komplexität, besprochen.
Die Diplomarbeit beinhaltet auch einen Theorieteil, der die quantentheoretische Funktionsweise und einen ausgewählten Algorithmus ausführlich bearbeitet, hier orientiert sich das Niveau an Lehrkräften.

Abstract

What is a quantum computer about and how can it be taught in secondary school?
This degree thesis engages in this topic and presents an educational instruction, including an introduction to quantum physics and the functioning of a quantum computer. At first it shows the most important persons and experiments of quantum physics, followed by two popluar quantum algorithms, both presented in a pupil orientated way.
In addition this degree thesis contains a theory part for teaching persons, in which the quantumtheoretic mechanics are shown.

Inhaltsverzeichnis

Kapitel 1

Unterrichtsplanung

Dieses Kapitel beinhaltet den Hauptteil dieser Diplomarbeit. Es soll ein Unterrichtskonzept skizziert werden, das in 5 Unterrichtseinheiten eine Einführung in die Quantenphysik gibt und die Theorie des Quantencomputers umreißt.

Die Quantenphysik wird nach Lehrplan in der 7. oder 8. Klasse der AHS Oberstufe unterrichtet. Man arbeitet in diesem Fall bereits mit älteren Schülern.

Meiner Meinung nach soll die moderne Physik in der Schule nur umrissen werden, damit die SchülerInnen, zumindest im Ansatz, schon einmal von diesen Theorien gehört haben. Die Komplexität dieser Theorien lässt sich mit den beschränkten zeitlichen und mathematischen Möglichkeiten kaum in vollem Umfang bewältigen.

Experimente sind, vor allem in der Quantenphysik, im Schulumfeld sehr schwer zu realisieren. Es gibt Kapitel die sich wesentlich besser eignen, wie beispielsweise der Elektromagnetismus. In der Quantenphysik rücken andere Schwerpunkte in den Vordergrund.

Beispielsweise ist der Übergang einer deterministischen Physik, in der alles berechenbar ist, zu einer Physik in der der Zufall eine maßgebliche Rolle spielt, ein interessantes Diskussionsthema. Weiters werden die SchülerInnen mit Gedankenexperimenten vertraut gemacht, eine Technik die der theoretischen Physik große Erkenntnisse gebracht hat.

Aus den oben genannten Gründen möchte ich in dieser Arbeit darauf achten, einen allgemeinbildenden Zugang zu wählen, bei dem weniger der Formalismus, sondern hauptsächlich die Entstehungsgeschichte und die dahinter liegenden Motive im Vordergrund stehen. Dies bedingt natürlich eine gewisse Dominanz von lehrerzentriertem Unterricht.

Wesentlich für diese Kapitel ist meiner Meinung nach der Wille, Diskussionen entstehen zu lassen und diese auch zu führen. Unglücklicherweise sind diese Diskussionen kaum schriftlich festzuhalten und am Ende der Einheit bleibt scheinbar nichts Greifbares, obwohl die Diskussion ein Hauptaspekt der physikalischen Forschung ist. Aus diesem Grund werde ich für jede Unterrichtsstunde ein Handout erstellen, in dem die wichtigsten (und natürlich auch prüfungsrelevanten) Punkte zusammengefasst sind.

Die Planung beinhaltet zu Beginn der Unterrichtseinheit eine 10 minütige Phase, die für organisatorische Tätigkeiten und wahrscheinlich in vielen Fällen, für kurze mündliche Prüfungen, im Rahmen des Notensystems, genutzt werden kann.

1.1 1. Einheit

Die erste Unterrichtsstunde soll den Schülern die ersten Schritte und wichtige Personen der Quantenphysik aufzeigen. Dazu versuche ich die geschichtliche Entstehung dieses Zweiges der Physik zusammen zu fassen (nach [1]).
Das Highlight dieser Stunde ist ein Auszug des Originaltexts von Albert Einstein, für den er den Nobelpreis erhielt. Ich finde es hat einen besonderen Reiz, eine tatsächliche Arbeit, einer der meist zitierten Personen der Physik, zu lesen.

1.1.1 Stundenbild

Zeit	Inhalt
00 - 10	Organisatorisches
10 - 20	Max Planck und der schwarze Strahler
20 - 30	Versuchserläuterung photoelektrischer Effekt und Probleme
30 - 40	Originaltext von Albert Einstein
40 - 50	Besprechung der Konsequenzen

1.1.2 Max Planck und der schwarze Strahler

Max Planck nimmt sicherlich eine wichtige Position bei der Entdeckung und Entwicklung der Quantenphysik ein. Er wurde 1858 in Kiel geboren und begann 1874 mit dem Studium der Physik.
Zu diesem Zeitpunkt war man noch der Meinung, die Physik sei eine abgeschlossene Wissenschaft. Newton kümmerte sich um die mechanischen Vorgänge und Maxwell beschrieb den Elektromagnetismus auch einwandfrei. Sowohl die

Mechanik Newtons, als auch die Interpretation von Licht als elektromagnetische Welle mussten in naher Zukunft anderen Theorien weichen.

Max Planck beschäftigte sich zu diesem Zeitpunkt mit einem Problem, für das es bis dahin noch keine zufriedenstellende Erklärung gab.
Erwärmt man ein Stück Metall weit genug, so beginnt dieses zunächst dunkelrot zu leuchten. Erhitzt man das Metallstück weiter, so ändert sich die Farbe von rot, zu gelb, bis es schließlich weiß leuchtet. Jeder glühende Körper sendet elektromagnetische Strahlung ab (innerhalb eines gewissen Bereichs nehmen wir es als Licht war), diese Körper bezeichnet man als schwarze Strahler.

Im 19. Jahrhundert gab es bereits Theorien, die versuchten dieses Phänomen zu beschreiben, jedoch funktionierten jene nur innerhalb gewisser Grenzen und widersprachen stellenweise einander sogar.

Max Planck machte es sich zur Aufgabe, einen Zusammenhang zwischen dem Spektrum des abgestrahlten Lichts und der Temperatur des Gegenstands herzustellen. Es gelang ihm eine Formel zu finden, diese hatte jedoch einen Schönheitsfehler. Planck hatte in seiner Formel einen numerischen Faktor, den er zunächst nur als mathematischen Kunstgriff sah und den es, so bald als möglich, zu eliminieren galt. Er postulierte, dass ein schwarzer Strahler immer nur Energie von einem Vielfachen jenes numerischen Faktors aufnehmen oder abstrahlen kann. Dieser Faktor geht in die Literatur als Planck'sches Wirkungsquantum mit dem Formelbuchstaben h ein und besitzt den Wert

$$h = 6,626 * 10^{-34} Js$$

So sehr Planck sein Wirkungsquantuum auch missfiel, es beschrieb exakt die experimentellen Tatsachen.

Konsequenzen

Dies war das erste Auftauchen der für die Quantenphysik so wichtigen Konstante h. Allerdings musste man sich nun auch mit der Tatsache anfreunden, dass es unteilbare Energieeinheiten gibt. Dies steht im Widerspruch zu der, bis zu dieser Zeit, so erfolgreichen kontinuierlichen Physik.
Der Universalgelehrte Gottfried Wilhelm Leibniz (1646 - 1726) sagte:"Nichts geschieht auf einen Schlag; und es ist einer meiner größten und bewährtesten Grundsätze, dass die Natur niemals Sprünge macht. Das nannte ich das Gesetz der Kontinuität."
Man muss sich die Folgerungen aus Plancks Formel auch unter den Gesichtspunkten der Zeit und der damals beteiligten Personen vorstellen. Es handelt sich hier immerhin um studierte Physiker, die höchst erfolgreich mit

den Ansätzen der kontinuierlichen Physik gearbeitet haben und plötzlich soll Energie nur quantisiert, also in kleinen Portionen, auftreten?
Es dauerte noch einige Zeit, bis sich die Erklärung Plancks wirklich durchsetzen konnte.
Durch seine Arbeit, seinen Eifer und die bedingungslose Akzeptanz der experimentellen Tatsachen initiierte er eine stürmische Entwicklung der Physik und wurde 1918 mit dem Nobelpreis für Physik geehrt.

1.1.3 Der photoelektrische Effekt

Ein weiteres Experiment, das man mit den damaligen Theoriekonstrukten nur unzureichend erklären konnte, ist der sogenannte photoelektrische Effekt. Der Versuchsaufbau und die Versuchsbeschreibung stammt aus dem Buch "Physik für Wissenschaftler und Ingenieure"von Paul A. Tippler [3].

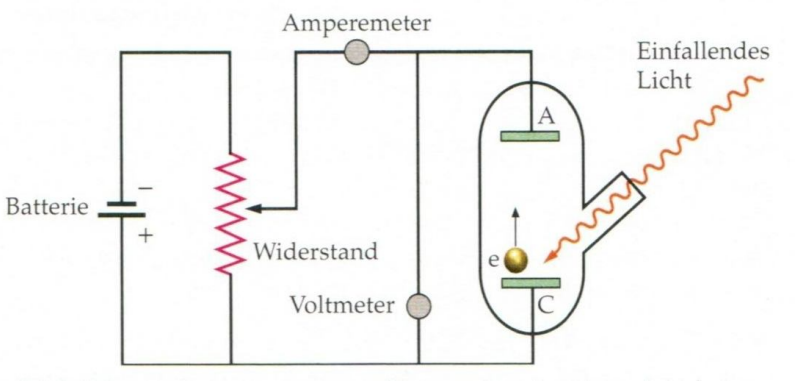


Abbildung 1.1: Versuchsaufbau Photoeffekt

Eine Kopiervorlage des Versuchsaufbaus befindet sich im Anhang.

Licht mit einer bestimmten Frequenz ν trifft auf eine Metallplatte, die dadurch Elektronen emittiert. Diese Elektronen werden von einem Kollektor aufgefangen. Mittels Amperemeter wird der fließende Strom gemessen.

Legt man eine elektrische Spannung zwischen Emitter und Kollektor an, so müssen die Elektronen eine gewisse (kinetische) Energie aufbringen, um den Kollektor zu erreichen. Erhöht man die Spannung bis kein Strom mehr fließt, kennt man die maximale Bewegungsenergie der von der Kathode emittierten Elektronen.

Zieht man die klassische Theorie, das Licht ist eine Welle, zu Rate, so ergeben sich folgende Schlüsse:

- Mit steigender Intensität des Lichts, müsste auch die kinetische Energie der herausgelösten Elektronen steigen, da diese mehr Energie aufnehmen können und folglich mit größerer Geschwindigkeit aus dem Metall austreten.
- Bei niedrigen Intensitäten dauert es, bis die Elektronen genug Energie aufgenommen haben, um sich von der Platte zu lösen

Die Ergebnisse des Experiments stehen allerdings im Widerspruch zu den obigen Vorhersagen:

- Die maximale kinetische Energie ist unabhängig von der Intensität des Lichts, bei gleicher Wellenlänge erhält man stets dieselbe Austrittsgeschwindigkeit.

1.1.4 Originaltext von Albert Einstein

Nach dem Vortrag der Lehrkraft über Planck und den photoelektrischen Effekt, ist es nun an der Zeit den SchülerInnen einen Auszug aus dem Originaltext von Albert Einstein auszuteilen. Es handelt sich hierbei um den Aufsatz aus 1905 mit dem Titel: "Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt."(siehe [5])
Für diese Arbeit wurde Albert Einstein 1921 mit dem Nobelpreis geehrt.

Ich bin der Ansicht, dass es für SchülerInnen durchaus spannend sein kann, einmal einen derartigen Text, wenn auch nur auszugsweise, zu lesen.

Es muss meiner Meinung nach jedoch unbedingt darauf hingewiesen werden, dass dies nur ein Teil der Arbeit ist und Albert Einstein die Lichtquantentheorie sehr wohl aus fundierten physikalischen Überlegungen abgeleitet hat.

Die Kopiervorlage des Originaltextes für die SchülerInnen befindet sich im Anhang.

Nachdem die Schüler den Text durchgelesen haben, sollte der Versuchsaufbau des photoelektrischen Effekts erneut aufgelegt werden und das Experiment nun vom Standpunkt dieser neuen Theorie aus beleuchtet werden.

1.1.5 Stundenabschluss

Das Nahziel dieser Unterrichtseinheit ist es, die SchülerInnen darauf vorzubereiten, dass die Theorie des Lichts als Welle nicht für alle Experimente anzuwenden ist. Dies soll im ersten Schritt die Notwendigkeit einer Quantentheorie demonstrieren. Die SchülerInnen sollen erkennen, dass es sich die Physik zur Aufgabe gemacht hat, eine Theorie für sämtliche Phänomene zu finden.
Da sich einige Experimente des damaligen Theoriekonstrukts entzogen haben, war die Notwendigkeit gegeben, eine umfassendere Theorie zu entwickeln.

Bemerkung: Auch die Annahme des Lichts als Teilchen kann den photoelektrischen Effekt nicht ausreichend erklären. So lässt sich beispielsweise der Streuungswinkel und die Intensitätsverteilung trotzdem nur über die Wellentheorie ableiten.

1.2 2. Einheit

Die zweite Einheit widmet sich dem Doppelspaltexperiment. Die SchülerInnen kennen dieses Experiment noch aus der Optik und sind auch bereits mit einem Erklärungsmodell vertraut. In dieser Einheit soll nun ein Verständnis für die quantenphysikalischen Ansichten dieses Experiments geschaffen werden.

Für diese Stunde wäre es vorteilhaft, einen schnell funktionierenden Beamer mit Internetanschluss zur Verfügung zu haben. In vielen Physiksälen ist bereits ein fixer Beamer installiert und durch den steten Preisverfall kann man hoffen, auch in den Klassenräumen in absehbarer Zeit ein vernünftiges Equipment vorzufinden.
Diese Unterrichtseinheit bedient sich eines Videoausschnitts, der von Dr. Fred Alan Wolf im 2004 veröffentlichten Film "What the #$*! Do We Know!?" stammt [6].

1.2.1 Stundenbild

Zeit	Inhalt
00 - 10	Organisatorisches
10 - 15	Dr. Quantum 1
15 - 25	Besprechung Dr. Quantum 1
25 - 30	Dr. Quantum 2
30 - 40	Wahrscheinlichkeitsinterpretation
40 - 50	Schrödingers Katze

1.2.2 Dr. Quantum

Nach dem Organisatorischen Teil der Stunde folgt die Präsentation des Videos von Dr. Fred Alan Wolf. Es handelt sich genauer gesagt um einen ca. 5 minütigen Animationsfilm zum Thema Doppelspalt. Dieses Video lässt sich glücklicherweise nach kurzer Suche in Internet-Videoportalen finden. Hierbei kann man sogar aus einer deutschen und einer englischen Version des Videos wählen.

Das Video zeigt einen animierten "Superprofessor" Dr. Quantum (Abb. 1.2), der den Urvater der Quantenexperimente, das Doppelspaltexperiment erklärt. Leider orientiert sich die Figur am klassischen Physikerbild: alt, grauhaarig, männlich. An dieser Stelle sollte man diese Vorurteile kurz entkräften und auf die junge, dynamische Generation von PhysikerInnen hinweisen.

