

Quantenrechnen

Quantum Computation

Vorlesung im Sommersemester 2003

Prof. Dr. Folkmar Bornemann

Fakultät für Mathematik

Technische Universität München

Quantenrechnen (Quantum Computation)

Vorlesung im Sommersemester 2003

Prof. Dr. Folkmar Bornemann

<http://www.ma.tum.de/m3/teaching/QCOMP03/>

0.	Einleitung	1
1.	Einführung in die Quantentheorie	11
2.	Schaltkreismodelle	81
3.	Einfache Quantenalgorithmen	147
4.	Das Problem der verborgenen Untergruppe	170
5.	Warum Primfaktorisation spannend ist	194
6.	Die Algorithmen von Shor	212
7.	Quanten-Fouriertransformation	238
8.	Der Quanten-Suchalgorithmus von Grover	260

Grenzen klassischer Computer

- Technologie: Steigerung der Leistungsfähigkeit (Moore'sche Gesetz) durch Miniaturisierung stößt in den nächsten 100 Jahren an ihre Grenzen
- Algorithmen: Simulation großer Quantensysteme unmöglich („curse of dimension“)?

„Physics meets Computer Science“

- Information ist physikalische Größe (Landauer Prinzip 1970)
- Reversible Computer sind möglich (Bennett 1973, Fredkin/Toffoli 1981)
- Quantensysteme „berechnen“ sich selbst (Feynman 1983)
- Computer sind Objekte der Realität: Berechenbarkeit keine Frage der Mathematik sondern der Physik (Deutsch 1985)

Quantencomputer können **fantastisch** viel mehr

- beweisbar exponentieller Speed-Up in akademischen Algorithmen modulo eines Orakels (Simon 1994)
- praktisch exponentieller Speed-Up bei der Primfaktorzerlegung einer Zahl n :
 - klassisch: „number sieve field“

$$\text{zeit} \simeq \exp(1.9(\ln n)^{1/3} (\ln \ln n)^{2/3})$$

- Quantenalgorithmus von Shor (1994):

$$\text{zeit} \simeq O((\ln n)^2 \ln \ln n \ln \ln \ln n)$$

Quantencomputer können **deutlich** mehr

- beweisbarer Speed-Up bei der Suche in unstrukturierten Mengen mit N Objekten
 - klassisch: zeit = $\Theta(N)$
 - Quantenalgorithmus von Grover (1996): zeit = $\Theta(\sqrt{N})$
 - entsprechende Algorithmen für Zählen und deskriptive Statistik
 - entsprechende Algorithmen für Summation und Quadratur

„Trade-Off“

- Realisierung erfordert wesentliche Fortschritte in Physik, Chemie und Ingenieurwissenschaften
- Blickpunkt der Informationsverarbeitung hat das Verständnis der Quantenmechanik verändert (insbesondere in Bezug auf die sog. Paradoxa)
- neues Paradigma in der theoretischen Informatik
- weitere interessante Algorithmen erfordern neue Ideen in Mathematik und Informatik
- $BPP \subset BQP \subset PSPACE$: der Nachweis, daß Quantencomputer wirklich superpolynomial besser sind, wird schwer...

Caveats

- der Rekord liegt derzeit bei „Maschinen“ mit 7 Qubits
- Quantencomputer hinreichender Größe werden vielleicht *nie* realisiert:
 - Fragilität der benötigten Quantenzustände („Dekohärenz“) technologisch beherrschbar?
 - Kosten?
- der aufsehenerregende Algorithmus von Shor hat vor allem *negative* praktische Bedeutung: seine Realisierung würde die Public-Key-Kryptographie heutiger Bauart obsolet machen

Klassische Computer

Bit = entweder 0 oder 1

Quantencomputer

$$\text{Qubit} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha e_0 + \beta e_1 = \alpha |0\rangle + \beta |1\rangle \in \mathbb{C}^2, \quad |\alpha|^2 + |\beta|^2 = 1$$

„Superposition“ aus zwei Zuständen 0 und 1

- $|\alpha|^2$ Wahrscheinlichkeit für Ergebnis 0
- $|\beta|^2$ Wahrscheinlichkeit für Ergebnis 1

Bemerkung: Begriff „Qubit“ wurde 1994 von Ben Schumacher geprägt

Erste Impressionen

- Quantenalgorithmen sind probabilistischer Natur
- Superposition von 0 und 1 im Qubit führt zur *Quantenparallelität*, d.h. alle möglichen Ergebnisse werden „gleichzeitig“ berechnet
- Design eines guten Quantenalgorithmus besteht darin, nur die interessanten Ergebnisse wahrscheinlich zu machen
- exponentieller Speed-Up ist denkbar, da n Qubits alle 2^n Binärzahlen mit n Stellen gleichzeitig behandeln

Grundlagen

- Basisverständnis von Quantentheorie, maßgeschneidert auf Informationsverarbeitung und Algorithmen
- multilineare Algebra (Tensorprodukte etc.)
- reversible Computer
- Schaltkreismodelle von Quantencomputern und Universalität

Algorithmen

- akademische Algorithmen von Deutsch/Josza, Bernstein/Vazirani und Simon
- Algorithmus von Shor
- Problem der verborgene Untergruppe (Shor, Kitaev)
- Algorithmus von Grover und seine Derivate

Quantenkommunikation

Mit einem Qubit lässt sich eigentlich nicht mehr Information übertragen als mit einem klassischen Bit, aber...

...wenn Alice und Bob vorher ein *EPR-Paar* teilen, so können sie

- „*super dense coding*“: mit einem einzigen Qubit über einen Quantenkommunikationskanal **zwei** klassische Bits übertragen
- bzw. dual dazu, und noch aufregender, „*quantum teleportation*“: mit zwei klassischen Bits über einen **klassischen** Kommunikationskanal ein Qubit übertragen:

„Beam me up, Scotty..“

Quantenfehlerkorrektur

Zwei prinzipielle Probleme...

- „Dekohärenz“: extreme Fragilität verschränkter Quantenzustände
- „no cloning theorem“: Quantenzustände sind prinzipiell **nicht** duplizierbar

..aber große Fortschritte

- Kommunikation: fehlerkorrigierende Codes (Shor 1995, Steane 1996)
- Rechner: fehlertolerante Schaltkreise (Shor 1995, Gottesman 1998)

Quantenkryptografie

Realisierung des Algorithmus von Shor kompromittiert klassische Public-Key-Kryptographie...

...aber Quantenkommunikation macht beweisbar abhörsichere kryptographische Protokolle möglich (Wiesner 1969, Bennett et al. 1984)

Quantentheorie = Theorie zur Vorhersage von Wahrscheinlichkeiten...

- elegant und konzeptionell einfach
- erstaunliche Genauigkeit
- kein bekannter Konflikt zwischen Theorie und Experiment
- beschreibt weites Spektrum naturwissenschaftlicher Phänomene: Superfluide, Supraleiter, Laser, chemische Reaktionen, Struktur der DNA, Existenz und Verhalten von Festkörpern, Farbe der Sterne etc.

...aber oft quer zu unserer Sprache und Intuition

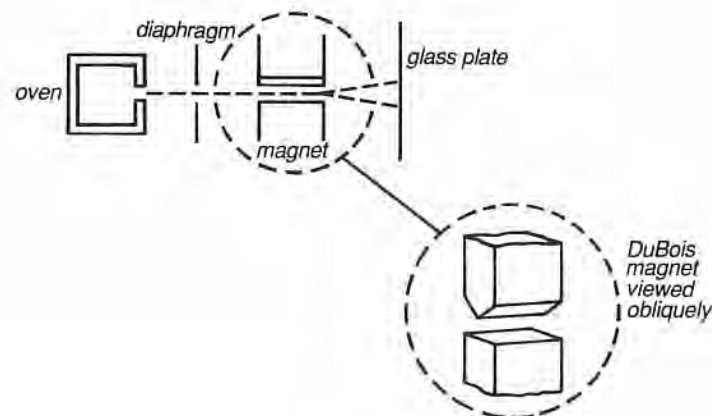
(1.1-1) DAS STERN-GERLACH EXPERIMENT (1922)

Auch in der Quantentheorie spricht man von und über *Teilchen*...

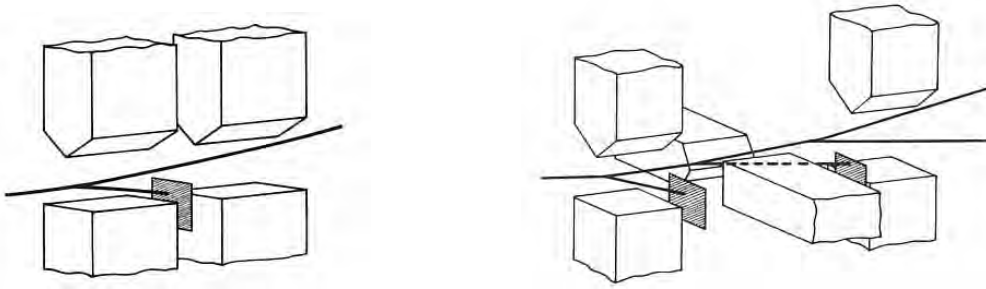
...auch wenn einige ihrer Eigenschaften den Teilchen unserer gewöhnlichen Vorstellungswelt völlig fremd sind.

Irgendwie ist noch nicht einmal klar, in welchem Sinne man überhaupt von "Eigenschaften" sprechen kann.

Beispiel: Stern-Gerlach Experiment (1922) für Spin-1/2-Teilchen



Auswahl eines Teilchenstrahls = Präparation einer „Eigenschaft“



- Test 1: Spin-up $|\uparrow\rangle$ oder Spin-down $|\downarrow\rangle$
- Test 2: Spin-rechts $|\rightarrow\rangle$ oder Spin-links $|\leftarrow\rangle$

Testergebnisse (Messung)

- $|\uparrow\rangle$ -Teilchen: $|\rightarrow\rangle$ bzw. $|\leftarrow\rangle$ gleich wahrscheinlich
- $|\rightarrow\rangle$ -Teilchen: $|\uparrow\rangle$ bzw. $|\downarrow\rangle$ gleich wahrscheinlich

Fazit: Teilchen mit „Eigenschaft“ $|\uparrow\rangle$ und $|\rightarrow\rangle$ **nicht** präparierbar.

Grundelemente einer Theorie

- Präparation: bringt physikalisches System in reproduzierbaren „Zustand“ ρ .
- Test (Messung): ordnet einem physikalischen System ein Ergebnis μ zu. In dieser Vorlesung: n-Level (diskrete) Quantensysteme

$$\mu \in \{\mu_1, \dots, \mu_n\}$$

Minimalforderung an eine Theorie

Korrelation von Präparation und Test

Zu jedem Test gehört also eine Abbildung

$$\rho \mapsto \{p_1, \dots, p_n\},$$

welche Ergebnis μ_k Wahrscheinlichkeit $0 \leq p_k \leq 1$ zuordnet; $\sum_{k=1}^n p_k = 1$.

- *wiederholbare Tests*: Erneute Ausführung des Tests ändert das Ergebnis nicht
- *vollständige Tests*: die Mächtigkeit n der Ergebnismenge ist maximal

Wir verstehen unter *Tests* bis auf Widerruf *wiederholbare Tests*.

Quantentheorie liefert Antwort auf

- Was geschieht (mit welcher Wahrscheinlichkeit)?

*Sie liefert **keine** Antwort auf*

- Warum geschieht es?
- Wie geschieht es?

Antworten auf die letzten beiden Fragen heißen *Interpretationen der Quantentheorie*.

Interpretationen der Quantentheorie

- prinzipiell nicht überprüfbare Spekulationen
- keine Erhöhung der prediktiven Fähigkeiten
- keine Vereinfachung des mathematischen Formalismus
- zuweilen phantasievoll, oft Science Fiction, und immer Geschmackssache
- lenken den Anfänger unnötig ab

Im Sinne des Occam'schen Messers sind sie höchst überflüssig:
Quantum Theory Needs No 'Interpretation' (Fuchs/Peres 2000)

Aussagen über physikalische Systeme = Aussagen über Tests an präparierten Systemen

Definition. $A \vdash B$, sprich „A impliziert stets B“:

- wenn ein physikalisches System nach einer gewissen Präparation mit Wahrscheinlichkeit 1 die Aussage A erfüllt
- dann erfüllt das System bei gleicher Präparation mit Wahrscheinlichkeit 1 auch die Aussage B

Notation

- 0 nie zutreffende Aussage („falsch“)
- 1 stets zutreffende Aussage („richtig“)

Klassische Logik: „tertium non datur“

$$A \wedge B = 0 \quad \Rightarrow \quad A \vdash \neg B$$

Quantentheorie

Es gibt Aussagen (Ereignisse) A und B, so dass sowohl

$$A \wedge B = 0, \quad A \wedge \neg B = 0.$$

Zwei solche Ereignisse heißen *inkompatibel*.

Beispiel

Stern-Gerlach-Experiment zeigt, daß die Spinzustände $A = |\uparrow\rangle$ und $B = |\rightarrow\rangle$ inkompatibel sind.

Implikation \vdash ist *Halbordnung* auf den Aussagen (Ereignissen)

$A \wedge B$, sprich „A und B“: größtes Element C, so daß $C \vdash A$, $C \vdash B$

$A \vee B$, sprich „A oder B“: kleinstes Element C, so daß $A \vdash C$, $B \vdash C$

Ereignisse bilden *Verband mit Null- und Einselement*

- Kommutativität: $A \circ B = B \circ A$ für $\circ \in \{\wedge, \vee\}$
- Assoziativität: $A \circ (B \circ C) = (A \circ B) \circ C$ für $\circ \in \{\wedge, \vee\}$
- Adjunktivität: $A \wedge (A \vee B) = A$, $A \vee (A \wedge B) = A$
- Nullelement: $A \wedge 0 = 0$, $A \vee 0 = A$
- Einselement: $A \wedge 1 = A$, $A \vee 1 = 1$

Definition.

$\neg A$, sprich „nicht A“ oder „Komplement (Gegenteil) von A“.

Es sind äquivalent

- ein physikalisches System erfüllt nach einer gewissen Präparation mit Wahrscheinlichkeit 1 (0) die Aussage A
- das System erfüllt bei gleicher Präparation mit Wahrscheinlichkeit 0 (1) die Aussage $\neg A$

Ereignisse bilden **komplementären** Verband

- $\neg(\neg A) = A$
- $A \wedge \neg A = 0$, $A \vee \neg A = 1$

Klassische Logik

Ereignisse bilden **distributiven** Verband, also *Boole'sche Algebra*

- $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$
- $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

Diese Distributivität ist in der Quantentheorie schlicht **falsch**.

Beispiel: (Stern-Gerlach-Experiment) $A = |\uparrow\rangle$, $\neg A = |\downarrow\rangle$, $B = |\rightarrow\rangle$

Aus Inkompatibilität von A und B folgt

- $B \wedge (A \vee \neg A) = B \wedge 1 = |\rightarrow\rangle$
- $\underbrace{(B \wedge A)}_{=0} \vee \underbrace{(B \wedge \neg A)}_{=0} = 0$

Modularer Verband

Es gilt in der Quantentheorie das schwächere Modularitätsgesetz

$$A \vdash C \text{ hat zur Folge, daß } A \vee (B \wedge C) = (A \vee B) \wedge C.$$

Motivation

- Aus $A \vdash C$ folgt $A \vdash (A \vee B) \wedge C$. Es gilt stets $B \wedge C \vdash (A \vee B) \wedge C$.
Also ohne jedes weitere Gesetz:

$$A \vdash C \text{ hat zur Folge, daß } A \vee (B \wedge C) \vdash (A \vee B) \wedge C.$$

- Gleichheit folgt aus Wunsch nach „komplett zufälligen Zustand“

Komplett zufälliger Zustand

Wahrscheinlichkeitsverteilung d auf den Ereignissen, so daß alle Ergebnisse gleich wahrscheinlich sind. Ein solches d erfüllt zumindest:

- $A \vdash B, A \neq B \implies d(A) < d(B)$
- $d(A) + d(B) = d(A \wedge B) + d(A \vee B)$

Fortführung der Motivation des Modularitätsgesetzes

Aus den Eigenschaften von d und den Verbandsgesetzen folgt

$$d(A \vee (B \wedge C)) = d((A \vee B) \wedge C).$$

Da wir $A \vee (B \wedge C) \vdash (A \vee B) \wedge C$ bereits gezeigt haben, muß wegen der ersten Eigenschaft von d sogar Gleichheit gelten, also das Modularitätsgesetz.

Quantenereignisse bilden einen irreduziblen Verband

Das bedeutet, es gibt keine *neutralen* Elemente X außer 0 und 1:

$$A = (A \wedge X) \vee (A \wedge \neg X) \quad \forall A$$

Motivation

Zu jedem Ereignis $A \neq 0, 1$ gibt es in der Quantentheorie inkompatible Ereignisse B , d.h. solche für die gilt

$$(A \wedge B) = (A \wedge \neg B) = 0.$$

Theorem. (diskrete Quantensysteme)

- (Birkhoff/von Neumann 1936)

Ein irreduzibler, modularer, komplementärer Verband ist isomorph zu einer endlichdimensionalen projektiven Geometrie über einem Schiefkörper \mathbb{K} mit involutorischem Antiisomorphismus.

- (Kolmogoroff 1932)

Besitzt diese Geometrie eine lokal kompakte Topologie, bezüglich derer die Verbandsoperationen stetig sind, so ist $\mathbb{K} = \mathbb{R}$, $\mathbb{K} = \mathbb{C}$ oder \mathbb{K} ist der Schiefkörper der Quaternionen.

Isomorphie zur projektiven Geometrie

Zustandsraum ist **Hilbertraum** $\mathcal{H} = (\mathbb{K}^n, \langle \cdot, \cdot \rangle)$

Ereignisse A identifiziert mit Unterräumen \mathcal{U}_A von \mathcal{H}

- $A \vdash B \iff \mathcal{U}_A \subset \mathcal{U}_B$
- $A \vdash \neg B \iff \mathcal{U}_A \perp \mathcal{U}_B$
- $\mathcal{U}_{\neg A} = \mathcal{U}'_A$, das orthogonale Komplement von \mathcal{U}_A in \mathcal{H}
- $\mathcal{U}_{A \wedge B} = \mathcal{U}_A \cap \mathcal{U}_B$
- $\mathcal{U}_{A \vee B} = \mathcal{U}_A + \mathcal{U}_B$
- $\mathcal{U}_0 = 0$
- $\mathcal{U}_1 = \mathcal{H}$

Quantenlogik der Projektoren

P_A ON-Projektion auf Unterraum U_A

- $A \vdash B \iff P_B P_A = P_A \iff P_A P_B = P_A$
- $A \vdash \neg B \iff P_B P_A = 0 \iff P_A P_B = 0$
- $P_{\neg A} = I - P_A$
- $P_{A \wedge B} = P_A P_B$ falls $[P_A, P_B] = 0$
- $P_{A \vee B} = P_A + P_B - P_A P_B$ falls $[P_A, P_B] = 0$
- $P_0 = 0$
- $P_1 = I$

Definition. A und B heißen *kompatibel*, falls $[P_A, P_B] = P_A P_B - P_B P_A = 0$; anderenfalls *inkompatibel*.

Welcher Körper ist der „richtige“?

Zwar sind Quantentheorien über den reellen Zahlen und den Quaternionen von Mathematikern eingehend studiert worden.

In der Beschreibung physikalischer Systeme hat sich allerdings nur $K = \mathbb{C}$ bewährt.

Warum gerade \mathbb{C} ?

Das überzeugendste Argument stammt derzeitig von Caves et al. (2000):

Nur für \mathbb{C} gilt das Quantenalogon zu einem berühmten Theorem von de Finetti in der klassischen Statistik. Dieses Theorem ermöglicht es, dem *a priori* Begriff der „Präparation“ durch eine *a posteriori* Statistik Inhalt zu geben.

Operative Auffassung

$$\text{Zustand } \pi : \{ \text{Ereignisse} \} \mapsto \{ \text{Wahrscheinlichkeiten} \}$$

Quantenlogik: Ereignisse = Orthogonalprojektionen $P : \mathcal{H} \rightarrow \mathcal{H}$

Nicht-kontextuell

Wahrscheinlichkeit hängt nur vom Ereignis und nicht vom Kontext der Messung ab

$$\pi : P \mapsto \pi(P) \in [0, 1]$$

mit den Eigenschaften

- $\pi(0) = 0$
- $\pi(I) = 1$
- $\pi(P + Q) = \pi(P) + \pi(Q)$ falls $PQ = 0$, d.h. $A_P \vdash \neg A_Q$

Satz von Gleason (1957).

Es sei $\dim \mathcal{H} \geq 3$. Jeder Zustand π wird *eindeutig* dargestellt durch

$$\pi(P) = \text{tr}(\rho P) \quad (\text{Born'sche Regel})$$

mit einer **Dichtematrix** $\rho \in \mathcal{M}_n$:

- ρ ist positiv, $\langle x, \rho x \rangle \geq 0$; also auch hermitesch, $\rho^\dagger = \rho$
- $\text{tr } \rho = 1$

Elementarer Beweis

Cooke/Keane/Moran 1985; verallgemeinert raffiniert

$$f : [0, 1] \rightarrow \mathbb{R} \text{ beschränkt, } f(x + y) = f(x) + f(y) \implies \exists c : f(x) = cx$$

Beispiel

Maximal zufälliger Zustand (**thermischer Zustand**)

$$\rho_{\text{therm}} = \frac{1}{n} I$$

behandelt alle Elementarereignisse (1-dimensionale Unterräume) gleich:

$$\text{tr}(\rho_{\text{therm}} P) = \frac{1}{n} \dim \text{range } P$$

Bemerkung

Liefert W-Verteilung d aus Motivation des Modularitätsgesetzes der Quantenlogik

Konvexität

Zustände eines Quantensystems, d.h. Dichtematrizen, bilden **konvexe Menge**

$$\rho_0, \rho_1 \text{ Dichtematrix} \implies \lambda_0 \rho_0 + \lambda_1 \rho_1 \text{ Dichtematrix}$$

für $\lambda_0, \lambda_1 \geq 0, \lambda_0 + \lambda_1 = 1$.

Interpretation

Neue Präparation durch *Auswürfeln* der Präparationen für ρ_0 bzw. ρ_1 mit Wahrscheinlichkeiten λ_0 bzw. λ_1

Extremalpunkte

Punkte einer konvexen Menge, welche sich nicht als echte Konvexkombination anderer Punkte ergeben

Lemma.

ρ *extremale* Dichtematrix genau dann, wenn es normierten Vektor $\psi \in \mathcal{H}$ gibt mit

$$\rho = \psi\psi^\dagger.$$

- solche Zustände heißen **rein**, alle anderen **gemischt**
- $\psi \in \mathcal{H}$ heißt **Wellenfunktion**
- ψ eindeutig bis auf Phasenfaktor $e^{i\phi}$, $\phi \in \mathbb{R}$

Beweis des Lemma.

- Spektraldarstellung einer Dichtematrix ρ :

$$\rho = \sum_{k=1}^m p_k \cdot \psi_k \psi_k^\dagger, \quad \sum_{k=1}^m p_k = 1, \quad \|\psi_k\| = 1, \quad p_k > 0.$$

- ρ *extremal* $\implies m = 1$ und $\rho = \psi_1 \psi_1^\dagger$.
- Ist $\rho = \psi\psi^\dagger = \lambda_0 \rho_0 + \lambda_1 \rho_1$ mit $0 < \lambda_0, \lambda_1$ und $\lambda_0 + \lambda_1 = 1$, so

$$\psi = \rho\psi = \lambda_0 \cdot \rho_0\psi + \lambda_1 \cdot \rho_1\psi,$$

Normierte Vektoren = Extremalpunkte der Kugel in \mathcal{H}

$$\curvearrowright \rho_0\psi = \psi, \rho_1\psi = \psi.$$

$$\text{Spektraldarstellung} \quad \curvearrowright \rho_0 = \rho_1 = \psi\psi^\dagger = \rho.$$

Interpretation

Darstellung eines Zustands in der Form

$$\rho = \sum_{k=1}^m p_k \cdot \psi_k \psi_k^\dagger, \quad \sum_{k=1}^m p_k = 1, \quad p_k \geq 0,$$

entspricht *Präparation* der reinen Zustände ψ_k mit Wahrscheinlichkeit p_k .

Angabe dieser Daten $(p_k, \psi_k)_k$ reicht zur Beschreibung aus, wir sprechen von der Präparation eines *Ensembles* reiner Zustände.

- reiner Zustand: Ensemble ist eindeutig
- gemischter Zustand: verschiedene Ensemblepräparationen möglich

Lemma (Test mit sicherem Ausgang).

System sei im Zustand ρ präpariert, so daß das Ereignis $P = \psi\psi^\dagger$ sicher ist,

$$\text{tr}(\rho P) = 1.$$

Dann gilt $\rho = P$, das System befindet sich im *reinen Zustand* ψ .

Beweis. Es gilt

$$1 = \text{tr}(\rho P) = \langle \psi, \rho \psi \rangle.$$

Damit gilt Gleichheit in der Cauchy-Schwarz'schen Ungleichung

$$|\langle \psi, \rho \psi \rangle| \leq \|\psi\| \cdot \|\rho \psi\| \leq 1$$

$$\curvearrowright \rho \psi = \psi.$$

Spektraldarstellung $\curvearrowright \rho = \psi\psi^\dagger = P$.

*Maximaler Test*Alternativen $\{1, \dots, n\}$ mit der Aussagenlogik

$$A_1 \vee \dots \vee A_n = 1, \quad A_i \vdash \neg A_j, \quad i \neq j, \quad A_j \neq 0,$$

also

$$P_1 + \dots + P_n = I, \quad P_i P_j = 0, \quad i \neq j, \quad P_j \neq 0.$$

Da n maximal:

$$P_j = e_j e_j^\dagger \text{ für ON-Basis } e_1, \dots, e_n.$$

- *Auswahl* des Testergebnis j präpariert Zustand $\rho_j = P_j$, da weiterer Test *sicher* das Ergebnis j lieferte
- *Eintritt* des Testergebnis j mit Wahrscheinlichkeit $\text{tr}(\rho P_j)$

*Fazit*Test liefert *gemischten* Zustand

$$\rho' = \sum_j \text{tr}(\rho P_j) \cdot P_j = \sum_j P_j \rho P_j.$$

In Basisdarstellung der Matrizen bzgl. „Testbasis“ e_1, \dots, e_n kurz:

$$\rho' = \begin{bmatrix} \rho_{11} & & \\ & \ddots & \\ & & \rho_{nn} \end{bmatrix} = \text{diag } \rho$$

„Test-Operator“ $\rho \mapsto \rho'$ ist affin, positiv, spurerhaltend, *irreversibel* und

$$\text{stochastisch : } \rho'_{\text{therm}} = \rho_{\text{therm}}.$$

Beispiel: Qubit (2-Level-Quantensystem) im reinen Zustand

$$\psi = \alpha e_0 + \beta e_1, \quad |\alpha|^2 + |\beta|^2 = 1,$$

bzgl. Rechenbasis (computational basis) e_0, e_1 . Dichtematrix:

$$\rho = \psi\psi^\dagger = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \cdot \begin{bmatrix} \bar{\alpha} & \bar{\beta} \end{bmatrix} = \begin{bmatrix} |\alpha|^2 & \alpha\bar{\beta} \\ \bar{\alpha}\beta & |\beta|^2 \end{bmatrix}$$

Testergebnis bzgl. Rechenbasis:

$$\rho' = \begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix} = |\alpha|^2 e_0 e_0^\dagger + |\beta|^2 e_1 e_1^\dagger$$

Interpretation: Test \rightarrow Qubit=Gemisch aus $\frac{|\alpha|^2}{100}\%$ à 0, $\frac{|\beta|^2}{100}\%$ à 1

(1.10-1) OBSERVABLE, HEISENBERG'SCHE UNBESTIMMTHEITSRELATION

Messung

verknüpft Ereignis $P_j = e_j e_j^\dagger$ eines maximalen Tests mit *Meßergebnis* $\alpha_j \in \mathbb{R}$.

