THM | CAMPUS GIESSEN
TECHNISCHE HOCHSCHULE MITTELHESSEN

MNI
Mathematik, Naturwissenschaften und Informatik

- Quantencomputing -
Skript SS 2020
Dozentin: Prof. Dr. Bettina Just

Skript erstellt
von

Dupleix Takoulegha, Markus Kretsch, Bettina Just
in den Sommersemestern 2014, 2015, 2018, 2019 und 2020

Vorwort

Über das Skript:

Das Skript entstand erstmals während der Vorlesung "Quantencomputing", die im SS2014 am FB MNI der THM im Masterstudiengang Informatik gehalten wurde.
Das Gebiet entwickelt sich schnell, und so ist auch das Skript jedesmal wieder anders. Im SS2018 kamen die vielen Möglichkeiten hinzu, online oder mit freeware selbst Quantenalgorithmen zu programmieren. Außerdem das adiabatische Quantencomputing. Im SS2019 wird die Veranstaltung erstmals im BSc-Studiengang als Blockveranstaltung angeboten. Im SS2020 ist die Vorlesung erstmals eine normale wöchentliche Veranstaltung - und auch erstmals eine online-Veranstaltung.

Wer Fehler findet, ist herzlich eingeladen, mir eine e-mail zu schicken. Dann wird im Laufe der Zeit das Skript immer besser. :-).

Bettina Just im SS2020

Inhaltsverzeichnis

1 Quantencomputing in der (Informatik)welt

Ursprung: Quantenphysik: Theorie ca. $1925 - 1935$ entwickelt vor allem:

Planck (Strahlungsgesetz/Energiequanten),

Heisenberg (Unschärferelation),

Schrödinger(Katze),

Einstein(Photoelektrischer Effekt, Nobelpreis 1921), Bohr(Atommodell),

Born(Kopenhagener Deutung Nobelpreis 1954),

....

Ziel: Beschreibung der Vorgänge im subatomaren Bereich.

Konkret: Wie verhalten sich Elektronen (Schale des Atoms) und Lichtteilchen? Sie sind so klein, dass die Beobachtung ihren Zustand ändert. [1] Daher vorwiegend statistische Aussagen möglich (aber nicht ausschließlich).

Experimente: Entwicklung des Lasers machte Experimente mit einzelnen Lichtteilchen nach und nach möglich.

Ergebnis: Sie verhalten sich

- entweder nicht "lokal". D.h., es gibt eine Wechselwirkung in Überlichtgeschwindigkeit (aktuelle Experimente: mit mindestens 10.000-facher Lichgeschwindigkeit, Quelle Wikipedia "Quantenverschränkung")
- oder nicht "realistisch". D.h., Teilchen haben bestimmte physikalische Eigenschaften (wie z.B. die Drehrichtung „spin") nicht an sich, sondern haben mehrere dieser Eigenschaften zugleich, und nehmen erst bei der Messung eine Ausprägung an.

Beides widerspricht unserem Weltbild.
Bohr: „Wer über die Quantenphysik nicht entsetzt ist, der hat sie nicht verstanden".
Feynman: „Wer behauptet, die Quantenphysik verstanden zu haben, der hat sie nicht verstanden".

Ist aber experimentell immer wieder bestätigt und nie widerlegt worden. (Wie das Prinzip geht, wird in der Vorlesung vertieft).

[1] Man stelle sich vor, Newton hätte die Eigenschaften fallender Äpfel nur beobachten können, indem er andere Äpfel darauf geworfen hätte.

Schritt in die Informatik: Angeblich war es Richard Feynmann (Veröffentlichung 1982), der die Idee hatte: Wenn Teilchen mit Überlichtgeschwindigkeit kommunizieren, und zugleich mehrere Zustände annehmen, dann müsste man doch tolle Computer damit bauen können. So wurde zu Beginn der 1980er Jahre ein Berechnungsmodell, „Quantengatter“ entwickelt (finale Definition von Deutsch 1985).
War aber Randthema, sowohl Hardware-Realisierung als auch Nutzen unklar, bis Peter Shor 1994 einen Quanten-Polynomialzeit-Algorithmus zur Faktorisierung natürlicher Zahlen veröffentlichte. Seither wird Quanten-Computing intensiv beforscht - auf der Hardware und Software-Seite.
Denn: Schnelle Faktorisierung ermöglicht das Brechen fast aller Internet-Verschlüsselungen (Brechen des RSA-Schemas). Also nicht nur der derzeit verschlüsselten Nachrichten, sondern auch der vielen abgespeicherten nicht entschlüsselten Nachrichten der Vergangenheit...
(Es gibt als neues Gebiet deshalb jetzt die Post-Quantum-Cryptography; sie entwickelt Verfahren, die gegen Quantencomputer gefeit sind, weil sie auf NP-vollständigen Problemen basieren).

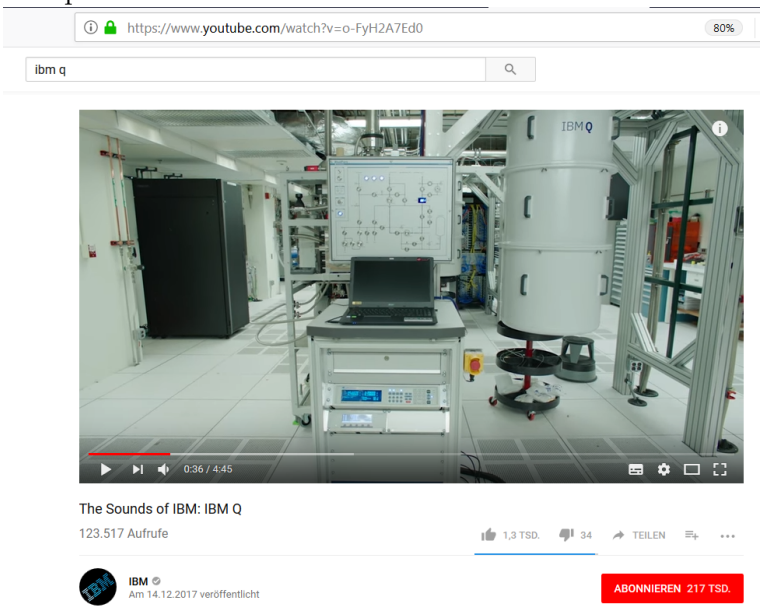
Hardware: Realisierung von $QBit$s durch:

- Ionenfallen
- SQUIDS (Systeme aus Supraleitern).
- polarisierte Photonen
- Quantenpunkte (was immer das sei)
- Kernspinresonanz

Frühjahr 2018:

- Google präsentiert Google Bristlecone, 72 QBits auf einem Chip
- Intel präsentiert Chip mit 49 QBits auf einem Chip

- ... Aber ein Chip macht noch keinen Computer. Quantencomputer sind ganze Räume, vor allem, weil sie auf -272 Grad gekühlt werden müssen. IBMs Q klingt wie eine Dampflokomotive:



Frühjahr 2109:

- IBM präsentiert zum erstenmal einen Stand alone Quantencomputer, einen Würfel von 2 m Seitenlänge, den IBM-Q system one.
- D-Wave hat einen Adiabatischen Quantencomputer (mit einem anderen Berechnungsmodell, eine ganz andere Vorgehensweise - manche sagen, er segelt unter falscher Flagge) mit über 2000 (Ziel: 4096) Bits. Noch vor drei Jahren glaubten viele, das sei die wahre Zukunft des Quantencomputings. Inzwischen hat das ursprüngliche Berechnungsmodell wieder aufgeholt und wird „Quantentechnologie 2.0“ genannt.
- **n QBits haben die Rechenleistung von 2^n normalen Bits in der gleichen Zeit**

Hardware-Problem: Fehleranfälligkeit.
Je mehr QBits, desto eher interagieren sie untereinander oder mit der Umwelt, und dann wird Berechnung falsch. Sie sind sehr schwer zu isolieren. Daher wird

1.) An fehlerkorrigierenden Algorithmen gearbeitet

2.) An hybriden Algorithmen gearbeitet: Quantenprozessoren mit ca 50-100 QBits erweitern klassische Computer.

Die wesentlichen Player:

- Geheimdienste (vermutlich).

- Google. Kaufte 2013 einen D-Wave, und hat nun selbst Quantenchip mit 72 QBits präsentiert. Arbeiten in beiden Quantencomputing-Welten. Ziel von Google ist es, die „Quantum Supremacy“ (dt. Quantendominanz) zu erreichen, d.h., einen Quantencomputer zu haben, der besser als die herkömmlichen Computer ist.
  (In 2019 behauptete google, mit einer bestimmten Aufgabe Problem sei die Quantum supremacy jetzt bewiesen. Diese könne nachweislich von einem Quantencomputer schneller gelöst werden als von einem herkömmlichen computer. Die Aufgabe ist im Grunde die Simulation eines Quantencomputers. Ein Spötter schrieb daraufhin, seine Kaffeetasse sei einem Quantencomputer überlegen. Denn sie könne besser das Zersplittern einer auf den Boden fallenden Kaffeetasse simulieren als ein Quantencomputer.)

- IBM. Haben ihr Q-Netzwerk, d.h. jeder kann in einer Cloud seine Quantenalgorithmen auf bis zu 20 QBits laufen lassen. Bisher 1,7 Mio Experimente von über 60.000 Nutzern. Und haben seit 2019 den ersten stand alone Quantencomputer, allerdings nur für Forschungseinrichtungen - er erfüllt längst noch nicht kommerzielle Ansprüche an Speicherplatz und Korrektheit.

- Microsoft. Wollen mit Q# gerüstet sein, Entwicklungsplattform für Quantenalgorithmen auf Basis von Visual Studio, frei verfügbar.

- Python: Seit 2019 gibt es die Python library CIRC für Quantenalgorithmen.

- Intel. Präsentierte im März 2018 einen 49-QBits Chip.

- Die EU. Hat Mitte 2017 das Projekt „Quantum Technology Flagship“ mit einem Volumen von 1 Mrd. Eur ins Leben gerufen (mit den Teilbereichen Communication, Computing, Sensoring, Simulation). Erste gemeinsame Tagung war im Frühjahr 2019.

- China. Haben angekündigt, 10 Mrd. Dollar in die Technologie zu investieren (Info aus Januar 2018). Sind Vorreiter bei der Technik mit Photonen, für Quanteninternet.

- Kanada. Haben seit 2016 das „Canadian Institute for Quantum Computing“ mit einer Anschubfinanzierung von 300 Mio Dollar - und D-Wave.

- Universitäten: Lange allen voran die Uni Innsbruck mit wissenschaftlich nachweisbaren Resultaten.

- Zahllose andere Universitäten, z.B. hat Berkeley 2010 herausgefunden, dass Pflanzen zur Photosynthese Quanteneffekte nutzen - ohne Energie zu verbrauchen.

Weltrekord zur Teleportation (Nicht-Lokalität, für Verschlüsselung): (zitiert u.A. nach Wikipedia, Quantenteleportation)
2004: 600m (Innsbruck (Zeilinger) + Boulder/Colorado)
2010: 16km (Team China)
2012: 143km La Palma - Teneriffa (internationales Team um Zeilinger)
2017: 1400 km von der Erde zu einem Satelitten (China + Zeilinger)

Weltrekorde Faktorisierung einer Zahl mit Quantencomputern:
2001: 15 faktorisiert(IBM San Jose, Ionenfallen)
2011: 21 faktorisiert(Univ Bristol, Photonen)
2012: 15 nochmals faktorisiert(Univ. California, Supraleitung)
(2012: 56153, aber mit D-Wave und adiabatischem Quantencomputing)
2016: 15 nochmals faktorisiert, mit 5 statt 12 QBits (Ionenfallen Univ. Innsbruck)

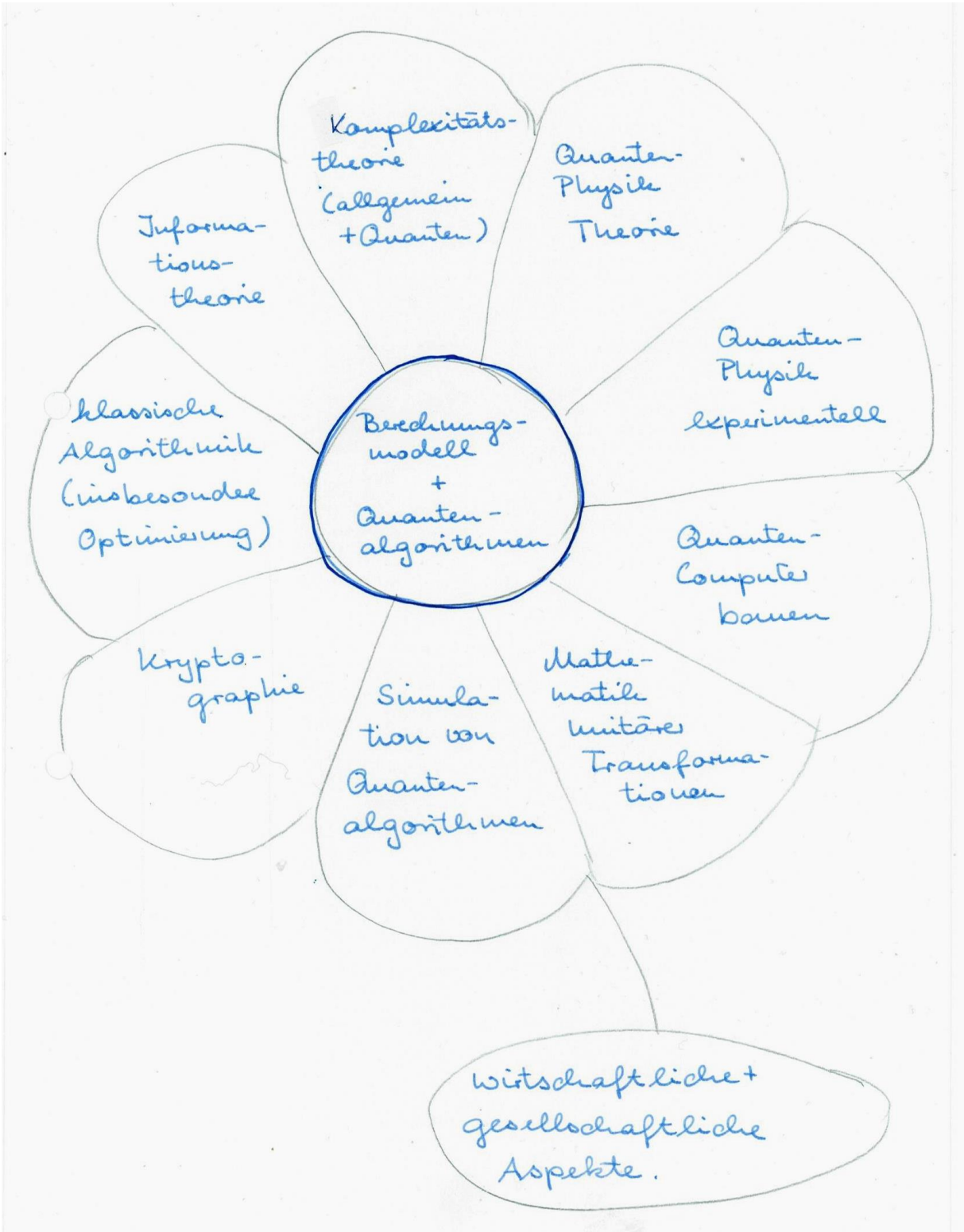
Anwendungsgebiete:

- Optimierungsprobleme - werden approximativ gelöst
- Datenbanksuche
- Simulation von Molekülen, Design von Materie
- Big Data Analysis
- Künstliche Intelligenz - noch Zukunftsmusik. Manche sagen, das wird nie etwas, andere sehen es in 5 Jahren die Welt revolutionieren und die menschliche Intelligenz in den Schatten stellen. Die Frist mit den 5 Jahren ist schon lange gültig ;).

Ziele der Vorlesung: (steht so in der Modulbeschreibung)
Die Studierenden

- haben eine Vorstellung von Quantenverschränkung und kennen das Berechnungsmodell des Quantencomputing anhand einfacher Algorithmen;
- sind in der Lage, einfache Quantenalgorithmen zu programmieren;
- sind darüber hinaus informiert über die wichtigsten Quantenalgorithmen, sowie deren Bedeutung und mögliche Anwendungen;
- kennen die aktuelle Situation der Hardware von Quantencomputern un dsind damit in der Lage, Informationen über neue Entwicklungen im Quantencomputing einzuordnen.

Schwerpunkt: Funktionsweise von Quantenalgorithmen.
Was wir machen und was die angrenzenden Gebiete sind, veranschaulicht die folgende Zeichnung.



Berechnungsmodell Quantencomputing ist anders als Berechnungsmodell klassisches Comuptuing (Turingmaschine). Denn Quantenbits (kurz QBits) sind anders als klassische Bits:

Klassisches Bit: Objekt, das genau zwei unterschiedliche Zustände annehmen kann, 0 und 1.
Klassische Schaltgatter führen Schaltungen zwischen Bits durch, und sind die Basis klassischer Computer.

Unterschiedliche physikalischen Realisationsmöglichkeiten:
- Draht, der keinen Strom führt oder Strom führt.
- Lampe, die leuchtet oder nicht leuchtet. (Aus den Anfangszeiten der Computerhardware)
- Zeiger (wie Uhrzeiger auf einem Zifferblatt), der die beiden Positionen waagrecht oder senkrecht annehmen kann.

Folgende beide Eigenschaften klassischer Bits sind so selbsverständlich, dass sie meist gar nicht genannt werden:

- (Realismus für Bits)
  Der Wert eines Bits ist zu jedem Zeitpunkt der Berechnung eindeutig definiert. Er kann ausgelesen werden, und der Auslesevorgang ändert den Wert nicht.

- (Lokalität für Bits)
  Wird der Wert eines bestimmten einzelnen Bits verändert, so ändert das nicht den Wert irgend eines anderen Bits.

Beide Eigenschaften kommen aus der klassischen Mechanik:

- (Realismus)
  Objekte haben Eigenschaften wie Gewicht, ihre Farbe, ihre Geschwindigkeit oder Größe, die man messen kann, und die dadurch nicht verändert werden.

- (Lokalität)
  Eine Aktion an einem Punkt des Raumes wirkt sich nicht unmittelbar auf physikalische Objekte an einem anderen Punkt des Raumes aus. Auswirkung muss durch Licht oder Materie übertragen werden, und braucht daher mindestens Lichtlaufzeit zwischen beiden Raumpunkten.

Quantenbit: Kann die Werte $|0\rangle$ oder $|1\rangle$ oder irgendetwas DAZWISCHEN annehmen kann.
Quantengatter führen Operationen auf QBits durch, und sind die Basis für Quantencomputer.

Unterschiedliche physikalischen Realisationsmöglichkeiten:
- Photonen, gefangene Ionen, Supraleitung...
- Zeiger (wie Uhrzeiger auf einem Zifferblatt), mit Positionen waagrecht oder senkrecht oder irgendetwas dazwischen.

Quantenbits haben NICHT die Eigenschaften des Realismus und der Lokalität aus der klassischen Mechanik, sondern diese beiden (beides sind die wesentlichen Grundlagen für das Quantencomputing):

- (Veränderung beim Messen)
  Wird ein Quantenbit gemessen, so liefert es einen der beiden Werte $|0\rangle$ oder $|1\rangle$, und niemals einen Wert dazwischen. Messung verändert also den Wert des Quantenbits (wenn es zwischen $|0\rangle$ und $|1\rangle$ war).

- (Quantenverschränkung)
  Veränderung eines Quantenbits an einem Punkt des Raumes kann unmittelbar, also im selben Augenblick, (also mit Überlichtgeschwindigkeit) die Eigenschaften eines anderen Quantenbits verändern.

Dass Objekte ihre Eigenschaften durch die Messung verändern, ist in der klassischen Informatik nicht vorgesehen, aber in der uns umgebenden Welt bekannt. Es gibt Situationen, in denen die Messung selbst die Situation verändert, z.B. in der Qualitätsprüfung von Bauteilen. Wird hier ein Belastungstest durchgeführt, ist das Bauteil hinterher nicht mehr so belastbar wie zuvor. Und wer Kinder hat, weiss ohnehin, dass sie sich anders verhalten, wenn sie beobachtet werden.

Das Phänomen der Quantenverschränkung ist jedoch so verblüffend, dass es von Einstein spukhafte Fernwirkung genannt wurde, und Bohr angeblich sagte:
„Wer über die Quantentheorie nicht entsetzt ist, der hat sie nicht verstanden.“
Die Eigenschaften der kleinsten Teilchen können sich so ändern wie die Eigenschaften eines Thronfolgers, der in dem Moment König wird, in dem der alte Monarch stirbt. Er ist sofort König - schneller als das Licht braucht, um die Distanz zwischen ihm und dem alten Monarchen zu überwinden.

Wie wird die spukhafte Fernwirkung nachgewiesen?
Und wie funktioniert das Berechnungsmodell des Quantencomputings, dass auf QBits basiert, die so seltsame Eigenschaften haben?

Das kommt in den nächsten Kapiteln dran.

2 Das Berechnungsmodell

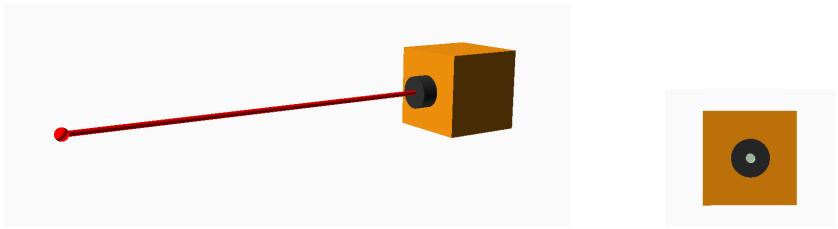
2.1 Physik: Superschnell kommunizierende Teilchen

In diesem Kapitel werden die Experimente idealtypisch gezeigt, die zeigen, dass QBits die Eigenschaften von Realismus und Lokalität NICHT haben.

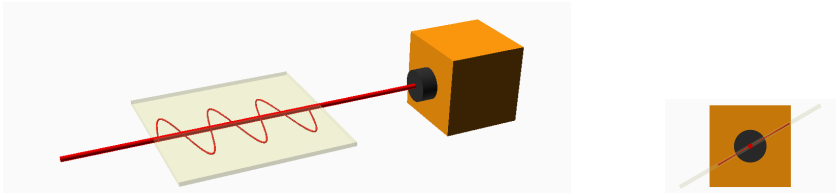
Die Gedankengänge gehen auf Einstein, Poldolsky und Rozen (1935) zurück. In ihrer Arbeit handelte es sich zunächst um Gedankenexperimente. Die Experimentalphysik war noch nicht so fortgeschritten, dass man die Experimente tatsächlich durchführen konnte. Inzwischen wurden die Experimente durchgeführt, und lieferten die im Gedankeneperiment progonstizierten Ergebnisse.
Hier werden sie idealisiert betrachtet. Details der technischen Realisierung, Behandlung von Messfehlern etc bleiben außen vor.

Betrachtet werden Photonen (Lichtteilchen). Diese können inzwischen mit Laser einzeln erzeugt werden. Sie sind ein Beispiel für die Realisierung von QBits.

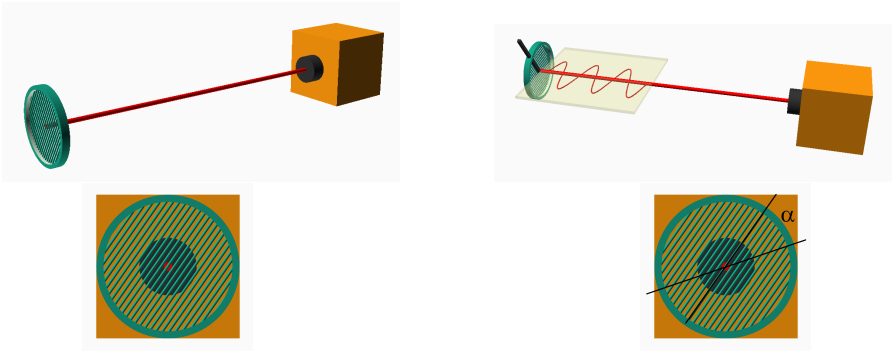
Definition: Ein Photon ist (für diese Vorlesung) ein punktförmiges Objekt, das aus einem Kasten kommt, und entlang einer Geraden (in Richtung seiner Ausbreitungsrichtung) fliegt. Die folgende Abbildung zeigt die Situation von vorne und von der Seite.



Es kann (muss aber nicht) eine Polarisation haben. Das bedeutet, dass es in einer Ebene schwingt, in der auch die Gerade mit der Ausbreitungsrichtung liegt.



Definition: Ein Photon kann mit einem Polarisationsfilter (man stelle sich ein Kühlschrankgitter vor) gemessen werden.



Es gibt zwei mögliche Messergebnisse:

- Entweder das Photon passiert den Polarisationsfilter. Dann fliegt es in seiner Ausbreitungsrichtung weiter, und ist in Richtung des Polarisationsfilters polarisiert.
- Oder das Photon wird vom Polarisationsfilter absorbiert. (Später werden wir uns vorstellen, dass es dann trotzdem weiter fliegt, aber senkrecht zum Winkel des Polarisationsfilters polarisiert ist).

Wann tritt welches Messergebnis ein?

- Ist das Photon nicht polarisiert (oder kennen wir seine Polarisiation nicht), so ist für jeden Winkel des Polarisationsfilters die Wahrscheinlichkeit für „passiert“ und „wird absorbiert“ je 1/2.
- Ist das Photon polarisiert, so ist die Wahrscheinlichkeit für „passiert“ umso größer, je kleiner der Winkel α zwischen seiner Polarisation und dem des Filters ist. (Frisbee fällt in Gulli).

  Ist $\alpha = 0$, so passiert das Photon immer.

  Ist $\alpha = 90°$, so passiert das Photon niemals.

  Ist $\alpha = 45°$, so passiert das Photon mit Wahrscheinlichkeit 1/2.

  Ganz allgemein passiert das Photon mit Wahrscheinlichkeit $(\cos\alpha)^2$. Daraus folgen schon die oben genannten Wahrscheinlichkeiten. Außerdem:

  Ist $\alpha = 30°$ so passiert das Photon mit Wahrscheinlichkeit 3/4, und

  Ist $\alpha = 60°$ so passiert das Photon mit Wahrscheinlichkeit 1/4.

Bemerkung:

i.) Messen verändert das Teilchen (QBit)!

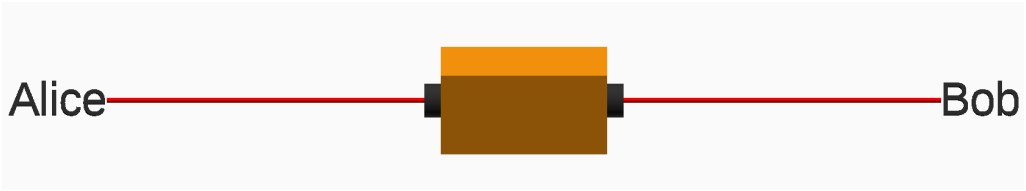
ii.) Die Definition modelliert das Gesetz von Malus, hier nach Wikipedia zitiert (Stand 24.7.2019):
„Das Gesetz von Malus (nach Etienne Louis Malus), seltener auch malussches Gesetz genannt, beschreibt die Intensität I einer linear polarisierten Welle der Anfangsintensität I_0 nach dem Durchgang durch einen idealen Polarisator in Abhängigkeit vom Winkel α, um den die optische Achse des Polarisators gegen die Polarisationsrichtung der Welle verdreht ist: $I = I_0 \cdot \cos^2 \alpha$

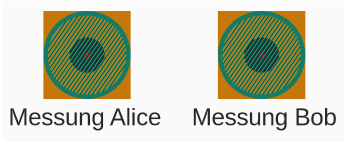
Die durchgelassene Strahlung ist in der Richtung des Filters polarisiert, die restliche Intensität (proportional zu $\sin^2 \alpha$ wird im Falle eines Polarisationsfilters absorbiert, im Falle eines polarisierenden Strahlteilers reflektiert.“

iii.) In der Vorlesung wird der Versuch zum Gesetz von Malus mithilfe eines Kühlschrankgitters und eines Bleistifts veranschaulicht.

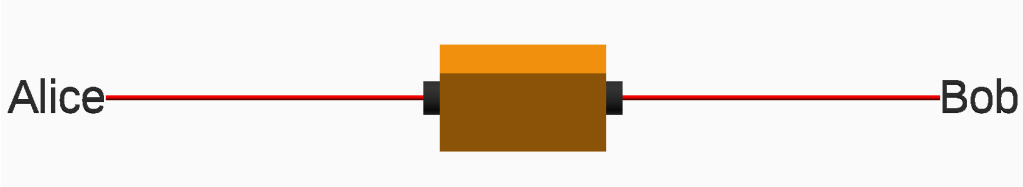
Ziel jetzt: Phänomen der Quantenverschränkung verstehen (naja, oder glauben), und auch, wie es in (idealisierten) Experimenten nachgewiesen wird.

Versuchsaufbau in allen drei Versuchen: Quelle erzeugt Paare von Photonen, die in zwei entgegengesetzte Richtungen weg fliegen und dann erst auf Seite A (bei Alice), dann auf Seite B (bei Bob) gemessen werden. Die Versuche unterscheiden sich darin, wie die Teilchen erzeugt werden, und in welchem Winkel sie gemessen werden.



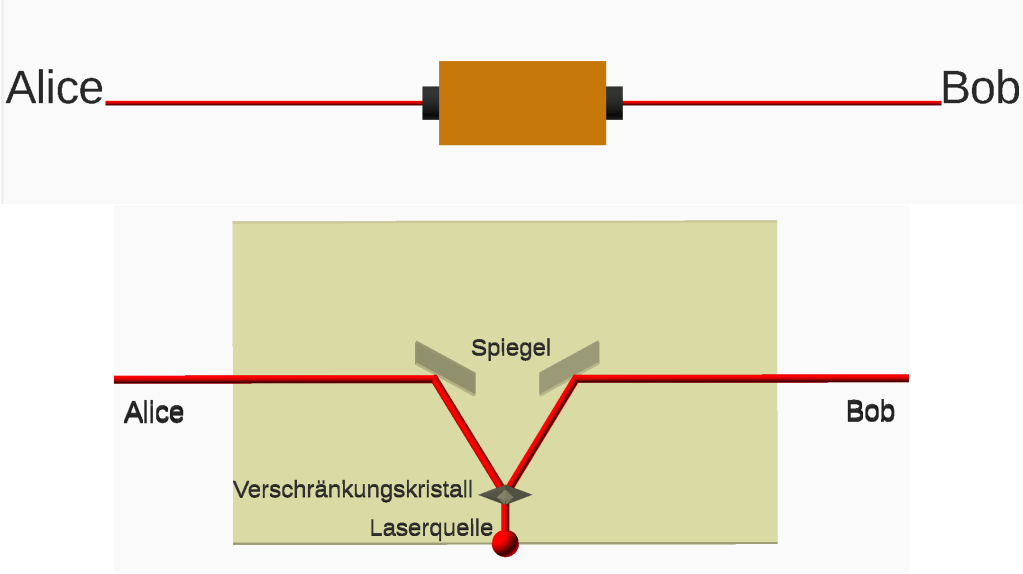


Versuch 1: Paare unabhängiger Teilchen, gemessen wird erst Seite A (für Alice), dann Seite B (für Bob), und zwar beide im gleichen Winkel α:



Ergebnis (für jeden Winkel α): Anteil passierender Teilchen ist auf jeder Seite 1/2; keine statistische Korrelation.

Versuch 2: Wie Versuch 1, aber jetzt sind die Paare verschränkt. Das bedeutet, dass sie nicht unabhängig erzeugt werden, sondern aus einem einzelnen Lichtteilchen stammen, das durch einen „Verschränkungskristall“ geschickt wird, und sich dabei aufspaltet in zwei Lichtteilchen. (Verschränkte Teilchen kann man seit dem frühen 20. Jahrhundert herstellen; wie das genau geht ist (im Moment) nicht Gegenstand der Vorlesung).



Gemessen wird wie oben auf beiden Seiten in irgendeinem, für beide gleichen, Winkel α (erst Seite A, dann Seite B).
Ergebnis (für jeden Winkel α): Anteil passierender Teilchen ist auf jeder Seite 1/2,
aber:
Vollständige Korrelation der Paare:
Für jedes Paar und jeden Winkel gilt: Entweder passieren beide, oder beide werden absorbiert... ...auch wenn Festlegung des Winkels so spät erfolgt, dass Kommunikation zwischen den Teilchen schneller als Lichtgeschwindigkeit c erfolgen müßte (aktuell : Mehr als $10.000 \cdot c$, zitiert nach Wikipedia, Quantenverschränkung).

Mögliche Erklärungen:

1. Einstein's Erklärung für diese „spukhafte Fernwirkung“ (spooky action at a distance): Es gibt „verborgene Variablen“ in den Teilchenpaaren, die die Meßergebnisse für jeden Winkel α bereits beim Abflug festlegen.
   Er meinte: Quantenmechanik muß um diese verborgenen Variablen erweitert werden (Einstein-Podolsky-Rozen, EPR, 1935).

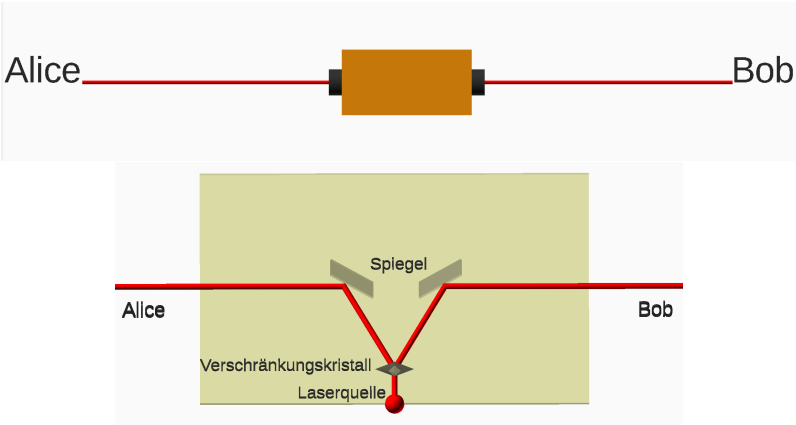
2. Interpretation der Quantenmechanik: Es steht nicht von vornherein fest, ob die Teilchen passieren werden oder nicht - das ist echter Zufall. Aber wenn Alice misst, und ihr Teilchen die Polarisation in Richtung α (oder $\alpha^{\perp}$ annimmt, nimmt Bobs Teilchen INSTANTAN, also in diesem Moment, dieselbe Polarisation an. Messen in Richtung α liefert also zwangsweise dasselbe Ergebnis.

