Inhaltsverzeichnis

7. Juli 2022

Vorbemerkungen

Kein Buch! Nur zum Gebrauch neben der Vorlesung bestimmt! Vor Druck- und anderen Fehlern wird gewarnt!!!

Voraussetzung: Theoretische Quantenmechanik. In dieser Vorlesung werden aber hauptsächlich die Punkte betont, die für QC nötig. Dies bringt einige Vereinfachunge technischer Natur (i. A endlich dimensionale Räume und beschränkte Operatoren), aber die begrifflichen Aspekte der QM werden hier sehr viel stärker in den Vordergrund gerückt:

- **Grössere Reichhatigkeit der Information** (Stichwort Qubit vs. Bit) und vor allem Dingen die
- **Parallelität der Information** (Stichwort: Überlagerung, Verschränkung *entanglement*)

Klasische Bücher:

W. Heisenberg
"Die Physikalischen Prinzipien de Quantentheorie" (1928, 2. 1931) Leipzig 1928 (2. 1931) [?] Heisenberg30

H. Weyl, "Gruppentheorie und Quantenmechanik" Leipzig 1928 (2. 1931)

J. von Neumann
"Mathematische Grundlagen der Quantenmechanik" (1932) Berlin 1932

P A M Dirac
"The Principles of Quantum Mechanics" (1930, 4. 1957) Oxford 1930 (4. 1957)

Auch in den spezialisierten Büchern zum QC finden sich Abschnitte über die QM allgemein, manchmal mit mehr Rücksicht auf Informatiker als auf Physiker.

Kapitel 1

Quantenmechanik, allgemein

1.1 Mini-Geschichte

Dies ist keine Geschichte der QM, sondern nur eine kurze Orientierung zur Einordnung der neueren Entwicklung in Richtung QC.

> "If there is any moment that marks the birth of quantum mechanics, it would be the vacation taken by the young Werner Heisenberg [?, ?] [1] in 1925" (S. Weinberg) .

Heisenberg schreibt kurz und bündig:

> "In der Arbeit soll versucht werden, Grundlagen zu gewinnen für eine quantentheoretische Mechanik, die ausschliesslich auf Beziehungen zwischen prinzipiell beobachtbaren Grössen basiert ist."

Die beobachtbaren Grössen (z.B. Energieniveaux eines Atoms) werden in Tabellen (Vektoren) angegeben. Auf diese wirken Matrizen, daher der frühe Name für die QM: Matrizenmechanik.

Dies erforderte für ein System wie das H-atom schon äusserst komplizierte Rechnung, eine gewaltige Vereinfachung erfolgte durch die Schrödinger-Gleichung [?] [2].

Bald wurde die Gleichwertigkeit der beiden Zugänge durch die damals besonders in Göttingen entwickelte Funktionalanalysis aufgedeckt: Hilbertraum kann durch Funktionen (Wellenfunktionen von Schrödinger) oder Vektoren (von Heisenberg, Born, Jordam und Pauli), die Operatoren sind bei Heisenberg Matrizen, bei Schrödinger Funktionsoperationen wie Ableitungen, Multiplikation mit Variablen etc.

[1] W. Heisenberg: Über quantentheoretische Umdeutung kinematischer und mechanischer Beziehungen

[2] E. Schrödinger: Quantisierung als Eigenwertproblem

	Hilbertraum		C^*	Phasenraum
	1925	1926	1932	< 1925
	Heisenberg	Schrödinger	v. Neumann	klassisch
Observable	Matrizen	$\partial_x, x \cdots$	$\in C^*$	$F(p,q)$
Zustände	Vektoren	Funktionen	$\in C^*$	$\rho(p,q)$
Mathem.	Lin. Algebra.	Funkt. Anal.	lin. Algebra	Diff-Int. Rechn.

Die formale Entwicklung der Quantenmechanik wurde weitgehend abgeschlossen durch John von Neumanns Buch: Mathematische Grundlagen der Quantenmechanik (1932).

Neben der klaren mathematischen Darstellung war ein äusserst wichtiger Beitrag des Mathematikers John von Neumann die Einführtung der gemischten Zustände, durch den statistischen Operator. Dieser Zugang führtte zu der recht abstrakten Formulierung der QP im Rahmen der abstrakten C^*-Algebren, die besonders bei Mathematikern sehr beliebt ist.

Der Schrödinger'sche Zugang brachte grosse technische Erleichterungen:

1) Gewaltige Vereinfachung beim Rechnen, Anstelle vom Manipulationen mit unendlichdimensionalen Matrizen traten übliche Funktionaloperationen wie Differentiation oder Multiplikation. Allerdings spielt im QC heute wieder der Matrixformalismus die füHilberträumende Rolle.

2) Das Korrepondenzprinzip, das erlaubt die klassischen Ausdrücke in quantenmechanische Operatoren zu überfüHilberträumen, liess sich leicht anwenden: z.B. Hamiltonfunktion $H(p,q) \to \mathbf{H}(p,q)$ durch $p \to -i\hbar\partial_q; q \to q\cdot$

3) Die Gleichungen waren im Funktionalzugang auch formal näher bei den vertrauten Ausdrücken aus der klassischen Physik als die Matrizen. Es handelt sich in der Schrödinger'schen Darstellung hauptsächlich partielleum Differentialgleichungen, wie in Elektrodynamik und Kontinuumsmechanik.

Diese formale Nähe zur klassischen Physik verstärkte den prinzipiellen Skeptizismus einiger Physiker, die wie Schrödinger und Einstein, im Herzen auf eine Rückkehr zur klassischen Physik hofften.

Besonders die Aspekte, die heute für das QC wesentlich sind, wie die Statistische Imterpretation, die Verschränkung und die daraus resultierende "Teleportartion" erregten dagegen Misstrauen, darauf gehen wir später nochmals ein (Schrödingersche Katez und Einstein, Podolski, Rosen Paradoxon)

Die Quantenphysik, die sich nach 1925 nicht als eine blosse EinscHilbertraumänkung der klassischen Physik, sondern als eine sehr viel weiter reichende Alternative zur klassischen Physik (Mechanik und Elektrodynamik) erwies, ist vielleicht die physikalische Theorie, die unser Leben am stärksten beeinflusst hat. Sie zeitigte gewaltige Erfolge, nicht nur in Atomphysik, für die sie hauptsächlich entwickelt wurde, sondern besonders auch in Festkörperphysik. Ein typische Frucht der Quantenphysik ist der Transistor [3]

Als Gamow 1928 den α-Zerfall der Kerne mit Hilfe der QM erklären konnte, war es noch eine Überraschung, dass diese auch in der Grössenordnung der Kernradien ($\approx 10^{-12}$ cm)

[3] J Bardeen, W Shockley and W Brattain 1948.

gültig ist. Bei der subnuklearen Physik (Teilchenphysik) erwartete man die Gültigkeit schon, aber es gab durchaus auch eine Epoche, in der man zwar nicht an der Gültigkeit der QP (in der Form der QFT) zweifelte, wohl aber an iHilberträumem Nutzen für viele Aspekte der Teilchenphysik [4].

Inzwischen ist allerdings die QFT wieder voll auferstanden und es gibt keine Gründe an IHilbertraum zu zweifeln bis hinab zu Grössenordnungen von $\approx 10^{-35}m$ (Planck Länge), denn ein noch offenes Problem ist allerdings die Vereinigung von Quantenphysik und Allgemeiner Relativitätstheorie.

Die praktischen Hauptbrobleme entsteht dadurch, dass viele Operatoren nicht beschränkt sind, was zu "nicht-normierbaren Eigenfunktionen" (Eigendistributionenen) in der QM führtt und zu Unendlichkeiten in der relativistischen QFT (Renormierungsprobelm). Von all diesen Problemen is das QC nicht berüHilbertraumt, da man sich hier auf endlichdimensionale Hilberträume beschränkt.

Die Beschäftigung mit den mehr grundsätzlichen Problemen die beim Übergangs von der klassischen Physik, an die wir durch unsre Anschauung gewöhnt sind, zur weniger anschaulichen QM hat in der jüngeren Zeit wieder zugenommen. Dies hat einen wesentlichen Grund in der experimentellen Entwicklung in der Atomphysik: Es gab grosse FortscHilbertraumitte in der Kühltechnik (man kommt immer näher zu $T = 0$) und es war möglich einzelne QM Systeme zu isolieren (Ionenfallen). (Paul und Dehmelt, Nobelpreis 1989, Haroche und Wineland, Nobelpreis 2012)

Entscheidend war auch die Entwicklung der Quantenoptik durch Laser.

Dies fürte auch zu einem verstärkten Interesse an den grundsätzlichen (manchmal etwas abschätzig "philosophisch" genannten) Problemen der QM; s. z. B. zu den Bellsche Ungleichungen. Das Ergebnis einiger Präzisionsexperimente in dieser Richtung hat die Mehrzahl der Physiker allerdings nicht überrachet:

Das Ergebnis war nämlich: **Die QM ist richtig !**

Ein grosser Spin-off Effekt dieser Entwicklung in der Atomphysik war das Quanten-Computing (QC) [5]

Gegenwärtig kann man das QC als Rückkehr zur Heisenbergschen Matrizenmechanik bezeichnen. Es ist aber rechnerisch sehr einfach, da die auftretenden Matrizen endlich dimensional sind, die Grundeinheit, das Qubit ist nur 2 dimensional. Der Durchbruch zum QC kam hier auch keinesfalls durch neue Einsichten in die QM, sondern durch die Entwicklung von Algorithnmen, die auf einfachen Prinzipien der QM beruhen.

Zu erwähnene ist hier besonders der Algorithmus von Shore, der komplexe Zahlentheoretische Theoreme zusammen mit Algorithmen, die auf den Prinzipien der QM basieren, zur Primzahlfaktorisierung benutzt.

Genauso wichtig war der ForscHilbertraumitt in der experimentellen Technik, die es erlaubt Systeme von Qubits über eine nützliche Zeit kohärent zu halten. Allerdings können wir

[4] Quantum field theory will not die, but just fade away, G Chew ca 1950

[5] Richard P Feynman. Simulating physics with computers, 1981. International Journal of Theoretical Physics, 21(6/7). Yuri Manin. Computable and Uncomputable. Sovetskoye Radio, Moscow, 128, 1980.

auf diesen wichtigen Aspekt in dieser Vorlesung, aus Mangel an Zeit und Expertise, nicht eingehen.

1.2 Allgemeine Grundlagen

1.2.1 Einige grundlegende mathematische Konzepte

Nur eine kurze Erinnerung und Wiederholung.

1.2.1.1 1) Hilbertraum $\mathcal{H}$

Ein Hilbertraum ist ein **vollständiger linearer Vektorraum mit Metrik (Skalarprodukt)**. Wir stellen mit Dirac ein Element davon durch einen "ket" $|\cdot\rangle$ dar. Es gilt das Superpositionsprinzip:

$\{|\psi\rangle, |\phi\rangle \cdots\} \in \mathcal{H}; \qquad \alpha, \beta \cdots \in \mathcal{C} \rightarrow, \alpha|\psi\rangle + \beta|\phi\rangle \in \mathcal{H};$

Für das Scalarprodukt gilt:

$\mathcal{H} \times \mathcal{H} \rightarrow \mathcal{C}$ bezeichnet mit $\langle\phi|\psi\rangle \in \mathcal{C}$

Schiefsymmetrisch (skew symmetric): $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$

Positiv $\langle\psi|\psi\rangle > 0 \; \forall \; |\psi\rangle \neq 0 \quad ||\psi|| = \sqrt{\langle\psi|\psi\rangle}$ heist **Norm** des Vektors $|\psi\rangle$.

Linear $\langle\phi|(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) = \alpha\langle\phi|\psi_1\rangle + \beta\langle\phi|\psi_2\rangle$

Nach Dirac wird der duale Vektor (der der links im Skalarprodukt steht) mit bra, $\langle\cdot|$ bezeichnet. Das Skalarprodukt hat also die Form *bra ket*: $\langle\cdot|\cdot\rangle$

Vollständigkeit] Der $\mathcal{H}$ is vollständig in der Norm, d.h. jede Cauchyfoge im $\mathcal{H}$ convergiert gegen ein Element des $\mathcal{H}$ [6]

Basis eines $\mathcal{H}$

Es gibt eine abzählbare Zahl von Basis-Vektoren. In den für das QC wesentlichen Hilberträumen ist diese Zahl endlich, dh. es gibt endlich viele Basisvektoren:

$$|1\rangle, |2\rangle, \cdots |N\rangle \tag{1.1}$$

als deren Summe jedes Element dargestellt werden kann:

$$|\phi\rangle = \sum_1^N \alpha_i \, |i\rangle \tag{1.2}$$

[6] Im QC spielen i. A. nur endlichdimensionale $\mathcal{H}$ eine Rolle, daher ist das Vollständigkeitsaxiom, das in der allgemeinen QM eminent wichtig ist, hier trivial.

Wir können ohne BescHilbertraumänkung der Allgemeinheit annehmen, dass die Basis orthonormal ist, d.h.

$$\langle i|k\rangle = \delta_{ik} \tag{1.3}$$

dann gilt: $\alpha_i = \langle i|\phi\rangle$ und wir haben allgemein:

$$|\phi\rangle = \sum_i \langle i|\phi\rangle\,|i\rangle \equiv \sum_i |i\rangle\langle i|\phi\rangle \tag{1.4}$$ z1

d.h.

$$\sum_i |i\rangle\langle i| = 1 \tag{1.5}$$ z2

Wenn ein vollständiges System nicht orthogonal ist, können wir es orthonormaliseren (VerfaHilberträumen von E. Schmidt):

$$\begin{aligned}
|\tilde{\psi}_1\rangle &= \frac{1}{\|\psi_1\|}|\psi_1\rangle \\
|\hat{\psi}_2\rangle &= |\psi_2\rangle - \langle\tilde{\psi}_1|\psi_2\rangle|\tilde{\psi}_1\rangle;\ |\tilde{\psi}_2\rangle = \frac{1}{\|\hat{\psi}_2\|}\hat{\psi}_2 \\
&\vdots \\
|\hat{\psi}_N\rangle &= |\psi_N\rangle - \sum_{i=1}^{N-1}\langle\tilde{\psi}_i|\psi_N\rangle;\ |\tilde{\psi}_N\rangle = \frac{1}{\|\hat{\psi}_N\|}|\hat{\psi}_N\rangle
\end{aligned} \tag{1.6}$$

Die neuen Vektoren

$$|\tilde{\psi}_1\rangle, |\tilde{\psi}_2\rangle, \cdots |\tilde{\psi}_N\rangle \tag{1.7}$$

bilden eine orthonormale Basis (vollständiges Orthonormalsystem **voS**

Strahl Ein Strahl (ray) im $\mathcal{H}$ ist der eindimensionale Unterraum von Vektoren, die sich nur durch einen komplexen Faktor $\alpha \neq 0$ unterscheiden. Normalerweise wählt man als den Representatnten dieser Klasse den Vektor aus, der die Norm 1 hat.

Direktes Produkt Das direkte Produkt zweier Hilberträume, $\mathcal{H}_A \otimes \mathcal{H}_B$ ist ein Hilbertraum, der alle geordneten Paare $|\psi\rangle_A, |\phi\rangle_B$ von Vektoren aus $\mathcal{H}_A$ und $\mathcal{H}_B$ und deren Summen enthält. Das Skalarprodukt eines solchen Paares ist Produkt der Skalaarprodukte:

$$\langle(\langle\psi|_A \otimes \langle\phi|_B)\,|(|\chi\rangle_A \otimes |\xi\rangle_B)\rangle = \langle\psi|\chi\rangle_A\,\langle\phi|\xi\rangle_B \tag{1.8}$$

Am einfachsten werden die Eigenschaften über die Orthonormalbasen beschrieben: Seien $\{|\psi_n\rangle_A\}$ und $\{|\phi_n\rangle_B\}$ solche Ortonormalbasen. Dann ist
$|m,n\rangle_{AB} = |\psi_m\rangle_A \otimes |\phi_n\rangle_B$ eine Orthonormalbasis von $\mathcal{H}_A \otimes \mathcal{H}_B$ mit dem Slalarprodukt

$$\langle m', n'|m, n\rangle_{AB} = \langle m'|m\rangle_A\,\langle n'|n\rangle_B = \delta_{m'm}\,\delta_{n',n} \tag{1.9}$$

Ein allgemeiner Zustand aus $\mathcal{H}_A \otimes \mathcal{H}_B$ ist demnach:

$$|\chi\rangle_{AB} = \sum_{m,n} \alpha_{m,n}|m,n\rangle_{AB} \tag{1.10}$$

Für endlichdimensionale Hilberträume gilt: $dim(\mathcal{H}_A \otimes \mathcal{H}_B) = dim(\mathcal{H}_A) \cdot dim(\mathcal{H}_b)$

Das direkte Produkt lässt sich assoziativ auf N Hilbertraum erweitern

$$(\mathcal{H}_1 \otimes \mathcal{H}_2) \otimes \mathcal{H}_3 = \mathcal{H}_1 \otimes (\mathcal{H}_2 \otimes \mathcal{H}_3) \equiv \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 \tag{1.11}$$

und allgemein

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \mathcal{H}_N \tag{1.12}$$

hat dann die Orthonormalbasis

$$|m_1, m_2 \cdots m_N\rangle = |m_1\rangle \otimes |m_2\rangle \otimes \cdot \otimes |m_N\rangle \tag{1.13}$$

Für endlichdimensionale Hilberträume gilt:
$dim(\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \mathcal{H}_N) = dim(\mathcal{H}_1) \cdot dim(\mathcal{H}_1) dim(\mathcal{H}_2) \cdots dim(\mathcal{H}_N)$

Im QC wird i. A. ein Hilbertraum betrachtete, der das direkte Produkt von N 2-dimensionalen Hilberträumen ist (Qubits). Dieser beschreibt dann einen Raum von der Dimension 2^N, d.h. die Zahl der Dimensionen wächst exponentiell mit der Zahl der Qubits.