Kodierung einer Messung

$$A = \sum_j \alpha_j P_j$$

Spektralzerlegung einer *hermiteschen Matrix (Observable)* A

Erwartungswert einer Messung im Zustand ρ

$$\langle A \rangle = \sum_{j=1}^n \alpha_j \underbrace{\text{tr}(\rho P_j)}_{\text{Wahrscheinlichkeit der Messung von } \alpha_j} = \text{tr}(\rho A)$$

Inkompatibilität: Messungen der Observablen A und B sind in Teilen inkompatibel, wenn A und B nicht in der gleichen Basis diagonalisierbar sind:

$$[A, B] = AB - BA \neq 0$$

Satz (Heisenberg'sche Unbestimmtheitsrelation, 1925).

$$\Delta(A)\Delta(B) \geq \langle [A, B] \rangle / 2.$$

$\Delta(A) = \langle A^2 \rangle - \langle A \rangle^2 = \text{Varianz}$ der Messung der Observablen A .

Beweis: Cauchy-Schwarz'sche Ungleichung...

Interpretation

Aussage über die Statistik der Messungen an einer großen Anzahl von Präparationen ein und des gleichen Zustands; *nicht* über die Genauigkeit einer einzelnen Messung. Wegen Inkompatibilität erfolgt Messung von A an einigen Systemen, Messung von B an *anderen*.

Zusammengesetzte Quantensysteme

m -Level-Quantensystem in \mathcal{H}_m und n -Level Quantensystem in \mathcal{H}_n bilden zusammen betrachtet ein weiteres Quantensystem

Maximaler Test

Tests in \mathcal{H}_m bzgl. Basis e_1, \dots, e_m und in \mathcal{H}_n bzgl. f_1, \dots, f_n

\curvearrowright mögliche Ergebnisse (i, j) , $i = 1 : m$, $j = 1 : n$.

Zusammengesetzter Zustandsraum = Tensorprodukt

$$\mathcal{H}_m \otimes \mathcal{H}_n, \quad \text{Dimension} = m \cdot n$$

Basisvektoren: formale Symbole $e_i \otimes f_j$, $i = 1 : m$, $j = 1 : n$

Tensorprodukt von Vektoren: Bilineare Fortsetzung von $(e_i, f_j) \mapsto e_i \otimes f_j$ zu

$$\otimes : \mathcal{H}_m \times \mathcal{H}_n \rightarrow \mathcal{H}_m \otimes \mathcal{H}_n$$

$$\left(u = \sum_i u_i e_i, v = \sum_j v_j f_j \right) \mapsto u \otimes v = \sum_{ij} u_i v_j \cdot e_i \otimes f_j$$

Das allgemeine Element in $\mathcal{H}_m \otimes \mathcal{H}_n$

$$\begin{aligned} \sum_{ij} w_{ij} e_i \otimes f_j &= \sum_j \left(\sum_i w_{ij} e_i \right) \otimes f_j = \sum_i e_i \otimes \left(\sum_j w_{ij} f_j \right) \\ &= \sum_i u_i \otimes v_i, \quad \{u_i\} \text{ oder } \{v_i\} \text{ Basis} \end{aligned}$$

Skalarprodukt auf $\mathcal{H}_m \otimes \mathcal{H}_n$

$$\langle u \otimes v, w \otimes z \rangle = \langle u, w \rangle \cdot \langle v, z \rangle$$

sesquilinear fortgesetzt

Tensorprodukte von Matrizen

$$M_{m,n} \otimes M_{k,l} = \mathcal{L}(\mathcal{H}_n \otimes \mathcal{H}_l, \mathcal{H}_m \otimes \mathcal{H}_k)$$

mit

$$(A \otimes B)(u \otimes v) = (Au) \otimes (Bv)$$

bilinear fortgesetzt

Satz von der Schmidt'schen Zerlegung (1906).

Für $w \in \mathcal{H}_m \otimes \mathcal{H}_n$ gibt es ON-Systeme $\{e_i\}$ in \mathcal{H}_m und $\{f_i\}$ in \mathcal{H}_n , so daß

$$w = \sum_{i=1}^{\kappa} \lambda_i e_i \otimes f_i, \quad \|w\|^2 = \sum_{i=1}^{\kappa} \lambda_i^2.$$

Dabei sind *invariant* für alle solchen Zerlegungen:

- $\lambda_i > 0$ Schmidt'schen Koeffizienten
- κ Schmidt'sche Zahl

Definition. $\kappa > 1$, so heißt w **verschränkt** (engl. **entangled**).

Beweis.

Seien e'_i und f'_j irgendwelche ON-Basen von \mathcal{H}_m bzw. \mathcal{H}_n .

$$w = \sum_{ij} w_{ij} e'_i \otimes f'_j.$$

Singulärwert-Zerlegung $U\Sigma V^T$ der Matrix $(w_{ij})_{ij}$ mit U, V unitär und $\Sigma = \text{diag}(\lambda_1, \dots)$, $\lambda_i \geq 0$, liefert

$$w = \sum_{ijk} u_{ik} \lambda_k v_{jk} e'_i \otimes f'_j = \sum_k \lambda_k \underbrace{\left(\sum_i u_{ik} e'_i \right)}_{=e_k} \otimes \underbrace{\left(\sum_j v_{jk} f'_j \right)}_{=f_k},$$

e_k (f_k) Spaltenvektoren der unitären Matrix U (V) \leadsto ON-System.

Die Invarianz zeigen wir später mit einer anderen Technik.

Identifizierung mit Matrizen

Kanonischer Isomorphismus

$$\begin{aligned} \text{vec} : M_{m,n} &\rightarrow \mathcal{H}_m \otimes \mathcal{H}_n \\ (w_{ij})_{ij} &\mapsto \sum_{ij} w_{ij} e_i \otimes f_j \end{aligned}$$

bzw. basisfrei

$$\begin{aligned} \text{mat} = \text{vec}^{-1} : \mathcal{H}_m \otimes \mathcal{H}_n &\rightarrow M_{m,n} \\ \sum_i u_i \otimes v_i &\mapsto \sum_i u_i v_i^T \end{aligned}$$

Beispiel: Matrixgleichung

$$A X B = C \iff (A \otimes B^T) \text{vec } X = \text{vec } C$$

Kronecker-Tensorprodukt (Zehfuß 1858)

Dimensionsgleichheit \curvearrowright

$$\mathcal{H}_m \otimes \mathcal{H}_n \cong \mathcal{H}_{m \cdot n}, \quad M_{m,n} \otimes M_{k,l} \cong M_{m \cdot k, n \cdot l}.$$

Wähle feste Beziehung für eine konkrete Basis:

$$e_i \otimes e_j = e_{(i-1)n+j}, \quad i = 1 : m, j = 1 : n.$$

Liefert generelle Blockstruktur: $A \in M_{m,n}, B \in M_{k,l} \curvearrowright$

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix} \in M_{m \cdot k, n \cdot l}.$$

Dimension = Zweierpotenz

$$m + n \text{ Qubits: } \mathcal{H}_{2^m} \otimes \mathcal{H}_{2^n} = \mathcal{H}_{2^{m+n}}$$

Index der Basen: Binärzahl $0 : 2^m - 1, 0 : 2^n - 1$ bzw. $0 : 2^{m+n} - 1$

Kronecker-Tensorprodukt

$$e_s \otimes e_t = e_{s,t}, \quad \text{oder kurz} \quad |s\rangle|t\rangle = |s,t\rangle,$$

s,t Verkettung der Binärzahlen s und t \curvearrowright führende Ziffern links

Beispiel

$$|00101\rangle|100\rangle = |00101100\rangle$$

ρ Dichtematrix eines Zustands auf $\mathcal{H}_A \otimes \mathcal{H}_B$

Tests im Teilsystem A: Zustand π_A auf \mathcal{H}_A

$$\pi_A(P) = \text{tr}(\rho(P \otimes I)).$$

Explizite Formel für zugehörige Dichtematrix auf \mathcal{H}_A

$$\pi_A(P) = \text{tr}(\rho_A P), \quad \rho_A = \text{tr}_B(\rho)$$

mit dem partiellen Spuroperator

$$\text{tr}_B : \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \rightarrow \mathcal{L}(\mathcal{H}_A)$$

$$\rho_A \otimes \rho_B \mapsto \rho_A \cdot \text{tr}(\rho_B), \text{ linear fortgesetzt}$$

Teilsystem B wurde **ausgespurt** (engl. **to trace out**)

Lemma.*Statistische Unabhängigkeit*

$$\text{tr}(\text{tr}_B(\rho)P_A) \cdot \text{tr}(\text{tr}_A(\rho)P_B) = \text{tr}(\rho(P_A \otimes P_B))$$

Unabhängigkeit von Messung $\Phi_B : \rho_B \mapsto \rho'_B$ im Teilsystem B

$$\text{tr}_B(\rho) = \text{tr}_B((I \otimes \Phi_B)\rho)$$

Interpretation

Es gibt *keinen* Test im System A, mit welchem festgestellt werden könnte, daß im System B etwas gemessen wurde.

The Church of the Larger Hilbert Space
– John Smolin, IBM

Prinzip der Erweiterbarkeit

System A ist mit Hilfe eines **Ancilla-Systems** B Teil eines erweiterten Systems

Anwendung

$\mathcal{H}_A = \mathcal{H}_2$ Qubit, Ancilla $\mathcal{H}_B = \mathcal{H}_n$, $n \geq 2$.

Zustände π_A und π_B liefern (statistische Unabhängigkeit) Zustand π auf $\mathcal{H}_A \otimes \mathcal{H}_B$

$$\pi(P \otimes Q) = \pi_A(P) \cdot \pi_B(Q)$$

Satz von Gleason \curvearrowright Dichtematrix ρ

$$\pi_A(P) \cdot \pi_B(Q) = \text{tr}(\rho(P \otimes Q)).$$

Also ist im erweiterbaren Fall der Satz von Gleason ist auch für Qubits gültig

$$\pi_A(P) = \text{tr}(\text{tr}_B(\rho)P) \quad \text{und} \quad \pi_B(Q) = \text{tr}(\text{tr}_A(\rho)Q)$$

Ausspuren reiner Zustände

Schmidt'sche Zerlegung eines reinen Zustandes in $\mathcal{H}_A \otimes \mathcal{H}_B$

$$\psi = \sum_{i=1}^{\kappa} \lambda_i e_i \otimes f_i, \quad \sum_{i=1}^{\kappa} \lambda_i^2 = 1, \quad \lambda_i > 0.$$

liefert wegen $\text{tr}(f_i f_j^\dagger) = f_j^\dagger f_i = \delta_{ij}$ Spektralzerlegung der partiellen Spuren

$$\rho = \psi \psi^\dagger = \sum_{i,j=1}^{\kappa} \lambda_i \lambda_j e_i e_j^\dagger \otimes f_i f_j^\dagger \quad \rightsquigarrow \quad \text{tr}_B(\rho) = \sum_{i=1}^{\kappa} \lambda_i^2 e_i e_i^\dagger$$

Hieraus folgt *Invarianz* der Schmidt'schen Koeffizienten und Zahl.

Fazit

Partielle Information über verschränkte reine Zustände liefert gemischte Zustände

Umkehrung

(Gemischter) Zustand ρ_A eines Systems A ist partielle Spur eines reinen Zustands

Dieser Prozeß heißt **Purifizierung**:

1. Spektralzerlegung $\rho_A = \sum_i \lambda_i^2 e_i e_i^\dagger$
2. definiere mit Ancilla-System $B = A$

$$\psi = \sum_i \lambda_i e_i \otimes e_i \in \mathcal{H}_A \otimes \mathcal{H}_B$$

3. es gilt nach Ausspuren

$$\rho_A = \text{tr}_B(\psi \psi^\dagger)$$

Frage

In welcher Form können Quantenzustände manipuliert werden?

Oder, wie muß ein **Superoperator** $\rho \mapsto \rho'$ beschaffen sein?

- *Konsistenz mit der Wahrscheinlichkeitsstruktur*

$\rho = \lambda_0 \rho_0 + \lambda_1 \rho_1$ durch Auswürfeln der Zustände ρ_0, ρ_1

$\implies \rho'$ durch entsprechendes Auswürfeln der Zustände ρ'_0, ρ'_1 :

$$\rho' = \lambda_0 \rho'_0 + \lambda_1 \rho'_1 \quad \curvearrowright \quad \text{Superoperatoren sind } \textit{affin}$$

- *Konsistenz mit der Zustandsstruktur*

Dichtematrizen werden auf Dichtematrizen abgebildet

Jede Matrix ist Linearkombination von Dichtematrizen \curvearrowright

Superoperator eindeutig fortsetzbar zu einer Abbildung

$$\Phi : M_n \rightarrow M_m$$

mit den Eigenschaften

- linear
- positiv: $\Phi(A) \geq 0$ für $A \geq 0$ (in Worten: A positiv semidefinit)
- spurerhaltend: $\text{tr}(\Phi(A)) = \text{tr}(A)$

Vollständige Positivität

Prinzip der Erweiterbarkeit \curvearrowright mit $\Phi : M_n \rightarrow M_m$ ist auch

$$\Phi \otimes I : M_n \otimes M_p \rightarrow M_m \otimes M_p$$

Superoperator, also positiv für jedes $p \geq 0$.

Solche Operatoren heißen **vollständig positiv**.

Beispiel

Transposition $\rho \mapsto \rho^T$

- positiv und spurerhaltend
- *nicht* vollständig positiv, also kein Superoperator

Theorem (Kraus 1971, Choi 1975)

Es sind äquivalent

- $\Phi : M_n \rightarrow M_m$ vollständig positiver, linearer Operator
- $\exists N \leq n \cdot m, V_1, \dots, V_N \in M_{m,n}$ mit

$$\Phi(A) = \sum_{i=1}^N V_i A V_i^\dagger, \quad A \in M_n \quad (\text{Kraus'sche Darstellung})$$

Zusätze

- Φ spurerhaltend $\iff \sum_i V_i^\dagger V_i = I$
- Φ stochastisch $\iff \sum_i V_i V_i^\dagger = I$

Beweis (M.-D. Choi 1975)*Beweis der Zusätze*

1. Einsetzen von $A = I$ in Kraus-Darstellung \leadsto Bedingung für Stochastizität
2. Spur invariant gegen zyklische Vertauschung \leadsto Bedingung für Spurerhaltung

$$\begin{aligned} \operatorname{tr}(A) &= \operatorname{tr}(\Phi(A)) = \sum_i \operatorname{tr}(V_i A V_i^\dagger) = \sum_i \operatorname{tr}(V_i^\dagger V_i A) \\ &= \operatorname{tr} \left(\left(\sum_i V_i^\dagger V_i \right) A \right), \quad A \in M_n, \\ &\iff I = \sum_i V_i^\dagger V_i \end{aligned}$$

*Fortsetzung des Beweises***3. Hilfsresultat**

- sei e_j ON-Basis von \mathcal{H}_n , $E_{ij} = e_i e_j^\dagger$ Basis von M_n
- dann gilt in $M_m \otimes M_n$ für $V \in M_{m,n}$

$$\sum_{ij} (V E_{ij} V^\dagger) \otimes E_{ij} = \operatorname{vec}(V) \cdot \operatorname{vec}(V)^\dagger$$

Beweis des Hilfsresultats

$$\begin{aligned} \left(\sum_{ij} (V E_{ij} V^\dagger) \otimes E_{ij} \right)_{rs, r's'} &= \sum_{ij} (V E_{ij} V^\dagger)_{rr'} (E_{ij})_{ss'} \\ &= (V E_{ss'} V^\dagger)_{rr'} = V_{rs} \bar{V}_{r's'} \\ &= (\operatorname{vec}(V) \cdot \operatorname{vec}(V)^\dagger)_{rs, r's'} \end{aligned}$$

Fortsetzung des Beweises (Hauptresultate)

$$4. E = \sum_{ij} E_{ij} \otimes E_{ij} \geq 0 \rightsquigarrow (\Phi \otimes I)(E) = \sum_{ij} \Phi(E_{ij}) \otimes E_{ij} \geq 0$$

5. Somit gibt es $N \leq n \cdot m$ Vektoren $v_k = \text{vec}(V_k) \in \mathcal{H}_m \otimes \mathcal{H}_n$ mit

$$(\Phi \otimes I)(E) = \sum_{k=1}^N v_k v_k^\dagger = \sum_{k=1}^N \text{vec}(V_k) \cdot \text{vec}(V_k)^\dagger$$

6. Hilfssatz macht daraus

$$(\Phi \otimes I)(E) = \sum_{ij} \sum_{k=1}^N (V_k E_{ij} V_k^\dagger) \otimes E_{ij}$$

7. Koeffizientenvergleich mit 4. zeigt

$$\Phi(E_{ij}) = \sum_{k=1}^N V_k E_{ij} V_k^\dagger, \quad \rightsquigarrow \quad \Phi(A) = \sum_{k=1}^N V_k A V_k^\dagger$$

Korollar

Es sind äquivalent

- Superoperator $\Phi : M_n \rightarrow M_m$ ist invertierbar (reversibel)
- $n = m$ und es gibt unitären Operator $U \in M_n$ mit

$$\Phi(A) = UAU^\dagger, \quad A \in M_n.$$

Bemerkung

Quantensysteme, welche sich reversibel verändern, heißen **geschlossen**.

Alle anderen heißen **offen**.

Beweis (B. 2001)

Φ und Φ^{-1} besitzen beide Kraus'sche Darstellung

$$\Phi^{-1}(A) = \sum_k W_k A W_k^\dagger, \quad \Phi(A) = \sum_l V_l A V_l^\dagger.$$

Mit $E = \sum_{ij} E_{ij} \otimes E_{ij}$ gilt

$$\sum_{ij} E_{ij} \otimes E_{ij} = (\Phi^{-1} \otimes I)(\Phi \otimes I)(E) = \sum_{ij} \sum_{kl} (W_k V_l E_{ij} V_l^\dagger W_k^\dagger) \otimes E_{ij},$$

also mit dem Hilfsresultat (I.13-6)

$$\text{vec}(I) \text{vec}(I)^\dagger = \sum_{kl} \text{vec}(W_k V_l) \text{vec}(W_k V_l)^\dagger.$$

Beweis des Korollars – Fortsetzung

Extremaleigenschaft von Rang-1-Matrizen (vgl. (I.8-1)) \leadsto

$$W_k V_l = \alpha_{kl} I, \quad \alpha_{kl} \in \mathbb{C}.$$

Nicht alle $\alpha_{kl} = 0 \leadsto$ o.E. $\alpha_{11} \neq 0$, $V_j = \alpha_{1j} V_1 / \alpha_{11}$ und daher

$$\Phi(A) = U A U^\dagger, \quad U = \sqrt{\sum_j \left| \frac{\alpha_{1j}}{\alpha_{11}} \right|^2} \cdot V_1.$$

Spurerhaltung \leadsto

$$I = \sum_j V_j^\dagger V_j = \sum_j \left| \frac{\alpha_{1j}}{\alpha_{11}} \right|^2 \cdot V_1^\dagger V_1 = U^\dagger U,$$

d.h. U ist unitär.

Theorem (Kraus 1983)

Zu jedem Superoperator $\Phi : M_n \rightarrow M_n$ gibt es einen Zustand ρ_{env} in einem Ancilla-System (Environment) \mathcal{H}_{env} und einen unitären Operator U auf $\mathcal{H}_n \otimes \mathcal{H}_{\text{env}}$ mit

$$\Phi(\rho) = \text{tr}_{\text{env}} (U(\rho \otimes \rho_{\text{env}})U^\dagger).$$

Interpretation

Jede Operation innerhalb eines *beliebigen* Quantensystems kann als *partielle* Information der Veränderung eines *geschlossenen* Systems gedeutet werden.

Fazit

Wir können uns auf *unitäre Operationen* und *partielle Spuren* beschränken. Als Schnittstelle zur klassischen Information werden wir auch *Messungen* einbeziehen.

Beweis

$$\Phi(A) = \sum_{k=1}^N V_k A V_k^\dagger \quad \leadsto \quad \mathcal{H}_{\text{env}} = \mathcal{H}_N \text{ mit ON-Basis } e_j.$$

Setze

$$U(\psi \otimes \psi_{\text{env}}) = \sum_k (V_k \psi) \otimes e_k, \quad \psi_{\text{env}} \in \mathcal{H}_{\text{env}} \text{ beliebig}$$

Operation unitär fortgesetztbar wegen

$$\langle U\psi \otimes \psi_{\text{env}}, U\phi \otimes \psi_{\text{env}} \rangle = \sum_{jk} \langle V_j \psi, V_k \phi \rangle \cdot \underbrace{\langle e_j, e_k \rangle}_{=\delta_{jk}} = \underbrace{\langle \sum_k V_k^\dagger V_k \psi, \phi \rangle}_{=I}.$$

Mit $\rho_{\text{env}} = \psi_{\text{env}} \psi_{\text{env}}^\dagger$ gilt also wegen $\text{tr}(e_j e_k^\dagger) = \delta_{jk}$

$$U(\rho \otimes \rho_{\text{env}})U^\dagger = \sum_{jk} (V_j \rho V_k^\dagger) \otimes e_j e_k^\dagger \quad \leadsto \quad \text{tr}_{\text{env}}(\dots) = \sum_k V_k \rho V_k^\dagger.$$

Lemma

ρ Zustand eines Quantensystems in $\mathcal{H}_A \otimes \mathcal{H}_B$.

Φ_A Superoperator auf \mathcal{H}_A , Φ_B auf \mathcal{H}_B .

Es gilt

$$\text{tr}_B((\Phi_A \otimes \Phi_B)\rho) = \Phi_A(\text{tr}_B(\rho)).$$

Beweis

Es reicht, das Resultat für $\rho = \rho_A \otimes \rho_B$ zu zeigen. Der allgemeine Fall folgt durch lineare Fortsetzung.

$$\begin{aligned} \text{tr}_B((\Phi_A \otimes \Phi_B)(\rho_A \otimes \rho_B)) &= \Phi_A(\rho_A) \text{tr}(\Phi_B(\rho_B)) \\ &= \Phi_A(\rho_A) \text{tr}(\rho_B) = \Phi_A(\text{tr}_B(\rho_A \otimes \rho_B)). \end{aligned}$$

Interpretation

Veränderungen außerhalb eines Teilsystems sind innerhalb des Teilsystems grundsätzlich *nicht feststellbar*.

Reversible Veränderung reiner Zustände

$\rho = \psi\psi^\dagger$ mit Wellenfunktion ψ , U unitär \curvearrowright

$$\rho' = U\rho U^\dagger = U\psi\psi^\dagger U^\dagger = \psi'\psi'^\dagger,$$

mit der verändertern Wellenfunktion

$$\psi' = U\psi.$$

Quantendynamik geschlossener Systeme

ein-parametrische Gruppe $U(t)$ unitärer Operatoren

$$U(t)U(s) = U(t+s).$$

Evolution eines reinen Zustands ψ_0 gemäß

$$\psi(t) = U(t)\psi_0.$$

Theorie gewöhnlicher Differentialgleichungen: $U(t)$ glatt \leadsto

$$i\dot{\psi}(t) = H\psi(t), \quad H = i\dot{U}(0),$$

die **Schrödinger-Gleichung** mit dem **Hamilton-Operator** H .

Lemma. Der Hamilton-Operator ist eine Observable.

Beweis

Differentiation der Unitaritätsbeziehung $I = U(t)U(t)^\dagger$ liefert

$$0 = \dot{U}(t) \cdot U(t)^\dagger + U(t)\dot{U}(t)^\dagger \Big|_{t=0} = \dot{U}(0) + \dot{U}^\dagger(0),$$

d.h. $\dot{U}(0)$ schief-hermitesch $\leadsto H = i\dot{U}(0)$ hermitesch.

Bemerkung

Die Eigenwerte von H heißen *Energie-Niveaus* des Systems.

Gesucht

Reversible Operationen auf Qubits, welche auch Observable sind, d.h.

$$U : \mathcal{H}_2 \rightarrow \mathcal{H}_2 \text{ unitär und hermitesch.}$$

Lemma. $U = \pm I$ oder

$$U = \alpha X + \beta Y + \gamma Z, \quad \alpha, \beta, \gamma \in \mathbb{R}, \quad \alpha^2 + \beta^2 + \gamma^2 = 1,$$

mit den **Pauli-Matrizen**

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Beweis. Übung.

X verallgemeinert logisches *nicht* auf Qubit:

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle.$$

Kommutatoren: $[X, Y] = 2i Z$, $[Y, Z] = 2i X$, $[Z, X] = 2i Y$

Tests bzgl. der jeweiligen Eigenräume sind also *inkompatibel*.

Antikommutatoren: $\{X, Y\} = \{Y, Z\} = \{Z, X\} = 0$.

Spektralzerlegungen

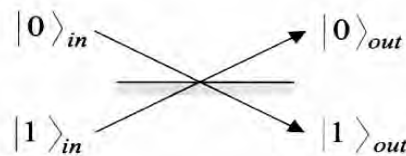
$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

$$Y = |+\rangle\langle +| - |-\rangle\langle -|, \quad |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

$$X = |\uparrow\rangle\langle \uparrow| - |\downarrow\rangle\langle \downarrow|, \quad |\uparrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\downarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

50/50-Strahlteiler (*beam splitter*)

z.B. halbdurchlässiger Spiegel für Photonen, eintreffend von oben bzw. unten werden sie mit 50%-Wahrscheinlichkeit gespiegelt oder durchgelassen.

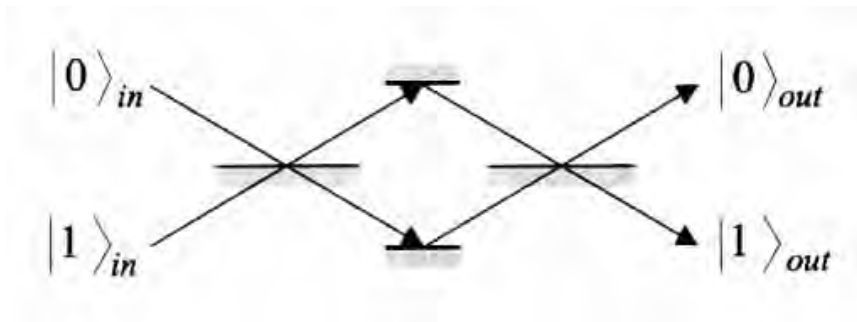


Zeilinger (Am. J. Phys. 49, 882, 1981):

im selbstreversiblen Fall bei geeigneter Basiswahl beschrieben durch die **Hadamard-Transformation**

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(X + Z).$$

Mach-Zehnder Interferometer



Wegen $H^2 = I$ verläßt ein von oben bzw. unten eintreffendes Teilchen das Interferometer *sicher* wieder nach oben bzw. unten.

Es ist aber *nicht* feststellbar, welchen Weg es zwischendurch genommen hat.

(1.16-1) EPR-PAARE UND VERSCHRÄNKUNG

ON-Basis auf Zustandsraum $\mathcal{H}_A \otimes \mathcal{H}_B = \mathcal{H}_2 \otimes \mathcal{H}_2$ zweier Qubits:

$$\begin{aligned}\psi_{00} &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}, & \psi_{01} &= \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \\ \psi_{10} &= \frac{|00\rangle - |11\rangle}{\sqrt{2}}, & \psi_{11} &= \frac{|01\rangle - |10\rangle}{\sqrt{2}}.\end{aligned}$$

Bell'sche Zustände (Bell 1964) bzw. **EPR-Paare** (Einstein/Podolsky/Rosen 1935).

Darstellung ist Schmidt'sche Zerlegung mit

- Schmidt'scher Zahl $\kappa = 2$
- Schmidt'schen Koeffizienten $1/\sqrt{2} \rightsquigarrow$ Zustände sind *maximal verschränkt*

Dichteoperatoren $\rho_{ij} = \psi_{ij}\psi_{ij}^\dagger$ erfüllen nach (1.12-4)

$$\text{tr}_A(\rho_{ij}) = \rho_{\text{therm}}, \quad \text{tr}_B(\rho_{ij}) = \rho_{\text{therm}}.$$

Beobachtung

$$(X \otimes X)\psi_{00} = \frac{|11\rangle + |00\rangle}{\sqrt{2}} = \psi_{00},$$

$$(Y \otimes Y)\psi_{00} = \frac{(-i)^2|11\rangle + i^2|00\rangle}{\sqrt{2}} = -\psi_{00},$$

also ist ψ_{00} Linearkombination der Eigenvektoren $|\uparrow\uparrow\rangle$ und $|\downarrow\downarrow\rangle$ bzw. $|+-\rangle$ und $|-\rangle$.