   Das klingt absurd, wie sollen die beiden mit Überlichgeschwindigkeit kommunizieren?

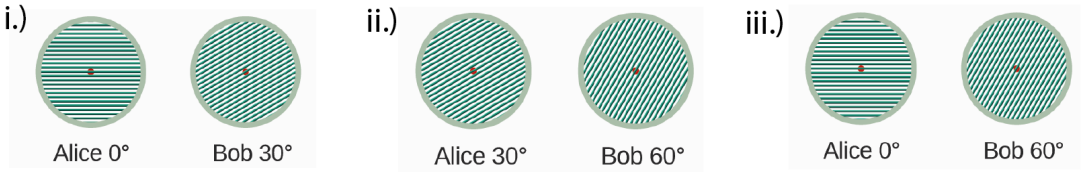
   Für ein einzelnes Teichen bedeutet es auch: Nicht-Realismus:
   Ein einzelnes Teilchen hat für die Winkel α ungleich $0°, 90°, 180°$ und $270°$ nicht einen der Zustände „passiert“ oder „wird absorbiert“, sondern beide gleichzeitig. Erst mit der Messung nimmt es einen der Zustände an, und schwingt dann im Winkel α bzw. $\alpha + 90°$. (Vergleich Wähler, Schrödinger's Katze).

   Für die Interaktion zwischen den Teilchen bedeutet es: Nicht-Lokalität:
   Die Messung eines Teilchens eines verschränkten Teilchenpaares ändert instantan die Polarisation des anderen.

Versuch 3: Zwei (wie in Versuch 2) verschränkte QBits werden ausgesendet.



Gemessen werden sie erst von A zufällig in $0°$ oder $30°$ gemessen, dann sofort von B in Richtung $30°$ oder $60°$ - so schnell, das Kommunikation mit Geschwindigkeit zwischen dem Ort von A und dem Ort von B in Geschwindigkeit $\leq c$ unmöglich ist. Versuchsergebnisse, bei denen beide in Richtung $30°$ gemessen haben, werden nicht weiter betrachtet (diese wurden ja schon in Versuch 2 behandelt). Folgende Messungen werden also durchgeführt:



Um zu sehen, ob die Quantenmechanik mit der spukhaften Fernwirkung recht hat, oder ob es verborgene Variablen gibt, wird die dann folgende Frage gestellt:

Frage: Welcher Anteil der Messungen beantwortet die folgende Auswertung mit „ja“?

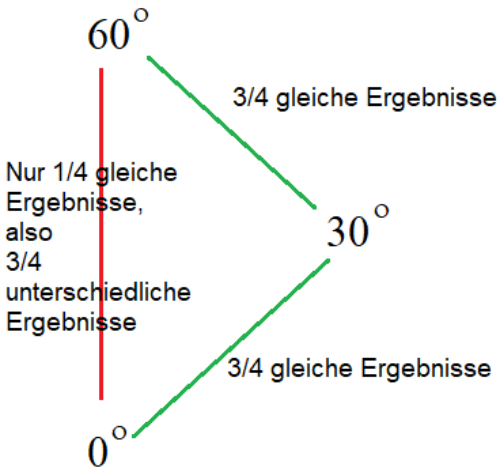
- Wenn Alice bei 0 Grad und Bob bei 30 Grad gemessen hat, sind dann die Ergebnisse beider Messungen gleich?
- Ansonsten, wenn Alice bei 30 Grad und Bob bei 60 Grad gemessen hat, sind dann die Ergebnisse beider Messungen gleich?
- Ansonsten, wenn also Alice bei 0 Grad und Bob bei 60 Grad gemessen hat, sind dann die Ergebnisse beider Messungen verschieden?

Idee hinter der Frage: Quantentheorie besagt (wobei „die meisten“ hier „ein Anteil von 3/4“ bedeutet, aber lassen wir es für das Verständnis der Idee zunächst bei „die meisten“):

i.) Misst Alice bei 0 und Bob bei 30, sind „die meisten“ Ergebnisse gleich.

ii.) Misst Alice bei 30 und Bob bei 60, sind „die meisten“ Ergebnisse gleich.

iii.) Misst Alice bei 0 und Bob bei 60, sind „die meisten“ Ergebnisse unterschiedlich.

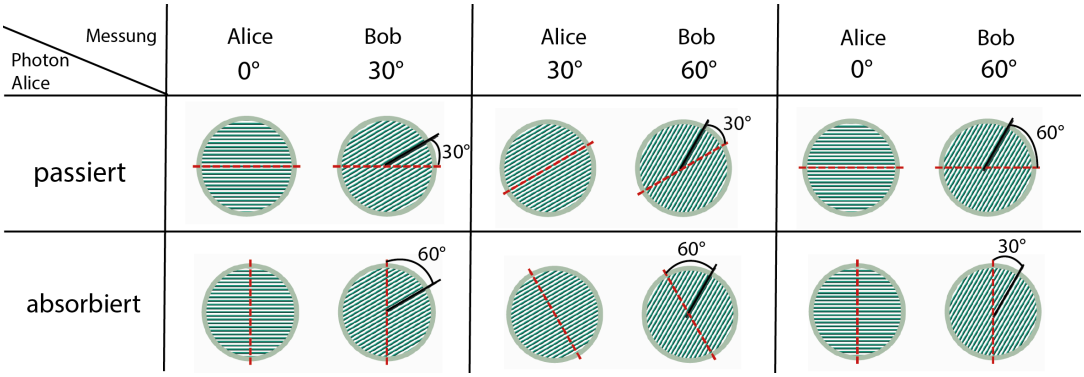


Aber wenn es verborgene Variablen gibt, die bei 0° und 30° „meistens“ die gleichen Ergebnisse liefern, und bei 30° und 60° „meistens“ die gleichen Ergebnisse liefern, so müssen sie auch bei 0° und 30° „meistens von meistens“ - also immer noch oft - die gleichen Ergebnisse liefern.

Ergebnis (Quantentheorie + Experiment):
Im Experiment wird die Frage wird nach Versuch 3 insgesamt statistisch in 3/4 aller Fälle mit „ja“ beantwortet.

Zunächst wird gezeigt, dass sich das perfekt mit der quantenmechanischen Interpretation deckt.

Folgende Messergebnisse sind theoretisch möglich:



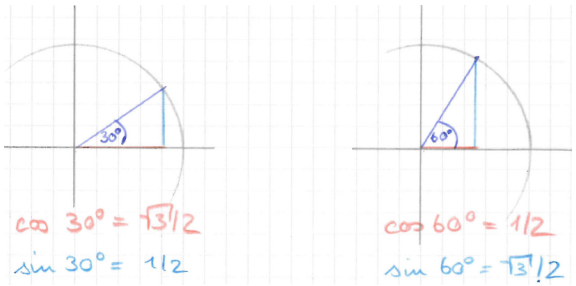
- Bei Bob geschieht im Experiment, bei den verschiedenen Messungen, folgendes:

  Ist der Differenzwinkel zu Alices Messung 30° (also, wenn er bei 0° und Alice bei 30° gemessen hat, oder wenn er bei 30° und Alice bei 60° gemessen hat), so verhält sich ein statistischer Anteil von 3/4 genauso wie das QBit bei Alice. D.h., bei 3/4 der Paare passieren beide oder werden beide absorbiert. Bei 1/4 der Paare verhalten sich beide QBits unterschiedlich.

  Ist der Differenzwinkel zu Alices Messung 60° (also, wenn Bob bei 0° und Alice bei 60° gemessen hat), so verhält sich ein statistischer Anteil von 3/4 anders als das QBit bei Alice. D.h., bei 3/4 der Paare passiert das QBit bei Alice und das bei Bob wird absorbiert, oder umgekehrt. Bei 1/4 der Paare verhalten sich beide QBits gleich.

- Diese Beobachtung wird durch die Quantenmechanische Interpretation perfekt erklärt. Denn wenn mit der Messung bei Alice das QBit von Bob die Polarisation von Alices QBit annimmt, und dann im Differenzwinkel von 30° gemessen wird, wird es sich mit Wahrscheinlichkeit $\cos^2 30° = 3/4$ genauso verhalten wie das QBit von Alice. Ist der Differnezwinkel 60°, so wird es sich mit Wahrscheinlichkeit $\cos^2 30° = 3/4$ entgegengesetzt zum QBit von Alice verhalten. (→ unten [1]für die Erinnerung an sin und cos)

[1]Erinnerung sin und cos beteiligte Winkel:



Wenn die Quantenmechanik um verborgene Variablen erweitert werden kann, müssten die diesen statistischen Effekt irgendwie erklären .... aber es gibt keine:

Satz, John Bell 1964: Erweiterung Quantenmechanik um verborgene Variablen ist nicht möglich.

Beweis: Wir nehmen an, jedes QBit-Paar „weiß“ bereits bei Abflug für jeden Winkel, ob es passieren wird, oder absorbieren wird. Dann sind die verborgenen Variablen für jedes QBit-Paar eine der folgenden 8 Möglichkeiten:

0 Grad	30 Grad	60 Grad
absorbiert	absorbiert	absorbiert
absorbiert	absorbiert	passiert
absorbiert	passiert	absorbiert
absorbiert	passiert	passiert
passiert	absorbiert	absorbiert
passiert	absorbiert	passiert
passiert	passiert	absorbiert
passiert	passiert	passiert

Wir fragen für jede Belegung, ob die Messergebnisse für Alice und Bob gleich (bei einem Differenzwinkel von 30°) oder unterschiedlich (bei einem Differenzwinkel von 60° sind. Das ist einfach hinzuschreiben:

0 Grad	30 Grad	60 Grad	Alice 0 Bob 30 Ergebnisse gleich?	Alice 30 Bob 60 Ergebnisse gleich?	Alice 0 Bob 60 Ergebnisse verschieden?
absorbiert	absorbiert	absorbiert	ja	ja	nein
absorbiert	absorbiert	passiert	ja	nein	ja
absorbiert	passiert	absorbiert	nein	nein	nein
absorbiert	passiert	passiert	nein	ja	ja
passiert	absorbiert	absorbiert	nein	ja	ja
passiert	absorbiert	passiert	nein	nein	nein
passiert	passiert	absorbiert	ja	nein	ja
passiert	passiert	passiert	ja	ja	nein

Man sieht:

- Sind die verborgenen Variablen fest, und wird die Messung von Alice und Bob unabhängig davon festgelegt, so ist die Wahrscheinlichkeit, dass die Frage mit „ja“ beantwortet wird, in allen Fällen höchstens 2/3.
- Das macht einen - wie auch immer gewichteten - statistischen Mittelwert von 3/4 unmöglich.

- Die Quantenmechanik, die die beobachteten Versuchsergebnisse erklärt, kann also nicht um verborgene Variablen ergänzt werden.
- Die Versuchsergebnisse können, wenn die Messungen unabhängig von den Photonen selbst festgelegt wurden, nicht durch verborgene Variablen erklärt werden.

Folgerung: Welt ist nicht „lokal“ oder nicht „realistisch“ (Begriffe aus EPR-Arbeit):

- lokal: Nichts (auch keine Information) bewegt sich schneller als c.
- realistisch: Eigenschaften physikalische Objekte stehen fest, unabhängig davon, ob sie jemand wahr nimmt.

Bemerkung:

i.) Für die Formulierung der „Bell’schen Ungleichung“ und den Nachweis, dass die Quantenmechanik sie verletzt, wurde John Bell 1990 für den Physik-Nobelpreis nominiert (verstarb leider vor der Entscheidung). Die Bell’sche Ungleichung verallgemeinert den oben beschriebenen Versuchsaufbau auf beliebige Winkel (siehe Wikipedia-Artikel dazu, sehr gut verständlich).

ii.) Experiment zum Nachweis der Verletzung der Bell’schen Ungleichung gibt es seit Ende der 1960 er Jahre. Es werden immer noch welche gemacht.

iii.) Viel Arbeit auf dem Weg vom idealisierten Experiment zum tatsächlichen (sogenannte „Schlupflöcher“ stopfen).

iv.) Man akzeptiert schließlich: QBits können sich mit Überlichtgeschwindigkeit absprechen. Und es ist nicht sinnvoll, von einem einzelnen QBit zu sprechen - QBits müssen als System betrachtet werden.
Das hat die Informatiker auf den Plan gerufen. Denn Systeme, die sich selbst organisieren können, haben ganz andere Möglichkeiten als einzelne Objekte, die von außen einzeln gesteuert werden können.

2.2 Informatik: Das Berechnungsmodell

2.2.1 Quantenregister

Lernziele:

i.) Wissen, was ein (informatisches) Quantenbit ist (algebraische Darstellung + graphische Darstellung).

ii.) Wissen, was ein Quantenregister aus n QBits ist (algebraische Darstellung als Summe von Basiszuständen, graphische Darstellung für $n \leq 3$, und Darstellung als Koeffizientenvektor z.B. für Matlab).

iii.) Zustände von Quantenregistern aus unverschränkten QBits berechnen können.

iv.) Den Unterschied zwischen verschränkten und unverschränkten Registerzuständen kennen.

v.) Wissen, was herauskommt, wenn man ein oder mehrere QBits in einem Quantenregister mißt (ausrechnen können, und graphische Vorstellung haben).

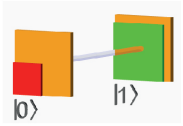
Definition: Ein QBit $|q\rangle$ ist ein Objekt mit Zustand $\beta_0 \cdot |0\rangle + \beta_1 \cdot |1\rangle$ mit $\beta_0, \beta_1 \in \mathbb{C}$ (in dieser Vorlesung praktisch immer: $\beta_0, \beta_1 \in \mathbb{R}$) und $|\beta_0|^2 + |\beta_1|^2 = 1$. $|0\rangle$ und $|1\rangle$ heißen Basiszustände. β_0 und β_1 heißen Wahrscheinlichkeitsamplituden.

Messen des QBits liefert mit Wahrscheinlichkeit $|\beta_0|^2$ den Basiszustand $|0\rangle$ und mit Wahrscheinlichkeit $|\beta_1|^2$ den Basiszustand $|1\rangle$. Nach dem Messen ist das QBit im entsprechenden Basiszustand.

Spielerei in der Vorlesung: Jeder „ist“ jetzt ein QBit und macht sich klar, was passiert, wenn jemand kommt und ihn/sie mißt.

Bemerkung : Graphische Vorstellung des QBits $\beta_0 \cdot |0\rangle + \beta_1 \cdot |1\rangle$:
Verbinde zwei Einheitsquadrate mit einer Linie. Bezeichne eines mit $|0\rangle$, das andere mit $|1\rangle$. Zeichne in das Quadrat mit Bezeichnung $|0\rangle$ ein Quadrat mit Seitenlänge $|\beta_0|$, in das Quadrat mit Bezeichnung $|1\rangle$ ein Quadrat mit Seitenlänge $|\beta_1|$ Quadrate grün bei positivem β, rot bei negativem β.

Beispiel für das QBit $-0.5 \cdot |0\rangle + \sqrt{3/4} \cdot |1\rangle$ (drei unterschiedliche Darstellungen - die Anordnung im Raum spielt im Moment noch keine Rolle):

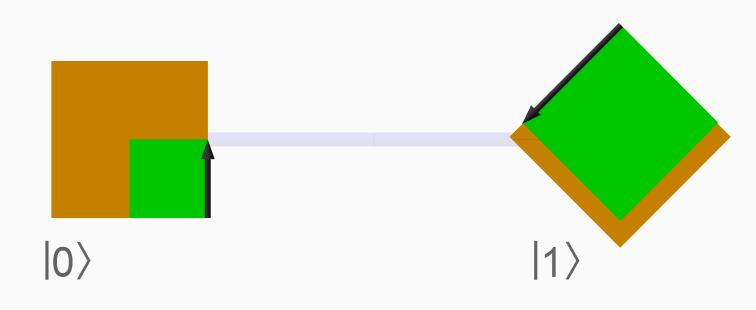


.

Messen liefert einen der Zustände, das Quadrat ist dann komplett rot oder grün (kommt später nochmal).

Bemerkung: Graphische Vorstellung des QBits $\beta_0 \cdot |0\rangle + \beta_1 \cdot |1\rangle$, wenn β_0 und $\beta_1$komplexe Zahlen sind (in Anlehnung an Feynmans QED):
Keine Farben notwendig. Die Einheitsquadrate können jetzt gedreht sein.

Beispiel für das QBit $0.5 \cdot e^{i\pi/2} \cdot |0\rangle + \sqrt{3/4} \cdot e^{i \cdot 5/4\pi} \cdot |1\rangle$:



.

Definition: Ein Quantenregister $|q_1 q_2 \cdots q_n\rangle$ mit n QBits $|q_1\rangle, |q_2\rangle, \cdots, |q_n\rangle$ ist ein Objekt mit Zustand

$$\begin{array}{rrl} & \alpha_0 & \cdot|0\,0\,\cdots\,0\,0\rangle \\ + & \alpha_1 & \cdot|0\,0\,\cdots\,0\,1\rangle \\ & \vdots & \\ + & \alpha_{2^n-1} & \cdot|1\,1\,\cdots\,1\,1\,\rangle \end{array}$$

mit $\alpha_0, \cdots, \alpha_{2^n-1} \in \mathbb{C}$ (hier meist: $\in \mathbb{R}$), wobei $|\alpha_0|^2 + \cdots + |\alpha_{2^n-1}|^2 = 1$.

Die Zustände $|0\ \cdots\ 0\,0\rangle, |0\ \cdots\ 0\,1\rangle, \cdots, |1\ \cdots\ 1\,1\rangle$ heißen Basiszustände des Registers, die Koeffizienten $\alpha_0, \cdots, \alpha_{2^n-1}$ (Wahrscheinlichkeits)-Amplituden der Basiszustände. (Erinnert an die Wertetabelle einer booleschen Funktion mit n Inputs.)

Schreibweise:

$$\begin{aligned} |0\ \cdots\ 0\,0\rangle &:= |0\rangle \cdot |0\rangle \cdot |0\rangle \cdot \cdots \cdot |0\rangle \\ |0\ \cdots\ 0\,1\rangle &:= |0\rangle \cdot |0\rangle \cdot \cdots \cdot |0\rangle \cdot |1\rangle \\ &\vdots \\ |1\ \cdots\ 1\,1\rangle &:= |1\rangle \cdot \cdots \cdot |1\rangle \end{aligned}$$

Nicht kommutative Multiplikation.

Beispiele:

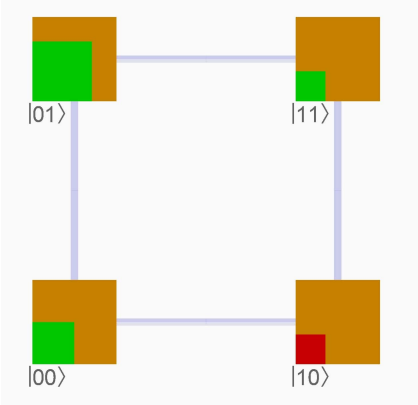
$n = 2$

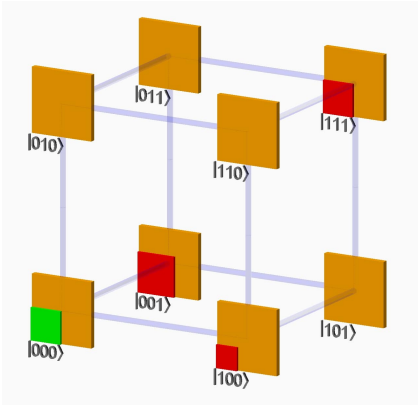
$$\begin{aligned}|q_1\ q_2\rangle &= \frac{1}{2}\cdot|00\rangle + \frac{1}{\sqrt{2}}\cdot|01\rangle - \frac{1}{\sqrt{8}}\cdot|10\rangle + \frac{1}{\sqrt{8}}\cdot|11\rangle \\ &\approx 0.5\cdot|00\rangle + 0.707\cdot|01\rangle - 0.354\cdot|10\rangle + 0.354\cdot|11\rangle.\end{aligned}$$

$n = 3$

$$\begin{aligned}|q_1\ q_2\ q_3\rangle =& \frac{1}{2}\cdot|000\rangle - \frac{\sqrt{3}}{\sqrt{8}}\cdot|001\rangle + 0\cdot|010\rangle + 0\cdot|011\rangle \\ &- \frac{1}{\sqrt{8}}\cdot|100\rangle + 0\cdot|101\rangle + 0\cdot|110\rangle - \frac{1}{2}\cdot|111\rangle \\ &\approx 0.5\cdot|000\rangle - 0.612\cdot|001\rangle - 0.354\cdot|100\rangle - 0.5\cdot|111\rangle.\end{aligned}$$

Graphische Darstellung: Quantenregister mit n QBits wird in n-dimensionalen Würfel dargestellt, mit jeweils Einheitsquadrat in den Ecken, darin Quadrate mit Seitenlänge der Wahrscheinlichkeitsamplituden (und somit Fläche der Wahrscheinlichkeiten).
Jedes QBit ist für eine Richtung zuständig:
Das erste QBit für links-rechts, das zweite QBit für unten-oben, das dritte für vorne-hinten.
Die Beispiele von oben werden wie folgt graphisch dargestellt:

$n = 2$: 

$n = 3$: 

.

Darstellung als Koeffizientenvektor: Oft (z.B. in Matlab) wird der Zustand

$$\begin{aligned} & \alpha_0 \cdot|0\,0\,\cdots\,0\,0\rangle \\ + \quad & \alpha_1 \cdot|0\,0\,\cdots\,0\,1\rangle \\ & \vdots \\ + \quad & \alpha_{2^n-1} \cdot|1\,1\,\cdots\,1\,1\,\rangle \end{aligned}$$

eines Quantenregisters einfach als Koeffizientenvektor dargestellt:

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{2^n-1} \end{pmatrix}$$

(Diesen Vektor kann man dann mit einer $2^n \times 2^n$-Matrix von links multiplizieren).

Verkürzte Darstellung des Zustandes als Summe: Schreibweisen alternativ:
Wenn QBits von 0 bis n-1 nummeriert sind:

$$|q_{n-1}\cdots q_1 q_0\rangle = \sum_{i=0}^{2^n-1} \alpha_i|i\rangle \qquad \text{oder auch} \qquad |q_1\cdots q_n\rangle = \sum_{i=0}^{2^n-1} \alpha_i|i\rangle$$

Hier ist für jedes $j \in \{1\cdots n\}$ das j-te Bit eines Basiszustandes $|i\rangle$ das an j-ter Stelle von links in der n-stelligen Binärdarstellung von i. Man sieht die Ähnlichkeit zur Darstellung eines Vektors als Koeffizientenvektor, oder als Linearkombination der Basisvektoren.

Definition: Der Zustand $|q_1\ q_2\ \cdots\ q_n\rangle$ heißt unverschränkt (engl: unentangled), wenn er durch Ausmultiplizieren eines Produktes

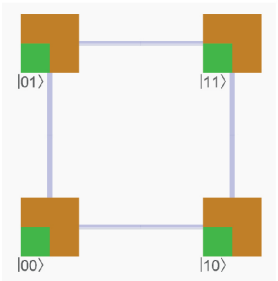
$$\underbrace{(\beta_{1,0}|0\rangle + \beta_{1,1}|1\rangle)}_{Zustand\ QBit\ 1} \cdot \underbrace{(\beta_{2,0}|0\rangle + \beta_{2,1}|1\rangle)}_{Zustand\ QBit\ 2} \cdot \ \cdots\ \cdot \underbrace{(\beta_{n,0}|0\rangle + \beta_{n,1}|1\rangle)}_{Zustand\ QBit\ n}$$

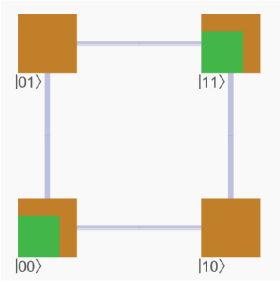
entsteht.
Ansonsten heißt der Zustand verschränkt (engl. entangled)

Beispiel: $n = 2$: Die Registerzustände bei den beiden QBits aus Experiment 1 und Experiment 2 des letzten Kapitels:

Experiment 1: $|q_1\ q_2\rangle = 0.5 \cdot |00\rangle + 0.5 \cdot |01\rangle + 0.5 \cdot |10\rangle + 0.5 \cdot |11\rangle$

Experiment 2: $|q_1\ q_2\rangle = \sqrt{0.5} \cdot |00\rangle + 0 \cdot |01\rangle + 0 \cdot |10\rangle + \sqrt{0.5} \cdot |11\rangle$.





Beispiel: $n = 3$

$$\begin{aligned}(\beta_0|0\rangle + \beta_1|1\rangle) \cdot (\gamma_0|0\rangle + \gamma_1|1\rangle) \cdot (\delta_0|0\rangle + \delta_1|1\rangle) =& \beta_0\gamma_0\delta_0|000\rangle + \beta_0\gamma_0\delta_1|001\rangle \\ &+\beta_0\gamma_1\delta_0|010\rangle + \beta_0\gamma_1\delta_1|011\rangle \\ &+\beta_1\gamma_0\delta_0|100\rangle + \beta_1\gamma_0\delta_1|101\rangle \\ &+\beta_1\gamma_1\delta_0|110\rangle + \beta_1\gamma_1\delta_1|111\rangle\end{aligned}$$

unverschränkt.

Beispiel:

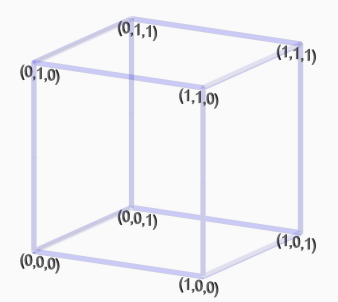
1. Drei „QBits“ berechnen ihren unverschränkten Zustand durch Ausmultiplizieren.
2. Drei „QBits“ „vereinbaren“ einen verschränkten Zustand, der nicht durch Ausmultiplizieren entsteht. Zum Beispiel:
$$\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{2}|101\rangle + \frac{1}{2}|111\rangle$$

Bemerkung: Ausmultiplikation von Zuständen von n QBits ergibt stets einen Zustand des Registers, also $|\alpha_0|^2 + \cdots + |\alpha_{2^n-1}|^2 = 1$ (Beweis Übungsaufgabe).

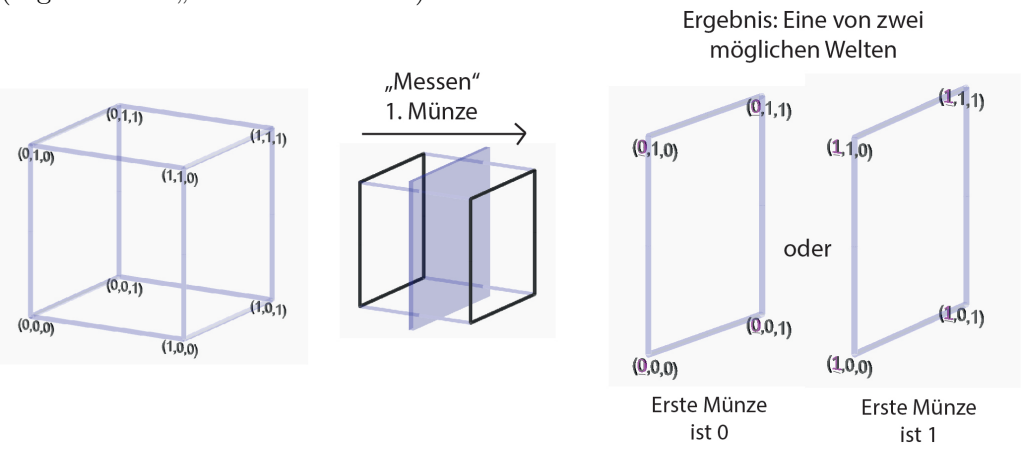
Wir haben: QBits und Register aus n QBits. Es folgt das **Messen** eines Bits in einem Register.

Vorüberlegung: „Messen“ im Zustandsraum eines Münzwurfs mit drei Münzen”:
„Messen“ bedeutet: Nachsehen, ob die Münze 0 oder 1 gezeigt hat.

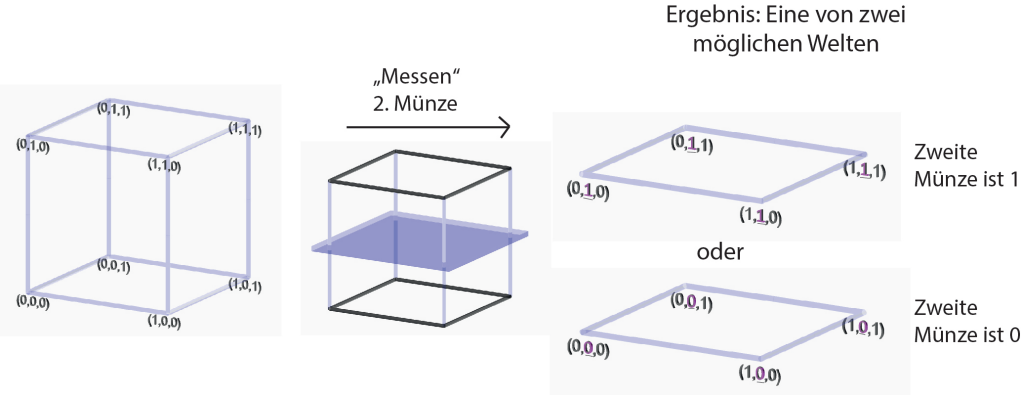
Der Zustandsraum eines Wurfes mit drei Münzen, graphisch dargestellt als Ecken eines Würfels.



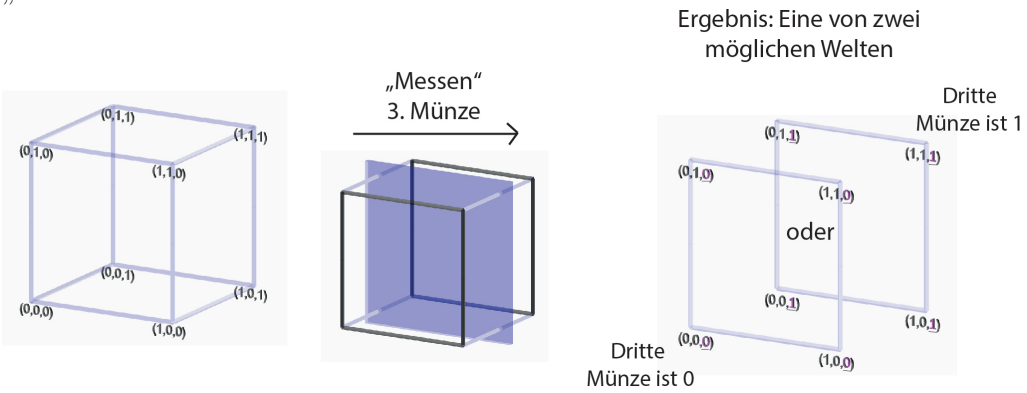
Die erste der drei Münzen wird angeschaut. Ergebnis ist eine von zwei möglichen Welten (sogenannten „Zustandsräumen“).



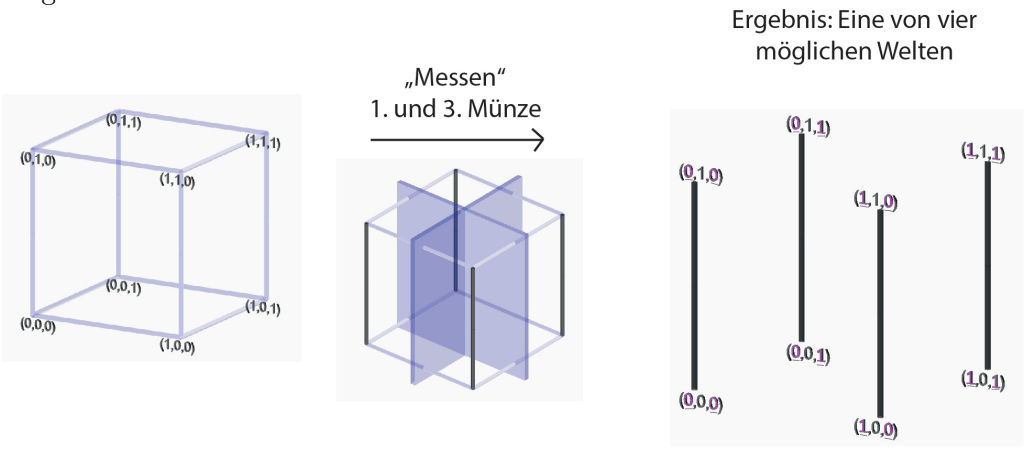
Die zweite der drei Münzen wird angeschaut. Ergebnis ist wieder eine von zwei möglichen Welten.



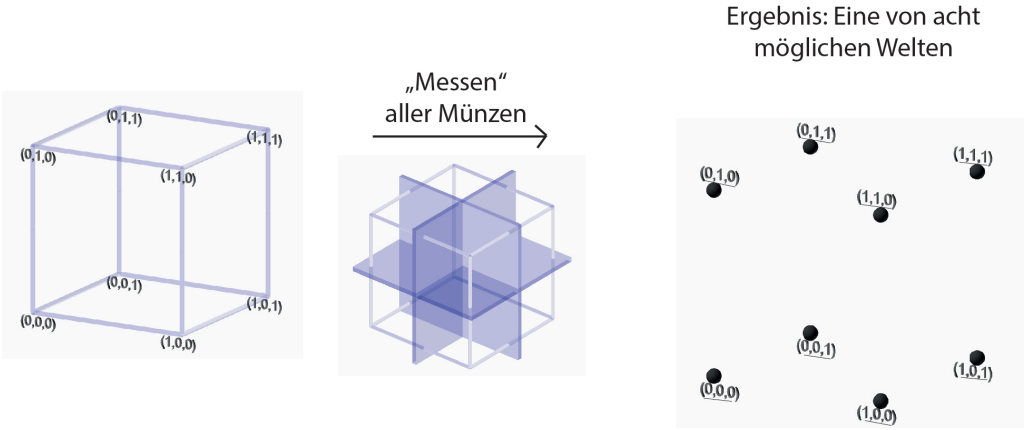
Die dritte der drei Münzen wird angeschaut. Ergebnis ist die vordere oder die hintere „Teilwelt“.