1.2.1.1.1 Beispiel für direkte Produkte in der QM : Direkte Produkte von Hilberträumen spielen in der Physik eine eminent wichtige Rolle.

Das vielleicht einfachste Beispiel dafür sind zwei Spin $\frac{1}{2}$ Teilchen: Für ein Teilchen gibt es den 2-dim Hilbertraum $\mathcal{H}_2$ mit z. B. den Basisvektoren $|\uparrow_z\rangle$, $|\downarrow_z\rangle$ Der Spin von 2 Teilchen (z.B. Hülle des He-Atoms) wird in dem direkten Produkt $\mathcal{H}_2 \otimes \mathcal{H}_2$ beschrieben. Ein Quantencomputer ist, zumindest zur Zeit, in einem direkten Produkt von N 2-dimensionalen Hilberträumen realisiert.

1.2.1.2 2)Lineare Operatoren

Bemerkung: Meist nimmt man in der Physik Linearität an, um die Probleme zu vereinfachen, z.B. beim Hooke'schen Gesetz. Es ist bemerkenswert, dass in der QM lineare Operatoren eine fundamentale Rolle spielen. Nichtlinearitäten bei den Operatoren, die in den deduktiven Aufbau der QM eingehen, müssen, wenn überhaupts sehr sehr klein sein, da sie zu messbaren Abweichungen z. B. in der Atomphysik mit iHilberträumer ungeheuren Präzision führtten. Auch für das QC is die Linearität der Operatoren wesentlich.

$\mathbf{A}$, $\mathbf{B} \cdots$ Lineare Abb im in einem Raum, für unsre Zwecke ein Hilbertraum $\mathcal{H}$: $\mathcal{H} \to \mathcal{H}$.

$$\mathbf{A} : |\psi\rangle \mapsto \mathbf{A}|\psi\rangle; \quad \mathbf{A}(\alpha|\psi_1\rangle + \beta|\psi_2\rangle = \alpha\mathbf{A}|\psi_1\rangle + \beta\mathbf{A}|\psi_2\rangle$$
$$(\mathbf{A} + \mathbf{B})|\psi\rangle = \mathbf{A}|\psi\rangle + \mathbf{B}|\psi\rangle; \ (\mathbf{AB})|\psi\rangle = \mathbf{A}(\mathbf{B}|\psi\rangle)$$

Der **adjungierte** Operator $\mathbf{A}^\dagger$ zu $\mathbf{A}$ ist definiert durch:

$$\langle \mathbf{A}^\dagger \phi | \psi \rangle = \langle \phi | \mathbf{A} \psi \rangle \tag{1.14}$$

Ein Operator ist **selbstadjungiert oder hermitisch**, wenn

$$\mathbf{A} = \mathbf{A}^\dagger \tag{1.15}$$

und **unitär** wenn

$$\mathbf{A}^{-1} = \mathbf{A}^{\dagger} \tag{1.16}$$

Ein unitärer Operator erhält das Skalarprodukt:

$$\langle \mathbf{A}\phi | \mathbf{A}\psi \rangle = \langle \mathbf{A}^{\dagger}\mathbf{A}\phi | \psi \rangle = \langle \mathbf{A}^{-1}\mathbf{A}\phi | \psi \rangle = \langle \phi | \psi \rangle \tag{1.17}$$

Ein Matrix-Operator $\mathbf{A} = \begin{pmatrix} A_{11} & A_{12} & \cdots \\ A_{21} & A_{22} & \cdots \\ A_{31} & A_{32} & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}$

ist selbstadjungiert (hermitisch), wenn gilt $A_{ik} = A^*_{ki}$

ist unitär wenn Zeilen und Spalten orthonormal sind:
$\sum_k A^*_{ki} A_{kl} = \delta_{il}$ und $\sum_k A^*_{ik} A_{lk} = \delta_{il}$

Ein **Projektionsoperator** $\mathbf{P}_{\psi} = |\psi\rangle\langle\psi|$ is die Abbildung auf ein Element des Hilbertraum:

$$\mathbf{P}_{|\psi\rangle} : |\phi\rangle \mapsto \langle\psi|\phi\rangle\,|\psi\rangle \tag{1.18}$$ project

Eigenwerte und die Spektraldarstellung

Ist die Wirkung eines Operators $\mathbf{E}$ auf einen Zustand $|\psi\rangle$ eine Multiplikation mit der Zahl E, d.h.

$$\mathbf{E}|\psi\rangle = E\,|\psi\rangle \tag{1.19}$$

dann heisst $|\psi\rangle$ Eigenvektor von $\mathbf{E}$ und E Eigenwert. Gibt es meHilberträumere linear unabhängige Eigenvektoren zu dem gleichen Wert von E, so ist der Zustand entartet. Sind ein oder meHilberträumere Eigenwerte entartet, so können die zugehörigen Eigenvektoren orthonormalisiert werden, z. B. nach E.Schmidt, (1.6).

Eine der Grundlagen der QM ist die Spektraldarstellung:

Die Eigenvektoren eines (beschränkten) unitären Operators bilden eine Orthonormalbasis [7]

Danach lässt sich jeder Vektor aus $\mathcal{H}$ als Summe von der Eigenvektoren darstellen: $|n\rangle$ mit $\mathbf{E}|n\rangle = E_n|n\rangle$ darstellen:

$$|\phi\rangle = \sum_n \rho_n\,|n\rangle \quad \text{with } \rho_n = \langle n|\phi\rangle \tag{1.20}$$

Im allgemeinen ist die Summe unendlich, in Anwendungen des QC aber endlich.

Man kann den Operator $\mathbf{E}$ darstellen als die Summe von Projektionsoperatoren auf die Eigenvektoren:

$$\mathbf{E} = \sum_n E_n\,|n\rangle\langle n| \tag{1.21}$$ sd

Denn $\mathbf{E}|\phi\rangle = \sum_n \langle n|\phi\rangle \mathbf{E}|n\rangle = \sum_n E_n\,|n\rangle\langle n|\phi\rangle$

[7] Viele wichtige Operatoren der QM sind nicht beschränkt und dann muss die Spektraldarstellung erweitert werden, z. B. durch Distributionen im Gelfandschen Raumtrippel. Beispiele sind die Eigendistribution des Ortsoperators, $\delta(x-a)$ oder des Impulsoperators $e^{i\,px}$.

Das **direkte Operatorprodukt** $\mathbf{M}_A \otimes \mathbf{N}_b$ wirkt im direkten Produkt $\mathcal{H}_A \otimes \mathcal{H}_B$:

$$(\mathbf{M}_A \otimes \mathbf{N}_B)(|\psi\rangle_A \otimes |\phi\rangle_B) = \mathbf{M}_A|\psi\rangle_A \otimes \mathbf{N}_B|\phi\rangle_B \tag{1.22}$$

Auch das direkte Operatorprodukt lässt sich assoziativ erweitern, ganz analog zum direkten Produkt der Hilberträume.

Es wirkt dann auf die Basisvektoren des entsprechenden direkten Produktes der Hilberträume:

$$\mathbf{A}_1 \otimes \mathbf{A}_2 \otimes \cdots \mathbf{A}_N|m_1, m_2 \cdots m_N\rangle = \mathbf{A}_1|m_1\rangle \otimes \mathbf{A}_2|m_2\rangle \otimes \cdots \mathbf{A}_N|m_N\rangle \tag{1.23}$$

Matrixdarstellung von Operatoren

Man kann die Koeffizienten der Entwicklung nach einem einem voS $\{|1\rangle, \cdots, |n\rangle, \cdots |N\rangle\}$ als Koordinaten kartesischer Vektoren mit komplexen Koordinaten wählen,

$$|\psi\rangle = \sum_n^N \langle n|\psi\rangle\, |n\rangle \Leftrightarrow \begin{pmatrix} \langle 1|\psi\rangle \\ \langle 2|\psi\rangle \\ \vdots \\ \langle N|\psi\rangle \end{pmatrix} \equiv \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_N \end{pmatrix} \tag{1.24}$$

In der Koordinatendarstellung ist ein linearer Operator eine Matrix:

$$\mathbf{A} \Leftrightarrow \begin{pmatrix} \langle 1|\mathbf{A}1\rangle & \langle 1|\mathbf{A}2\rangle & \cdots & \langle 1|\mathbf{A}N\rangle \\ \langle 2|\mathbf{A}1\rangle & \langle 2|\mathbf{A}2\rangle & \cdots & \langle 2|\mathbf{A}N\rangle \\ \vdots & \vdots & \vdots & \vdots \\ \langle N|\mathbf{A}1\rangle & \langle N|\mathbf{A}2\rangle & \cdots & \langle N|\mathbf{A}N\rangle \end{pmatrix} \equiv \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1N} \\ A_{21} & A_{22} & \cdots & A_{1N} \\ \vdots & \vdots & \vdots & \vdots \\ A_{N1} & A_{N2} & \cdots & A_{NN} \end{pmatrix} \tag{1.25}$$

$$\text{Bew: } \langle k|\mathbf{A}|\psi\rangle = \langle k|\mathbf{A} \underbrace{\sum_n |n\rangle\langle n}_{\mathbf{I}}\, |\psi\rangle = \sum_n A_{kn}\psi_n$$

Die Matrizen die von einem Operator $\mathbf{A}$ durch zwei verschiedene voS erzeugt werden, sind unitär ähnlich, da zwei verschiedene voS eines Raumes durch eine unitäre Operation verknüpft sind.

Bew. A) Seien $\{|k\rangle_R\}$ und $\{|k\rangle_S\}$ zwei verschiedene voSe. Sei $|k\rangle_R = \mathbf{W}|k\rangle_S$

Dann gilt ${}_R\langle j|k\rangle_R =_S \langle j|W^\dagger|W|k\rangle_S = \delta_{jk}$ Daraus folgt $W^\dagger W = \mathbf{I}$, d.h. W ist unitär.

$${}_R\langle j|\mathbf{A}|k\rangle_R =_S \langle j|W^\dagger \mathbf{A} W|k\rangle_S \tag{1.26}$$

In der Produktbasis zweier (oder meHilberträumer) Hilberträume verlangt eine Darstellung der Operatoren als Matrizen (2-fach indizierte Tensoren) eine lineare Anordung der Vektoren, z.B. nach dem Diagonalschema. Dies hatten wir schon in der letzten Stunde bei Herrn

Marquard gesehen, z.B. wenn bei $|m,n\rangle$ die erste Basisi $|m\rangle = \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$ und die zweite $|n\rangle = \begin{pmatrix} q_0 \\ q_1 \end{pmatrix}$, dann

$$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \otimes \begin{pmatrix} q_0 \\ q_1 \end{pmatrix} = \begin{pmatrix} p_0 q_0 \\ p_0 q_1 \\ p_1 q_0 \\ p_1 q_1 \end{pmatrix} \tag{1.27}$$

Es gibt aber auch dem Problem angemessenere Darstellungen, z. B. die Computatorische Basis, die wir noch ausführtlich betrachten werden.

1.2.1.2.1 Spur . Die Spur einer Matrix ist die Summe über die Diagonalelemente:

$$\mathrm{Tr}(\mathbf{A}) = \sum_k A_{kk} = \sum_k \langle k|\mathbf{A}|k\rangle \tag{1.28}$$

Die Spur ist zyklisch, wie man leicht nacHilberträumechnet.

$$\mathrm{Tr}(\mathbf{A}\,\mathbf{B}\,\mathbf{C}) = \sum_{ikm} A_{ik}B_{km}C_{mi} = \sum_{ikm} C_{mi}A_{ik}B_{km} = \ \mathrm{Tr}(\mathbf{C}\,\mathbf{A}\,\mathbf{B}) \tag{1.29}$$

Daraus folgt: Die Spur ist vom gewählten voS unabhängig. Denn zwei voSe, $\{|k_{(R)}\rangle\},\ \{|j_{(S)}\rangle\}$ sind durch einen unitäre Operator verbunden, d.h.

$$\mathrm{Tr}_R\mathbf{A} =_R \langle j|\mathbf{A}|j\rangle_R =_S \langle j|W^\dagger\mathbf{A}W|j\rangle_S = \ \mathrm{Tr}_S\mathbf{W}^\dagger\mathbf{A}\mathbf{W} = \ \mathrm{Tr}_S\mathbf{W}\mathbf{W}^\dagger\mathbf{A} = \ \mathrm{Tr}_S\mathbf{A} \tag{1.30}$$

Funktionen von Operatoren Wenn eine Funktion eine Reihenentwicklung besitzt, so kann eine Funktion von Operatoren über diese Reihenentwicklung definiert werden.

$$f(x) = \sum_n f_n x^n \to f(\mathbf{A}) = \sum_n f_n \mathbf{A}^n \tag{1.31}$$

Ist $\mathbf{A}$ selbstadjungiert und hat daher ein voS von Eigenvektoren $|n\rangle$, s. (1.21) mit den Eigenwerten a_n , dann kann man die Operatorfunktion über: $f(\mathbf{A})|n\rangle = f(a_n)\,|n\rangle$ auch ohne Reihendarstellung definieren.

$$f(\mathbf{A})|\phi\rangle = f(\mathbf{A})\sum_n \langle n|\phi\rangle\,|n\rangle = \sum_n f(a_n)\,\langle n|\phi\rangle\,|n\rangle \tag{1.32}$$

Man kann daraus die wichtige Beziehung herleiten: Die Exponentialfunktion von i mal einem sa. Operator ist ein unitärer Operator.

Sei $\mathbf{E}^\dagger = \mathbf{E}$. Dann ist $\mathbf{U} = e^{i\mathbf{E}}$ ein unitärer Operator.

1.2.2 Mathematisch deduktiver Aufbau der QM.

Für das QC ist der **mathematische Aufbau der QM** entscheidend. Seine Grundzüge gehen weitgrhend auf den grossen Mathematiker und Mitbegründer der Informatik, John von Neumann (1903-1957) zurück. Dies braucht Ihnen abre keineswegs Angst einzujagen, denn die Anwendungen im QC beruhen, zumindest in der gegenwärtigen Form, durchaus auf sehr einfachen mathematischen Modellen, im wesentlichen auf endlich dimensionalen Räumen.

Im wesentlichen können Sie im QC für Hilbertraum stets endlich dimensionalen Cartesische Raum über den komplexen Zahlen setzten und für Operatoren Matrizen (Matrizes, Matrices).

Da ich von einer Kenntnis der theoretischen QM (z.B. Theorie 4) ausgehe und ich nicht möchte, dass sie sich gleich langweilen, beginne ich unmittelbar mit dem deduktiven Aufbau der sich vielleicht von dem der üblichen Vorlesung nicht in der Sache, wohl aber in der Anordnung unterscheidet. Allerdings wird auch nicht die grösstmögliche Allgemeinheit angestrebt, aber auf mögliche Verallgemeinerungen hinweisen.

Eine der überzeugendsten Darlegungen des mathematischen Aufbaus der QP ist immer noch das Originalwerk John von Neumann's von 1932!!.

1 **Observable** werden in der Quantenphysik durch eine Algebra selbstadjungierter linearer Operatoren in einem Hilbertraum beschrieben.
Die möglichen Messwerte von Observablen sind die Eigenwerte dieser Operatoren.

2 Ein **Zustand** wird in der QP durch einen selbstadjungierten, positiven Operator $\boldsymbol{\rho}$ im Hilbertraum mit der Spur 1 beschrieben (s. Sect. ??[so]). Dieser Operator heisst "**Dichtematrix**" oder **"statistischer Operator"** .
Der **Erwartungswert** einer Observablen $\mathcal{O}$ ist eine lineare Abbildung des Produktes von Zustand mit Observabler auf die reelen Zahlen:

$$\langle\mathcal{O}\rangle = \mathrm{Tr}\rho\,\mathcal{O} = \sum\langle\psi_m|\,\rho\,\mathcal{O}|\psi_m\rangle; \qquad \mathrm{Tr}\rho = \sum\langle\psi_m|\rho|\psi_m\rangle = 1; \tag{1.33}$$

[ew]

wobei $\{\ldots|\psi_m\rangle\ldots\}$ ein **beliebiges** voS in $\mathcal{H}$ ist.
Ist der statistische Operator ein Projektionsoperator auf einen normierten Hilbertraum Vektor $|\phi\rangle$, $\boldsymbol{\rho} = \mathbf{P}_\phi = |\phi\rangle\langle\phi|$, dann nennt man diesen Zustand einen reinen Zustand, der durch den Hilbertraum Vektor $|\phi\rangle$ beschrieben wird.

Anmerkungen

Zu 1:
Im Vergleich dazu: In der klassischen Physik werden Observable und Zustände werden durch (verallgemeinerte) **Funktionen** beschrieben.