Tatsächlich gilt sogar

$$\psi_{00} = \frac{|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle}{\sqrt{2}} = \frac{|+-\rangle + |-\rangle}{\sqrt{2}}.$$

Das Einstein-Podolsky-Rosen-„Paradoxon“ (1935)

- A und B sind sehr weit auseinander und teilen EPR-Paar ψ_{00}
- A und B führen unabhängige Messungen an ihrem Teilchen des Paares aus

Ergebnisse sind etwa:

Messung (A)	Z	Z	X	Z	Z	Y	Z	Z	Y	Z	Z	X
Ergebnis (A)	0	1	↑	0	0	+	1	0	-	1	1	↓
Messung (B)	Z	X	X	Z	Z	Y	Z	Y	X	Z	Z	X
Ergebnis (B)	0	↓	↑	0	0	-	1	+	↓	1	1	↓

Beobachtung

Perfekte Korrelation der Ergebnisse im Falle der gleichen Wahl einer Messung.

Was soll paradox sein?

Argumentation von Einstein, Podolsky und Rosen:

- Lokalität
Messung in B kann System A nicht beeinflussen, keine „spukhafte Fernwirkung“ (Einstein)
- Realität
wenn B „Eigenschaft“ für System A voraussagen kann (z.B. wenn A Z misst, kommt 0 heraus), muss dem „Element der Realität“ im System A entsprechen

quantenmechanisch *inkompatible* Aussagen können so simultan Realität werden (z.B. in der 2. Messung: 1 und ↓).

Fazit von Einstein/Podolsky/Rosen

Quantentheorie ist „unvollständige“ Beschreibung der Realität.
Es muß „verborgene Parameter“ geben.

Bell'sche Ungleichung (1964)

Lokaler Realismus und Quantentheorie sagen für ein bestimmtes (schematisches) Experiment verschieden starke Korrelationen voraus.

Quantenoptisches Experiment von Aspect (1982)

Quantentheorie ist bestätigt, lokaler Realismus widerlegt

Heutzutage (wenigstens) zwei Schulen:

- Realisten
sprechen weiter von „Eigenschaften“, lassen Nichtlokalität (Fernwirkung) zu.
- Korrelationisten
Quantentheorie macht Aussagen über Messungen und statistische Korrelationen, nicht über reale „Eigenschaften“ von Einzelsystemen

Frage

Kann Alice zwei klassische Bits an Bob übertragen, indem sie *ein* Qubit verschickt?

Antwort 1

Nicht ohne weiteres, da mit einem einzelnen Qubit nur ein klassisches Bit an Information zuverlässig übertragen werden kann (Holevo-Schranke 1973).

Antwort 2

Ja, wenn Alice und Bob *vorab* ein EPR-Paar geteilt haben (Bennett/Wiesner 1992).

Fazit

EPR-Paare sind heute technologische Resource, kein philosophisches Mysterium.

Auf der einfachen Beobachtung

$$(Z^{\beta_1} X^{\beta_2} \otimes I)\psi_{00} = \psi_{\beta_1\beta_2}, \quad \beta_1, \beta_2 \in \{0, 1\}$$

basiert das *Protokoll* des **Superdense Coding**:

1. Alice und Bob teilen das EPR-Paar ψ_{00}

viel später...

2. Alice unterwirft ihr Teilchen der Operation $Z^{\beta_1} X^{\beta_2}$
3. Alice schickt ihr Teilchen an Bob
4. Bob misst Teilchenpaar in Bell'scher Basis und erhält die Bits β_1, β_2 mit W-keit 1

Experimentell bestätigt durch Mattle/Weinfurter/Kwiat/Zeilinger 1996 in Innsbruck.

Das Bit

Wertebereich ist Restklassenkörper

$$\{0, 1\} = \{\text{gerade, ungerade}\} = \mathbb{Z}_2$$

- Multiplikation $\hat{=}$ logisches *und*

$$\text{AND} : \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_2, \quad (x, y) \mapsto xy = x \text{ AND } y$$

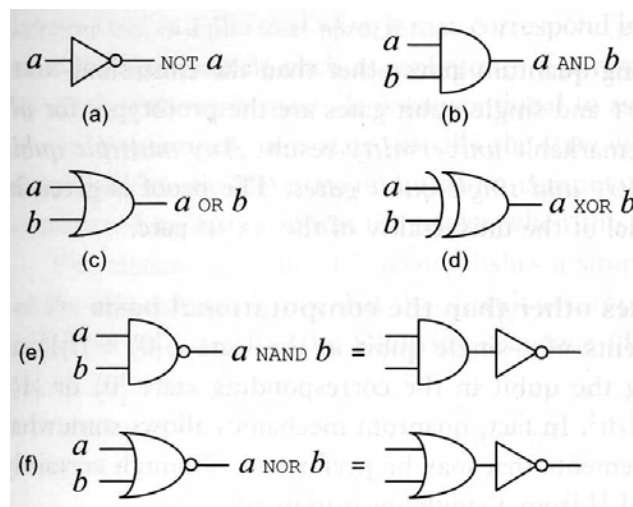
- Addition $\hat{=}$ logisches *exklusives oder*

$$\text{XOR} : \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_2, \quad (x, y) \mapsto x + y = x \oplus y = x \text{ XOR } y$$

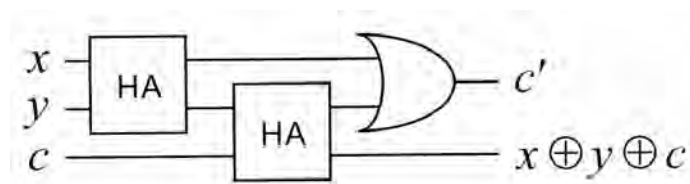
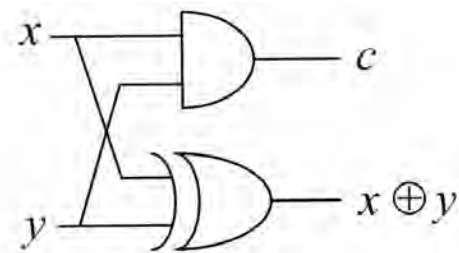
- Negation

$$\text{NOT} : \mathbb{Z}_2 \rightarrow \mathbb{Z}_2, \quad x \mapsto \bar{x} = \neg x = \text{NOT } x$$

Elementare Gatter



- jede Leitung = ein Bit
- azyklischer Graph \curvearrowright links/rechts = vorher/nachher

Beispiel**Addierwerk (Half-adder und full-adder)**

$\oplus = \text{XOR} = \text{Addition auf } \mathbb{Z}_2 = \{0, 1\}$

Universalitätssatz

Jedes $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ realisierbar aus folgenden „Bauteilen“:

- Leitungen
- Ancilla-Bits: Hilfsbits, „präpariert“ als 0 oder 1
- FANOUT: kopiert ein Bit auf zwei
- CROSSOVER oder SWAP: vertauscht zwei Bits
- elementare Gatter: AND, XOR und NOT

Beweis

O.E. $m = 1$, d.h. *Boole'sche Funktion*. Induktion nach n .

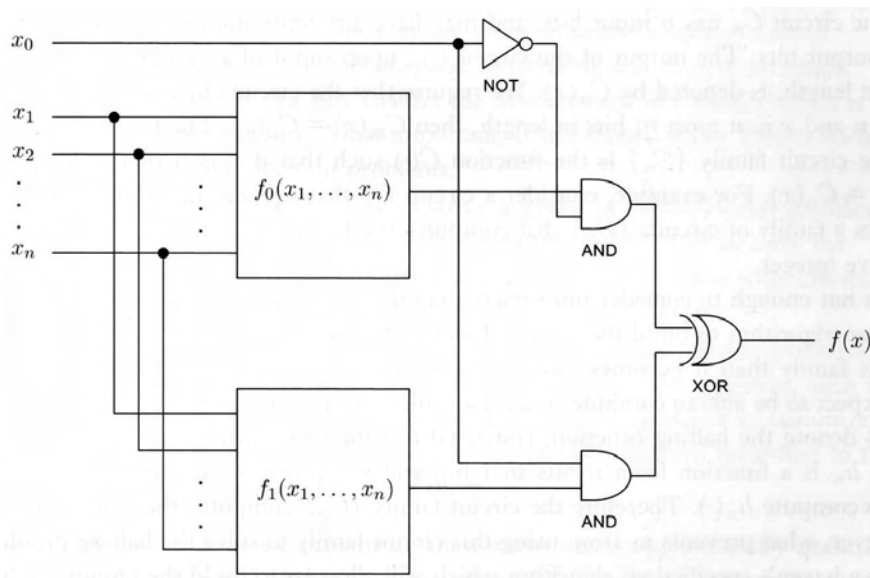
$n = 1$: Möglichkeiten für $f : \{0, 1\} \rightarrow \{0, 1\}$

1. f Identität: eine Leitung
2. f vertauscht 0 und 1: NOT-Gatter
3. $f \equiv 0$: $f(x) = x \cdot 0$
4. $f \equiv 1$: $f(x) = \neg(x \cdot 0)$

$n \rightarrow n + 1$: Definiere zwei n -Bit-Funktionen

$$f_0(x_1, \dots, x_n) = f(0, x_1, \dots, x_n), \quad f_1(x_1, \dots, x_n) = f(1, x_1, \dots, x_n)$$

(2.1-6) SCHALTKREISMODELL KLASSISCHER COMPUTER

Beweis – Fortsetzung**Bemerkung**

NAND-Gatter statt $\{\text{AND}, \text{XOR}, \text{NOT}\}$ reicht.

*Entscheidungsprobleme*Besitzt Zeichenkette x Eigenschaft \mathcal{L} ?Formalisierung: Auswertung einer Boole'schen Funktion f

- $\{0, 1\}^* = \{x : \text{endliche Zeichenkette aus den Zeichen 0 und 1}\}$
- $f : \{0, 1\}^* \rightarrow \{0, 1\}$
- $\mathcal{L} = \{x : f(x) = 1\}$

Beispiele

- (A) Ist die Zahl x prim?
- (B) Hat der durch x codierte Graph einen Hamilton'schen Kreis?
- (C) Hält das durch x repräsentierte C-Programm an?

Universalitätssatz liefert Familie $\{C_n\}_n$ von Schaltkreisen mit

$$x \in \{0, 1\}^* \text{ der Länge } n \implies C_n(x) = f(x).$$

Aber (Turing 1936)Halteproblem (C) ist unentscheidbar, d.h. f nicht berechenbar.Also ist C_n nicht algorithmisch angebbbar.*Forderung*

Algorithmus (z.B. auf Turing-Maschine), welcher „den Schaltkreis zeichnet“,

$$n \mapsto C_n.$$

↪ Schaltkreise äquivalentes Modell der Berechenbarkeit

Uniforme Familien von Schaltkreisen

Turing-Maschine für $n \mapsto C_n$ hat polynomielle Laufzeit in n .

Komplexitätsklassen für Entscheidungsprobleme

- **P**
Zeitbedarf wächst polynomiell in n
- **NP**
es gibt Zertifikat für Antwort „Ja“, in polynomieller Laufzeit überprüfbar
- **PSPACE**
Speicherbedarf wächst polynomiell in n

Randomisierung (probabilistische Maschine)

ausgewählte Ancilla-Bits aus „Wurf einer fairen Münze“ präpariert

Komplexitätsklasse

- **BPP**
polynomielle probabilistische Maschine entscheidet mit
Irrtumswahrscheinlichkeit $\leq 1/4$

Chernoff'sche Schranke

n -fache Wiederholung und „Mehrheitsentscheid“

$$\text{Irrtumswahrscheinlichkeit} \leq e^{-n/8}$$

Hierarchie

$$\mathbf{P} \subset \mathbf{NP} \subset \mathbf{PSPACE}, \quad \mathbf{P} \subset \mathbf{BPP} \subset \mathbf{PSPACE}$$

Beispiele

- Problem (A) in \mathbf{P} (Agrawal/Kayal/Saxena 2002)
 - Problem (B) ist \mathbf{NP} -vollständig (Karp 1972), d.h.
 - $B \in \mathbf{NP}$
 - $B \in \mathbf{P} \Rightarrow \mathbf{P} = \mathbf{NP}$
- nur Algorithmen *exponentieller* Laufzeit bekannt

Offene Probleme

Ist irgendeine der obigen Inklusionen eine Gleichheit? $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$

Wie verhält sich \mathbf{BPP} zu \mathbf{NP} ? $\mathbf{BPP} \stackrel{?}{\subset} \mathbf{NP}$

Beobachtung

elementare Gatter AND, XOR, NAND, etc. sind *irreversibel*

Frage

Ist *reversibles* Rechnen möglich?

Motivation

- Landauers Prinzip (1961)
 - *reversible* Manipulation benötigt prinzipiell *keine* Energie
 - Löschen eines Bits $\hat{=}$ Energieabgabe an Umgebung ($\geq k_B T \ln 2$)
- Superoperatoren $\hat{=}$ unitäre Operatoren und partielle Spur $\hat{=}$ reversible Manipulation und „Löschen“ von Information



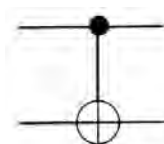
Aus: R. Landauer, *Information is Physical*, *Physics Today*, May 1991, 23–29

(2.3-2) REVERSIBLE KLASSISCHE SCHALTKREISE

Reversible Gatter: $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ bijektiv

Beispiele

- $n = 1$: NOT
- $n = 2$: CNOT (*controlled NOT*)

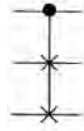


Zwei äquivalente Beschreibungen:

$$(0, a) \mapsto (0, a), \quad (1, a) \mapsto (1, \neg a), \quad \text{bzw.} \quad (c, a) \mapsto (c, c \oplus a).$$

Das Gatter CNOT heißt deswegen auch *reversible XOR*.

n = 3:

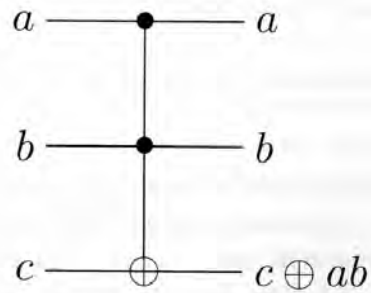


- FREDKIN oder *controlled SWAP*:

$$(0, a, b) \mapsto (0, a, b), \quad (1, a, b) \mapsto (1, b, a).$$

- TOFFOLI oder *controlled CNOT*:

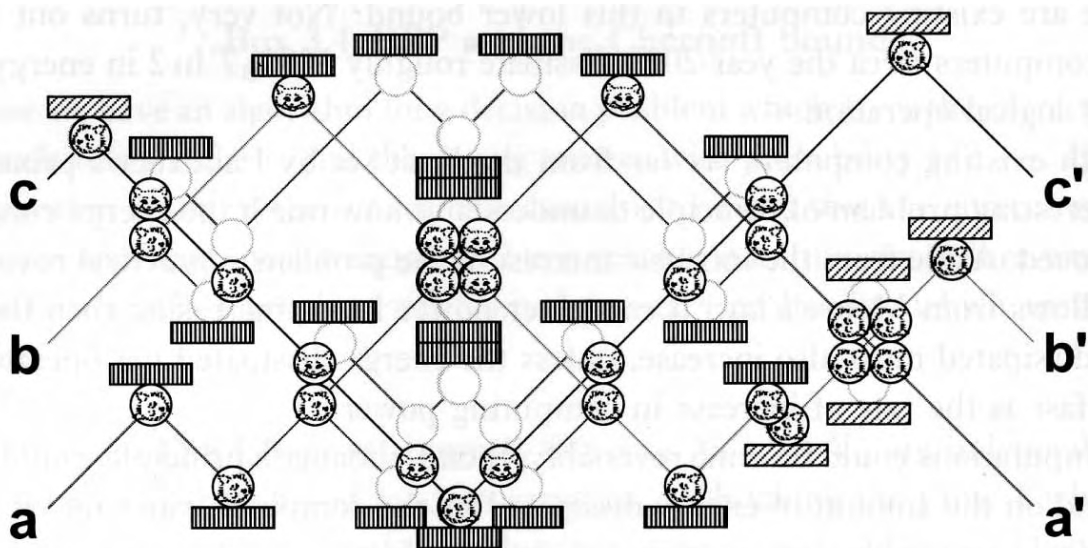
Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



Dissipationsfreier Billardball-Computer

Fredkin/Toffoli, *Internat. J. Theoret. Phys.* 21(3/4), 219-253 (1982)

Implementierung des FREDKIN-Gatters nach Feynman/Ressler



1 = „Ball“, 0 = „kein Ball“

Universalitätssatz

Das FREDKIN-Gatter ist universell.

D.h., $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ mit Hilfe von Ancilla- und Garbage-Bits in der Form

$$(x, a) \mapsto (f(x), g(x))$$

als reversibler Schaltkreis aus folgenden „Bauteilen“ darstellbar:

- Leitungen
- FREDKIN-Gatter

Bemerkung

Der gleiche Satz gilt für das Toffoli-Gatter.

Fazit

Billard-Computer ist universeller dissipationsfreier Computer

Beweis

Anwendung des FREDKIN-Gatters liefert

- AND: $(x, y, 0) \mapsto (x, \bar{x}y, xy)$
- FANOUT, NOT: $(x, 0, 1) \mapsto (x, x, \bar{x})$
- SWAP: $(1, x, y) \mapsto (1, y, x)$

Satz folgt nun aus Universalität von NAND, SWAP und FANOUT.

Bemerkung

Es gibt kein universelles reversibles Gatter auf $n = 2$ Bits.

Beweisidee: reversible Gatter auf $n = 2$ Bits sind linear über \mathbb{Z}_2 .

Problem

Garbage-Bits

- „müllen“ den Speicher zu
- nicht als Ancilla-Bits recyclefähig, da Werte „unvorhersehbar“
- zurücksetzen (löschen) kostet Energie

Später Preis für Reversibilität?

Abhilfe

Nutze den Werdegang der Garbage-Bits durch **Uncomputation** (Bennett 1973)

Zusätzlich zu universellem Gatter wird benötigt

- NOT: \curvearrowright Ancilla-Bits können als 0 präpariert werden
- CNOT: \curvearrowright FANOUT ohne Garbage-Bit,

$$(c, 0) \mapsto (c, c \oplus 0) = (c, c).$$

Uncomputation

Schrittweise Änderung des reversiblen Schaltkreises für $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$:

1. Ausgangspunkt: $(x, 0) \mapsto (f(x), g(x))$.
2. Garbage-freier FANOUT: $(x, 0, 0) \mapsto (x, x, 0) \mapsto (x, f(x), g(x))$.
3. Weiteres m-Bit Register:
 $(x, 0, 0, y) \mapsto (x, f(x), g(x), y) \mapsto (x, f(x), g(x), y \oplus f(x))$.
4. Rückwärtsrechnung vom Schritt 2:
 $(x, 0, 0, y) \mapsto (x, f(x), g(x), y \oplus f(x)) \mapsto (x, 0, 0, y \oplus f(x))$.

Zusammenfassung

Reversible Standardrealisierung von f

$$(x, y) \mapsto (x, y \oplus f(x))$$

Komplexitätsklassen

Reversible Standardrealisierung von $f \rightsquigarrow$ keine Änderung von

- **P, BPP, NP**

falls *nur* reversible Schaltkreise zugelassen werden.

Bennett (1989), Li/Tromp/Vitányi (1996/98): entsprechendes gilt für

- **PSPACE**

Bemerkung

Theorie reversibler Schaltkreise \rightsquigarrow

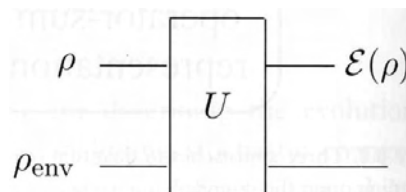
erhebliche Fortschritte bei integrierten Schaltkreisen niedriger Leistungsaufnahme in CMOS-Technologie (Merkle 1993, Younis/Knight 1994).

Quantencomputer als Superoperator

U unitär,

$$\rho \mapsto \mathcal{E}(\rho) = \text{tr}_{\text{env}} (U(\rho \otimes \rho_{\text{env}})U^\dagger).$$

„env“ steht für die Ancilla-Qubits, im Ergebnis durch partielle Spur „gelöscht“

Quantencomputer als Schaltkreis

Obere Leitungen $\hat{=}$ Qubits mit *höherwertigen* Bits in Indizierung des Tensorprodukts

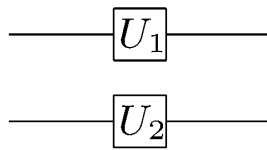
Rechenregeln für Quantenschaltkreise

- verschiedene Schreibweisen für unabhängige Operationen auf 2 Qubits



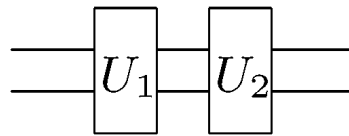
$$A|\psi\rangle \otimes B|\phi\rangle = (A \otimes B)(|\psi\rangle \otimes |\phi\rangle) = (A \otimes B)|\psi\phi\rangle$$

- Tensorprodukt $\hat{=}$ *parallele* Ausführung von Gattern



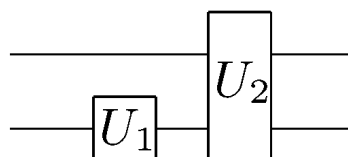
realisiert $U_1 \otimes U_2 \in M_4$ für $U_1, U_2 \in M_2$

- Matrixprodukt $\hat{=}$ *serielle* Ausführung von Gattern



realisiert $U_2 \cdot U_1 \in M_4$ für $U_1, U_2 \in M_4$

- *durchgezogene* „Quantenleitung“ entspricht *Identität*



realisiert $U_2 \cdot (I \otimes U_1) \in M_4$ für $U_1 \in M_2, U_2 \in M_4$

Quantengatter \triangleq fester unitärer Operator auf wenigen Qubits

Reversible klassische Gatter als Quantengatter

reversibles (=bijektives) $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ definiert unitären Operator

$$U_f : \mathcal{H}_2^{\otimes n} \rightarrow \mathcal{H}_2^{\otimes n}, \quad U_f |x\rangle = |f(x)\rangle \text{ für } x \text{ Bitstring der Länge } n,$$

d.h. die zugehörige *Permutationsmatrix*.

Fazit

Reversible klassische Schaltkreise können durch Quantengatter abgebildet werden

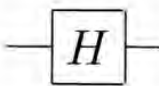
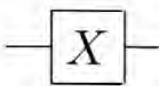
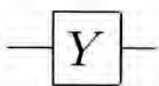
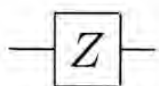
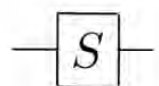
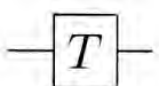
Wirkung auf Rechenbasis entspricht klassischer Operation

Beispiele

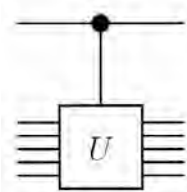
- CNOT: $U |c, x\rangle = |c, c \oplus x\rangle, \quad U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

- SWAP: $U |x, y\rangle = |y, x\rangle, \quad U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

Beispiele (Gatter auf einem Qubit)

Hadamard		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Gesteuerte Operationen („if...then“)



$$C(U) : \mathcal{H}_2^{\otimes(n+1)} \rightarrow \mathcal{H}_2^{\otimes(n+1)}, \quad |c, x\rangle \mapsto |c, U^c(x)\rangle$$

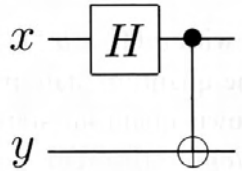
Rekursiv entsprechend $C^{k+1}(U) = C(C^k(U))$, $C^1(U) = C(U)$, d.h.

$$C^k(U) \cdot |c_1, \dots, c_k, x\rangle = |c_1, \dots, c_k, U^{c_1 \dots c_k} x\rangle.$$

Beispiele

$$\text{CNOT} = C(X), \text{ FREDKIN} = C(\text{SWAP}), \text{ TOFFOLI} = C^2(X)$$

Präparation der Bell'schen Zustände



liefert ψ_{xy} .

Als Gleichung

$$\psi_{xy} = C(X) \cdot (H \otimes I) \cdot |x, y\rangle.$$

Messung eines Qubits in Rechenbasis

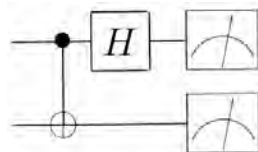
Abbildung $\mathcal{H}_2 \rightarrow \mathbb{Z}_2$



Notation: doppelte Linien = Leitungen für klassische Bits

Anwendung

Messung in Bell'scher Basis (invers zur Präparation)



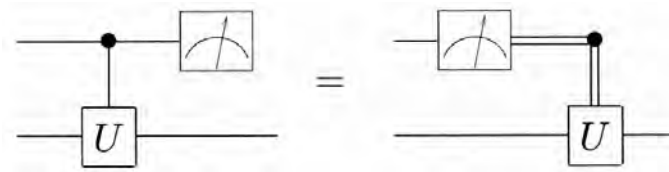
Mit Wahrscheinlichkeit 1

$$\psi_{xy} \mapsto (x, y).$$

Satz. (Prinzip der impliziten Messung)

Nicht mehr benötigte Qubits können, ohne das Verhalten der restlichen Qubits zu verändern, als gemessen angesehen werden.

Beweis. Folien (1.12-2) und (1.13-13).

Satz. (Prinzip der verschobenen Messung, Griffiths/Niu 1996)**Beweis****Blockstrukturierung des Kronecker-Tensorprodukts**

$$\rho_{\text{in}} = \begin{bmatrix} \rho_{00} & \rho_{10}^\dagger \\ \rho_{10} & \rho_{11} \end{bmatrix}, \quad C(U) = \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix}.$$

Partielle Spuren (c = Kontroll-Qubit, r = restliche Qubits)

$$\text{tr}_r(\rho_{\text{in}}) = \begin{bmatrix} \text{tr}(\rho_{00}) & * \\ * & \text{tr}(\rho_{11}) \end{bmatrix}, \quad \text{tr}_c(\rho_{\text{in}}) = \rho_{00} + \rho_{11}.$$

- Messung des Kontroll-Qubits

0 mit Wahrscheinlichkeit $\text{tr}(\rho_{00}) \rightsquigarrow \rho_r = \rho_{00} / \text{tr}(\rho_{00})$

1 mit Wahrscheinlichkeit $\text{tr}(\rho_{11}) \rightsquigarrow \rho_r = \rho_{11} / \text{tr}(\rho_{11})$

Schaltkreis rechts präpariert also die Ausgabe

$$\rho_{\text{out}} = \text{tr}(\rho_{00}) \cdot \frac{\rho_{00}}{\text{tr}(\rho_{00})} + \text{tr}(\rho_{11}) \cdot U \frac{\rho_{11}}{\text{tr}(\rho_{11})} U^\dagger = \rho_{00} + U \rho_{11} U^\dagger.$$

- Anwendung der gesteuerten U-Operation

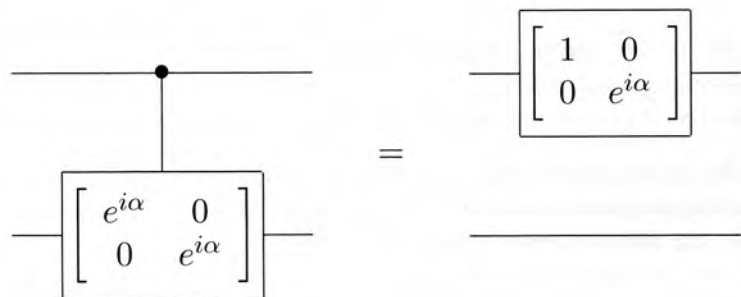
$$C(U) \rho_{\text{in}} C(U)^\dagger = \begin{bmatrix} \rho_{00} & \rho_{10}^\dagger U^\dagger \\ U \rho_{10} & U \rho_{11} U^\dagger \end{bmatrix}.$$

Schaltkreis links präpariert also die gleiche Ausgabe

$$\rho_{\text{out}} = \text{tr}_c(C(U) \rho_{\text{in}} C(U)^\dagger) = \rho_{00} + U \rho_{11} U^\dagger.$$

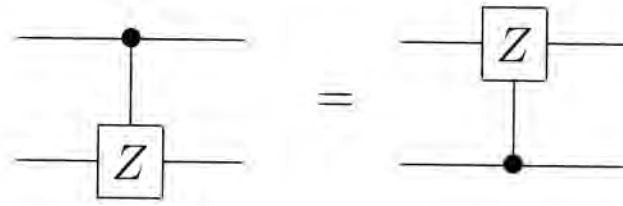
(2.5-1) EINFACHE GLEICHUNGEN FÜR QUANTENGATTER

Lemma.