Die erste und dritte der drei Münzen werden angeschaut. Ergebnis ist eine von vier möglichen Welten.



Alle Münzen werden angeschaut. Ergebnis ist eine von acht Welten, es gibt keine Unsicherheit mehr.



Diese graphische Veranschaulichung des Messvorgangs wird auf die Situation übertragen, in der nicht Münzwürfe, sondern QBits in Quantenregistern gemessen werden.

Definition: Gegeben sei ein Register mit n QBits im Zustand $|q_1 \cdots q_n\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$.

Für $j \in \{1 \cdots n\}$ sei

$I_{j,0} = \{i \in \{0, \cdots, 2^n - 1\} :$ j-tes Bit von links in der Binärdarstellung von i ist$|0\rangle\}$

und

$I_{j,1} = \{0, \cdots, 2^n - 1\} \setminus I_{j,0}$

$= \{i \in \{0, \cdots, 2^n - 1\} :$ j-tes Bit von links in der Binärdarstellung von i ist$|1\rangle\}$

Wird das j-te Bit des Registers gemessen, so nimmt es mit Wahrscheinlichkeit $\sum_{i \in I_{j,0}} |\alpha_i|^2$ den Wert $|0\rangle$ an. Das Register ist dann im Zustand

$$\frac{\sum_{i \in I_{j,0}} \alpha_i |i\rangle}{\sqrt{\sum_{i \in I_{j,0}} |\alpha_i|^2}}$$

Beachte: alle $|i\rangle$, die hier vorkommen, haben an Position j eine $|0\rangle$.

Mit Wahrscheinlichkeit $\sum_{i \in I_{j,1}} |\alpha_i|^2$ nimmt es den Wert $|1\rangle$ an. Das Register hat dann den Zustand

$$\frac{\sum_{i \in I_{j,1}} \alpha_i |i\rangle}{\sqrt{\sum_{i \in I_{j,1}} |\alpha_i|^2}}$$

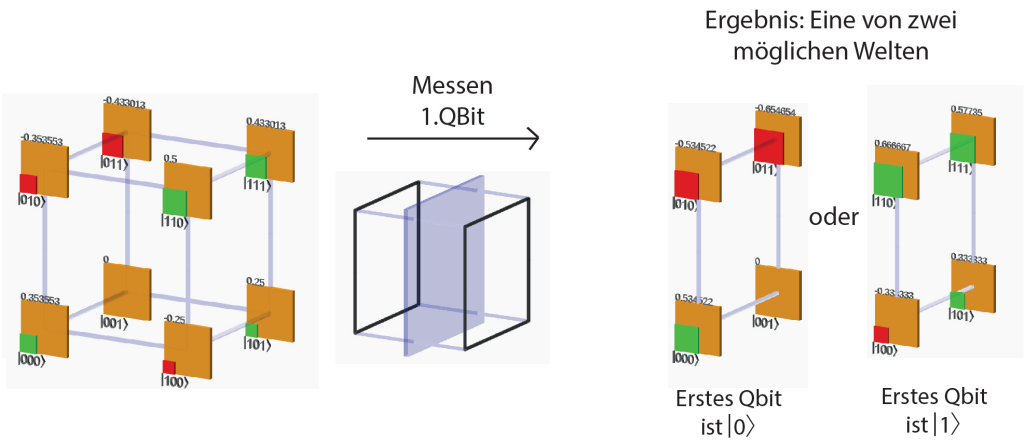
Beachte: alle $|i\rangle$, die hier vorkommen, haben an Position j eine $|1\rangle$.

Beispiel:

1.

$$\begin{aligned} |q_1\ q_2\ q_3\rangle &= \frac{\sqrt{2}}{4} \cdot |000\rangle + 0 \cdot |001\rangle - \frac{\sqrt{2}}{4} \cdot |010\rangle - \frac{\sqrt{3}}{4} \cdot |011\rangle \\ &\quad - \frac{1}{4} \cdot |100\rangle + \frac{1}{4} \cdot |101\rangle + \frac{1}{2} \cdot |110\rangle + \frac{\sqrt{3}}{4} \cdot |111\rangle. \end{aligned}$$

Das erste der drei QBits wird gemessen. Ergebnis ist eine von zwei Welten.



Messen des ersten QBits liefert das Ergebnis $|0\rangle$ mit Wahrscheinlichkeit

$$\frac{2}{16} + 0 + \frac{2}{16} + \frac{3}{16} = \frac{7}{16}.$$

Das Quantenregister ist dann in einem Zustand, der in der graphischen Darstellung der linken Seite des Würfels entspricht: das erste QBit ist hier $|0\rangle$. Die kleinen Quadrate in dieser Welt behalten ihre Farbe bei. Ihre Größe wird angepasst, damit die Flächensumme der kleinen Quadrate wieder 1 ergibt. Das wird durch Multiplikation der Flächen mit $16/7$ erreicht, also durch Multiplikation der Kantenlängen mit $\sqrt{16/7}$.
(Es handelt sich um ein Rechnen mit bedingten Wahrscheinlichkeiten, wobei für Quanten jede Wahrscheinlichkeit aus einer Wahrscheinlichkeitsamplitude kommt.)

Das Quantenregister ist also in dem Fall, dass das erste QBit das Messergebnis $|0\rangle$ ergab, im Zustand

$$\begin{aligned} |q_1\ q_2\ q_3\rangle &= \sqrt{\frac{16}{7}} \cdot \left(\frac{\sqrt{2}}{4} \cdot |000\rangle + 0 \cdot |001\rangle - \frac{\sqrt{2}}{4} \cdot |010\rangle - \frac{\sqrt{3}}{4} \cdot |011\rangle \right) \\ &= \frac{\sqrt{2}}{\sqrt{7}} \cdot |000\rangle + 0 \cdot |001\rangle - \frac{\sqrt{2}}{\sqrt{7}} \cdot |010\rangle - \frac{\sqrt{3}}{\sqrt{2}} \cdot |011\rangle. \end{aligned}$$

Mit Wahrscheinlichkeit $9/16$ liefert Messen des ersten QBits das Ergebnis $|1\rangle$. Das Quantenregister ist dann in einem Zustand, der in der graphischen Darstellung der rechten Seitenfläche des Würfels entspricht.

Der Zustand ist (nach Multiplikation der Wahrscheinlichkeitsamplituden mit $\sqrt{16/9}$, um wieder auf eine Flächensumme von 1 zu kommen):

$$|q_1\ q_2\ q_3\rangle = \frac{1}{3} \cdot |100\rangle + \frac{1}{3} \cdot |101\rangle - \frac{2}{3} \cdot |110\rangle - \frac{\sqrt{3}}{3} \cdot |111\rangle.$$

2. $|q_1q_2q_3\rangle = \frac{1}{\sqrt{2}}\cdot\underbrace{|000\rangle}_{\alpha_0} + \frac{1}{2}\cdot\underbrace{|101\rangle}_{\alpha_5} + \frac{1}{2}\cdot\underbrace{|111\rangle}_{\alpha_7}$ gemessen wird QBit 2. Mit Wahrscheinlichkeit $(\frac{1}{\sqrt{2}})^2 + (\frac{1}{2})^2 = \frac{3}{4}$ nimmt QBit 2 den Wert $|0\rangle$ an. Das Register ist dann im Zustand

$$\begin{aligned}\frac{\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{2}\cdot|101\rangle}{\sqrt{\frac{3}{4}}} &= \frac{2}{\sqrt{3}\cdot\sqrt{2}}\cdot|000\rangle + \frac{1}{\sqrt{3}}|101\rangle \\ &= \sqrt{\frac{2}{3}}\cdot|000\rangle + \sqrt{\frac{1}{3}}|101\rangle\end{aligned}$$

   Mit Wahrscheinlichkeit $(\frac{1}{2})^2 = \frac{1}{4}$ nimmt QBit 2 den Wert $|1\rangle$ an. Das Register ist dann im Zustand $\frac{\frac{1}{2}|111\rangle}{\sqrt{(\frac{1}{2})^2}} = |111\rangle$.

3. Eigene Beispiele, verschränkte und unverschränkte Zustände, ein Bit messen.

Definition: Messen mehrerer QBits bedeutet: Nacheinander die Bits messen. Die Reihenfolge ist für das Ergebnis unerheblich (→Übungsaufgabe), das Ergebnis also wohldefiniert.

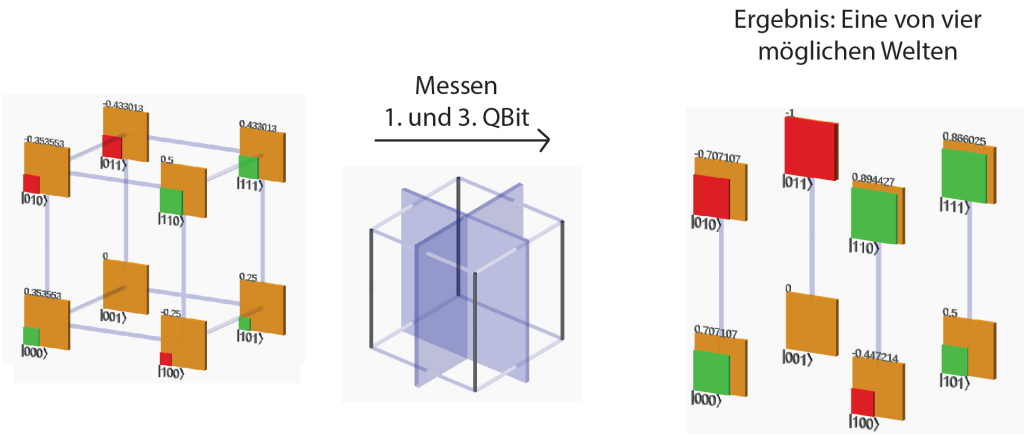
Bemerkung: Übungsaufgabe technisch schwer. Verständnis der Aussage aber wichtig für weitere Vorlesung, Verständnis kann man auch mit Beispielen erreichen, vielleicht auch mit Programmierung. Zum Messen von Beispielen gibt es auch Übungsaufgaben.

Beispiel:

i.) Beispiel von oben:

$$\begin{aligned}|q_1\ q_2\ q_3\rangle \quad = \quad & \frac{\sqrt{2}}{4}\cdot|000\rangle + 0\cdot|001\rangle - \frac{\sqrt{2}}{4}\cdot|010\rangle - \frac{\sqrt{3}}{4}\cdot|011\rangle \\ & - \frac{1}{4}\cdot|100\rangle + \frac{1}{4}\cdot|101\rangle + \frac{1}{2}\cdot|110\rangle + \frac{\sqrt{3}}{4}\cdot|111\rangle.\end{aligned}$$

Das erste und dritte QBit wird gemessen. Es gibt vier mögliche Ergebnisse.



- Mit Wahrscheinlichkeit 1/4 sind beide QBits $|0\rangle$.
  Das Register ist dann im Zustand $\sqrt{1/2} \cdot |000\rangle + \sqrt{1/2} \cdot |010\rangle$.
- Mit Wahrscheinlichkeit 3/16 ist das erste QBit $|0\rangle$, und das dritte $|1\rangle$.
  Das Register ist dann im Zustand $0 \cdot |000\rangle + 1 \cdot |010\rangle$.
  (Hier gibt es also auch keine Unsicherheit mehr bezüglich des zweiten QBits, es ist stets im Zustand $|1\rangle$.)
- Mit Wahrscheinlichkeit 5/16 ist das erste QBit $|1\rangle$, und das dritte $|0\rangle$.
  Das Register ist dann im Zustand $\sqrt{1/5} \cdot |100\rangle + \sqrt{4/5} \cdot |110\rangle$.
- Mit Wahrscheinlichkeit 1/4 sind beide QBits $|1\rangle$.
  Das Register ist dann im Zustand $\sqrt{1/4} \cdot |101\rangle + \sqrt{3/4} \cdot |111\rangle$.

ii.) $|q_1 q_2 q_3\rangle = \frac{1}{\sqrt{2}} \cdot |000\rangle + \frac{1}{2}|100\rangle + \frac{1}{\sqrt{8}}|101\rangle + \frac{1}{\sqrt{8}}|111\rangle$.

Messen QBits $|q_1\rangle$ und $|q_3\rangle$ liefert:

mit Wahrscheinlichkeit $(\frac{1}{\sqrt{2}})^2 = \frac{1}{2} : |q_1\rangle = |q_3\rangle = |0\rangle$.

Zustand Register ist dann $|000\rangle$.

mit Wahrscheinlichkeit $(\frac{1}{2})^2 = \frac{1}{4} : |q_1\rangle = |1\rangle, |q_3\rangle = |0\rangle$.

Zustand Register ist dann $|100\rangle$.

mit Wahrscheinlichkeit $(\frac{1}{\sqrt{8}})^2 + (\frac{1}{\sqrt{8}})^2 = \frac{1}{4} : |q_1\rangle = |1\rangle, |q_3\rangle = |1\rangle$.

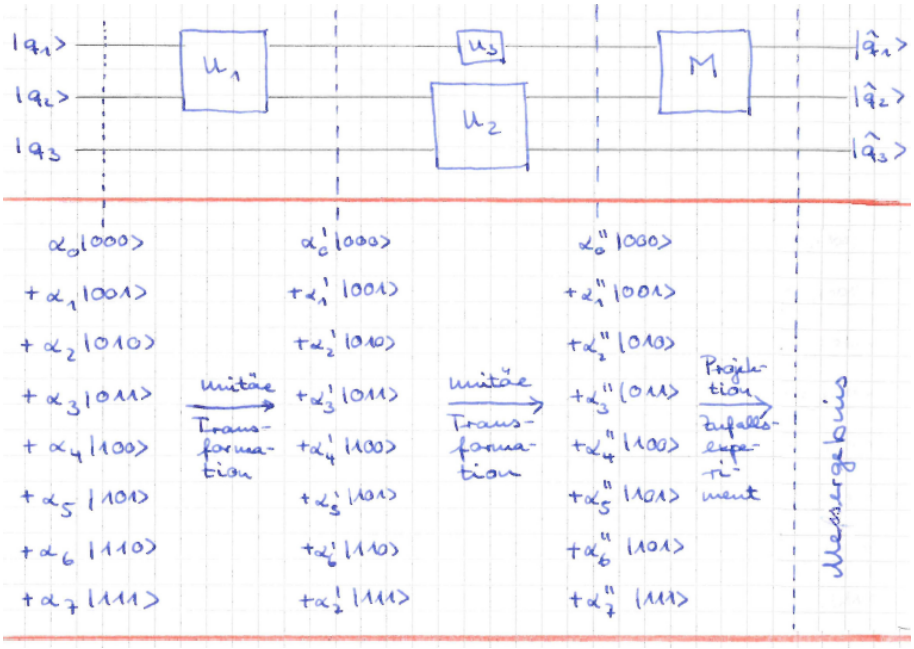
Zustand Register ist dann $\frac{1}{\sqrt{2}}|101\rangle + \frac{1}{\sqrt{2}}|111\rangle$.

Werden alle drei QBits gemessen, ist der Zustand des Registers ein Basiszustand. Hierfür gibt es acht Möglichkeiten:
$|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$ und $|111\rangle$. Die Wahrscheinlichkeit jeder Möglichkeit ist das Quadrat ihrer Wahrscheinlichkeitsamplitude.

2.2.2 Quantenalgorithmen, Quantenschaltkreise

Lernziele:

- Wissen, was unitäre Transformationen sind;
- Wissen, wie ein Quantenschaltkreis aussieht und analysiert wird, z.B.



- Übungsblatt 02 vollständig bearbeitetn können (und es bearbeiten :)).

Ende Lernziele.

Auf gehts.

Normalerweise ist die Reihenfolge ja

$$\text{Gatter} \longrightarrow \text{Schaltkreis} \longrightarrow \text{Algorithmus}.$$

Wir gehen umgekehrt vor, und machen zunächst einen Ausflug in die lineare Algebra.

Erinnerung Vektoren $b_1, \cdots, b_N \in \mathbb{R}^N (bzw. \mathbb{C}^N)$ heißen Basis des $\mathbb{R}^N$, wenn sie linear unabhängig sind. Jeder Vektor $v \in \mathbb{R}^N$ (bzw. $\mathbb{C}^N$) hat dann eine eindeutige Darstellung. $v = \sum_{i=1}^{N} \lambda_i b_i$, mit $\lambda_i \in \mathbb{R}$ (bzw. $\mathbb{C}$) für $i = 1, \cdots, N$.

Ende Erinnerung

Definition: Die Basis $b_1, \cdots, b_N \in \mathbb{R}^N$ (bzw. $\mathbb{C}^N$) heißt Orthogonalbasis, wenn für alle $1 \leq i, j \leq N$ mit $i \neq j$ gilt $b_i \perp b_j$, und heißt Orthonormalbasis, wenn zusätzlich $\|b_i\| = 1$ für $i = 1, \cdots, N$ gilt. Dabei ist $\|\cdot\|$ die euklidische Norm im $\mathbb{R}^N$ (bzw. $\mathbb{C}^N$).

Anschauung: Orthonormalbasen entstehen durch Drehungen/Spiegelungen aus der Standardbasis.

Definition: Die $N \times N$-Matrix $M = (m_{ij})_{1 \leq i,j \leq N}$ mit $m_{ij} \in \mathbb{R}$(bzw. $\mathbb{C}$) für $1 \leq i, j \leq N$ heißt unitär, wenn gilt: $M^{-1} = M^{*T}$.

Dabei: $M^{-1} \mathrel{\widehat{=}}$ Inverse, $M^T \mathrel{\widehat{=}}$ Transponierte, $M^* \mathrel{\widehat{=}}$ (elementweise) komplex konjugierte.

Beispiele unitärer Matrizen:

i.)
$$M = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$$

ii.)
$$M = \frac{1}{5} \cdot \begin{pmatrix} 3 & 4i \\ -4 & 3i \end{pmatrix}$$

iii.)
$$M = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

Bem.:

i.) M ist genau dann unitär, wenn die Zeilen (sowie die Spalten) eine Orthogonalbasis bilden.

ii.) Ist M unitär und $m_{ij} \in \mathbb{R}$, so ist $M^{-1} = M^T$.

Def.: Sei U eine unitäre Matrix. Dann heißt die lineare Abbildung

$U : \mathbb{R}^N \to \mathbb{R}^N$ bzw. U: $\mathbb{C}^N \to \mathbb{C}^N$ mit $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto U \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

unitäre Transformation.

Bem.: Unitäre Transformationen entsprechen Drehspiegelungen des Raumes.

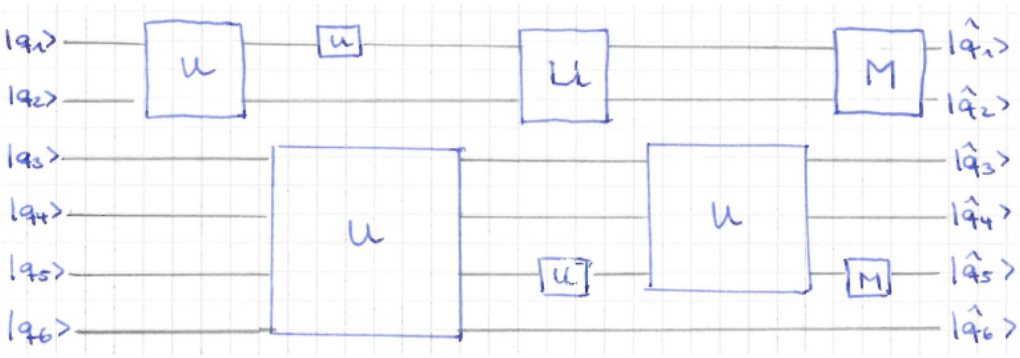
Def.: Der Zustandsraum: eines Quantenregisters mit QBits ist der von $|0\ldots0\rangle$,$|0\ldots01\rangle$, …, $|1\ldots1\rangle$ aufgespannte Vektorraum über $\mathbb{R}$ bzw. $\mathbb{C}$.
(Man überzeugt sich: Alle formalen Linearkombinationen $\sum_{i=0}^{2^n-1} \lambda_i \cdot |i\rangle$ die bilden einen Vektorraum.
Dabei meine $|i\rangle$ den Basiszustand, bei dem die Binärdarstellung von i innerhalb der $|.\rangle$ steht.
Man überzeugt sich auch: Nicht jeder Vektor im Zustandsraum ist ein möglicher Zustand. Nur Zustände, deren euklidische Länge 1 beträgt, können angenommen werden.)

Def.: Ein Quantenalgorithmus ist eine Folge von Quantenschaltkreisen (s. u.), wobei die unitären Transformationen aus Quantengattern kommen. (vgl. Sortieralgorithmen: Ein Schaltkreis für jedes n). Bem.: Die Def. wird später noch etwas erweitert.

Def.: Ein Quantenschaltkreis besteht aus :

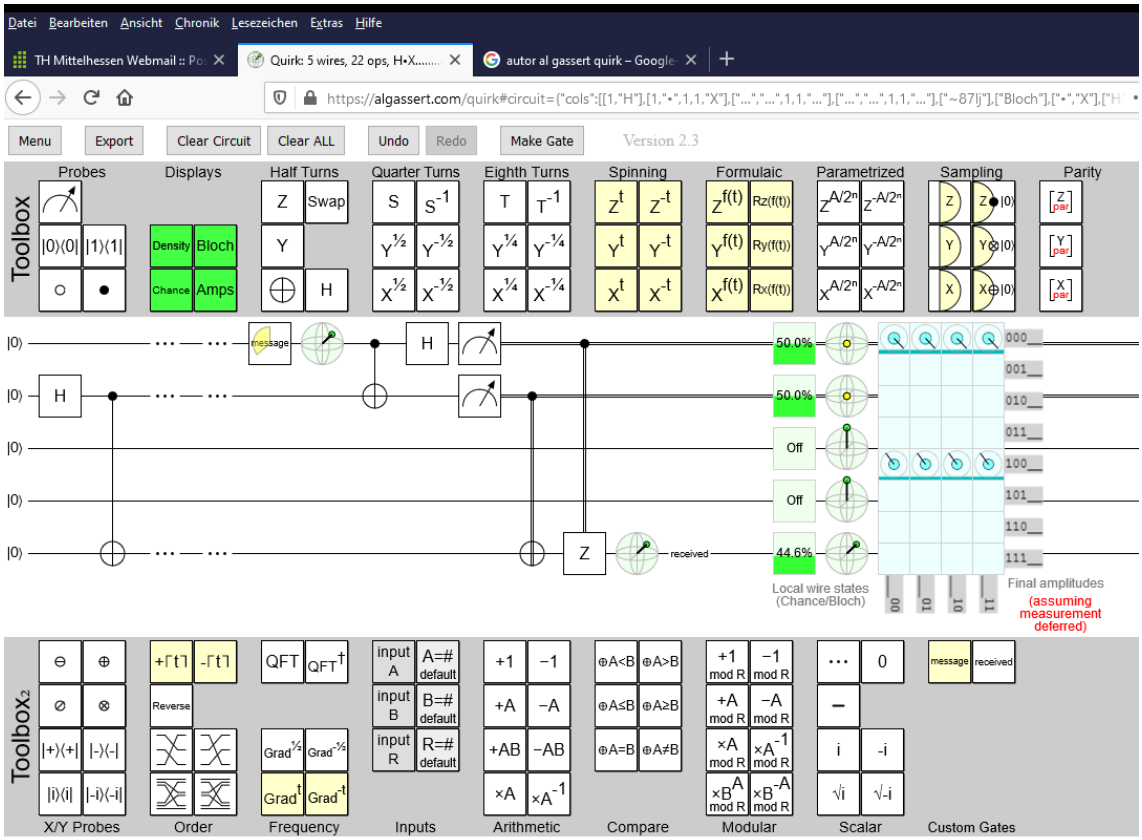
- Einem Input von n QBits, $n \in \mathbb{N}$
- Einem Output von n QBits, gemessen oder nicht
- Einer wohldefiniertem Folge aus unitären Transformationen des Zustandsraumes und am Schluß einer Messung von QBits.

Veranschaulichung (nur intuitiv, damit Sie ein Bild haben) $n = 6$

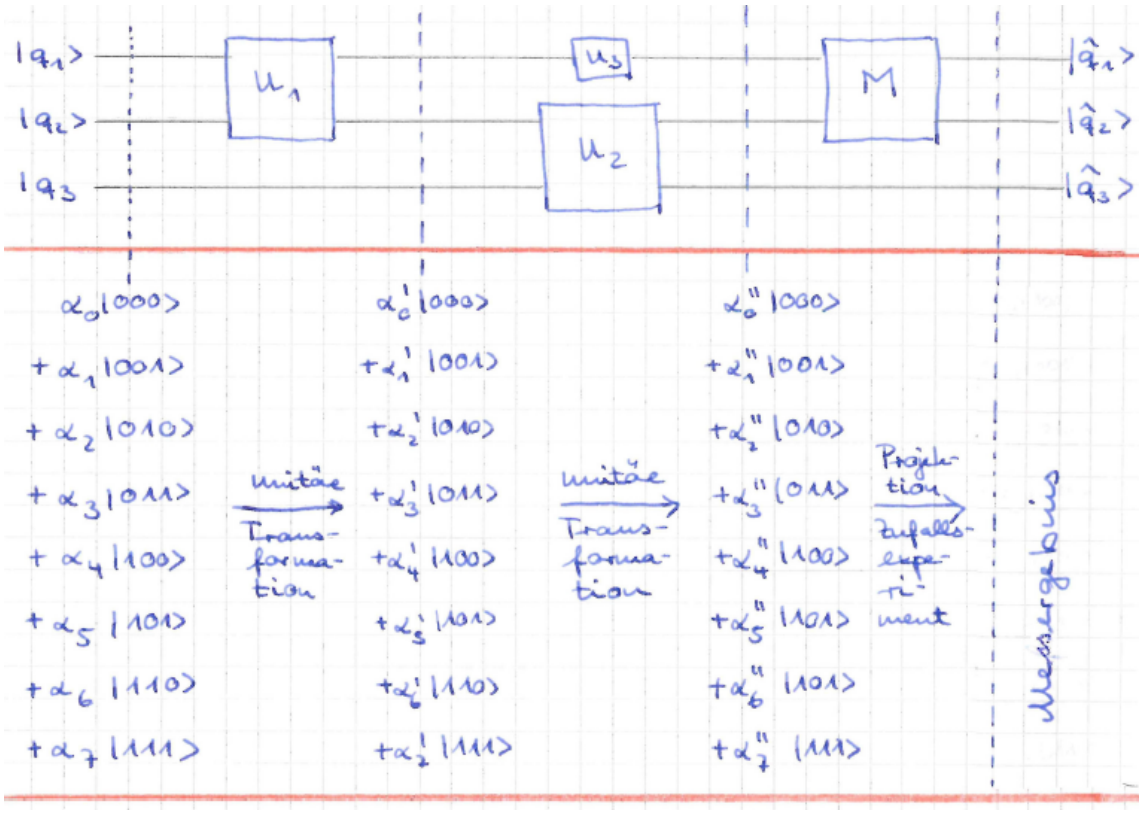


Bemerkung: Ein sehr schönes drag and drop open-source Tool, das direkt im Browser läuft, findet sich unter
https://algassert.com/quirk

So sehen die Quantenschaltkreise in quirk aus:


Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
TH Mittelhessen Webmail :: Po
Quirk: 5 wires, 22 ops, H•X.....
autor al gassert quirk – Google
https://algassert.com/quirk#circuit={"cols":[[1,"H"],[1,"•",1,1,"X"],["...","...",1,1,"..."],["...","...",1,1,"..."],["~87ij"],["Bloch"],["•","X"],["H
Menu
Export
Clear Circuit
Clear ALL
Undo
Redo
Make Gate
Version 2.3
Toolbox
Probes
Displays
Half Turns
Quarter Turns
Eighth Turns
Spinning
Formulaic
Parametrized
Sampling
Parity
Density
Bloch
Chance
Amps
Swap
message
received
50.0%
50.0%
Off
Off
44.6%
Local wire states (Chance/Bloch)
Final amplitudes (assuming measurement deferred)
Toolbox2
X/Y Probes
Order
Frequency
Inputs
Arithmetic
Compare
Modular
Scalar
Custom Gates
Reverse

Analyse von Quantenalgorithmen erfolgt im Zustandsraum Unitäre Transformationen, jeweils zwischen den gestrichelten Linien:



und :

$$\begin{pmatrix} \alpha_0' \\ \vdots \\ \alpha_7' \end{pmatrix} = \begin{pmatrix} \text{Matrix} \\ \text{zu} \\ U_1 \end{pmatrix} \cdot \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_7 \end{pmatrix}$$

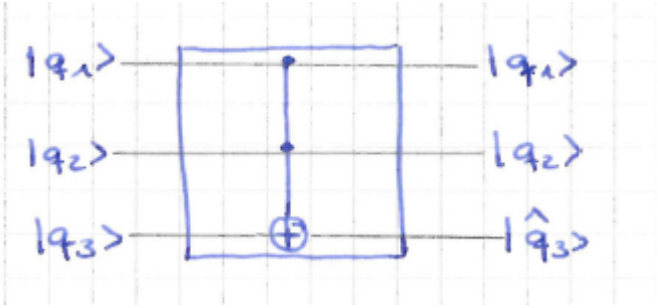
Dabei ist „Matrix zu U_1“ eine unitäre $2^3 \times 2^3$-Matrix.

$$\begin{pmatrix} \alpha_0'' \\ \vdots \\ \alpha_7'' \end{pmatrix} = \begin{pmatrix} \text{Matrix} \\ \text{zu } U_2 \\ \text{und gleichzeitig } U_3 \end{pmatrix} \cdot \begin{pmatrix} \alpha_0' \\ \vdots \\ \alpha_7' \end{pmatrix}$$

Dabei ist „Matrix zu U_1 und gleichzeitig zu U_2“ wieder eine unitäre $2^3 \times 2^3$-Matrix.

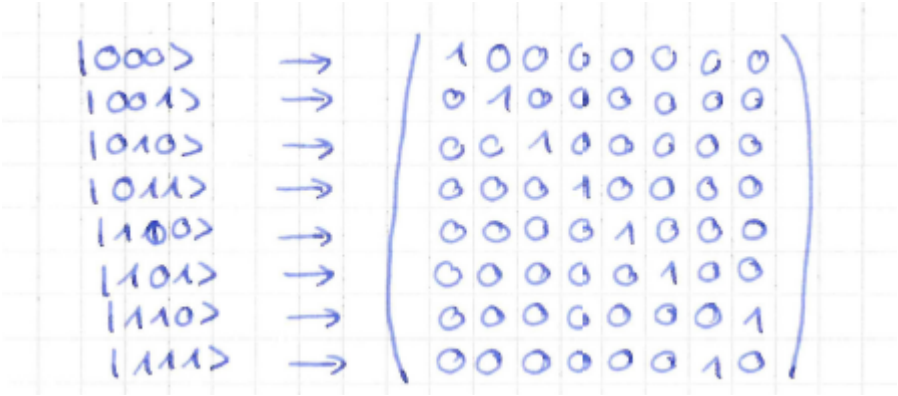
Um da ein Verständnis zu entwickeln ist üben, üben angesagt, und das tun wir jetzt(später macht es die Mathematik etwas einfacher, Stichwort „Tensoren“ für diejenigen, die sich auskennen).

Bsp: Das Toffoli-Gatter



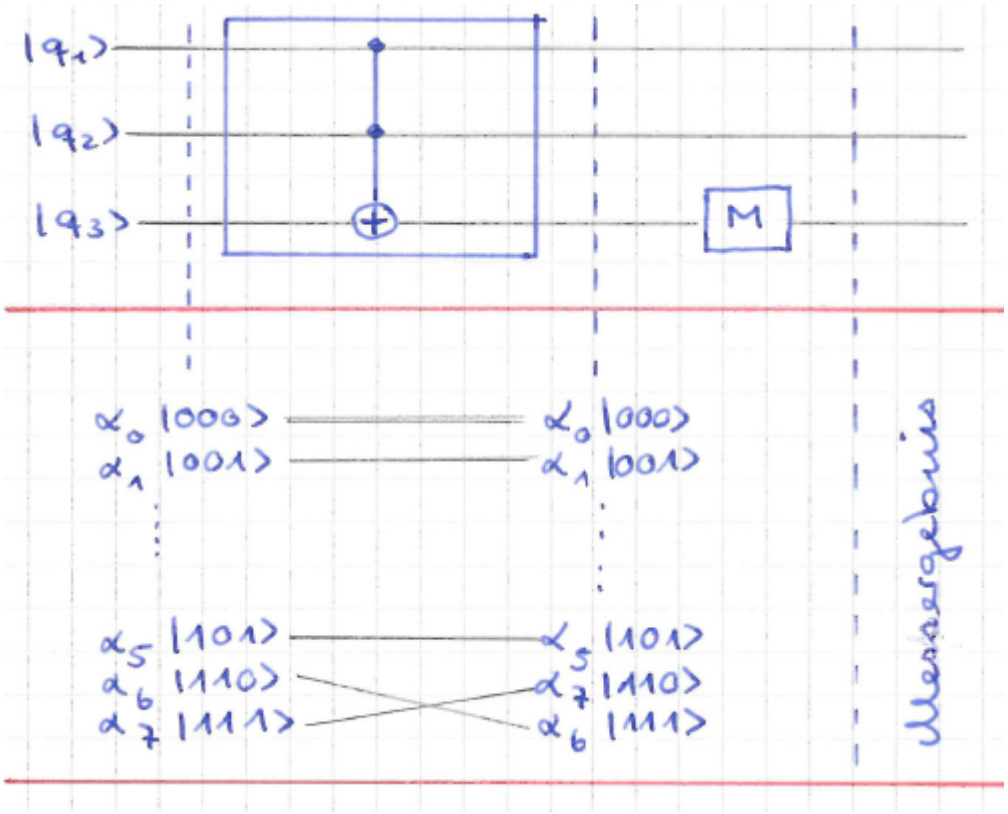
auf 3 QBits ist definiert durch die Übergänge der Basiszustände $|abc\rangle$ mit $(a, b, c) \in \{0,\ 1\}^3$
$|abc\rangle \mapsto |ab(c \oplus (a \wedge b))\rangle$.
(Bem.: q_1 und q_2 sind Steuerbit(Control bits), q_3 ist das Zielbit (target bit).)