Natürlich müssen sowohl die Operatoren in der QP als auch die Funktionen in der klassischen Physik näher spezifiziert werden. Allgemein gilt in der klassischen Physik: (Verallgemeinerte) Funktionen auf dem Phasenraum, z.B. $E = \frac{p^2}{2m}$ für die kietische Energie. $\delta(q-q_0)\,\delta(p-p_0)$ für einen Massenpunkt, $\frac{1}{Z}e^{-E(p,q)/kT}$ für ein kanonisches Ensemble,

In der QP gilt allgemein : Die Operatoren der QP müssen Elemente einer C^* Algebra sein.

Wir verzichten hier auf die grösstmögliche Allgemeinheit und wir verwenden, wie oben bereits getan: Operatoren in einem Hilbertraum. Beim QC auftretende Hilberträume sind sogar noch besonders einfach, sie sind i. A. endlich dimensional und die Operatoren sind endlich dimensionale selbstadjungierte Matrizen.

Ein wesentlicher Unterschied zwischen klassischer und Quanten-Physik besteht darin, dass die Observablen in der KP miteinander vertauschen. Ob ich erst den Impuls messe und dann den Ort ist gleichgültig, da Funktionen miteinander vertauschen: $g(x) \cdot h(x) = h(x) \cdot g(x)$. Dies gilt nicht in der QP, s. Abs. **??**.

Zu 2:
Die im QC auftretenden Operatoren sind i. A. endlich dimensionale Matrizen.

Oft wird der statistische Operator in der QM auf Kosten der "reinen Zustände" etwas stiefmütterlich behandelt, daher einige Anmerkungen.

Da der statistische Operator selbstadjungiert ist, gibt es ein voS $|\psi_n\rangle$ in dem er auch diagonal ist, d.h.

$$\langle\psi_n|\mathbf{O}|\psi_m\rangle = p_n\delta_{nm} \leftrightarrow \mathbf{O} = \sum_n p_n|\psi_n\rangle\langle\psi_n| \tag{1.34}$$

mit $p_n \geq 0, \quad \sum_n p_n = 1$ Der Operator $\mathbf{P}_n = |psi_n\rangle\langle\psi_n|$ ist ein Projektionsoperator auf $|\psi_n\rangle$ denn

$$\mathbf{P}_n|\phi\rangle = \langle\psi_n|\phi\rangle\,|\psi_n\rangle \tag{1.35}$$

Beispiele: Beim Spin $\frac{1}{2}$ sind die reinen Zustände beschrieben durch Spinoren, etwa $\chi_+ = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ oder $\chi_- = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Ein allgemeiner Zustand ist dagegen ein unpolarisiertes Gemisch von + und − Zuständen, beschrieben durch den statistischen Operator $\boldsymbol{\rho} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$. Der statistische Operator für den reinen Zustand $\chi_- = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ist der statistisch Operator $\boldsymbol{\rho} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, der Projektionsoperator auf den Zustand χ_-.

Besonders wichtig ist der statistische Operator in der Quantenstatistik. Hier wird das System aufgespalten in ein Wärmebad der Tempratur T und das untersuchte System, z. B. Gasmoleküle in einem festen Volumen) . Der statistische Operator ist bei fester Temperatur T (kanonisches Ensemble) durch den Hamiltonoperator (Energie-Operator) $\mathbf{H}$ gegeben:

$$\boldsymbol{\rho} = \exp[-\mathbf{H}/(k_BT)]/Z \tag{1.36}$$

k_B ist die Boltzmannkonstante, $Z = Tr\exp[-\mathbf{H}/(k_BT)]$, ist die "Zustandssumme".

In der klassischen Mechanik entspricht dem statistischen Operator eine (ausgedehnte) Verteilungsfunktion im Phasenraum, dem reinen Zustand dagegen δ-Funktionen.

Da besonders im QC die Zusammensetzung von Systemen (Qubits) eine grosse Rolle spielt, wollen wir auch das folgende Axiom separat einfüHilberträumen:

3 Wird ein System durch den Hilbertraum $\mathcal{H}_A$ und ein anderes durch den Hilbertraum $\mathcal{H}_B$ beschrieben, dann wird das Gesamtsystem durch das direkte Produkt $\mathcal{H}_A \otimes \mathcal{H}_B$ beschrieben.

Anmerkungen: Wir werden später nochmals ausfürlich auf zusammengestate Systeme eingehen, besonders im Zusammenhang mit Verschränkung (*entanglement*) und Dekohärenz. Es weden hier nur einige vertraute Beispiele aus der QM gebracht.

Bsp: Sind wir nur an den Atomspektren interessiert, so werden nur die Elektronen quantenmechanisch beschrieben. Der Kern wird als eine klassische Grösse behandelt. Wollen wir allerdings das ganze Atom beschreiben, müssen wir auch noch die Bestandteile des Kerns, die Nukleonen quantenmechanisch beschreiben. Das gesamte Atom wird also in dem Produktraum $\mathcal{H}_{\text{Nukleonen}} \otimes \mathcal{H}_{\text{Elektronen}}$ beschrieben.

Die Behandlung zusammengesetzter Systeme in der QM ist analog zur klassischen Mechanik. Ein Massenpunkt wird dargestellt dort als ein Punkt im 6-dimensionalen Phasenraum R_6 (3 Orts, 3 Impulskoordinaten); für zwei Massenpunkte benötigt man den 12-dimensionalen Phasenraum $R_{12} = R_6 \otimes R_6$.

4 Bei einer **Messung** der Observablen $\mathcal{O}$ geht ein reiner Zustand $|\phi\rangle$ in einen Eigenzustand der Observablen $|\psi_n\rangle$ über d.h. $\mathcal{O}|\psi_n\rangle = O_n|\psi_n\rangle$, das Ergebniss der Messung ist dann O_n (Reduktion der Wellenfunktion). Die Wahrscheinlichkeit für diesen Übergang ist $|\langle\psi_n|\phi\rangle|^2$. Ein Dichteoperator geht in einen Projektionsoperator $P_{|\psi_n\rangle} = |\psi_n\rangle\langle\psi_n|$ über.

Anmerkungen:

Weitere Formulierungen und Erweiterungen des Axioms zur Messung werden, der Vollständigkeit halber, am Ende aufgeführt.

5 Die **zeitliche Entwicklung** (Dynamik) eines Systems von der Zeit t bis t' wird durch einen unitären Operator

$$\mathbf{U}(t,t') = e^{i(t'-t)\mathbf{H}/\hbar} \tag{1.37}$$

zt

beschrieben.Der selbstadjungierte Oierator $\mathbf{H}$ heisst der Hamiltonoperator (Energieoperator) des Systems.

Auch hierauf gehen wir im Abschnitt aa 1.2.3 ausführlicher ein.

Das vielleicht wichtigste physikalische Prinzip zu einer Konstruktion von Hamiltonoperatoren QM ist das:

6 **Korrepondenzprinzip** Man erhält quantenmechanische Observablen aus klassischen, indem man die klassischen dynamischen Variablen durch QM Operatoren ersetzt.

Die drei Orts- und drei Impulsoperatoren eines Teilchen erfüllen die Vertauschungsrelationen:

$$[\mathbf{Q}_j, \mathbf{Q}_k] = 0; \quad [\mathbf{P}_J, \mathbf{P}_k] = 0; \quad [\mathbf{P}_j, \mathbf{Q}_k] = -i\hbar\,\delta_{kl} \tag{1.38}$$

vt

So ist z.B. der Hamiltonoperator für das Elektron im Wasserstoffatom:

$$\mathbf{H} = \frac{1}{2m}\vec{\mathbf{P}}^2 + \frac{e^2}{|\vec{\mathbf{Q}}|} \tag{1.39}$$ HHop

Wie bereits erwähnt, hat bei einem Mehrteilchenproblem jedes Teilchen "seinen eigenen Hilbertraum" und der Hilbertraum für das Gesamte System ist das direkte Produkt der Hilberträume.

1.2.2.0.1 Verallgemeinerung der mathematischen Beschreibung des Messprozesses Für viele realisierbaren Messungen ist das Messaxion in der Form 4 nicht erfüllt. Bei Messungen von Photonen überlebt das Photon den Messprozess i.A. nicht. Im Photomultiplier werden sie z. B. dadurch nachgewiesen, dass sie absorbiert werden. Erst durch die Präzisionsmessungen von Laroche (Nobelpreis 2012) konnten Photonen "zerstörungsfrei" nachgewiesen werden. Der Messprozess spielt auch im QC eine wichtige Rolle, deswegen werden hier zwei weitere, etwas weitergefasste Versionen des Messaxioms 4 zitiert (s. NC, p.84ff), die insbesondere auch Nachweise durch Absorption beschreiben.

4' Jedem Messwert m ist ein Messoperator $\mathbf{M}_m$ zugeordnet. Messungen in der QM werden duch eine Ansammlung von

$$\mathbf{Mess-Operatoren} \quad \{\mathbf{M}_m\} \text{ mit } \sum \mathbf{M}_m^\dagger \mathbf{M}_m = \mathbf{I} \tag{1.40}$$

beschrieben.

Der Messwert für einen Zustand $|\phi\rangle$ nimmt mit einen durch m indizierten Wert mit der Wahrscheinlichkeit

$$p(m) = \langle\phi|\mathbf{M}_m^\dagger \mathbf{M}_m|\phi\rangle \text{ an} \tag{1.41}$$

Der Zustand ist nach der Messung

$$\frac{\mathbf{M}_m|\phi\rangle}{\sqrt{\langle\phi|\mathbf{M}_m^\dagger \mathbf{M}_m|\phi\rangle}} \tag{1.42}$$

Die alternative Fassung des Mess-Axioms, 4' lässt es z.B. zu, dass der Zustand mach der Messung ganz verschwunden ist, z. B. ein Photon im Photomultiplier. Die projektive Messung in (3) ist demnach ein Spezialfall: Die Messoperatoren für die Observable des sa. Operators $\mathbf{E}$ sind seine Eigenwerte von Eigenwert E_m:

$$\mathbf{E}|\Psi_m\rangle = e_k|\Psi_m\rangle \tag{1.43}$$

Wegen der Vollstänigkeit der Eigenwerte gilt:

$$\sum \mathbf{P}_m = 1 \quad \text{mit } \mathbf{P}_m = |\Psi_m\rangle\langle\Psi_m| \tag{1.44}$$

Damit sind die Messoperatoren $\mathbf{M}_m$ gleich den Projektionsoperatoren auf die Eigenzustände.

Für die quantitative probabilistische Interpretation der Messung selbst ist nur das Produkt $\mathbf{M}_m^\dagger \mathbf{M}_m$ nötig, der Einzeloperator $\mathbf{M}$ nur zur Bestimmung des Endzustandes. Verzichtet man auf diese Information, so reicht das Produkt $\mathbf{M}_m^\dagger \mathbf{M}_m$ aus. Dies führtt zu einer weiteren Fassung, dem POVM- Mess-Axiom:

4" **POVM (Positive, operatorvalued measure)** Seien $\mathbf{V}_m$ positive Operatoren mit $\sum_m \mathbf{V}_m = 1$, dies sind die ,,operatorwertigen Masse". Der Messwert für einen Zustand $|\phi\rangle$ nimmt einen durch m indizierten Wert mit der Wahrscheinlichkeit

$$p(m) = \langle\phi||\mathbf{V}_m\phi\rangle \text{ an} \tag{1.45}$$

Wir können uns die Ansammlung der Projektionsoperatoren $\mathbf{P}_k = |\Psi_k\rangle\langle\psi_k|$ aus Axiom 4, die der Messoperatoren M_m aus Axiom 4' oder die der Operatorwertigen Masse V_m von 4" als ein Spektrometer vorstellen das den zu messenden Zustand nach gewissen vorgegebenen Werten sortiert.

Diese Verallgemeinerung gilt auch, wie oben erwähnt, noch für solche Messprozesse, bei denen der gemessene Zustand nach der Messung überhaupt nicht mehr vorhanden ist, wie dies z. B. beim Nachweis eines Photons i. A. der Fall ist.

Allerdings reicht, streng genommen zur Behandlung von Emission und Absorption die übliche Quantenmechanik nicht aus, man muss daher diese zur Quantenfeldtheorie erweitern. Wie die Quantenmechanik, insbesondere die Vertauschungsrelationen, auf der "höheren" Mechanik

1.2.3 Anmerkungen zu den Axiomen der QP

Die Grundlage für das Verständnis der Quantenmechanik geht auf die statistische Interpretaion durch Max Born [8] zurück, sie wird im allgemeinen die "Kopenhagener Deutung" genannt. Bedeutend war Heisenbergs Die Physikalischen Prinzipien der Quantenmechanik [9] . Die mathematisch-axiomatische Fassung geht auf den Mathematiker John von Neumann [10] zurück. Die kurzen Bemerkungen hier sollen die rein axiomatische Formulierung aus vorigem Absatz etwas erweitern und vertiefen.

1.2.3.1 Spektralsatz und Unschärfe

In der Anwendung der QM auf die Atomphysik betrachtet man meist nur isolierte Systeme und daher reine Zustände und interessiert sich für Observable und die zeitliche Entwicklung. Insbesondere das Spektrum der Eigenwerte und die zeitliche Entwicklung wird betrachtet.

In der Festkörperphysik ist oft die Wechselwirkung mit einem anderen System entscheidend, (z.B. einem Wärmebad) und man betrachtet den statistischen Operator, der z.B. für ein System im Wärmebad die Form hat: $\rho = \frac{1}{Z} e^{-\mathbf{H}/(\mathbf{kT})},\ Z = \mathrm{Sp}\left(e^{-\mathbf{H}/(\mathbf{kT})}\right)$

[8] Max Born: Zur Quantenmechanik der Stoßvorgänge. In: ZeitscHilbertraumift für Physik. Band 37, Nr. 12, 1926, S. 863–867, doi:10.1007/BF01397477

[9] Leipzig, Hirzel 1930

[10] Johann v. Neumann, Mathematische Grundlagen der Quantenmechanik, Springer 1932

Aus dem Mess-Axiom (3) folgt direkt: Der Erwartungswert von $\mathbf{E}$ ist für einen Zustand $|\phi\rangle$ gegeben durch

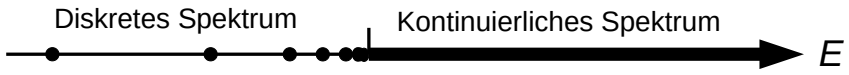
$$\langle \mathbf{E} \rangle = \langle \phi | \mathbf{E} \, | \phi \rangle. \tag{1.46}$$

Zwei Messgrössen können nur gleichzeitig scharf gemessen werden, wenn die Operatoren der Observablen kommutieren. Eine direkte Konsequenz der grundlegenden Vertauschungsrelation von Impulsoperator $\mathbf{P}$ und Ortsoperator $\mathbf{Q}$

$$[\mathbf{P}, \mathbf{Q}] = i\hbar \tag{1.47}$$

ist, dass Ort und Impuls prinzipiell nicht gleichzeitig scharf gemessen werden können (Heisenbergsche Unschärferelation).

Die meisten in der Physik auftretenden Operatoren sind nicht beschränkt und haben i.a. auch einen kontinuierlichen Bereich von Eigenwerten, das kontunuierliche Spektrum. Beim H-Atom sind die gebundenen Austände ($E < 0$ diskret), aber für ein ungebundenes Elektron-Proton-system ($E \geq 0$) ist jeder Energiezustand möglich und messbar.



Glücklicherweise spielt das für die Theorie des QC keine Rolle, da hier die Oertoren endlich dimensionale Matrizen sind.

1.2.3.2 Zeitliche Entwicklung

Die Zeitliche Etwicklung eines Systems wird nach **4'** durch einen Unitären Operator $\mathbf{U}(t, t') = e^{i(t'-t)\mathbf{H}/\hbar}$ beschrieben. Die Unitarität des Operators garantiert die Erhaltung der Wahrscheinlichkeit und impliziert dass $\mathbf{H}$ ein selbstadjungierter Operator ist:

$$\mathbf{U}^*(t,t)' \cdot \mathbf{U}(t,t) = e^{-i(t'-t)\mathbf{H}^*/\hbar} \, e^{+i(t'-t)\mathbf{H}/\hbar} = e^{-i(t'-t)(\mathbf{H}^*-\mathbf{H})/\hbar} = \mathbf{1} \tag{1.48}$$

woraus folgt: $\mathbf{H}^* - \mathbf{H} = 0$.

Wir beobachten also als die zeitabhängigkeit der Erwartungswerte von $\mathbf{A}$:

$$\langle \phi | e^{-i(t'-t)\mathbf{H}/\hbar} | \mathbf{A} | e^{+i(t'-t)\mathbf{H}/\hbar} | \phi \rangle \tag{1.49}$$ ze

Wir können nun die beobachtbare Zeitabhängigkeit des Erwartungswertes (1.49) entweder einerm Zeitabhängigen Operator zuschreiben (Heisenbergbild)

$$\mathbf{A}_t = e^{-it\,\mathbf{H}/\hbar} \, \mathbf{A} \, e^{+it\mathbf{H}/\hbar} \tag{1.50}$$ heis

oder auch einem zeitabhängigen Zustand zuschreiben (Schrödingerbild)

$$|\phi\rangle_t = e^{+it\,\mathbf{H}/\hbar} |\phi\rangle \tag{1.51}$$ sch

zuschreiben. Diese Transformation vom Schrödinger zum Heisenbergbild und umgekehrt war wichtig zur Zeit der Entdeckung der QM, scheint abre heute recht offensichtlich.