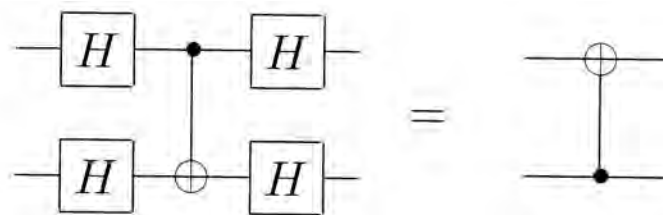
Beweis.

$$C \left(\begin{bmatrix} e^{i\alpha} & \\ & e^{i\alpha} \end{bmatrix} \right) = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & e^{i\alpha} & \\ & & & e^{i\alpha} \end{bmatrix} = \begin{bmatrix} 1 & \\ & e^{i\alpha} \end{bmatrix} \otimes I.$$

Lemma.**Beweis.**

Mit dem MATLAB-Paket der Vorlesung:

```
>> SetBasicGates;
>> C1 = {1
        Ctrl(Z)}; U1 = Circuit2Operator(C1);
>> C2 = {Ctrl(Z)
        1      }; U2 = Circuit2Operator(C2);
>> Equal(U1,U2)
ans = true
```

Lemma.**Beweis.**

```
>> C1 = {H 1      H
        H CNOT H}; U1 = Circuit2Operator(C1);
>> C2 = {CNOT
        1      }; U2 = Circuit2Operator(C2);
>> Equal(U1,U2)
ans = true
```

Lemma.**Beweis.**

```

>> C = {1      CNOT 1
         CNOT 1  CNOT};
>> U = Circuit2Operator(C);
>> Equal(U,SWAP)
ans = true

```

Dual zum Superdense Coding

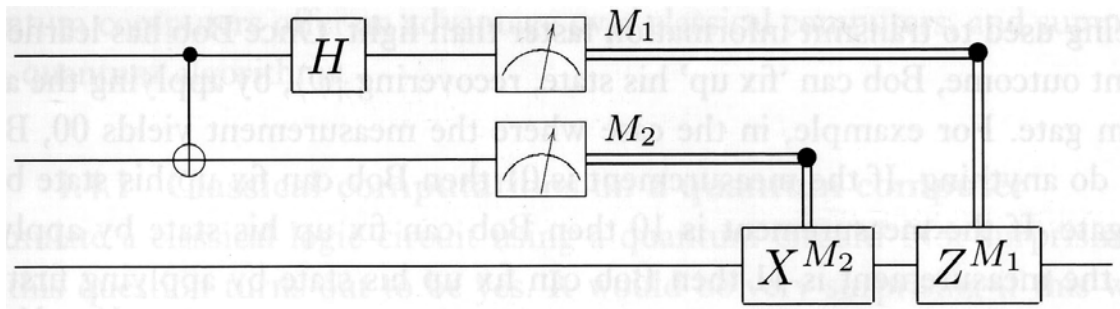
...wenn Alice und Bob vorher ein *EPR-Paar* teilen, so kann Alice an Bob mit zwei klassischen Bits über einen **klassischen** Kommunikationskanal ein Qubit übertragen:

„Beam me up, Scotty..“

Für Alice gilt

- *keine* Messung des Qubits
- *keine* Kenntnis der Präparation des Qubits

Schema (Bennett/Brassard/Crépeau/Josza/Peres/Wootters 1993)



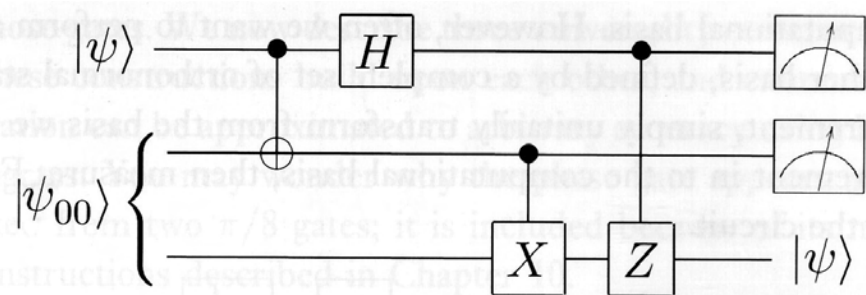
Alice: Qubits #1 & #2

Bob: Qubit #3

Input: Qubit #1 = ψ , Qubits #2 & #3 = ψ_{00}

Output: Qubit #3 = ψ

Äquivalenter Schaltkreis nach „Prinzip der verschobenen Messung“



Satz.

Für U Teleportationsschaltkreis und $\rho_{00} = \psi_{00}\psi_{00}^\dagger$ gilt

$$\text{tr}_{\text{Alice}}(U(\rho \otimes \rho_{00})U^\dagger) = \rho.$$

Beweis.

Wegen Linearität des zugehörigen Superoperators reicht es, Gleichheit für eine Basis $\{\rho_1, \rho_2, \rho_3, \rho_4\}$ von M_2 aus Dichtematrizen zu zeigen.

Wir wählen $\rho_j = \psi_j \psi_j^\dagger$ als reine Zustände mit

$$\psi_1 = |0\rangle, \quad \psi_2 = |1\rangle, \quad \psi_3 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad \psi_4 = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle).$$

```
>> psi_in(:,1) = Ket('0');
>> psi_in(:,2) = Ket('1');
>> psi_in(:,3) = (Ket('0')+ Ket('1'))/sqrt(2);
>> psi_in(:,4) = (Ket('0')+i*Ket('1'))/sqrt(2);

>> psi_00 = (Ket('00')+Ket('11'))/sqrt(2);
```

Beweis-Fortsetzung

```
>> TELEPORT = Circuit2Operator({ 1      H  w  1
                                CNOT  w  1  w
                                w      w  CX  CZ });

>> for j=1:4
    [psi_out,p] = TraceOut(...
        TELEPORT*Tensor(psi_in(:,j),psi_00),0,2,1);
    [psi_out,p] = EnsembleSimplify(psi_out,p);
    success = Equal(psi_in(:,j),psi_out);
    if isequal(success,'false'), break; end
end
>> success
success = true
```

Experimenteller Nachweis

quantenoptische Experimente

- 4 Teilchen-Experiment (Innsbruck 1997):
Bouwmeester/Pan/Mattle/Eibl/Weinfurter/Zeilinger
- 2 Teilchen-Experiment (Rom 1998):
Boschi/Branca/De Martini/Hardy/Popescu

Beim Innsbrucker-Experiment führt Bob $Z^{M_1} X^{M_2}$ *nicht* aus. Die klassische Kommunikation liefert für $M_1 = M_2 = 0$ nur eine *Auswahlanweisung* an Bob; *reduzierte Effizienz* der Teleportation.

Literatur

Bouwmeester/Ekert/Zeilinger (Hrsg.): The Physics of Quantum Information, Springer-Verlag, Berlin, Heidelberg, New York 2000.

(2.7-1) REDUKTION GESTEUERTER GATTER

Wir machen uns auf den Weg zum Universalitätssatz...

Zwischenziel

Gesteuertes Gatter $C^n(U) \in M_2^{\otimes(n+1)}$, mit I-Qubit-Gatter $U \in M_2$, ausdrücken durch CNOT- und I-Qubit-Gatter.

Theorie von Barenco/Bennett/Cleve/DiVincenzo/Margolus/Shor/Sleator/Smolin/Weinfurter (1995)

*I. "Schaltbare" Darstellung von U***Lemma.**

Für $U \in M_2$ unitär gibt es $\alpha \in [0, 2\pi]$ und unitäre Matrizen $A, B, C \in M_2$, so daß

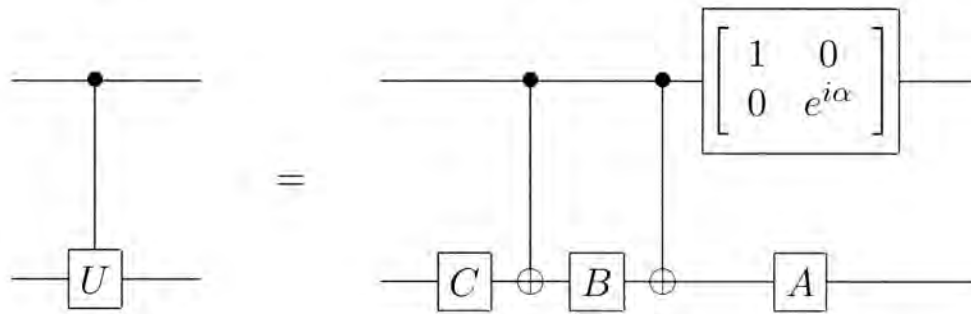
$$U = e^{i\alpha} A X B X C, \quad A B C = I.$$

Beweis. Einfach, aber technisch. Details im Internet.

2. Reduktion von $C(U)$

Korollar.

$C(U)$ ist durch CNOT- und I-Qubit-Gatter ausdrückbar,



Beweis.

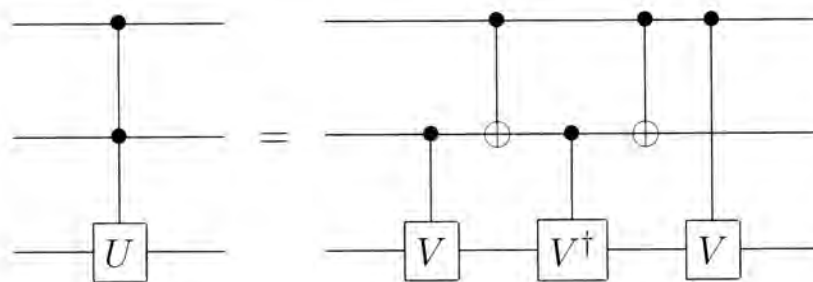
Aus dem Lemma folgt

$$C(U) = C(e^{i\alpha}) (I \otimes A) C(X) (I \otimes B) C(X) (I \otimes C).$$

Verwende das Resultat aus (2.5-1) für $C(e^{i\alpha})$.

3. Reduktion von $C^2(U)$ auf $C(V)$

Wähle V unitär mit $V^2 = U$



Beweis.

Aus $VV^\dagger = V^\dagger V = I$ folgt

$$|c_1 c_2, x\rangle \mapsto |c_1 c_2, V^{c_1} (V^\dagger)^{c_1 \oplus c_2} V^{c_2} x\rangle = \begin{cases} |c_1 c_2, V^2 x\rangle & \text{für } c_1 c_2 = 1 \\ |c_1 c_2, x\rangle & \text{für } c_1 c_2 = 0 \end{cases} = |c_1 c_2, U^{c_1 c_2} x\rangle.$$

Anwendung auf das TOFFOLI-Gatter $C^2(X)$

Es ist $Z = S^2 \rightsquigarrow$

$$X = HZH = HS^2H = HSH \cdot HSH = V^2, \quad V = HSH.$$

Also läßt sich TOFFOLI = $C^2(X)$ durch $C(V)$ und CNOT ausdrücken.

Reduktion von $C(V)$ nach (2.7-2)

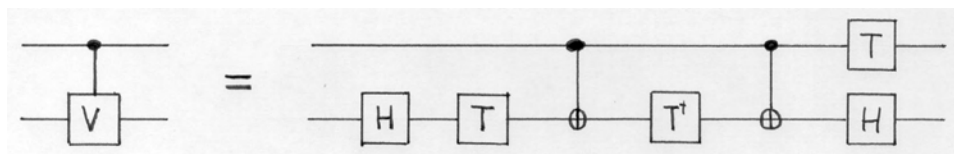
Aus $S = T^2$ und $T = e^{i\pi/4}XT^\dagger X$ folgt

$$V = e^{i\pi/4} \underbrace{H}_{=A} \cdot X \cdot \underbrace{T^\dagger}_{=B} \cdot X \cdot \underbrace{TH}_{=C}, \quad ABC = H \cdot T^\dagger \cdot TH = H^2 = I.$$

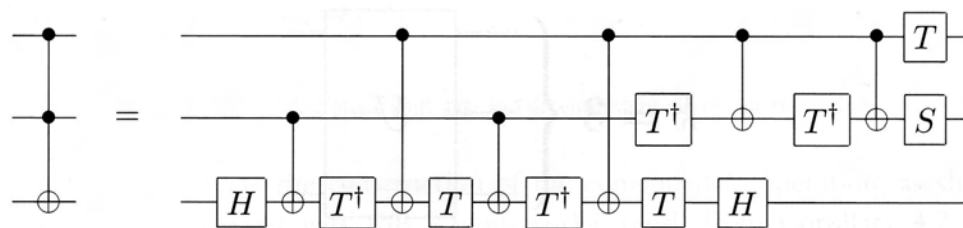
(2.7-5) REDUKTION GESTEUERTER GATTER

Anwendung auf das TOFFOLI-Gatter $C^2(X)$ – Fortsetzung

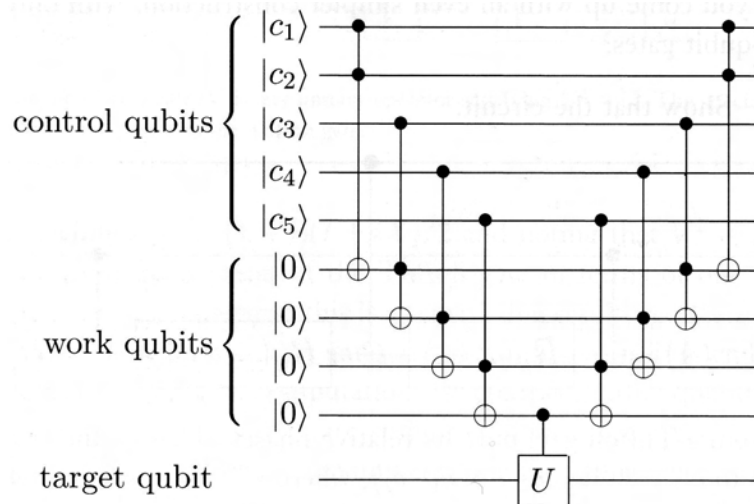
(2.7-2) \rightsquigarrow



(2.7-6) und etwas „Ausputzen“ \rightsquigarrow



Bemerkung: Analoge Reduktion *nicht* möglich für klassische reversible Schaltkreise.

4. Reduktion von $C^n(U)$ auf TOFFOLI und $C(U)$ Beispiel $n = 5$ 

Standardkonstruktion reversibler Schaltkreise inkl. „uncomputation“ der Hilfsqubits.

Aufwand: $O(n)$ Gatter

(2.8) ZWEI-LEVEL-GATTER SIND UNIVERSSELL

Satz. (Reck/Zeilinger/Bernstein/Bertani 1994)

Unitäre Gatter auf zwei Leveln sind universell.

D.h., jedes unitäre $U \in M_2^{\otimes n}$ läßt sich zerlegen als

$$U = U_1 \cdot \dots \cdot U_q, \quad q = 2^{n-1}(2^n - 1),$$

U_j wirkt nur auf zwei Komponenten der Rechenbasis nicht-trivial.

Beweis.

q Givens-Rotationen $U_1^\dagger, \dots, U_q^\dagger$ bringen U auf obere Dreiecksgestalt mit positiver Diagonale (QR-Zerlegung der Numerischen Mathematik...):

$$U_q^\dagger \cdot \dots \cdot U_1^\dagger \cdot U = R, \quad \text{diag}(R) \geq 0.$$

U unitär $\Leftrightarrow R$ unitär, also wegen seiner Struktur $R = I$.

Problem des Universalitätssatzes (2.8)

Komponenten verschiedener Qubits werden verknüpft.

Satz. (DiVincenzo 1995)

Jedes unitäre $U \in M_2^{\otimes n}$, welches nur auf zwei Komponenten der Rechenbasis nicht-trivial wirkt, läßt sich durch CNOT- und I-Qubit-Gatter realisieren.

Also sind CNOT- und I-Qubit-Gatter universell.

Beweis.

Die zwei Basisvektoren, auf denen Hülle U nicht-trivial wie $\tilde{U} \in M_2$ wirkt, seien

$$|s\rangle = |s_1 \dots s_n\rangle, \quad |t\rangle = |t_1 \dots t_n\rangle.$$

Beweis – Fortsetzung.

Hilfsmittel: **Gray-Code** zur Verbindung von s und t

- Sequenz $\{g_0, \dots, g_m\}$ von Binärzahlen, $g_0 = s$, $g_m = t$, so daß g_j und g_{j+1} in genau einer Binärstelle differieren, $m \leq n$.

Idee zur Implementierung von U

1. $|g_0\rangle \leftrightarrow |g_1\rangle \leftrightarrow \dots \leftrightarrow |g_{m-1}\rangle$
2. gesteuertes \tilde{U} auf dem Qubit, welches dem Bit entspricht, an dem g_{m-1} und $g_m = t$ differieren
3. $|g_{m-1}\rangle \leftrightarrow |g_{m-2}\rangle \leftrightarrow \dots \leftrightarrow |g_0\rangle$

Alle anderen Basisvektoren bleiben jeweils *unverändert*.

Beweis – Fortsetzung.

Implementierung von $|g_\mu\rangle \leftrightarrow |g_{\mu+1}\rangle$

g_μ unterscheide sich von $g_{\mu+1}$ genau im k -ten Bit,

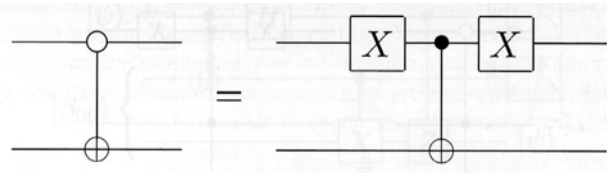
$$|x_1 \dots x_n\rangle \mapsto \begin{cases} |x_1 \dots x_{k-1} \bar{x}_k x_{k+1} \dots x_n\rangle & \text{falls } x_j = (g_\mu)_j, j \neq k, \\ |x_1 \dots x_n\rangle & \text{sonst.} \end{cases}$$

\curvearrowright mehrfach gesteuertes X , nach (2.7) realisierbar durch:

Gatter CNOT, H, T und X .

Bemerkung

X -Gatter wird benötigt, um Abfrage auf 0 statt 1 zu erlauben,



Beweis – Fortsetzung.

Implementierung von \tilde{U}

g_{m-1} unterscheide sich von g_m genau im k -ten Bit,

$$|x_1 \dots x_n\rangle \mapsto \begin{cases} |x_1 \dots x_{k-1} \tilde{U}x_k x_{k+1} \dots x_n\rangle & \text{falls } x_j = (g_m)_j, j \neq k, \\ |x_1 \dots x_n\rangle & \text{sonst.} \end{cases}$$

\curvearrowright mehrfach gesteuertes \tilde{U} , nach (2.7) realisierbar durch:

Gatter V , V^\dagger , CNOT, H, T und X ,

wobei $V^2 = U$ zu wählen ist.

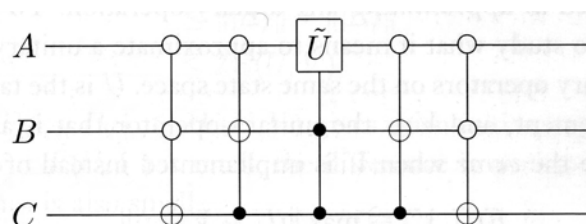
*Beispiel*Unitäre Matrix in $M_2^{\otimes 3}$,

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}, \quad \tilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}.$$

Wirkt nicht-trivial nur auf den Basisvektoren $|000\rangle$ und $|111\rangle$.*Beispiel – Fortsetzung:*

Gray-Code

A	B	C
0	0	0
0	0	1
0	1	1
1	1	1

Schaltkreis für \tilde{U} 

Zusammenfassung

für unitäres $U \in M_2^{\otimes n}$ auf n Qubits i.a.

- Zerlegung in 2-Level-Gatter: $O(4^n)$ Gatter
- Gray-Code hat Länge $O(n)$
- mehrfach gesteuertes X und \tilde{U} benötigt $O(n)$ Gatter

Abschätzung der Komplexität

$$\#\text{Gatter des Typs CNOT oder I-Qubit-Gatter} = O(n^2 \cdot 4^n)$$

(2.10) DISKRETE MENGE (FAST) UNIVERSELLER GATTER

Frage: Gibt es endliche Zahl universeller Gatter?

Antwort

- *nein*, da I-Qubit-Gatter überabzählbar...
- *ja*, wenn wir ϵ -Approximationen V zulassen, ϵ beliebig klein,

$$\|U - V\|_2 \leq \epsilon,$$

Wir sprechen dann von **Fast-Universalität**.

Satz. (Boykin/Mor/Pulver/Roychowdhury/Vatan 1999)

Die Gatter CNOT, H und T sind fast-universell.

Approximationsfehler: $E(U, V) = \|U - V\|_2.$

Lemma.

- Für Sequenzen von Quantengattern gilt

$$E(U_m U_{m-1} \dots U_1, V_m V_{m-1} \dots V_1) \leq \sum_{j=1}^m E(U_j, V_j).$$

- Sei ρ Dichtematrix.

Die Anwendung der unitären Operatoren U bzw. V liefert Zustände $\rho_U = U\rho U^\dagger$ und $\rho_V = V\rho V^\dagger$.

Für die Wahrscheinlichkeiten des Ereignis P , P ON-Projektion, gilt

$$|\operatorname{tr}(\rho_U P) - \operatorname{tr}(\rho_V P)| \leq 2E(U, V).$$

Beweis.

Da ρ Dichtematrix ist, gilt

$$\begin{aligned} |\operatorname{tr}(\rho_U P) - \operatorname{tr}(\rho_V P)| &= |\operatorname{tr}(\rho U^\dagger P U) - \operatorname{tr}(\rho V^\dagger P V)| \\ &= |\operatorname{tr}(\rho U^\dagger P (U - V)) - \operatorname{tr}(\rho (V^\dagger - U^\dagger) P V)| \\ &\leq |\operatorname{tr}(\rho U^\dagger P (U - V))| + |\operatorname{tr}(\rho (V^\dagger - U^\dagger) P V)| \\ &\leq \|U^\dagger P (U - V)\|_2 + \|(V^\dagger - U^\dagger) P V\|_2 \\ &\leq \|U - V\|_2 + \|V^\dagger - U^\dagger\|_2 = 2E(U, V). \end{aligned}$$

Summenformel → Übung.

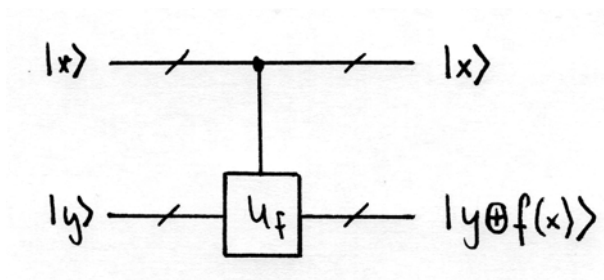
Reversible Standardrealisierung (2.3-8) von $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$

$$(x, y) \mapsto (x, y \oplus f(x)).$$

Implementierung des reversiblen Schaltkreises durch Quantengatter liefert bei gleicher Komplexität unitären Operator

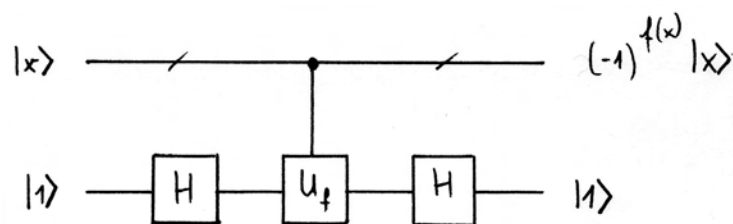
$$U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle.$$

Schaltkreis-Symbol (f-gesteuertes NOT)



Alternative für Boole'sche Abbildungen $f : \{0, 1\}^n \rightarrow \{0, 1\}$

Schaltkreis (f-gesteuerte Phase)



Kurz, ohne Ancilla,

$$|x\rangle \mapsto (-1)^{f(x)} |x\rangle.$$

Beweis. $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ und

$$\begin{aligned} (|x\rangle|0\rangle - |x\rangle|1\rangle)/\sqrt{2} &\mapsto (|x\rangle|f(x)\rangle - |x\rangle|\neg f(x)\rangle)/\sqrt{2} = \\ &(-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle)/\sqrt{2}. \end{aligned}$$

Uniforme Familie $\{Q_n\}_n$ von Quantenschaltkreisen

(Klassische) Turing-Maschine liefert $n \mapsto Q_n$ in polynomieller Laufzeit (Yao 1993)

Komplexitätsklassen für (klassische) Entscheidungsprobleme

- **QP**: # Quantengatter = Polynom(n).
Messung \curvearrowright Entscheidung mit 100%-Wahrscheinlichkeit korrekt.
- **BQP**: # Quantengatter = Polynom(n).
Messung \curvearrowright Entscheidung mit Wahrscheinlichkeit $\geq 75\%$ korrekt.

Chernoff'sche Schranke: m -fache Wiederholung und „Mehrheitsentscheid“

$$\text{Irrtumswahrscheinlichkeit} \leq e^{-m/8}.$$

Frage: # Quantengatter?

- # CNOT- und I-Qubit-Gatter (Universalität (2.9-1))

oder

- # CNOT-, H und T-Gatter (Fast-Universalität (2.10-1))

Antwort: spielt keine Rolle für **BQP**...

In dieser Vorlesung: # CNOT- und I-Qubit-Gatter

Satz. (Bernstein/Vazirani 1997)

$$\mathbf{P} \subset \mathbf{BPP} \subset \mathbf{BQP} \subset \mathbf{PSPACE}.$$

Bemerkung. $\mathbf{P} \stackrel{?}{=} \mathbf{PSPACE}$ ist weiterhin noch völlig offen \curvearrowright

$$\mathbf{BPP} \stackrel{?}{=} \mathbf{BQP} \text{ ungeklärt.}$$

Beweisidee.

- **BPP** \subset **BQP** folgt aus der Realisierbarkeit des Toffoli-Gatters (2.7-8) und Standardrealisierung (2.12-1).
- **BQP** \subset **PSPACE**:
Quantencomputer Q_n werde im Zustand $|0\rangle$ gestartet, führt Gatter $U_1, \dots, U_{p(n)}$ aus. Wahrscheinlichkeit für n -Qubit Basisvektor $|y\rangle$ nach Messung zum Schluß:

$$|\langle y | U_{p(n)} \dots U_2 U_1 | 0 \rangle|^2.$$

Jede dieser 2^n Zahlen läßt sich mit polynomielltem Speicherplatz mit hoher Genauigkeit klassisch berechnen.

Beweisidee – Fortsetzung.

Die Basisrelation $\sum_{x=0}^{2^n-1} |x\rangle \langle x| = I$ liefert (diskretes Feynman'sches Wegintegral...)

$$\begin{aligned} \langle y | U_{p(n)} \dots U_2 U_1 | 0 \rangle &= \\ \sum_{x_1, \dots, x_{p(n)-1}} \langle y | U_{p(n)} | x_{p(n)-1} \rangle &\langle x_{p(n)-1} | U_{p(n)-1} \dots U_2 | x_1 \rangle \langle x_1 | U_1 | 0 \rangle. \end{aligned}$$

Jeder Faktor $\langle x_j | U_j | x_{j-1} \rangle$ ist für CNOT-Gatter und I-Qubit-Gatter bei hoher Genauigkeit mit polynomielltem Speicherplatz berechenbar und kann nach Multiplikation gelöscht werden. Buchführung von Produkt und Summe erfordert ganze zwei Speicherplätze.

Rechenzeit dieser klassischen Simulation ist *exponentiell* in n .