Abbildung 1.2: Dr. Quantum

Nach einer kurzen Einführung von Dr. Quantum wird mit einer Murmelkanone auf ein Hindernis mit zuerst nur einem, dann mit zwei Spalten geschossen. Auf einer dahinter liegenden Tafel bilden sich die Spalten ab (Abb 1.3).

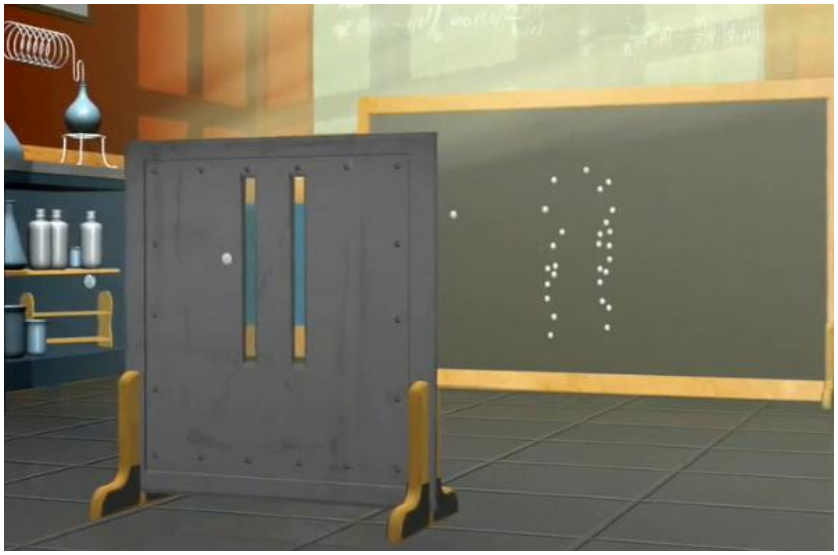


Abbildung 1.3: Doppelspalt mit Murmeln

Im nächsten Schritt wird das gleiche Experiment mit Wasserwellen wiederholt und das entstehende Interferenzmuster beobachtet. Hierbei wird auch die Verstärkung und Auslöschung von Wellenbergen und Wellentälern erläutert (Abb. 1.4).

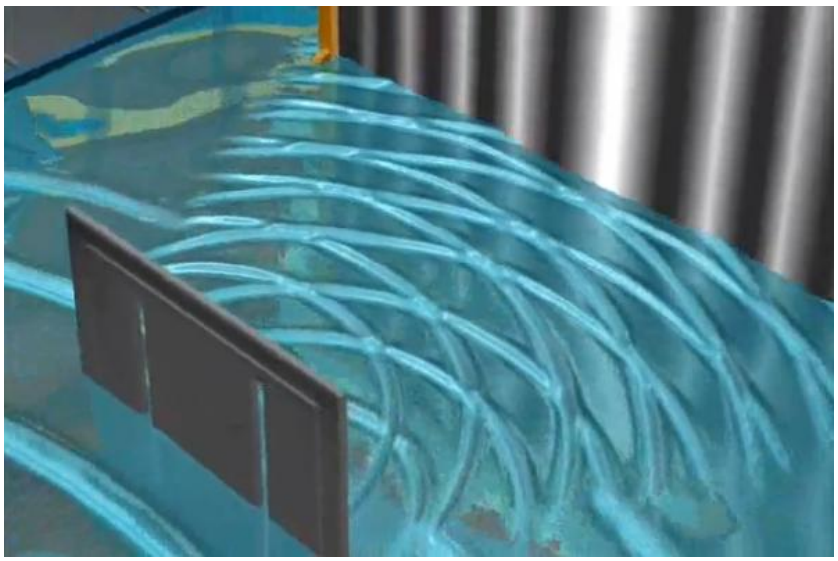


Abbildung 1.4: Interferenzbild von Wellen am Doppelspalt

So weit, so gut. Nun vollzieht Dr. Quantum den Schritt in die Quantenwelt

und beschießt den Doppelspalt anstatt Murmeln mit einem Strahl aus Elektronen. Hier müssten sich eigentlich, genau wie bei den Murmeln, wieder zwei vertikale Streifen mit den Einschusslöchern ausbilden.

Dr. Quantum staunt nicht schlecht, als er auf seinem Schirm ein Interferenzmuster wie bei einer Welle feststellt (Abb. 1.5). Zur Erinnerung: Wir schießen mit Elektronen! Mit Materie! Diese müsste sich eigentlich genau wie die Murmeln verhalten.

Abbildung 1.5: Elektronenstrahl am Doppelspalt

Noch beeindruckender: Auch der Beschuss mit einzelnen Elektronen führt in der Animation, wie auch bei realen Experimenten, zu dem aus der Wellentheorie bekannten Interferenzmuster!

Nach diesem Abschnitt (ca. 3:30) würde ich das Video vorerst pausieren. Es wurde bereits sehr viel Information verpackt und jetzt muss diese wiederholt und aufgearbeitet werden.
Dies ist wieder ein spannender Teil der Unterrichtsstunde, da hier die bisherigen Modelle schlicht und ergreifend versagen.

1.2.3 Besprechung Dr. Quantum

Nach diesem Stoß ins kalte Wasser gibt es sicherlich und hoffentlich einige SchülerInnen, die der gezeigten Information keinen Glauben schenken. Leider hat es meiner Meinung nach wenig Sinn, ein reales Experiment für die

Interfernenzbildung der Elektronen zu skizzieren, da diese Experimente nicht so leicht greifbar sind.
Man sollte diesen Moment allerdings nutzen um den SchülerInnen klar zu machen, dass zu Beginn niemand seine wirkliche Freude an diesen Resultaten hatte, da sie nicht mit der Alltagserfahrung übereinstimmen.
Bis zur quantenphysikalischen Betrachtung dieses Experiments gab es in der Physik zwei Ansätze, die wunderbar nebeneinander arbeiteten:

- Physik des Diskreten: Hierbei ist die Beschreibung von Massenpunkten gemeint, die beispielsweise sehr erfolgreich im Rahmen der Mechanik eingesetzt wird.
- Physik des Kontinuierlichen: Dies beinhaltet den Feldbegriff, der eine zentrale Rolle bei der Beschreibung von elektromagnetischen Phänomenen spielt.

Man ist also bereits mit dem Verhalten von Feldern und Wellen vertraut jedoch konnte man sich keinen Reim daraus machen, wie ein Elektron (also ein ganz "normales Teilchen") plötzlich Eigenschaften einer Welle zeigen sollte.
Dies löste eine große Diskussion unter den damaligen führenden Wissenschaftlern aus, die erst einige Jahre später durch ein wegweisendes Experiment einer neue Theorie beendet wurde (später mehr).

1.2.4 Die Wahrscheinlichkeitsinterpretation

Wir versuchen nun, die Brücke zwischen den Experimenten und der Quantentheorie zu bauen (nach [4]).
Aus der klassischen Theorie der Welle wissen wir:

$$\text{Intensität} \propto \text{Betragsquadrat der Amplitude}$$

In der vorangegangenen Stunde haben die SchülerInnen gelernt, dass Licht aus Energiepaketen, den so genannten Photonen, besteht. Wir können also schließen, dass hohe Intensität durch ein Auftreffen von vielen solchen Energiepaketen verursacht wird. Verteilen sich die Einschläge nun auf eine abgegrenzte Fläche, so kann sagen, dass dunkle Gebiete eine kleinere Wahrscheinlichkeit für ein Auftreffen haben als helle.
Wir folgern:

$$\text{Intensität} \propto \text{Wahrscheinlichkeit}$$

Setzen wir nun unsere beiden Überlegungen zusammen, erhalten wir:

Wahrscheinlichkeit $\propto$ Betragsquadrat der Amplitude

So abstrus es auch klingen mag: Wir beschreiben die Teilchen nun mit Hilfe von Wahrscheinlichkeitswellen (die also interferieren können) und berechnen die Auftrittswahrscheinlichkeit über das Betragsquadrat der Amplitude.
Die Quantentheorie liefert wunderbar einfache Rezepte zur Berechnung einer Vielzahl von Experimenten.

Es macht meiner Meinung nach nun wenig Sinn, tiefer in die Berechnungen dieser Wahrscheinlichkeitswellen einzugehen. Die mathematischen Fähigkeiten und vermutlich auch der Wille damit zu rechnen, sind kaum gegeben. Die SchülerInnen haben zu diesem Zeitpunkt zumindest einmal von diesen Wahrscheinlichkeitswellen gehört und das soll fürs Erste auch genügen.

1.2.5 Dr. Quantum die zweite

Der erste Videoteil mit Dr. Quantum hat ca. bei 3:30 gestoppt und wir sind nun bereits mit der Wahrscheinlichkeitsinterpretation vertraut. Dr. Quantum versucht nun eine Erklärung für das Verhalten des Elektrons zu geben, wenn es ganz alleine durch den Doppelspalt schießt (Abb 1.6). An dieser Stelle sollte man das Video anhalten und auf die Wahrscheinlichkeitswelle verweisen. Die Wahrscheinlichkeitswellen interferieren wie gewohnt, das Betragsquadrat liefert die Wahrscheinlichkeit für ein Auftreffen.

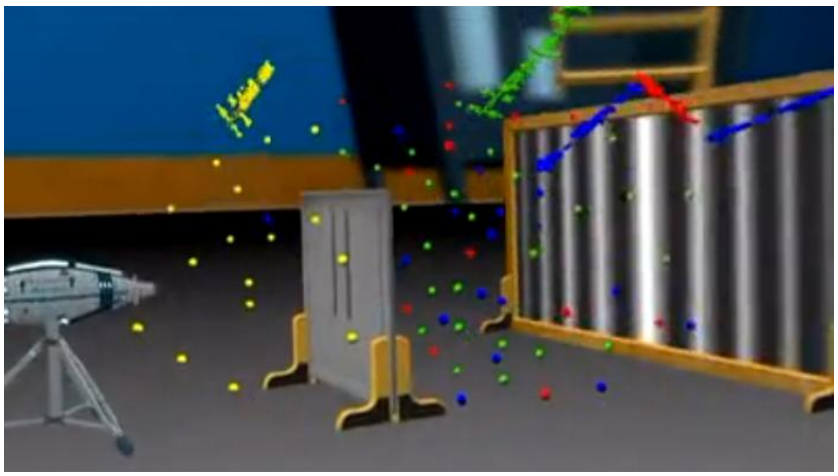


Abbildung 1.6: Dr. Quantum veranschaulicht Superposition

Nun stellt Dr. Quantum ein Messgerät an einem der Spalte auf. Dies zwingt das Elektron, sich für einen der beiden Wege zu entscheiden und beeinflusst

das System, sodass kein Interferenzmuster mehr entsteht. Dies nutzen wir um anzumerken, dass eine Messung direkten Einfluss auf das System hat (Abb. 1.7).

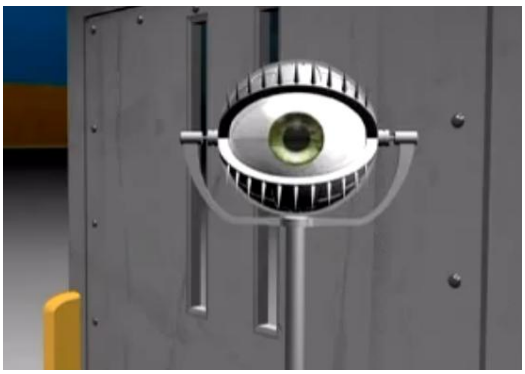


Abbildung 1.7: Ein Beobachter observiert einen Spalt

1.2.6 Schrödingers Katze

Mit ziemlicher Sicherheit hat man es nun geschafft, die SchülerInnen vollkommen zu verwirren. All die Informationen über Wahrscheinlichkeiten, Interferenzmuster, Zustände und Beobachter sind gewöhnungsbedürftig und brauchen Zeit um einzusickern.
Aus diesem Grund widmen wir uns nun der Thematik aus einer neuen Richtung und bemühen das von Erwin Schrödinger erdachte Gedankenexperiment.

Skizzieren wir die Situation: Wir haben eine Katze, die in einer zunächst offenen Kiste sitzt. Diese wurde mit einem Tötungsmechanismus versehen, der mit einer bestimmten Wahrscheinlichkeit ein Giftgas freisetzt.
Die Katze hat also bei geöffneter Kiste zwei mögliche "Zustände":

- Der Mechanismus ist noch nicht ausgelöst → die Katze lebt (Abb. 1.8)
- Der Mechanismus wurde ausgelöst → die Katze ist gestorben (Abb. 1.9)

In unserer makroskopischen Welt, in der die Quantenphysik nicht in den Vordergrund tritt, sind diese beiden Zustände absolut unterscheidbar.

Man stelle sich nun folgendes vor: Wir verschließen den Deckel unserer Kiste und da der Tötungsmechanismus nur mit einer gewissen Wahrscheinlichkeit

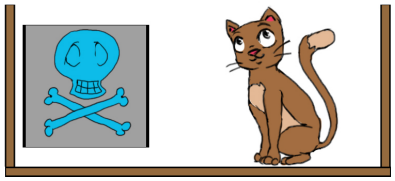


Abbildung 1.8: Die Katze lebt

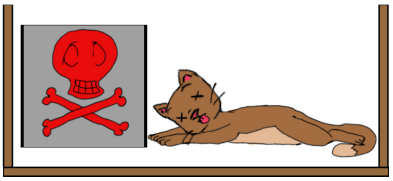


Abbildung 1.9: Die Katze ist tot

ausgelöst wird, können wir von außen nicht feststellen, ob die Katze nun tot oder noch lebendig ist. Erst durch das Öffnen und Hineinsehen (also Messen) wird die Katze tot oder lebendig.
Solange die Kiste geschlossen ist, wissen wir nicht, wie es der Katze gerade ergeht. Beide Möglichkeiten existieren parallel (Abb. 1.10).

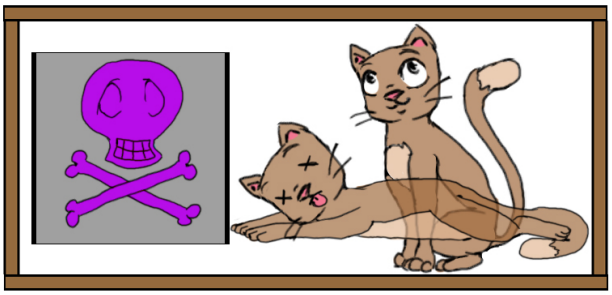


Abbildung 1.10: Katze ist tot UND lebendig

Solch überlagerte Zustände nennt man Superposition und findet man in der Quantenphysik ständig.
Wir sehen auch, dass eine Messung die Superposition zerstört, da sich die Katze nun in einem der beiden Zustände befinden muss. Erst durch die Messung wird einer der beiden Zustände realisiert, zuvor existieren beide parallel.

An dieser Stelle sollte man vielleicht noch darauf hinweisen, dass bis jetzt

noch keine Katze ihr Leben für dieses Experiment gelassen hat. Es handelt sich um ein Gedankenexperiment.

Ein anderes sehr bekanntes Anschauungsbild wurde 1940 von Charles Addams [7], seines Zeichens auch Schöpfer der Addams Family, gezeichnet. Es zeigt einen Schifahrer der gleichzeitig links und rechts an einem Baum vorbeifährt (Abb. 1.11).