Unitäre Matrix also (Spalten sind die Bilder der Basisvektoren):



(man überzeugt sich: ist unitär).
Für jeden Informatiker ist klar, was passiert, wenn ein Basiszustand des Zustandsraumes in das Toffali-Gitter eingeht. Aber so ein gemischter Quanten-Status?

Bsp.: Der Zustand
$|q_1 q_2 q_3\rangle = \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{2}|100\rangle + \frac{1}{\sqrt{8}}|101\rangle + \frac{1}{\sqrt{8}}|111\rangle$
läuft in folgenden Quantenschaltkreis:



Frage: Was ist das (Meß)Ergebnis der Berechnung?

Antwort: Nach Anwendung des Toffoli-Gatters ist das System im Zustand
$\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{2}|100\rangle + \frac{1}{\sqrt{8}}|101\rangle + \frac{1}{\sqrt{8}}|110\rangle$.

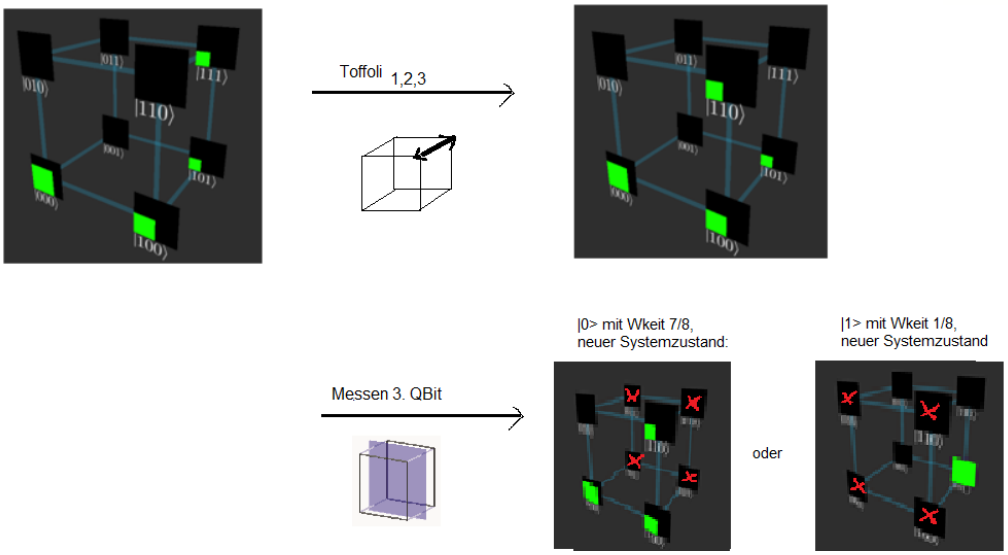
Messen des dritten QBits liefert dann:

$|q_3\rangle = |1\rangle$ mit Wkeit $\frac{1}{8}$;
das System ist dann im Zustand $|101\rangle$.

$|q_3\rangle = |0\rangle$ mit Wkeit $\frac{7}{8}$;
das System ist dann im Zustand

$$\begin{aligned}
&\sqrt{\tfrac{8}{7}} \cdot (\tfrac{1}{\sqrt{2}}|000\rangle + \tfrac{1}{2}|100\rangle + \tfrac{1}{\sqrt{8}}|110\rangle \\
&= \tfrac{2}{\sqrt{7}}|000\rangle + \sqrt{\tfrac{2}{7}}|100\rangle + \tfrac{1}{\sqrt{7}}|110\rangle \\
&= \tfrac{1}{\sqrt{7}} \cdot (2 \cdot |00\rangle + \sqrt{2}|10\rangle + |11\rangle) \cdot |0\rangle
\end{aligned}$$

Graphische Darstellung auf der nächsten Seite:



Bem.: i.)Man beachte die unterschiedlichen, gleichwertigen Schreibweisen in der Darstellung der Quantenregister im oben stehenden Beispiel.
ii.) Warum unitäre Transformationen auf dem ZUSTANDSraum?
Antwort (etwas handwaving): Man kann sich vorstellen, dass man mit einem einzelnen QBit nichts machen kann, als die eigene Position zu ihm zu verändern. Das sieht dann aus, als hätte man es gedreht und gespiegelt, und sieht aus wie eine unitäre Transformation auf dem $\mathbb{R}^2$.
Bei n QBits kann man die eigene Position zu jedem der QBits UNABHÄNGIG VONEINANDER verändern. Das führt zu Transformationen auf dem $\mathbb{R}^{2^n}$.

2.2.3 Quantengatter

Lernziele:

i.) Die Quantengatter Id, X, (Y), Z, H, CNOT und TOFFOLI mit ihren unitären Transformationen, ihrer graphischen Darstellung im Würfel und auf algassert kennen;

ii.) Die Konzepte gesteuerter unitärer Transformationen und von Quantenorakeln kennen, incl. unitärer Transformationen;

iii.) Eigene erste Quantenschaltkreise auf drei QBits entworfen und ausprobiert haben.

Quantengatter: Elementare Bauteile der Quantenschaltkreise. Arbeiten auf 1, 2 oder 3 QBits.
Aus ihnen kann man alle unitären Transformationen auf n QBits zusammensetzen.

Quantengatter auf 1 QBit: .

i.) **Identität**

Wirkung auf Basiszustände:
$|0\rangle \mapsto |0\rangle$
$|1\rangle \mapsto |1\rangle$
Unitäre Matrix: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

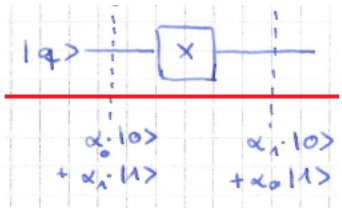
läßt $|q\rangle$ unverändert (spielt nur eine begleitende Rolle, wenn auf anderen Bits des Schaltkreises Transformationen ausgeführt werden).

ii.) **Pauli-X**-Transformation (das NOT im Quantencomputing)

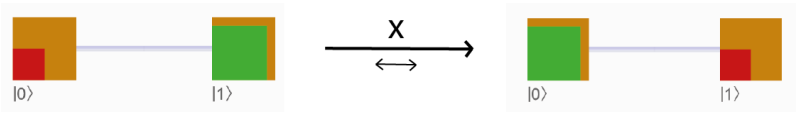
Darstellung im Schaltkreis:

Wirkung auf Basiszustände:
$|0\rangle \mapsto |1\rangle$
$|1\rangle \mapsto |0\rangle$
Unitäre Matrix: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

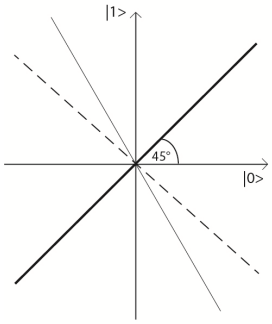
Wirkung auf beliebigen Zustand: $\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$



Graphische Veranschaulichung / Beispiel:



Technische Umsetzung: Spiegelung des QBits an der Winkelhalbierenden des 1. Quadranten



Pauli-X

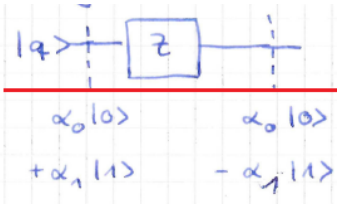
Übung in der Vorlesung: Was ist die unitäre Matrix, wenn X auf das erste QBit eines Registers aus zwei QBits angewandt wird?
Wie kann man sich graphisch die Wirkung auf das Quantenregister vorstellen?

iii.) **Pauli-Z**-Transformation

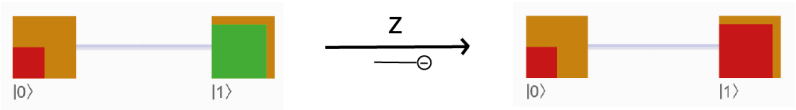
Darstellung im Schaltkreis:

Wirkung auf Basiszustände:
$|0\rangle \mapsto |0\rangle$
$|1\rangle \mapsto -|1\rangle$
unitäre Matrix: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

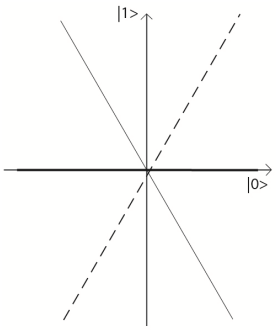
Wirkung auf beliebigen Zustand:



Graphische Veranschaulichung / Beispiel:



Technische Umsetzung: Spiegelung des QBits an der $|0\rangle$ Achse



Pauli-Z

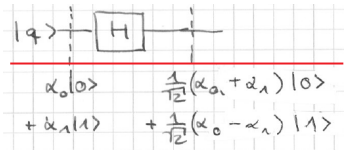
Übung in der Vorlesung: Was ist die unitäre Matrix, wenn Z auf das zweite QBit eines Registers aus drei QBits angewandt wird?
Wie kann man sich graphisch die Wirkung auf das Quantenregister vorstellen?

iv.) **Hadamard**-Transformation

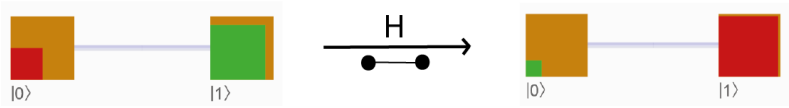
Darstellung im Schaltkreis:

Wirkung auf Basiszustände:
$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
unitäre Matrix: $\frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

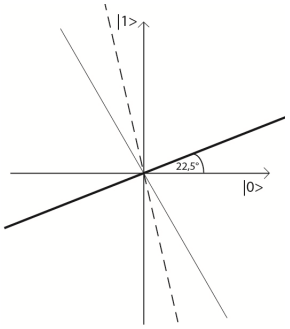
Wirkung auf beliebigen Zustand:



Graphische Veranschaulichung / Beispiel:



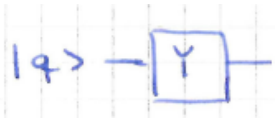
Technische Umsetzung: Spiegelung des QBits an der 22.5°- Achse



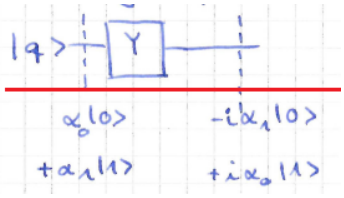
Hadamard

Übung in der Vorlesung: Was ist die unitäre Matrix, wenn H auf das zweite QBit eines Registers aus zwei QBits angewandt wird?
Wie kann man sich graphisch die Wirkung auf das Quantenregister vorstellen?

v.) **Pauli-Y**-Transformation (über $\mathbb{C}$)



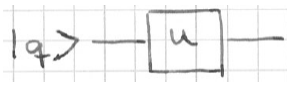
Wirkung auf Basiszustände:
$|0\rangle \mapsto i|1\rangle$
$|1\rangle \mapsto -i|0\rangle$
unitäre Matrix: $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Wirkung auf beliebigen Zustand:



vi.) **Allgemeine unitäre Transformation eines QBits**:

Satz: Jede reelle unitäre 2×2-Matrix hat die Gestalt $\begin{pmatrix} u & v \\ -v & u \end{pmatrix}$
oder $\begin{pmatrix} u & v \\ v & -u \end{pmatrix}$
mit $u, v \in \mathbb{R}, |u|^2 + |v|^2 = 1$.

Bew.: Übungsaufgabe

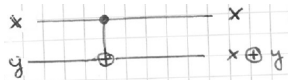


Bem.: Man überzeugt sich, dass alle vorgenannten Transformationen diese Gestalt haben.

Quantengatter auf 2 QBits:

i.) **CNOT** (Controlled not, gesteuerte Negation):
Bedeutung: Target Bit wird negiert, genau dann wenn Controll Bit den Wert 1 hat.

Darstellung im Schaltkreis:



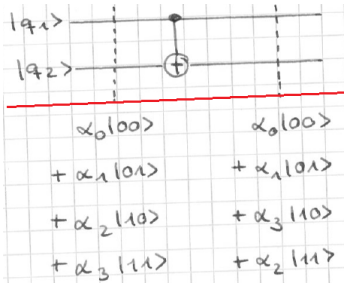
Wirkung auf Basiszustände:

$$|00\rangle \mapsto |00\rangle$$
$$|01\rangle \mapsto |01\rangle$$
$$|10\rangle \mapsto |11\rangle$$
$$|11\rangle \mapsto |10\rangle$$

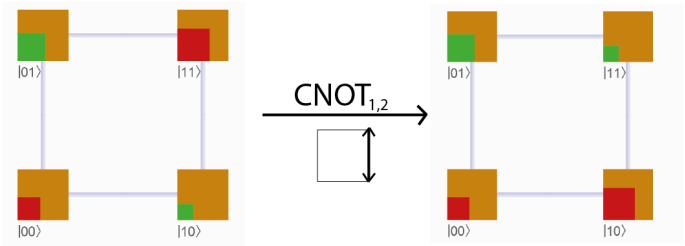
Unitäre Matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Wirkung auf allgemeinen Zustand:



Graphische Veranschaulichung / Beispiel:

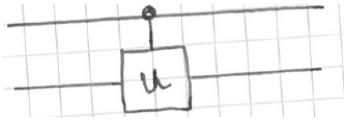


Technische Umsetzung: Anspruchsvoll und fehleranfällig. Das Steuerqbit wird in die Nähe eines Atoms gebracht, dass dadurch angeregt wird. Danach wir das Zielqbit

in die Nähe des Atoms gebracht, und wird durch dessen Anregung verändert (sehr handwaving).

Übung in der Vorlesung: Was ist die unitäre Matrix, wenn H auf das dritte QBit als Steuerbit und das erste als Zielbit eines Registers aus drei QBits angewandt wird? Wie kann man sich graphisch die Wirkung auf das Quantenregister vorstellen?

ii.) **Gesteuertes U** (eine Möglichkeit der Verallgemeinerung von CNOT)



Bedeutung: Auf Target Bit wird genau dann die unitäre Transformation U angewandt, wenn Steuerbit den Wert 1 hat.

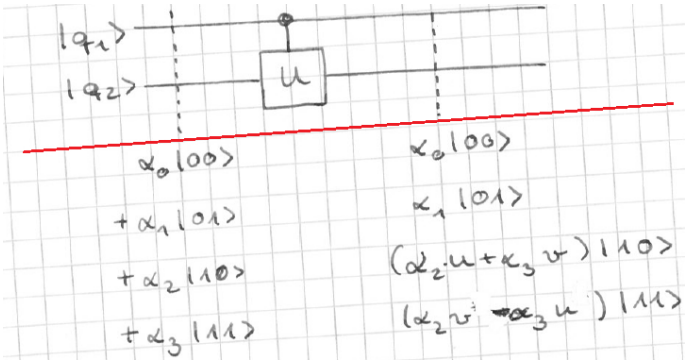
Wirkung auf Basiszustände:

$$\begin{aligned} |00\rangle &\mapsto |00\rangle \\ |01\rangle &\mapsto |01\rangle \\ |10\rangle &\mapsto |1\rangle \cdot U(|0\rangle) \\ |11\rangle &\mapsto |1\rangle \cdot U(|1\rangle) \end{aligned}$$

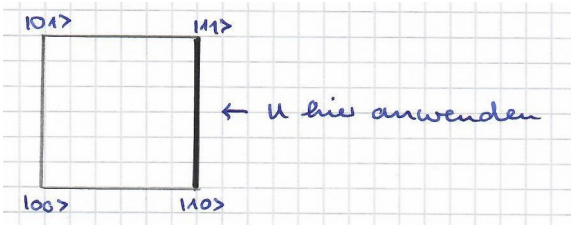
Unitäre Matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & & \\ 0 & 0 & & \mathrm{U} \end{pmatrix}$$

Wirkung auf allgemeinen Zustand.
Nur Fall U= $\begin{pmatrix} u & v \\ -v & u \end{pmatrix}$

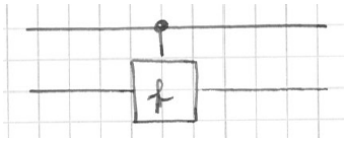


Graphische Veranschaulichung:



Bem.: CNOT ist gesteuertes U für U=Pauli-X.

iii.) **Quantenorakel** (eine andere Möglichkeit der Verallgemeinerung von CNOT)



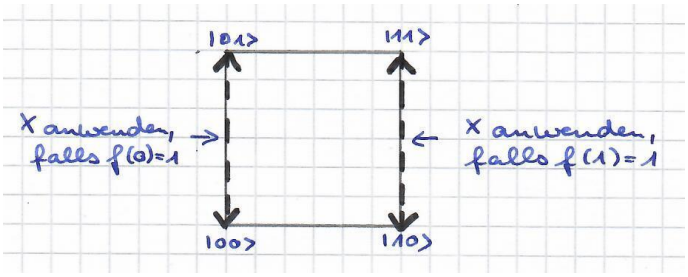
für eine beliebige (nicht notwendig bijektive) Funktion $f : \{0,1\} \to \{0,1\}$.
Bedeutung: Zielbit (Targetbit) wird genau dann negiert, wenn f(Steuerbit) $= 1$ gilt.
Wirkung auf die Basiszustände:

$|00\rangle \mapsto |0\rangle|f(0)\rangle$
$|01\rangle \mapsto |0\rangle|1 \oplus f(0)\rangle$
$\downarrow$
$f(0) = 1 \Leftrightarrow$ Reihenfolge vertauscht

$|10\rangle \mapsto |1\rangle|f(1)\rangle$
$|11\rangle \mapsto |1\rangle|1 \oplus f(0)\rangle$
$\downarrow$
$f(1) = 1 \Leftrightarrow$ Reihenfolge vertauscht

Wirkung auf den allgemeinen Zustand für die 4 möglichen Funktionen $f \to$ Übungsaufgabe.

Graphische Veranschaulichung:

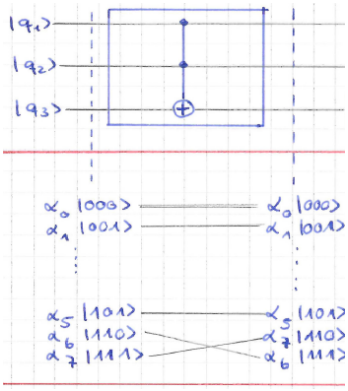


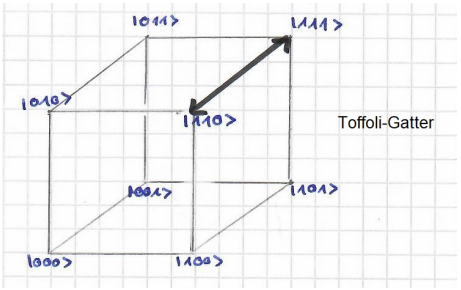
Bem.: CNOT ist gesteuertes U für U=Id.

Übung in der Vorlesung: Betrachtet wird die Funktion $f(0) = 1, f(1) = 0$. Was ist die unitäre Matrix ihres Quantenorakels, wenn es auf das erste QBit als Steuerbit und das zweite als Zielbit eines Registers aus drei QBits angewandt wird?
Wie kann man sich graphisch die Wirkung auf das Quantenregister vorstellen?

Quantengatter auf 3 QBits: Nur Toffoli-Gatter, wurde bereits behandelt: Bedeutung: 3. Bit wird negiert genau dann, wenn die anderen beiden 1 sind.

Wirkung auf den allgemeinen Zustand und graphische Veranschaulichung:





Wirkung auf Basiszustände:

$$
\begin{aligned}
|000\rangle &\mapsto |000\rangle \\
|001\rangle &\mapsto |001\rangle \\
|010\rangle &\mapsto |011\rangle \\
|011\rangle &\mapsto |010\rangle \\
|100\rangle &\mapsto |100\rangle \\
|101\rangle &\mapsto |101\rangle \\
|110\rangle &\mapsto |111\rangle \\
|111\rangle &\mapsto |110\rangle
\end{aligned}
$$

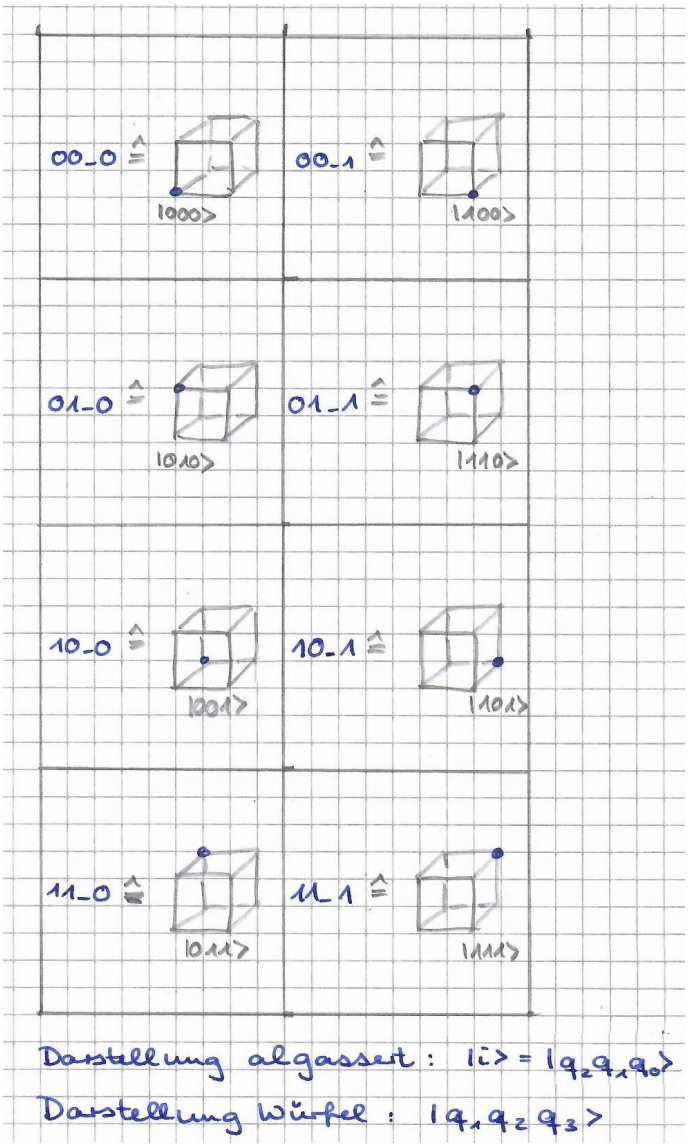
Unitäre Matrix:

$$
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}
$$

Das sind die wesentlichen Gatter für diese Vorlesung.
Im online-Tool quirk auf algassert-com findet man viele weitere Quantengatter, die in den meisten Fällen die komplexen Zahlen benötigen.

Ein Quantenregister wird bei algassert in umgekehrter Reihenfolge dargestellt.
Statt $|q_1\ q_2\ q_3\rangle$ also in der Form $q_1\ q_1\ q_0\rangle$. Diese ist auf den ersten Blick unanschaulicher, entspricht aber besser der Binärdarstellung $|i\rangle$.

Hier ist für ein Quantenregister aus drei QBits eine Umrechnungstabelle:
Welches algassert-Feld entspricht welchem Feld im Würfel?



2.3 Mathematik: Unitäre Transformationen und Tensorprodukt

Lernziele:

1.) Wissen, dass die Berechnungen von Quantenschaltkreisen umkehrbar sind (solange nicht gemessen wird).
Es geht also keine Information verloren, anders als z.B. beim klassischen AND).

2.) Tensorprodukt von Matrizen und von Vektoren bilden können.

3.) Anwendung von Tensorprodukten in Quantenschaltkreisen:

i.) Ausmultiplizieren unverschränkter Qauntenzustände zu einem einzigen Registerzustand;

ii.) Finden der unitären Transformation, wenn in einem Schritt parallele Gatter angewandt werden (z.B. CNOT auf erstes und zweites QBit, gleichzeitig H auf das dritte);

iii.) Kombination aus i.) und ii.).

4.) Spielen mit Matlab, Algassert, Qurakel und IBM-Q.

Damit sind dann die theoretischen und programmtechnischen Grundlagen gelegt für Quantenalgorithmen im Rest der Vorlesung :).

Definition: Eine $N \times N$-Matrix U mit komplexen Einträgen heißt unitär, wenn gilt $U^{-1} = U^{*T}$. Die zugehörige lineare Abbildung heißt unitäre Transformation.

Satz: Unitäre Transformationen sind Drehspiegelungen. Sie erhalten Winkel (genauer: das Skalarprodukt) und Längen.

Bew: (Nicht in der Vorlesung)
Seien $x, y \in \mathbb{C}^N, x = \begin{pmatrix} x_1 \\ \vdots \\ x_6 \end{pmatrix}, y = \begin{pmatrix} y_1 \\ \vdots \\ y_6 \end{pmatrix}$. Das Skalarprodukt $\langle x|y\rangle$ von x und y ist definiert als

$$\langle x|y\rangle = \sum_{i=1}^{n} x_i^* y_i$$

(als Matrix geschrieben: $\langle x|y\rangle = x^{*T}y$), die Norm (oder Länge) von x ist $\sqrt{\langle x|x\rangle}$. Sei nun U unitär. Dann ist (in Matrixschreibweise, und weil $U^{*T} = U^{-1}$):

$$\begin{aligned} \langle Ux|Uy\rangle &= (Ux)^{*T} * Uy \\ &= (U^* x^*)^T * Uy \\ &= x^{*T} \cdot U^{*T} \cdot Uy \\ &= x^{*T} \cdot y \\ &= \langle x|y\rangle \end{aligned}$$

Satz: (Beweis Übungsaufgabe für diejenigen mit Mathematikerherz)
Unitäre $N \times N$-Matrizen bilden eine Gruppe (mit der Matrixmultiplikation).

Folgerung: (aus beiden Sätzen)

1. Unitäre Transformationen mit der Hintereinanderausführung bilden eine Gruppe.
2. Durch eine unitäre Transformation wird ein zulässiger Quantenregisterzustand wieder in einen zulässigen Quantenregisterzustand überführt.
   Denn ein zulässiger Quantenregisterzustand ist ein Vektor des $\mathbb{R}^{2^n}$ der Länge 1.
3. Jede unitäre Transformation kann (durch Anwenden der inversen Transformation) rückgängig gemacht werden. Dadurch kommt das Quantenregister wieder in den Zustand vor der Transformation. Das bedeutet: In Quantenschaltkreisen geht beim Anwenden der Quantengatter keine Information verloren, solange nicht gemessen wird (im Gegensatz zum Anwenden klassischer Bits wie z.B. AND. Ist $a \wedge b = 0$, so können die Werte von a und b nicht mehr zurückkonstruiert werden).

Jetzt geht's zum Tensorprodukt:

Definition: Seien $A = (a_{ij})$, $B = (b_{ij})$ Matrizen beliebigen Formats: A eine $r \times n$-Matrix, B eine $s \times m$-Matrix. Dann ist das Tensorprodukt $A \otimes B$ die $r \cdot s \times n \cdot m$-Matrix.

$$\begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{r1}B & \dots & a_{rn}B \end{pmatrix}$$

Beispiel: Selbst eines erfinden.

Definition: Seien $v \in \mathbb{R}^n$(oder $\mathbb{C}^n$), $w \in \mathbb{R}^m$(oder $\mathbb{C}^m$), so ist $v \otimes w$ der Vektor, den man erhält, wenn man beide Vektoren als Spalten schreibt und das (Matrix-)Tensorprodukt bildet: Ein (Spalten)vektor mit $n \cdot m$ Komponenten.

Satz: (Ohne Beweis)

1. Tensorprodukt und Matrixmultiplikation vertragen sich: Seien A, B, v, w wie oben, so ist
   $$(A \cdot v) \otimes (B \cdot w) = (A \otimes B) \cdot (v \otimes w)$$
2. Tensorprodukte unitärer Matrizen sind unitär.

Übung:

- Zu Teil 1. des Satzes: Bitte überzeugen Sie sich, dass es mit den Formaten passt.
- Zu Teil 2. des Satzes: Bitte überzeugen Sie sich, dass das Tensorprodukt quadratischer Matrizen wieder eine quadratische Matrix ist, auch wenn beide unterschiedliches Format haben.

Bemerkung: (Nicht in der Vorlesung)
Normalerweise wird das Tensorprodukt für Vektorräume eingeführt: Seien V_1, V_2 Vektorräume mit Basen $e_1, \cdots, e_n$ bzw $f_1, \cdots, f_m$, so ist das Tensorprodukt $V_1 \otimes V_2$ der Vektorraum mit Basis $\{e_i f_j : i = 1 \cdots n, j = 1 \cdots m\}$. Das Tensorprodukt zweier Vektoren $v = \sum v_i e_i \in V_1$ und $w = \sum w_j f_j \in V_2$ ist dann definiert als $\sum_{i,j} v_i w_j e_i \otimes f_j$.
In diesem Sinne ist der Zustandsraum eines Quantenregisters (als Vektorraum) das Tensorprodukt der Zustandsräume der einzelnen QBits.

Beachte: Nicht jeder Vektor des Tensorproduktes kann als Tensorprodukt von Vektoren der beteiligten Räume dargestellt werden (Ausblick .... nur diejenigen, die unverschränkten Zuständen entsprechen ...).

Anwendung des Tensorproduktes auf Quantenschaltkreise:

1. „Ausmultiplizieren“ von Zuständen unverschränkter Quantenregister:

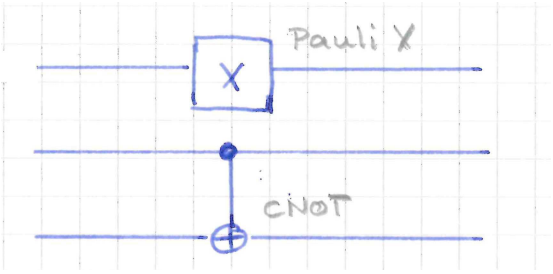
$$\begin{aligned} |q_1\rangle &= \beta_0|0\rangle + \beta_1|1\rangle \\ |q_2 q_3\rangle &= \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle \\ \Rightarrow |q_1 q_2 q_3\rangle &= \sum_{i=0}^{7} \gamma_i |i\rangle \end{aligned}$$

mit

$$\begin{pmatrix} \gamma_0 \\ \vdots \\ \gamma_7 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} \beta_0\alpha_0 \\ \beta_0\alpha_1 \\ \beta_0\alpha_2 \\ \beta_0\alpha_3 \\ \beta_1\alpha_0 \\ \beta_1\alpha_1 \\ \beta_1\alpha_2 \\ \beta_1\alpha_3 \end{pmatrix}$$

(das erhält man auch beim Ausmultiplizieren von
$(\beta_0|0\rangle + \beta_1|1\rangle) \cdot (\alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle)$

2. Finden der unitären Transformation, wenn in einem Schritt parallele Gatter angewandt werden:
   Bsp:



   Die zugehörige unitäre Matrix ist

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

3. (Kombination von 1. und 2.) Wirkung paralleler Gatter auf unverschränkte Teilregister. Wird auf ein Quantenregister mit dem Zustand aus b.) der Schaltkreis aus a angewandt, ist der Koeffizientenvektor des Zustands danach

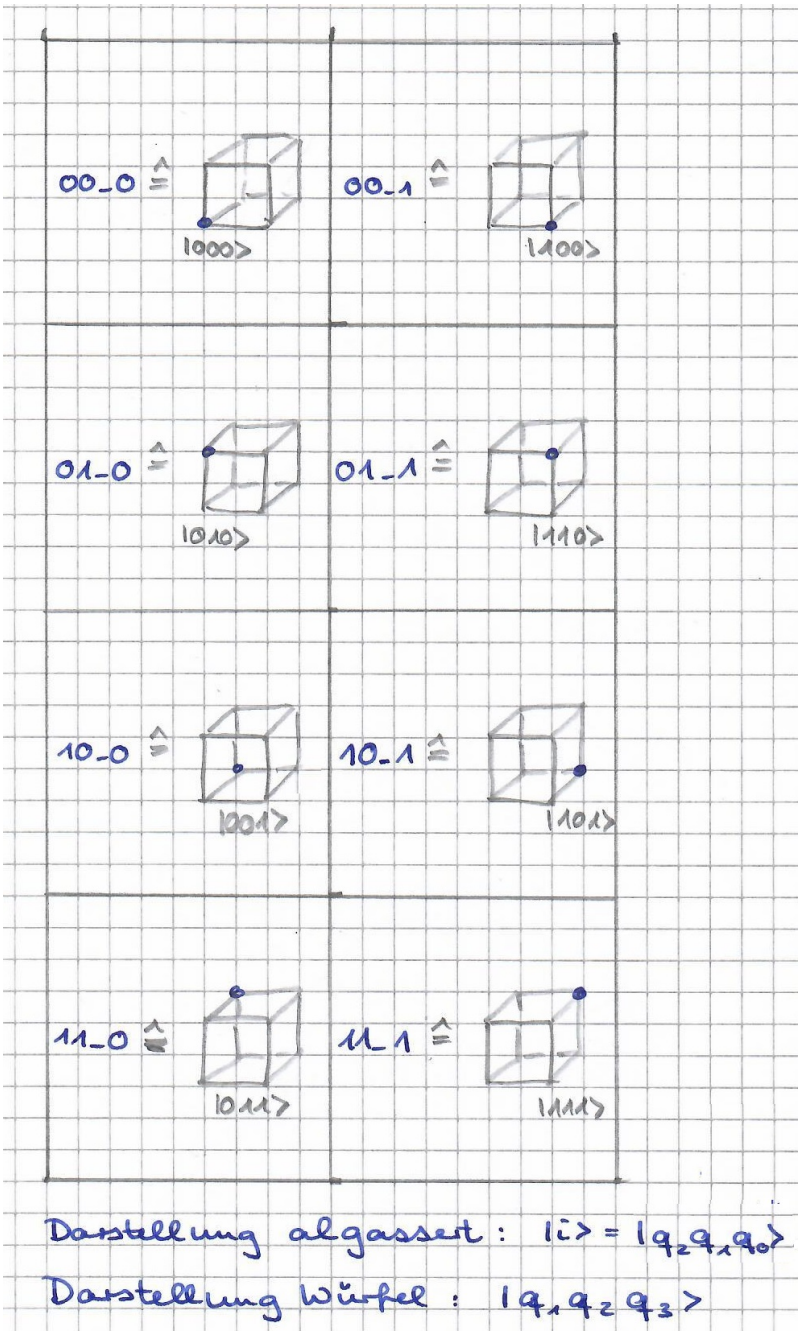
$$\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \right) \otimes \left(\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} \right)$$

$$= \begin{pmatrix} \beta_1 \\ \beta_0 \end{pmatrix} \otimes \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_3 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} \beta_1\alpha_0 \\ \beta_1\alpha_1 \\ \beta_1\alpha_3 \\ \beta_1\alpha_2 \\ \beta_0\alpha_0 \\ \beta_0\alpha_1 \\ \beta_0\alpha_3 \\ \beta_0\alpha_2 \end{pmatrix}$$

Bemerkung: Die Anwendung des Tensorproduktes funktioniert nur bei Schaltkreisen, in denen die parallelen Transformationen auf aufeinanderfolgende QBits angewandt werden. Also z.B. nicht, wenn CNOT auf das erste und dritte Bit angewandt wird, und nichts (Id, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$) oder Pauli-X auf das zweite. Hierzu gibt es eine Übungsaufgabe.