Problemstellung

Gegeben Boole'sches Orakel bzw. *Black-Box* $f : \{0, 1\}^n \rightarrow \{0, 1\}$ mit

- entweder: f ist *ausgewogen* (d.h. gleich häufig 0 oder 1)
- oder: f ist *konstant*.

Orakel darf als Quanten-Black-Box befragt werden, d.h.

$$U_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$$

wird wie ein elementares Gatter behandelt.

Entscheidungsproblem DJ: Ist f ausgewogen oder konstant?

Klassischer deterministischer Algorithmus

In irgendeiner Reihenfolge verschiedene Anfragen x an das Orakel f :

- sobald zwei verschiedene Antworten: „ausgewogen“,
- nach $2^{n-1} + 1$ gleichen Antworten: „konstant“.

Denn: zu jeder Reihenfolge existiert ausgewogene Funktion, so daß die ersten 2^{n-1} Antworten gleich ausfallen...

Klassische Komplexität *relativ* zum Orakel f ist also *exponentiell*,

$$DJ \notin \mathbf{P}^f.$$

Klassischer probabilistischer Algorithmus

In zufälliger Reihenfolge verschiedene Anfragen x an das Orakel f :

- sobald zwei verschiedene Antworten: „ausgewogen“,
- nach k gleichen Antworten: „konstant“.

Irrtumswahrscheinlichkeit im zweiten Fall, falls f doch ausgewogen:

$$p_k = \binom{2^{n-1}}{k} / \binom{2^n}{k} \leq 2^{-k}$$

Bereits $k = 2$ liefert

$$DJ \in \mathbf{BPP}^f.$$

Für $k = 67$ ist schon $p \leq 10^{-20}$.

Idee des Quanten-Algorithmus

Quanten-Parallelität

$$U_f \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle,$$

d.h. eine einzige Befragung des Quanten-Orakels kodiert *alle* klassischen Antworten.

Fragen:

- Wie präpariert man den reinen Zustand $\psi_{\text{all}} = \sum_x |x\rangle / \sqrt{2^n}$?
- Wie mißt man die gesuchte Antwort aus $U_f \psi_{\text{all}}$?

Antwort: Hadamard-Transformation...

Lemma.

Für eine n -Bit-Zahl $x = x_1 \dots x_n$ gilt

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle.$$

Dabei fassen wir jede Zahl $0 \leq z \leq 2^n - 1$ ebenfalls als n -Bit-Zahl $z = z_1 \dots z_n$ auf und definieren das bitweise \mathbb{Z}_2 -„Skalar“-produkt:

$$x \cdot z = x_1 z_1 \oplus \dots \oplus x_n z_n.$$

Beweis.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, d.h. für $n = 1$:

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{z=0}^1 (-1)^{xz} |z\rangle.$$

Beweis – Fortsetzung.

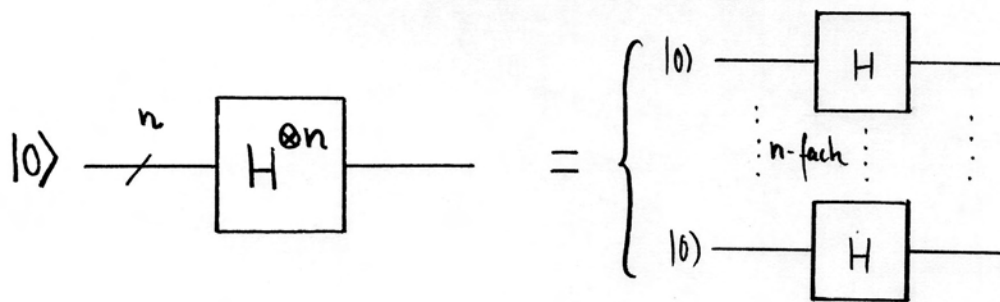
Nach den Rechenregeln für Tensorprodukte gilt daher

$$\begin{aligned} H^{\otimes n}|x\rangle &= H^{\otimes n}|x_1 \dots x_n\rangle = H|x_1\rangle \otimes \dots \otimes H|x_n\rangle \\ &= \left(\frac{1}{\sqrt{2}} \sum_{z_1=0}^1 (-1)^{x_1 z_1} |z_1\rangle \right) \otimes \dots \otimes \left(\frac{1}{\sqrt{2}} \sum_{z_n=0}^1 (-1)^{x_n z_n} |z_n\rangle \right) \\ &= \left(\frac{1}{\sqrt{2}} \right)^n \sum_{z_1=0}^1 \dots \sum_{z_n=0}^1 (-1)^{x_1 z_1} \dots (-1)^{x_n z_n} \cdot |z_1 \dots z_n\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle. \end{aligned}$$

Korollar 1.

$$\psi_{\text{all}} = H^{\otimes n}|0\rangle.$$

Fazit: Präparation von ψ_{all} durch den n -Qubit-Schaltkreis



Aus dem Lemma folgt ferner

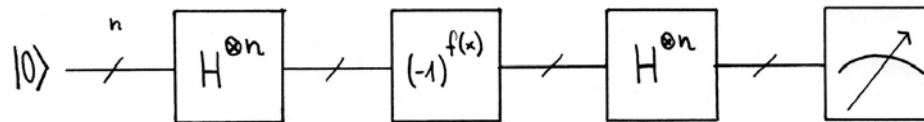
$$\begin{aligned} H^{\otimes n} U_f \psi_{\text{all}} &= H^{\otimes n} \left(\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \right) \\ &= \sum_z \left(\frac{1}{2^n} \sum_x (-1)^{f(x)} (-1)^{x \cdot z} \right) |z\rangle. \end{aligned}$$

Koeffizient vor Basisvektor $|0\rangle$ lautet

$$\frac{1}{2^n} \sum_x (-1)^{f(x)} = \begin{cases} 0, & \text{falls } f \text{ ausgewogen,} \\ \pm 1, & \text{falls } f \text{ konstant.} \end{cases}$$

Fazit: Typ von f durch Messung sicher unterscheidbar.

Der Quanten-Algorithmus von David Deutsch und Richard Jozsa (1992)



Ergebnis der Messung sei n -Bit-Zahl x .

- $x \neq 0$: f ist ausgewogen
- $x = 0$: f ist konstant

Fazit

eine *einzig*e Befragung des Quanten-Orakels reicht;
relativ zum Orakel des Deutsch-Jozsa-Problems gilt

$$\text{DJ} \in \mathbf{QP}^f, \quad \mathbf{P}^f \neq \mathbf{QP}^f.$$

Realisierung im MATLAB-Paket der Vorlesung

```
psi = Ket(dec2bin(0,n));
psi = Hadamard(psi);
psi = FControlledPhase(psi,'DJOracle',type);
psi = Hadamard(psi);
[dummy,res] = Measure(psi,0,n,0);
switch res
case 0
    disp('Result: constant function')
otherwise
    disp('Result: balanced function')
end
```

Experimente

basierend auf NMR-Technologie (nuclear-magnetic-resonance):

- $n = 1$ Jones/Mosca (1998)
- $n = 1$ Chuang/Vandersypen/Zhou/Leung/Lloyd (1998)
- $n = 2$ Linden/Barjat/Freeman (1998)
- $n = 4$ (partiell) Marx/Fahmy/Myers/Bermel/Glaser (1999) mit BOC-($^{13}\text{C}_2$ - ^{15}N - $^2\text{D}_2^\alpha$ -Glyzin)-Fluorid
- $n = 3$ Collins/Kim/Holton/Sierzputowska-Gracz/Stejskal (2001)

(3.2-1) DER ALGORITHMUS VON SIMON (1994)

Problemstellung

Gegeben sei Orakel $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ mit

- es gibt Periode $0 \neq a \in \mathbb{Z}_2^n$, so daß für $x \neq y$

$$f(x) = f(y) \iff x = y \oplus a.$$

Orakel darf als Quanten-Black-Box befragt werden, d.h.

$$U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$$

wird wie ein elementares Gatter behandelt.

Aufgabe: Berechne die Periode a .

Zugehöriges Entscheidungsproblem SIMON

Es sei entweder f bijektiv ($a = 0$) oder wie oben. Was ist der Fall?

Klassischer probabilistischer Algorithmus

Jeder Algorithmus richtet k zufällige, verschiedene Anfragen an das Orakel f

- falls zwei Antworten gleich $\leadsto a$
- sonst: „failed“

Lemma.

Für $k \leq 2^{n-1} + 1$ ist die Erfolgswahrscheinlichkeit $p_k \leq k^2/2^n$.

Beweis.

Bedingte Wahrscheinlichkeit einer erfolgreichen k ten Anfrage nach $k-1$ erfolglosen ist

$$(k-1)/(2^n - (k-1)),$$

da genau $k-1$ von $2^n - (k-1)$ verbleibenden Anfragen erfolgreich sind.

Es folgt die Rekursion

$$p_k = p_{k-1} + \frac{k-1}{2^n - (k-1)}(1 - p_{k-1}) \leq p_{k-1} + \frac{k-1}{2^n - (k-1)}.$$

Mit $p_1 = 0$ folgt so

$$p_k \leq \sum_{j=1}^k \frac{j-1}{2^n - (j-1)} \leq \sum_{j=1}^k \frac{j-1}{2^n - (k-1)} \leq \frac{k^2/2}{2^n - 2^{n-1}} = \frac{k^2}{2^n}.$$

Fazit

Selbst für *exponentiell* viele Anfragen

$$k = 2^{n/4}$$

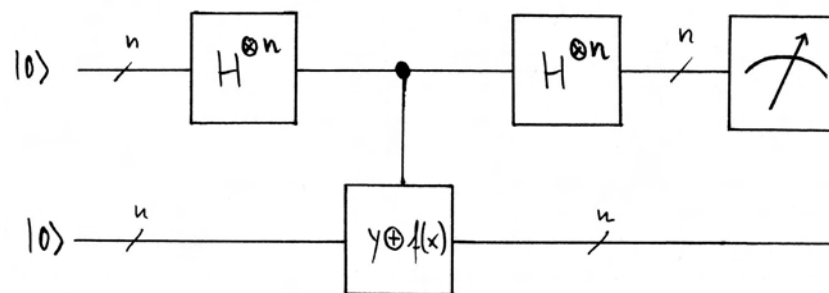
ist die Erfolgswahrscheinlichkeit noch immer *exponentiell klein*

$$p \leq 2^{-n/2}.$$

Dies überträgt sich auf das Entscheidungsproblem, also gilt relativ zum Orakel f

$$\text{SIMON} \notin \mathbf{BPP}^f.$$

Der Quantenalgorithmus von Daniel Simon (1994)



Lemma.

Messung des ersten Registers ergibt mit je gleicher Wahrscheinlichkeit $2^{-(n-1)}$ eine der 2^{n-1} Zahlen $y \in \mathbb{Z}_2^n$, für die

$$a \cdot y = 0.$$

Beweis.

Zu $w \in R = \text{range}(f)$ wählen wir x_w mit $f(x_w) = w$.

Der Quantenzustand des Simon'schen Schaltkreises vor Messung ist

$$\begin{aligned}
 & (H^{\otimes n} \otimes I) U_f (\psi_{\text{all}} \otimes |0\rangle) \\
 &= (H^{\otimes n} \otimes I) \left(\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle \right) = \frac{1}{2^n} \sum_{x,y} (-1)^{x \cdot y} |y\rangle |f(x)\rangle \\
 &= \frac{1}{2^n} \sum_{w \in R, y} \left((-1)^{x_w \cdot y} + (-1)^{(x_w \oplus a) \cdot y} \right) |y\rangle |w\rangle \\
 &= \frac{1}{2^n} \sum_{w \in R, y} (-1)^{x_w \cdot y} (1 + (-1)^{a \cdot y}) |y\rangle |w\rangle \\
 &= \frac{1}{2^{n-1}} \sum_{w \in R} \sum_{a \cdot y = 0} (-1)^{x_w \cdot y} |y\rangle |w\rangle.
 \end{aligned}$$

(3.2-7) DER ALGORITHMUS VON SIMON (1994)

Beweis – Fortsetzung.

Nach dem *Prinzip der impliziten Messung* (2.4-8) o.E. Messung auch des zweiten Registers:

- Wahrscheinlichkeit $2^{-2(n-1)}$ für Ergebnis (y, w) mit
 $a \cdot y = 0$ und $w \in R$.

$$\#R = 2^{n-1}$$

Daher Messung des ersten Registers allein:

- Wahrscheinlichkeit $2^{-(n-1)}$ für Ergebnis y mit $a \cdot y = 0$.

Realisierung im MATLAB-Paket der Vorlesung

```

psi = Ket(dec2bin(0,n));
ancilla = 0;
psi = Hadamard(psi);
psi = FControlledNot(psi,ancilla,'SimonOracle',[ ]);
psi = Measure(psi,n,n,0);
psi = Hadamard(psi);
[dummy,y] = Measure(psi,0,n,0);

```

Frage: Schön und gut, aber wie bekommt man a ?

Idee einer klassische Nachbearbeitung

- $0 \neq a \in \mathbb{Z}_2^n$ eindeutig bestimmt durch über \mathbb{Z}_2 linear unabhängige Vektoren $y_1, \dots, y_{n-1} \in \mathbb{Z}_2^n$ mit

$$a \cdot y_j = 0 \quad j = 1 : n - 1.$$

- wiederholte Anwendung des Algorithmus von Simon bis linear unabhängige Menge von y_j vorliegt

Erwartete Anzahl der Wiederholungen: $O(n)$...

Alternative

$(n - 1)$ -fache Ausführung des Algorithmus von Simon $\curvearrowright y_1, \dots, y_{n-1}$

- y_1, \dots, y_{n-1} linear unabhängig $\curvearrowright \alpha$
- sonst: „failed“

Erfolgswahrscheinlichkeit

$$\begin{aligned}
 p &= \underbrace{\left(1 - \frac{2^0}{2^{n-1}}\right)}_{W.: y_1 \notin \text{lin}\{0\}} \cdot \underbrace{\left(1 - \frac{2^1}{2^{n-1}}\right)}_{W.: y_2 \notin \text{lin}\{y_1\}} \cdot \dots \cdot \underbrace{\left(1 - \frac{2^{n-2}}{2^{n-1}}\right)}_{W.: y_{n-1} \notin \text{lin}\{y_1, \dots, y_{n-2}\}} \\
 &= \prod_{k=1}^{n-1} (1 - 2^{-k}) > \prod_{k=1}^{\infty} (1 - 2^{-k}) = 0.2887 \dots > 1/4.
 \end{aligned}$$

Fazit

Relativ zum Orakel f gilt also

$$\text{SIMON} \in \mathbf{BQP}^f$$

und daher

$$\mathbf{BPP}^f \neq \mathbf{BQP}^f.$$

Bemerkung

Verfeinerter Algorithmus (Brassard/Høyer 1997) liefert Erfolg mit 100%,

$$\text{SIMON} \in \mathbf{QP}^f.$$

Achtung

Dies ist *Hinweis*, aber *kein Beweis*, daß Quantencomputer für gewisse Probleme exponentiell schneller sind als klassische probabilistische Computer

Begründung

Läßt sich eine α -periodische Funktion f mit einem polynomiellen Schaltkreis realisieren, so könnte α „von innen“ heraus, durch Studium des Schaltkreises effizient ermittelt werden, nicht nur durch Auswertung des „Orakels“ $x \mapsto f(x)$...

Bedeutung des Algorithmus von Simon...

...Inspiration von Peter Shor zur Primfaktorisierung

Problemstellung: (Boneh/Lipton 1995, Jozsa 1997)

Gegeben

- endliche abelsche Gruppe $(G, +)$
- $K < G$ Untergruppe
- Orakel $f : G \rightarrow X$ mit

$$f(x) = f(y) \iff x - y \in K$$

Orakel darf als Quanten-Black-Box befragt werden.

Aufgabe: Bestimme die Untergruppe K .

Beispiele

- (a) Proto-Problem von Shor zur Vorbereitung der Primfaktorzerlegung
- $G = \mathbb{Z}_N = \{0, 1, \dots, N - 1\}$ zyklische Gruppe der Addition modulo N
 - $K = \{0, r, 2r, \dots\}$ für $r \mid N$
 - $f : G \rightarrow X$ ist r -periodisch
 - **Gesucht:** Periode r
- (b) Das Problem von Simon:
- $G = (\mathbb{Z}_2^n, \oplus)$
 - $K = \{0, a\}$ mit $a \neq 0$
 - $f : G \rightarrow X$ ist a -periodisch
 - **Gesucht:** Periode a
- (c) Diskreter Logarithmus \curvearrowright später
(ein weiteres wichtiges Problem der Kryptographie...)

*Definition.***Charakter auf G**

$$\chi : (G, +) \rightarrow (\mathbb{C}^\times, \cdot) \quad \text{Homomorphismus.}$$

Operation

$$(\chi_1 \cdot \chi_2)(g) = \chi_1(g) \cdot \chi_2(g)$$

macht die Menge G^* aller Charaktere auf G zu einer abelschen Gruppe mit Einselement

$$\chi_0 \equiv 1.$$

G^* heißt **Charaktergruppe** oder zu G **duale Gruppe**.

Beobachtung

Für $g \in G$ gilt nach dem Satz von Lagrange

$$|G|g = 0 \quad \Leftrightarrow \quad \chi(g)^{|G|} = \chi(0) = 1.$$

Also ist $\chi(g)$ eine $|G|$.te Einheitswurzel in \mathbb{C} , insbesondere ist

$$|\chi(g)| = 1$$

und damit

$$\chi^{-1} = \bar{\chi}.$$

Lemma. Für $G = G_1 \times G_2$ gilt $G^* = G_1^* \times G_2^*$.

Beweis.

Ein kanonischer Isomorphismus $G_1^* \times G_2^* \rightarrow G^*$ wird vermöge

$$(\chi_1, \chi_2)(g_1, g_2) = \chi_1(g_1) \cdot \chi_2(g_2)$$

hergestellt.

Beispiele

$$(a) \quad G = \mathbb{Z}_N: \quad \chi_k(j) = e^{\frac{2\pi i}{N}kj} \quad k, j = 0 : N - 1.$$

$$(b) \quad G = \mathbb{Z}_2: \quad \chi_x(y) = e^{\frac{2\pi i}{2}xy} = (-1)^{xy} \quad x, y = 0, 1.$$

$$(c) \quad G = \mathbb{Z}_2^n = \underbrace{\mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_{n\text{-fach}}: \quad \text{wegen Lemma (4.2-3) gilt}$$

$$\chi_x(y) = (-1)^{x_1 y_1} \cdot \dots \cdot (-1)^{x_n y_n} = (-1)^{x \cdot y}.$$

Dabei verstehen wir $x = x_1 \dots x_n, y = y_1 \dots y_n$ als n -Bit-Binärzahlen.

Satz. Es gilt die Isomorphie $(G, +) \simeq (G^*, \cdot)$.

Beweisidee.

(4.2-4) zeigt die Behauptung für $G = \mathbb{Z}_N$. Nach dem Struktursatz für endliche abelsche Gruppen gilt

$$G \simeq \mathbb{Z}_{N_1} \times \dots \times \mathbb{Z}_{N_k}$$

für gewisse Zahlen N_1, \dots, N_k .

Bemerkung. Ein solcher Isomorphismus $g \mapsto \chi_g$, wobei natürlich

$$\chi_{g+g'} = \chi_g \cdot \chi_{g'},$$

sei ab jetzt ausgezeichnet. In den Beispielen (4.2-4) war er *explizit*.

Definition.

Sei $K < G$. Die **Annihilatorgruppe** von K ist

$$K^\circ = \{g \in G : \chi_g|_K = 1\}.$$

Lemma. (Charakterisierung des Annihilators)

$$\sum_{h \in K} \chi_g(h) = \begin{cases} |K| & \text{falls } g \in K^\circ, \\ 0 & \text{sonst.} \end{cases}$$

Beweis.

Setze

$$\alpha = \sum_{h \in K} \chi_g(h).$$

Für beliebiges festes $h' \in K$ durchläuft mit h auch $h' + h$ ganz $K \Leftrightarrow$

$$\alpha = \sum_{h \in K} \chi_g(h' + h) = \chi_g(h') \cdot \alpha.$$

Falls $\alpha \neq 0$, so ist $\chi_g(h') = 1$. Da $h' \in K$ beliebig,

$$\chi_g|_K = 1 \quad \Leftrightarrow \quad g \in K^\circ.$$

Korollar 1.

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{falls } \chi = \chi_0, \\ 0 & \text{sonst.} \end{cases}$$

Korollar 2. Orthogonalität der Charaktere $G^* \subset \mathbb{C}^{|G|}$

$$\langle \chi_g, \chi_{g'} \rangle = \sum_{h \in G} \bar{\chi}_g(h) \chi_{g'}(h) = \begin{cases} |G| & \text{falls } g = g', \\ 0 & \text{sonst.} \end{cases}$$

Beweis. $\bar{\chi}_g \cdot \chi_{g'} = \chi_{g'-g}$. Korollar 1 liefert Behauptung.

(4.4-1) FOURIER-TRANSFORMATION AUF GRUPPEN

Funktion $f : G \rightarrow \mathbb{C}$, d.h. $f \in \mathbb{C}^{|G|}$.

Fourier-Transformation

$$\hat{f} = \mathcal{F}f : G \rightarrow \mathbb{C}$$

fasst f als Koeffizientenvektor für die Charaktere auf:

$$\hat{f}(g) = \frac{1}{\sqrt{|G|}} \sum_{h \in G} \bar{\chi}_h(g) f(h).$$

Basisdarstellung

$$\mathcal{F}|h\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \bar{\chi}_h(g) |g\rangle.$$

Aus dieser Basisdarstellung folgt sofort

$$\mathcal{F}^\dagger |h\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \chi_g(h) |g\rangle.$$

Satz. Die Fourier-Transformation $\mathcal{F} : \mathbb{C}^{|G|} \rightarrow \mathbb{C}^{|G|}$ ist *unitär*, d.h.

$$\mathcal{F}^\dagger \mathcal{F} = \mathcal{F} \mathcal{F}^\dagger = I.$$

Bemerkung.

Es gibt also Quantenschaltkreise zur Realisierung von \mathcal{F} .

Ihre *Konstruktion* und *Effizienz* wird später ein Thema sein.

Beweis.

Es gilt

$$\begin{aligned} \mathcal{F}^\dagger \mathcal{F} |h\rangle &= \mathcal{F}^\dagger \frac{1}{\sqrt{|G|}} \sum_{g \in G} \bar{\chi}_h(g) |g\rangle \\ &= \frac{1}{|G|} \sum_{h', g \in G} \chi_{h'}(g) \bar{\chi}_h(g) |h'\rangle \\ &= \frac{1}{|G|} \sum_{h' \in G} |G| \delta_{h'h} |h'\rangle = |h\rangle. \end{aligned}$$

Beim Übergang zur letzten Zeile wurde die Orthogonalität (4.3-3) der Charaktere genutzt.

Beispiele

(a) $G = \mathbb{Z}_2^n$, $f \in \mathbb{C}^{2^n} = \mathbb{H}_2^{\otimes n}$.

Aus $\chi_x(y) = (-1)^{x \cdot y}$ folgt mit Lemma (3.1-5)

$$\mathcal{F}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle = \mathbb{H}^{\otimes n} |x\rangle.$$

Also ist

$$\mathcal{F} = \mathcal{F}^\dagger = \mathbb{H}^{\otimes n}$$

das n -fache Tensorprodukt der *Hadamard-Transformation*.

Beispiele

(b) $G = \mathbb{Z}_N$, $f \in \mathbb{C}^N$.

Aus $\chi_k(j) = e^{\frac{2\pi i}{N}kj}$ folgt

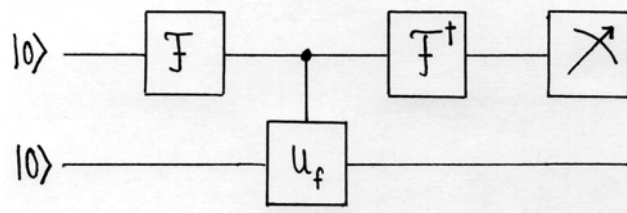
$$\hat{f}_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-\frac{2\pi i}{N}kj} f_j.$$

Dies ist die klassische *diskrete Fourier-Transformation*.

Basisdarstellung: Für $j = 0, \dots, N-1$ gilt

$$\mathcal{F}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-\frac{2\pi i}{N}kj} |k\rangle.$$

Quantenalgorithmus nach Richard Jozsa (1997)

**Satz.**

Messung des ersten Registers ergibt mit je gleicher Wahrscheinlichkeit $|K|/|G|$ eines der $|G|/|K|$ Elemente

$$g \in K^\circ.$$

Beweis.

Zunächst gilt

$$\mathcal{F}|0\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle = \psi_{\text{all}}$$

und daher

$$U_f(\psi_{\text{all}} \otimes |0\rangle) = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle.$$

Wir wählen Repräsentantensystem $R \subset G$ für die Restklassen G/K , d.h. jedes g läßt sich *eindeutig* zerlegen als

$$g = h + h' \quad h \in R, h' \in K.$$

Beweis – Fortsetzung.

Da f konstant auf jeder Restklasse ist, ist der Zustand vor der Messung wegen der Charakterisierung von K° in Lemma (4.3-1)

$$\begin{aligned} (\mathcal{F}^\dagger \otimes I)U_f(\psi_{\text{all}} \otimes |0\rangle) &= \frac{1}{|G|} \sum_{g',g \in G} \chi_{g'}(g) |g'\rangle |f(g)\rangle \\ &= \frac{1}{|G|} \sum_{g' \in G, h \in R} \chi_{g'}(h) \left(\sum_{h' \in K} \chi_{g'}(h') \right) |g'\rangle |f(h)\rangle \\ &= \frac{|K|}{|G|} \sum_{g' \in K^\circ, h \in R} \chi_{g'}(h) |g'\rangle |f(h)\rangle. \end{aligned}$$

Beweis – Fortsetzung.

Nach dem *Prinzip der impliziten Messung* (2.4-8) o.E. Messung auch des zweiten Registers:

$$|\chi_{g'}(h)|^2 = 1 \Leftrightarrow$$

- Wahrscheinlichkeit $|K|^2/|G|^2$ für Ergebnis $(g', f(h))$ mit

$$g' \in K^\circ \text{ und } h \in R.$$

$\#R = |G|/|K| \Leftrightarrow$ Messung des ersten Registers allein:

- Wahrscheinlichkeit $|K|/|G|$ für Ergebnis $g' \in K^\circ$.

(a) *Problem von Simon*

$G = \mathbb{Z}_2^n$, $K = \{0, a\}$. Untergruppe K ist zyklisch, also

$$g \in K^\circ \iff \chi_g(a) = (-1)^{g \cdot a} = 1 \iff g \cdot a = 0.$$

Mit $\mathcal{F} = \mathcal{F}^\dagger = H^{\otimes n}$ sind also Algorithmus und Satz (4.5-1) gerade eine Wiederholung von (3.2-5).

Klassische Nachbearbeitung wie in (3.2-9/10).

(b) *Perioden-Problem*

$G = \mathbb{Z}_N$, $K = \{0, r, 2r, \dots, (s-1)r\}$ für $N = r \cdot s$. Untergruppe K ist auch hier zyklisch, also gilt

$$g \in K^\circ \iff \chi_g(r) = e^{\frac{2\pi i}{N} gr} = 1 \iff N | g \cdot r \iff s | g.$$

Demnach

$$K^\circ = \{0, s, 2s, \dots, (r-1)s\}.$$

Algorithmus (4.5-1) liefert also $j \cdot s$, wobei jedes $j = 0 : r-1$ mit gleicher Wahrscheinlichkeit $1/r$ auftritt.

Frage: Wie gelangt man zu s und damit zu $r = N/s$?

Klassische Nachbearbeitung des Perioden-Problems

- zwei Durchläufe von (4.5-1) $\leadsto j_1s, j_2s$
- $\hat{s} = \text{GGT}(j_1s, j_2s)$
- falls $\hat{s} \nmid N$: *failed*
- $\hat{r} = N/\hat{s}$
- falls $f(\hat{r}) \neq f(0)$: *failed*
- $r = \hat{r}$

Lemma. Wahrscheinlichkeit eines Mißerfolgs $< 40\%$.