Abbildung 1.11: Schifahrer fährt links und rechts

1.3 3. Einheit

In den ersten beiden Unterrichtsstunden wurden einige Experimente vorgestellt, die zur Entwicklung der Quantenphysik geführt haben. Außerdem wurden die SchülerInnen bereits mit dem Konzept der Wahrscheinlichkeitswellen vertraut gemacht. Die dritte Einheit erwähnt nun noch einige Begriffe und Aussagen, die man meiner Meinung nach, mit Abschluss einer allgemeinbildenden höheren Schule kennen sollte.
Nachdem zumindest eine kleine Grundlage der Quantenphysik gelegt wurde, brauchen wir noch eine kurze Zusammenfassung einiger Begriffe aus der Informatik, um uns dann wirklich auf den Quantencomputer stürzen zu können. Dieser EDV-Teil ist als optional anzusehen und richtet sich nach der betreffenden Klasse. Sehr oft sind diese Themen schon im Informatikunterricht

behandelt worden, bzw. muss davon ausgehen, dass die SchülerInnen sich auch privat schon einiges an Vorwissen angeeignet haben.

1.3.1 Stundenbild

Zeit	Inhalt
00 - 10	Organisatorisches
10 - 15	Der Laplacesche Dämon
15 - 20	Gott würfelt nicht
20 - 25	Was ist ein Computer?
25 - 35	Datenbanken
35 - 50	Algorithmen (Binary Search)

1.3.2 Der Laplacesche Dämon

Pierre-Simon (Marquis de) Laplace lebte von 1749 bis 1827 und war ein angesehener Wissenschaftler. Er verfasste viele bedeutende Werke, unter anderem wichtige Schriftstücke zur Wahrscheinlichkeitstheorie und zur Astrophysik. Der Laplacesche Dämon ist das Sinnbild einer deterministischen Physik. In einer deterministischen Physik ist jeder Vorgang die direkte Folge eines vergangenen Ausgangszustandes und gleichzeitig die Grundlage für die zukünftige Entwicklung.
Oft wird hier der Vergleich mit einem komplizierten Getriebe aus Zahnrädern bemüht. Kennt man die Lage aller Zahnräder und wie diese ineinander greifen, so läuft dieses Uhrwerk ohne der Möglichkeit einer Intervention von selbst ab.
Ein Laplacescher Dämon braucht also nur den Ort und den Bewegungszustand aller Teilchen (Zahnräder) zu kennen und könnte bis in alle Zukunft die Bewegungen vorausberechnen. Dies wirft natürlich gewisse philosophische Probleme auf, die mit dem freien Willen zu tun haben.

1.3.3 Gott würfelt nicht

Ein solcher Laplacescher Dämon wie im vorangegangen Kapitel ist natürlich reine Fiktion aber dennoch beinhaltet dieses Bild auch ein Quenchen Wahrheit. Bis zur Entwicklung der Quantenphysik spielte ein echter Zufall in der Physik keine Rolle. Probleme mit Vorhersagen gab es aufgrund ungenauer Bestimmung von Randbedingungen oder mathematischer Vereinfachungen.

Die Quantenphysik hingegen rechnet sehr erfolgreich mit Wahrscheinlichkeiten. Es ist nicht vorherzusagen welchen Weg ein Teilchen beim Doppelspalt

wählt oder wann die Katze vergiftet wird.

Diese Eigenschaft der Quantenphysik missfiel sogar einem ihrer Mitbegründer. Die Rede ist von Albert Einstein.
In einem legendärem Briefwechsel mit Max Born schrieb Einstein:
"Die Theorie liefert viel, aber dem Geheimnis des Alten bringt sie uns doch nicht näher. Jedenfalls bin ich überzeugt davon, dass der nicht würfelt." (nach [8])
Mit *"der Alte"* ist in diesem Fall Gott gemeint. Einstein wird der Auspruch: *"Gott würfelt nicht"* zugeschrieben.

Einstein und einige andere Wissenschaftler dieser Zeit konnten sich mit der stochastischen Beschreibung der Quantenphysik nicht anfreunden und vermuteten, dass es nur die Näherung einer anderen, fundamentaleren Theorie sein müsse.
Er forderte, dass auch die Quantentheorie eine lokal realistische Theorie sein müsse. In diesem Zusammenhang bedeutet:

lokal Die Messung eines Objekts darf keine augenblicklichen Auswirkungen auf ein anderes, räumlich entferntes, Objekt zeigen

realistisch Die Messung fördert eine bereits vorher vorhandene Eigenschaft zu Tage, auch wenn man diese wegen ungenügender Kenntnis von verborgenen Parametern nicht kennt

Es hat sich in bahnbrechenden Experimenten gezeigt, dass die Quantenmechanik keine lokal realistische Theorie ist.

Dieser, vielleicht auch etwas philosophische Streit, ging über mehrere Jahre, bis erstmalig ein Experiment eine solche Frage klären konnte.
Der Physiker John Stewart Bell fand eine Ungleichung, die von jeder lokal realistischen Theorie erfüllt werden musste. Er ersann ein Experiment, bei dem eine lokal realistische Theorie (so sie existieren sollte) und die Quantentheorie unterschiedliche Ergebnisse voraussagten und ließ die Natur (also das Experiment) als Schiedsrichter fungieren.
Das Ergebnis war eindeutig: Die Quantentheorie wurde bestätigt.
Weiters war nun fast[1] zweifelsfrei belegt, dass die quantenphysikalischen Phänomene nicht durch eine lokal realistische Theorie beschrieben werden können.

[1] Es gibt noch Schlupflöcher, die durch den experimentalen Aufbau entstehen

1.3.4 Was ist ein Computer?

Wir beenden nun vorerst den Ausflug in die Quantenphysik und versuchen uns Richtung Quantencomputer zu bewegen. Zunächst stellt sich natürlich die Frage: Was ist ein Computer überhaupt?

Bereits die ersten Kulturen der Menschheit mussten sich mit Zahlen beschäftigen. In direkter Folge entstanden damit natürlich auch die Grundrechenarten. Wie wir alle wissen, können auch diese bereits relativ schwierig im Kopf zu lösen sein, weshalb man auch schon seit frühester Menschheitsgeschichte nach technischen Hilfsmitteln gesucht hat. Die ersten Rechenbehelfe funktionierten durch Manipulation von Objekten (Abakus). Später wurden mechanische Rechenmaschinen basierend auf Zahnrädern und ähnlichem entwickelt. Die Entdeckung des Elektromagnetismus machte, mit Hilfe von Relais, die ersten Computer möglich, die auf elektrischen Schaltungen basierten. Diese füllten allerdings ganze Lagerhallen, waren sehr aufwändig zu betreiben und dies hinderte die Verbreitung .

Den großen Durchbruch gab es erst mit der Transistortechnologie. Heute meint man mit Computer fast ausschließlich einen auf Transistoren basierenden Mikrochip. Diese Chips führen Berechnungen mit unglaublicher Geschwindigkeit aus und ermöglichen erst das, was wir als Computer bezeichnen.

Das Wort Computer leitet sich aus dem englischen Verb *to compute* ab, dass vom lateinischen *computare* = zusammenrechnen abstammt.

Ein Computer besteht, ganz vereinfacht, aus einer Recheneinheit, einem Speicher und der Peripherie. Man bezeichnet all die Objekte, die man "angreifen" kann als Hardware Die Recheneinheit holt sich Daten aus dem Speicher und führt Befehle aus, die in der sogenannten Software niedergeschrieben sind. Diese Manipulation der Daten ist das eigentliche Rechnen des Computers.
Die Recheneinheit wird CPU für Central Processing Unit genannt.

1.3.5 Mooresches Gesetz

Die Transistortechnolgie hat in den letzten Jahren große Fortschritte in der Entwicklung erlebt. Die Technik ist mittlerweile in der Lage Transistoren im zweistelligen Nanometerbereich zu bauen und auf diesem Wege immer mehr Schaltkreise auf gleich bleibenden Raum unterzubringen, was im Endeffekt zu einer Leistungssteigerung führt.
Das Mooresche Gesetz wurde 1965 von Gordon Moore formuliert und besagt

im Wesentlichen, dass sich die Anzahl der Transistoren auf einem Chip jedes Jahr verdoppelt [9]. Moore vermutete, dass diese Annahme zumindest 10 Jahre, also bis 1975 halten müsste. Die Geschichte hat jedoch gezeigt, dass das Mooresche Gesetz weit über dieses Datum hinaus gültig sein würde, wobei die Verdopplungszeit immer wieder neu eingeschätzt wurde. Die Struktur einer exponentiellen Steigerung lässt sich allerdings nicht bestreiten (Abb. 1.12:

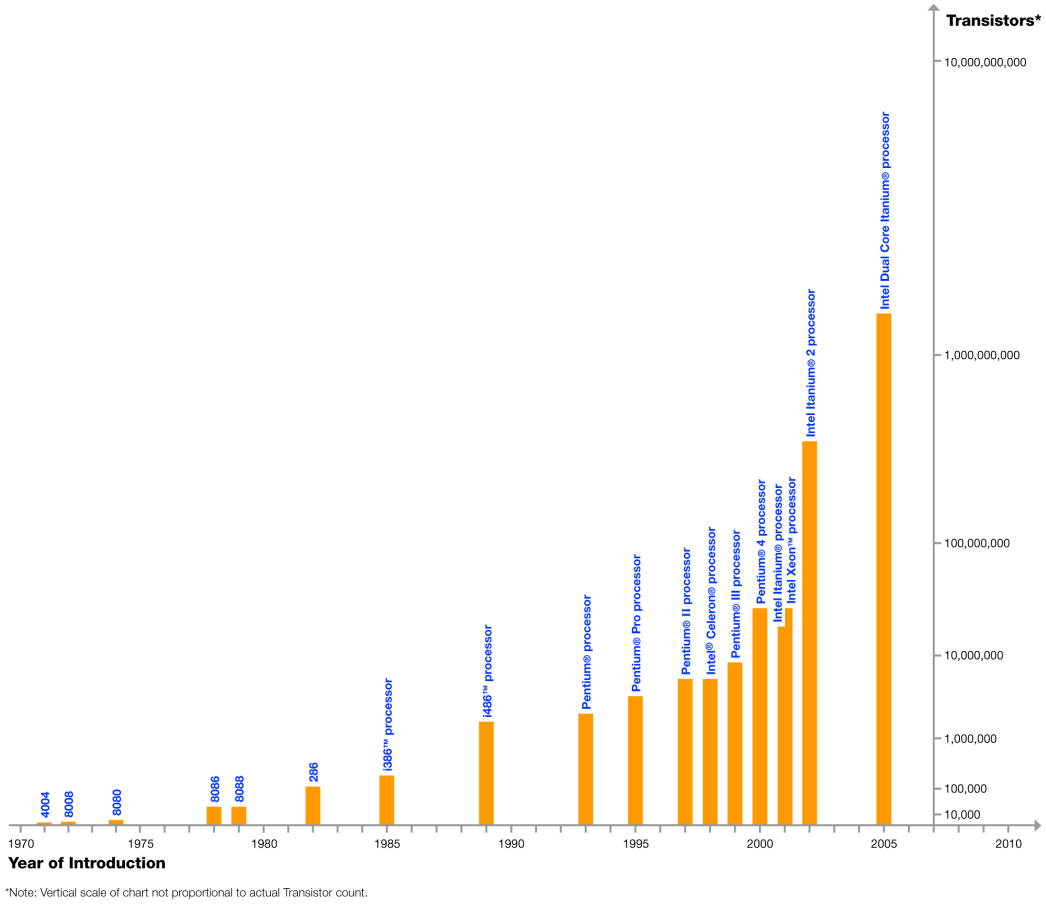


Abbildung 1.12: Entwicklung der Transistorendichte

Mittlerweile sind die Transistoren jedoch schon so klein geschrumpft, dass nicht mehr sehr viel Spielraum nach unten besteht. Aus diesem Grund sucht man nach Möglichkeiten, den immer größer werdenden Bedarf an Rechenleistung durch andere Technologien zu befriedigen.
Ein Ansatz der derzeit sehr stark verfolgt wird, ist das verteilte Rechnen, auch GRID-Computing genannt. Dabei werden viele schwächere Prozessoren verwendet um trotzdem eine sehr hohe Rechenleistung zu erzielen. Besonders

in großen Rechenzentren, wie beispielsweise im CERN, setzt man auf diese Technologie.

Die Quantenphysik stellt mir ihrer mathematischen Struktur und ihren Eigenheiten einen interessanten Rahmen für die Entwicklung neuartiger Rechenmaschinen bereit. Es gibt mittlerweile sogar schon einige Anwendungsfälle, bei denen ein auf der Quantenphysik basierender Computer, also ein Quantencomputer, einem herkömmlichen auf Transistoren basierenden Computer überlegen ist (später mehr).

1.3.6 Datenbanken

Eine der großen Stärken von EDV-Systemen ist die effiziente Speicherung, Verwaltung und Bearbeitungsvielfalt von großen Datenmengen. Diese Daten werden in speziellen Systemen, den sogennanten Datenbanken abgelegt.

Als Beispiel für eine einfache Datenbank kann man die Kontaktliste im Handy ansehen.
Hier gibt es für jeden Namen genau eine Telefonnummer und für jede Telefonnummer genau einen passenden Namen. [2]

Name	Telefonnumer
Alex	68437
Berta	35168
Claudia	46843
Dominik	23791
Eva	75135

Diese Art von Datenbank wird in der EDV als sortierte Liste bezeichnet.
Unsere Liste ist nach dem Namen sortiert, die Telefonnummern haben einsichtigerweise keine Strukturierung.

Ein großes Anliegen der Programmierer ist es, die Anzahl der Zugriffe auf die Datenbank möglichst gering zu halten.
Als Zugriff können wir uns beispielsweise das Auslesen von Namen und Telefonnummer der zweiten Position innerhalb der Liste vorstellen. Diese Anfragen an die Datenbank sind in der Regel sehr zeitintensiv, da große Speicherkapazitäten (wie sie für große Datenbanken benötigt werden) meist durch

[2] Den Fall zweier identischer Namen im Telefonbuch lassen wir hier geschickt unter den Tisch fallen

längere Zugriffszeiten erkauft werden müssen. [3]
Dass die Suche nach dem passenden Namen Zeit in Anspruch nimmt, kann man bei vielen Mobiltelefonen beobachten. Das Telefon bekommt die Nummer des Anrufers mitgeschickt und zeigt diese auch sofort an, das Auffinden des zugehörigen Namens dauert allerdings und deshalb scheint der Kontaktname erst später auf.

1.3.7 Algorithmen

Im vorangegangen Kapitel sind wir mit dem Begriff der Datenbank vertraut gemacht worden und wissen, dass Zugriffe auf die Datenbank zeitintensiv sind.

Eine der wichtigsten Aufgaben von Programmieren ist es nun, möglichst gute und schnelle "Strategien" zu entwickeln, um die Daten zu bearbeiten, bzw. auszulesen.