Zur Übung: Bitte spielen Sie mit Matlab, Algassert, Qurakel und IBM-Q. Nun sind die theoretischen und programmiertechnischen Grundlagen für Quantenalgorithmen gelegt.

Hier noch einmal die Umrechnungsvorschrift der Zustandsbezeichnungen von Algassert und Qurakel:



3 Erste Quantenalgorithmen

Lernziele:

1.) Verstanden haben, wie ein klassischer Schaltkreis mit m Gattern durch einen Quantenschaltkreis mit $O(m)$ Quantengattern simuliert werden kann. (Das bedeutet, dass jedes Berechnungsproblem mit Quantenalgorithmen mindestens so schnell gelöst werden kann wie mit klassischen Algorithmen).

2.) Folgende Algorithmen gesehen haben, und verstanden haben, dass sie funktionieren:

i.) Erzeugung von Zufallsbits;

ii.) Teleportation;

iii.) Schlüsselaustausch in der Kryptographie (BB84-Protokoll)

iv.) Dichte Codierung;

v.) Entschlüsselung von Quantenorakeln (Algorithmen von Deutsch, Deutsch-Josza und Vazirani).

3.) Übergreifende Fähigkeiten zur Analyse von Quantenalgorithmen erworben haben. Es gibt drei Möglichkeiten zur Analyse, die je nach Situation angewendet werden:

i.) Am vollständigsten, aber auch am aufwändigsten: Analyse mittels der unitären Transformationen.

ii.) Falls der Input gegeben ist und eine einfache Form hat, z.B. ein Basiszustand ist: Schrittweise Berechnung der Registerzustände im Laufe der Berechnung.

iii.) Für Schaltkreise mit bis zu drei QBits: Graphische Veranschaulichung am „Würfel“.

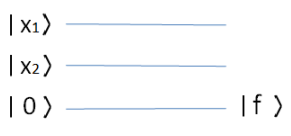
3.1 Klassische Boolesche Funktionen

Wir wollen zeigen, dass man mit Quantenschaltkreisen alle booleschen Funktionen $f : \{0,1\}^n \to \{0,1\}$ berechnen kann. Das zeigen wir explizit für alle 16 booleschen Funktionen auf $n = 2$ QBits. Für größere n wird am Beispiel illustriert, wie Funktionen über ihre DNF mithilfe von „garbage-qbits“ realisiert werden.
Man sieht dann, dass man diese Methode auch nutzen kann, um beliebige klassische Schaltkreise mit m Gattern (auf je 1 oder zwei klassischen Bits) in Quantenschaltkreise mit maximal $5m$ Quantengattern simulieren kann.

Satz: Die folgenden Quantenschaltkreise berechnen die 16 unterschiedlichen klassischen Booleschen Funktionen auf 2 Input-Bits:

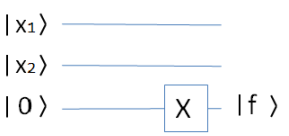
Const 0:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	0
1	0	0
1	1	0



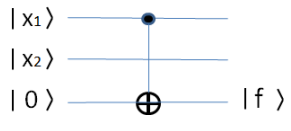
Const 1:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	1
1	0	1
1	1	1



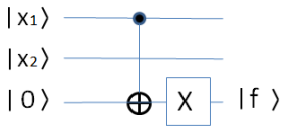
X1:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	0
1	0	1
1	1	1



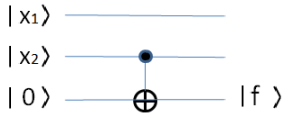
Not X1:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	1
1	0	0
1	1	0



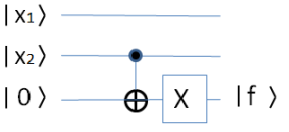
X2:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	1
1	0	0
1	1	1



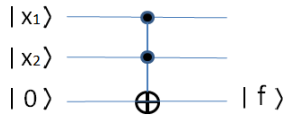
Not X2:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	0
1	0	1
1	1	0



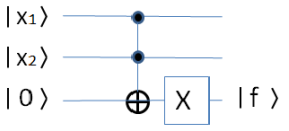
AND:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	0
1	0	0
1	1	1



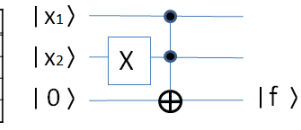
Not AND:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	0
1	0	0
1	1	1



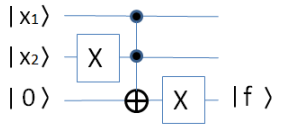
Not =>:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	0
1	0	1
1	1	0



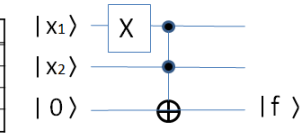
=>:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	1
1	0	0
1	1	1



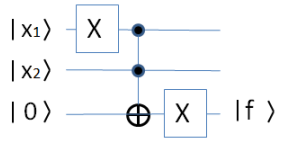
Not <=:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	1
1	0	0
1	1	0



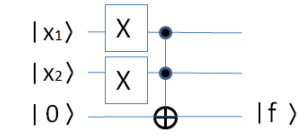
<=:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	0
1	0	1
1	1	1



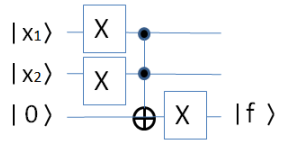
Not OR:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	0
1	0	0
1	1	0



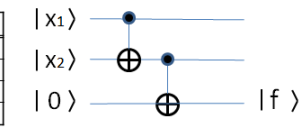
OR:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	1
1	0	1
1	1	1



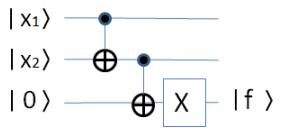
XOR:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	1
1	0	1
1	1	0



⇔:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	0
1	0	0
1	1	1



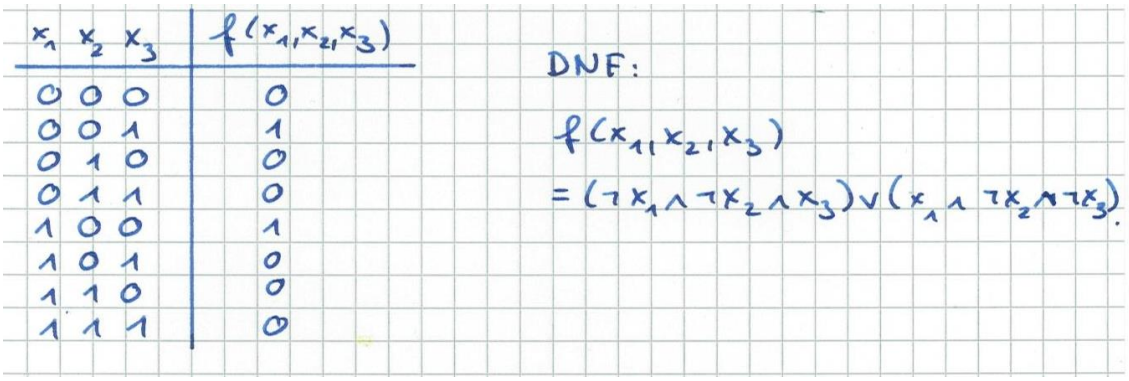
Bew.: Man überzeugt sich für jede Funktion im Einzelnen, ist eine Übungsaufgabe.

Übung in der Vorlesung: Für eine der Funktionen alle drei Analysemethoden austesten.

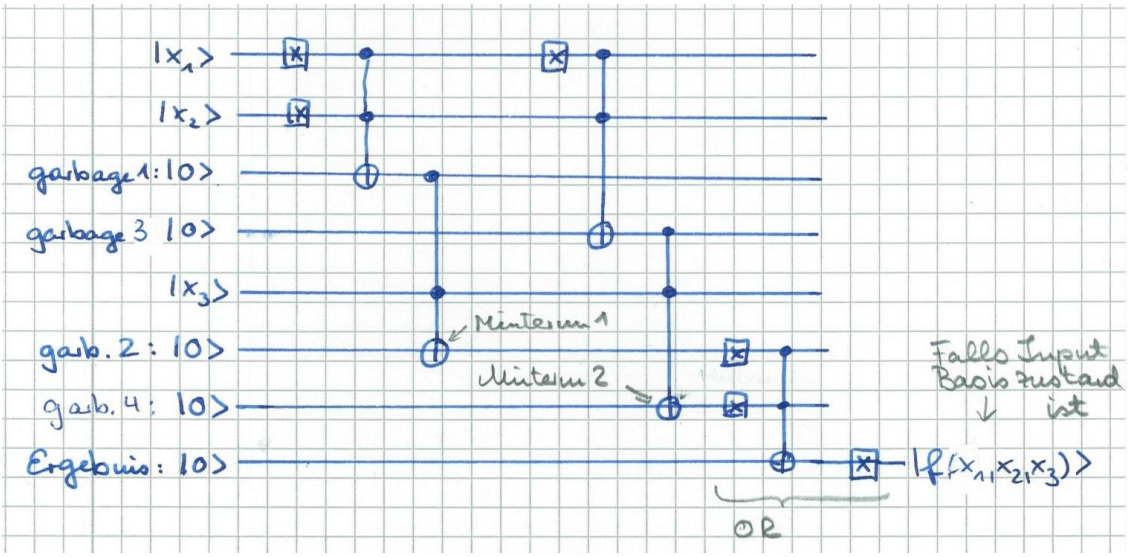
Wie nun boolesche Funktionen auf $n > 2$ Input-Bits mithilfe ihrer Disjunktiven Normalform und hinreichend vielen „garbage-QBits“ berechnet werden, wird an einem Beispiel für $n = 3$ illustriert.

Beipiel: Die folgende Funktion wird durch den darunter stehenden Quantenschaltkreis berechnet:

Funktion:



Quantenschaltkreis:



Satz: Jedes $f : \{0,1\}^n \to \{0,1\}$ kann durch einen Quantenschaltkreis berechnet werden. Dabei genügt es, pro Minterm $n-1$ Garbage-QBits vorzusehen, und für das OR am Schluss noch einmal #Minterme $-$ 2 weitere Garbage-QBits.

Bew.: Ein formaler Beweis entfällt, die Intuition sollte nach dem Beispiel klar sein.

Bem.: Die Quantenschaltkreise zur Berechnung der $f : \{0,1\}^n \to \{0,1\}$ greifen wiederholt auf die Input-Bits zu. Das geht, denn bei Input eines Basiszustandes haben sie stets einen eindeutigen Wert $|0\rangle$ oder $|1\rangle$. Beweis: Mit einem Input-Q-Bit geschehen während der Berechnung nur zwei unterschiedliche Dinge:

i.) Es wir eine Reihe von Pauli-X-Transformationen amgewendet, und

ii.) es wird zur Steuerung von Toffoli- und CNOT-Gattern verwendet angewendet.

Durch vollständige Induktion nach der Anzahl der Operationen zeigt man, dass jedes QBit tatsächlich während der ganzen Berechnung einen eindeutigen Zustand hat.
Anmerkung: Das wäre nicht der Fall, wenn zwischendurch die Hadamard-Transformation angewandt würde. Durch diese wird ein System aus einem Basiszustand in einen überlagerten Zustand versetzt.

Satz: Jeder klassische Schaltkreis mit m Gattern (auf je einem oder zwei klassischen Input-Bits) kann durch einen Quantenschaltkreis mit höchstens $4m$ Quantengattern simuliert werden.
„Simulation“ bedeutet: Der Quantenschaltkreis liefert auf den Basiszuständen denselben Output wie der klassische Schaltkreis.

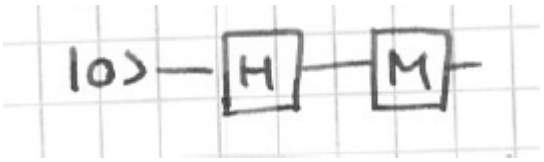
Bew.: Nachbau des Schaltkreises als Quantenschaltkreis wie oben bei der DNF. Jedes klassiche Gatter kann durch höchstens 4 Quantengatter simuliert werden.

3.2 Zufallsgeneratoren

Erzeugung von echtem Zufall ist auf klassischen Computern nicht möglich, da diese deterministisch sind - erzeugt werden hier nur Pseudozufallszahlen. Wer den Algorithmus kennt, kann also die „Zufallszahlen“ eines klassischen Computers nachrechnen, und die nächste „Zufallszahl“ sicher vorhersagen.

QBits verhalten sich echt zufällig (was Einstein nicht mochte ; er behauptet „Gott würfelt nicht“).

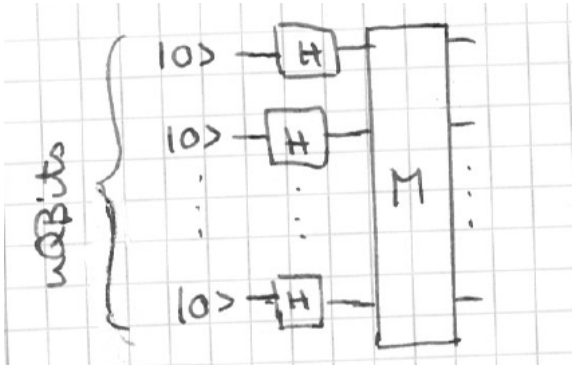
Satz: Der folgende Quantenschaltkreis liefert ein echtes Zufallsbit:



Bew.: Nach Anwenden von H ist das Bit im Zustand $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
Messen liefert jeweils mit Wkeit $\frac{1}{2}$ den Output $|0\rangle$ oder $|1\rangle$.

Bem.: Hardware für Quanten-Zufallsbits gibt es für um die 3.000 Eur zu kaufen, hier Bilder von IBM-qrbg121 und von Quantis QRNG PCIe - USB:

Satz: Der folgende Q-Schaltkreis liefert n unabhängige echte Zufallsbits, $n \in \mathbb{N}$:



Bew.: Nach Anwenden der Hadamard-Transformationen ist das Register im Zustand $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot \ldots \cdot (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2^n}} \cdot \sum_{i=0}^{2^n-1} |i\rangle$. Messen liefert also jeden Basiszustand $|i\rangle$ mit gleiche Wahrscheinlichkeit.

3.3 Teleportation

Eine der spektakulärsten Anwendungen von Quantencomputing:

1997 Arbeitsgruppe um Zeilinger in Wien: Erstmaliger Nachweis von Teleportation im Labor.

2003 Arbeitsgruppe um Gisin in Genf: Teleportation über 55m, erstmals außerhalb des Labors;

2004 Gruppe um Zeilinger: Teleportation über Distanz von 600m, von einem Ufer der Donau zu ihrem anderen Ufer;

2010 Arbeitsgruppe in Shanghai um Xian Min Lin: Teleportation über 16 km;

2012 Arbeitsgruppe an der chinesischen Universität für Wissenschaft und Technik um Pan Jian-Wei: Teleportation über Distanz von 97 km;

2012 Arbeitsgruppe um Zeilinger: Teleportation über Entfernung von 143 km zwischen La Palma und Teneriffa;

2017 internat. Arbeitsgruppe, u.A. mit Beteiligung von Zeilinger und Pan Jian-Wei: Telportation über 1400 km von der Erde zum chinesischen Quantensatelliten Micius;

2017 dieselbe Arbeitsgruppe: 7600 km zwischen Österreich und China.

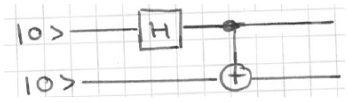
Neuere Forschung: Überbrückung ultrakleiner Distanzen statt besonders großer, für Nutzung im Rechner selbst.

Hintergrund: Legendär: „Scotty, beam me up, there is no intellegent life down here“.

Hilfsmittel - und Frage: Benutzt werden verschränkte QBits, sogenannte EPR-Paare, benannt nach Einstein-Podolsky-Rosen. Wie werden die hergestellt?

Antwort der Physiker: Z.B.: Man schickt ein Lichtteiclhen durch einen Verschränkungskristall.

Antwort der Informatiker:



Zustand nach Hadamard:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

Zustand nach CNOT:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Verschränkte Bits hergestellt.

Jetzt können wir teleportieren. Übrigens keine Materie, sondern Eigenschaften, Information also.

Teleportation: (Bennet et al 1993, erste Realisierung 1997)

Aufgabe: A(Alice) und B (Bob) besitzen je ein QBit eines EPR-Paares, $|a\rangle$ und $|b\rangle$.
Alice besitzt zusätzlich ein QBit $|\psi\rangle$, das sie an Bob schicken möchte.
Sie hat aber keine Möglichkeit, ein QBit zu Bob zu transportieren (keinen "Quantenkanal", nur einen klassischen Kanal (Telefon)).
Messen kann sie $|\psi\rangle$ nicht, das würde den Zustand von $|\psi\rangle$ verändern.
Wie wird $|b\rangle$ in den Zustand $|\psi\rangle$ gebracht?

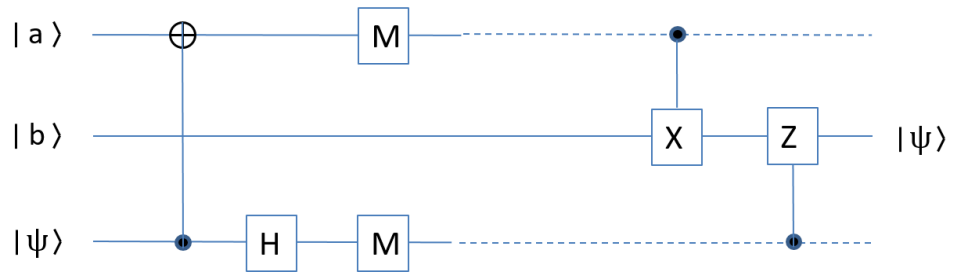
Idee: Verschränken von $|\psi\rangle$ und $|a\rangle$ holt Information über $|x\rangle$ „Zwischen die QBits"des Registers; Messen von $|\psi\rangle$ läßt die Information danach ganz zwischen $|a\rangle$ und $|b\rangle$ ($\rightarrow$ Übungsaufgabe)

Vergleich: Manche sagen, wie im täglichen Leben: Heiraten und Geldvermögen.

Verfahren im Plaintext: (nach Homeister)

1. Alice wendet ein CNOT-Gatter an: $|\psi\rangle|a\rangle \leftarrow |\psi\rangle|a \oplus \psi\rangle$
2. Alice wendet auf das zu übermittelnde Bit die Hadamard-Transformation an: $|\psi\rangle \leftarrow H(\psi)$
3. Alice mißt $|\psi\rangle$ und $|a\rangle$ und schickt das Ergebnis über den klassischen Kanal an Bob.
4. Ist $|a\rangle = |1\rangle$, wendet Bob Pauli-X auf $|b\rangle$ an: $|\psi\rangle \leftarrow X(|b\rangle)$
5. Ist $|a\rangle = |1\rangle$, wendet Bob Pauli-Z auf $|b\rangle$ an: $|b\rangle \leftarrow Z(|b\rangle)$.

Schaltkreis:



Dabei bedeutet "– – –", dass die Information über einen klassischen Kanal kommt.

Korrektheit:

Sei $\psi = \alpha|0\rangle + \beta|1\rangle$, wobei α und β Alice und Bob unbekannt sind.

Zustand des Quantenregisters zu Beginn:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \cdot (\alpha|0\rangle + \beta|1\rangle) = \frac{\alpha}{\sqrt{2}}(|000\rangle + |110\rangle) + \frac{\beta}{\sqrt{2}}(|001\rangle + |111\rangle).$$

Zustand nach Anwendung CNOT:

$$\frac{\alpha}{\sqrt{2}}(|000\rangle + |110\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |011\rangle) = \frac{\alpha}{\sqrt{2}}(|00\rangle + |11\rangle) \cdot |0\rangle + \frac{\beta}{\sqrt{2}}(|10\rangle + |01\rangle) \cdot |1\rangle.$$

Zustand nach Anwendung H:

$$\frac{\alpha}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle) \cdot (|0\rangle + |1\rangle) + \frac{\beta}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \cdot (|10\rangle + |01\rangle) \cdot (|0\rangle - |1\rangle).$$

Anders geschrieben (Vorbereitung zur Messung des ersten und dritten QBits):

$$\begin{aligned} & |0\rangle \cdot (\frac{\alpha}{2} \cdot |0\rangle + \frac{\beta}{2} \cdot |1\rangle) \cdot |0\rangle \\ + \; & |0\rangle \cdot (\frac{\alpha}{2} \cdot |0\rangle - \frac{\beta}{2} \cdot |1\rangle) \cdot |1\rangle \\ + \; & |1\rangle \cdot (\frac{\alpha}{2} \cdot |1\rangle + \frac{\beta}{2} \cdot |0\rangle) \cdot |0\rangle \\ + \; & |1\rangle \cdot (\frac{\alpha}{2} \cdot |1\rangle - \frac{\beta}{2} \cdot |0\rangle) \cdot |1\rangle. \end{aligned}$$

Messen liefert also:

- $|00\rangle$ mit Wahrscheinlichkeit $\frac{1}{4}$; $|b\rangle$ ist dann im Zustand $\alpha|0\rangle + \beta|1\rangle$
- $|01\rangle$ mit Wahrscheinlichkeit $\frac{1}{4}$; $|b\rangle$ ist dann im Zustand $\alpha|1\rangle - \beta|0\rangle$
- $|10\rangle$ mit Wahrscheinlichkeit $\frac{1}{4}$; $|b\rangle$ ist dann im Zustand $\alpha|0\rangle + \beta|1\rangle$
- $|11\rangle$ mit Wahrscheinlichkeit $\frac{1}{4}$; $|b\rangle$ ist dann im Zustand $\alpha|1\rangle - \beta|0\rangle$

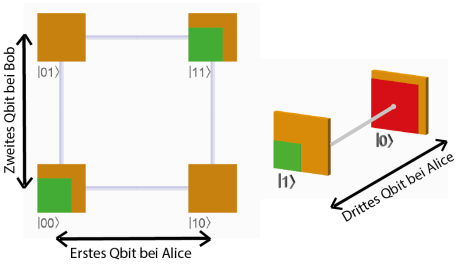
Ist $|a\rangle = |1\rangle$ (Fälle $|10\rangle$ und $|11\rangle$), überführt Pauli-X Bob's QBit in den Zustand $\alpha|0\rangle + \beta|1\rangle$ bzw. $\alpha|0\rangle - \beta|1\rangle$.

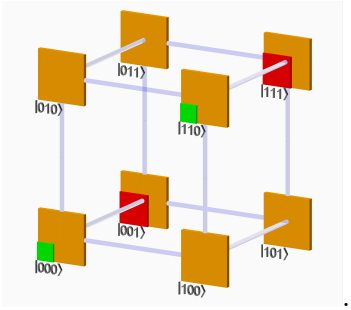
Ist zusätzlich das Messerbegnis des dritten Qbits 1 (Fälle $|01\rangle$ und $|11\rangle$), so überführt Pauli-Z dann $|b\rangle$ in
$\alpha|0\rangle + \beta|1\rangle$.

Illustration: Am Beispiel $\psi = 0.5 \cdot |0\rangle - \sqrt{3/4} \cdot |1\rangle$.

Sei $\psi = \alpha|0\rangle + \beta|1\rangle$, wobei α und β Alice und Bob unbekannt sind.

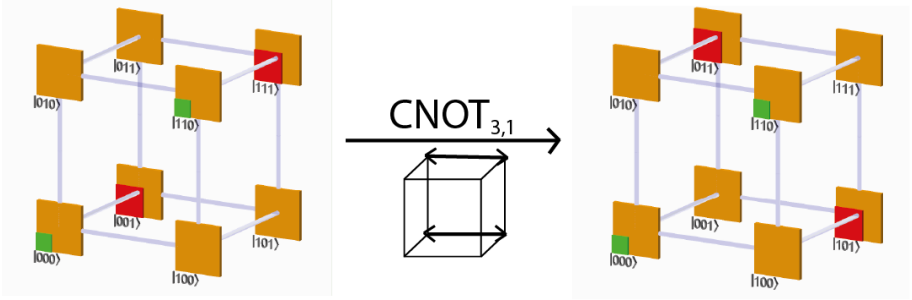
Zustand des Quantenregisters zu Beginn:



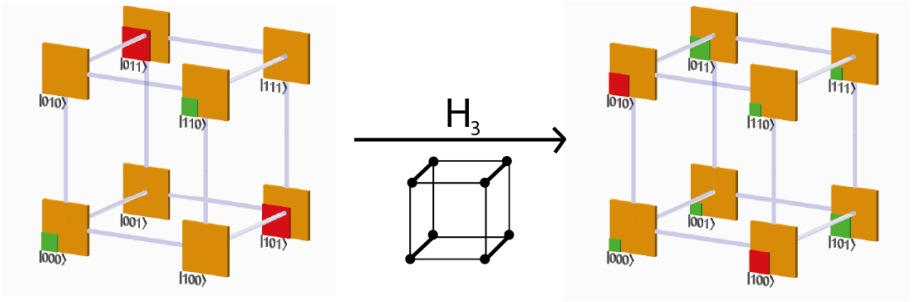
, also 

.

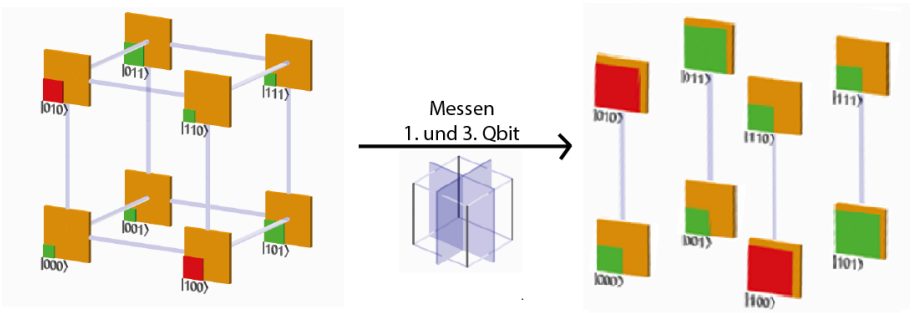
CNOT wird angewandt (Steuerbit ist drittes QBit, Zielbit ist erstes QBit):



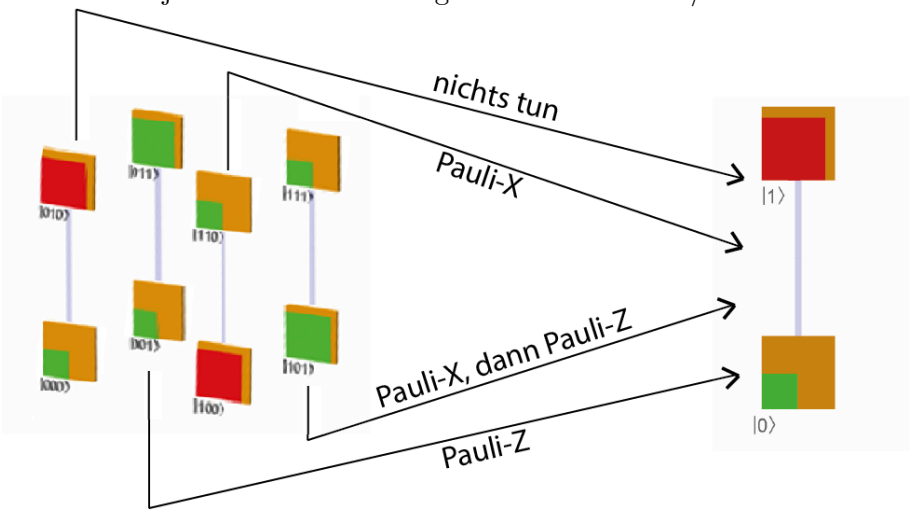
H wird auf das dritte QBit angewandt:



Das erste und dritte QBits werden gemessen, alle Ergebnisse mit Wahrscheinlichkeit 1/4, denn sie sind alle gleich wahrscheinlich:



Bob wendet je nach Alices Messergebnist Pauli-X und/oder Pauli-Z an:



Bem.: In der Kryptographie gibt es immer Eve, die die Kommunikation zwischen Alice und Bob belauscht.
Hier bekommt sie keinerlei Information. Nur ein zufälliges Paar von Bits.
Die „eigentliche“ Information wird über die Quantenverschränkung übertragen, unerreichbar für Eve.

3.4 BB84-Protokoll: Kryptographie, Schlüsseltausch

Problemstellung Schlüsseltausch:

Alice und Bob wollen sich auf eine Reihe von Zufallsbits (klassische Bits) einigen. Diese benötigen sie z.B., um einen gemeinsamen Schlüssel zum Verschlüsseln von Nachrichten zu verwenden.

Sie verfügen über einen konventionellen Kanal (z.B. Telefon) und einen Quantenkanal (z.B. Glasfaserkabel). Beide sind aber einem möglichen Lauscher zugänglich.

Wie können sie mittels der Eigenschaften von QBits einen zufälligen Schlüssel austauschen, wobei ein Lauscher keine Information über den Schlüssel erhalten soll, und außerdem entdekct werden soll?

Charles H. Bennett und Gilles Brassard fanden 1984 eine Möglichkeit.

(Algorithmus) BB84-Protokoll:

i.) Alice startet im Zustand $|0\rangle$ und wendet mit Wahrscheinlichkeit 1/2 Pauli-X an. Nun kennt sie ihr Zufallsbit.

ii.) Mit Wahrscheinlichkeit 1/2 wendet sie H an und sendet das QBit über den Quantenkanal zu Bob.

iii.) Bob wendet H ebenfalls mit Wahrscheinlichkeit 1/2 an und misst sein QBit. Das Messergebnis ist Bobs Bit.

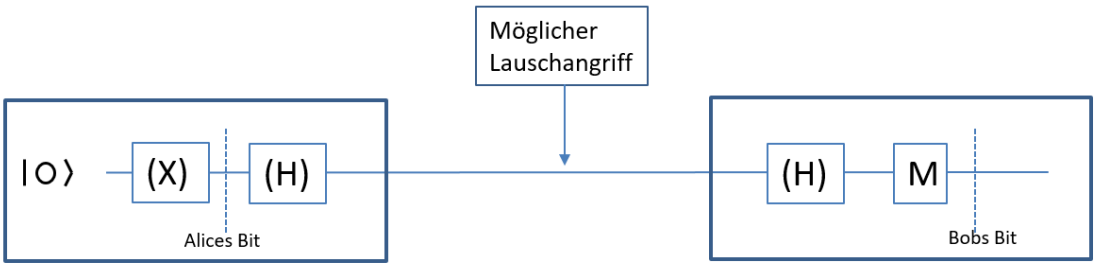
iv.) Alice und Bob verbinden sich über den klassischen Kanal.

Hat genau einer von ihnen H angewandt, wird das Bit verworfen.

Ansonsten:

Mit Wahrscheinlichkeit 1/2 einigen sie sich, das Bit zu nutzen.

Mit Wahrscheinlichkeit 1/2 vergleichen sie ihre Bits, und verwerfen sie anschließend. Ist das Ergebnis unterschiedlich, so beweist das einen Lauscher in der Leitung (oder eine fehlerhafte Leitung).



Analyse:

i.) Verfahren arbeitet korrekt, wenn kein Lauscher „Eve“ anwesend ist und der Kanal nicht fehlerhaft ist, denn die beiden H's heben sich auf.

ii.) Wegen des no cloning-Theorems (siehe unten) kann der Lauscher nicht das QBit klonen und eine Kopie weiter zu Bob schicken.

iii.) Information des Lauschers, wenn er nicht in den Quantenkanal eingreift: Nur die Information, welche Hadamard-Transformationen Alice und Bob angewandt haben, keinerlei Information über das Bit.

iv.) Für die Analyse über den Erfolg von Lauschangriffen genügt es, die folgenden vier unterschiedlichen Situationen zu betrachten:

		
Kein Bitvergleich		
Bitvergleich		

Begründung: Eine Situation ist beschrieben durch folgende Parameter:

• Information ob $|a\rangle = |0\rangle$ oder $|a\rangle = |1\rangle$, dabei bezeichnet $|a\rangle$ den Zustand des QBits bei Alice nach der möglichen Anwendung von Pauli-X;

• Information, ob Alice H angewandt hat;

• Information, ob Bob H angewandt hat;

• Information, ob Alice und Bob ihre Bits verglichen (und dann verwarfen).

Das sind $2^4 = 16$ Situationen.

Im Schnitt jede zweite Situation wird verworfen, weil von Alice und Bob genau eine Hadamard-Transformation angewandt wurde. Diese Situationen brauchen nicht weiter betrachtet werden - sie verdoppeln nur den Aufwand, sind aber für die Sicherheit nicht von Belang.

Für die Analyse von Angriffen eines Lauschers dürfen wir wir o.B.d.A. annehmen, es sei $|a\rangle = |0\rangle$. Denn die Analysen können direkt auf den Fall $|a\rangle = |1\rangle$ übertragen werden.

v.) Zur Analyse einer Situation sind die folgenden Fragen zu beantworten:

• Ist $|b\rangle = |0\rangle$? Das beantwortet, ob durch den Eingriff von Eve der Schlüsselaustausch zwischen Alice und Bob gestört wurde.

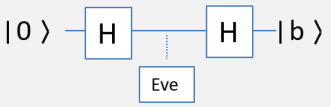
• Ist $|e\rangle = |0\rangle$? Das beantwortet, ob Eve das richtige Bit in Händen hält.

• Wird Eve entdeckt?

vi.) Für jeden möglichen Angriff müssen diese drei Fragen für jedes der vier Felder beantwortet werden. Denn Eve befindet sich beim Lauschangriff in einer der vier Situationen, dass beide H angewendet haben oder beide nicht, und dass ein Bitabgleich stattfinden wird oder nicht, **weiß aber zum Zeitpunkt des Angriffs nicht, in welcher**.