Bemerkung. Also ist nach 102 Befragungen von f die Wahrscheinlichkeit eines Mißerfolgs $< 10^{-20}$.

Beweis.

Die Situation entspricht:

Wähle zufällig $j_1, j_2 \in \{0, \dots, r-1\}$. Erfolg, falls j_1, j_2 teilerfremd.

Hierfür ist die Wahrscheinlichkeit

$$\prod_{q \text{ prim}} \left(1 - \underbrace{P(q|j_1)}_{\text{W. für } q|j_1} \underbrace{P(q|j_2)}_{\leq 1/q} \right) \geq \prod_{q \text{ prim}} (1 - q^{-2})$$

$$= \frac{1}{\sum_{k=1}^{\infty} k^{-2}} = \frac{6}{\pi^2} > 0.6$$

- Implementierung der Fourier-Transformation \mathcal{F} für $G = \mathbb{Z}_N$, $N = 2^n$
Quantenschaltkreis mit polynomiellm Aufwand in $n = \#\text{Qubits}$
↪ Periodenermittlung in **BQP**^f
- Was tun, falls N keine Zweierpotenz?
- Was hat Periodenermittlung mit Primfaktorisation zu tun?
- Warum ist Primfaktorisation spannend?

Symmetrische Verfahren (Private-Key-Cryptosystems)



Design-Wunsch

Entschlüsselung *ohne* Kenntnis von K genauso schwer wie systematische Suche („brute force attack“) nach K im Schlüsselraum

Aufwand für Eve: k -Bit Schlüssel $K \rightsquigarrow O(2^k) = \text{exponentiell}$

Problem: sicherer Austausch des Schlüssels K vorab

Berühmte moderne Beispiele (block ciphers)

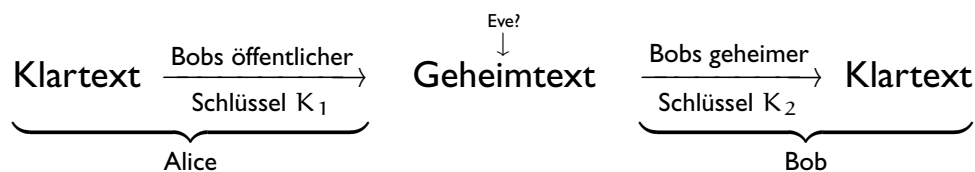
Name	Jahr	Schlüssellänge [Bits]	patentiert
DES	1977	56	nein (NIST)
Triple-DES	1979	112	nein
IDEA	1992	128	ja, bis 2011
AES (Rijndael)	2001	128, 192, 256	nein (NIST)

Sicherheit

John Gilmore (EFF), 1999: DES challenge III mit *brute force attack* „geknackt“ in 22h 15' auf 100 000 weltweit verteilten PCs

128 Bit-Schlüssel: Faktor $5 \cdot 10^{21}$ aufwendiger!

Asymmetrische Verfahren (Public-Key-Cryptosystems)



Diffie-Hellman 1976

Einwegfunktion $f : \text{Klartext} \mapsto \text{Geheimtext}$

- f injektiv, einfach auszuwerten (Komplexität **P**)
- f^{-1} extrem aufwendig (Komplexität **NP \ P** ?)

mit „Falltür“ (*trapdoor functions*)

- f^{-1} einfach auszuwerten bei Kenntnis von K_2 (Komplexität **P**)

Zur Praxis

- zur Rekonstruktion des geheimen Schlüssels K_2 für f^{-1} sind subexponentielle Algorithmen bekannt, d.h. leicht bessere Verfahren als „brute force“ \curvearrowright
Schlüssellängen asymmetrischer Verfahren deutlich *länger* als bei symmetrischen: > 512 Bits
- asymmetrische Verfahren *aufwendiger* (\approx Faktor 1000) als symmetrische \curvearrowright

Hybridverfahren

- asymmetrisch: Verschlüsselung eines zufälligen „Wegwerfsschlüssels“ K (session key)
- symmetrisch: Verschlüsselung des Klartexts mit K

A. Faktorisierungsproblem

Einwegfunktion = Multiplikation

$$f : \underbrace{(p, q)}_{\text{Primzahlen}} \mapsto \underbrace{n = p \cdot q}_{\text{RSA-Modul}}$$

- Bestimmung L -stelliger Primzahlen: Komplexität **P**
- Multiplikation: Komplexität **P**

aber

- Faktorisierung z. Zt. nur in subexponentieller Zeit
(*general number field sieve*, Pollard und Buhler/Pommerance ~ 1990)

$$\text{CPU-Zeit} \simeq \exp(1.9(\ln n)^{1/3}(\ln \ln n)^{2/3}).$$

Details Beispiel A

- Test einer Zahl p auf Primalität:
 - Monte-Carlo-Algorithmus (Rabin/Miller 1980):
Zertifikat für p nicht prim; p prim hingegen *nur* mit beliebig kleiner Irrtumswahrscheinlichkeit,

$$\text{CPU-Zeit} = O(\ln^2 p \ln \ln p \ln \ln \ln p).$$

- Las-Vegas-Algorithmus (Atkin/Morain 1993):
Zertifikate für p nicht prim *und* prim

$$\text{erwartete CPU-Zeit} = O(\text{Polynom}(\ln p)).$$

Details Beispiel A

- Multiplikation zweier ℓ -stelliger Zahlen nach Schönhage/Strassen 1971

$$\text{CPU-Zeit} = O(\ell \ln \ell \ln \ln \ell).$$

Beachte: $\ell = O(\ln n)$ in unserem Beispiel...

Bemerkung

Diese Einwegfunktion ist noch keine Falltür-Funktion...

...ist aber die „Mutter“ von Falltür-Funktionen.

Gleiches gilt für das nächste Beispiel.

B. Das Problem des diskreten Logarithmus

p Primzahl; g Primitivwurzel modulo p

Einwegfunktion = modulare Exponentiation

$$f: k \bmod (p-1) \mapsto g^k \bmod p.$$

- modulare Exponentiation: Komplexität **P**
- Primitivwurzel: Komplexität **P** für gewisse p

aber

- diskreter Logarithmus $g^k \mapsto k$ z. Zt. nur in subexponentieller Zeit (Gordon 1993)

$$\text{CPU-Zeit} \simeq \exp(O((\ln p)^{1/3} (\ln \ln p)^{2/3})).$$

Details Beispiel B

...zunächst etwas Zahlentheorie...

- $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}_n^\times = \{k \in \mathbb{Z}_n : \text{GGT}(k, n) = 1\}$
- $\#\mathbb{Z}_n^\times = \phi(n)$ Euler'sche ϕ -Funktion (Totient)
 - p prim: $\phi(p) = p - 1$
 - $n = p \cdot q$ RSA-Modul: $\phi(n) = (p - 1)(q - 1)$

- **Satz von Euler-Fermat**

$$a^{\phi(n)} = 1 \bmod n \quad \forall a \in \mathbb{Z}_n^\times$$

- **Satz von Lambert**

Für p prim ist \mathbb{Z}_p^\times zyklisch, d.h es gibt *Primitivwurzel* $g \in \mathbb{Z}_p^\times$, so daß

$$\mathbb{Z}_p^\times = \{g^k \bmod p : k = 0, \dots, p-2\}.$$

Details Beispiel B

Modulare Exponentiation $x = g^k \bmod n$

Algorithmus

```

k = kℓ ... k0 Binärdarstellung
x = gk0
for i = 1 : ℓ
    g = g2 mod n
    if ki then x = x · g mod n end if
end for

```

Aufwand: $\ell = O(\ln k)$, $k \leq \phi(n) \leq n$, d.h. wegen (5.2-3)

$$\text{CPU-Zeit} = O((\ln^2 n) (\ln \ln n) (\ln \ln \ln n)).$$

Mathematica: `x=PowerMod[g,k,n]`

(Rivest/Shamir/Adleman 1978)

Falltürfunktion

modulare Potenzfunktion (RSA-Funktion)

$$f : x \mapsto x^e \bmod n.$$

(n, e) Bobs öffentlicher Schlüssel, x Klartextblock

- $n = p \cdot q$ RSA-Modul
- f injektiv, falls e teilerfremd zu $\phi(n) = (p-1)(q-1)$

Falltür: Kenntnis der Faktorisierung von n .

Sicherheit: Jede z. Zt. bekannte effektive Dechiffrierung ist äquivalent zur Kenntnis der Faktorisierung von n .

Patentschutz: in den USA von 1983 bis 2000

Dechiffrierung

$$f^{-1} : y \mapsto y^d \bmod n$$

d Bobs geheimer Schlüssel, y Geheimtextblock

Satz. $d = e^{-1} \bmod \phi(n)$.

Beweis. Nach dem Satz von Euler gilt

$$y^d = x^{d \cdot e} = x^{1+j\phi(n)} = x \bmod n.$$

Bemerkungen

- d effektiv berechenbar mit Euklidischem Algorithmus bei Kenntnis von $\phi(n)$, d.h. Kenntnis der Faktorisierung von n
- Kenntnis von $d \curvearrowright$ effektive Faktorisierung von n

(5.4-1) DIGITALE SIGNATUREN

Aufgabe

überzeuge Alice, daß Text von Bob stammt

Signierung

$$\underbrace{\text{Text} \xrightarrow[\text{Signatur-Schlüssel}]{\text{Bobs geheimer}}}_{\text{Bob}} : \{\text{Text, Signatur}\}$$

Verifikation

$$\{\text{Text, Signatur}\} : \underbrace{\xrightarrow[\text{Signatur-Schlüssel}]{\text{Bobs öffentlicher}}}_{\text{Alice}} \{\text{True, False}\}$$

Sicherheit: Valide Signatur erlaubt *keine* Rückschlüsse auf geheimen Schlüssel

Dualität zu asymmetrischer Verschlüsselung (Diffie/Hellman 1976)

Jedes asymmetrische Verfahren eignet sich zur Signatur

1. Bob „entschlüsselt“ mit seinem *geheimen* Schlüssel den Text:

$$\text{Signatur} = \text{„Entschlüsselung“}(\text{Text})$$

2. Alice „verschlüsselt“ mit Bobs *öffentlichem* Schlüssel die Signatur und testet

$$\text{Text} = \text{„Verschlüsselung“}(\text{Signatur}) \quad ?$$

Falls ja, so folgt aus der Sicherheit des Kryptosystems, daß nur Bob die Nachricht signieren konnte.

Zur Praxis

- aus *Aufwandsgründen* wird nicht der Text selbst unterschrieben
- sondern eine *kryptographische Prüfsumme* (message digest) fester Länge k
- Standard für k : 128 bzw. 160 Bits
- message digest aus kryptographischer *Hashfunktion* $f : \mathbb{N} \rightarrow \mathbb{Z}_2^k$.

Design-Wunsch: *faktisch kollisionsfrei*, d.h. es dürfen keine zwei Texte mit der gleichen Prüfsumme effektiv berechenbar sein.

Beispiele

- MD5 (Rivest 1991): 128-Bit Digest
- SHA-1 (NIST 1995): 160-Bit Digest

US-amerikanischer *digital signature standard* DSS (NIST 1994)

basiert nicht auf der Dualität (5.4-2), sondern auf einer Idee von ElGamal (1985).

Praktische und rechtliche Gründe

- Trennung von Signatur und Verschlüsselung
- RSA-Patent

Sicherheit von DSS basiert auf rechnerischer Schwierigkeit diskreter Logarithmen.

Digitale Signatur nach ElGamal (1985)

Vorbereitung: p prim, $\alpha \in \mathbb{Z}_p^\times$ Primitivwurzel

- Geheimer Signatur-Schlüssel: $a \in \mathbb{Z}_{p-1}$
- Öffentlicher Signatur-Schlüssel: $(p, \alpha, \beta = \alpha^a \bmod p)$

- Signierung

$x \in \mathbb{Z}_{p-1}$ message digest. Wähle zufälliges $k \in \mathbb{Z}_{p-1}^\times$

$$\text{Signatur} = \{\gamma = \alpha^k \bmod p, \delta = (x - a\gamma)k^{-1} \bmod (p-1)\}$$

- Verifikation

$$\beta^\gamma \gamma^\delta = \alpha^x \bmod p ?$$

Beweis der Verifikationsformel

Nach Konstruktion von β, γ gilt

$$\beta^\gamma \gamma^\delta = \alpha^{a\gamma+k\delta} \pmod{p}.$$

Da α Primitivwurzel ist, ist genau dann $\beta^\gamma \gamma^\delta = \alpha^x \pmod{p}$, wenn

$$a\gamma + k\delta = x \pmod{\phi(p)}, \quad \phi(p) = p - 1.$$

Genauso wurde aber δ konstruiert.

Sicherheit

Es ist kein effektiverer Algorithmus zum Bruch dieser Signatur bekannt, als das Lösen des diskreten Logarithmus \pmod{p} .

(6.1-1) FAKTORISIERUNG ALS PERIODENBESTIMMUNG

n ungerade, zusammengesetzte Zahl, keine Primzahlpotenz

Definition.

Für $x \in \mathbb{Z}_n^\times$ heißt die *kleinste* Zahl $1 \leq r \leq \phi(n)$ mit $x^r = 1 \pmod{n}$ *Ordnung* von x .

Es gilt $r \mid \phi(n)$.

Beobachtung

Ordnungsbestimmung = Periodensuche (4.1-2)

$$f_x : \mathbb{Z}_{\phi(n)} \rightarrow \mathbb{Z}_n^\times, \quad k \mapsto x^k \pmod{n}, \quad \text{ist } r\text{-periodisch.}$$

↪ prinzipieller Quantenalgorithmus (4.5-1), vgl. (4.6-2)

↪ effektiver Quantenalgorithmus (Shor 1994), Details später

Zusammenhang mit Faktorisierung (Miller 1976)

Faktorisierung von n läßt sich auf Ordnungsbestimmung reduzieren

1. Idee

Sei $x \in \mathbb{Z}_n^\times$ **millersch**, d.h. habe *gerade* Periode $r = 2k$ mit

$$x^k \neq -1 \pmod n.$$

Also $(x^k \pm 1) \not\equiv 0 \pmod n$, aber $x^{2k} - 1 = (x^k - 1)(x^k + 1) \equiv 0 \pmod n$.

Dies liefert *echten Faktor* von n :

$$1 < \text{GGT}(x^k - 1, n) < n$$

Berechnung mit Euklidischem Algorithmus in *polynomieller Zeit*.

2. Idee

Wähle $x \in \mathbb{Z}_n^\times$ *zufällig*.

- Frage: Wie groß ist die *Wahrscheinlichkeit*, daß x millersch?
- Antwort: $\geq 1/2 \rightsquigarrow$ effektiver Las Vegas-Algorithmus

Satz. (Miller 1976) Mindestens die *Hälfte* aller $x \in \mathbb{Z}_n^\times$ ist millersch.

Beweisskizze. (Nur für RSA-Module $n = p_1 \cdot p_2$.)

$x \in \mathbb{Z}_n^\times$ habe Ordnung r modulo n , r_i modulo p_i .

Chinesischer Restsatz $\rightsquigarrow r = \text{KGV}(r_1, r_2)$.

Hilfsresultat

x millersch $\iff |r_1|_2 \neq |r_2|_2$

- $|r_1|_2 = |r_2|_2 = 0 \iff r$ ungerade
- $|r_1|_2 = |r_2|_2 > 0 \iff r/2 = (r_i/2) \cdot (2k_i + 1)$

$$\iff x^{r/2} = \left(x^{r_i/2}\right)^{2k_i+1} \equiv -1 \pmod{p_i}.$$

Beweisskizze – Fortsetzung

Hieraus und aus dem Chinesischer Restsatz folgt

$$\begin{aligned} & \text{Anteil der nicht millerschen } x \in \mathbb{Z}_n^\times \\ &= \text{Anteil der } (x_1, x_2) \in \mathbb{Z}_{p_1}^\times \times \mathbb{Z}_{p_2}^\times \text{ mit } |r_1|_2 = |r_2|_2 \\ &\leq \text{max. Anteil der } x_1 \in \mathbb{Z}_{p_1}^\times \text{ mit vorgegebenem } |r_1|_2 \end{aligned}$$

Letzterer ist $\leq 1/2$ wegen der zyklischen Struktur von $\mathbb{Z}_{p_1}^\times$.

Bemerkung

Abschätzung läßt sich nicht verschärfen: genau die Hälfte aller $x \in \mathbb{Z}_{77}^\times$ ist millersch.

*Zusammenfassung***Algorithmus zur Faktorisierung von n**

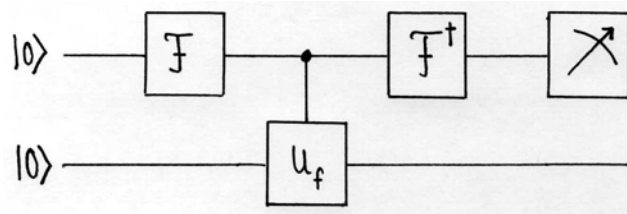
1. wähle zufällig $1 < x < n$
2. falls $\text{GGT}(x, n) > 1 \curvearrowright$ echter Faktor gefunden: **success**
3. bestimme Ordnung r von x in \mathbb{Z}_n^\times (\leftarrow Quantenalgorithmus!)
4. falls r ungerade: **failed**
5. falls $x^{r/2} = -1 \pmod n$: **failed**
6. $\text{GGT}(x^k - 1, n)$ ist echter Faktor: **success**

Mißerfolgswahrscheinlichkeit nach k Durchläufen $\leq 2^{-k}$

Erwartungswert der Anzahl der Durchläufe bis zum Erfolg ≤ 2

Aufgabe: Bestimme Ordnung $r \bmod \phi(n)$ von $a \in \mathbb{Z}_n^\times$.

Proto-Quantenalgorithmus (4.5-1) zur Ordnungsbestimmung



- f modularer Exponentiation von a modulo n

$$f : \mathbb{Z}_{\phi(n)} \rightarrow \mathbb{Z}_n^\times, \quad k \mapsto a^k \bmod n.$$

- \mathcal{F} Fourier-Transformation in $\mathbb{Z}_{\phi(n)}$.

Messung: Ergibt gleichverteilt Vielfaches von $\phi(n)/r$. Nachbearbeitung liefert r .

Warum „Proto“?

- $\phi(n)$ unbekannt, setzt Faktorisierung von n voraus
- alternativ könnte

$$f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n^\times, \quad k \mapsto a^k \bmod n$$

mit irgendeinem Vielfachen m der Ordnung r zugrunde gelegt werden.

Aber wenn r unbekannt ist, wie kommt man zu m ?

- Fouriertransformation \mathcal{F} auf \mathbb{Z}_q
nur für $q = 2^\ell$ einfach realisierbar durch effizienten Quantenalgorithmus

Für welche n ist der Proto-Quantenalgorithmus realisierbar?

- n ungerade mit $\phi(n) = 2^\ell$

Somit n Produkt verschiedener Fermat'scher Primzahlen $2^k + 1$

nur fünf bekannt: 3, 5, 17, 257, 65537.

Eine gebildete Marginalie

Genau für diese ungeraden n sind die regelmäßigen n -Ecke mit Zirkel und Lineal konstruierbar.

Ein Schelm, der Böses dabei denkt...

*To read our E-mail; how mean
of the spies and their quantum machine;
be comforted though,
they do not yet know
how to factorize twelve or fifteen.
– Volker Strassen*

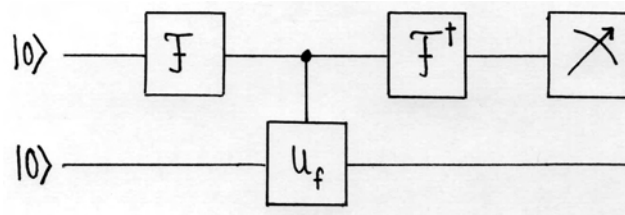
Der einfachste Fall

$n = 15 = 3 \cdot 5$ mit $\phi(n) = 2^3$

Qubits: 3 im ersten Register, $4 = \lceil \log_2(n) \rceil$ im zweiten Register

Dezember 2001: Experimentell realisiert mit 7-Qubit NMR-Technologie von Vandersypen/Steffen/Breyta/Yannoni/Sherwood/Chuang (IBM Almaden, Stanford)

Allgemeiner Shor'scher Algorithmus zur Periodenbestimmung:



$$f: \mathbb{Z} \rightarrow X \quad r\text{-periodisch}$$

\mathcal{F} Fourier-Transformation auf \mathbb{Z}_q , $q = 2^\ell$.

- # Qubits im ersten Register: ℓ
- # Qubits im zweiten Register: $\lceil \log_2(|X|) \rceil$

Frage: Was ergibt die Messung?

Zustand nach U_f : $\frac{1}{\sqrt{q}} \sum_t |t\rangle |f(t)\rangle$.

Zustand vor Messung:

$$\frac{1}{q} \sum_{k,t=0}^{q-1} e^{\frac{2\pi i}{q} kt} |k\rangle |f(t)\rangle = \sum_{k=0}^{q-1} \sum_{s=0}^{r-1} \underbrace{\left(\frac{1}{q} \sum_{t:f(t)=f(s)} e^{\frac{2\pi i}{q} kt} \right)}_{=\gamma_{ks}} |k\rangle |f(s)\rangle.$$

Werte $f(s)$ für $s = 0, \dots, r-1$ paarweise verschieden \curvearrowright

Vektoren $|k\rangle |f(s)\rangle$ bilden ON-System \curvearrowright

Messung in beiden Registern:

Resultat $(k, f(s))$ mit Wahrscheinlichkeit $|\gamma_{ks}|^2$.

Es gilt $f(t) = f(s)$ mit $0 \leq t < q$, $0 \leq s < r$ genau dann, wenn

$$t = s + jr, \quad 0 \leq j \leq m_s = \left\lfloor \frac{q-1-s}{r} \right\rfloor.$$

Daher ergibt sich

$$\gamma_{ks} = \frac{e^{\frac{2\pi i}{q} ks}}{q} \sum_{j=0}^{m_s} e^{\frac{2\pi i}{q} j kr} = \frac{e^{\frac{2\pi i}{q} ks}}{q} \sum_{j=0}^{m_s} e^{\frac{2\pi i}{q} j \{kr\}_q},$$

wobei $\{kr\}_q = kr \bmod q$ genau jener Rest sei, für den

$$-q/2 < \{kr\}_q \leq q/2.$$

(6.2-4) PERIODENBESTIMMUNG: DER ALLGEMEINE FALL

Beschränken wir uns auf die k mit $-r/2 \leq \{kr\}_q \leq r/2$.

Dann besitzt für $q \geq 14r$ das Resultat $(k, f(s))$ die Wahrscheinlichkeit

$$\begin{aligned} |\gamma_{ks}|^2 &= \frac{1}{q^2} \left| \sum_{j=0}^{m_s} e^{\frac{2\pi i}{q} \{kr\}_q j} \right|^2 = \frac{1}{q^2} \frac{\sin^2 \frac{\pi \{kr\}_q (m_s+1)}{q}}{\sin^2 \frac{\pi \{kr\}_q}{q}} \\ &\geq \frac{4}{\pi^2} \frac{1}{r^2} \left(1 - \left(\frac{\pi r}{2q} \right)^2 \right) > \frac{0.4}{r^2}. \end{aligned}$$

Prinzip der impliziten Messung (2.4-8) \curvearrowright

Messung des ersten Registers: (da r Möglichkeiten für $f(s)$)

Wahrscheinlichkeit $> 0.4/r$ für jedes k mit $|\{kr\}_q| \leq r/2$.

Frage: Was bedeutet $-r/2 \leq \{kr\}_q \leq r/2$?

Es gibt also eine ganze Zahl $0 \leq d < r$ mit $-r/2 \leq kr - dq \leq r/2$.

Division durch rq zeigt

$$\left| \frac{k}{q} - \frac{d}{r} \right| \leq \frac{1}{2q}.$$

Lemma. Es gibt nur einen einzigen Bruch d/r mit $r^2 < q$, welcher durch k/q im diesem Sinne approximiert wird.

Beweis: Wäre $d'/r' \neq d/r$ ein weiterer Kandidat, erhielten wir den *Widerspruch*

$$\frac{1}{q} < \frac{|d'r - dr'|}{r r'} = \left| \left(\frac{k}{q} - \frac{d'}{r'} \right) - \left(\frac{k}{q} - \frac{d}{r} \right) \right| \leq 2 \cdot \frac{1}{2q}.$$

Folgerung

Unter der Voraussetzung $r^2 < q$ gilt also:

- Ist $k_1 \dots k_\ell$ die Binärdarstellung von $0 \leq k < q = 2^\ell$ mit $|\{kr\}_q| \leq r/2$, so ist

$$0.k_1 \dots k_\ell$$

korrekt gerundete Dualbruchapproximation (Mantissenlänge ℓ) genau eines Bruchs d/r mit $0 \leq d < r$.

- Umgekehrt besitzt natürlich jeder solche Bruch wenigstens eine solche Approximation, also ein zugehöriges k mit $|\{kr\}_q| \leq r/2$.

Frage: Wie berechnet man die Zuweisung $k \mapsto d/r$?

Antwort: Kettenbruchtheorie

Satz. (Legendre)

Kettenbruch einer rationalen Zahl $0 \leq x < 1$ sei

$$x = \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_N}}}} = [0, a_1, a_2, \dots, a_N], \quad a_j \in \mathbb{N}.$$

Gilt für $0 \leq d < r$ die Abschätzung

$$\left| x - \frac{d}{r} \right| < \frac{1}{2r^2},$$

so ist $d/r = [0, a_1, a_2, \dots, a_m]$ ein m .ter Näherungsbruch von x und läßt sich mit dem Euklidischen Algorithmus effizient berechnen.

Beispiel

$$k/q = 377/1024 = [0, 2, 1, 2, 1, 1, 10, 5]$$

Gesucht ist d/r mit $r^2 < q$ und

$$\left| \frac{k}{q} - \frac{d}{r} \right| \leq \frac{1}{2q} < \frac{1}{2r^2}.$$

Lösungsbruch d/r ist eindeutig, falls er existiert. Hier $d/r = 7/19$.

Näherungsbruch	Approximation	Nenner
$[0, 2] = 1/2$	zu schlecht	brauchbar
$[0, 2, 1] = 1/3$	zu schlecht	brauchbar
$[0, 2, 1, 2] = 3/8$	zu schlecht	brauchbar
$[0, 2, 1, 2, 1] = 4/11$	zu schlecht	brauchbar
$[0, 2, 1, 2, 1, 1] = 7/19$	gut	brauchbar
$[0, 2, 1, 2, 1, 1, 10] = 74/201$	gut	zu groß

*Beispiel – Fortsetzung*Berechnung vom Bruch d/r

Euklidischer Algorithmus	Zähler u_i	Nenner v_i
$1024 = 2 \cdot 377 + 270$	$1 = 2 \cdot 0 + 1$	$2 = 2 \cdot 1 + 0$
$377 = 1 \cdot 270 + 107$	$1 = 1 \cdot 1 + 0$	$3 = 1 \cdot 2 + 1$
$270 = 2 \cdot 107 + 56$	$3 = 2 \cdot 1 + 1$	$8 = 2 \cdot 3 + 2$
$107 = 1 \cdot 56 + 51$	$4 = 1 \cdot 3 + 1$	$11 = 1 \cdot 8 + 3$
$56 = 1 \cdot 51 + 5$	$7 = 1 \cdot 4 + 3$	$19 = 1 \cdot 11 + 8$
$51 = 10 \cdot 5 + 1$	$74 = 10 \cdot 7 + 4$	$201 = 10 \cdot 19 + 11$
$5 = 5 \cdot 1 + 0$	$377 = 5 \cdot 74 + 7$	$1024 = 5 \cdot 201 + 19$

Abbruch beim ersten Nenner $v_{m+1} > \sqrt{q} = 32 \curvearrowright$ Einzigster Lösungskandidat: $u_m/v_m = 7/19$.*Zusammenfassung***Satz (Shor 1994).**Sei $q > \max(14r, r^2)$.

- Messung im Quantenalgorithmus (6.2-1) liefere $0 \leq k < q$.
- k/q werde wie in (6.2-9) durch Kettenbruchalgorithmus in „Kandidaten“ d_*/r_* umgerechnet.