Diese "Strategien" werden in der Informatik als Algorithmus bezeichnet. [4]

In weiterer Folge werden wir uns einen speziellen Algorithmus herausgreifen und diesen näher erläutern: den sogenannten Binary Search.
Dieser Algorithmus wird für die Suche in sortierten Listen verwendet und wir werden dies exemplarisch in unserer Beispieldatenbank durchführen. Wir wollen nun die Telefonnummer von Dominik mit möglichst wenig Zugriffen erhalten.

Zu Beginn belegen wir zwei Variablen [5]:

plow Obere Suchgrenze: Im ersten Durchlauf mit Nummer des ersten Eintrags

phigh Untere Suchgrenze: Im ersten Durchlauf mit Nummer des letzten Eintrags

[3] Aus diesem Grund sind in allen Computern die sogennanten Arbeitsspeicher verbaut. Ein Speicher mit wesentlich kleinerem Fassungsvermögen als die Festplatte, jedoch mit einer um ein Vielfaches schnelleren Zugriffszeit

[4] Genauer: Ein Algorithmus ist eine aus endlich vielen, eindeutigen Schritten bestehende Handlungsvorschrift zum Lösen eines Problems.

[5] Die Variablennamen können natürlich frei gewählt werden

	Name	Telefonnumer
plow →	Alex	68437
	Berta	35168
	Claudia	46843
	Dominik	23791
phigh →	Eva	75135

In unserem Beispiel steht nun in plow der Wert 1 und in phigh der Wert 5.

Von den beiden Variablen plow und phigh bilden wir nun den arithmetischen Mittelwert pmid.

	Name	Telefonnumer
plow →	Alex	68437
	Berta	35168
pmid →	**Claudia**	**46843**
	Dominik	23791
phigh →	Eva	75135

Hier findet der erste Datenbankzugriff statt. Wir fragen die Datenbank, was sich hinter der noch anonymen Nummer 3 verbirgt. Als Antwort bekommen wir Claudia und ihre Telefonnummer.
Wir befinden uns aber auf der Suche nach Dominiks Telefonnummer. Wir wissen, dass Claudia (alphabetisch gesehen) kleiner als Dominik ist, und es sich um eine sortierte Liste handelt. Aus diesem Grund scheiden alle Einträge zwischen plow und pmid aus.
Wir setzen nun die untere Suchgrenze (plow) auf das gerade untersuchte Element (pmid) und beginnen wieder zwischen plow und phigh zu suchen.

	Name	Telefonnumer
	Alex	68437
	Berta	35168
plow →	Claudia	46843
pmid →	**Dominik**	**23791**
phigh →	Eva	75135

Aus den neuen Werten von plow und phigh berechnen wir wieder das arithmetische Mittel und erhalten den Wert 4.

Eine Anfrage an die Datenbank mit dieser Nummer liefert uns die gewünschte Telefonnummer von Dominik und wir können unsere Suche beenden.

Dieses Beispiel soll zeigen, wie man durch Einsatz eines guten Algorithmus Zeit (Datenbankzugriffe) sparen kann. Wir haben für das Auffinden der Telefonnummer lediglich zwei Datenbankzugriffe benötigt.

Im Anhang der Diplomarbeit befindet sich eine größere Liste, mit der man diesen Algorithmus vor der Klasse durchspielen kann. Am Besten kopiert man diesen auf eine Overheadfolie und verwendet einen Nicht-Permanent-Stift. So kann man nach jeden Schritt die alten Indizes (Pfeile) weglöschen und die Folie bleibt übersichtlich gestaltet.

1.4 4. Einheit

Jetzt ist es endlich geschafft und wir können uns auf die Quantenalgorithmen stürzen. Dieser Teil ist bewusst ohne Mathematik gehalten, da man damit die SchülerInnen schneller vergrault als man sich vorstellen kann. Es soll gezeigt werden, wie ein Quantenalgorithmus arbeitet und auf welche Dinge man bei Quantencomputern achten muss (nach [1] und [2])

1.4.1 Stundenbild

Zeit	Inhalt
00 - 10	Organisatorisches
10 - 20	Einleitung
20 - 35	Amplitudenverstärkung
35 - 50	Probleme mit dem Quantencomputer

1.4.2 Einleitung

Der erste Algorithmus mit dem wir uns beschäftigen werden, wurde im Jahre 1996 von Lov Grover entwickelt. Dieser Algorithmus bearbeitet eine sehr weit verbreitete Problemstellung der Informatik: dem Suchen in unsortierten Listen.

Wir nehmen jetzt wieder Bezug auf das Datenbankbeispiel der vorigen Unterrichtseinheit

Name	Telefonnumer
Alex	68437
Berta	35168
Claudia	46843
Dominik	23791
Eva	75135

Wir sind bereits mit einem sehr guten Algorithmus zum Auffinden eines bestimmten Namens vertraut. Ganz anders sieht der Fall jedoch aus, wenn wir uns auf die Suche nach einer bestimmten Telefonnummer begeben.

Ein konkretes Beispiel aus dem Umfeld der SchülerInnen: Die Freundin durchsucht das Handy ihres Freundes und entdeckt eine Rufnummer zu der kein Name vorhanden ist. Sie will nun wissen, ob sie die Nummer in ihrem eigenen Handy gespeichert hat.
Es bleibt ihr nichts anderes übrig, als jeden Eintrag der Reihe nach zu durchsuchen. Im schlimmsten Fall müsste sie dazu die gesamte Liste durchsehen, was natürlich bei vielen Kontakten sehr lange dauern kann.

Ganz allgemein kann man sagen, dass der Rechenaufwand für dieses Problem linear mit der Größe der Datenbank ansteigt.
Genau mit dieser Thematik beschäftigt sich der Suchalgorithmus von Grover.

1.4.3 Die Amplitudenverstärkung

Der wesentliche Geschwindigkeitsvorteil des Grover Algorithmus ergibt sich durch die Technik der Amplitudenverstärkung.

Zu Beginn wird eine Superposition über alle "Telefonnummern" erzeugt (Abb. 1.13). Diese Telefonnummern bilden, in unserem Verständnis, auf Quantenzustände ("Katzen") ab, die gemessen oder durch Quantenoperatoren geschickt werden könnnen.

Würde man nun eine Messung am Gesamtsystem durchführen, so erhält man, mit jeweils gleicher Wahrscheinlichkeit, eine der Telefonnummern.
Für eine erneute Messung müsste man das System wieder vollkommen neu präparieren, da jeder Messvorgang das Quantensystem beeinflusst und die für uns wesentliche Information zerstört wird.

Diese Superposition lässt man nun aber durch einen Quantenoperator laufen, der die Amplitude unserer gesuchten Telefonnummer mit einem negativen Vorzeichen versieht, die anderen Amplituden jedoch unverändert lässt.

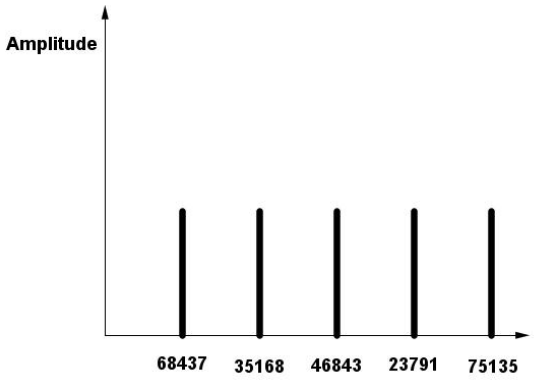


Abbildung 1.13: Superposition über alle Telefonnummern

Dieser Vorgang entspricht der Anfrage an die Datenbank. Durch den Quantenparallelismus ist es nicht relevant, wie viele Telefonnummern in dieser Superposition enthalten sind (Abb 1.14).

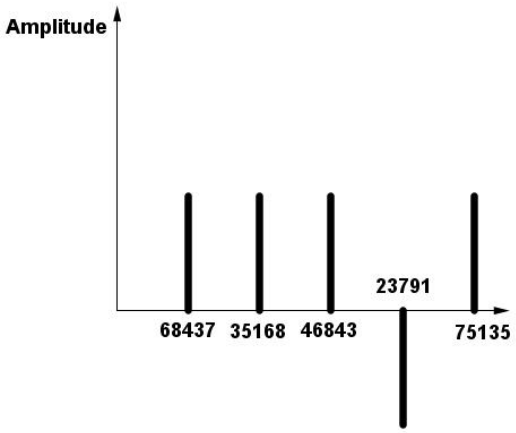


Abbildung 1.14: Gesuchte Amplitude wird gekippt

Diese Aktion hat bis jetzt nur bedingt Erfolg gebracht. Würde man nun eine Messung am System durchführen, so erhält man wieder zufällig und mit jeweils gleicher Wahrscheinlichkeit eine der Telefonnummern.
Wir erinnern uns: Die Wahrscheinlichkeit einen bestimmten Eintrag zu messen, entspricht dem Quadrat der Amplitude. In diesem Fall wird das negative Vorzeichen einfach wegquadriert und wir erhalten gleiche Wahrscheinlichkeiten für alle Einträge.

Jetzt zeigt sich der Grund für den letzten Schritt: Es gibt nämlich einen

Quantenoperator, der die einzelnen Amplituden um den Mittelwert aller Amplituden spiegelt (Abb. 1.15).
Man erkennt schnell: Der Mittelwert muss, wegen des einen negativen Eintrags, ein wenig unter den "falschen"Telefonnummern liegen.

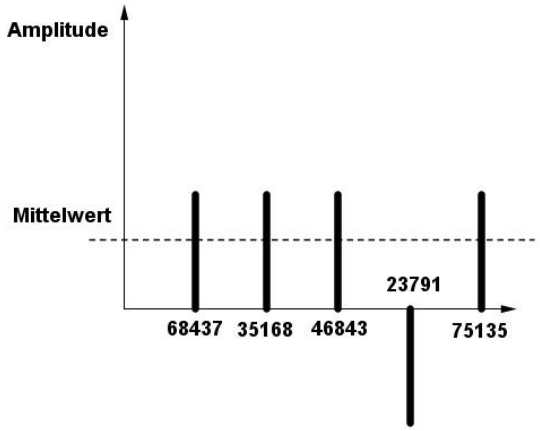


Abbildung 1.15: Spiegelung um den Mittelwert

Die Spiegelung um diesen gesenkten Mittelwert bringt folgendes Bild (Abb. 1.16):

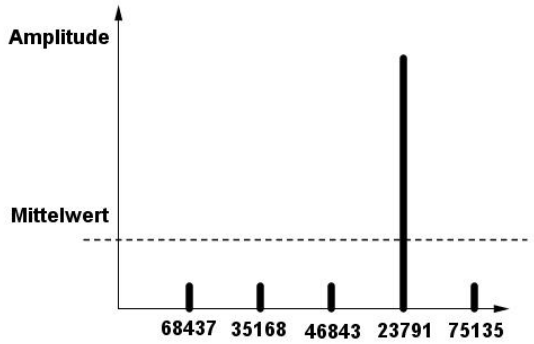


Abbildung 1.16: Ergebnis der Amplitudenverstärkung

Nun haben wir bei einer Messung des Systems, eine sehr große Wahrscheinlichkeit die richtige Nummer zu erwischen. Auch wenn wir mit einer gewissen Wahrscheinlichkeit eine "falsche"Telefonnummer erhalten, so war trotzdem nur eine einzige Anfrage an die Datenbank notwendig.
In diesem kleinen Beispiel genügt bereits ein Durchgang dieser Grover-Iteration um die Amplitude des Resultats genügend zu verstärken. Bei größeren Daten-

mengen kann man diesen Vorgang einige Male wiederholen, um mit genügend großer Wahrscheinlichkeit das richtige Ergebnis zu messen.
Man kann dieses Spielchen jedoch nicht beliebig oft wiederholen, da ab einer gewissen Anzahl an Durchläufen die Amplitude wieder zu sinken beginnen kann.

1.4.4 Probleme mit dem Quantencomputer

Der soeben vorgestellte Algorithmus birgt neben einem großen Geschwindigkeitsvorteil eine ganze Reihe an technischen Problemen. Im mathematischen Modell funktioniert der beschriebene Vorgang sehr gut, die Umsetzung in eine tatsächliche physikalische Rechenmaschine bereitet jedoch viele Schwierigkeiten.

Eine grundlegende Eigenschaft von physikalisch realisierten Rechenmaschinen ist, dass die Operationen auf die Daten nicht immer das "richtige" Ergebnis liefert. Man muss deshalb, wie auch bei auf Transistoren basierenden Computern, versuchen, Fehler so gut als möglich zu vermeiden und bereits eingetretene Fehler zu erkennen und zu korrigieren.

Bei klassischen Computern wird daher ein digitales Signal, das nur 0 und 1 kennt verwendet. Das Bit 0 steht hierbei für eine "kleine" Spannung und die 1 für eine "große" Spannung. Daher kann sich der tatsächliche Wert der Spannung innerhalb eines bestimmten Bereichs bewegen, ohne gleich einen Fehler zu produzieren. Dies ist also eine Fehler-Vermeidungs-Strategie.

Eine Möglichkeit bereits eingetretene Fehler zu erkennen, besteht darin, zusätzliche Bits mitzuschicken, die sich aus den übermittelten Daten berechnen lassen.

Ein einfaches Beispiel: Die zu übertragende, sieben Bit lange Nachricht ist 0101100. Nun zählen wir die Anzahl der Vorkommenden Einsen. Bei einer geraden Anzahl hängen wir als Kontrollbit eine 0, bei ungerader Anzahl von Einsen eine 1 an.

0101100	ungerade Anzahl an Einsen	$\rightarrow$	01011001
0101101	gerade Anzahl an Einsen	$\rightarrow$	01011010

Der Empfänger der Nachricht überprüft bei Erhalt, ob das Kontrollbit zu den übertragenen Daten passt. Ist ein Übertragungsfehler passiert und ein Bit beispielsweise von 0 auf 1 gesprungen, so ändert sich klarerweise auch die Anzahl der Einsen und somit das Kontrollbit. Man hat damit einen Fehler

erkannt, kann allerdings nicht rekonstruieren, an welcher Stelle dieser Fehler aufgetreten ist. Als Fehlerkorrektur könnte man die Nachricht erneut anfordern und hoffen, dass sie unbeschadet ankommt. Diese Technik wird in der jetzigen Informatik häufig angewandt.

Unglücklicherweise sind diese Kontrollmechanismen nicht auf den Quantencomputer übertragbar.
Ein großes Problem bei Quantencomputern ist die sogenannte Dekohärenz: Wir erinnern uns an Schrödingers Katze. Eine Superposition aus Tot und Lebendig, die durch Öffnen des Deckels zur Realität wird. Genau dieser Deckel bereitet bei der Konstruktion eines realen Quantencomputers große Schwierigkeiten. Wir wissen, dass eine Messung die Superposition im Inneren zerstört. Der Deckel soll nun das System vor Messungen schützen, was jedoch nicht so einfach in die Praxis umzusetzen ist, da dieser fast immer mit einer nicht verschwindenden Wahrscheinlichkeit ein bisschen oder ganz geöffnet wird.