Aus (1.51) folgt unmittelbar die Schrödinger Gleichung:

$$-i\hbar\partial_t |\phi\rangle_t = \mathbf{H} e^{+it\,\mathbf{H}/\hbar}|\phi\rangle = \mathbf{H}\,|\phi\rangle_t \tag{1.52}$$ sch-a

sowie

$$-i\hbar\partial_t\,\mathbf{A}_t = -i\hbar\partial_t\left(e^{-it\,\mathbf{H}/\hbar}\,\mathbf{A}\,e^{+it\mathbf{H}/\hbar}\right) = -\mathbf{H}\,\mathbf{A}_t + \mathbf{A}_t\,\mathbf{H} = -[\mathbf{H},\mathbf{A}] \tag{1.53}$$ heis-a

1.2.3.3 Zusammengestzte Systeme und der statistische Operator

Ein isoliertes System in der Quantenmechanik ist eine Idealisierung, in der Realität wird ein System stets mit der Umwelt stets in Kontakt sein. Dies gilt besonders für makroskopische Systeme, wie z.B. eine Katze. Hier liegen die einzelnen Zustände des Systems so nahe beisammen, dass schon die kleinste Wirkun von aussen das System beeinflusst (z.B. Gravitationswellen).

Axiom 3 hilft uns aber, auch für nicht isolierte Systeme einige relevente Aussagen über die Darstellung von Zuständen zu machen. Dazu betrachten wir 2 Systeme, A und B die zusammengefasst isoliert sein sollen, d.h. Zustände in $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ können als reine Zustände betrachtet werden. Im folgenden sei

$|n_A\rangle\cdots$ ein vollständiges orthonormalsystem in $\mathcal{H}_A$ und $|\nu_B\rangle\cdots$ ein vollständiges orthonormalsystem in $\mathcal{H}_B$

Jeder (reine) Zustand $|ps\rangle \in \mathcal{H}_{AB}$ lässt sich darstellen als

$$|\psi\rangle = \sum_{n,\nu} a_{n\mu}|n\rangle_A \otimes |\mu\rangle_B \quad \text{mit} \sum_{n,\nu} \|a_{n\mu}\|^2 = 1 \tag{1.54}$$ rz

Wir wollen nun im System A die Observable $\mathbf{M}_A$ messen, aber das System B nicht beachten. Dann beobachten wir effektiv die Observable $\mathbf{M}_A \otimes \mathbf{I}$ Der Erwartungswert dieser Observablen ist

$$\begin{aligned}
\langle \mathbf{M}_A\rangle &= \langle\psi|\mathbf{M}_A\otimes\mathbf{I}|\psi\rangle && (1.55)\\
&= \left(\sum_{n,\nu} a^*_{n\nu}\ {}_A\langle n|\otimes\ {}_B\langle\nu|\right)\mathbf{M}_A\otimes\mathbf{I}_B\left(\sum_{m,\mu} a_{m\mu}\,|m\rangle_A\otimes|\mu\rangle_B\right) && (1.56)\\
&= \sum_{m,n,\mu,\nu} a^*_{n\nu}\,a_{m\mu}\langle n|\mathbf{M}_A|m\rangle_A\,\delta_{\nu\mu} && (1.57)\\
&= \sum_{m,n,\mu} a^*_{n\mu}\,a_{m\mu}\underbrace{\langle m|m\rangle_A}_{1}\langle n|\mathbf{M}_A|m\rangle_A && (1.58)\\
&= \sum_{m,n}\ {}_A\langle m|\underbrace{\sum_{\mu} a^*_{n\mu}\,a_{m\mu}|m\rangle_A\ {}_A\langle n|}_{\boldsymbol{\rho}_A}\mathbf{M}_A|m\rangle_A && (1.59)\\
&= \mathrm{Tr}_A(\boldsymbol{\rho}_A\cdot\mathbf{M}_A) && (1.60)
\end{aligned}$$

$$\boldsymbol{\rho}_A = \sum_{mn\mu} a_{m\mu}\, a^*_{n\mu\ A} |m\rangle\langle n|_A \tag{1.61}$$ rho

Aus der Definition von $\boldsymbol{\rho}_A$ ((??) oder (??) und aus (1.54) folgen die wichtigen Eigenschaften:

(A) $\boldsymbol{\rho}_A^\dagger = \boldsymbol{\rho}_A$

(B) $\forall \phi \in \mathcal{H}_A : \quad \langle\phi||\boldsymbol{\rho}_a\,\phi\rangle \geq 0$

(C) $\mathrm{Tr} \quad \boldsymbol{\rho}_A = 1$

Damit haben wir auch gesehen, dass die Beschreibung eines Zustandes durch den statistischen Operator auch gültig ist, wenn ein System mit einem anderen (äusseren) in Verbindung steht, dessen ähere Eigenschaften uns aber nicht interessieren (z.B. Wärmebad).

1' Ein Zustand wird durch einen Operator $\boldsymbol{\rho}_A$ mit den obigen Eigenschaften (**A - C**) beschrieben. Der Erwartungswert für eine Observable $\mathbf{M}$ ist gegeben durch

$$\langle \mathbf{M} \rangle_A = \mathrm{Tr}\boldsymbol{\rho}_A \cdot \mathbf{M} \tag{1.62}$$

Ist der Hamiltonoperator für die Zustände im gemeinsamen Hilbertraum $\mathcal{H}_A \otimes \mathcal{H}_B$ gegeben durch $\mathbf{H}_A \otimes \mathbf{H}_B$ so ist die zeitliche Entwicklung von $\boldsymbol{\rho}$ gegeben durch,

$$\boldsymbol{\rho}_A(t) = e^{-i\mathbf{H}_A t}\boldsymbol{\rho}_A e^{i\mathbf{H_A}t} \tag{1.63}$$

Daraus folgt das Analog zur Schrödingergleichung, s. 1.53 : heis-a

$$i\hbar\partial_t \boldsymbol{\rho}_A(t) = [\mathbf{H}_A, \boldsymbol{\rho}_A(t)] \tag{1.64}$$

Die Beschreibung durch reine Zustände ist auch darin enthalten, nämlich dann wenn der statistische Operator ρ ein Projektionsoperator P_n auf einen Vektor n im Hilbertraum ist:

$$\boldsymbol{\rho} = P_n \equiv |n\rangle\langle n| \tag{1.65}$$ rein

Der Erwartungswert eines s.a. Operators $\mathbf{M}$.

$$\mathrm{Tr}(\boldsymbol{\rho}_\mathrm{n}\,\mathbf{M}) = \sum_\mathrm{i} \langle \mathrm{m_i}|\mathrm{n}\rangle\langle \mathrm{n}|\,\mathbf{M}|\mathrm{m_i}\rangle \tag{1.66}$$

Wir wählen das orthonormalsystem so, dass ein Vektor $|m_j\rangle = |n\rangle$ ist damit erhalten wir

$$\mathrm{Tr}(\boldsymbol{\rho}_\mathrm{n}\,\mathbf{M}) = \sum_\mathrm{i} \langle \mathrm{m_i}|\mathrm{n}\rangle\langle \mathrm{n}|\,\mathbf{M}|\mathrm{m_i}\rangle = \langle \mathrm{n}|\,\mathbf{M}|\mathrm{n}\rangle \tag{1.67}$$

d.h. der Erwartungswert für einen reinen Zustand.

Diagonale Dichtematrix: Da der statistische Operator $\boldsymbol{\rho}_A$ selbsadjungiert ist, lässt er sich seine Matrix stets diagonalisieren, mit den Eigenwerten p_n. Sei $|n\rangle$ das vonS in dem $\boldsymbol{\rho}$ diagonal ist, dann gilt:

$$\boldsymbol{\rho}_A = \sum_n p_n\, |n\rangle\langle n| \tag{1.68}$$

d.h. der durch $\boldsymbol{\rho}_A$ beschriebene Zustand ist ein **Ensemble** von reinen Zuständen , die sich mit der Wahrscheinlichkeit p_n im Zustand $|n\rangle$ befinden.

Beim AC spielt der Hilbertraum, der das direkte Produkt von N 2-dimensionalen Hilberträumen (Qubits) ist, eine besondere Rolle. In ihm ist das direkte Produkt der Basisvektoren eine viel verwendete Basis (Computatorische Basis):

$$|i_N\rangle \otimes |i_{N-1}\rangle \otimes \cdots |i_1\rangle; \quad i_k = 0, 1 \tag{1.69}$$

schmidt

1.2.4 Die Schmidt Darstellung

Für die Informatik ist es bequem Numerierungen mit 0 und nicht mit 1 zu beginnen.

Die Schmidt Darstellung gibt ein Mass für die Verschränkung eines Zustandes.

Seien $\mathcal{H}_A$ und $\mathcal{H}_B$ zwei Hilberträume. Ein Zustand $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ kann durch die voS $|-n\rangle_A \in \mathcal{H}_A$ und $|\mu\rangle_B \in \mathcal{H}_B$ dargestellt werden als:

$$|\psi\rangle_{AB} = \sum_{n=0}^{N}\sum_{\mu=0}^{M} a_{n\mu}|\bar{n}\rangle_A \otimes |\mu\rangle_B = \sum_{\mu=0}^{M} a_{n\mu}|\mu\rangle_B \tag{1.70}$$ rz2

Allgemein gilt für die Partialspur in $\mathcal{H}_B$ des Projektionsoperators $|\psi\rangle_{ABBA}\langle\psi|$:

$$\sum_{\nu} {}_B\langle\nu|\psi\rangle_{AB\,BA}\langle\psi|\nu\rangle_B \equiv \boldsymbol{\rho}_A = \sum_{mn\mu,\mu',\nu} a_{r\mu}\, a^*_{s\mu}\; |\bar{r}\rangle_{A\,A}\langle\bar{s}|\delta_{\mu,\nu}\delta\mu'\nu = \sum_{mn} A_{rs}|\bar{r}\rangle_{A\,A}\langle\bar{s}|; \tag{1.71}$$ rz3

mit $A_{sr} = \sum_\nu a^*_{s\nu}\, a_{r\nu}$

Die Matrix gilt: $\mathbf{A} = A_{mn}$ ist selbstadjungiert, d.h. es gibt eine unitäre Transformation $\mathbf{U}$ in $\mathcal{H}_A$ die $\mathbf{A}$ diagonalisiert:

$$\mathbf{U}\,\mathbf{A}\,\mathbf{U}\dagger = \begin{pmatrix} p_1 & 0 & 0 & \dots \\ 0 & p_2 & 0 & \dots \\ \vdots & \vdots & & \end{pmatrix}; \quad p_k \geq 0; \tag{1.72}$$ diag

$$\mathbf{U}\,\mathbf{U}^\dagger = \mathbf{U}^\dagger\,\mathbf{U} = \mathbf{I}; \quad \sum_m U^*_{mr}\, U_{ms} = \delta_{rs} \tag{1.73}$$

Die Zahl der von Null verschiedenen Eigenwerte der Matrix $\mathbf{A}$ heisst Schmidt-Zahl, N_{Sch}; sie spieltfür die Berechnung der Verschränkung, wie wir noch sehen werden, eine entscheidende Rolle.

Wir führen nun die neue Basis $|m\rangle_A$ ein, bezüglich derer $\mathbf{A}$ diagonal ist die wir noch so angeordnet haben, dass für alle $m > N_{Sch}$ die Diagonalelemente $p_m = 0$.

$$|m\rangle_A = \sum_r U_{mr}|\bar{r}\rangle \tag{1.74}$$ rtom

Zum Übergang in diese Basis schieben in (??) die $\mathbf{I} = \mathbf{U} \dagger \mathbf{U}$ ein und erhalten:

$$\begin{aligned}
\boldsymbol{\rho}_A &= \sum_{mn} A_{rs} |\bar{r}\rangle_{A\,A}\langle\bar{s}| && (1.75)\\
&= \sum_{r',s',m,n} A_{sr}\, U^*_{mr} U_{mr'}\, U_{ns} U^*_{ns'}\, |\bar{r}'\rangle_{A\,A}\langle\bar{s}'| && (1.76)\\
&= \sum m, n, s, r U^*_{mr}\, U_{ns}\, A_{sr} |m\rangle_{A\,A}\langle n| && (1.77)\\
&= \sum_{m=0}^{N_{Sch}} p_m\, |m\rangle_{A\,A}\langle m| && (1.78)
\end{aligned}$$

wobei wir beim letzten Schritt (1.72) benutzt und alle verschwindenden Terme ($p_k = 0$) weggelassen haben.

Wir nutzen die Umkehrung von (??), nämlich

$$|\bar{r}\rangle = \sum_{m=0}^{N_{Sch}} U^*_{mr} |m\rangle_A \tag{1.79}$$

aus und erhalten für den Ausgangszustand $|\psi\rangle_{AB}$ in der neuen (i. A. nicht vollständigen) Basis $|m\rangle_A$

$$\begin{aligned}
|\psi\rangle_{AB} &= \sum_{r,\mu} a_{r\mu} |\bar{r}\rangle_A \otimes |\mu\rangle_B && (1.80)\\
&= \sum_{\mu,r,m} a_{r\mu}\, U^*_{mr}\, |m\rangle_A \otimes |\mu\rangle_B && (1.81)\\
&= |m\rangle_A \otimes |\hat{m}\rangle_B && (1.82)
\end{aligned}$$

wobei $|\hat{m}\rangle_B = \sum_{\mu,r} a_{r\mu}\, U^*_{mr} |\mu\rangle_B$. Es gilt:

$$\langle\hat{n}|\hat{m}\rangle_B = \sum_{r,\mu,r',\mu'} a_{r\mu} U^*_{mr}\, a^*_{r'\mu'} U_{nr'} \delta_{\mu'\mu} = p_m \delta_{nm} \tag{1.83}$$

wobei wieder (1.72) benutzt wurde.

Wir normalisiern $|\hat{m}\rangle_B$:

$$|\tilde{m}\rangle_B = \frac{1}{\sqrt{p_m}} |\hat{m}\rangle_B = \frac{1}{\sqrt{p_m}} \sum_{\mu,r} a_{r\mu}\, U^*_{mr} |\mu\rangle_B \tag{1.84}$$

und erhalten damit die **endgültige Form der Schmidt Darstellung** für einen Zustand $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$:

$$|\psi\rangle_{AB} = \sum_{m=0}^{N_{Sch}} \sqrt{p_m}\, |m\rangle_A \otimes |\tilde{m}\rangle_B \tag{1.85}$$ sche

Ein Zustand ist verschränkt, wenn die Schmidt-Zahl N_{Sch} grösser als 1 ist, d.h. wenn die Matrix $\mathbf{A}$, $A_{sr} = \sum_\nu a^*_{s\nu}\, a_{r\nu}$, s. (1.71), mindestens 2 Eigenwerte ungleich Null hat.

Die Zustände $|m\rangle_A$, die in der Schmidt-Darstellung auftreten, sind so gewählt, dass sie au einer diagonalen Dichtematix in $\mathcal{H}_A$ führen:

$$\boldsymbol{\rho}_A = \sum_{m=0}^{N_{Sch}} p_n \, |m\rangle_A \; {}_A\langle m| \quad \text{with } p_n > 0 \tag{1.86}$$

Wichtige Konsequenz:

Ist ein Zustand verschränkt, dann wird er durch eine Messung in einem der beiden Hilberträume irreversibel verändert.

Bew. Sei $|\psi\rangle_{AB} = \sum_{m=0}^{N_{Sch}} \sqrt{p}\,|m\rangle_A \otimes |\tilde{m}\rangle_B$ mit $N_{Sch} \geq 1$. Eine Messung in $\mathcal{H}_A$ ist eine Projektion auf einen Vektor $|q\rangle_A$ aus $\mathcal{H}_A$:

$$|\psi\rangle_{AB} \to |q\rangle_A \, {}_A\langle q| \otimes \mathbf{I}_B \, |\psi\rangle_{AB} = |q\rangle_A \otimes |\tilde{r}\rangle \tag{1.87}$$

mit dem Zustand $|\tilde{r}\rangle = \sum_{m=0}^{N_{Sch}} \sqrt{p_m}\langle q|m\rangle_A |\tilde{m}\rangle_B \in \mathcal{H}_B$. D.h. der usrprünglich verschrämkte Zustand wurde zu einem anderen, nicht verschränkten, irreversibel geändert.

1.2.4.1 Beispiele

Spin 0 aus 2 Spin $\frac{1}{2}$ Zuständen : Zur Eingewöhnung benutzen wir auch immer die CB:

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |+\tfrac{1}{2}\rangle; \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |-\tfrac{1}{2}\rangle \tag{1.88}$$

$$|m\,n\,r, \cdots\rangle \equiv |m\rangle_1 \otimes |n\rangle_2 \otimes |r\rangle \otimes \cdots \quad m, n, r \in 0, 1 \tag{1.89}$$

$$|J=0\rangle = \frac{1}{\sqrt{2}}\Big(|+\tfrac{1}{2}\rangle_A \otimes |-\tfrac{1}{2}\rangle_B - |-\tfrac{1}{2}\rangle_A \otimes |+\tfrac{1}{2}\rangle_B\Big) = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) \tag{1.90}$$

Die Matrix $\mathbf{A}$, s. (1.71) ist für diesen Fall: $\mathbf{A} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$, d.h. hat 2 Eigenwerte, damit ist der Zustand verschränkt.