Auf diese Weise erhält man die gekürzte Form jedes der r Brüche

$$d/r, \quad 0 \leq d < r,$$

mit Wahrscheinlichkeit $\geq 0.4/r$.

Frage: Wie gelangt man nun zu r ?

Antwort: Wie beim Proto-Algorithmus in (4.6-2).

Dort wurde für $N = s \cdot r$ mit je gleicher Wahrscheinlichkeit einer der r Werte $d \cdot s$, $0 \leq d < r$ gemessen, bzw. äquivalent

$$\frac{d}{r} = \frac{d \cdot s}{N},$$

erhalten.

Die Nachbearbeitung aus (4.6-3) ist also prinzipiell übertragbar.

Nachbearbeitung des Periodenproblems

- zwei Durchläufe des Shor'schen Algorithmus $\curvearrowright d_*/r_*, d_{**}/r_{**}$
- $\hat{r} = \text{KGV}(r_*, r_{**})$
- falls $f(\hat{r}) \neq f(0)$: **failed**
- also $r = \hat{r}$: **success**

Lemma. Erfolgswahrscheinlichkeit ist $\geq 9.6\%$.

Beweis. Erfolg, wenn $d_*/r_* = d_1/r$ und $d_{**}/r_{**} = d_2/r$ mit $\text{GGT}(d_1, d_2) = 1$. Nach (6.2-10) tritt jedes der r^2 Paare (d_1, d_2) mit Wahrscheinlichkeit $\geq 0.4^2/r^2$ auf. Nach (4.6-4) sind von all diesen Paaren mehr als 60% teilerfremd. Also liegt die Erfolgswahrscheinlichkeit bei $\geq 0.6 \cdot 0.4^2 = 0.096$.

Parameterwahl für die Ordnungsbestimmung

Periodenbestimmung für $f : k \in \mathbb{Z} \mapsto a^k \bmod n \in \mathbb{Z}_n^\times$. Hier gilt

$$0 < r \leq \phi(n) < n,$$

so daß $q \geq n^2$ bei $n \geq 14$ allen Voraussetzungen genügt. Also

- $\ell = 2 \lceil \log_2 n \rceil$ Qubits im ersten Register
- $\lceil \log_2 n \rceil$ Qubits im zweiten Register

Aufwandsabschätzung für die Ordnungsbestimmung

Da die Fouriertransformation mit $O(\ell^2)$ Gattern realisierbar ist, dominiert der Aufwand für die Quantenrealisierung eines reversiblen Schaltkreises der modularen Exponentiation:

$$\text{Gesamtaufwand für (6.2-1)} = O((\ln^2 n)(\ln \ln n)(\ln \ln \ln n)).$$

Quantenalgorithmus zur Primfaktorisation

Bis auf die Details der Fouriertransformation auf \mathbb{Z}_{2^ℓ} ist der Algorithmus vollständig beschrieben.

- Erwartete Rechenzeit ist

$$O((\ln^2 n)(\ln \ln n)(\ln \ln \ln n)),$$

d.h. *polynomiell* in der Eingabelänge $\lceil \log_2 n \rceil$

- Faktorisierung ist ein Problem in **BQP**

Dies war der erste „Durchbruch“ für das junge Gebiet der Quantenalgorithmen. Peter Shor erhielt dafür auf dem ICM 1998 in Berlin den *Nevanlinna-Preis*, eine Art Nobelpreis für mathematische Aspekte der Informatik.

Daten: p prim, g Primitivwurzel modulo p , $p \nmid x$

Aufgabe: löse $g^k = x \pmod{p}$

Zugehöriges Hidden-Subgroup-Problem (Shor 1996)

- $G = (\mathbb{Z}_{\phi(p)} \times \mathbb{Z}_{\phi(p)}, +)$
- Homomorphismus $f : G \rightarrow (\mathbb{Z}_p^\times, \cdot)$, $(\ell, m) \mapsto x^\ell g^m \pmod{p}$
- $K = \text{Kern } f = \{(\ell, m) : m = -\ell k \pmod{\phi(p)}\}$
- Charaktere $\chi_{\lambda, \mu}(\ell, m) = \exp\left(\frac{2\pi i}{\phi(p)}(\lambda\ell + \mu m)\right)$
wegen Lemma (4.2-3) und Beispiel (4.2-4a)

Die Untergruppe K kodiert die gesuchte Lösung $k \pmod{\phi(p)}$

Quantenalgorithmus (4.5-1)

liefert gleichverteilt ein Element aus

$$K^\circ = \{(\lambda, \mu) \in G : \lambda = \mu k \pmod{\phi(p)}\}.$$

Dabei trifft man mit *Erfolgs-Wahrscheinlichkeit* ($p \geq 23$)

$$\frac{\phi(\phi(p))}{\phi(p)} \geq 1/4 \ln \ln p$$

auf ein zu $\phi(p)$ teilerfremdes μ . Die Lösung ist dann

$$k = \lambda \mu^{-1} \pmod{\phi(p)}.$$

Beispiel

Für eine Germain-Primzahl $p = 2q + 1$, q prim, ist die Erfolgs-Wahrscheinlichkeit sogar

$$\frac{\phi(\phi(p))}{\phi(p)} = \frac{q-1}{p-1} = \frac{q-1}{2q} \simeq \frac{1}{2}.$$

Caveat

Wegen der Restriktion der Fouriertransformation auf \mathbb{Z}_q mit $q = 2^\ell$, ist dieser Algorithmus unmittelbar auch nur für *Fermat'sche Primzahlen* p anwendbar.

Allgemeiner Algorithmus

- ersetzt G durch $\mathbb{Z}_q \times \mathbb{Z}_q$ mit $q = 2^\ell$, $\ell = 2\lceil \log_2 n \rceil$
- approximiert die Wahrscheinlichkeiten des Hidden-Subgroup-Algorithmus
- aufwendige klassische Nachbearbeitung

Details

Originalarbeit von Peter Shor, SIAM J. Comp. 26, 1484–1509, 1997.

Ziel

Quanten-Fouriertransformation (QFT) aus schneller Fouriertransformation (FFT)

FFT ist ein „*divide et impera*“- („teile und herrsche“-) Algorithmus, d.h. das Problem wird auf die Lösung gleichartiger Probleme kleinerer Größe zurückgespielt.

Gruppentheoretische Herleitung

Fouriertransformation über G aus Fouriertransformation über *Untergruppe* $H < G$

Notation

- G, H endliche abelsche Gruppen
- $\phi : H \hookrightarrow G$ homomorphe Einbettung, d.h. H ist *isomorph* zu Untergruppe von G
- R Restklassenrepräsentanten $\text{mod } \phi(H)$, d.h. für jedes $g \in G$

$$g = r + \phi(h) \quad \text{eindeutig mit } r \in R, h \in H.$$

- diese eindeutige Zerlegung definiert zwei Abbildungen $\sigma : G \rightarrow H, \rho : G \rightarrow R$ mit

$$\text{id}_G = \rho + \phi \circ \sigma$$

- $m = |R| = |G|/|H|$

Notation – Fortsetzung

- da $G \simeq G^*$ und $H \simeq H^*$, gibt es einen Homomorphismus

$$\pi : G \rightarrow H, \quad \text{so daß } \chi_g^G \circ \phi = \chi_{\pi(g)}^H \quad \forall g \in G.$$

Dabei haben wir χ^G für Charaktere auf G , χ^H für solche auf H geschrieben. Diese Superskripte werden wir weglassen, falls keine Gefahr eines Mißverständnisses besteht.

Bemerkung

Es ist

$$\text{Kern } \pi = \phi(H)^\circ,$$

der Annihilator der isomorphen Kopie von H in G .

Reduktion der Fouriertransformation von G auf H

Sei $f : G \rightarrow \mathbb{C}$. Dann gilt für die Fouriertransformierte

$$\begin{aligned} \mathcal{F}_G^\dagger f(g) &= \frac{1}{\sqrt{|G|}} \sum_{g' \in G} \chi_g(g') f(g') \\ &= \frac{1}{\sqrt{m}} \sum_{r \in R} \chi_g(r) \frac{1}{\sqrt{|H|}} \sum_{h \in H} \underbrace{\chi_g(\phi(h))}_{=\chi_{\pi(g)}^H(h)} \underbrace{f(r + \phi(h))}_{=f_r(h)} \\ &= \frac{1}{\sqrt{m}} \sum_{r \in R} \chi_g(r) (\mathcal{F}_H^\dagger f_r)(\pi(g)) \end{aligned}$$

Es definiert $f_r : H \rightarrow \mathbb{C}$, $h \mapsto f(r + \phi(h))$, für jede Restklasse eine Funktion auf H .

Reduktionsformel

$$\mathcal{F}_G^\dagger f(g) = \frac{1}{\sqrt{m}} \sum_{r \in R} \chi_g(r) (\mathcal{F}_H^\dagger f_r)(\pi(g))$$

Wir wollen nun zu einer *Matrixdarstellung* bei Auffassung von $f \in \mathbb{C}^{|G|}$ etc. gelangen.

- Für einen Basisvektor („Deltafunktion“) $f = |g\rangle$ gilt

$$f_r = \begin{cases} |\sigma(g)\rangle & \text{für } r = \rho(g) \\ 0 & \text{sonst} \end{cases}$$

- Prolongationsmatrizen $P_r : \mathbb{C}^{|H|} \rightarrow \mathbb{C}^{|G|}$, $r \in R$,

$$|h\rangle \mapsto \frac{1}{\sqrt{m}} \sum_{g \in \pi^{-1}(h)} \chi_g(r) |g\rangle$$

- Restriktionsmatrix $R : \mathbb{C}^{|G|} \rightarrow \mathbb{C}^{|H|}$

$$|g\rangle \mapsto |\sigma(g)\rangle$$

Lemma.

Es gilt die Matrix-Faktorisierung

$$\mathcal{F}_G^\dagger |g\rangle = P_{\rho(g)} \mathcal{F}_H^\dagger R |g\rangle.$$

Bemerkung.

Dies bildet die Grundlage von FFT-Algorithmen für abelsche Gruppen.

Beweis.

Wenden wir die Reduktionsformel auf $f = |g\rangle$ an, so gilt mit

$$\mathcal{F}_H^\dagger |\sigma(g)\rangle = \sum_{h \in H} \alpha_h |h\rangle$$

$$\left(\mathcal{F}_G^\dagger |g\rangle \right) (g') = \frac{1}{\sqrt{m}} \chi_{g'}(\rho(g)) \alpha_{\pi(g')}.$$

Da jedes $g' \in G$ von der Form $g' \in \pi^{-1}(h)$ für *genau ein* $h \in H$ ist, nämlich für $h = \pi(g')$, folgt hieraus die Behauptung:

$$\begin{aligned} \mathcal{F}_G^\dagger |g\rangle &= \frac{1}{\sqrt{m}} \sum_{g' \in G} \chi_{g'}(\rho(g)) \alpha_{\pi(g')} |g'\rangle \\ &= \sum_{h \in H} \alpha_h \frac{1}{\sqrt{m}} \sum_{g' \in \pi^{-1}(h)} \chi_{g'}(\rho(g)) |g'\rangle = \sum_{h \in H} \alpha_h P_{\rho(g)} |h\rangle \\ &= P_{\rho(g)} \mathcal{F}_H^\dagger |\sigma(g)\rangle = P_{\rho(g)} \mathcal{F}_H^\dagger R |g\rangle \end{aligned}$$

Der Rahmen

- $G = \mathbb{Z}_{2^n}$, $H = \mathbb{Z}_{2^{n-1}}$ (das riecht nach Rekursion...) $\curvearrowright m = 2$
- $\mathbb{C}^{|G|} = \mathbb{C}^{2^n} = (\mathbb{C}^2)^{\otimes n}$, d.h. der Zustandsraum von n Qubits
- wir schreiben \mathcal{F}_n für \mathcal{F}_G etc.
- Elemente in G sind n -Bit Dualzahlen $g = \gamma_n \dots \gamma_1$,
entsprechend in H ($n - 1$)-Bit Dualzahlen $h = \eta_{n-1} \dots \eta_1$
- Charaktere:

$$\chi_g^G(g') = \exp\left(\frac{2\pi i}{2^n} g g'\right), \quad \chi_h^H(h') = \exp\left(\frac{2\pi i}{2^{n-1}} h h'\right).$$

Konkretisierung der abstrakten Theorie

- Einbettung $\phi : H \rightarrow G$, $h \mapsto 2 \cdot h$, d.h. *Linksshift*

$$\gamma_{n-1} \dots \gamma_1 \mapsto \gamma_{n-1} \dots \gamma_1 0.$$

- Jedes $g = \gamma_n \dots \gamma_2 \gamma_1$ in G besitzt die eindeutige Zerlegung

$$\gamma_n \dots \gamma_2 \gamma_1 = \underbrace{\gamma_n \dots \gamma_2 0}_{=\phi(\sigma(g))} + \underbrace{\gamma_1}_{=\rho(g)}.$$

\curvearrowright Restklassenrepräsentanten $R = \{0, 1\}$ und:

- $\rho : G \rightarrow R$, $g \mapsto g \bmod 2$, d.h.

$$\gamma_n \dots \gamma_1 \mapsto \gamma_1$$

- $\sigma : G \rightarrow H$,

$$\gamma_n \dots \gamma_2 \gamma_1 \mapsto \gamma_n \dots \gamma_2,$$

d.h. *Rechtsshift*

Konkretisierung der abstrakten Theorie – Fortsetzung

- Wegen

$$\begin{aligned} \exp\left(\frac{2\pi i}{2^{n-1}} g h\right) &= \exp\left(\frac{2\pi i}{2^n} g 2h\right) = \chi_g^G(\phi(h)) \\ &= \chi_{\pi(g)}^H(h) = \exp\left(\frac{2\pi i}{2^{n-1}} \pi(g) h\right) \end{aligned}$$

gilt $\pi : G \rightarrow H$, $g \mapsto g \bmod 2^{n-1}$, d.h.

$$\gamma_n \dots \gamma_1 \mapsto \gamma_{n-1} \dots \gamma_1.$$

Konkretisierung der abstrakten Theorie – Fortsetzung

- Restriktionsmatrix $R : |\gamma_n \dots \gamma_2 \gamma_1\rangle \mapsto |\gamma_n \dots \gamma_2\rangle$
- Es gibt genau zwei Prolongationsmatrizen P_r , $r \in R = \{0, 1\}$,

$$|h\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{g \in \pi^{-1}(h)} \chi_g(r) |g\rangle = \frac{1}{\sqrt{2}} (\chi_{0h}(r) |0h\rangle + \chi_{1h}(r) |1h\rangle).$$

Dabei ist

$$\chi_{0h}(1) = \exp\left(\frac{2\pi i}{2^n} h\right) = \omega^h, \quad \omega = \exp\left(\frac{2\pi i}{2^n}\right),$$

und

$$\chi_{1h}(1) = \exp\left(\frac{2\pi i}{2^n} (2^{n-1} + h)\right) = e^{\pi i} \omega^h = -\omega^h.$$

Konkretisierung der abstrakten Theorie – Fortsetzung

Also

- Prolongationsmatrix $P_0 : |h\rangle \mapsto \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes |h\rangle$
- Prolongationsmatrix P_1

$$P_1 : |h\rangle \mapsto \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes \omega^h |h\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes M|h\rangle$$

mit der Multiplikationsmatrix $M : \mathbb{C}^{2^{n-1}} \rightarrow \mathbb{C}^{2^{n-1}}$

$$M = \text{diag}(1, \omega, \omega^2, \dots, \omega^{2^{n-1}-1}).$$

- Faktorisierung nach Lemma (7.1-6) für $g = \gamma_n \dots \gamma_2 \gamma_1$

$$\mathcal{F}_n^\dagger |g\rangle = P_{\rho(g)} \mathcal{F}_{n-1}^\dagger R |g\rangle = P_{\gamma_1} \mathcal{F}_{n-1}^\dagger |\gamma_n \dots \gamma_2\rangle.$$

Rekursive Formulierung der FFT (Cooley-Tukey 1965)

Ausgeschrieben lautet die Faktorisierung nun:

$$\mathcal{F}_n^\dagger |\gamma_n \dots \gamma_1\rangle = \begin{cases} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \mathcal{F}_{n-1}^\dagger |\gamma_n \dots \gamma_2\rangle & \text{für } \gamma_1 = 0 \\ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes M \mathcal{F}_{n-1}^\dagger |\gamma_n \dots \gamma_2\rangle & \text{für } \gamma_1 = 1 \end{cases}$$

bzw. wegen $\mathcal{F}_n^\dagger = \overline{\mathcal{F}_n}$

$$\mathcal{F}_n |\gamma_n \dots \gamma_1\rangle = \begin{cases} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \mathcal{F}_{n-1} |\gamma_n \dots \gamma_2\rangle & \text{für } \gamma_1 = 0 \\ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes \overline{M} \mathcal{F}_{n-1} |\gamma_n \dots \gamma_2\rangle & \text{für } \gamma_1 = 1 \end{cases}$$

Multilineare Algebra erlaubt also, die FFT sehr kompakt zu schreiben.

Rekursives klassisches Programm

z.B. in Matlab direkt so programmierbar, Skalierung mit $1/\sqrt{2^n}$ wie üblich „gespart“:

```
function x = fft_(x)
if length(x) > 1
    % extrahiere Diagonale M aus vorab berechneten Potenzen
    x = Tensor([ 1; 1], fft_(x(even))) ...
        + Tensor([ 1;-1],M.*fft_(x(odd )));
end
return
```

Komplexität A_n

auf Vektoren der Länge $N = 2^n$

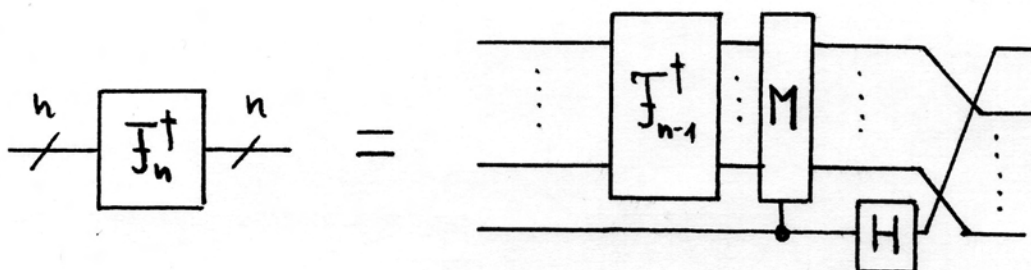
$$\begin{aligned}
 A_n &= \underbrace{2^n}_{\text{Addition der Vektoren}} + \underbrace{2^{n-1}}_{\text{Multiplikation mit } M} + 2A_{n-1} \\
 &= \frac{3}{2}2^n + 2 \left(\frac{3}{2}2^{n-1} + 2(\dots) \right) = \frac{3}{2}n2^n = \frac{3}{2}N \log_2 N.
 \end{aligned}$$

(7.3-1) QUANTEN-FOURIERTRANSFORMATION: DER SCHALTKREIS

Quanten-Schaltkreis

\mathcal{F}_n^\dagger ist unitärer Operator auf Zustandsraum von n Qubits.

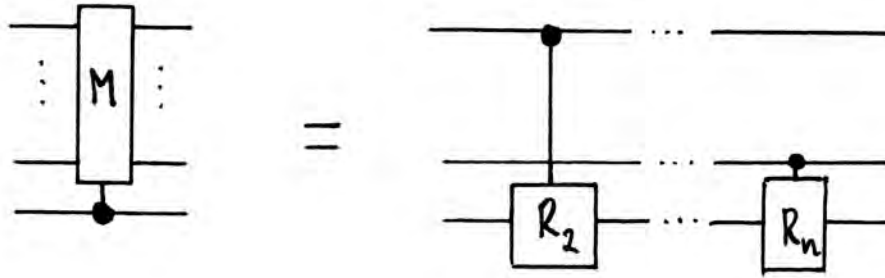
Darstellung (7.2-6) liefert unmittelbar folgende rekursive Beschreibung:



Aufgabe

Für die Quanten-Fouriertransformation muß nur noch das gesteuerte M-Gatter durch elementare Gatter ausgedrückt werden...

Lemma. Es gilt



$$\text{mit } R_k = \begin{bmatrix} 1 & \\ & e^{2\pi i/2^k} \end{bmatrix}.$$

Komplexität der QFT: (Shor/Coppersmith/Deutsch/Cleve)

Anzahl A_n der Gatter für n Qubits

$$A_n = O(n) + A_{n-1} = O(n^2) = O(\log^2 N).$$

Beweis.

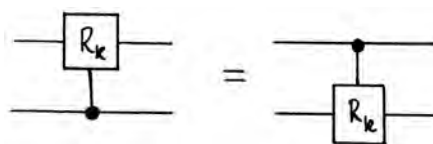
- es gilt die Faktorisierung (vgl. Algorithmus (5.2-6))

$$M = \text{diag}(1, \omega^{2^{n-2}}) \otimes \dots \otimes \text{diag}(1, \omega) = R_2 \otimes \dots \otimes R_n.$$

- also wirkt das von unten gesteuerte M wie

$$|x_2 \dots x_n, c\rangle \mapsto M^c |x_2 \dots x_n\rangle \otimes |c\rangle = R_2^c |x_2\rangle \otimes \dots \otimes R_n^c |x_n\rangle \otimes |c\rangle.$$

- das Steuer-Qubit kann nach oben gebracht werden:

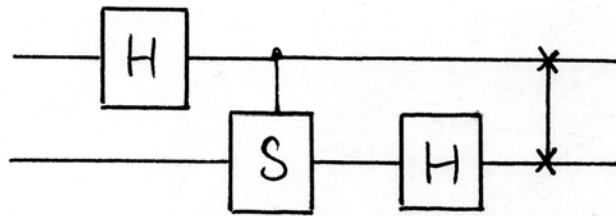


Denn Steuer- und Ziel-Qubit vertauschen:

$$|c, x\rangle \mapsto |c, R_k^c x\rangle = e^{2\pi i c x / 2^k} |c, x\rangle = |R_k^c c, x\rangle.$$

Beispiele

- $n = 2$

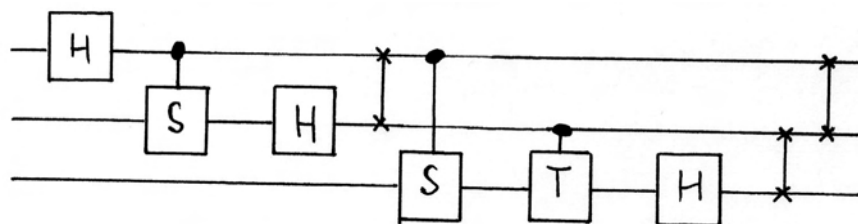


Zur Erinnerung

$$R_2 = \begin{bmatrix} 1 & \\ & i \end{bmatrix} = S, \quad R_3 = \begin{bmatrix} 1 & \\ & \exp(\pi i/4) \end{bmatrix} = T.$$

Beispiele – Fortsetzung

- $n = 3$



Beispiele – Fortsetzung

- $n = 3$: Protoalgorithmus von Shor ($N=15, a=7$)

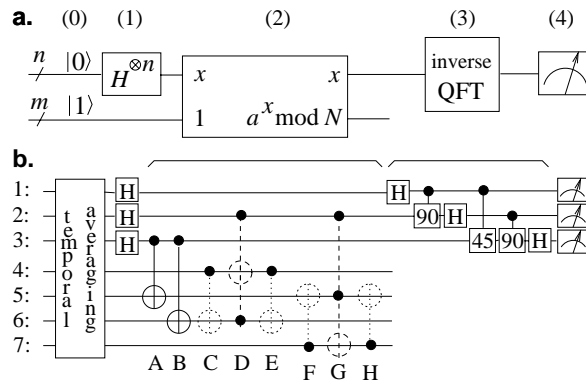


Figure 1

L. Vandersypen NATURE 07-Sep-01

aus der Originalpublikation (Nature 414, 883–887, 2001) der experimentellen NMR-Realisierung von Vandersypen et al.

Realisierung im MATLAB-Paket der Vorlesung

```

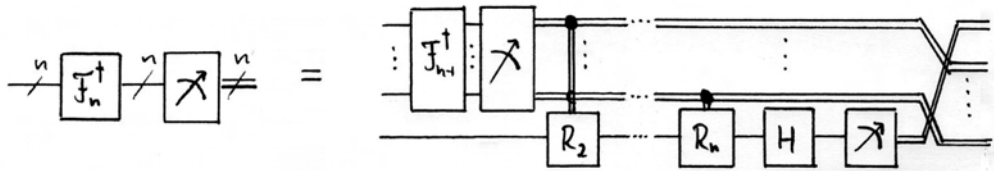
for j=1:n
    psi = Place(H, [j], n)*psi;
    for k=2:n-j+1
        psi = Place(Ctrl(R(k,trans)), [j k+j-1], n)*psi;
    end
end
psi = QubitPermute([n:-1:1])*psi;

```

Dabei sind alle SWAP-Gatter an das Ende verschoben worden.

„Semi-klassischer“ Schaltkreis: (Griffiths/Niu 1996)

Prinzip der verschobenen Messung (2.4-8) liefert



- Vorteil: Fouriertransformation mit unmittelbar anschließender Messung ist *ausschließlich* unter Verwendung von *1-Qubit-Gattern* realisierbar
- Nachteil: vorgezogene Messungen könnten „zu früh“ stören

NMR-Quantencomputer realisieren diese Idee nicht.

Problemstellung

Gegeben sei ein Boole'sches *Orakel* bzw. *Black-Box* $f : X \rightarrow \{0, 1\}$.

- $|X| = N = 2^n$
- Für $S = \{x \in X : f(x) = 1\}$ sei die *Anzahl* $|S| = M \geq 1$ *bekannt*.

Orakel kann als Quanten-Black-Box befragt werden, d.h.

$$U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$$

liegt als Quantenschaltkreis polynomieller Komplexität vor.

Aufgabe: Finde ein $x \in S$.

„Unstrukturierte“ Datensätze ...

... wenn die Kenntnis des inneren Aufbaus von f *nicht* weiterhilft.

Das Orakel f verhält sich „so gut wie“ zufällig.

Beispiele

- **NP**-vollständige Probleme: $f(x)$ testet Zertifikat x
- Symmetrische Kryptosysteme (DES, AES, etc.): $f(x)$ testet Schlüssel x .

In beiden Fällen bleibt klassisch nur das systematische Durchmusterung aller möglichen Zertifikate bzw. Schlüssel.

Klassischer probabilistischer Algorithmus

Jeder Algorithmus richtet k verschiedene Anfragen an das Orakel f

- falls $f(x) = 1$ für eine der Anfragen: $x \in S$ gefunden
- sonst: „failed“

Lemma.

Wahrscheinlichkeit für Erfolg in *genau* der k .ten Anfrage:

$$p_k = \frac{M}{N - k + 1} \frac{\binom{N-M}{k-1}}{\binom{N}{k-1}}.$$

Erwartete Anzahl von Befragungen des Orakels:

$$E(\# \text{ Suchschritte}) = \sum_{k=1}^{N-M+1} k \cdot p_k = \frac{N+1}{M+1}.$$

1. Idee

Präpariere (*approximativ*) den Zustand

$$\psi_{\text{good}} = \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle.$$

Messung liefert dann mit hoher Wahrscheinlichkeit ein $x \in S$.

Beobachtung

Der einfach präparierte Zustand $\psi_{\text{all}} = H^{\otimes n}|0\rangle$ erfüllt die Beziehung

$$\psi_{\text{all}} = \sqrt{\frac{N-M}{N}} \psi_{\text{bad}} + \sqrt{\frac{M}{N}} \psi_{\text{good}}, \quad \psi_{\text{bad}} = \frac{1}{\sqrt{N-M}} \sum_{x \notin S} |x\rangle,$$

d.h. ist Element der *reellen Ebene* $E = \text{lin}_{\mathbb{R}}\{\psi_{\text{bad}}, \psi_{\text{good}}\}$.

2. Idee

Drehe ψ_{all} ungefähr in den Zustand ψ_{good} , dabei ist der

$$\text{ideale Drehwinkel} = \arccos \sqrt{M/N}$$

a priori *bekannt*.

Problem: die Ebene E ist zunächst unbekannt...