Auch die Operatoren die auf die Quantenbits angewendet werden sind nur sehr schwer zu realisieren. Ein realer Quantenoperator unterscheidet sich von einem modellierten Operator, wie ihn die Theorie verwendet. Es treten zusätzliche physikalische Wechselwirkungen auf, die man im Algorithmus nicht miteinbezogen hat.

Wir stellen fest: Es hat sich bis jetzt noch keine ultimative Lösung für all diese Probleme gefunden und es ist nach wie vor ein spannendes Gebiet auf dem die Forschung arbeiten kann.

1.5 5. Einheit

In der vorangegangenen Einheit wurde über die Probleme bei der Realisierung eines Quantencomputers gesprochen. In dieser Stunde soll noch ein großer Motivator für die Entwicklung eines Quantencomputers vorgestellt werden. Es dreht sich zusammenfassend um Shor´s Algorithmus der in der Lage ist, eine Zahl effizient in seine Primfaktoren zu zerlegen. Warum dies wichtig ist, möchte ich zu Beginn der Stunde vorstellen

1.5.1 Stundenbild

Zeit	Inhalt
00 - 10	Organisatorisches
10 - 15	Die RSA-Verschlüsselung
15 - 20	Shors Algorithmus
20 - 30	Rückblick und Ausblick
30 - 50	Puffer

1.5.2 Die RSA - Verschlüsselung

Die sichere Kommunikation war der Menschheit ebenfalls seit Beginn ihrer Geschichte eine wichtige Angelegenheit. Mittlerweile gibt es unzählige Verfahren zur Verschlüsselung von Nachrichten, die jedoch alle ein gemeinsames Problem haben:
Wie bei einem Türschloss braucht man um diese verschlüsselten Nachrichten zu öffnen einen Schlüssel. Die große Gefahr bei der sicheren Datenübertragung besteht im sicheren Transport des Schlüssels. Man muss bei einem Transport des Schlüssels über das Internet davon ausgehen, dass unbeteiligte Personen "mitlauschen".

Ein Team aus drei Mathematikern entwickelte 1977 ein Verfahren, bei dem die gesamte Kommunikation zwischen Sender und Empfänger belauscht werden kann, ohne der Möglichkeit die Nachricht in absehbarer Zeit zu entschlüsseln. Es handelt sich um ein sogenanntes asymmetrisches Verschlüsselungsverfahren. Es wurde 1983 zum Patent angemeldet und nach den Anfangsbuchstaben der drei Entwickler benannt: RSA (Roland L. Rivest, Adi Shamir und Leonard Adleman)[10].

Das Verfahren basiert auf einer sogenannten Einwegfunktion. Dies bezeichnet eine Funktion, die sehr leicht in die eine aber sehr schwer in die andere Richtung durchzuführen ist. In diesem konkreten Fall geht es um die Multiplikation zweier großer Primzahlen, die sehr einfach auszuführen ist. Für die Faktorisierung einer großen Zahl in ihre Primfaktoren wird jedoch sehr viel Zeit benötigt, weil kein einfaches Verfahren, wie für die Multiplikation, bekannt ist.

Das RSA-Verfahren berechnet aus einem Produkt zweier Primzahlen zwei neue Zahlen, wobei eine zum Ver- und die andere zum Entschlüsseln der Nachricht dient. Das Produkt aus den Primzahlen und eine der daraus berechneten Zahlen, bilden gemeinsam den sogenannten Public Key und werden an die Öffentlichkeit ausgegeben. Nun kann jeder eine Nachricht verschlüsseln

aber nur der Besitzer der zweiten Zahl (Private Key) ist in der Lage, diese wieder zu entschlüsseln. Der Private Key verbleibt während der gesamten Verschlüsselung lokal am eigenen Rechner und somit wird ein Lauschangriff über das Internet ausgeschlossen.

1.5.3 Shors Algorithmus

Um die Wirkung von RSA zu verdeutlichen bekommen die SchülerInnen folgende Aufgabe gestellt: Sie sollen die Zahl 1073 in ein Produkt zweier Zahlen zerlegen. Sie werden dies mit sehr großer Wahrscheinlichkeit nicht bewerkstelligen. Nach kurzer Zeit löst man das Rätsel auf und präsentiert die beiden Zahlen 29 und 37. Einige SchülerInnen werden nun den Taschenrechner zu Hilfe nehmen und das Ergebnis überprüfen.
Die SchülerInnen sollen erkennen: Ich könnte die beiden Primzahlen zwar bestimmen, jedoch würde dieser Versuch sehr viel Zeit in Anspruch nehmen.

Genau auf diesem Prinzip basiert die RSA-Verschlüsselung. Es ist zwar prinzipiell möglich, die beiden Faktoren zu finden, jedoch würde dies so viel Zeit in Anspruch nehmen, dass die Information in der Zwischenzeit wertlos geworden wäre.

An dieser Stelle kommt Shors Algorithmus ins Spiel. Der Ablauf selbst ist meiner Meinung nach für die Schule zu kompliziert, da sehr viele Ergebnisse aus der Algebra benötigt werden, die einfach nicht zur Verfügung stehen.
Die SchülerInnen sollen allerdings darauf hingewiesen werden, dass ein Quantencomputer zumindest theoretisch in der Lage ist, das Problem der Primfaktorenzerlegung in absehbarer Zeit zu lösen, was die RSA-Verschlüsselung wertlos machen würde.

1.5.4 Rückblick und Ausblick

Wir haben nun die beiden bekanntesten Algorithmen und Anwendungsgebiete des Quantencomputers besprochen. Wir stellen fest, dass der Quantencomputer, zumindest bis jetzt, kein Allheilmittel in der Computertechnologie ist.

Die vorgestellten Algorithmen wurden allerdings mit sehr kleinen Eingaben und unter Laborbedingungen bereits erfolgreich getestet.
So hat man 2001 die Zahl 15 in ihre Primfaktoren zerlegt. Die Zerlegung in 3 und 5 war zwar bereits im Vorhinein bekannt, es stellt jedoch trotzdem einen wichtigen Beweis für die prinzipielle Machbarkeit dar.

Weltweit forschen viele Wissenschaftler an verschiedensten Ansätzen, einen brauchbaren Quantencomputer zu erschaffen. Es gibt einige vielversprechende Ansätze und man liest immer wieder von Erfolgsmeldungen.
Wir müssen uns allerdings darüber im Klaren sein, dass die Theorie beim Quantencomputer wesentlich weiter fortgeschritten ist, als die Hardware. Die Vorteile eines Quantencomputers werden erst schlagend, wenn ein nicht störanfälliger Rechner für große Eingaben zur Verfügung steht.
Quantencomputer werden für ganz spezielle Aufgaben entwickelt werden und parallel zu den uns bekannten Computern existieren. Für Anwendungen, an die wir uns bis jetzt schon sehr gewöhnt haben, wie Bürosoftware, Computerspiele,... werden auch in Zukunft klassische Computer die Arbeit erledigen. Erst wenn eine spezielle Anforderung auftaucht, die von einem Quantencomputer besser erledigt werden kann, wird dieser auch eingesetzt werden.

Eine Anwendung der Quantenphysik, die wahrscheinlich sehr bald große Verbreitung finden wird, ist die Quantenkryptographie. Wie man dieses Thema in der Schule behandeln kann bearbeitet die Diplomarbeit von Heidemarie Knobloch "Quantenkryptographie in der Schule" [11].

Kapitel 2

Theorie

Dieser Abschnitt der Diplomarbeit ist für Lehrkräfte geplant, die sich etwas näher mit der Theorie der Quantencomputer auseinander setzen möchten. Der Einsatz im Unterricht ist allerdings nur bedingt sinnvoll, da die SchülerInnen nicht über das notwendige formale Hintergrundwissen verfügen, das für die Quantenphysik erforderlich ist.

2.1 Quantencomputer am Beispiel Grover Algorithmus

Dieses Kapitel widmet sich im speziellen der quantentheoretischen Funktionsweise eines Quantencomputers. Der/Die Leser/in dieses Kapitels sollte bereits einigermaßen mit der Quantentheorie vertraut sein, da hier nur die für einen Quantencomputer notwendigen Aspekte ausgearbeitet sind (nach [1] und [2]).

Der Theorieteil liefert alle Bestandteile, um einen prominenten Vertreter der Quantenalgorithmen zu verstehen: Den Suchalgorithmus von Grover.

2.1.1 Rechenbasis und Operatoren

Das Modell des Quantencomputers basiert auf zweidimensionalen Vektoren im Hilbertraum, den sogenannten Quantenbits.
Ein Quantenbit ϕ wird durch folgende Superposition beschrieben:

$$|\phi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \tag{2.1}$$

Wobei α_0 und α_1, die sogenannten Amplituden, komplexe Zahlen mit

$$|\alpha_0|^2 + |\alpha_1|^2 = 1 \tag{2.2}$$

sind.

Hier zeigt sich bereits ein großer Unterschied zu einem klassischen Rechner. Ein gewöhnliches Bit ist entweder 1 oder 0. Bei einem Quantenbit sind theoretisch unendlich viele Zwischenzustände über den orthogonalen Basisvektoren $|0\rangle$ und $|1\rangle$ möglich (Abb. 2.1).

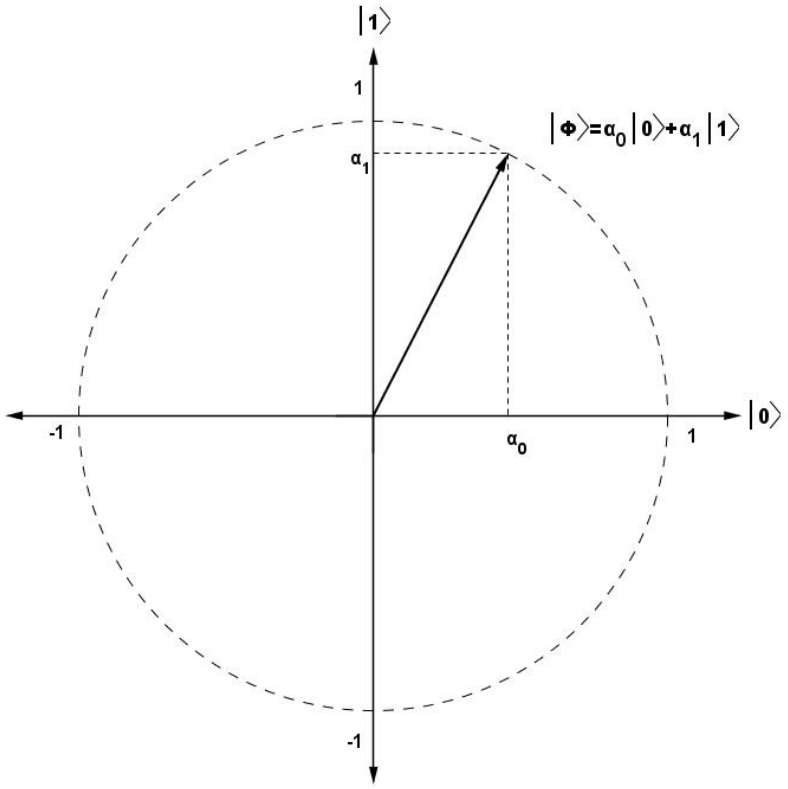


Abbildung 2.1: Graphische Veranschaulichung eines Quantenbits

Ein Quantencomputer mit nur einem einzigen Quantenbit wäre natürlich etwas witzlos. Man fasst daher eine Menge von n Quantenbits zu einem sogenannten Quantenregister zusammen. Es hat sich als weiteres Axiom der Quantenphysik gezeigt, dass die Verknüpfung von Quantensystemen mittels des Tensorprodukts ($\otimes$) beschrieben werden muss.

Ich erläutere dies nun für zwei Quantenbits A und B:

$$A \otimes B = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$$

Verwendet man beispielsweise nun die beiden Quantenbits $|1\rangle$ und $|0\rangle$, so schreibt man das Tensorprodukt: $|1\rangle \otimes |0\rangle = |10\rangle$

In Vektorschreibweise betrachtet ergibt sich:

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Mit Hilfe des Tensorprodukts lassen sich in einem n großen Register 2^n ganze Zahlen darstellen. So können in einem Quantenregister bestehend aus nur 4 Bits bereits die Zahlen von 0 bis 15 abgebildet werden.

Ein weiterer Vorteil der Quantenbits besteht darin, dass man in einem einzelnen Quantenregister eine Superposition über mehrere Zustände gleichzeitig speichern und verarbeiten kann.
Man kann also in nur einem Register gleichzeitig die Zahlen 5 und 11 zu speichern.

$$|\phi\rangle = \frac{1}{\sqrt{2}}|0,1,0,1\rangle + \frac{1}{\sqrt{2}}|1,0,1,1\rangle$$

Der Einfachheit halber verwendet man, anstatt der Binärdarstellung in den n einzelnen Quantenbits, die wesentlich besser lesbare Dezimaldarstellung:

$$|\phi\rangle = \frac{1}{\sqrt{2}}|5\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Führt man nun an diesem Register eine Messung des Zustandes durch, so erhält man jeweils mit einer Wahrscheinlichkeit von $\frac{1}{2}$ die Zahl 5 oder die Zahl 11.
Eine solche Messung führt das Register allerdings wieder in einen neuen Zustand über, die alten Informationen gehen verloren.

Operatoren

Mittlerweile sind wir in der Lage Zahlenwerte zu speichern. Als nächsten Schritt muss noch geklärt werden, wie die Daten bearbeitet werden können.

Quantencomputer basieren auf unitären [1] Operatoren, von denen die meisten durch Matrizen dargestellt werden können. Eine wesentliche Eigenschaft dieser Matrizen besteht darin, dass sie eindeutig umkehrbar sind.

Dies stellt eine starke Einschränkung dar, da sehr viele Operationen nicht eindeutig umkehrbar sind.
Betrachtet man zum Beispiel die Modulo-Operation, so stellt man schnell fest:

$$5 \bmod 3 = 2$$

$$11 \bmod 3 = 2$$

Hat man nur das Ergebnis zur Verfügung, so ist nicht klar, ob die Rechnung mit 5, 11, 8 oder 1037 [2] durchgeführt wurde.

Aus diesem Grund führt ein Quantencomputer den Eingangszustand in einem zweiten, separaten Quantenregister mit.
Gerechnet wird also mit zwei Registern, einem Register $|x\rangle$ für das Argument mit der Länge n und einem Register $|y\rangle$ für das Ergebnis mit der Länge m.

Einsichtigerweise können in einem Register der Länge m nur $2^m - 1$ verschiedene Zahlen größer Null gespeichert werden. Sollte im Rahmen der Rechnung nun eine noch größere Zahl auftreten, so wird nach den Regeln der modularen Arithmetik mit den Resten (Modulo-Operation) weitergerechnet.

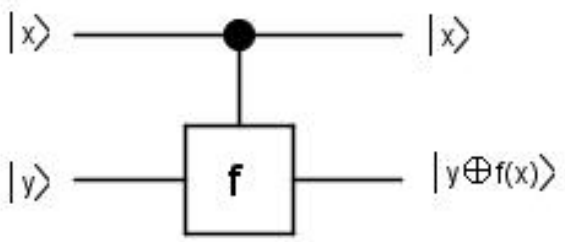


Abbildung 2.2: Schematische Darstellung einer Funktionsberechnung

[1] Eine Matrix A heißt genau dann unitär, wenn gilt: $A^{-1} = A^t$
[2] 1037 = 3 x 345 + 2 ⇒ 1037 mod 3 = 2

2.1.2 Die Superposition der Datenbank

Für den Grover-Algorithmus muss eine Superposition über die einzelnen Einträge in der Datenbank erstellt werden. Dazu verwendet man den sogenannten Hadamard-Operator.