Betrachten wir dagegen den Spin 1 Zustand mit z-Komponente +1 Spin:

$$|J=1, J_3=1\rangle = |+\tfrac{1}{2}\rangle_A \otimes |+\tfrac{1}{2}\rangle_B = |00\rangle \tag{1.91}$$

so hat die Darstellung von vornherein nur einen Summanden ($N_{Sch} = 0$), er ist also nicht verschränkt.

Ist man am Verhalten zweier Spins in Rahmen der Drehimpulsphysik interessiert ist es sinnvol

die Drehimpuls Basis zu wählen:

$$
\begin{aligned}
|J=0, J_z=0\rangle &= \frac{1}{\sqrt{2}}\Big(|+\tfrac{1}{2}\rangle_A \otimes |-\tfrac{1}{2}\rangle_B - |-\tfrac{1}{2}\rangle_A \otimes |+\tfrac{1}{2}\rangle_B\Big) = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) \\
|J=1, J_z=+1\rangle &= |+\tfrac{1}{2}\rangle_A \otimes |+\tfrac{1}{2}\rangle_B = \frac{1}{\sqrt{2}}\Big(|00\rangle\Big) \\
|J=1, J_z=\ 0\rangle &= \frac{1}{\sqrt{2}}\Big(|+\tfrac{1}{2}\rangle_A \otimes |-\tfrac{1}{2}\rangle_B + |-\tfrac{1}{2}\rangle_A \otimes |+\tfrac{1}{2}\rangle_B\Big) = \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big) \\
|J=1, J_z=-1\rangle &= |-\tfrac{1}{2}\rangle_A \otimes |-\tfrac{1}{2}\rangle_B = \frac{1}{\sqrt{2}}\Big(|11\rangle\Big)
\end{aligned}
$$

FUr die Informatik ist oft die sog. Bell-Basis, die aus 4 verschränkten Zustaänden besteht, angemessener.

$$\frac{1}{\sqrt{2}}\Big(|+\tfrac{1}{2}\rangle_A \otimes |-\tfrac{1}{2}\rangle_B - |-\tfrac{1}{2}\rangle_A \otimes |+\tfrac{1}{2}\rangle_B\Big) = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) \tag{1.92}$$

$$\frac{1}{\sqrt{2}}\Big(|+\tfrac{1}{2}\rangle_A \otimes |-\tfrac{1}{2}\rangle_B + |-\tfrac{1}{2}\rangle_A \otimes |+\tfrac{1}{2}\rangle_B\Big) = \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big) \tag{1.93}$$

$$\frac{1}{\sqrt{2}}\Big(|+\tfrac{1}{2}\rangle_A \otimes |+\tfrac{1}{2}\rangle_B - |-\tfrac{1}{2}\rangle_A \otimes |-\tfrac{1}{2}\rangle_B\Big) = \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big) \tag{1.94}$$

$$\frac{1}{\sqrt{2}}\Big(|+\tfrac{1}{2}\rangle_A \otimes |+\tfrac{1}{2}\rangle_B + |-\tfrac{1}{2}\rangle_A \otimes |-\tfrac{1}{2}\rangle_B\Big) = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) \tag{1.95}$$

Man rechnet leicht nach, dass alll diese Zustände zur Matrix $\mathbf{A} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$ führen

Beim Zustand $|\psi\rangle = \frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)$ sieht man sofort dass er als $|\psi\rangle = \frac{1}{2}(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)$ dargestellt werden kann, also nicht verschränkt ist. Man kann auch die Matrix $\mathbf{A}$ (s. (1.71)) brechnen: $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Die Eigenwerte sind die Lösungen von $(1-x)^2 - 1 = 0$, d.h. es gibt nur einen von 0 verschiedenen Eigenwert, also $N_{Sch} = 0$, $|\psi\rangle$ ist nicht verschränkt.

Das Konzept lässt successive sich auch auf **mehr als zwei Hilberträume** ausdehnen. Ist $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_3 \otimes \mathcal{H}_3$ kann man zuerst $(\mathcal{H}_1 \otimes \mathcal{H}_2) \otimes \mathcal{H}_3$ analysieren

Oft sind gerade die Terme mit vielen Summanden nicht verschränkt. Z.B. ist der Zustand
$\frac{1}{\sqrt{8}}\Big(|0\,0\,0\rangle + |0\,0\,1\rangle + |0\,1\,0\rangle + |0\,1\,1\rangle + |1\,0\,0\rangle + |1\,0\,1\rangle + |1\,1\,0\rangle + |1\,1\,1\rangle\Big)$
nicht verschränkt.

Er hat zwar viele Summanden, aber man überzeugt sich, dass er als ein Term, nämlich als $|m\rangle \otimes |m\rangle \otimes |m\rangle$ geschrieben werden kann.

1.2.5 Entropie in der QP

Grob gesprochen ist die Entropie ausserhalb der reinen Thermodynamik ein quantitatives Mass für unsre Unkenntnis über die Mikrozutände einee Gesamtzustandes. Je ausgedehnter

ein System im Phasenraum ist, z.B. je grössr das Volumen einer bestimmten Gassmenge ist, desto grösser ist unsere Unkenntnis z. B über die Lage eines einzelnen Atoms. Das ist die Grundlage für die statistische Definition der Entropie durch Boltzmann:

$$S = k_B \log \Omega \tag{1.96}$$

wobei Ω das Volumen des erreichbaren Phasenraums ist.

Hierbei ist angenommen dass das System gleichverteilt über den Phasenraum ist. Die Wahrscheinlichkeit ein System in einem bestimmten Bereich aufzufinden ist also $w = 1/\Omega$. Eine eine erweiterte Formulierung bei allgemeiner Wahrscheinlichkeitsverteilung über den Phasenraum, $w(\Omega)$, ist ist das Integral der über diese AufenthaltsWahrscheinlichkeit:

$$S = -k_B \int w(\Omega) \log w(\Omega)\, d\Omega \tag{1.97}$$

Dies führtt zur Q-Entropie (v. Neumann):

$$S_Q = -\langle \boldsymbol{\rho} \rangle \equiv -\operatorname{Tr}[\boldsymbol{\rho} \log \boldsymbol{\rho}] = -\sum_n p_n \log p_n \tag{1.98}$$

die letzte Gleichung folgt aus der stets möglichen Wahl eines voS, in dem $\boldsymbol{\rho}$ diagonal ist.

Ein reiner Zustand hat in als statistischen Operator einen Projektionsoperator (1.18) $\mathbf{P}_{|\rangle}$, der in die folgende Matrixform gebracht werden kann:

$$\boldsymbol{\rho} = \mathbf{P}_{|1\rangle} = \begin{pmatrix} 1 & 0 & \cdots \\ 0 & 0 & \dots \\ 0 & 0 & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix} \tag{1.99}$$

d.h. diesem Falle ist $S_Q = \log 1 = 0$.

Ein maximal unbestimmter Zustand in einem d dimensionalen Raum ist ein statistischer Operator mit gleichem Gewicht für alle Zustände:

$$\boldsymbol{\rho} = \sum_{n=1}^{d} \frac{1}{d} \mathbf{P}_{|d\rangle} = \begin{pmatrix} \frac{1}{d} & 0 & \cdots \\ 0 & \frac{1}{d} & \dots \\ 0 & 0 & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix} \tag{1.100}$$

d.h. $S_Q = \log d$

1.2.6 Das Korrespondenzprinzip und die "höhere Mechanik"

Es wurde bereits erwähnt dass das Korrespndenzprinzip das vielleicht wichtigste Prinzip der QP ist. Es gibt einem die Vorschriften für die Konstruktion des Hamiltonoperators aus den bewährten Ausdrücken der klassischen Physik. Es erklärt auch, warum man in vielen Fällen denken konnte, dass die klassiche Physik das letzte Wort sei: Betrachtet man nur die

Erwartungswerte, so erhält man aus der QP und dem Korrespondenzprinzip das Resultat, dass sich die Erwartungswerte so verhalten, wie man nach der klassischen Physik berechnet.

Hier soll noch ein Aspekt des Korrepondenzprinzips erwähnt werden, der vielleicht am wenigsten verstanden ist. Wie in (**6**) erwähnt, erfüllen Orts- und Impulsoperatoren die Vertauschungsrelationen:

$$[\mathbf{Q}_j, \mathbf{Q}_k] = 0; \quad [\mathbf{P}_J, \mathbf{P}_k] = 0; \quad [\mathbf{P}_j, \mathbf{Q}_k] = -i\hbar\,\delta_{kl} \tag{1.101}$$

Ort und Impuls sind in der klassischen Mechanik harmonisch konjugierte Variable die in den Hamilton-Jakobischen Gleichungen auftreten:

$$\partial_t q_i = \frac{\partial H}{\partial p_i} \quad \partial_t p_i = -\frac{\partial H}{\partial q_i} \tag{1.102}$$

.Eine besondere Rolle spielen die "kanonischen Transformationen", d.h. solche Transformationen, bei denen die Bewegungsgleichungen die gleiche Form haben. Invarianten unter kanonischen Trasformationen sind u.a. die **Poisson Klammern**

$$\{u, v\} \equiv \sum_k \left(\frac{\partial u}{\partial q_k}\frac{\partial v}{\partial p_k} - \frac{\partial u}{\partial p_k}\frac{\partial v}{\partial q_k} \right) \tag{1.103}$$

u, v sind beliebige Funktionen der kanonischen Variablen.

Setzt man $u = q_m,\ v = p_n$ so erhält man:

$$\{q_m,\, p_n\} = \sum_k (\delta_{mk}\,\delta_{nk}) = \delta_{mn} \tag{1.104}$$

und genauso: $\{q_m,\, q_n\} = \{p_m,\, p_n\} = 0$

Der senior research student P A M Dirac (geb. 1902) schlug vor, die Poisson-Klammern durch Kommutatoren zu ersetzen [11]

$$\{\cdots, \cdots\} \to \frac{-i}{\hbar}[\cdots, \cdots] \tag{1.105}$$ HL

Dass dies mehr ist als eine mathematische Spielerei ist, erkennt man, wenn man die Liouville Gleichung für die zeitliche Entwicklung einer Dichteverteilung ρ in der klassischen statistischen Mechanik betrachtet. Sie lautet

$$\partial_t\, \rho = \{H, \rho\} \tag{1.106}$$

wobei H die Hamiltonfunktion der klassischen Mechanik ist.

[11] (Proc. Royal Soc. A 109, 642 (1925)): In a recent paper Heisenberg puts forward a new theory, which suggests that it is not the equations of classical mechanics that are in any way at fault, but that the mathematical operations by which physical results are deduced from them require modification. All the information supplied by the classical theory can thus be made use of in the new theory.... We make the fundamental assumption that difference between the Heisenberg products of two quantum quantities is equal to $i\hbar$ times their Poisson bracket expression.

Machen wir die Ersetzung (I.105) an dieser Liouville Gleichung, und ersetzen ρ durch den QP statistischen Operator und die Hamiltonfunktion H durch den Hamiltonoperator $\mathbf{H}$ so erhalten wir

$$\partial_t \rho = \frac{-i}{\hbar}[\mathbf{H}, \rho\} \tag{1.107}$$

d.h. genau die von der QP geforderte zeitliche Entwicklung (I.53).

Noch wichtiger ist diese kanonische Quantisierung in der Feldtheorie. Sie erlaubt hier den Übergang von einer klassischen zu einer **Quanten-Feldtheorie**. Hier entspricht dem q das Feld und dem p der kanonische Feldimpulls nach Euler Lagrange.

In der Elektrodynamik entspricht das Potential A_μ der Variablen q und dem p der "kanonische adjungierte Feldimpuls" der klassischen Feldtheorie, $\Pi_j = \partial_j A_0 - \partial_0 A_j$ und so erhält man für die Quantelektrodynamik die Quantisierungsbedingung:

$$[\mathbf{A}_\mu(t, \vec{x}), \Pi_j(t, \vec{y})] = -\boldsymbol{i}\hbar\delta_{\mu j}\delta(\vec{x} - \vec{y}) \tag{1.108}$$

1.2.7 Erweiterungen der Axiome der QP

1.2.7.0.1 C^* Algebren Die Formulierung der Axiome der Quantenmechanik in der Sprache der C^*- Algebren ist keine neue Quantisierungsmethode, aber eine recht abstrakt mathematische Formulierung, die vesucht ohne nichtbeobachtbare Grössen auszukommen (Daher auch der Name *Observablen-Algebra*).

Dieser Zugang geht davon aus, dass die Beobachtungen sich auf zwei wesentliche Komponeneten reduzieren lassen:

1) Die Mehode mit der wir messen, die die **Observablen** bestimmt (z.B Energie, Spin,....) und
2) der **Zustand**, für den wir ein Messergebnis, d.h. eine reele Zahl, erhalten.

Die Observablen, die in der üblichen Formulierung selbstadjungierte Operatoren im Hilbertraum sind, werden verallgemeinert zu Elementen einer Algebra mit gewissen Rechenregeln, den sogenannten C^*-Algebren.

Ein **Zustand** Φ einer C^*–Algebra ist eine lineare Abbildung der Elemente der Observablenalgebra auf die positiven reelen Zahlen, $\Phi(\mathcal{A}) \to \mathbb{C}_+$ mit $\Phi(\mathbf{1}) = 1$.

Ein Zustand heißt rein, wenn er sich nicht als Linearkombination zweiert verschiedener Zustände $\lambda\Phi_1 + (1 - \lambda)\Phi_0$ zerlegen lässt.

Die Formulierung der QM durch Dichteoperatoren kommt der durch C^* Algebren sehr nahe. Die Observablen sind selbstadjungierte Operatoren im Hilbertraum, ein Zustand ist die Spurbildung mit dem statistischen Operator. Rin reiner Zustand ist eine Projektion auf einen eindimensionalen Hilbertraum.

1.2.7.0.2 Rein probabilistische Interpretation der QM. Eine Rein probabilistische Inerprotation der QM schlägt C. Wetterich vor. Dabei wird wesentlich Gebrauch von der **bedingten Wahrscheinlichkeit** (Bayes'sche Statistik) gemacht. Lit:

www.thphys.uni-heidelberg.de/~wetterich/Vorlesungen/Foundations%20of%20quantum%20mechanics%202021/Foundations_of_Quantum_Mechanics.pdf}
inspirehep.net/literature/1828609}

1.2.8 Frühe Kritik an der QM

In fast allen ausfürlicheren Abhandlungen über QC wird das EPR Paradoxon und Schrödingers Katzte erwähnt, sie sind auch instruktiv über die Besonderheiten der QM. Deshalb seien sie hier kurz vorgestellt.

1.2.8.1 EPR

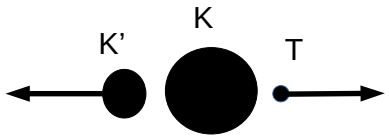
Beim Messprozess (Axiom 3) wurde und wird bemäkelt, dass für die Messung selbst nicht die durch Axiom 4 beschriebene zeitliche Entwicklung gilt. Auch die inhärent statistische Natur der Quantenmechanik wurde von vielen nicht "als der letzte Jakob" anerkannt. Der prominenteste Verter Berühmt ist Albert Einstein. Er schrieb 1926, kurz nach dem Erscheinen der wesentlichen Arbeit von Born, Heisenberg und Jordan, an seinen Freund Max Born, der ja die statistische Interpretation vorschlug:

> Die Quantenmechanik ist sehr achtunggebietend. Aber eine innere Stimme sagt mir, dass das doch nicht der wahre Jakob ist. Die Theorie liefert viel, aber dem Geheimnis des Alten bringt sie uns kaum näher. Jedenfalls bich ich überzeugt, dass der nicht würfelt. (Brief vom 4.12.1926)

Was das QC angeht ist Born's spätere Antwort auf Einsteins Kritik an der QM prophetisch:

„If God has made the world a perfect mechanism, He has at least conceded so much to our imperfect intellect that in order to predict little parts of it, we need not solve innumerable differential equations, but can use dice with fair success." (Max Born Ëinstein's Statistical Theoriesïn Albert Einstein : Philosopher-Scientist (1951) edited by Paul Arthur Schilpp, p. 176)

Etwa 10 Jahre nach seiem Brief am Born glaubte Einstein, einen Beweis für seine Vermutung gefunden zu haben, dass die QM nicht vollständig sein kann. Er veröffentlichte ihn mit zwei Mitarbeitern, er enhält das berühmte EPR Pradoxon, das auch in jeder Abhandlung über QC erwähnt wird, Im Grunde ist es sehr einfachs. Abb. 1.1: Nehmen wir einen ruhenden radioaktiven Kern der in zwei Teile zerfällt: $K \to K' + T$. Wegen der Impulserhaltung gilt: $\vec{p}_{K'} = -\vec{p}_T$. Messen wir also den Impuls von K', so kennen wir auch den von T. Also haben sowohl K als auch T beide einen wohldefinierten (scharfen) Impulswert. EPR schlossen nun: Wenn wir Ort und Impuls kennen können, dann muss er auch dem Teilchen ungeteilt zukommen. Die populärste Theroie (Bohm) war die der verborgenen Parameter: Es gibt neben Ort und Impuls noch weitere Parameter, zur Bestimmung eines Teilchens, die wir aber nicht kennen, und die Unschärfe ist nur eine Konseqaenz unsrer Unkenntnis über diese



$$\vec{p}_{K'} = -\vec{p}_T$$

epr Abbildung 1.1: The EPR paradox, Einstein, A; B Podolsky; N Rosen ; Can Quantum-Mechanical Description of Physical Reality be Considered Complete?. Physical Review. 47 (10): 777–780.