Wirkung des Orakels U_f

in der unbekanntenen Ebene E gilt

$$U_f(\alpha\psi_{\text{bad}} + \beta\psi_{\text{good}}) = \alpha\psi_{\text{bad}} - \beta\psi_{\text{good}},$$

d.h. U_f ist *Spiegelung* an der Achse durch ψ_{bad} .

3. Idee

Konstruiere zunächst *irgendeine* Drehung in E . Hierzu brauchen wir einfach eine weitere Spiegelung.

Einziger Kandidat: Spiegelung R an Achse durch ψ_{all} ,

$$R = 2\psi_{\text{all}}\psi_{\text{all}}^\dagger - I.$$

Die Drehung

$G = R \cdot U_f$ ist Drehung um den Winkel θ , wobei $\theta/2$ der Winkel zwischen den Spiegelungsachsen ψ_{all} und ψ_{bad} ist:

$$\cos(\theta/2) = \sqrt{\frac{N-M}{N}}.$$

G heißt *Grover-Iteration*.

Satz. (Grover 1996, Boyer/Brassard/Hoyer/Tapp 1998)

Sei $M \leq N/2$. Dann gilt für den Zustand

$$\psi_k = G^k \psi_{\text{all}} = \alpha_k \psi_{\text{bad}} + \beta_k \psi_{\text{good}}, \quad \alpha_k, \beta_k \in \mathbb{R},$$

nach der Anzahl k an Iterationen mit

$$k = \left\lceil \frac{\arccos \sqrt{M/N}}{\theta} \right\rceil \leq \left\lceil \frac{\pi}{4} \sqrt{\frac{N}{M}} \right\rceil$$

die Abschätzung

$$\beta_k^2 = \cos^2 \left(\arccos \sqrt{M/N} - k\theta \right) \geq \cos^2(\theta/2) = 1 - \frac{M}{N} \geq \frac{1}{2}.$$

Anschließende Messung in der Rechenbasis liefert daher mit mindestens 50% Wahrscheinlichkeit ein $x \in S$.

Beweis.

Es gilt nach Konstruktion

$$\left| \underbrace{k\theta}_{\text{Drehwinkel von } G^k} - \underbrace{\arccos \sqrt{M/N}}_{\text{idealer Drehwinkel}} \right| \leq \theta/2,$$

so daß wegen $M \leq N/2$

$$\beta_k^2 = \cos^2 \left(\arccos \sqrt{M/N} - k\theta \right) \geq \cos^2(\theta/2) = 1 - \frac{M}{N} \geq \frac{1}{2}.$$

Aus der einfachen Abschätzung $\theta/2 \geq \sin(\theta/2) = \sqrt{M/N}$ folgt

$$k = \left\lceil \frac{\arccos \sqrt{M/N}}{\theta} \right\rceil \leq \left\lceil \frac{\pi}{2\theta} \right\rceil \leq \left\lceil \frac{\pi}{4} \sqrt{\frac{N}{M}} \right\rceil.$$

Fazit

Der Quanten-Suchalgorithmus braucht nur

$$\# \text{ Suchschritte} = O(\sqrt{N/M})$$

statt der $O(N/M)$ eines klassischen Algorithmus. Dies ist zwar keine exponentielle, so doch eine substantielle Beschleunigung mit einer enormen Fülle an möglichen Anwendungen.

Fragen

- effizienter Schaltkreis für $R = 2\Psi_{\text{all}}\Psi_{\text{all}}^\dagger - I$?
- ist die Anzahl der Suchschritte noch verbesserungsfähig?
- was kann man tun, wenn M nicht a priori bekannt ist?

Schaltkreis für R .

Wegen $\psi_{\text{all}} = H^{\otimes n} |0\rangle$ gilt $R = H^{\otimes n} \underbrace{(2|0\rangle\langle 0| - I)}_{=R_*} H^{\otimes n}$.

Dabei rechnet man sofort nach, daß

$$R_* |x\rangle = \begin{cases} |x\rangle & \text{falls } x = 0, \\ -|x\rangle & \text{sonst.} \end{cases}$$

Lemma. Für R_* gilt ein einfacher Schaltkreis mit $O(n)$ -Gattern,

$$R_* = -X^{\otimes n} C^{n-1}(Z) X^{\otimes n}.$$

Bemerkung. Die Phasenverschiebung um π hat keinen Einfluß auf den Algorithmus von Grover und braucht daher nicht implementiert zu werden: $X^{\otimes n} C^{n-1}(Z) X^{\otimes n}$ statt R_* genügt.

Beweis.

Für die Pauli-Matrix Z gilt

$$Z^c |\xi\rangle = (-1)^{c \wedge \xi} |\xi\rangle,$$

also für die $(n-1)$ -fache Steuerung $C^{n-1}(Z)$

$$\begin{aligned} & (-X^{\otimes n} C^{n-1}(Z) X^{\otimes n}) |x_1 \dots x_n\rangle \\ &= -|x_1 \dots x_{n-1}\rangle \otimes XZ^{(-x_1 \wedge \dots \wedge -x_{n-1})} X|x_n\rangle \\ &= -(-1)^{(-x_1 \wedge \dots \wedge -x_n)} |x_1 \dots x_{n-1}\rangle \otimes X^2|x_n\rangle \\ &= (-1)^{(x_1 \vee \dots \vee x_n)} |x_1 \dots x_n\rangle = R_* |x_1 \dots x_n\rangle \end{aligned}$$

Nach (2.7-9) läßt sich $C^{n-1}(Z)$ durch $O(n)$ elementare Gatter darstellen.

Die Schwierigkeit

Die Wahl der richtigen Anzahl k an Grover-Iterationen ist *entscheidend* für den Erfolg der Quanten-Suche.

It is like cooking a soufflé. The state is placed in the ‘quantum oven’ and the desired answer rises slowly. You must open the oven at the right time, neither too soon not too late, to guarantee success. Otherwise the soufflé will fall—the state collapses to the wrong answer.

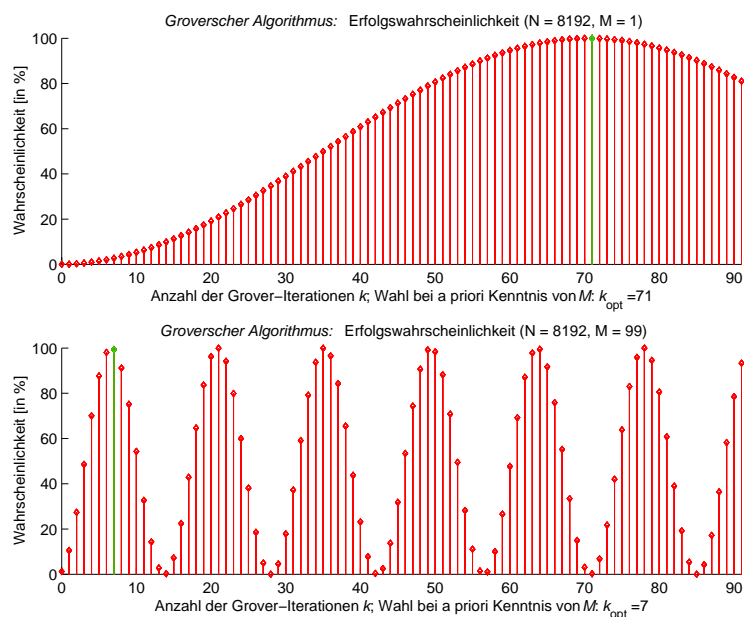
–Kristen Fuchs zitiert von Andrew Steane (1997)

Die Wahl des richtigen k basiert auf der *a priori* Kenntnis von M .

Frage: Wie soll man k aber wählen, wenn M *unbekannt* ist?

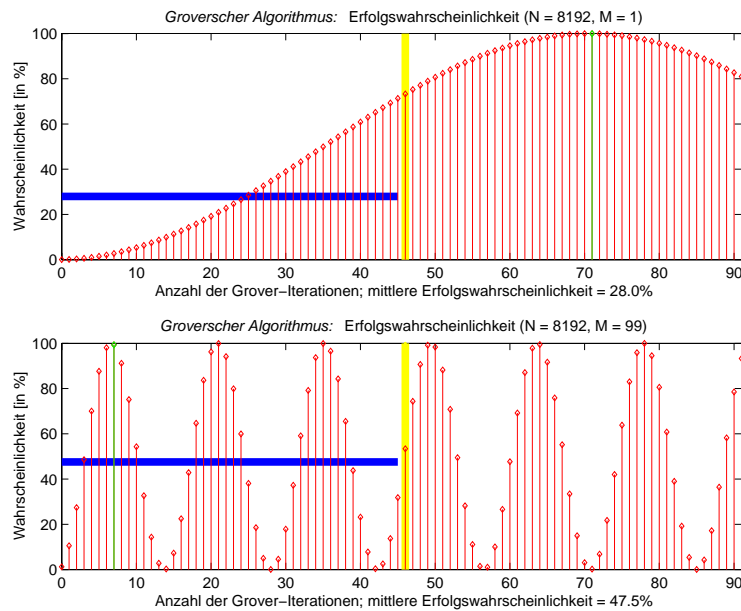
Beispiel

Eine *falsche* Wahl kann zum Desaster führen...



Beobachtung

Eine zufällige Wahl führt zum Erfolg...



(8.3-4) QUANTEN-SUCHE BEI UNBEKANNTER ANZAHL

Allgemeiner Quanten-Suchalgorithmus

1. wähle $k \in \{0, \dots, k_*\}$ zufällig (gleichverteilt)
2. führe Grover-Algorithmus mit k Iterationen aus $\curvearrowright \chi$
3. falls $f(\chi) = 1$: *success*
4. sonst: *failed*

Satz (Boyer/Brassard/Høyer/Tapp 1996).

Es sei $1 \leq M < N$. Für $k_* = \lceil \sqrt{N}/2 \rceil$ ist die Erfolgswahrscheinlichkeit des Algorithmus $\geq 25\% + O(N^{-1})$.

Wird der Algorithmus bis zum Erfolg wiederholt, so gilt

$$E(\# \text{ Suchschritte}) \leq \sqrt{N} + O(N^{-1/2}).$$

Beweis.

Gemäß (8.2-4) beträgt die Erfolgswahrscheinlichkeit nach genau k Grover-Iteration wegen $\sin(\theta/2) = \sqrt{M/N}$

$$p_k = \cos^2(k\theta - \arccos \sqrt{M/N}) = \sin^2((k + 1/2)\theta).$$

Also ist die Erfolgswahrscheinlichkeit des allgemeinen Quanten-Suchalgorithmus

$$\begin{aligned} p_{\text{Erfolg}} &= \frac{1}{k_*} \sum_{k=0}^{k_*-1} p_k = \frac{1}{k_*} \sum_{k=0}^{k_*-1} \sin^2((k + 1/2)\theta) \\ &= \frac{1}{2} - \frac{\sin(2k_*\theta)}{4k_* \sin \theta} \geq \frac{1}{2} - \frac{1}{4k_* \sin \theta}. \end{aligned}$$

Beweis – Fortsetzung.

Nun ist für $k_* = \lceil \sqrt{N}/2 \rceil$

$$4k_* \sin \theta = 8k_* \cdot \sin(\theta/2) \cdot \cos(\theta/2) \geq 4\sqrt{N} \cdot \sqrt{M/N} \cdot \sqrt{(N-M)/N}.$$

Für $1 \leq M \leq N-1$ gilt

$$\sqrt{M} \cdot \sqrt{N-M} \geq \sqrt{N-1},$$

und daher insgesamt

$$p_{\text{Erfolg}} \geq \frac{1}{2} - \frac{1}{4k_* \sin \theta} \geq \frac{1}{2} - \frac{1}{4} \sqrt{\frac{N}{N-1}} = \frac{1}{4} + O(N^{-1}).$$

Beweis – Ende.

Der allgemeine Suchalgorithmus benötigt im Mittel die Anzahl

$$\frac{1}{k_*} \sum_{k=0}^{k_*-1} k = \frac{k_* - 1}{2}$$

an Grover-Iterationen und muß erwartete $1/p_{\text{Erfolg}}$ Male wiederholt werden.

Also gilt

$$\begin{aligned} E(\# \text{ Suchschritte}) &= \frac{k_* - 1}{2} \cdot \frac{1}{p_{\text{Erfolg}}} \leq \frac{\sqrt{N}}{4} \cdot (4 + O(N^{-1})) \\ &= \sqrt{N} + O(N^{-1/2}). \end{aligned}$$

Gibt es welche ($M \geq 1$) oder nicht ($M = 0$), das ist die Frage...

... was kann geschlossen werden, wenn nach r -facher Wiederholung des allgemeinen Suchalgorithmus kein Element gefunden wurde?

In der Literatur findet sich häufig die Behauptung, daß in dem Fall aus Satz (8.3-4) sofort folgen würde:

$$(\text{Wahrscheinlichkeit für } M = 0) \geq 1 - (3/4)^r.$$

Dem ist nicht so!

Es handelt sich um einen auch unter Mathematikern weit verbreiteten Irrtum im Umgang mit bedingten Wahrscheinlichkeiten.

Analyse

Satz (8.3-4) liefert lediglich, daß

$$P(\text{kein Erfolg nach } r \text{ Versuchen} \mid M \geq 1) \leq (3/4)^r,$$

Die Behauptung hingegen will die Aussage treffen, daß

$$P(M \geq 1 \mid \text{kein Erfolg nach } r \text{ Versuchen}) \leq (3/4)^r.$$

Der Satz von Bayes besagt aber ($F = \text{kein Erfolg nach } r \text{ Versuchen}$):

$$\begin{aligned} P(M \geq 1 \mid F) &= \frac{P(F \mid M \geq 1) P(M \geq 1)}{P(F)} \\ &= \frac{P(F \mid M \geq 1) P(M \geq 1)}{\underbrace{P(F \mid M \geq 1) P(M \geq 1)}_{\leq (3/4)^r} + \underbrace{P(F \mid M = 0) P(M = 0)}_{=1}}. \end{aligned}$$

Nur mit *a priori* Wissen über die Wahrscheinlichkeiten

$$p = P(M = 0), \quad 1 - p = P(M \geq 1),$$

ist eine sinnvolle Aussage der gewünschten Art möglich!

Beispiele

- $p = 0$. Hier gilt: $P(M \geq 1 \mid \text{kein Erfolg nach } r \text{ Versuchen}) = 1$.
- $p = 1/2$. Dies entspricht maximaler *Unentschiedenheit* zwischen den beiden Alternativen $M = 0$ oder $M \geq 1$. Es gilt:

$$P(M \geq 1 \mid \text{kein Erfolg nach } r \text{ Versuchen}) \leq \frac{(3/4)^r}{1 + (3/4)^r} \simeq (3/4)^r.$$

Diese Wahl von p ist wohl der „instinktive“ Hintergrund des Fehlschlusses in (8.3-9).

Satz (Boyer/Brassard/Høyer/Tapp 1996).

Es sei $M = 1$.

Gegeben sei irgendein Quanten-Suchalgorithmus „Brand X“, der k Suchanfragen an das Orakel U_f richtet.

Liegt unabhängig von f nach abschließender Messung eine Erfolgswahrscheinlichkeit von mindestens 50% vor, so ist

$$k \geq c\sqrt{N}(1 + o(1)), \quad c = 0.3244 \dots$$

Bemerkung.

Die untere Schranke $k = \Theta(\sqrt{N})$ ist sogar zwei Jahre *älter* als der Algorithmus von Grover (Bennett/Bernstein/Brassard/Vazirani 1994).

Beweis – der Rahmen.

- eindeutiges Suchergebnis zum Orakel f sei x
- Suchalgorithmus „Brand X“:
 - zusammengesetzt aus Superoperatoren und Suchanfragen
 - Superoperator nach (1.13-11) als unitärer Operator mit anschließender partieller Messung (Ausspuren...) aufgefaßt
 - Teilmessungen werden nach (2.4-8) ans Ende des Algorithmus verschoben
also ist Zustand vor der Messung am Ende des Algorithmus

$$\psi_k^x = V_k (I \otimes U_f) V_{k-1} (I \otimes U_f) \dots (I \otimes U_f) V_1 (I \otimes U_f) V_0 |0\rangle,$$

mit unitären „Zwischenschrittoperatoren“ V_0, \dots, V_k .

Beweis – die Strategie.

Betrachte den Suchalgorithmus „Brand X“ als *Störung* des Orakel-unabhängigen Ablaufs

$$\psi_k = V_k \cdot V_{k-1} \cdot \dots \cdot V_1 \cdot V_0 |0\rangle$$

und studiere die Größe

$$\Delta_k^2 = \sum_x \|\psi_k^x - \psi_k\|^2.$$

- Störungsrechnung (Lineare Algebra): $\Delta_k = O(k)$.
 - Δ_k „zu klein“ macht die ψ_k^x „zu unabhängig“ von x , einen Erfolg „zu unwahrscheinlich“.
- Erfolgswahrscheinlichkeit von mindestens 50% liefert so eine untere Schranke:
 $\Delta_k = \Theta(\sqrt{N})$.

Resultat: $k = \Theta(\sqrt{N})$.

Beweis – die obere Abschätzung.

Zweifache Anwendung der Dreiecksungleichung liefert:

$$\begin{aligned} \Delta_{k+1} &= \left(\sum_x \|(I \otimes U_f)\psi_k^x - \psi_k\|^2 \right)^{1/2} \\ &\leq \left(\sum_x \left(\underbrace{\|(I \otimes U_f)(\psi_k^x - \psi_k)\|}_{=\|\psi_k^x - \psi_k\|} + \underbrace{\|(I \otimes U_f - I)\psi_k\|}_{=2|\langle e_x, \psi_k \rangle|} \right)^2 \right)^{1/2} \\ &\leq \underbrace{\left(\sum_x \|\psi_k^x - \psi_k\|^2 \right)^{1/2}}_{=\Delta_k} + 2 \underbrace{\left(\sum_x |\langle e_x, \psi_k \rangle|^2 \right)^{1/2}}_{\leq \|\psi_k\|=1} \\ &\leq \Delta_k + 2. \end{aligned}$$

Wegen $\Delta_0 = 0$ folgt hieraus sofort $\Delta_k \leq 2k$.

Beweis – die untere Abschätzung.

Zweifache Anwendung der „umgekehrten“ Dreiecksungleichung liefert für ein geeignetes System orthonormierter Vektoren $\{\phi_x\}_x$:

$$\begin{aligned} \Delta_k &= \left(\sum_x \|\psi_k^x - \psi_k\|^2 \right)^{1/2} = \left(\sum_x \|(\psi_k - \phi_x) - (\psi_k^x - \phi_x)\|^2 \right)^{1/2} \\ &\geq \left(\sum_x \left| \|\psi_k - \phi_x\| - \|\psi_k^x - \phi_x\| \right|^2 \right)^{1/2} \\ &\geq \underbrace{\left(\sum_x \|\psi_k - \phi_x\|^2 \right)^{1/2}}_{=E_k} - \underbrace{\left(\sum_x \|\psi_k^x - \phi_x\|^2 \right)^{1/2}}_{=F_k}. \end{aligned}$$

Wir müssen E_k nach unten und F_k nach oben abschätzen.

Beweis – die Abschätzung von E_k nach unten.

Zunächst gilt

$$\|\psi_k - \phi_x\|^2 = 2 - 2\Re\langle\phi_x, \psi_k\rangle \geq 2 - 2|\langle\phi_x, \psi_k\rangle|.$$

Also folgt mit der Cauchy-Schwarz-Ungleichung

$$\begin{aligned} E_k^2 &= \sum_x \|\psi_k - \phi_x\|^2 \geq 2N - 2 \sum_x 1 \cdot |\langle\phi_x, \psi_k\rangle| \\ &\geq 2N - 2 \left(\sum_x 1^2 \right)^{1/2} \cdot \underbrace{\left(\sum_x |\langle\phi_x, \psi_k\rangle|^2 \right)^{1/2}}_{\leq \|\psi_k\|=1} \\ &\geq 2N - 2\sqrt{N} = 2N(1 + o(1)). \end{aligned}$$

Somit $E_k \geq \sqrt{2N}(1 + o(1))$.

Beweis – die Abschätzung von F_k nach oben.

Zunächst gilt

$$\|\psi_k^x - \phi_x\|^2 = 2 - 2\Re\langle\phi_x, \psi_k^x\rangle.$$

Wir müssen also $\Re\langle\phi_x, \psi_k^x\rangle$ nach unten abschätzen.

Hier kommt die Erfolgswahrscheinlichkeit von mindestens 50% ins Spiel:

Die Schluß-Messung.

Nach der allgemeinen Begriffsbildung von „Quanten-Zustand“, „Ergebnis“ und „Messung“ sind den Ergebnissen $x \in X$ paarweise orthogonale ON-Projektoren P_x zugeordnet, für die also gilt

$$\langle P_x \psi_k^x, \psi_k^x \rangle \geq 1/2.$$

Beweis – das Ende.

Spezifizieren wir jetzt das System $\{\phi_x\}_x$ von orthonormierten Vektoren durch $\phi_x = P_x \psi_k^x / \|P_x \psi_k^x\|$, so gilt

$$\langle\phi_x, \psi_k^x\rangle = \langle P_x \psi_k^x, \psi_k^x \rangle^{1/2} \geq 1/\sqrt{2}, \quad \leadsto \quad \|\psi_k^x - \phi_x\|^2 \leq 2 - \sqrt{2},$$

und damit

$$F_k = \left(\sum_x \|\psi_k^x - \phi_x\|^2 \right)^{1/2} \leq \sqrt{2 - \sqrt{2}} \cdot \sqrt{N},$$

Zusammenfassend gilt mit $E_k \geq \sqrt{2N} (1 + o(1))$

$$2k \geq \Delta_k \geq E_k - F_k \geq 2c\sqrt{N} (1 + o(1)), \quad c = \left(\sqrt{2} - \sqrt{2 - \sqrt{2}} \right) / 2,$$

d.h. die Behauptung $k \geq c\sqrt{N} (1 + o(1))$.

Bemerkung.

Falls der Suchalgorithmus „Brand X“ die Erfolgswahrscheinlichkeit maximiert, so hat Zalka 1999 gezeigt, daß gilt

$$k \geq c\sqrt{N}(1 + o(1)), \quad c = \pi/4 = 0.785 \dots$$

Da der Algorithmus von Grover derart „erfolgsmaximal“ ist und im vorliegenden Fall $M = 1$ genau $k \simeq \pi\sqrt{N}/4$ Suchanfragen erfordert, ist er *asymptotisch exakt optimal*.

(8.6-1) GRENZEN VON QUANTEN-ALGORITHMEN

Das Paritätsproblem

Gegeben ein Orakel $f_* : X \rightarrow \{0, 1\}$, d.h. $f = (-1)^{f_*} : X \rightarrow \{-1, +1\}$.

- $|X| = N = 2^n$
- $S = \{x \in X : f_*(x) = 1\} = \{x \in X : f(x) = -1\}$

Orakel kann als Quanten-Black-Box befragt werden, d.h.

$$U_f : |x\rangle \mapsto f(x)|x\rangle$$

liegt als Quantenschaltkreis polynomieller Komplexität vor.

Aufgabe: Ist $|S|$ gerade oder ungerade, d.h. ist

$$\text{par}(f) = \prod_x f(x) = +1 \text{ oder } = -1 ?$$

Klassische Algorithmen. (deterministisch *und* probabilistisch)

- das Ergebnis hängt von allen Antworten $f(x)$, $x \in X$, ab
- weniger als N Anfragen bedeuten, das Ergebnis nur „zu raten“

Komplexität: genau N Anfragen an das Orakel.

Quantenalgorithmen.

- $N = 2$: Deutsch-Jozsa-Algorithmus (3.1-9) liefert Antwort nach *einer* einzigen Anfrage an das Orakel U_f
- $N > 2$: bilde Gruppen von $N/2$ Paaren $\{x_0, x_1\} \curvearrowright$ Fall $N = 2$

Dieser Quantenalgorithmus benötigt genau $N/2$ Anfragen.

...geht es besser? **Nein.**

Satz (Farhi/Goldstone/Gutmann/Sipser 1998).

Gegeben sei *irgendein* Quantenalgorithmus „Parity“, der

$$k < N/2 \text{ Suchanfragen}$$

an das Orakel U_f richtet.

„Parity“ liefere für alle Orakel f die *richtige* Parität mit einer Wahrscheinlichkeit $p_f \geq 50\%$.

Dann gilt:

$$p_f = 50\%$$

Interpretation

Ein brauchbarer Quantenalgorithmus mit $k < N/2$ wäre genauso gut wie „pures Raten“ ohne Befragung des Orakels.

Beweis – der Rahmen.

Wie bei (8.5-2) und (8.5-7) gilt

- Zustand vor der Messung am Ende des Algorithmus „Parity“

$$\psi_f = V_k (I \otimes U_f) V_{k-1} (I \otimes U_f) \dots (I \otimes U_f) V_1 (I \otimes U_f) V_0 |0\rangle$$

- Messung der Parität +1 ist durch einen ON-Projektor P_+ gegeben, so daß gilt

$$\langle P_+ \psi_f, \psi_f \rangle \geq 1/2 \quad \text{für } \text{par}(f) = +1,$$

$$\langle P_+ \psi_f, \psi_f \rangle \leq 1/2 \quad \text{für } \text{par}(f) = -1.$$

Beweis – Fortsetzung.

Spektralzerlegung

$$U_f = \sum_x f(x) P_x, \quad P_x \text{ ON-Projektor auf Basisvektor } |x\rangle.$$

Eingesetzt in die Messwahrscheinlichkeit $\langle P_+ \psi_f, \psi_f \rangle$:

$$\begin{aligned} \langle P_+ \psi_f, \psi_f \rangle &= \sum_{x_1} \dots \sum_{x_{2k}} \langle 0 | V_0^\dagger P_{x_1} V_1^\dagger \dots V_{k-1}^\dagger P_{x_k} V_k^\dagger \cdot P_+ \\ &\quad \cdot V_k P_{x_{k+1}} V_{k-1} \dots V_1 P_{x_{2k}} V_0 |0\rangle \cdot \prod_{j=1}^{2k} f(x_j) \\ &= \sum_{x_1} \dots \sum_{x_{2k}} \alpha_{x_1 \dots x_{2k}} \cdot \prod_{j=1}^{2k} f(x_j), \end{aligned}$$

mit von f unabhängigen Koeffizienten $\alpha_{x_1 \dots x_{2k}}$.

Beweis – Fortsetzung.

Demnach gilt

$$\begin{aligned} \sum_{f:\text{par}(f)=+1} \underbrace{\langle P_+ \psi_f, \psi_f \rangle}_{\geq 1/2} &- \sum_{f:\text{par}(f)=-1} \underbrace{\langle P_+ \psi_f, \psi_f \rangle}_{\leq 1/2} \\ &= \sum_f \text{par}(f) \langle P_+ \psi_f, \psi_f \rangle \\ &= \sum_{x_1} \cdots \sum_{x_{2k}} \alpha_{x_1 \dots x_{2k}} \cdot \underbrace{\sum_f \text{par}(f) \prod_{j=1}^{2k} f(x_j)}_{=0 \text{ für } 2k < N} = 0. \end{aligned}$$

Wäre auf der Seite ganz links auch nur eine Ungleichung bzgl. $1/2$ strikt, so wäre diese Seite echt größer 0.

Also gilt $\langle P_+ \psi_f, \psi_f \rangle = 1/2$ für alle f .

Beweis – Ende.

Für $2k < N$ gilt

$$\sum_f \text{par}(f) \prod_{j=1}^{2k} f(x_j) = \sum_f \prod_{x \in X} f(x) \prod_{j=1}^{2k} f(x_j) = 0.$$

Denn es gibt mindestens ein $x_* \in X$, welches nur *ein einziges* Mal in dem Doppelprodukt als Argument von f auftaucht. Nun gibt es zu jedem f genau einen Partner f' , welcher sich *nur* im Vorzeichen beim Argument x_* unterscheidet, so daß

$$\prod_{x \in X} f(x) \prod_{j=1}^{2k} f(x_j) + \prod_{x \in X} f'(x) \prod_{j=1}^{2k} f'(x_j) = 0$$

Arrangiert man die Summe über alle f als Summe über alle verschiedenen Paare (f, f') , so folgt die Behauptung.