Dargestellt wird diese unitäre Operation durch folgende Matrix H:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Wendet man diese Matrix auf den Zustand $|0\rangle$ eines Quantenbits an, so erhält man die gleichgewichtete Superposition $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ [3].

Damit eine Anwendung wie der Suchalgorithmus von Grover Sinn ergibt, will man selbstverständlich mehrere Quantenbits, also ein Quantenregister, verwenden.

Um dies zu bewerkstelligen bedarf es wieder eines kurzen Ausflugs in die Mathematik, um uns mit dem Tensorprodukt für Matrizen vertraut zu machen.

Das Tensorprodukt für zwei 2x2 Matrizen ist folgendermaßen definiert:

$$A \otimes B = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \otimes \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \begin{pmatrix} a_1 \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} & a_2 \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \\ a_3 \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} & b_4 \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \end{pmatrix} =$$

$$\begin{pmatrix} a_1b_1 & a_1b_2 & a_2b_1 & a_2b_2 \\ a_1b_3 & a_1b_4 & a_2b_3 & a_2b_4 \\ a_3b_1 & a_3b_2 & a_4b_1 & a_4b_2 \\ a_3b_3 & a_3b_4 & a_4b_3 & a_4b_4 \end{pmatrix}$$

Bildet man nun des Tensorprodukt aus zwei Hadamard-Operatoren, so erhält man:

$$H \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} H & H \\ H & -H \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

[3] $H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

Dieses Verfahren lässt sich auch auf n Hadamard-Operatoren erweitern und ergibt die Matrix H_n.
Wendet man nun die Matrix H_n auf ein n Bit großes Quantenregister an, so entspricht dies der Anwendung der Hadamardmatrix auf jedes einzelne Bit des Registers.
Für unsere Zwecke eignet sich: H_n mit $|0..0\rangle$. Dies ergibt eine gleichgewichtete Superposition über alle darstellbaren Zahlen von 0 bis $2^n - 1$.

Mit diesem Wissen könnnen wir nun einen geeigneten Anfangszustand $|\Omega\rangle$ für den Grover-Algorithmus präparieren, indem wir die Einträge durchnummerieren und die Hadamard-Matrix verwenden:

Index	Name	Telefonnumer
0	Alex	68437
1	Berta	35168
2	Claudia	46843
3	Dominik	23791
4	Eva	75135

$$|\Omega\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \frac{1}{\sqrt{5}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle)$$

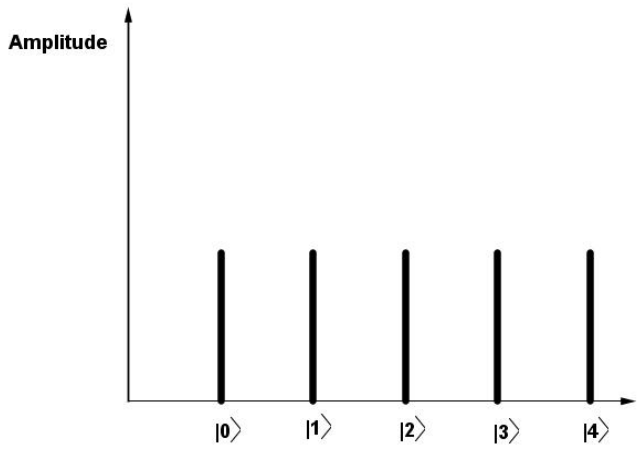


Abbildung 2.3: Superposition der Amplituden

2.1.3 Die Amplitudenverstärkung

Da wir nun einen geeigneten Zustand präpariert haben, muss als nächstes die Amplitude mit der gesuchten Nummer verstärkt werden.

Als Abfrage der Datenbank können wir uns folgende Funktion f(x) vorstellen:

$$f(x) = \begin{cases} 1 & x = l \\ 0 & sonst \end{cases}$$

l steht hier für den Index mit der gesuchten Telefonnummer.
Auch dieses Mal ist wieder die Nummer 23791 gesucht, welche dem Index l=3 der Datenbank entspricht.

Die obige Funktion wird nun benutzt, um die Amplituden der Superposition zu bearbeiten. Wir wissen bereits, dass Funktionen auf unitären Operationen beruhen müssen und wir darum mit zwei Registern rechnen. Im ersten Register steht $|\Omega\rangle$, im zweiten verwenden wir ein Quantenbit mit der Superposition $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Nun betrachten wir, welche Wirkung die Funktion f(x) auf einen (einzelnen) Zustand x hat:

$$|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{f} |x\rangle \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle) = |x\rangle (-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Wir erkennen:

- Der Zustand des zweiten Registers läuft unverändert aus der Operation
- Liefert f(x) den Wert 1, so wird das Vorzeichen von $|x\rangle$ geändert

Diese Operation wird in der Literatur auch als Kickback bezeichnet.

Verwenden wir den Kickback nun mit der Superposition $|\Omega\rangle$, so liefert dieser genau bei x=l=3 den Wert 1 und das Vorzeichen der Amplitude unserer gesuchten Telefonnummer wird gewechselt (Abb. 2.4).

Im letzten Schritt der Groveriteration wird eine Spiegelung vorgenommen. Die Operation $a \to -a$ bewirkt eine Spiegelung um die x-Achse.

Ein Operator U_s mit der Gestalt $U_s = 2|\Omega\rangle\langle\Omega| - \mathbb{1}$ sorgt nun für die gewünschte Spiegelung am Mittelwert der anderen Amplituden.
Die mehrmalige Anwendung der Kombination aus Kickbacks und U_s verstärkt schließlich die Amplitude so stark, dass eine Messung des Registers mit sehr hoher Wahrscheinlichkeit den richtigen Eintrag liefert (Abb. 2.5).

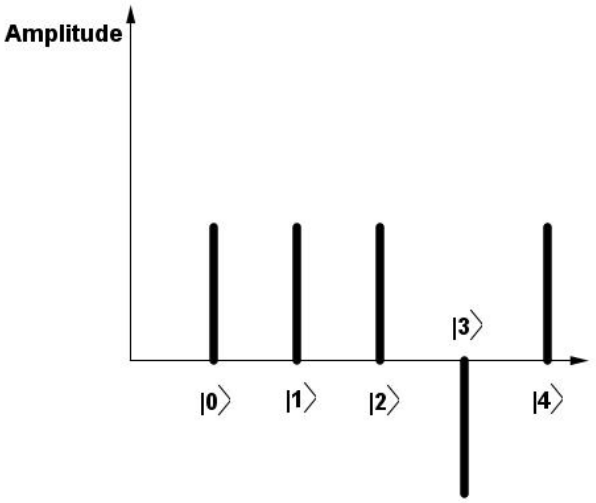


Abbildung 2.4: Gesuchte Amplitude erhält Vorzeichen-Flip

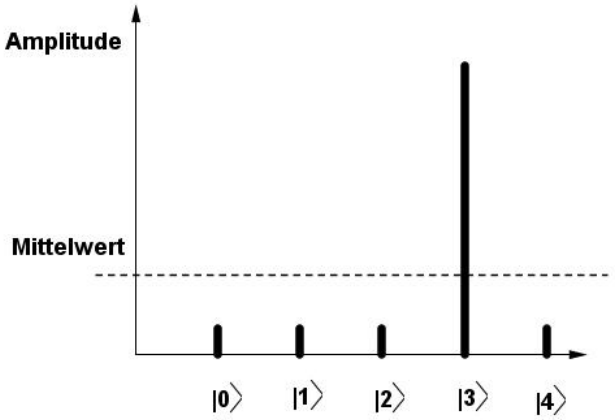


Abbildung 2.5: Ergebnis der Amplitudenverstärkung

Man muss allerdings darauf achten, diesen Vorgang nicht zu oft zu wiederholen, da man auch an dem gewünschten Zustand "vorbeischießen" kann und sich die Amplitude des gewünschten Zustands wieder zu senken beginnt. Die Verkettung der beiden Spiegelungen erzeugt hier eine Drehung des Zustandsvektors. Dieser nähert sich immer weiter dem Optimum an, dreht man allerdings weiter, so beginnt er sich wieder zu senken (Abb 2.6):

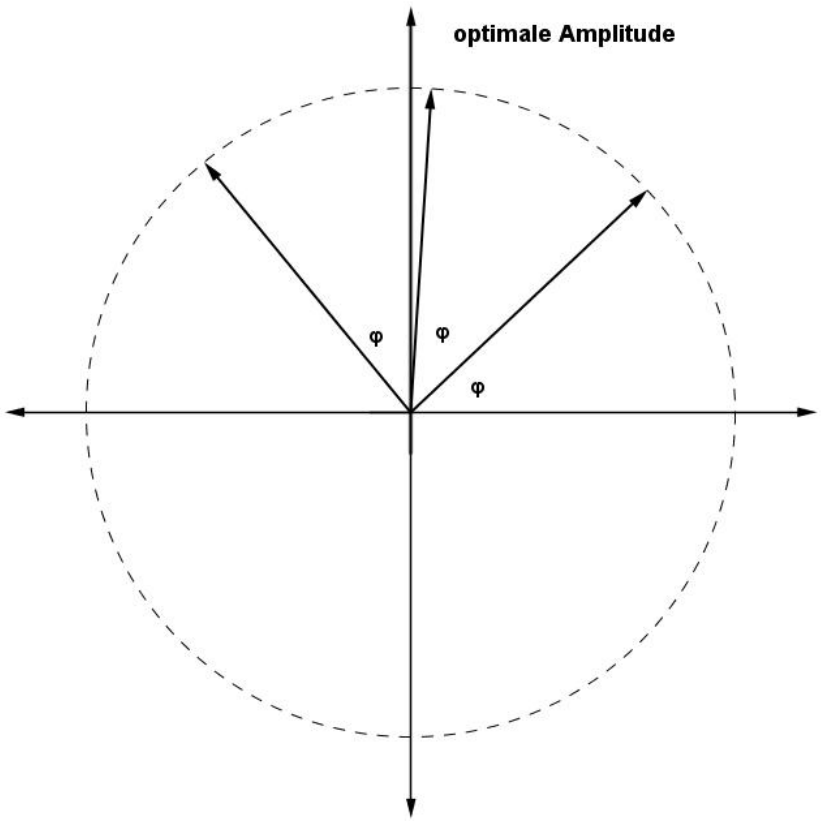


Abbildung 2.6: Rotation des Zustandsvektors

2.1.4 Abschließende Bemerkungen

Wir haben nun gesehen, wie der Suchalgorithmus von Grover in der Theorie funktioniert. Quantencomputer beruhen auf dem Konzept, die Wahrscheinlichkeit für die Messung des richtigen Eintrags zu erhöhen. Die Überprüfung ob ein Ergebnis stimmt oder nicht ist schnell durchzuführen. Hat man ein falsches Ergebnis erhalten, so wird der Algorithmus erneut durchgeführt und gehofft, den gesuchten Wert zu erhalten.
Dies ist ein weiterer Unterschied zu herkömmlichen Computern. Bei elektronischen Computern wird das Ergebnis berechnet und in der Regel erhält man auch das richtige. Ein Quantencomputer hingegen liefert das Ergebnis nur mit einer gewissen Wahrscheinlichkeit.
Bildet man den Erwartungswert, wie lange die Berechnung wahrscheinlich dauern wird, so liegen die Werte deutlich unterhalb der klassischen Computer.

2.2 Komplexitätstheorie am Beispiel Shors Algorithmus

Der Geschwindigkeitsvorteil von Shors Algorithmus zur Zerlegung von Primzahlen ist natürlich belegbar. Dazu müssen wir uns allerdings kurz mit den Grundlagen der Komplexitätstheorie beschäftigen (nach [1]).

2.2.1 Komplexitätsklassen

Viele Probleme der Informatik verhalten sich bezüglich ihres Laufzeitverhaltens ähnlich. Diese werden in so genannten Komplexitätsklassen zusammengefasst.

Die Komplexitätsklasse P

In die Komplexitätsklasse P fallen alle Probleme, bei denen die Eingabenlänge (n) und die Laufzeit in einem polynomialen Zusammenhang stehen.

Ein Beispiel für P wäre die Addition zweier Zahlen. Wir kennen einen einfachen Algorithmus für die Addition noch aus der Volksschule. Die einzelnen Ziffern werden unter Berücksichtigung des Übertrags von rechts nach links addiert. Für jede zusätzliche Ziffer (Eingabelänge) wird ein zusätzlicher Rechenschritt absolviert.
Wir sehen: die Laufzeit steigt linear mit der Eingabelänge (also polynomial)

Die Probleme der Komplexitätsklasse P lassen sich mit herkömmlichen Computern effizient lösen. Sobald man gezeigt hat, dass ein Problem innerhalb dieser Klasse liegt, findet sich meist auch ein Algorithmus mit kleinem Exponenten.

Die Komplexitätsklasse NP

Im Gegensatz zu P lassen sich Probleme der Klassen NP nicht in polynomialer Laufzeit lösen.
Ein Beispiel bei dem man vermutet dass es in NP liegt ist das *Problem des Handlungsreisenden*, besser bekannt in der englischen Übersetzung als *travelling salesman problem*, kurz TSP.

Die Aufgabenstellung des TSP sieht folgendermaßen aus:
Ein Handlungsreisender muss eine fixe Anzahl n an Kunden besuchen. Diese sind räumlich getrennt, die Abstände zwischen jeweils zwei Kunden sind bekannt. Gesucht ist nun die kürzeste Route, um alle Kunden zu besuchen.

Eine Möglichkeit dieses Problem anzugehen wäre, einfach alle möglichen Routen zu berechnen und anschließend die kürzeste auszuwählen. Nach kurzer stochastischer Überlegung stellt man fest, dass es für n Städte $\frac{(n-1)!}{2}$ verschiedene Reiserouten gibt. Eine kurze Zahlenspielerei

Anzahl Städte	mögliche Routen
10	1.814.400
11	19.958.400
15	65.000.000.000
20	1.200.000.000.000.000.000

Man erkennt, dass nur eine geringfügige Erhöhung der Kundenbesuche bereits eine Unzahl an neuen Möglichkeiten mit sich bringt (man erinnere sich an die Addition).

Diese Erkenntnis ist natürlich nicht der Weisheit letzter Schluss, da es für dieses Problem mittlerweile wesentlich effizientere Algorithmen gibt. Eines haben sie jedoch alle gemeinsam: Es wurde noch kein Algorithmus gefunden, der den optimalen Weg in polynomialer Laufzeit ermittelt.

$\mathbf{P \neq NP}$ oder $\mathbf{P = NP}$

Dies ist eines der großen (noch) ungelösten Probleme der Mathematik. Es geht darum ob es für Fragestellungen der Klasse NP, zumindest theoretisch, überhaupt einen Algorithmus geben kann, der das Problem in polynomialer Laufzeit löst.