"Verborgenen Parameter" (*hidden variables.*) Das Problem wurde später von Bohm auf ein 2-Spin System übertragen und gab Anlass zu den berühmten Bell'schen Ungleichungen, auf die wir später eingehen werden und deren Verletzung man als den endgültigen Triumph Max Born's betrachten kann.

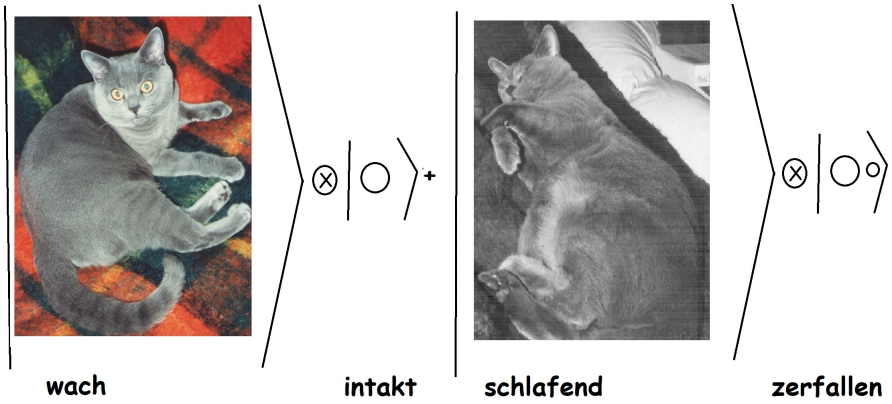
Die zeitgenössischen Reaktionen auf Einsteins Kritik an der QM waren sehr geteilt. Die meisten der jüngeren Physiker nahmen sie nicht sonderlich ernst, Niels Bohr hingegen ging auf sie sehr detailliert ein. Hier ist ein von Bohr entworfenes Modell für den Nachweis, dass die Heisenberg'sche Unschärfe auch im Falle der Gravitation gilt (Schilp, aaO p. 227).

Zur Vermeidung von Abmahnungen ausgelassene Abbildung

1.2.8.2 Schrödingers Katze

Das Axiom über zusammengestetzte Systeme, Nr. 5, klingt zunächst harmlos und einleuchtend, hat aber, in Verbindung mit dem Superpositionsprinzip (Axiom 1) weitreichende Konsequenzen.

Der Satz: ,,Ist $|\psi\rangle_A$ im System A und $|\phi\rangle_B$ im System B präpariert, dann wird der Zustand im gemeinsamen System durch $|\psi\rangle_A \otimes |\phi\rangle_B$ beschrieben" ist in der Tat einleuchtend, aber in Verbindung mit der Forderung dass auch . $|\psi_1\rangle_A \otimes |\phi_1\rangle_B + |\psi 2\rangle_A \otimes |\phi_2\rangle_B$ ein physikalisches System beschreibt führtt er zu weitreichenden Konsequenzen. Dieses Phänomen wird als Verschränkung (entanglement) bezeichnet und ist in der Mikrophysik sehr wichtig und bestens bestätigt. In der Makrophysik allerdings führtt es zu "burlesken Fällen". Besonders bekannt ist die "Schrödingersche Katze", die eine Superposition von einer lebendigen und einer toten Katze ist.



Schrödingers Katze

Die Ampulle enthällt kein Gift, sondern ein Schlafmittel,

Hier ist das Originalzitat von Schrödinger aus der Arbeit, in der die Bedeutung der Verschränkung erkannt wurde (**Die Naturwissenschaften**, 48, p. 807ff (1935) Die gegenwärtige Situation in der Quantenmechanik.

> .....Man kann auch ganz burleske Fälle konstruieren. Eine Katze wird in eine Stahlkammer gesperrt, zusammen mit folgender Höllenmaschine (die man gegen den direkten Zugriff der Katze sichern muß): in einem Geigerschen ZählroHilbertraum befindet sich eine winzige Menge radioaktiver Substanz, so wenig, daß im Laufe einer Stunde vielleicht eines von den Atomen zerfällt, ebenso waHilbertraumscheinlich aber auch keines; geschieht es, so spricht das ZählroHilbertraum an und betätigt über ein Relais ein Hämmerchen, das ein Kölbchen mit Blausäure zertrümmert. Hat man dieses ganze System eine Stunde lang sich selbst überlassen, so wird man sich sagen, daß die Katze noch lebt, wenn inzwischen kein Atom zerfallen ist. Der erste Atomzerfall würde sie vergiftet haben. Die Psi-Funktion des ganzen Systems würde das so zum Ausdruck bringen, daß in iHilbertraum die lebende und die tote Katze (s.v.v.) zu gleichen Teilen gemischt oder verschmiert sind. Das Typische an solchen Fällen ist, daß eine ursprünglich auf den Atombereich beschränkte Unbestimmtheit sich in grobsinnliche Unbestimmtheit umsetzt, die sich dann durch direkte Beobachtung entscheiden läßt. Das hindert uns, in so naiver Weise ein „verwaschenes Modell“ als Abbild der Wirklichkeit gelten zu lassen.

Das Problem, dass makroskopische Überlagerungen (wie tote und lebendige Katze) absurd erscheinen werden aber durch das Phänomen der Dekohärenz [12] erklärt. Ein makkroskopischer Körper wird so stark von der Umgebung beeinflusst, dass dadurch die Verschränkung, die auf festen Phasenbeziehungen basiert, extrem schnell (quasi-instantan) zerstört wird.

Aber auch die sehr gut bestätigten Verschränkungen in der Mikrophysik haben viele Physiker gestört, vor allem auch wieder Einstein, da sie auf eine seiner Meinung nach unmögliche

[12] H. Dieter Zeh, “On the Interpretation of Measurement in Quantum Theory”, Foundations of Physics, vol. 1, pp. 69–76, (1970)

instantane Fernwirkung hinausliefen [13]. Allerdings wurde das Hauptargument von Einstein, Podolsky und Rosen durch Experimente wiederlegt, wir kommen darauf im Zusammenhang mit den Bell'schen Ungleichungen zurück.

QC, und vor allem seine Vorteile gegenüber dem klassischen Computer, beruhen gerade ganz wesentlich auf den umstrittenen Prinzipien der QM, während die Dekohärenz, die den Übergang zur klassischen Physik erklärt, die Möglichkeiten zur Konstruktion von Quantencomputern gewaltig einschränkt.

1.2.9 Verborgene Variable (Hidden variables)

Einstein versuchte schon früh, sein Missbehagen an der QM konstruktiv zu untermauern, auf einer Akademiesitzung machte er 1927 einen Vorschlag, dessen Veröffentlichung er aber zurückzog.

Auf der Solvay-Konferenz 1927, wo die meisten dr massgeblichen Physiker anwesend waren, machte de Broglie den Vorschlag, in einer Teilchentheorie ein Führungsfeld einzuführen, dass wir nicht beobachten können, aber z.B. zu den Interferenzerscheinungen beim Doppelspalt führ. Er fand wenig Anklang (J. Bell: "he was laughed out of court")

David Bohm entwickelte diese Theorie genau in der Weise, dass sie alle Phänomene genau wie die QM beschreibt. Allerdings nur für nichtrelativistische QM, keinerlei Hinweis (und Versuch?) die Quantenfeldtheorie (z.B. Teilchen Erzeugun und Vernichtung) zu erklären.

Da sie konstruiert wurde, um die QM genau zu rekonstuieren, keinerlei Bedeutung für QC.

Historischer Hinweis: Newton, der das Licht als Teilchenstrahl auffasste, musste zur Erklärung der Newton'schen Ringe "verborgene Variable" einführen (Opticks, Book 2, Part III, 1704): Er schrieb den Teichenstrahlen gewisse Eigenschaften (fits) zu, die entscheiden, ob der Strahl an einer Grenzfläche eindringt oder reflektiert wird.

1.3 Alternative Quantisierungs-Methoden

Der Vollständigkeit halber, und da man ja nie weiss, wie sich ein Gebiet entwickelt, seien hier zwei recht verschiedene andere Beziehungen zwischen klassischer und Quantenphysik erwähnt.

1.3.1 Pfadintegral, stark vereinfacht

Bei der oben angegebenen axiomatischen Darstellung de QM ist der Grundbegriff der Zustand, und das macht diese Formulierung, besonders in der ursprünglichen Matrix-Formulierung auch zu einem sehr guten Ausgangspunkt für das QC.

[13] A. Einstein, B. Podolsky, N. Rosen: Can quantum-mechanical description of physical reality be considered complete?, Phys. Rev. 47 (1935), S. 777–780 doi:10.1103/PhysRev.47.777

Es gibt aber auch noch einen weiteren Zugang zur QM, der besonders in Computersimulationen zur QFT eine grosse Rolle spielt, nämlich der durch Pfadintegrale. Er geht zurück auf eine Idee von Dirac, wurde aber von R. Feynman erstmals ausgeführt. Bei ihm steht nicht der Zustand, sondern der Prozess im Mittelpunkt. Für den gegenwärtigen Zugang zum QC scheint er wenig zu bringen, aber als alternativer Zugang zur QM ist er dennoch erwähneneswert, zumal er den Übergang von der QM zur klassischen Physik viel deutlicher zeigt.

Wenn ich den Ort und Impuls eines Teichens zu einer betsimmteh Zeit, t_0 kenne, so kann ich in der klassischen Physik seine Bahnkurve mithilfe der Bewegungsgleichungen eindeutig berechnen. Dies geht mit Hilfe bereits der Euler-Lagrange'schen Gleichungen.

Sei $\mathcal{L}(q, \dot{q})$ die Lagrangefunktion eines Systems (kinetische minus potentielle Energie); Hierbei ist q der Ort und $\dot{q}$ die Geschwindigkeit. Die klassische Bewegungskurve $q_(t)$ macht die Wirkung $S = \int dt\, \mathcal{L}[q, \dot{q}]$ d.h. $\frac{\delta S}{\delta q} = 0$ was zu den Bewegungsgleichunen führt.

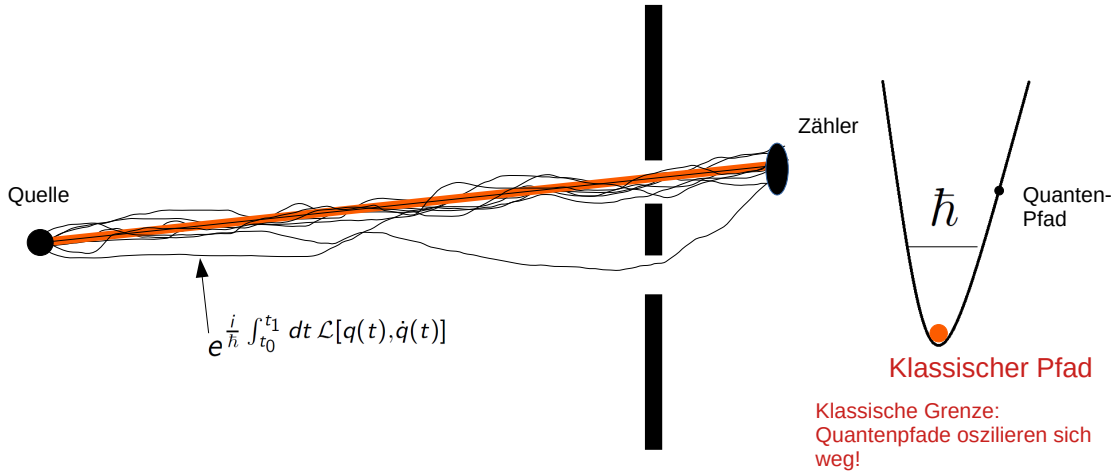
$$\frac{\delta S}{\delta q} = 0 \quad \rightarrow \quad \partial_t \underbrace{\frac{\partial \mathcal{L}(q, \dot{q})}{\partial \dot{q}}}_{p} = \frac{\mathcal{L}(q, \dot{q})}{\partial q} \tag{1.109}$$

Der klassische Pfad ist also der, bei dem die Wirkung minimal (stationär) ist.

In der QM sind alle Pfade möglich und die Wahrscheinlichkeitsamplitude des Übergangs z.B. eines Massenpunktes der zur Zeit t_0 an der Stelle $q(0)$ ist zu der Stelle q_1 ist das Integral über alle Pfade, wobei jeder Pfad die exponentialfunktion der Wirkung als Gewicht bekommt: $e^{iS/\hbar} = e^{\frac{i}{\hbar}\int dt \mathcal{L}[q(t), \dot{q}(t)]/\hbar}$ bekommt:

$$G(q_0, t_0, q_1, t_1) = \int\limits_{\substack{q(t_0) = q_0; \\ q(t_1) = q_1}} [\mathcal{D}q(t)]\, e^{\frac{i}{\hbar}\int_{t_0}^{t_1} dt\, \mathcal{L}[q(t), \dot{q}(t)]} \tag{1.110}$$

Vom Blickwinkel der QM aus, betrachtet man in der klassischen Physik nur die **wahrscheinlichste** aller möglichen Bahnkurven bei der die Wirkung minimal ist. Wenn immer die Effekte der Abweichung viel grössr als $\hbar = 6.6260701510^{-34}$ J s sind, ist dies sehr gut gerechtfertigt. Die nichtklassischen Bahnen "oszillieren sich weg", da der imaginäre Exponent sehr gross ist.



$$G(q_0, t_0, q_1, t_1) = \int_{\substack{q(t_0)=q_0;\\ q(t_1)=q_1}} [\mathcal{D}q(t)]\, e^{\frac{i}{\hbar}\int_{t_0}^{t_1} dt\, \mathcal{L}[q(t),\dot{q}(t)]}$$

Wie erwähnt ist dieser Zugang zur Quantenphysik in der Quantenfeldtheorie sehr wichtig. Allerdings sind die oscilierenden Integrale im Exponenten nicht nur numerisch, sondern auch mathematisch schwer zu fassen und man behandelt die Ausdrücke in einer Euklidischen Formulierung, bei der die Zeit t durch die "Euklidische Zeit" $\boldsymbol{i}\tau$ ersetzt wird. Dann geht das oscillierende Integral $e^{\frac{i}{\hbar}\int_{t_0}^{t_1} dt\, \mathcal{L}[q(t),\dot{q}(t)]}$ in das exponentiell gedämpfte $e^{\frac{-1}{\hbar}\int_{\tau_0}^{\tau_1} d\tau\, \mathcal{L}[q(\tau),\dot{q}(\tau)]}$ über, das sowohl numerisch als auch analytisch sehr viel gutartiger ist.

Ein gebundener Zustand, der in der Minkowski-Welt osziliert wie $e^{\frac{i}{\hbar} t E_b}$, ist in der Euklidischen Welt mit $\tau = \boldsymbol{i}t$ exponentiell gedämpft, $e^{\frac{-1}{\hbar} \tau E_b}$ und kann so auch in der Euklidischen Welt identifiziert werden.

Wir sind deshalb auf diese "stochastische Interpretation" der QM eingegangen weil das Rechnen mit klassischen Computern und einem Zufallsgenerator für gewisse Probleme effizienter sein kann (s. Vorl. XXX) und es durchaus Meinungen gibt dass manche Probleme, die nach heutiger Vorstellung nur auf einem QC efficient behandelt werden können, mit Hilfe stochastischer Methoden auch auf einem klassischen Computer sehr viel effizienter als mit streng deterministischen Methoden gelöst werden können. **Vielleicht** könnte da die Pfadintegral Methode ein Wegweiser sein.

1.3.2 Holographische Quantisierung, AdS/CFT ; noch stärker vereinfacht

Einer **klassichen** Gravitationstheorie in 5 Raum-Zeit Dimensionen entspricht einer **Quanten**feldtheorie in 4 Raum-Zeit Dimensionen.

Etwas spezifischer:

Klassische 5-dimensionale Theorie:

$ds^2 = \frac{1}{x_5^2}(-dx_1^2 - dx_2^2 - dx_3^2 + dx_4^2 + dx_5^2)$ (Anti-de-Sitter Metrik)

$\Updownarrow$

Quantisierte 4-dimensionale Theorie:
$ds^2 = -dx_1^2 - dx_2^2 - dx_3^2 + dx_4^2$, übliche Minkowski Metrik, noch viele zusätzliche Symmetrien (super-conforme Theorie).