Übung in der Vorlesung:

a.) Analyse des CNOT-Angriffs (d.h., Eve benutzt das QBit in Kanal als Steuerbit für ihr eigenes mit $|0\rangle$ initialisiertes QBit):

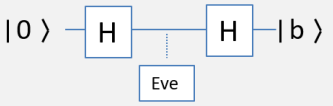
		
Kein Bitvergleich	Ist |b> = |0>? Ist |e> = |0>? Wird Eve entdeckt?	Ist |b> = |0>? Ist |e> = |0>? Wird Eve entdeckt?
Bitvergleich	Ist |b> = |0>? Ist |e> = |0>? Wird Eve entdeckt?	Ist |b> = |0>? Ist |e> = |0>? Wird Eve entdeckt?

Ergebnis:

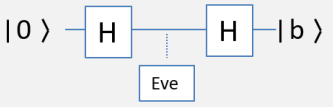
		
Kein Bitvergleich	Ist |b> = |0>? Ja Ist |e> = |0>? Ja Wird Eve entdeckt? Nein	Ist |b> = |0>? Mit Wkeit 1/2 Ist |e> = |0>? Mit Wkeit 1/2 Wird Eve entdeckt? Nein
Bitvergleich	Ist |b> = |0>? Ja Ist |e> = |0>? Ja Wird Eve entdeckt? Nein	Ist |b> = |0>? Mit Wkeit 1/2 Ist |e> = |0>? Mit Wkeit 1/2 Wird Eve entdeckt? Mit Wkeit 1/2

.

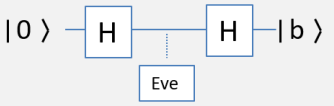
b.) Analyse des Messen-und-Weiterleiten-Angriffs (d.h., Eve misst das QBit im Kanal und speist das Messergebnis wieder ein):

		
Kein Bitvergleich	Ist |b> = |0>? Ist |e> = |0>? Wird Eve entdeckt?	Ist |b> = |0>? Ist |e> = |0>? Wird Eve entdeckt?
Bitvergleich	Ist |b> = |0>? Ist |e> = |0>? Wird Eve entdeckt?	Ist |b> = |0>? Ist |e> = |0>? Wird Eve entdeckt?

Ergebnis:

		
Kein Bitvergleich	Ist |b> = |0>? Ja Ist |e> = |0>? Ja Wird Eve entdeckt? Nein	Ist |b> = |0>? Mit Wkeit 1/2 Ist |e> = |0>? Mit Wkeit 1/2 Wird Eve entdeckt? Nein
Bitvergleich	Ist |b> = |0>? Ja Ist |e> = |0>? Ja Wird Eve entdeckt? Nein	Ist |b> = |0>? Mit Wkeit 1/2 Ist |e> = |0>? Mit Wkeit 1/2 Wird Eve entdeckt? Mit Wkeit 1/2

c.) Analyse des H-Messen-H-Weiterleiten-Angriffs (d.h., Eve wendet H auf das Qbit im Kanal an, misst, wendet wieder H an und leitet das so erhaltene QBit weiter an Bob):

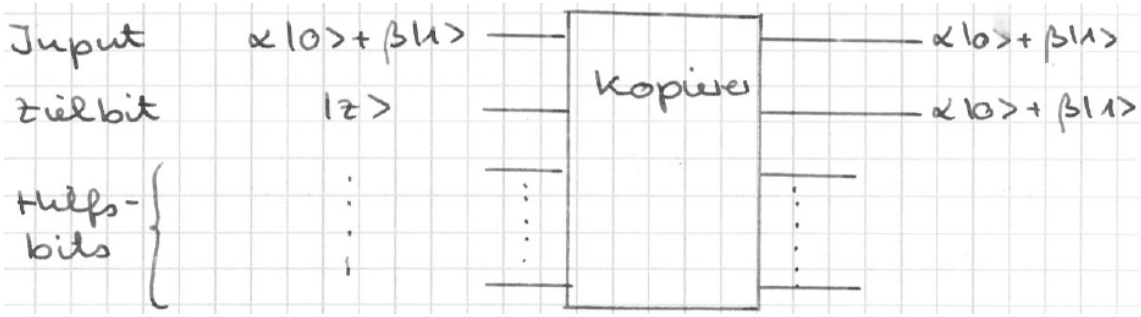
		
Kein Bitvergleich	Ist |b> = |0>? Ist |e> = |0>? Wird Eve entdeckt?	Ist |b> = |0>? Ist |e> = |0>? Wird Eve entdeckt?
Bitvergleich	Ist |b> = |0>? Ist |e> = |0>? Wird Eve entdeckt?	Ist |b> = |0>? Ist |e> = |0>? Wird Eve entdeckt?

.

Bemerkung: Die Situation des Lauschers im BB84-BProtokoll ist der Grund dafür, dass oft geschrieben wird, in der Quantenkryptographie würden Lauscher entdeckt.
Die genaue Aussage ist (für die betrachteten Angriffe von Eve):
• Mit Wahrscheinlichkeit 1/2 hat Eve das richtige Bit in Händen und wird nicht entdeckt (voller Erfolg für Eve);
• mit Wahrscheinlichkeit 1/2 hat Eve nur ein Zufallsbit in Händen;
• mit Wahrscheinlichkeit 1/4 hat Bob nach einem Angriff nur ein Zufallsbit in Händen;
• Mit Wahrscheinlichkeit 1/8 wird Eve entdeckt (das heißt aber, dass z.B. bei 25 Lauschangriffen Eve nur mit einer Wahrscheinlichkeit von $(7/8)^{25} <\approx 0.035$ unentdeckt bleibt).

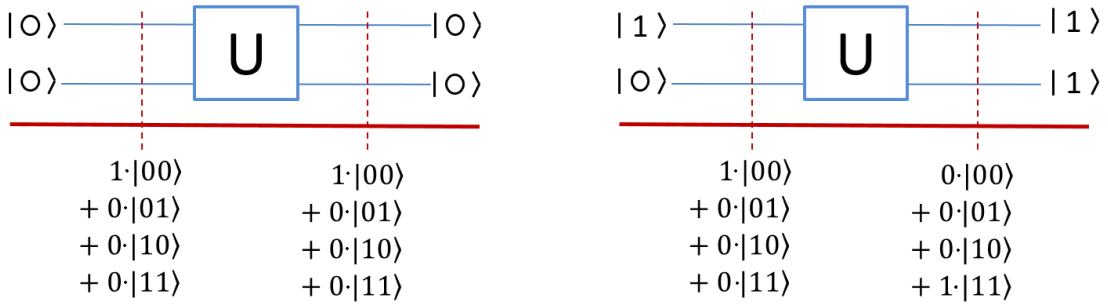
Satz: (No Cloning Theorem)
Es gibt keinen Quantenschaltkreis, der ein beliebiges QBit auf ein Zielbit kopiert.

Veranschaulichung: Sowas gibt es nicht:

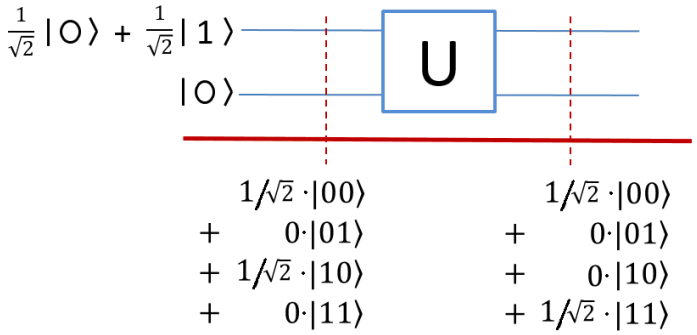


Ende der Veranschaulichung

Beweisidee: Spezialfall: Keine Hilfsbits, und Zielbit mit $|0\rangle$ initialisiert.
Der Kopierer führt dann eine unitäre Transformation U auf zwei QBits aus und kopiert sowohl den Zustand $|0\rangle$ als auch den Zustand $|1\rangle$ des Input-Bits, also $U|00\rangle = |00\rangle$ und $U|10\rangle = |11\rangle$):



Damit liefert der Kopierer aber bei Input des QBits $1/\sqrt{2} \cdot |0\rangle + 1/\sqrt{2} \cdot |1\rangle$ den Zustand $U(1/\sqrt{2} \cdot |00\rangle + 1/\sqrt{2} \cdot |10\rangle$, also $1/\sqrt{2}(|00\rangle + |11\rangle)$.



Das ist nicht der Klon des Inputs, dieser wäre $0.5 \cdot (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$.

Beweis: (Nach Homeister, "Quantencomputing verstehen", S. 82)
Angenommen, es gibt eine Kopierttransformation U und eine feste Input-Belegung $|s\rangle$ des Zielbits und der Hilfsbits, sodass für jeden Zustand $|q\rangle$ des Input-Bits gilt:

$$U(|q\rangle \otimes |s\rangle) = |q\rangle \otimes |q\rangle \otimes |s_q\rangle$$

mit einem vom Input abhängigen Outputzustand $|s_q\rangle$ der Hilfsbits.

Wendet man das auf zwei unterschiedliche Input-Bits $|q_1\rangle$ und $|q_2\rangle$ an, erhält man

$$U(|q_1\rangle \otimes |s\rangle) = |q_1\rangle \otimes |q\rangle \otimes |s_{q_1}\rangle \text{ und}$$
$$U(|q_2\rangle \otimes |s\rangle) = |q_2\rangle \otimes |q\rangle \otimes |s_{q_2}\rangle$$

Unitäre Transformationen sind winkelerhaltend, also stimmen stets die Skalarprodukte der Urbilder und der Bilder überein. Es ist also $< Uv|Uw >=< v|w >$ für alle Vektoren v, w. Das bedeutet

$$< q_1 \otimes s \,|\, q_2 \otimes s >=< q_1 \otimes q_1 \otimes s_{q_1} \,|\, q_2 \otimes q_2 \otimes s_{q_2} >$$

Da sich Skalarprodukt und Tensorprodukt vertragen, kann man umformen:

$$< q_1 \,|\, q_2 >< s \,|\, s >=< q_1 \,|\, q_2 >< q_1 \,|\, q_2 >< s_{q_1} \,|\, s_{q_2} >$$

Die Gleichung ist erfüllt, wenn $< q_1 \,|\, q_2 >= 0$, wenn also q_1 und q_2 senkrecht stehen. Andernfalls kann sie umgeformt werden zu

$$< s \,|\, s >=< q_1 \,|\, q_2 >< s_{q_1} \,|\, s_{q_2} >$$

also (da $|s\rangle$ Zustand eines Teilregisters ist und somit $< s \,|\, s >= 1$ gilt:

$$1 =< q_1 \,|\, q_2 >< s_{q_1} \,|\, s_{q_2} >$$

Da q_1, q_2, s_{q_1} und s_{q_2} Registerzustände sind und damit Länge 1 haben, sind ihre Skalarprodukte untereinander dem Betrag nach höchstens 1. Die 1 wird nur bei Parallelität erreicht. Somit kann die Gleichung nur dann erfüllt sein, wenn q_1 und q_2 parallel sind.

Klont also ein Kopierer den Zustand $|q\rangle$ eiens QBits korrekt, so kann er außer diesem Zustand nur dazu parallele oder orthogonale QBits klonen. D.h., es gibt keinen Kopierer, der beliebige QBits klonen kann. Q.e.d.

3.5 Dichte Codierung

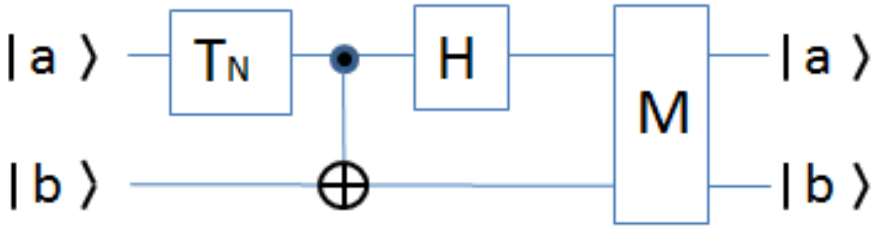
Ein Ausflug in die Informationstheorie: Diese beschäftigt sich mit dem Informationsgehalt (und den Redundanzen) in Nachrichten, und der dichten, bestcodierten Speicherung von Informationen auf Datenträgern.
Erkenntnis wird sein: Es ist möglich, die Information von zwei klassischen Bits auf einen QBit zu transportieren, wenn dieses Teil eines EPR-Paares ist.

Aufgabe: Alice will eine der Nachrichten $N = (x, y) \in \{(0,0), (0,1), (1,0), (1,1)\}$ an Bob schicken.
Sie besitzen zwei verschränkte QBits $|a\rangle, |b\rangle$ im Zustand $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, und die Möglichkeit, ein QBit zu senden(Quantenkanal).

Lösung: Alice wählt die von der Nachricht abhängige Transformation T_N aus

$$T_N = \begin{cases} ID, & \text{falls } N = (0,0) \\ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, & \text{falls } N = (0,1) \\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, & \text{falls } N = (1,0) \\ Z \cdot X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, & \text{falls } N = (1,1) \end{cases}$$

Sie wendet T_N auf $|a\rangle$ an und schickt es Bob.
Bob wendet CNOT auf $|ab\rangle$ an, und misst beide Bits.
Ist das Ergebnis der Messung $|xy\rangle$, so war $N = (x, y)$, $x, y \in \{0, 1\}$.



Satz: Das Verfahren arbeitet in allen 4 Fällen korrekt.

Bew: Übungsaufgabe, man muss die vier Fälle unterscheiden.

Bem: i.) Beweisidee algebraisch: Die unitäre Matrix von Bobs Transformation ist

$$U = (H \otimes Id) * CNOT = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix}$$

Durch die vorgeschaltete Transformation T_N entscheidet Alice, ob die erste und letzte Spalte oder die zweite und dritte Spalte gemessen werden, und ob sie zuvor addiert oder subtrahiert werden.

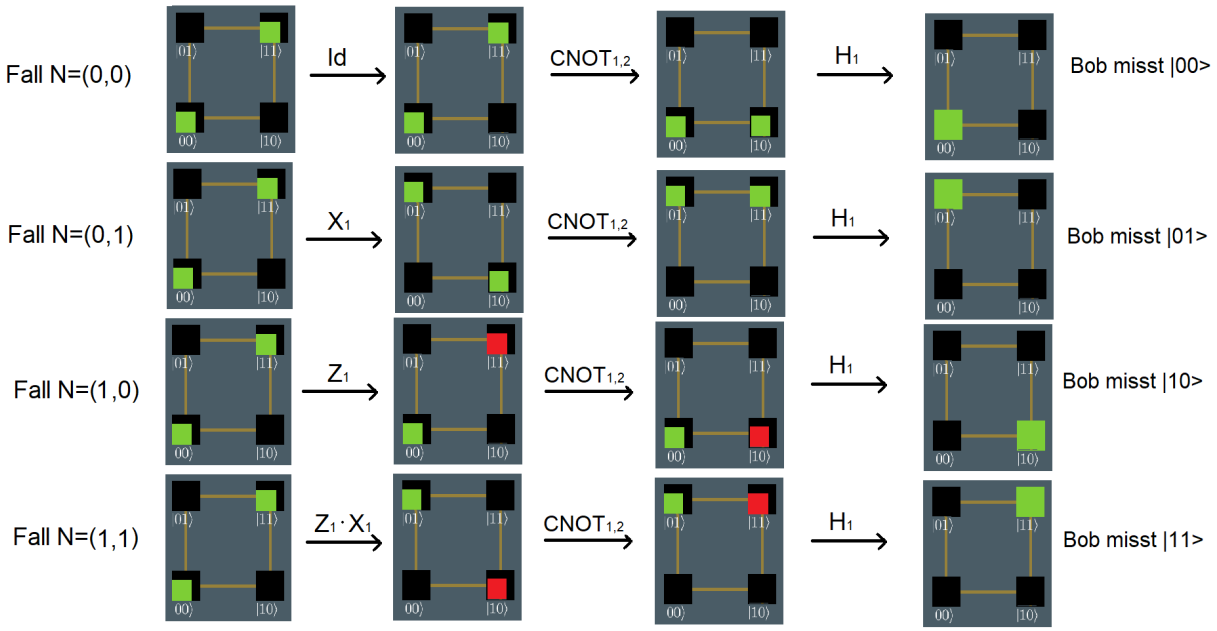
ii.) Wie kommt man auf sowas?
Der Zustandsraum zweier QBits, ein $\mathbb{R}^2 \otimes \mathbb{R}^2$, hat die Standardbasisvektoren $|00\rangle, |01\rangle, |10\rangle$ und $|11\rangle$. Jeder Vektor im Zustandsraum ist also eine Linearkombination $\sum_{i=0}^{3} \alpha_i |i\rangle$.

Die folgenden Vektoren bilden ebenfalls eine Basis des Zustandsraumes, die Bell-Basis aus Bell-Zuständen:

$$\Phi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad ,\Phi^- = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad ,$$
$$\Psi^+ = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad ,\Psi^- = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Die Bell-Basis ist recht weit bekannt, und die Idee des Algorithmus ist es, dass Alice ihr QBit in einen der vier Bell-Zustände versetzt. Duchr CNOT und Hadamard werden dann beide QBits in einen ihrer 4 Basiszustände zurücktransformiert.

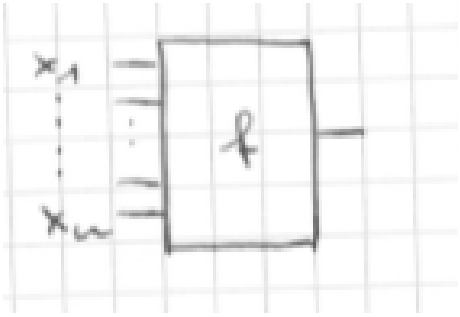
iii.) Graphische Veranschaulichung der dichten Codierung, je eine Zeile pro Fall:



3.6 Quantenorakel entschlüsseln

Die Algorithmen von Deutsch, Deutsch-Jozsa und Bernstein-Vazirani

Definition: Ein (klassisches) Orakel für eine Funktion $f : \{0,1\}^n \to \{0,1\}$ ist ein Bauteil mit n Input-Bits und einem Output-Bit, das die Funktion berechnet:

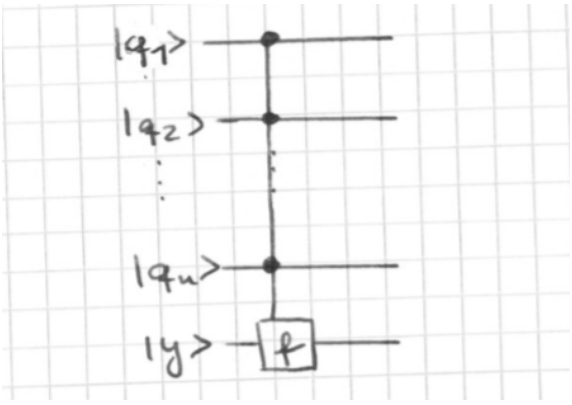


Anwendungen: z.B. Komplexitätstheorie, NP-Vollständigkeits-Beweise.

Bemerkungen: Gegeben Orakel, gesucht die Funktion f:

- Ohne weitere Information muß man 2^n Inputs ausprobieren, das Orakel also 2^n mal aufrufen.
- Mit Zusatzinformationen kommt man evtl. mit weniger Aufrufen des Orakels aus. Ist z.B. $f = const$ bekannt, genügt ein Aufruf mit einem beliebigen Input.

Definition: Ein Quantenorakel für $f : \{0,1\}^n \to \{0,1\}$ ist ein Quantengatter mit $n+1$ Inputs



und folgender Wirkung auf die Basiszustände

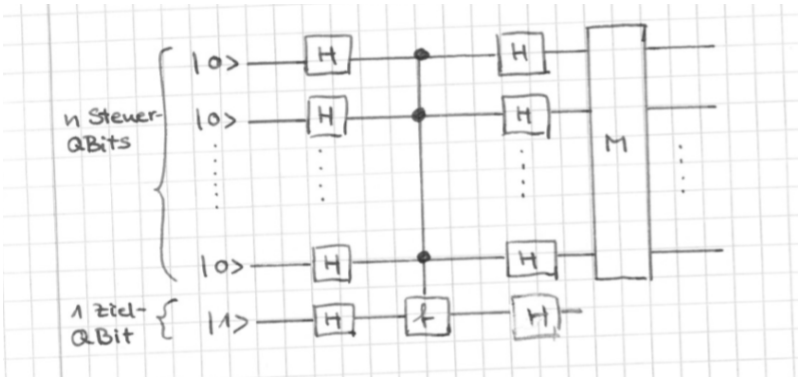
$$|x_1 \cdots x_n y\rangle \mapsto |x_1 \cdots x_n\rangle |y \oplus f(x)\rangle$$

Mit anderen Worten: y-Bit wird negiert genau dann, wenn $f(x_1, \cdots, x_n) = 1$

Aufgabe: Gegeben Quantenorakel für f und Zusatzinformation, dass f entweder konstant (d.h. entweder überall 1 oder überall 0) ist, oder balanciert(d.h., genau auf der Hälfte des Inputs 1 und auf der anderen Hälfte des Inputs 0) ist. Entscheide, ob f balanciert oder konstant ist.

Bemerkung: Aufrufe für ein klassisches Orakel: Im Worst case $2^{n-1}+1$ Aufrufe.
Wir zeigen: Es geht mit einem einzigen Aufruf des Quantenorakels.

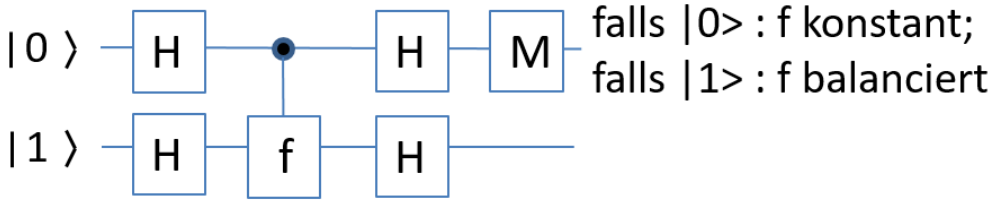
Satz: (Algorithmus von Deutsch-Jozsa, 1992) Sei $f : \{0,1\}^n \to \{0,1\}$ konstant oder balanciert. Dann liefert der folgende Quantenschaltkreis das Ergebnis $|0\cdots 0\rangle$ genau dann, wenn f konstant ist:



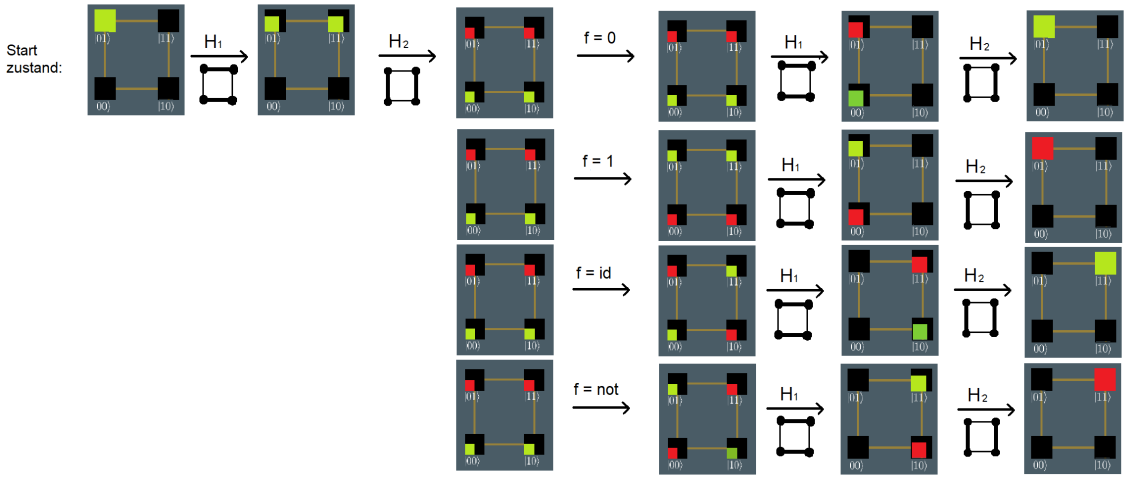
Bemerkung:

i.) Wie kann das sein: Die Steuerbits werden transformiert, zur Steuerung benutzt (nicht gemessen!) und rücktransformiert, und ändern ihren Zustand? Das tun sie, weil sich die Vorzeichen vor den Basiszuständen $(x_1, \cdots, x_n)$ durch den Aufruf vom Quantenorakel ändern, wenn $f(x_1, ..., x_n) = 1$ gilt.

ii.) Veranschaulichung für $n = 1$: Schaltkreis:



Graphische Analyse:



Messen des ersten QBits liefert $|0\rangle$, falls f konstant war, und $|1\rangle$, falls f die Identität oder das NOT ist (also balanciert).

iii.) Für $n \geq 2$ kommt die graphische Veranschaulichung an ihre Grenzen.
Nich tmehr jede Funktion ist konstant oder balanciert.
Wendet man den Deutsch-Josza-Algorithmus auf das Quantenorakel der AND-Funktion an, erhält man als Endzustand:
$0.5 \cdot (|001\rangle + |011\rangle + |101\rangle - |111\rangle)$
(wer möchte, überzeugt sich).

Beweis: (Korrektheit des Verfahrens für beliebiges n)
Nach Anwendung der ersten Hadamard-Transformationen ist das Register im Zustand

$$\frac{1}{\sqrt{2}^{n+1}} \cdot (|0\rangle + |1\rangle)^n \cdot (|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}^{n+1}} \cdot (\sum_{\substack{x \in \{0,1\}^n \\ x = (x_1, \cdots, x_n)}} |x_1 \cdots x_n\rangle) \cdot (|0\rangle - |1\rangle)$$

Nach Anwendung des Quantenorakels ist das Register im Zustand

$$|\psi\rangle = \frac{1}{\sqrt{2}^{n+1}} \cdot (\sum_{x \in \{0,1\}^n} |x_1 \cdots x_n\rangle \cdot (-1)^{f(x)}) \cdot (|0\rangle - |1\rangle)$$

Denn:

Fall $f(x_1, \cdots, x_n) = 0 \Rightarrow$ Quantenorakel überführt Zustand

$$\frac{1}{\sqrt{2}}|x_1 \cdots x_n\rangle \cdot (|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|x_1 \cdots x_n 0\rangle - |x_1 \cdots x_n 1\rangle)$$

in sich selbst, also

$$(-1)^{f(x)}|x_1 \cdots x_n\rangle \cdot (|0\rangle - |1\rangle)$$

Fall $f(x_1, \cdots, x_n) = 1 \Rightarrow$ Quantenorakel überführt Zustand

$$\frac{1}{\sqrt{2}}|x_1 \cdots x_n\rangle(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|x_1 \cdots x_n 0\rangle - |x_1 \cdots x_n 1\rangle)$$

in

$$\frac{1}{\sqrt{2}}(|x_1 \cdots x_n 1\rangle - |x_1 \cdots x_n 0\rangle) = \frac{1}{\sqrt{2}}|x_1 \cdots x_n\rangle \cdot (|1\rangle - |0\rangle) = (-1)^{f(x)} \cdot |x_1 \cdots x_n\rangle \cdot (|0\rangle - |1\rangle)$$

Sei nun H_n das n-fache Tensorprodukt der Hadamard-Matrix $\frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.
Man überzeugt sich, dass in der ersten Zeile von H_n überall die Zahl $\frac{1}{\sqrt{2^n}}$ steht.(Weitere Eigenschaften von $H_n \rightarrow$ Übungsaufgabe)
H_n ist eine unitäre Transformation (denn es ist ein Tensorprodukt unitärer Transformationen).
Der Zustand $|\psi\rangle$ wird durch Anwenden von $H_n \otimes H$ überführt in einen Zustand

$$(\sum_{x \in \{0,1\}^n} \alpha_x \cdot |x_1 \cdots x_n\rangle) \cdot |1\rangle$$

für bestimmte $\alpha_x \in \mathbb{C}$ mit $\sum |\alpha_x|^2 = 1$
Wir betrachten $\alpha_{0\cdots 0}$, das erste Element des Vektors

$$H_n \cdot \frac{1}{\sqrt{2}^n} \cdot \underbrace{\begin{pmatrix} (-1)^{f((0\cdots 0))} \\ (-1)^{f((0\cdots 01))} \\ \vdots \\ (-1)^{f((1\cdots 1))} \end{pmatrix}}_{:=v}$$

Ist f konstant, sind alle Koeffizienten von v identisch (+1 oder -1), und es ist $\alpha_{0\cdots 0} = \pm\frac{1}{\sqrt{2}^n} \cdot 2^n \cdot \frac{1}{\sqrt{2}^n} = 1$
Dann ist aber $\alpha_x = 0$ für alle $x \neq (0, \cdots, 0)$, denn sonst wäre $\sum_x |\alpha_x|^2 > 1$.
Die Messung ergibt also sicher den Zustand $|0 \cdots 0\rangle$.
Ist f balanciert, so hat genau die Hälfte der Koeffizienten von v den Wert 0, die andere Hälfte den Wert 1. Es ist also $\alpha_{0\cdots 0} = 0$, und die Messung ergibt nie den Wert $|0 \cdots 0\rangle$.

Übungsaufgabe: Diesen Algorithmus für $n = 1$ und $n = 3$ nachvollziehen.
(Optional: Auch noch den Algorithmus von Bernstein-Vazirani, nächter Abschnitt, wenn Sie ihn sich selbst anlesen möchten ;)).

Der Algorithmus von Bernstein-Vazirani(1993):

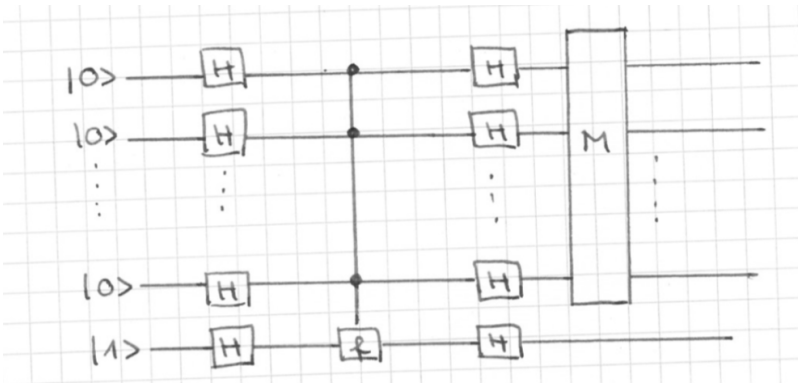
Hintergrund: Im Algorithmus von Deutsch-Jozsa kommt also der Zustand $|0\cdots 0\rangle$ für balancierte f gar nicht, für konstante f immer heraus. Bernstein und Vazirani haben 1993 gefunden, dass andere Funktionen f andere Zustände „ganz oder gar nicht“ liefern. Ein Beispiel ist der folgende Algorithmus von Bernstein-Vazirani (wobei der kritische Leser schon bemerkt, dass diese Algorithmen noch nicht in der Lage waren, das Quantencomputing aus seinem Schattendasein ans Licht zu holen - das hat erst 1994 der Faktorisierungsalgorithmus von Shor geschafft).

Input: Ein Quantenorakel für $f : \{0,1\}^n \to \{0,1\}$, für das bekannt ist: $f(x_1, \cdots, x_n) = (x_1, \cdots, x_n) * (a_1, \cdots, a_n)$ für ein $a \in \{0,1\}^n$.
Dabei ist * das Skalarprodukt mod 2.

Output: $a \in \{0,1\}^n$

Verfahren:

i.) Wende das Quantengatter des Deutsch-Jozsa-Algorithmus an:



ii.) Gibt das Meßergebnis $a \in \{0,1\}^n$ aus.

Anzahl Gatter: Ein Orakelaufruf, $2(n+1)$ Hadamard-Gatter (es reichen auch $2n+1$ Gatter, denn y muss am Ende nicht mehr transformiert werden), und eine Messung von n QBits.

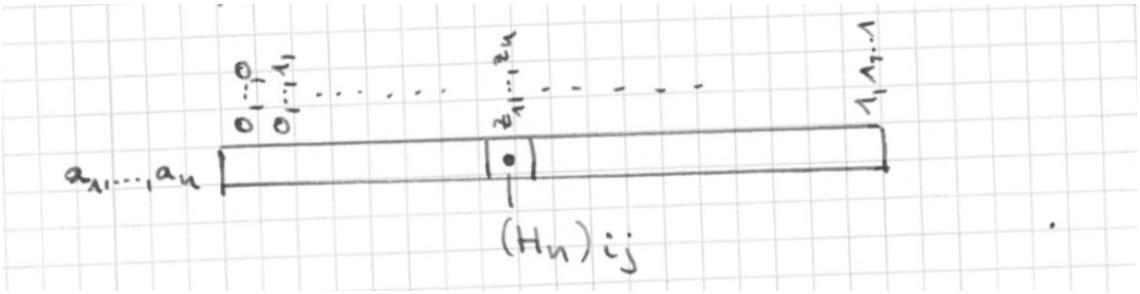
Korrektheit: Wie in der Analyse des Algorithmus von Deutsch-Jozsa zeigt man: Vor der Messung ist das QRegister im Zustand

$$(\sum_{k=0}^{2^k-1} \alpha_k |k\rangle) \cdot |1\rangle.$$

Dabei ist

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{2^n-1} \end{pmatrix} = H_n \cdot \frac{1}{\sqrt{2}^n} \cdot \begin{pmatrix} (-1)^{f(0,\cdots,0,0)} \\ (-1)^{f(0,\cdots,0,1)} \\ (-1)^{f(0,\cdots,1,0)} \\ \vdots \\ (-1)^{f(1,\cdots,1,1)} \end{pmatrix}$$

Sei i der Index, der zu $(a_1, \cdots, a_n)$ gehört, also $i = \sum_{k=1}^{n} a_k 2^{n-k}$.
Wir betrachten die i-te Zeile der Hadamard-Matrix H_n. Sei $j \in \{0, \cdots, 2^n - 1\}$ ein Spaltenindex, $j = \sum_{k=1}^{n} z_k 2^{n-k}$ für $z_1, \cdots, z_n \in \{0, 1\}$.