2.2.2 Shors Algorithmus

Die RSA Verschlüsselung basiert, wie schon erwähnt, auf dem Produkt zweier großer Primzahlen. Wenn es gelingt, dieses Produkt wieder zu faktorisieren, so ist die Verschlüsselung geknackt.

Stellen wir nun einige kurze Überlegungen zum Rechenaufwand an.

Kennt man eine Zahl n so kommt jede Zahl zwischen 2 und $\sqrt{n}$ in Frage, ein echter Teiler von n zu sein. Die Zahl n wird durch eine gewisse Anzahl von Bits m, der Eingabelänge, dargestellt. Die Anzahl der Möglichkeiten berechnet sich aus der Eingabelänge m durch $\sqrt{2^m}$.

Wir erkennen in dieser Abhängigkeit eine Exponentialfunktion, die auf lange Sicht jede Polynomfunktion übertreffen wird. Dieser Zusammenhang ist zwar nicht ganz so extrem wie beim TSP (Faktorielle), jedoch zeigt sich auch hier,

dass wir uns nicht mehr in der leicht berechenbaren Komplexitätsklasse P befinden.

Der Faktorisierungsalgorithmus von Shor ist durch die Auslagerung eines zeitaufwändigen Rechenschritts in einen Quantencompter in der Lage, dieses Problem in polynomialer Laufzeit zu knacken (genaue Ableitung siehe [1]).

In absehbarer Zeit wird es allerdings noch keinen physikalisch realisierten Quantencomputer geben, der diesen Algorithmus für große Eingaben durchführen kann. Die RSA-Verschlüsselung wird also noch einige Zeit sicher bleiben.

Anhang A

Handouts

Quantenphysik: Die ersten Schritte

Schwarze Strahler: Bringt man ein Metallstück zum Glühen, so sendet dies elektromagnetische Strahlung aus, die wir auch als Licht wahrnehmen können (rot glühen,…)

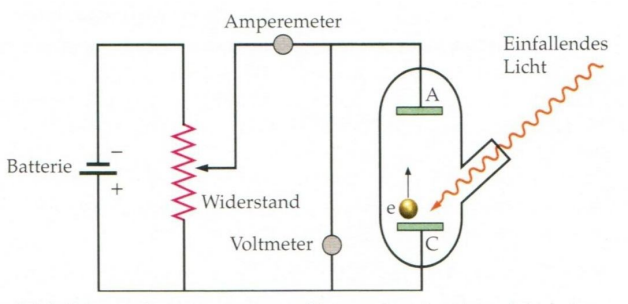
Die physikalischen Theorien vor 1900 waren nicht in der Lage, die experimentellen Tatsachen der schwarzen Strahler zufrieden stellend zu erklären.

Max Planck (1858 – 1974) fand eine Formel, die das Experiment hervorragend beschrieb. Diese Formel benötigte jedoch einen "mathematischen Kunstgriff", nämlich die Einführung einer zusätzlichen Konstante.

Max Planck entdeckte das nach ihm benannte **Plank´sche Wirkungsquantum h.**

Er stellte fest, dass ein Körper nur ganzzahlige Vielfache dieses Wirkungsquantums als Energie aufnehmen bzw. abgeben kann

Photoelektrischer Effekt



Metallplatte (C) wird mit Licht bestrahlt, es lösen sich Elektronen. Diese müssen gegen angelegte Spannung zum Detektor (A). Erhöht man die Spannung bis kein Strom mehr fließt, kennt man maximale Bewegungsenergie der herausgelösten Elektronen

Problem mit Theorie des Lichts als Welle:

Bei höherer Lichtintensität müssten die Elektronen eine größere Bewegungsenergie haben, das Experiment zeigt jedoch, dass dies nicht der Fall ist.

Lösung erfolgt durch Albert Einstein:

Das Licht besteht aus diskreten Energiepakten, den so genannten Lichtquanten oder Photonen. Diese geben ihre gesamte Energie an das Elektron ab und wenn diese einen gewissen materialabhängigen Wert übersteigt, so wird das Elektron aus der Platte gelöst. Den Rest erhält das Elektron in Form kinetischer Energie.

Quantenphysik: Welle, Teilchen oder beides?

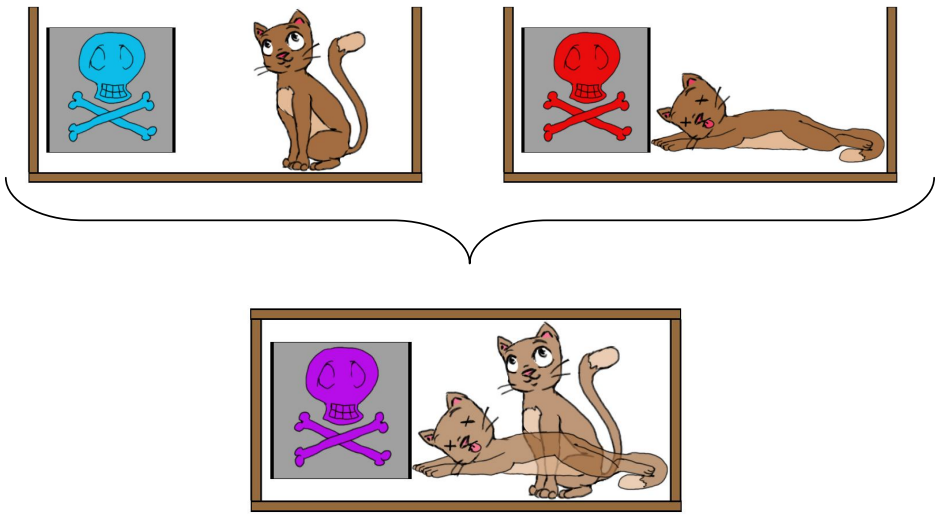
Dr. Quantum: Video ist auf gängigen Internet-Videoportalen zu finden

Physik des Diskreten: Modell des Teilchens, Massepunkts (Mechanik)
Physik des Kontinuierlichen: Theorie der Felder (Elektromagnetismus)

Die Quantenphysik stellt eine Verbindung zwischen den beiden Denkansätzen her, da Teilchen im Experiment auch Welleneigenschaften zeigen (Video)

Für Wellen gilt: Intensität ~ Betragsquadrat der Amplitude
Für Teilchen: Intensität ~ Auftreffwahrscheinlichkeit
Insgesamt: **Betragsquadrat der Amplitude ~ Aufenthaltswahrscheinlichkeit**

Schrödingers Katze: Eine Katze wird in eine Kiste mit quantenphysikalischem Tötungsmechanismus gesteckt. Schließt man den Deckel, weiß man nicht ob die Katze noch am Leben oder schon gestorben ist. Sie ist gewissermaßen beides gleichzeitig. Erst durch das Öffnen des Deckels und Hineinschauen (Messen) nimmt die Katze einen Zustand an.
Überlagerung von Zuständen heißt **Superposition**



Quantenphysik: Gott würfelt doch

Laplacescher Dämon: Der Laplacesche Dämon ist das Sinnbild einer deterministischen Physik. In einer deterministischen Physik ist jeder Vorgang die direkte Folge eines vergangenen Ausgangszustandes und gleichzeitig die Grundlage für die zukünftige Entwicklung.

Oft wird hier der Vergleich mit einem komplizierten Getriebe aus Zahnrädern bemüht. Kennt man die Lage aller Zahnräder und wie diese ineinander greifen, so läuft dieses Uhrwerk ohne der Möglichkeit einer Intervention von selbst ab.

Ein Laplacescher Dämon braucht also nur den Ort und den Bewegungszustand aller Teilchen (Zahnräder) zu kennen und könnte bis in alle Zukunft die Bewegungen vorausberechnen. Dies wirft natürlich gewisse philosophische Probleme auf, die mit dem freien Willen zu tun haben.

Gott würfelt nicht: Berühmter Ausspruch von Albert Einstein. Er konnte die stoachastische Natur der Quantenphysik nur schwer akzeptieren. Einstein glaubte an die Existenz von noch unbekannten, verborgenen Variablen, die das Verhalten der einzelnen Teilchen bestimmen.

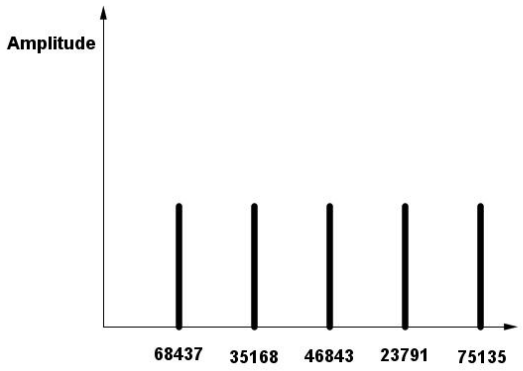
Bell-Ungleichung: Es gab lange Zeit Streit über die Quantentheorie, da sie sich grundlegend von anderen Theorien unterscheidet. Bisher gab es nur lokal realistische Theorien:

- **lokal** Die Messung eines Objekts darf keine augenblicklichen Auswirkungen auf ein anderes, räumlich entferntes, Objekt zeigen
- **realistisch** Die Messung fördert eine bereits vorher vorhandene Eigenschaft zu tage, auch wenn man diese wegen ungenügender Kenntnis von verborgenen Parametern nicht kennt

John Bell fand ein Experiment, bei dem jede lokal realistische Theorie, so sie existieren möge, einen anderen Wert als die Quantenphysik voraussagte und lies die Natur entscheiden: Die Quantenphysik wurde bestätigt.
Die Quantenphysik ist keine lokal realistische Theorie

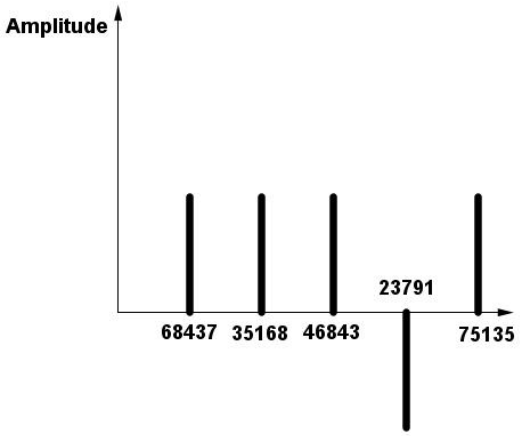
Quantencomputer: Grovers Algorithmus

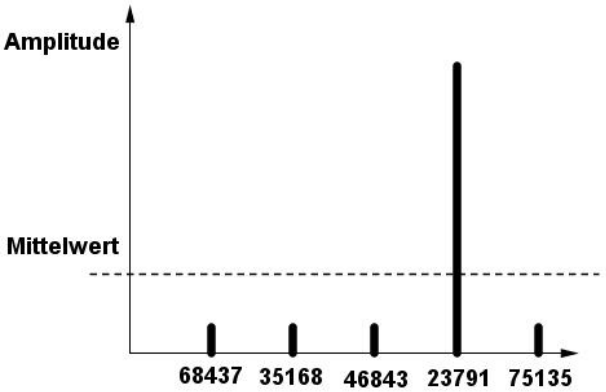
Suche in unsortierten Listen (Handykontakte nach Telefonnummer)



Zunächst wird eine Superposition über alle Telefonnummern erstellt. Eine Messung würde nun, immer mit der gleichen Wahrscheinlichkeit, eine der Telefonnummern liefern

Anschließend läuft eine Anfrage an die Datenbank. Die Amplitude der gesuchten Telefonnummer wird gekippt, die anderen bleiben.
Vorteil: Beim Quantencomputer ist es egal, wie viele Nummern in der Superposition sind





Die Amplituden werden um den Mittelwert gespiegelt und die gesuchte Amplitude wird verstärkt. Bei einer Messung erhält man mit hoher Wahrscheinlichkeit die richtige Nummer.

Quantencomputer: Faktorisierung

RSA-Verschlüsselung: Große Zahlen sind nur schwer in Primfaktoren zu zerlegen. RSA verwendet zwei große Primzahlen und berechnet daraus zwei Schlüssel. Mit Public Key wird veröffentlicht und jeder kann damit Nachrichten verschlüsseln. Der Private Key verbleibt die ganze Zeit beim Empfänger und nur mit diesem lassen sich die Nachrichten wieder entschlüsseln.
Das Primzahlenprodukt ist ebenfalls öffentlich. Gelingt es diese Zahl zu faktorisieren, ist die Verschlüsselung geknackt. Der Zeitaufwand ist mit herkömmlichen Computern gewaltig.

Shors Algorithmus: Ein genau auf dieses Problem optimierter Quanten-Algorithmus. Mit ihm wäre man in der Lage, die Faktorisierung in kurzer Zeit zu berechnen. Die größte Zahl, die bisher faktorisiert wurde, ist 15.

Albert Einstein

Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt.

(erschienen 1905 in Annalen der Physik 17, 132 – 148)

Auszug aus Originaltext:

§ 8. Über die Erzeugung von Kathodenstrahlen durch Belichtung fester Körper.