Kapitel 2

Qubits in der Quantenmechanik

2.1 Ein Qubit

2.1.1 Informationsgehalt eines Qubits

Der einfachste nicht-triviale Hilbertraum ist zwei-dimensional, er hat also 2 Baisivektoren, $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, seine Elemente heissen Qubits. In der Quanten-Informatik benutzt man meist die computatorische Basis (CB) mit den Vektoren

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{entspricht dem 0-bit in der klassischen Informatik} \tag{2.1}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{entspricht dem 1-bit in der klassischen Informatik} \tag{2.2}$$

Ein Qubit $|\psi\rangle$ ist als Element eines 2-dimensionalen Raumes Summe von 2 Basisvektoren:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad \text{mit } |\alpha|^2 + |\beta|^2 = 1 \tag{2.3}$$

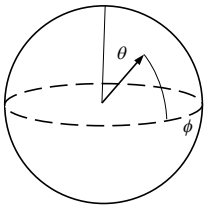
Es kann in die Form gebracht werden:

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\right) \quad 0 \le \theta,\, \phi \le 2\pi \tag{2.4}$$

bloch

Bei der Beobachtung eines Zustands spielt die gemeinsame Phase γ keine Rolle, da wir nur Erwartungswerte $\langle\psi||O\psi\rangle$ messen, zu denen γ nicht beiträgt. Damit ist ein Qubit durch die 2 Winkel θ und ϕ bestimmt, die als Polar und Azimutalwinkel eines Punktes auf einer Einheitskugel betrachtet werden können. Diese Kugel wird als *Bloch-Kugel* bezeichnet. s. Abb.

Man benutzt $\theta/2$ damit für beide Winkel der volle Bereich 0 bis 2π eindeutig ausgefüllt wird. Ohne den Faktor $\frac{1}{2}$ wäre θ, ϕ, γ der gleiche Zustand wie $\theta + \pi, \phi, \gamma + \pi$, dies hat sogar einen tieferen mathematischen Grund



Was ist der Informationsgehalt eines Qubits? Zur vollständigen Bestimmung eines Qubits dienen die Oberflächenpunkte der Bloch-Kugel, 2.4, also liegen die möglichen Parameter in dem ganzen Kontinuum der Kugeloberfläche. Bei Messungen der Komponenten der CB, d.h. mit dem Observablen Operatoren

$$\mathcal{P}_{|0\rangle} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{bzw.} \quad cP_{|1\rangle} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.5}$$

ergibt sich allerdings immer nur das er entweder im Zustand $|0\rangle$ oder $|1\rangle$ ist, und zwar mit der Wahrscheinlichkeit $|\cos^2\frac{\theta}{2}|^2$ bzw $|\sin^2\frac{\theta}{2}|^2$, also im Grunde auch nicht mehr Information als bei einem klassischen bit mit Zufallesgenerator. Wir hatten ja auch als einfachste Anwendumg eines QC den Zufallgenerator kennengelernt (Vorl. 3)

Aber dennoch gibt es grosse Unterschiede: Die information über die Phase ϕ in (2.4) geht zwar bei der Einzelmessung verloren, aber für die zeitliche Entwicklung sind alle Parameter wesentlich. Zwei Zustände mit verschiedener Phase ϕ sind zwei verschiedene Hilbertraum zustände ynd können z.B. ganz verschiedene zeitliche Entwicklungen haben. Ein vielleicht noch wichtigerer Unterschied tritt bei Zustaänden mit 2 oder mehr Qubits auf, die in der Einleitung kurz besprochene Verschränkung. Darauf kommen wir im folgenden noch oft zurück.

Der reiche Informationsinhalt eines Qubits, aber sehr die beschränkte Zugänglichkeit zu diesem macht sich bei einem System aus mehreren Qubits noch stärker bemerkbar, da im Endeffekt immer nur **eine** reelle Zahl gemessen wird. Das Ziel eines Algorithmus muss also sein, dass ein Zustand, und natürlich der jeweils interessanteste, mit sehr hoher Wahrscheinlichkeit gemessen wird. Wie wir später sehen ist dies auch der leitende Gedanke bei zwei sehr wichtigen Quantenalgorithmen, dem von Deutsch und dem von Shore.

Die minimale Entropie eines Qibits ist, wie für alle reinen Zustäde in der QM $S_Q = 0$, die maximale Entropie ist, da $d = 2$ in (1.100) $S_Q = log2$.

2.1.2 Pauli'sche σ Matrizen

In der QM spielen selbstadjungierte Operatoren, $\mathbf{A}^\dagger = \mathbf{A}$ als mögliche Observable eine grosse Rolle. Aus diesen lassen sich durch Exponentierung selbstadtungierte konstruieren:

$$\left(e^{\boldsymbol{i}\mathbf{A}}\right)^\dagger = e^{\boldsymbol{i}\mathbf{A}^\dagger} = e^{-\boldsymbol{i}\mathbf{A}} = \left(e^{\boldsymbol{i}\mathbf{A}}\right)^{-1} \tag{2.6}$$

darstellen.

Die allgemeinst Form eines sa. Operators **A** in 2 Dimensionen ist:

$$A = \begin{pmatrix} a & \beta^* \\ \beta & d \end{pmatrix} \text{ mit } a, b \in \mathbb{R}\ \beta \in \mathbb{C}$$

A lässt sich durch eine Linearkombination der drei sogenannten Pauli Matrizen ($\vec{\sigma}$) und der Einheitsmatrix **I** darstellen, wobei

$$\boldsymbol{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \boldsymbol{\sigma}_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \boldsymbol{\sigma}_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.7}$$ sim

$$A = \tfrac{1}{2}(a+d)\,\mathbf{1} + \ \mathrm{Re}\beta\,\boldsymbol{\sigma}_1 + \ \mathrm{Im}\beta\,\boldsymbol{\sigma}_2 + \tfrac{1}{2}(a-d)\,\boldsymbol{\sigma}_3 \tag{2.8}$$

Wie man leicht nachrechnet sind die 3 σ Matrizen selbstadjungierte Matrizen und erfüllen die Vertauschungsrelationen

$$[\boldsymbol{\sigma}_k, \boldsymbol{\sigma}_n] \equiv \boldsymbol{\sigma}_k\,\boldsymbol{\sigma}_n - \boldsymbol{\sigma}_k\,\boldsymbol{\sigma}_n = 2i\ \epsilon_{knm}\,\boldsymbol{\sigma}_m. \tag{2.9}$$ vr

Sie erfüllen auch die Äntivertauschungsrelationen":

$$\{\boldsymbol{\sigma}_k, \boldsymbol{\sigma}_n\}_+ = \boldsymbol{\sigma}_k\,\boldsymbol{\sigma}_n + \boldsymbol{\sigma}_k\,\boldsymbol{\sigma}_n = 2\,\delta_{ik}\,\mathbf{1} \tag{2.10}$$ avr

Au diesen Relationen und der Selbstadjungiertheit folgen Beziehungen, die einen immer wieder überraschen. z.B.

$$\begin{aligned}(\alpha\,\boldsymbol{\sigma}_k + \beta\,\boldsymbol{\sigma}_n)^\dagger(\alpha\,\boldsymbol{\sigma}_k + \beta\,\boldsymbol{\sigma}_n) &= (\alpha^*\,\boldsymbol{\sigma}_k + \beta^*\,\boldsymbol{\sigma}_n)(\alpha\,\boldsymbol{\sigma}_k + \beta\,\boldsymbol{\sigma}_n) \\ &= \left(|\alpha|^2 + |\beta|^2\right)\mathbf{I} + \alpha^*\beta\left(\tfrac{1}{2}\{\boldsymbol{\sigma}_k, \boldsymbol{\sigma}_n\}_+ \tfrac{1}{2}[\boldsymbol{\sigma}_k, \boldsymbol{\sigma}_n]\right) + \alpha\,\beta^*\left(\tfrac{1}{2}\{\boldsymbol{\sigma}_n, \boldsymbol{\sigma}_k\}_+ \tfrac{1}{2}[\boldsymbol{\sigma}_n, \boldsymbol{\sigma}_k]\right) \\ &= \left(|\alpha|^2 + |\beta|^2 + \mathrm{Re}(\alpha^*\,\beta)\,\delta_{kn}\right)\mathbf{I} - \mathrm{Im}(\alpha^*\,\beta)\,\epsilon_{kn\ell}\,\boldsymbol{\sigma}_\ell\end{aligned}$$

d.h. füer $a, b \in \mathbb{R}$ ist $\frac{1}{\sqrt{a^2+b^2}}(a\,\boldsymbol{\sigma}_k + b\,\boldsymbol{\sigma}_n)$ nicht nur selbstadjungiert, sondern auch **unitär**.

2.1.3 Bahndrehimpuls und Spin

Dies ist eine ganz kurze Wiederholung aus der allgemeinen QM. I. A. sind die Einheiten $\hbar = 1$.

Der Drehimpulsoperator in der QM ist nach dem Korrespondnezprinip

$$\vec{\mathbf{L}} = [\vec{\mathbf{Q}} \times \mathbf{P}];\ \ \mathbf{L}_k = \sum_{rs} \epsilon_{krs}\mathbf{Q}_r\mathbf{P}_s \tag{2.11}$$

Daraus berechnet man mit Hilfe von
$[AB, CD] = A[B, C]D + [A, C]BD + [C, A]BD + C[A, D]B$

$$[\mathbf{L}_k, \mathbf{L}_m] = \boldsymbol{i}\epsilon_{kmn}\mathbf{L}_n \tag{2.12}$$

Aus den Vertauschungsrelationen folgt, dass der Operator

$$\vec{\mathbf{L}}^2 = \mathbf{L}_1^2 + \mathbf{L}_2^2 + \mathbf{L}_3^2 \tag{2.13}$$

mit allen $\mathbf{L}_i$ vertauscht. Seine ganzzahligen Eigenwerte $\ell \cdot (\ell+1)$ bestimmen den Gesamtdrehimpuls $\ell \geq 0$. Die Eigenwerte des Operators $\mathbf{L}_k$ können dann die ganzzahligen Werte $-\ell \leq m \leq \ell$ annehmen.

Der Matrix-operatoren $\frac{1}{2}\boldsymbol{\sigma}_i$ haben die gleichen Vertauschungsregeln wie die Drehimpulsoperatoren.

Da $\frac{1}{4}\sum_k \boldsymbol{\sigma}_k^2 = \frac{1}{2}\cdot\frac{3}{2}$ ist, kann man sagen die $\frac{1}{2}\sigma$ Matrizen sind Spin (auf alt-deutsch Eigendrehimpuls) Operatoren für ein Spin $\frac{1}{2}$ Teilchen

$$\mathbf{J}_k^{(s)} = \tfrac{1}{2}\boldsymbol{\sigma}_k \quad \text{with} \quad [\mathbf{J}_k^{(s)}, \mathbf{J}_n^{(s)}] = i\,\epsilon_{knm}\mathbf{J}_m^{(s)} \tag{2.14}$$

Der Gesamtdrehimpuls ist allgemein die Summe aus dem Bahndrehimpuls und dem Spin:

$$\vec{\mathbf{J}} = \vec{\mathbf{L}} + \vec{\mathbf{J}}^{(s)} \tag{2.15}$$

Die Darstellung (2.7), bei der die Matrix $\boldsymbol{\sigma}_3$ diagonal ist, hat die Basisvektoren

$$|\uparrow_3\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad |\downarrow_3\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.16}$$ mu-si

Hierbei bedeudet $|\uparrow_3\rangle$ dass der Spin in +3-Richtung zeigt, und entsprechend $|\downarrow_3\rangle$ in -3-Richtung.

Man kann sich ein Qubit durch ein Spin 1/2 Teilchen (Elektron oder z.B. Ag-Atom) vorstellen, bei dem der CB Vektor $|0\rangle$ einem $|\uparrow_3\rangle$ und der CN Vektor $|1\rangle$ einem $|\downarrow_3\rangle$ entspricht.

Man rechnet leicht nach, dass die Eigenzustände des Spin-$\frac{1}{2}$-Operators

$$\mathbf{J}_1^{(S)} = \tfrac{1}{2}\boldsymbol{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.17}$$

sind

$$|\uparrow_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}; \quad \tfrac{1}{2}\boldsymbol{\sigma}_1|\uparrow_1\rangle = +\tfrac{1}{2}|\uparrow_1\rangle \tag{2.18}$$

$$|\downarrow_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}; \quad \tfrac{1}{2}\boldsymbol{\sigma}_1|\downarrow_1\rangle = -\tfrac{1}{2}|\downarrow_1\rangle \tag{2.19}$$

Ganz allgemein sind die Drehimpulsoperatoren die "Generatoren" der Drehoperatoren in einem Hilbertraum. Einer Drehung um die Achse $\hat{n}$ mit dem Drehwinkel θ ist im Qubit-Raum ist die unitäre Transformation

$$\mathbf{U}(\hat{n},\theta) = \exp[-i\theta\hat{n}\cdot\vec{\mathbf{J}}] \tag{2.20}$$

zugeordnet im 2-dimensionalen Hilbertraum also

$$\mathbf{U}(\hat{n},\theta) = \exp[-i\frac{\theta}{2}\hat{n}\cdot\vec{\boldsymbol{\sigma}}] = \mathbf{1}\,\cos\frac{\theta}{2} - i\,\hat{n}\cdot\vec{\boldsymbol{\sigma}}\,\sin\frac{\theta}{2} \tag{2.21}$$ rot

Für den letzten Ausdruck wurde die Exponentialfunktion entwickelt und die Anti-vertauschung in (2.9) dabei ausgenutzt.

Wir behandeln im Abschn. 2.2 das Verhalten von Teilchen mit Spin im Magnetfeld.

gq

2.1.4 Quantengatter *quantum gates*

Quantengatter (*quantum gates*) sind eine Übertragung der klassischen Gatter, die auf Bits wirken, in die Quantenwelt. Da die Quantendynamik wahrscheinlichkeitserhaltend und reversibel ist, m""ussen auch die Quanten-Gatter wahrscheinlichkeitserhaltend sein, d.h. unitär.

Für den klassischen Computer gibt es nur ein Gatter, das auf einen einzigen Bit wirkt, das NOT gate:

$$\mathrm{NOT}\{0\} = \{1\}; \quad \mathrm{NOT}\{1\} = \{0\} \tag{2.22}$$

Dem NOT gate entspricht beim Qubit das X-gate:

$$\mathbf{X}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \quad \text{d.h. } \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.23}$$ xgate

Es ist identisch mit der Pauli-Matrix $\boldsymbol{\sigma}_1$. Ein weiteres wichtiges 1-Qubit gate istdas Z gate

$$\mathbf{Z}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} \quad \text{d.h. } \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.24}$$ zgate

Das Hadamard gate $\mathbf{H}$ ist eine Summe der beiden:

$$\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z}) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(\boldsymbol{\sigma}_1 + \boldsymbol{\sigma}_3) \tag{2.25}$$ hgate

Sie wirken auf die CB wie folgt:

Das $\mathbf{X}$ gate vertauscht die beiden Basisvektoren:

$$\mathbf{X}|0\rangle = |1\rangle; \ \mathbf{X}|1\rangle = |0\rangle \tag{2.26}$$

Das $\mathbf{Z}$ gate dreht die Phase des $|1\rangle$

$$\mathbf{Z}|0\rangle = |0\rangle; \ \mathbf{Z}|1\rangle = -|1\rangle \tag{2.27}$$

Das $\mathbf{H}$ gate macht die Überlagerung:

$$\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big); \ \mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big); \tag{2.28}$$ hgate2

2.1.5 Zeitliche Entwicklung eines Qubits

Die zeitliche Entwicklung eines reinen Zustandes $|\psi, t\rangle$ (Schrödingerbild) ist allgemein gegeben durch (s. Axiom XXX).

$$|\psi, t\rangle = e^{\boldsymbol{i}\mathbf{H}t}|\psi\rangle \tag{2.29}$$

Die allgemeinste Form eines (Raum- und Zeit-unabhängigen) Hamiltonoperators im 2-dimensionalen (Qubit) Raum ist

$$\mathbf{H} = \begin{pmatrix} a & c\,e^{\boldsymbol{i}\psi} \\ c\cdot e^{-\boldsymbol{i}\psi} & b \end{pmatrix}; \quad a, b, c, \psi \in \mathcal{R} \tag{2.30}$$

Ist $|\psi_E\rangle$ ein Eigenwert von $\mathbf{H}$, d.h

$$\mathbf{H}|\psi_E\rangle = E|\psi_E\rangle \tag{2.31}$$

dann gilt:

$$|\psi_E, t\rangle = e^{\boldsymbol{i}Et}|\psi_E\rangle \tag{2.32}$$

Schreiben wir die Eigenwertgleichung (hier 2 lineare Gleichungen) als

$$(\mathbf{H} - E\mathbf{I})|\psi_E\rangle = 0 \tag{2.33}$$

sehen wir sofort, dass für eine nichttriviale Lösung gelten muss:

$$\det(\mathbf{H} - E\mathbf{I}) = || \begin{pmatrix} a-E & c\,e^{\boldsymbol{i}\psi} \\ c\cdot e^{-\boldsymbol{i}\psi} & b-E \end{pmatrix} || = 0 \tag{2.34}$$ sec

Aus (2.34) bestimmen wir die Die Eigenwerte von $\mathbf{H}$ zu:

$$\mathbf{H}|\pm\rangle = E_\pm|\pm\rangle; \quad E_\pm = \frac{a+b}{2} \pm \sqrt{\frac{(a-b)^2}{4} + c^2} \tag{2.35}$$

die Eigenzustände sind:

$$|+\rangle = \begin{pmatrix} C_+ \\ S_+ \end{pmatrix}, \quad \text{with } C_+ = \cos\phi_+,\ S_+ = e^{-\boldsymbol{i}\psi}\sin\phi_+; \quad \tan\phi_+ = \frac{E_+ - a}{c} \tag{2.36}$$

$$|-\rangle = \begin{pmatrix} S_- \\ C_- \end{pmatrix}, \quad \text{with } C_- = \cos\phi_-,\ S_- = e^{+\boldsymbol{i}\psi}\sin\phi_-; \quad \tan\phi_- = \frac{E_- - b}{c} \tag{2.37}$$

mit der Zeitabhängigkeit:

$$e^{\boldsymbol{i}Ht/\hbar}\left(\alpha_+|+\rangle + \alpha_-|-\rangle\right) = \alpha_+\, e^{\boldsymbol{i}E_+t/\hbar}|+\rangle + \alpha_-\, e^{\boldsymbol{i}E_-t/\hbar}|-\rangle \tag{2.38}$$

wobei α_+, α_- aus den Anfangsbedingunen folgen: $\alpha_\pm = \langle\pm|\psi\rangle$.