Dann ist ($\rightarrow$ Übungsaufgabe)

$$(H_n)_{ij} = \frac{1}{\sqrt{2}^2} \cdot (-1)^{(a_1,\cdots,a_n) \cdot (z_1,\cdots,z_n)}$$

Deshalb ist

$$\alpha_i = \frac{1}{2^n} \cdot \sum_{z \in \{0,1\}^n, z=(z_1,\cdots,z_n)} (-1)^{(a_1,\cdots,a_n)*(z_1,\cdots,z_n)} \cdot (-1)^{f(z_1,\cdots,z_n)} = 1$$

weil $f(z_1, \cdots, z_n) = (a_1, \cdots, a_n) \cdot (z_1, \cdots, z_n)$. (Man sieht: Die -1en treffen auf die -1en, die +1en auf die +1en).
D.h., alle anderen α_j sind 0, $j \in \{0, \cdots, 2^{n-1}\} \setminus \{i\}$.
Messen der ersten n Bits des Registers liefert also den Zustand $|i\rangle$, also $|a_1, \cdots, a_n\rangle$.

4 Grover-Iteration zur Suche in unstrukturierten Daten

Lernziele:

- Die Grundidee des Grover-Algorithmus verstanden haben (d.h., Problemstellung und Lösungsansatz kennen)
- Grover-Algorithmus selbst für $n = 3$ analysiert haben
- (Fortgeschrittene) Laufzeitanalyse für $n = 5$ nachvollzogen haben
- (Abstrakteres Ziel) Einmal einen echten Quantenalgorithmus (d.h., eine Folge von Schaltkreisen) und seine Analyse gesehen haben.

4.1 Problemstellung und Grundidee

Problemstellung: Suche aus $N = 2^n$ unstrukturierten Daten, z.B. unstrukturierten Einträgen in einer Datenbank, einen gegebenen Wert heraus.
Allgemeiner: Suche für eine gegebenen Funktion den URBILDwert eines gegebenen BILDwertes.
Bsp: Suche im gedruckten Telefonbuch den Inhaber einer vorgegebenen Telfonnummer.

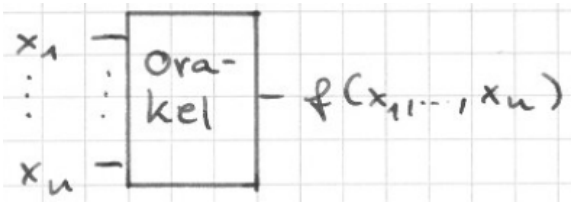
Adresse bzw. Funktionsinput (Urbild)	Inhalt bzw. Funktionswert (Bildwert)
$0 \dots 0$	$f(0 \dots 0)$
$0 \dots 1$	$f(0 \dots 1)$
$\vdots$	$\vdots$
$1 \dots 1$	$f(1 \dots 1)$

Allgemein: $f : \{0,1\}^n \to$ Wertebereich.

Hier immer: $f : \{0,1\}^n \to \{0,1\}$

- Technische Vereinfachung im Folgenden, um zum Kern des Problems zu kommen: Wir nehmen weiter an, es gibt genau EIN $\hat{x} = (\hat{x}_1, \cdots, \hat{x}_n)$ mit $f(\hat{x}) = 1$, ansonsten sei $f(x) = 0$.

- Klassische Situation: Lesender Zugriff über Schnittstelle, das „Orakel"



Klassische Komplexität Funktionswertberechnung (d.h., gegeben $x_1, \ldots, x_n$, bestimme $f(x_1, \ldots, x_n)$):

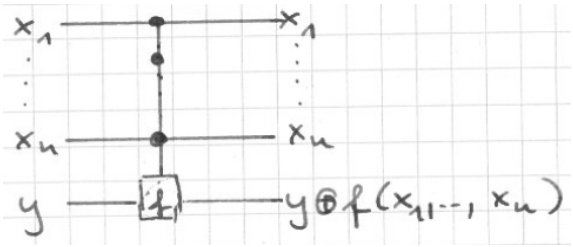
1 Orakelaufruf.

Klassische Komplexität Urbildberechnung (d.h., gegeben $f(x_1, \ldots, x_n)$, finde Urbild $x_1, \ldots, x_n$):

Im Mittel $\frac{N}{2}$, im worst case N, also in beiden Fällen $O(N)$ Orakelaufrufe.

Anwendung nicht nur Datenbanken, sondern alle „leicht" zu berechnenden Funktionen. Z.B. auch Test von Zeugen bei NP-vollständigen Problemen.

- Quantenalgorithmen: Zugriff über Quantenorakel



Quantenkomplexität mit Grovers Algorithmus: (Probabilistisch) mit $O(\sqrt{N}) = O(2^{n/2})$ Aufrufen eines Quantenorakels.
Immer noch exponentiell in der Länge des Inputs, aber auch exponentiell schneller als klassischer Algorithmus. Auch Quantenalgorithmen können also NP-vollständige Probleme nicht in probabilistischer Polynomialzeit lösen.

Vorschau Vorgehen:

i.) Zwei wesentliche Zutaten bereitstellen:

„Orakel mit $y = H|1\rangle$ dreht Vorzeichen der Trefferampliduden um" und

„Spiegelung am Mittelwert"

ii.) Anschauliche Grundidee des Grover-Algorithmus verstehen

iii.) Analyse des Algorithmus für $n = 3$

iv.) Analyse des Algorithmus für beliebiges n.

Satz: (Eigenschaften eines Quantenorakels - zum warm werden :)):

a.) Ist Input Basiszustand, so ist Output Basiszustand. Genauer:

Input $(x_1, \ldots, x_n) \in \{0,1\}^n,\ y = 0 \Rightarrow$ Quantenorakel liefert bei Eingabe des Basiszustandes $|x_1\ x_2 \ldots\ , x_n\ 0\rangle$ den Basiszustand $|x_1\ x_2 \ldots\ x_n f(x_1\ \ldots, x_n)\rangle$.

Input $(x_1\ \ldots\ x_n) \in \{0,1\},\ y = 1 \Rightarrow$ Quantenorakel liefert bei Eingabe des Basiszustandes $|x_1\ x_2 \ldots\ x_n 1\rangle$ den Basiszustand $|x_1\ x_2 \ldots\ x_n\ \neg f(x_1, \ldots, x_n)\rangle$

b.) Für $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ liefert das Quantenorakel

bei Input $|x_1, \ldots, x_n\rangle \cdot (\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$

den Output $(-1)^{f(x_1,\ldots,x_n)} \cdot |x_1, \ldots, x_n\rangle \cdot (\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Beweis: a.) klar. Beweis b.):

$$|x_1, \ldots, x_n\rangle \cdot (\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)) \mapsto |x_1, \ldots, x_n\rangle \cdot \frac{1}{\sqrt{2}} \cdot (|f(x)\rangle - |1 \oplus f(x)\rangle)$$

$$= \begin{cases} |x_1, \ldots, x_n\rangle \cdot \frac{1}{\sqrt{2}} \cdot (|0\rangle - |1\rangle) & \text{falls } f(x) = 0 \\ |x_1, \ldots, x_n\rangle \cdot \frac{1}{\sqrt{2}} \cdot (|1\rangle - |0\rangle) & \text{falls } f(x) = 1 \end{cases}$$

$$= (-1)^{f(x)} \cdot |x_1, \ldots, x_n\rangle \cdot \frac{1}{\sqrt{2}} \cdot (|0\rangle - |1\rangle).$$

Folgerung: Orakel mit $y = H|1\rangle$ dreht Vorzeichen der Trefferampliduden um: Ist bei Aufruf des Quantenorakels der Zustand des Registers

$$|q_1 ... q_n\ \rangle \cdot y = \left(\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \right) \cdot y$$

mit $y = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ und beliebigen Amplituden α_x, so ist der Zustand nach Aufruf des Quantenorakels

$$|q_1 ... q_n\ \rangle \cdot y = \left(\sum_{x \in \{0,1\}^n} \pm\alpha_x |x\rangle \right) \cdot y$$

wobei genau die α_x das negative Vorzeichen haben, für die $f(x) = 1$ gilt.

Beispiel zur Vorzeichenumkehr der Trefferamplituden:

Zustand $|q_1 q_2 q_3\rangle$ sei $\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{2}|001\rangle - \frac{1}{2}|110\rangle$.

Anwenden des Quantenorakels für $f(x_1, x_2, x_3) = x_1 \vee x_2 \vee x_3$ und $y = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ liefert

$$\left(\frac{1}{\sqrt{2}}|000\rangle - \frac{1}{2}|001\rangle + \frac{1}{2}|110\rangle \right) \cdot \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right).$$

Es folgt die zweite Zutat, das Spiegeln am Mittelwert.

Satz: **Spiegelung am Mittelwert** Für $N \in \mathbb{N}$ sei D_N die $N \times N$-Matrix

$$D_N = -\begin{pmatrix} 1 & & & \\ & 1 & 0 & \\ & 0 & \ddots & \\ & & & 1 \end{pmatrix} + \tfrac{2}{N} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & & & \vdots \\ 1 & 1 & \dots & 1 \end{pmatrix},$$

also

$$(D_N)_{ij} = \begin{cases} -1 + \frac{2}{N} & \text{für } i = j, \quad i,j \in \{0, \cdots, N-1\} \\ \frac{2}{N} & \text{für } i \neq j, \quad i,j \in \{0, \cdots, N-1\} \end{cases}$$

Dann gilt:

i.) D_N ist unitär

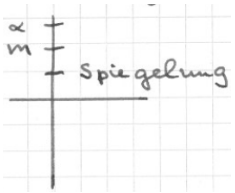
ii.) Für jeden Koeffizientenvektor $(\alpha_0, \cdots, \alpha_{N-1}) \in \mathbb{R}^N$ spiegelt die durch D_N beschriebene lineare Abbildung jeden Koeffizienten am Mittelwert $m = \sum_{i=0}^{N-1} \alpha_i / N$

$$D_N \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} -\alpha_0 + 2m \\ -\alpha_1 + 2m \\ \vdots \\ -\alpha_{N-1} + 2m \end{pmatrix}.$$

Beweis: Übungsaufgabe.

Bemerkung:

i.) Warum Spiegelung?
Veranschaulichung Spiegelung von α an irgendeinem Wert m:



Wert Spiegelung $= \alpha - 2(\alpha - m) = -\alpha + 2m$.

Man überlegt es sich auch für andere Lagen von α und m.

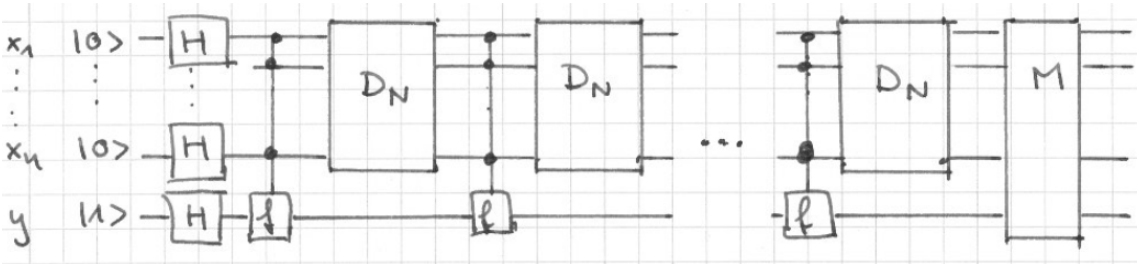
ii.) Man kann D_N mit $O(n)$ Quantengattern bauen, denn es ist $D_N = H^{\otimes n} \cdot R_N \cdot H^{\otimes n}$.

Dabei ist $H^{\otimes n}$ das n-fache Tensorprodukt der $2 \times 2-$Hadamard-Matrix, und R_N ist die $n \times n$Einheitsmatrix, die nur an der Position Zeile 1, Saplte 1 verändert wurde: Hier steht eine -1 statt einer 1.

Nun muss man natürlich auch wieder überlegen, dass R_N mit $O(n)$ Gattern hergestellt werden kann. Siehe dazu Homeister, „Quantencomputing verstehen“ :) .

Grundidee des Grover-Algorithmus

Hier ist der Schaltkreis (noch nicht quantifiziert, wie oft das Orakel aufgerufen wird):



Idee hinter dem Algorithmus ist das „Katapult“ :

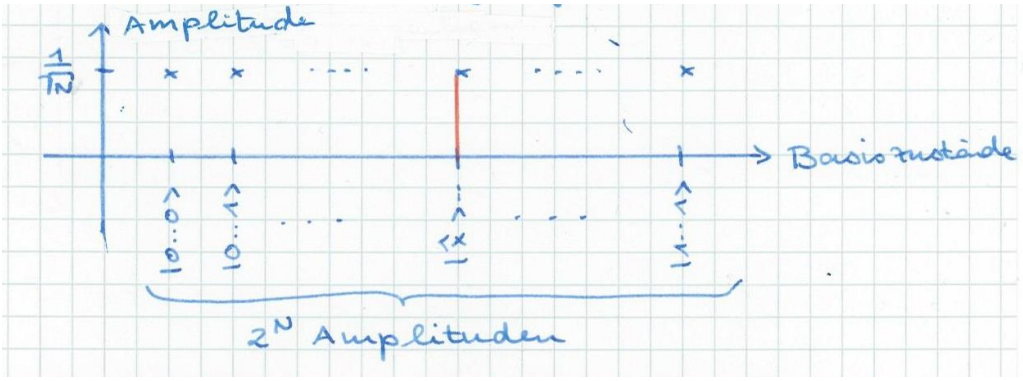
i.) Zustandsvektor nach Anwendung der Hadamard-Transformation:

Alle x-Ampliduden sind $1/\sqrt{N}$

y ist im Zustand $H|1\rangle$

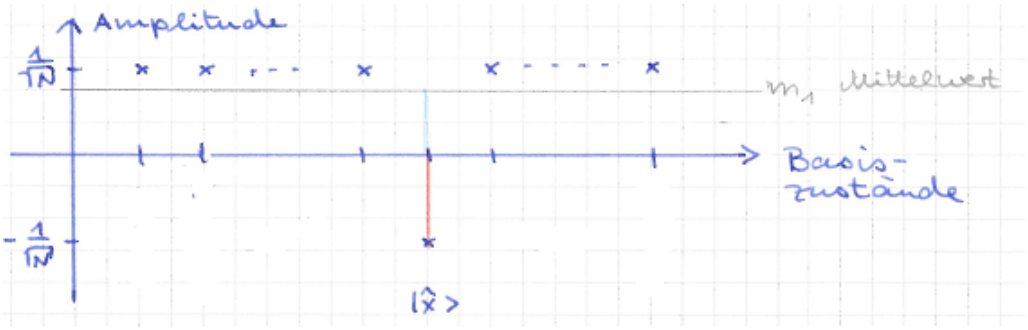
(y bleibt auch in diesem Zustand und wird daher nicht mitgezeichnet)

Die Amplituden der ersten n QBits sind:

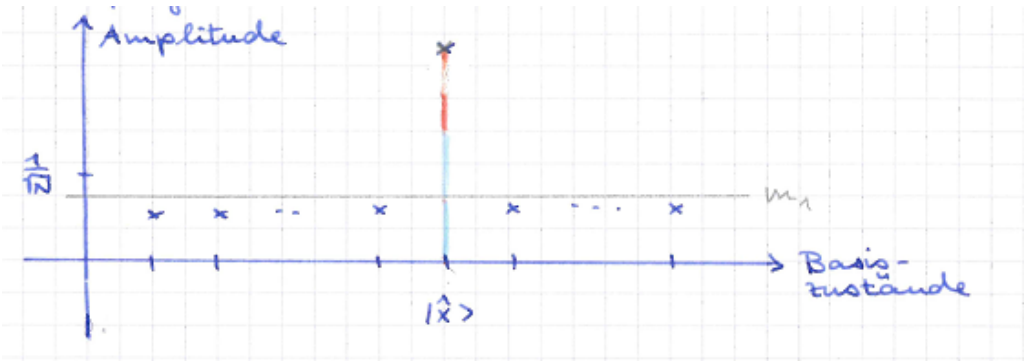


Bekannt ist nur, dass $|\hat{x}\rangle$ mit $f(\hat{x}) = 1$ existiert und eindeutig ist. $|\hat{x}\rangle$ ist gesucht.

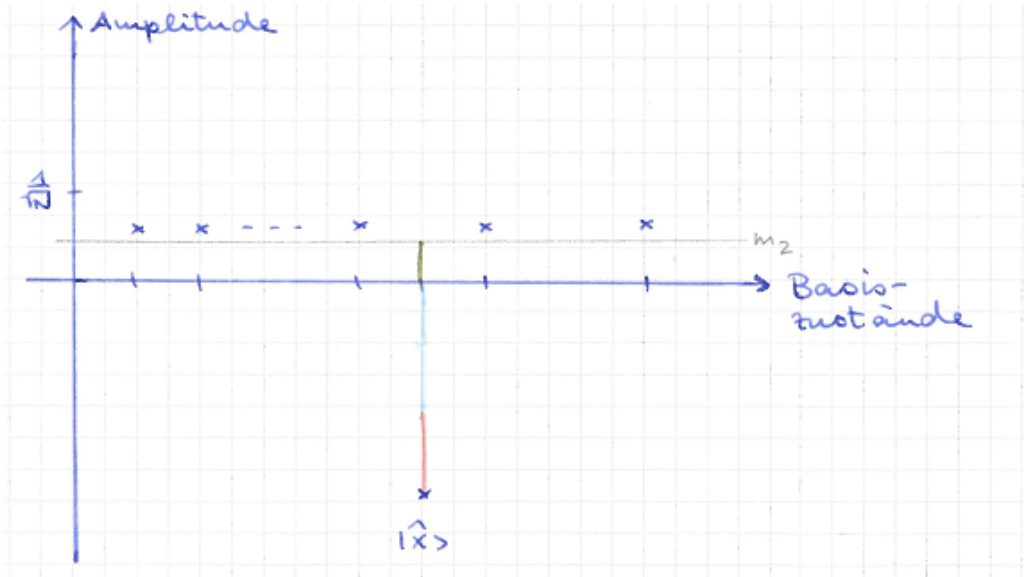
ii.) Quantenorakel anwenden



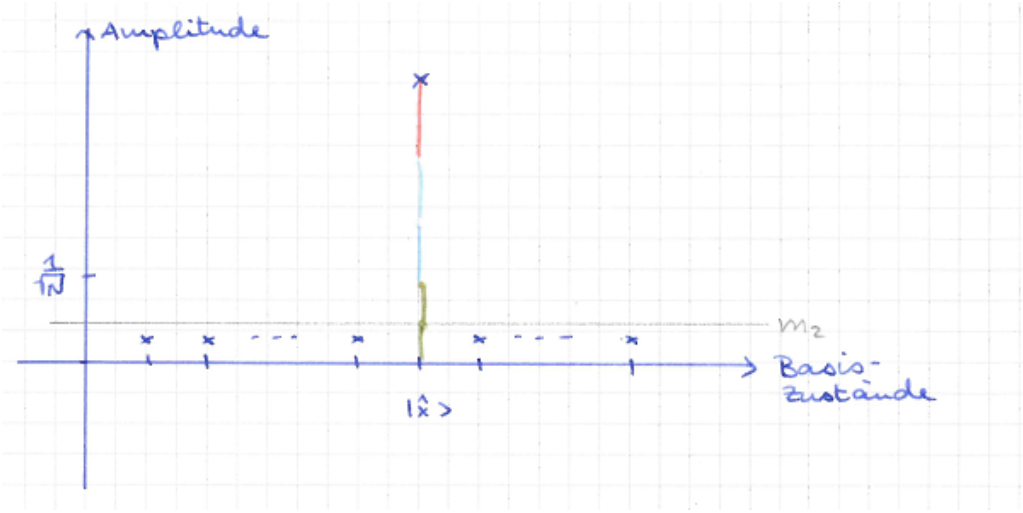
iii.) Spiegeln am Mittelwert



iv.) Quantenorakel anwenden:



v.) Spiegeln am (neuen) Mittelwert



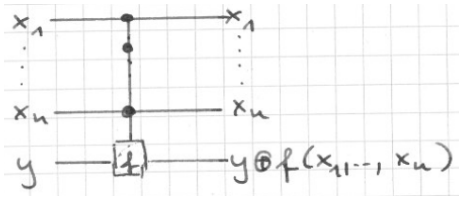
$\cdots$ etc, bis Messung mit höchster Wkeit $|\hat{x}\rangle$ liefert (Amplitiude für $\hat{x}$ wird wieder kleiner, sobald die Amplitude für die anderen Basisvektoren negativ werden).

Die Kunst ist es nun, die genau richtige Anzahl von Anwendungen des Quantenorakels und D_N zu finden, und zu beweisen, dass es $= (\sqrt{N})$ ist.

4.2 Grover-Algorithmus für n=3, N=8

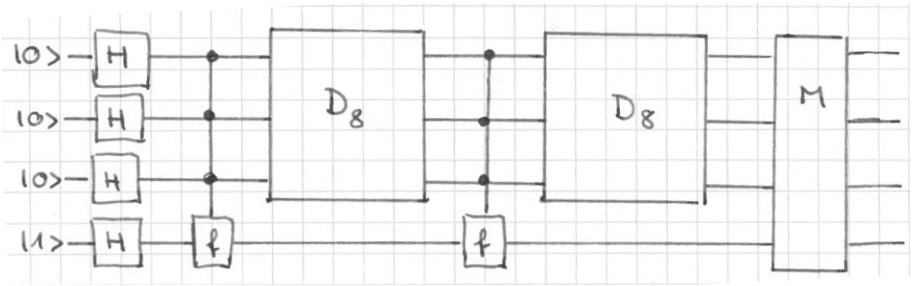
Aufgabenstellung: $f : \{0,1\}^3 \to \{0,1\}$ sei 1 an genau einer Stelle $\hat{x} = (\hat{x}_1, \hat{x}_2, \hat{x}_3)$, und sei sonst 0.

Gegeben ist ein Quantenorakel



Finde das $\hat{x} = (\hat{x}_1, \hat{x}_2, \hat{x}_3) \in \{0,1\}^3$ mit $f(\hat{x}) = 1$ mit möglichst wenigen Orakelaufrufen.

Grover's Algorithmus für $n = 3$:



Gib die ersten drei Bits des Messergebnisses aus. Dabei ist D_8 die unimodulare Transformation, die durch die folgende 8×8-Matrix beschrieben wird:

$$\begin{pmatrix} -\frac{3}{4} & \frac{1}{4} & \cdots & & \frac{1}{4} \\ \frac{1}{4} & -\frac{3}{4} & \ddots & & \vdots \\ \frac{1}{4} & \frac{1}{4} & \ddots & & \frac{1}{4} \\ \vdots & \ddots & \ddots & & \\ \frac{1}{4} & \cdots & \frac{1}{4} & \frac{1}{4} & -\frac{3}{4} \end{pmatrix} = -E_8 + \frac{2}{8} \cdot \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & \dots & 1 \\ 1 & 1 & \dots & \dots & 1 \\ \vdots & & & & \vdots \\ 1 & \dots & \dots & \dots & 1 \end{pmatrix}$$

Analyse von Grover's Algorithmus für n=3:

Satz: (Beweis Übungsaufgabe):

i.) D_8 ist unitär.

ii.) Wirkung von D_8 als lineare Abbildung ist Spiegelung am Mittelwert:

Sei $(\alpha_0, \dots, \alpha_7) \in \mathbb{R}^8$ und $m = \sum \alpha_i / 8$.

Dann ist

$$D_8 \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_7 \end{pmatrix} = \begin{pmatrix} -\alpha_0 + 2m \\ -\alpha_1 + 2m \\ \vdots \\ -\alpha_7 + 2m \end{pmatrix}.$$

Satz: Grover's Algorithmus für $n = 3$ liefert mit Wkeit $\frac{121}{128}$ einen Wert $|\hat{x}_1\hat{x}_2\hat{x}_3\rangle|0\rangle$ oder $|\hat{x}_1\hat{x}_2\hat{x}_3\rangle|1\rangle$ mit $f(\hat{x}_1, \hat{x}_2, \hat{x}_3) = 1$.
(Der Algorithmus liefert also nicht ganz sicher das gewünschte Ergebnis, sondern nur mit hoher Wahrscheinlichkeit.)

Beweis: Den Beweis dieses Sätzes bitte selbst durchführen.

Hier sind die Zwischenresultate des Beweises, die Zustände im Zustandsraum:

- Nach Anwendung Hadamard-Transformationen

$$\frac{1}{\sqrt{8}} \cdot (\sum_x |x\rangle) \cdot \frac{1}{\sqrt{2}} \cdot (|0\rangle - |1\rangle)$$

- Nach Anwendung des ersten Quantenorakels:

$$\frac{1}{\sqrt{8}} \cdot (-|\hat{x}\rangle + \sum_{x \neq \hat{x}} |x\rangle) \cdot \frac{1}{\sqrt{2}} \cdot (|0\rangle - |1\rangle)$$

- Nach darauffolgender Anwendung von D_8: (mit $m = \frac{6}{8} \cdot \frac{1}{\sqrt{8}}$)

$$\frac{1}{\sqrt{8}} \cdot (\frac{5}{2}|\hat{x}\rangle + \sum_{x \neq \hat{x}} \frac{1}{2}|x\rangle) \cdot \frac{1}{\sqrt{2}} \cdot (|0\rangle - |1\rangle))$$

Bemerkung: Messen würde jetzt $\hat{x}$ mit Wkeit $\frac{25}{32}$ liefern.

- Nach Anwendung des zweiten Quantenorakels:

$$\frac{1}{\sqrt{8}} \cdot (-\frac{5}{2}|\hat{x}\rangle + \sum_{x \neq \hat{x}} \frac{1}{2}|x\rangle) \cdot \frac{1}{\sqrt{2}} \cdot (|0\rangle - |1\rangle))$$

- Nach darauffolgende Anwendung D_8: ($m = \frac{1}{8\sqrt{8}}$)

$$\frac{1}{\sqrt{8}} \cdot (-\frac{11}{4}|\hat{x}\rangle - \sum_{x \neq \hat{x}} \frac{1}{4}|x\rangle) \cdot \frac{1}{\sqrt{2}} \cdot (|0\rangle - |1\rangle))$$

- Messen liefert:

  $(\hat{x}_1, \hat{x}_2, \hat{x}_3)$ mit Wkeit $(\frac{1}{\sqrt{8}} \cdot \frac{11}{4})^2 = \frac{121}{128}$

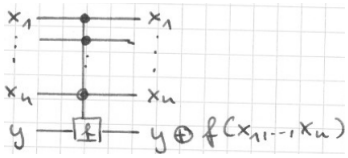
  ($|\hat{x}_1\hat{x}_2\hat{x}_3\rangle|0\rangle$ und $|\hat{x}_1\hat{x}_2\hat{x}_3\rangle|1\rangle$) je mit Wkeit $\frac{1}{2}, \frac{121}{128}$).

Ende Beweis

Bemerkung: Würde man statt zweimal dreimal das Quantenorakel und D_8 anwenden, und dann messen, erhielte man $|\hat{x}\rangle$ nur noch mit Wkeit $\frac{169}{512}$, also weniger beim zweimaligen Anwenden (Beweis $\rightarrow$ Übungsaufgabe).
Dieser Effekt führte dazu, dass Grover's Algorithmus mit einem Soufflée verglichen wurde, das beim Backen immer besser wird, aber wieder zusammenfällt, wenn man es zu lange backt.

4.3 Grover-Algorithmus für beliebiges $n \in \mathbb{N}, N = 2^n$

Aufgabenstellung: $f : \{0,1\}^n \to \{0,1\}$ sei 1 an genau einer Stelle $\hat{x} = (\hat{x}_1, \cdots, \hat{x}_n)$, sonst 0.
Gegeben ist ein Quantenorakel



Finde $\hat{x} = (\hat{x}_1, \cdots, \hat{x}_n) \in \{0,1\}^n$ mit $f(\hat{x}) = 1$ mit möglichst wenig Orakelaufrufen.

Benutzte Transformation neben Quantenorakel

Satz: Für $N \in \mathbb{N}$ sei D_N die $N \times N$-Matrix

$$D_N = -\begin{pmatrix} 1 & & & \\ & 1 & 0 & \\ & 0 & \ddots & \\ & & & 1 \end{pmatrix} + \tfrac{2}{N} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & & & \vdots \\ 1 & 1 & \dots & 1 \end{pmatrix},$$

also

$$(D_N)_{ij} = \begin{cases} -1 + \frac{2}{N} & \text{für } i = j, \quad i,j \in \{0, \cdots, N-1\} \\ \frac{2}{N} & \text{für } i \neq j, \quad i,j \in \{0, \cdots, N-1\} \end{cases}$$

Dann gilt:

i.) D_N ist unitär, und kann in $O(n)$ Quantengattern realisiert werden.

ii.) Für jeden Koeffizientenvektor $(\alpha_0, \cdots, \alpha_{N-1}) \in \mathbb{R}^N$ spiegelt die durch D_N beschriebene lineare Abbildung jeden Koeffizienten am Mittelwert $m = \sum_{i=0}^{N-1} \alpha_i / N$

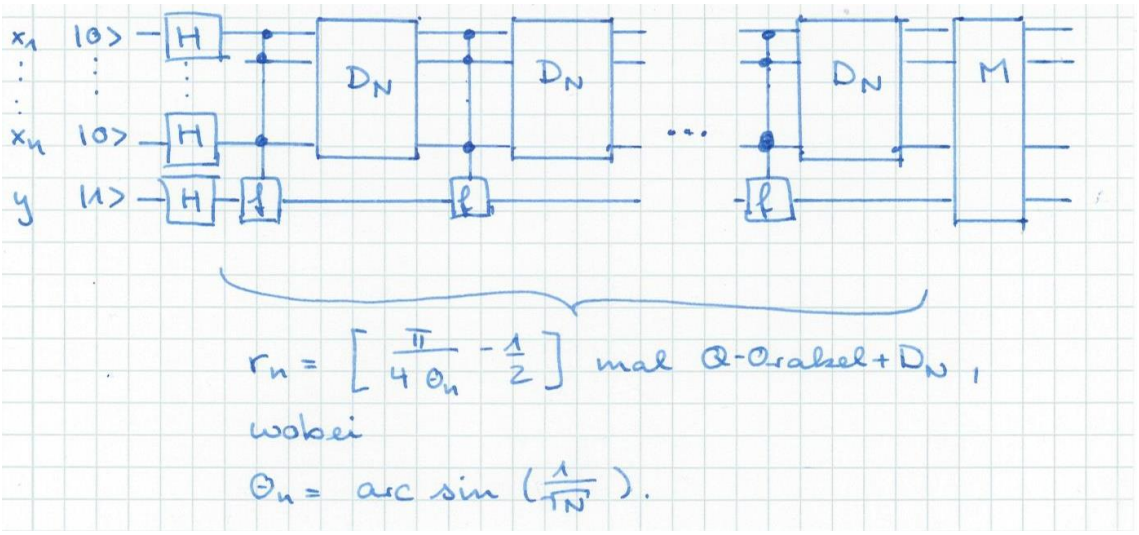
$$D_N \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} -\alpha_0 + 2m \\ -\alpha_1 + 2m \\ \vdots \\ -\alpha_{N-1} + 2m \end{pmatrix}.$$

Beweis: Übungsaufgabe, Realisation mit $O(n)$ Gattern siehe Homeister.

Der Algorithmus

Satz:

a.) Der folgende Quantenschaltkreis findet $\hat{x}$ mit Irrtumswkeit höchstens $\frac{1}{N}$, dabei bedeutet [.] kaufmänisches Runden:



b.) Der Schaltkreis beinhaltet $O(\sqrt{N})$ Orakelaufrufe.

Bemerkung: Idee hinter dem Algorithmus: Das „Katapult“ , siehe im ersten Abschnitt des Kapitel bei der „Grundidee“.

Beweis des Satzes - Analyse des Grover's Algorithmus

a.) Betrachte Zustände $|x_1, \cdots, x_n\rangle$ im 2^n-dimensionalen Zustandsraum, die jeweils nach Ausführung des Orakels und D_N angenommen werden (der Gesamtzustand ist dann jeweils $|x_1 \cdots x_n\rangle \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$).
Ein Zustand $\sum_{i=0}^{2^n-1} \alpha_i \cdot |i\rangle$ wird der Einfachheit halber als Tupel $(\alpha_0, \alpha_1, \cdots, \alpha_{2^n-1})$ geschrieben, wie in der LA-Vorlesung.

Der gesuchte Zustand $|\hat{x}\rangle$ hat das Koeffiziententupel $(0, \cdots, 0, 1, 0, \cdots, 0)$.
O.B.d.A. $(1, 0, \cdots, 0)$.
(Denn es ist für den Algorithmus unwichtig, welcher Basisvektor gesucht wird).

Der Beweis führt über 7 Lemmata, also Vorüberlegungen, die dann in den Beweis münden. Gesprochen wird nur von den Amplituden der ersten n QBits, da das letzte QBit nach der ersten Hadamard-Transformation stets den Zustand $H|1\rangle$ beibehält.

Lemma 1: Nach den Hadamard-Transformationen hat jede erreichte Zustand die Gestalt $(a, b, b, \cdots, b)$ mit $a, b \in \mathbb{R}$.

Beweis:

- Zustandvektor nach Hadamard ist $\frac{1}{\sqrt{N}}(1, \cdots, 1)$, hat die Gestalt.
- Ein Datenbankorakel überführt einen Zustand $(a, b, \cdots, b)$ in $(-a, b, \cdots, b)$, behält also die Gestalt bei.
- Anwendung von D_N liefert für ein geeignetes $c \in \mathbb{R}$:

$$(-E_N + \tfrac{2}{N} \cdot \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}) \cdot \begin{pmatrix} a \\ b \\ \vdots \\ b \end{pmatrix} = \begin{pmatrix} c \\ \frac{2}{N} \cdot (a + (N-1)b) - b \\ \vdots \\ \frac{2}{N} \cdot (a + (N-1)b) - b \end{pmatrix},$$

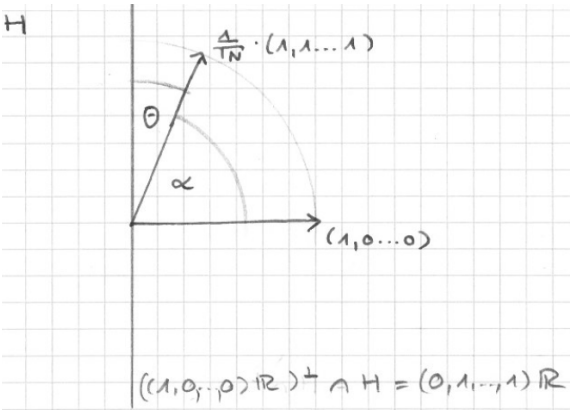
  behält also ebenfalls die geforderte Gestalt bei.