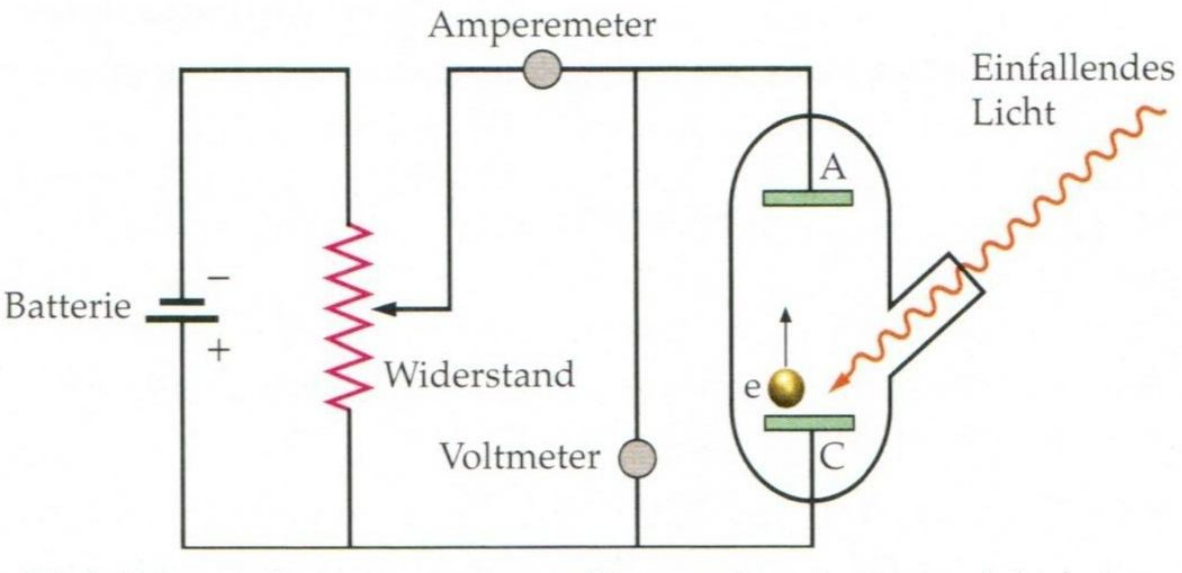
Die übliche Auffassung, daß die Energie des Lichtes kontinuierlich über den durchstrahlten Raum verteilt sei, findet bei dem Versuch, die lichtelektrischen Erscheinungen zu erklären, besonders große Schwierigkeiten, welche in einer bahnbrechenden Arbeit von Hrn. Lenard dargelegt sind.[1])

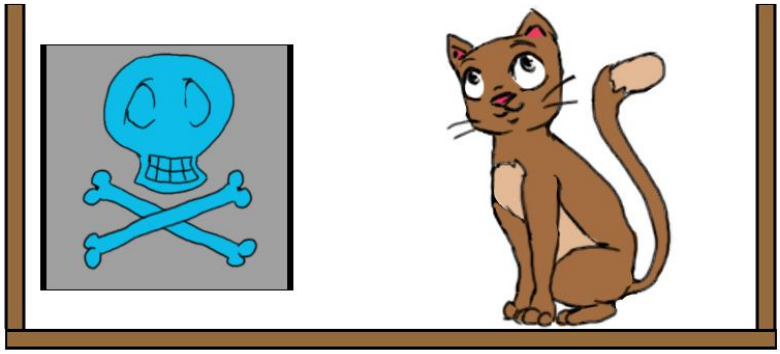
Nach der Auffassung, daß das erregende Licht aus Energiequanten von der Energie $(R/N)\beta\nu$ bestehe, läßt sich die Erzeugung von Kathodenstrahlen durch Licht folgendermaßen auffassen. In die oberflächliche Schicht des Körpers dringen Energiequanten ein, und deren Energie verwandelt sich wenigstens zum Teil in kinetische Energie von Elektronen. Die einfachste Vorstellung ist die, daß ein Lichtquant seine ganze Energie an ein einziges Elektron abgibt; wir wollen annehmen, daß dies vorkomme. Es soll jedoch nicht ausgeschlossen sein, daß Elektronen die Energie von Lichtquanten nur teilweise aufnehmen. Ein im Innern des Körpers mit kinetischer Energie versehenes Elektron wird, wenn es die Oberfläche erreicht hat, einen Teil seiner kinetischen Energie eingebüßt haben. Außerdem wird anzunehmen sein, daß jedes Elektron beim Verlassen des Körpers eine (für den Körper charakteristische) Arbeit P zu leisten hat, wenn es den Körper verläßt. Mit der größten Normalgeschwindigkeit werden die unmittelbar an der Oberfläche normal zu dieser erregten Elektronen den Körper verlassen. Die kinetische Energie solcher Elektronen ist

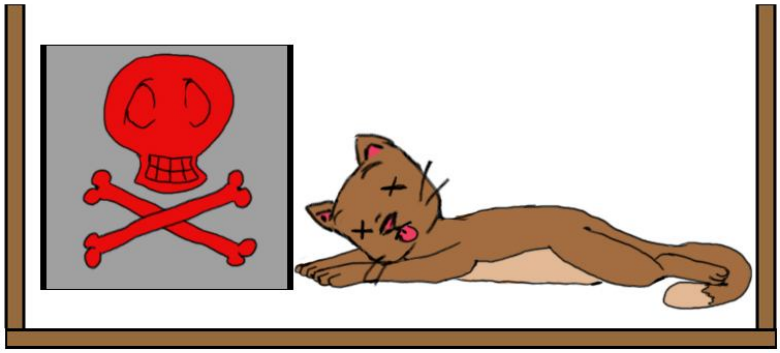
$$\frac{R}{N}\beta\nu - P.$$

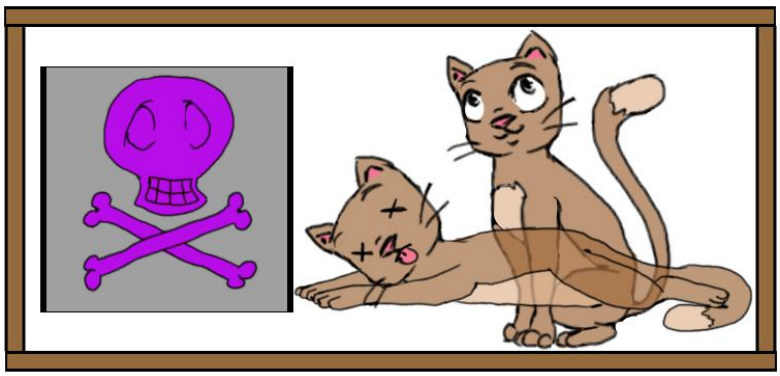
Anhang B

Overhead-Folien


Amperemeter
Einfallendes
Licht
A
Batterie
−
+
Widerstand
e
Voltmeter
C

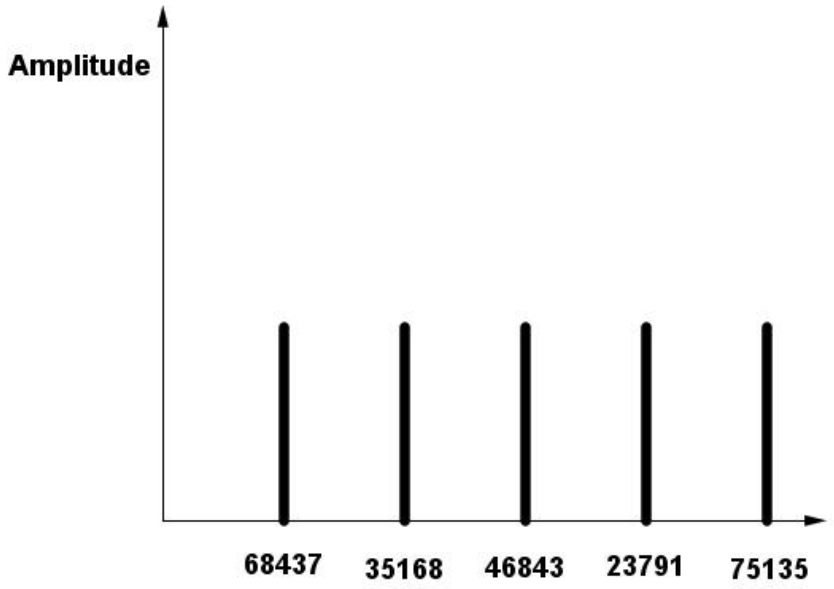


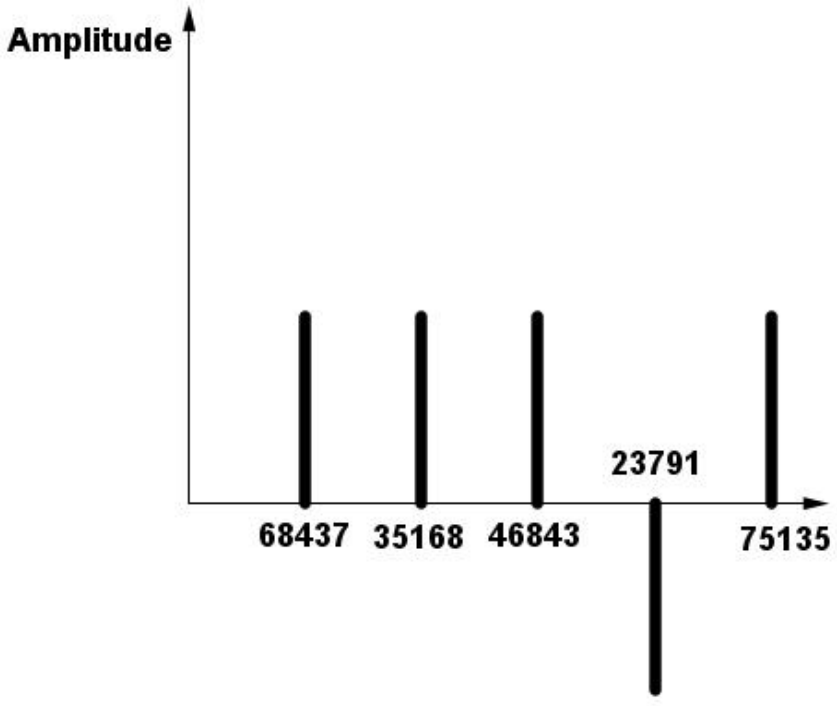


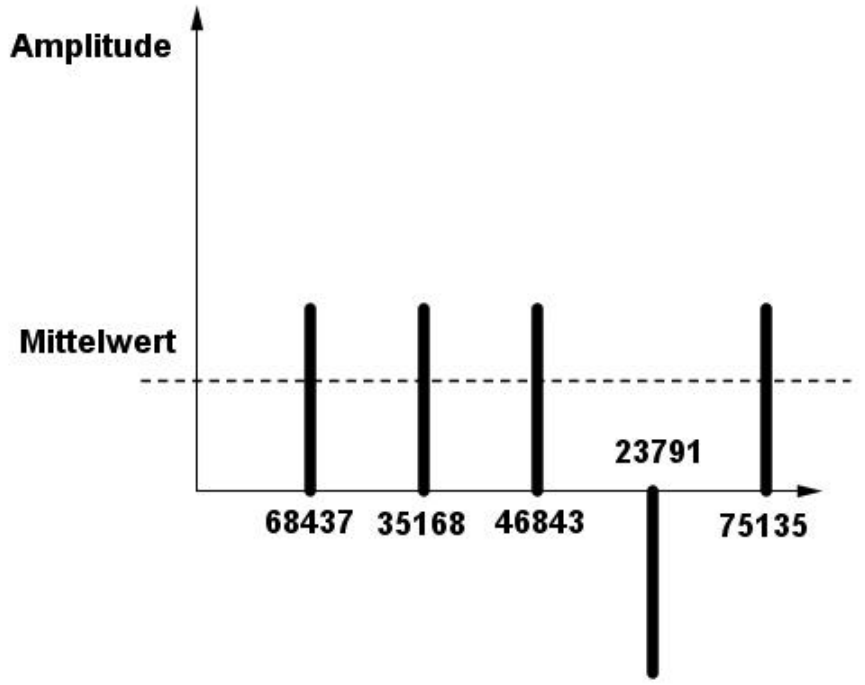


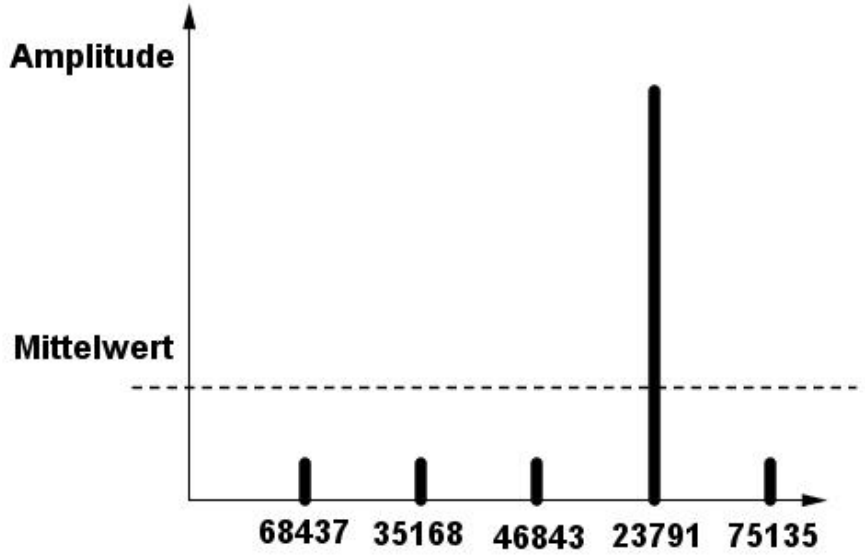
1	Alex	82703
2	Beatrix	28513
3	Claudia	87951
4	Domink	61345
5	Eva	83529
6	Florian	98316
7	Gerald	41948
8	Hanna	49442
9	Iris	36771
10	Julia	26516
11	Kathi	91126
12	Lisa	89657
13	Markus	32999
14	Nina	94539
15	Oliver	67148
16	Peter	44005
17	Rudi	78041
18	Stefan	86412
19	Theresa	16174
20	Ulli	21109
21	Vera	28444
22	Walter	95899
23	Xaver	25523
24	Yvonne	12382
25	Zelda	84620

Name	Telefonnumer
Alex	68437
Berta	35168
Claudia	46843
Dominik	23791
Eva	75135






Amplitude
Mittelwert
23791
68437
35168
46843
75135


Amplitude
Mittelwert
68437
35168
46843
23791
75135

Abbildungsverzeichnis

Literaturverzeichnis

[1] Matthias Homeister: *Quantum Computing verstehen* Wiesbaden, 2008

[2] Jürgen Audretsch: *Verschränkte Systeme* Weinheim, 2005

[3] Paul A. Tipler; Gene Mosca: *Physik für Wissenschaftler und Ingenieure* München, 2004

[4] Bernhard Baumgartner: *Prinzipien der modernen Physik* Wien, 2005

[5] Albert Einstein: *Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt.* Annalen der Physik, Vierte Folge, Band 17, 1905

[6] Fred A. Wolf: *What the#$*! Do We Know!?* Lord of the Wind Films, 2004

[7] Charles Addams: *The Skier* The New Yorker, 1940

[8] Albert Einstein: *Brief an Max Born, 4. Dez. 1926.* Einstein-Archiv 8-180

[9] Gordon E. Moore: *Cramming more components onto integrated circuits* Electronics, Volume 38, Number 8, 1965

[10] Roland Rivest; Adi Shamir; Leonard Adleman: *Cryptographic communications system and method* Massachusets intitute of technology, 1983

[11] Heidemarie Knobloch: *Quantenkryptographie in der Schule* Wien, 2009

Nachwort

In diesen letzten Zeiten möchte ich bei Allen bedanken, die mich auf meinem Weg durchs Studium begleitet haben und insbesondere bei meiner Diplomarbeitsbetreuerin Frau Univ. Doz. Mag. Dr. Beatrix Hiesmayr, die mir bei der Gestaltung dieser Diplomarbeit freie Hand lies und immer wieder, auch kurzfristig, Zeit für mich fand.

Ein besonderer Dank gilt natürlich meinen Eltern, Herbert und Sieglinde Greindl, die mir dieses Studium erst ermöglicht haben. Sie gaben mir nicht nur den finanziellen Rückhalt, sondern unterstützten mich zu jeder Zeit vorbehaltlos und in jede Richtung.
Auch meinen Großeltern, Alfred und Theresia Schobesberger, möchte ich meinen Dank für die Mitfinanzierung des Studiums aussprechen.
Abschließend möchte ich mich noch bei meiner kleinen Schwester, Eva Greindl, für die Anfertigung einiger Zeichnungen dieser Diplomarbeit bedanken.

Lebenslauf

Persönliche Daten

Name:	Stefan Greindl
Geburtsdatum:	30.12.1986
Geburtsort:	Wels
Staatsbürgerschaft:	Österreich
Vater:	Herbert Greindl
Mutter:	Sieglinde Greindl

Ausbildung

1997-1193	Volksschule Wels
1997-2001	BRG Brucknerstraße Wels
2001-2006	HTBLA Edv und Organisation Leonding
2006-2011	Lehramtsstudium Mathematik und Physik