- So bleibt die Gestalt Schritt für Schritt erhalten.

Lemma 2: Jeder nach Hadamard erreichte Zustand liegt in
$H = span(\underbrace{(1, \cdots, 1)}_{\sqrt{N} \cdot Anfangszustand}, \underbrace{(1, 0, \cdots, 0)}_{ZielZustand})$

Beweis: Folgt aus Lemma 1, denn
$span((1, \cdots, 1), (1, 0, \cdots, 0)) = \left\{(a, b, \cdots, b) \in \mathbb{R}^N : a, b \in \mathbb{R}\right\}$.

Zwischenstand: Alle Zustände liegen also in eine Ebene (im $\mathbb{R}^N$). Somit sind alle Hilfsmittel der ebenen Geometrie nutzbar.

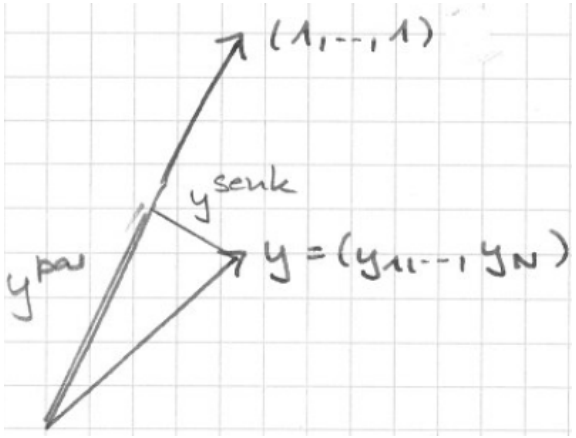


Lemma 3: Anwendung eines DB-Orakels auf einen Zustand in H entspricht einer Spiegelung an $(0, 1, \cdots, 1)\mathbb{R}$.

Beweis: $(0, 1, \cdots, 1)\mathbb{R} = ((1, 0, \cdots, 0)\mathbb{R})^{\perp} \cap H$,
und DB-Orakel dreht Vorzeichen der ersten Komponente um.

Lemma 4: Anwendung von D_N auf einen Zustand $y = (y_1, \cdots, y_N) \in H$ entspricht geometrisch einer Spiegelung an $(1, 1, \cdots, 1)\mathbb{R}$.

Beweis: Erinnerung an orthogonale Zerlegung:



Spiegelung an $(1, \cdots, 1)\mathbb{R}$ bedeutet:
$y \mapsto y - 2y^{senk}$.

z.z: D_N bewirkt $y \mapsto y - 2y^{senk}$.

Gilt, weil:

$$y^{par} = \frac{(1, \cdots, 1) \cdot y}{\|(1, \cdots, 1)\|^2} \cdot (1, \cdots, 1) = \frac{\sum y_i}{N} \cdot (1, \cdots, 1).$$
$$y^{senk} = y - y^{par}.$$

Somit ist $y \mapsto y - 2y^{senk} = y - 2(y - y^{par}) = -y + 2y^{par}$ die lineare Abbildung mit

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \mapsto - \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} + \frac{2}{N} \cdot \begin{pmatrix} \sum y_i \\ \vdots \\ \sum y_n \end{pmatrix}$$

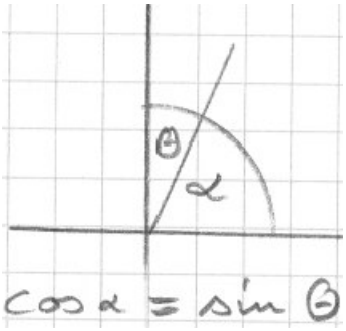
Die Behauptung folgt, weil

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = (-E_N + \frac{2}{N} \cdot \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}) \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} + \frac{2}{N} \begin{pmatrix} \sum y_i \\ \vdots \\ \sum y_n \end{pmatrix}$$

Lemma 5: Der Winkel α zwischen $(1, 0, \cdots, 0)$ und $(1, \cdots, 1)$ beträgt $\alpha = \arccos(\frac{1}{\sqrt{N}})$.

Beweis: Erinnerung lineare Algebra:
Der Winkel zwischen zwei Vektoren x und y ist $\arccos(\frac{x \cdot y}{\|x\| \cdot \|y\|})$.
Hier: $\arccos(\frac{1}{\sqrt{N}})$.

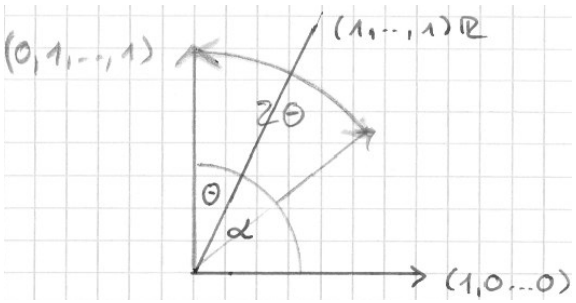
Lemma 6: Sei $\Theta = \frac{\pi}{2} - \alpha$ (bzw. $90° - \alpha$),
Also $\Theta = \arcsin(\frac{1}{\sqrt{N}})$.



Dann entspricht die Anwendung eines DB-Orakel, gefolgt von D_N, einer Drehung um 2Θ im Uhrzeigersinn.

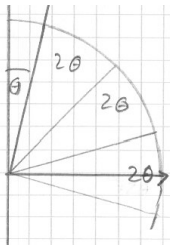
Beweis: Die Hintereinanderausführung von zwei Speigelungen in der Ebene ergibt stets eine Drehung.
Der Drehwinkel ist für alle Punkte gleich. Es genügt also, ihm für einen Punkt zu bestimmen.

Man sieht leicht: Der Drehwinkel für $(0, 1, \cdots, 1)$ ist 2Θ im Uhrzeigersinn (Spiegelung an $(0, 1, \cdots, 1)\mathbb{R}$ bewirkt nichts, Spiegelung an $(1, \cdots, 1)\mathbb{R}$ bewirkt Drehung um 2Θ im Uhrzeigersinn



Lemma 7: Nach $\tau = \left[\frac{\pi}{4} \cdot \frac{1}{\Theta} - \frac{1}{2}\right]$ Orakeln(gefolgt jeweils von D_N) ist der Winkel zwischen dem Zielvektor $(1, 0, \cdots, 0)$ und dem aktuellen Zustandsvektor kleiner oder gleich Θ.

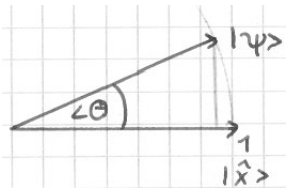
Beweis:



Könnte man Anteile von Schritten gehen, wäre nach $\tilde{\tau} = \frac{\alpha}{2\Theta}$ Schritten der Zielvektor erreicht.
$\tilde{\tau} \in \mathbb{R}$ erfüllt $\frac{\pi}{2} - \Theta = 2\tilde{\tau}\Theta$, also $\tilde{\tau} = \frac{\pi}{4\Theta} - \frac{1}{2}$.
Wählt man $\tau = [\tilde{\tau}]$, so ist der Winkel zwischen dem Zielvektor und dem Zustandsvektor nach τ Schritten kleiner als Θ.

Beweis des Satzes:

a.) Messen in Zustand $|\psi\rangle$ nach dem letzten D_N im Winkel kleiner Θ zum Zielzustand $|\hat{x}\rangle$, liefert einen anderen Basisvektor als $|\hat{x}\rangle$ nur mit Wkeit kleiner $(\sin(\Theta))^2$



Dabei ist die blaue senkrechte Linie kürzer als $\sin(\Theta)$.
Die Irrtumswkeit ist also kleiner als $(\sin(\Theta))^2 = (\sin(\arcsin(\frac{1}{\sqrt{N}})))^2 = \frac{1}{N}$.

b.) Für kleine Winkel Θ ist $\sin(\Theta) \approx \Theta$, also (wegen $(\sin(\Theta)) = \frac{1}{\sqrt{N}}$ im Algorithmus)

$$r_n \approx \left[\frac{\pi}{4 \cdot \frac{1}{\sqrt{N}}} - \frac{1}{2}\right] \approx \sqrt{N} \cdot \frac{\pi}{4} = O(\sqrt{N}). \qquad \text{Q.e.d.}$$

Bemerkung:

i.) Grover's Algorithmus ist optimal in dem Sinne, dass die Aufgabenstellung nicht mit weniger als $O(\sqrt{N})$ Orakelaufrufen gelöst werden kann.

ii.) $O(\sqrt{N})$ ist (wegen $N = 2^n$) immer noch exponentiell in n.

iii.) Daher glaubt man nicht, dass Polynomialzeit-Quantenalgorithmen für NP-vollständige Probleme existieren (jedes NP-vollständige Problem kann als DB-Suche modelliert werden).

5 Quanten-Fehlerkorrektur

Lernziele: Gegeben Quantenschaltkreis, der gelegentlich QBits verfälscht.
Verstanden haben, wie eine Fehlerkorrektur möglich ist
(QBits können ja nicht gelesen werden, ohne sie zu verändern, und können auch nicht geklont werden).

5.1 Basisidee Quantenfehlerkorrektur

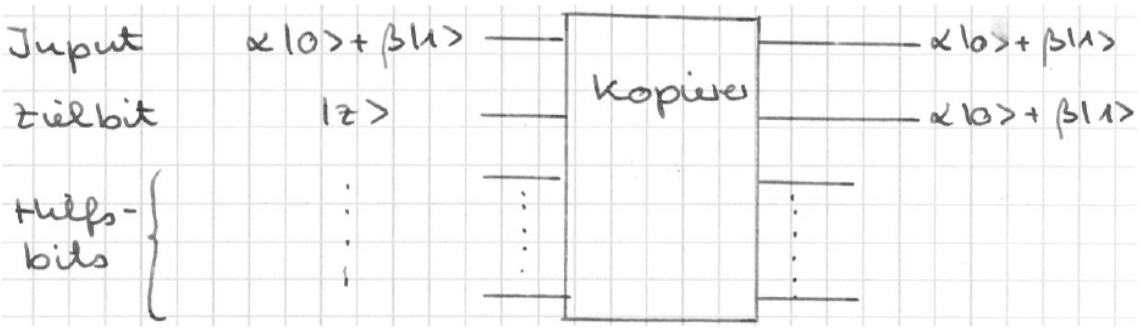
Erinnerung Fehlerkorrektur klassisch:

- zu sendedes Bit wird dreimal gesendet.
- Empfängt Empfänger ungleiche Bits, so ist ein Fehler aufgetreten.
- Er korrigiert gemäß „Mehrheitsentscheid “.
- funktionniert „gut “, wobei „gut “Analysegegenstand ist.

Geht für Quantenkanäle nicht, wegen des No-Cloning-Theorems (siehe BB84-Protokoll, Abschnitt III.4):

Satz: (No Cloning-Theorem)
Es gibt keinen Quantenschaltkreis, der ein beliebiges QBit auf ein Zielbit kopiert.

Veranschaulichung: Sowas gibt es nicht:



Somit funktioniert die klassische Art, Fehler zu erkennen und zu beheben, bei QBits nicht.

Basis Idee Quantenfehlerkorrektur:

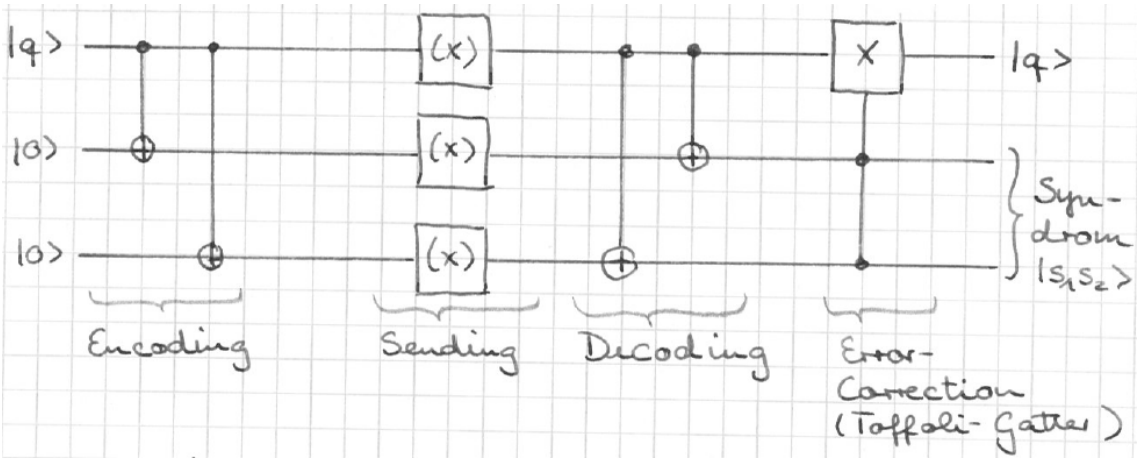
- $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ soll gesendet werden.
- Erzeuge Zustand $\alpha \cdot |0 \cdots 0\rangle + \beta|1 \cdots 1\rangle$
  (beachte: $\alpha \cdot |0 \cdots 0\rangle + \beta|1 \cdots 1\rangle \neq (\alpha \cdot |0\rangle + \beta|1\rangle)^n$
- Sende alle QBits
- Miß die hinteren QBits.
- korrigiere das erste QBit entsprechend.

Fehlerarten , die ein QBit $|q\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ im Kanal verändern können:

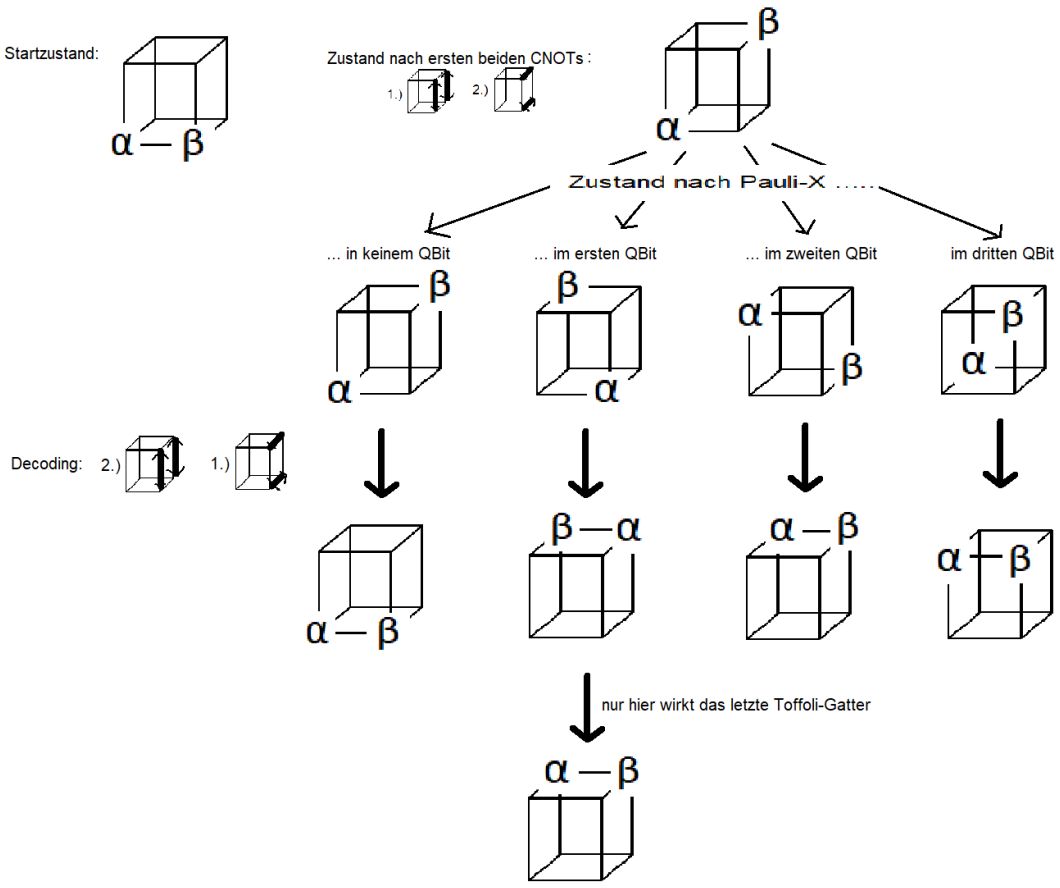
- Bit-Flip: $\alpha \cdot |0\rangle + \beta \cdot |1\rangle \mapsto \beta \cdot |0\rangle + \alpha \cdot |1\rangle$, also $|q\rangle \mapsto X|q\rangle$
- Phase-Flip: $\alpha \cdot |0\rangle + \beta \cdot |1\rangle \mapsto \alpha \cdot |0\rangle - \beta \cdot |1\rangle$, also $|q\rangle \mapsto Z|q\rangle$
- Kombinationen:
  $\alpha \cdot |0\rangle + \beta \cdot |1\rangle \mapsto \beta \cdot |0\rangle - \alpha \cdot |1\rangle$, also $|q\rangle \mapsto ZX|q\rangle$, und
  $\alpha \cdot |0\rangle + \beta \cdot |1\rangle \mapsto -\beta \cdot |0\rangle + \alpha \cdot |1\rangle$, also $|q\rangle \mapsto XZ|q\rangle$
- Beliebiger Fehler: $U = \begin{pmatrix} u & v \\ -v & u \end{pmatrix}$ bzw. $U = \begin{pmatrix} u & v \\ v & -u \end{pmatrix}$,
  $\alpha \cdot |0\rangle + \beta \cdot |1\rangle \mapsto (\alpha u + \beta v) \cdot |0\rangle \pm (\alpha u - \beta v) \cdot |1\rangle$, also $|q\rangle \mapsto U|q\rangle$

5.2 Korrektur Bit-Flip: (3-QBit)Bit Flip Code

Satz: Der folgende Schaltkreis liefert das Input-Bit $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ wenn im möglicherweise fehlerhaften Kanal kein QBit oder genau ein QBit geflippt wird.



Beweis: Übungsaufgabe. Graphpische Veranschaulichung:



Bemerkung:

i.) Eine Messung des Syndroms muß nicht unbedingt durchgeführt werden. Sie würde liefern:
$|s_1 s_2\rangle = |00\rangle \Leftrightarrow$ kein Übertragungsfehler
$|s_1 s_2\rangle = |01\rangle \Leftrightarrow$ Bit-Flip im 3. QBit
$|s_1 s_2\rangle = |10\rangle \Leftrightarrow$ Bit-Flip im 2. QBit
$|s_1 s_2\rangle = |11\rangle \Leftrightarrow$ Bit-Flip im 1. QBit.

ii.) Nur im Falle des Bit-Flip im 1. QBit muß eine Fehlerkorrektur erfolgen (genau dann handelt das Toffoli-Gatter).

iii.) Werden zwei oder alle drei QBits beim Senden geflippt, funktioniert die Fehlerbehebung nicht mehr (wie im klassischen Fall).

5.3 Korrektur Phase-Flip

Phase Flip auf QBit: Anwendung Pauli-Z-Transformation $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Wirkung auf QBit: $\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0|0\rangle - \alpha_1|1\rangle$.

Idee zur Fehlerkorrektur: Zurückführen auf Bit-Flip.
Denn:

Satz: Sei(wie üblich) $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
Dann ist
i.) $H \cdot X \cdot H = Z$ und
ii.) $H \cdot Z \cdot H = X$.

Beweis:

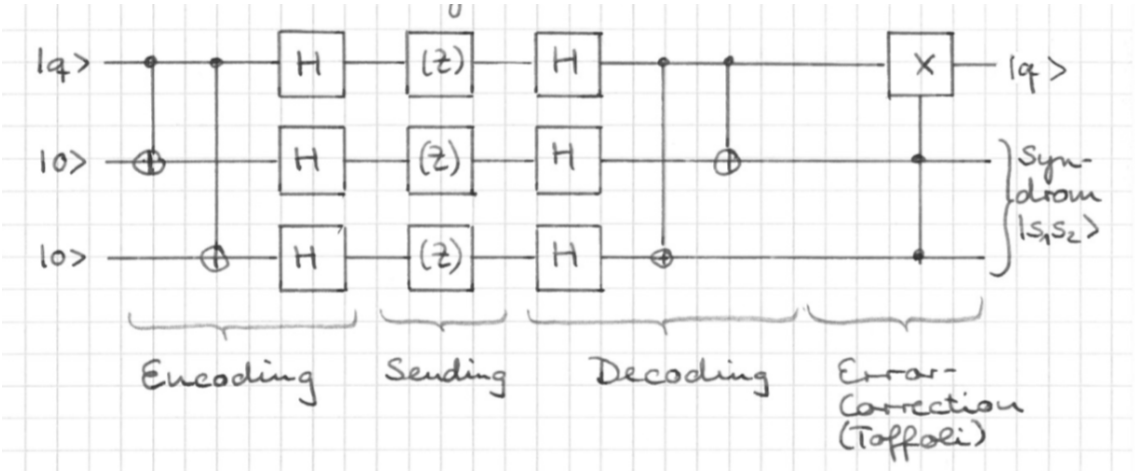
i.) Nachrechnen:

$$\begin{aligned} H \cdot X \cdot H &= \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \\ &= \frac{1}{2} \cdot \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} \\ &= Z \end{aligned}$$

ii.) Folgt aus i.) :

$$
\begin{aligned}
& H \cdot X \cdot H = Z && | \cdot \text{H von links} \\
\Longrightarrow \quad & H^2 \cdot X \cdot H = H \cdot Z && | \text{ nutze } H^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
\Longrightarrow \quad & X \cdot H = H \cdot Z && | \cdot \text{ H von rechts, und } H^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
\Longrightarrow \quad & X = H \cdot Z \cdot H
\end{aligned}
$$

Satz: Der folgende Schaltkreis liefert das Input-Bit $|q\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$, wenn im möglicherweise fehlerhaften Kanal ein Phase-Flip auf kein oder genau eines der drei QBits angewendet wird:



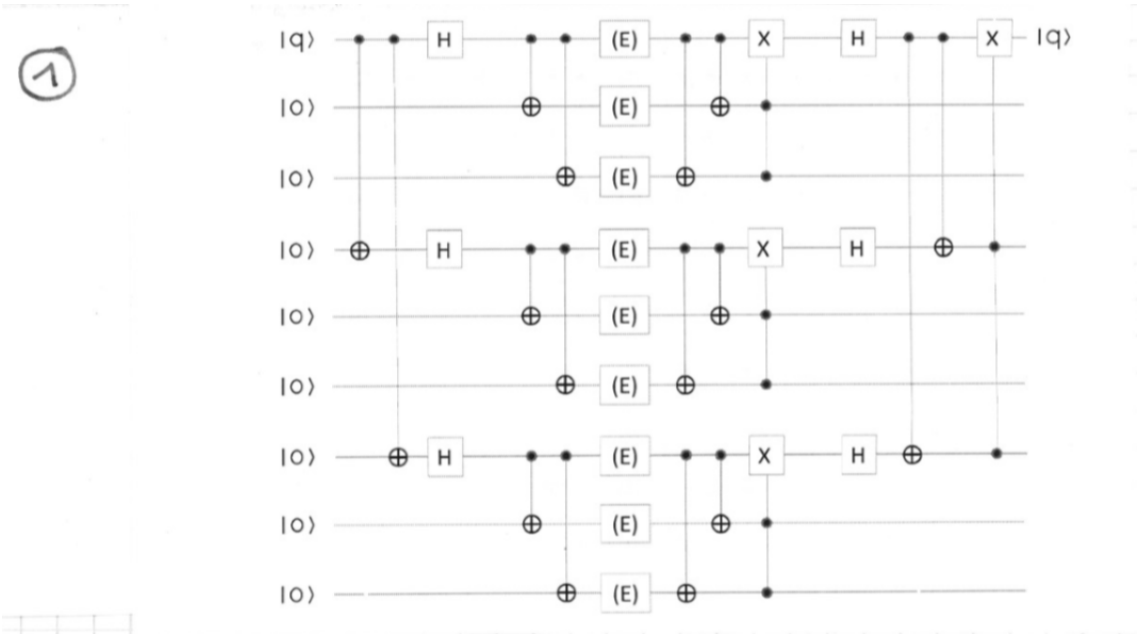
Beweis: Satz gilt wegen der Korrektheit des Bit-Flip-Codes. Denn $H \cdot (Z) \cdot H = (X)$, mit anderen Worten: Falls im i-ten Bit ($i \in \{1, 2, 3\}$) ein Phase-Flip durchgeführt wird, arbeitet der Schaltkreis genau wie der des Bit-Flip-Codes, wenn im i-ten Bit ein Bit-Flip durchgeführt wird. Im Fall einer korrekten Übertragung arbeitet der Schaltkreis ebenfalls genau wie der Bit-Flip-Code im Fall korrekter Übertragung.

5.4 Korrektur Kombination Bit-Flip und Phase-Flip: Der Shor Code(1995)

Satz: Der folgende Schaltkreis (1) liefert das Input-QBit $|q\rangle = \alpha|0\rangle + \beta|1\rangle$, wenn im möglicherweise fehlerhaften Kanal auf höchstens ein QBit eine der folgenden Transformationen (E) angewandt wird:

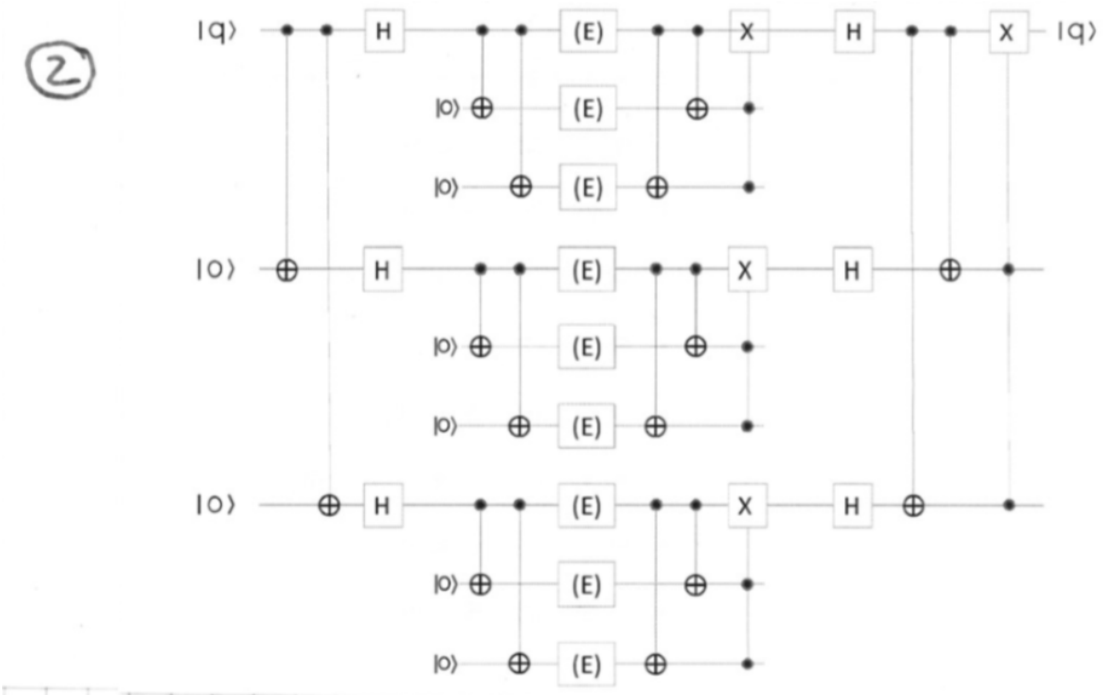
$$\begin{aligned} \text{Pauli X}: &\quad \alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0|1\rangle + \alpha_1|0\rangle \\ \text{Pauli Z}: &\quad \alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0|0\rangle - \alpha_1|1\rangle \\ \text{ZX}: &\quad \alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle - \alpha_0|1\rangle \end{aligned}$$

Wird XZ angewandt, also $\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto -\alpha_1|0\rangle + \alpha_0|1\rangle$, liefert er $-|q\rangle = -\alpha|0\rangle - \beta|1\rangle$.

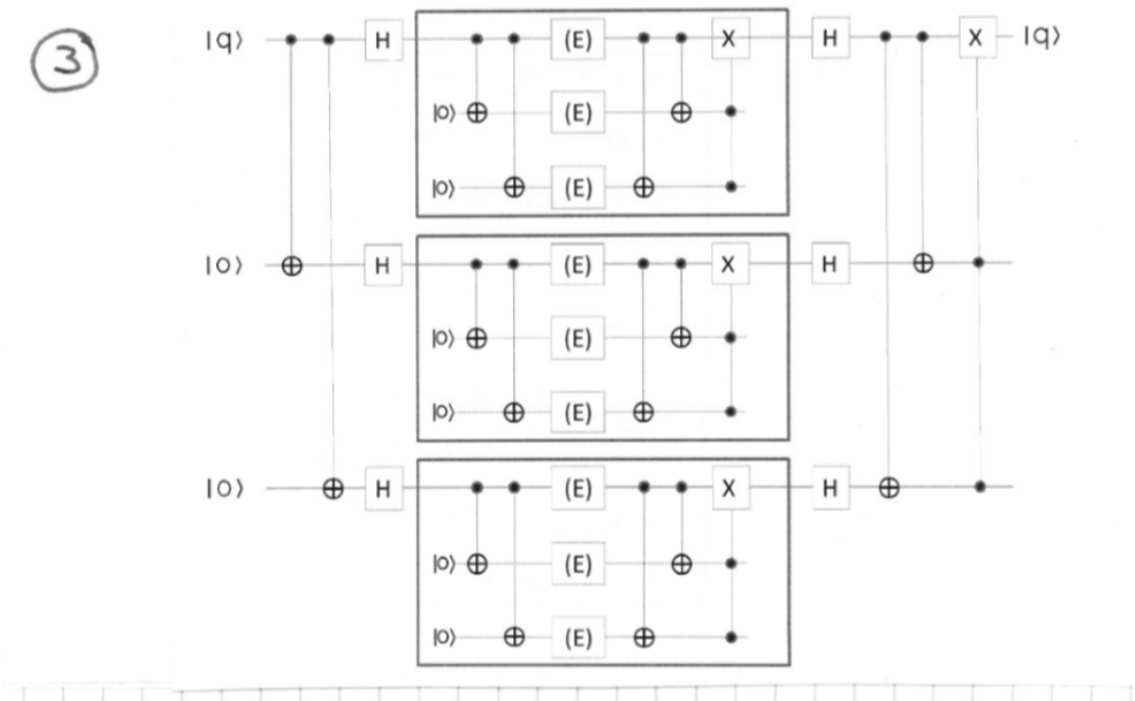


Bemerkung: Schaltkreis von Shor(1995), hat ein Forschungsfeld sogenannter „stabilisierender Quantum-Codes“ eröffnet.

Beweis: (Nein, wir gehen nicht in den Zustandsraum von 9 QBits!) Eine andere Darstellung des Schaltkreises ist (2):



Dies ist ein äußerer Schaltkreis, der dreimal den gleichen inneren Schaltkreis aufruft:



Der innere Schaltkreis ist der Schaltkreis des 3 QBits-Flip-Code. Rest $\mapsto$ Übungsaufgabe.

6 Adiabatisches Quantencomputing

Hintergrund: Die Firma D-Wave in Kanada propagiert seit einigen Jahren, sie könne Quantencomputer mit Hunderten (Stand März 2019: über 5.000) QBits bauen.
Beim D-Wave-Computer handelt es sich jedoch nicht um einen Quantencomputer im Sinne des bisher betrachteten Berechnungsmodells.

Ganz grob gesprochen funktioniert der D-Wave-Computer wie folgt: (Zitiert aus Wikipedia, „Quantencomputer“, Stand 03.07.2020)

„Die Idee des adiabatischen Quantencomputers ist es, ein System zu konstruieren, das einen zu dieser Zeit noch unbekannten Grundzustand hat, der der Lösung eines bestimmten Problems entspricht, und ein anderes, dessen Grundzustand leicht experimentell zu präparieren ist. Anschließend wird das leicht zu präparierende System in das System überführt, an dessen Grundzustand man interessiert ist, und dessen Zustand dann gemessen. Wenn der Übergang langsam genug erfolgt ist, hat man so die Lösung des Problems .“

Will man also z.B. das Minimum einer Funktion f bestimmen, so könnte man ein System präparieren, dass der Funktion $g(x) = x^2$ entspricht. Hier kennt man das Minimum $x = 0$. Führt man nun langsam (adiabatisch) die Funktion $g(x)$ in f über, so wird das Minimum $x = 0$ in das Minimum der Funktion f überführt.
Die Probleme, die der D-Wave-Computer lösen kann, sind Approximierungsprobleme. Er findet normalerweise nicht die optimale Lösung, sondern eine Lösung, die bis auf ca 5 Prozent am Optimum liegt. Das reicht für alle praktischen Anwendungen.
Wirklich schwierige Probleme der Zukunft sind also möglicherweise nicht mehr die NP-vollständigen Probleme, sondern diejenigen, die keine approximativen Lösungen besitzen. Z.B. Faktorisierung ;).
Die Physik des D-Wave-Computers kann nicht mehr mit dem einfachen Modell eines polarisierten Lichtteilchens erklärt werden. Es muss nun auch die Energie des Teilchens, also seine Frequenz (innerhalb der Ebene, in der es schwingt) betrachtet werden.
In dieser Veranstaltung wird das Modell nur kurz angesprochen. D-Wave veröffentlicht fast nicht, es ist sehr schwer, Informationen zum adiabatischen Quantencomputing zu finden. Empfohlen wird der Vortrag von Elisabeth Lobe und Tobias Stollenwerk von DLR Simualtionssoftware in Braunschweig, „Adiabatisches Quantencomputing“ aus dem Jahr 2015, den man über eine einfache google-Abfrage findet.

Ein Artikel über adiabatisches Quantencomputing findet sich in c't Heft 12 aus 2020. Der Artikel ist in Moodle hochgeladen. Er schildert auch das Problem, WIE man überhaupt ein gegebenes Optimierungsproblem in einen Input für einen D-Wave-Computer umformuliert.

Mit dem Konjunkturpaket vom Juni 2020 hat die Bundesregierung Eur 2 Mrd für die Forschung an Quantentechnologien bereitgestellt. Deutschland soll - auch gemeinsam im europäischen Verbund - weltweit konkurrenzfähig werden. Es bleibt spannend :).