Besonders informativ ist die Situation für den Fall a = b.

Dann gilt: $E_\pm = a \pm |c|$ und $\phi_\pm = \pm\pi/4$

$|+\rangle = \begin{pmatrix} \cos\frac{\pi}{4} \\ e^{-\boldsymbol{i}\psi}\sin\frac{\pi}{4} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ e^{-\boldsymbol{i}\psi} \end{pmatrix} \equiv \frac{1}{\sqrt{2}}(|0\rangle + e^{-\boldsymbol{i}\psi}|1\rangle)$

$|-\rangle = \begin{pmatrix} e^{\boldsymbol{i}\psi}\sin\left(-\frac{\pi}{4}\right) \\ \cos\frac{\pi}{4} \end{pmatrix} = \frac{-1}{\sqrt{2}}\begin{pmatrix} e^{\boldsymbol{i}\psi} \\ -1 \end{pmatrix} \equiv \frac{-1}{\sqrt{2}}(e^{\boldsymbol{i}\psi}|0\rangle - |1\rangle$

Betrachten wir den Ausgangszustand $|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ Dann ist $\alpha_+ = \frac{1}{\sqrt{2}},\ \alpha_- = -\frac{e^{-\boldsymbol{i}\psi}}{\sqrt{2}}$

$$\begin{aligned}
|\psi, t\rangle &= \frac{1}{\sqrt{2}}e^{i(a+|c|)t/\hbar}\alpha_+|+\rangle + \frac{1}{\sqrt{2}}e^{i(a-|c|)t/\hbar}\alpha_-|-\rangle \\
&= \frac{1}{2}(e^{\boldsymbol{i}(a+|c|)t/\hbar}|+\rangle + e^{\boldsymbol{i}(a-|c|)t/\hbar}e^{-\boldsymbol{i}\psi}|-\rangle) \\
&= \tfrac{1}{2}e^{\boldsymbol{i}at/\hbar}\left(|0\rangle(e^{\boldsymbol{i}|c|t/\hbar} + e^{-\boldsymbol{i}|c|t/\hbar}) + |1\rangle e^{-i\psi}(e^{\boldsymbol{i}|c|t/\hbar} - e^{-\boldsymbol{i}|c|t/\hbar})\right) \\
&= e^{\boldsymbol{i}at/\hbar}\left(\cos\frac{|c|t}{\hbar}|0\rangle + \sin\frac{|c|t}{\hbar}\,e^{-i\psi}|1\rangle\right)
\end{aligned}$$

Die gemeinsame Phase $e^{ia\,t/\hbar)}$ ist ohne weiteren Belang. Interessant ist, dass der Zustand nach der Zeit $\frac{|c|t_\perp}{\hbar} = \frac{\pi}{2}$, d.h. nach $t_\perp = \frac{\pi\hbar}{2|c|} = \frac{\pi\hbar}{E_+ - E_-}$ vom Zustand $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ zum orthogonalen Zustand $\boldsymbol{i}e^{-\boldsymbol{i}\psi}|1\rangle = \begin{pmatrix} 0 \\ \boldsymbol{i}e^{-\boldsymbol{i}\psi} \end{pmatrix}$ übergeht.

Ganz allgemein sieht man direkt: Haben wir zwei Zustände $|0\rangle$ und $|2E\rangle$ mit der Energie respective 0 und $2E$, so geht der Zustand $|\psi(0)\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |2E\rangle)$ nach der Zeit $t = \frac{\pi\hbar}{2E}$ in den orthogonalen Zustand $|\psi(0)\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |2E\rangle)$ über. Dies wird in arXiv:quant-ph/9710043v2 zur Basis von überlegungen zur Maximalgeschwindigkeit dynamischer Entwicklungen gemacht (Vorsicht: die Autoren benutzen sowohl $\hbar$ als auch $h = \hbar/(2\pi)$)

Man beachte dass durch die zeitliche Entwicklung die Relative Phase vom Zustand zur Zeit $t = 0$ zu allen Zuständen einer späteren Zeit festgelegt ist.

Um einigermassen stabile Zustände zu erreichen, muss man den Anfangszustand so wählen, dass er in einem Grundzustand (in obigem Falle also $|-\rangle$ ist oder in einem angeregten atomaren Zustatnd , der aufgrund der Quantenzahlen metastabil ist, z.B. in einem $^3P_2$ Zustand über einem $^1S_0 - Zustand$. Den angeregten metastabilen Zustand kann man durch otisches Pumpen, z.B. über einen noch höheren Zustand bevölkern.

st-g

2.2 Der Stern Gerlach Vesuch als Prototyp einer Messung

2.2.1 Drehimpuls und magnetisches Moment

Ein wichtiges physikalisches System, das in einem 2-dimensionalen Hilbertraum beschrieben wird und das Physikern besonders vertraut ist, ist ein Teilchen mit Spin 1/2. Wir wollen hier nicht die ganze Drehimpulsgymnastik vorführen, die auf der Darstellungstheorie der Drehgruppe basiert, sondern beschränken uns auf die Ergebnisse. Besonderes Augenmerk richten wir dbei auf den Messprozess, der sich hier in vielen seinen Facetten sehr anschaulich darstellen lässt.

Nach den Gesetzen der klassischen Elektrodynamik und dem Korrespondenprinzips leitet man für die Wechselwirkungsenergie eines auf einer geschlossenen Bahn sich bewegenden geladenen Teilchens mit dem Drehimpuls $\vec{\mathbf{L}}$ und einem Magnetfeld $\vec{B}$ die Wechselwirkungsenergie

$$H_W = \mu(\vec{\mathbf{L}} \cdot \vec{B}), \tag{2.39}$$

wobei $\mu = \frac{e\hbar}{2m}$ mit e der Ladung und m der Masse des Teilchens ist.

Für Ladung und Masse eines Elektrons hat μ den Wert

$$\mu_B = -9.27\ldots \text{ J/T (Joule durch Tesla).}$$

(Das $-$ Zeichen kommt von der negativen Ladung des Elektrons)

Für ein Elektron ist die Beziehung zwischen Energie im Magnetfeld und Gesamtdrehimpuls:

$$H_W = -\mu_B(\vec{\mathbf{L}} + \mu_{an}\tfrac{1}{2}\vec{\boldsymbol{\sigma}}) \cdot \vec{B} \quad \mu_{an} \approx 2 \tag{2.40}$$

muH

Die Geschichte des Spins, des Drehimpulses und der magnetischen Momente ist ein *high-Tech* und ein *High-Math*-Krimi mit den hauptsächlichen Helden Pauli [1], Dirac, Weil und Stern. Er gab der Entwicklung der modernen Physik (und Technik) wesentliche Impulse.

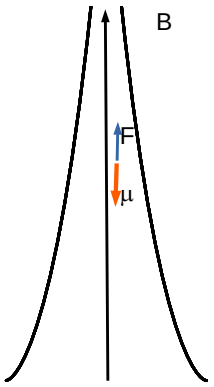
Das magnetische Moment erlaubt eine einfache Messung des Spins $\mathbf{J}_3^{(S)}$ eines Teilchens.

Ein inhomogenes Magnetfeld übt auf einen Dipol eine Kraft aus, sie ist in der klassischen E-dynamik

$$F = \vec{\partial}(\mu \cdot B) \tag{2.41}$$

Ist kann man die Ortsabhängigkeit von μ vernachlässigen, so erhält man:

$$F_i = \sum_k (\mu_k \cdot \frac{\partial}{\partial x_i} B_k(x)) \tag{2.42}$$



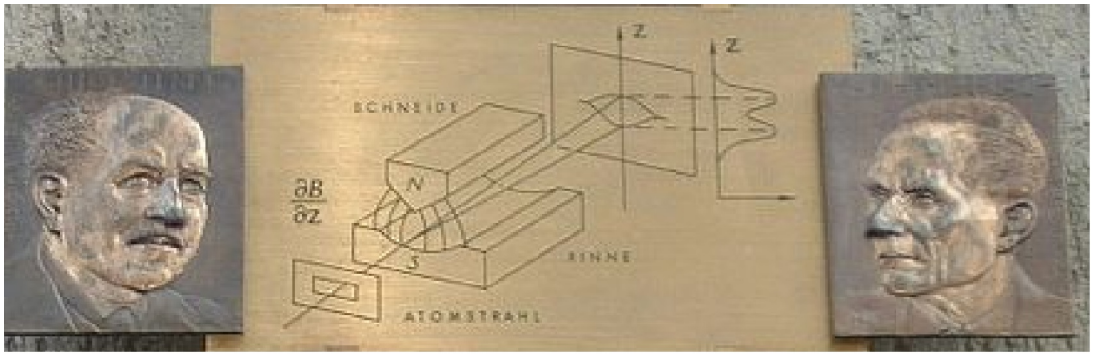
Haben wir ein starkes Magnetfeld in 3 Richtung mit einer geringen Inhomogenität $\partial_3 B_3 > 0$ so wird eine Komponente $(\vec{\mu} \cdot \vec{F}) > 0$ nach oben und die andere $(\vec{\mu} \cdot \vec{F}) < 0$ nach unten abgelenkt.

Das magnetische Moment eines Elektrons is, s. (2.40) ist $-\mu_{an}\mu_B \underbrace{\mathbf{J}_3^{(S)}}_{\frac{1}{2}\sigma_3}$ und deswegen werden die beiden möglichen Spin-Einstellungen $\pm\frac{1}{2}$ in verschiedene Richtungen abgelenkt.

Man betrachtet einen Strahl von Spin $\frac{1}{2}$ Teilchen, z.B. neutrale Silberatome, bei denen nur der Spin des Aussenelektrons ($\mathbf{L} = 0$) beiträgt.

Dass Stern und Gerlach diese Aufspaltung 1922 tatsächlich nachweisen konnten, war ganz emtscheidend für die Akzeptanz der QM, (d.h. der alten QM von Planck, Einstein, Bohr

[1] Eine zusätzliche Pointe: Der Spin als Eigendrehimpuls $\frac{1}{2}$ wurde 1925 von den jungen Physikern Goudsmit und Uhlenbeck vorgeschlagen. Sie bekamen nach der Einreichung der Arbeit kalte Füsse und wollten sie zurückziehen. Aber der Herausgeber Ehrenfest, meinte: "Sie sind beide jung genug, um sich eine Dummheit leisten zu können"



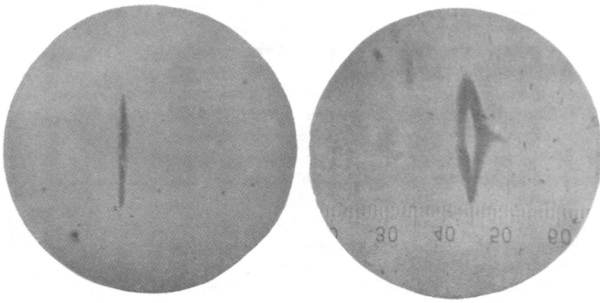


Fig. 2. Fig. 3.

Abbildung 2.1: Tafel zur Erinnerung an das Stern-Gerlach Experiment in Frankfurt, Abb. der Aufspaltung aus der Originalarbeit

969 und Sommerfeld). Pauli an Gerlach: „Jetzt wird wohl auch der ungläubige Stern von der
970 Richtungsquantelung überzeugt sein." Die Zweifel Stern's waren zu dieser Zeit mehr als
971 berechtigt: 1922 gab es noch keine Quanten**theorie** sondern nur zusätzliche Vorschriften zur
972 klassischen Physik.

973 2.2.2 Der Stern Gerlach Versuch als Realisierung eines Messpro-
974 zesses

975 Der Stern-Gerlach Versuch ist also eine Realisierung für den Messprozess der Drehimpulskon-
976 ponente $(\vec{e}_H \cdot \vec{\mathbf{J}})$. Ist die (Haupt-)Richtung des Magnetfelds die z-Achse, so ist die Observable
977 $\mathbf{J}_3 = \frac{1}{2}\boldsymbol{\sigma}_3$ und die beiden Messoperatoren sind die Projektionen

$$\mathbf{P}_{\uparrow 3} = |\uparrow_3\rangle\langle\uparrow_3| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{2.43}$$

$$\mathbf{P}_{\downarrow 3} = |\downarrow_3\rangle\langle\downarrow_3| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.44}$$

Ein Zustand $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, mit $|\alpha|^2 + |\beta|^2 = 1$ wird also nach dem quantenmechanischem Messprozess (Axiom 3) sich mit der Wahrscheinlichkeit

$||\mathbf{P}_{\uparrow 3}|\psi\rangle||^2 = |\alpha|^2$ im Zustand $\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\uparrow_3\rangle$

befinden und mit der Wahrscheinlichkeit

$||\mathbf{P}_{\downarrow 3}|\psi\rangle||^2 = |\beta|^2$ im Zustand $\begin{pmatrix} 0 \\ 1 \end{pmatrix} = |\downarrow_3\rangle$.

Schicken wir einen Strahl von Teilchen in diesem Zustand $|\psi\rangle$ durch einen in z Richtung inhomogenen Magneten (Abb. 2.2) so wird die $|\uparrow\rangle$ Komponente in Richtung des abnehmenden Magnetfelds abgelenkt, und ensprechend, die $|\downarrow\rangle$ in die entgegengestzte Richtung. Die Intensität des einen abgelenkten Strahles ist also $|\alpha|^2$, die des anderen $|\beta|^2$.

Schicken wir den einen Strahl, der sich nach der Ablenkung im Zustand $\mathbf{P}_{\uparrow 3}|\psi\rangle$durch einen zweiten Stern Gerlach in z Richtung, wird dieser nicht mehr aufgespalten (Abb. 2.2.

Wird der Magnet so gedreht, dass die Hauptrichtung des Feldes in die x-Achse zeigt, so ist die Observable $\mathbf{J}_1 = \frac{1}{2}\boldsymbol{\sigma}_1$ und die beiden Messoperatoren sind die Projektionen

$$\mathbf{P}_{\uparrow 1} = |\downarrow_1\rangle\langle\downarrow_1| = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \tag{2.45}$$

$$\mathbf{P}_{\downarrow 1} = |\downarrow_1\rangle\langle\downarrow_1| = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \tag{2.46}$$

Der gleiche Zustand $\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ wird also nach der Messung sich mit der Wahrscheinlichkeit

Wird der Magnet so gedreht, dass die Hauptrichtung des Feldes in die x-Achse zeigt, so ist die Observable $\mathbf{J}_1 = \frac{1}{2}\boldsymbol{\sigma}_1$ und die beiden Messoperatoren sind die Projektionen

$$\mathbf{P}_{\uparrow 1} = |\downarrow_1\rangle\langle\downarrow_1| = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \tag{2.47}$$

$$\mathbf{P}_{\downarrow 1} = |\downarrow_1\rangle\langle\downarrow_1| = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \tag{2.48}$$

Der gleiche Zustand $\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ wird also nach der Messung sich mit der Wahrscheinlichkeit

$||\mathbf{P}_{\uparrow 1}|\psi\rangle||^2 = |\alpha + \beta|^2$ sich im Zustand $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |\rightarrow_1\rangle$ befinden und mit $||\mathbf{P}_{\downarrow 1}|\psi\rangle||^2 = |\alpha - \beta|^2$ sich im Zustand $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = |\downarrow_1\rangle$.

Die Intensität des einen abgelenkten Strahles ist also $\frac{1}{4}|\alpha + \beta|^2$, die des anderen $\frac{1}{4}|\alpha - \beta|^2$. Schicken wir den einen Strahl im Zustand $\mathbf{P}_{\uparrow 1}|\psi\rangle$ durch einen zweiten Stern Gerlach in x Richtung, wird dieser nicht mehr aufgespalten, da gilt $\mathbf{P}_{\uparrow 1}\mathbf{P}_{\uparrow 1}|\psi\rangle = \mathbf{P}_{\uparrow 1}|\psi\rangle$

Der grösste Widerspruch zur klassischen Erwartung entsteht, wenn wir erst an einen Strahl der nur aus $|\uparrow_3\rangle$ besteht durch einen nach $\mathbf{J}_1$ sortierenden Stern-Gerlach schicken und an dem den Teill mit den $|\rightarrow_1\rangle$ noch eimal $\mathbf{J}_3$ misst.

Da der Strahl beim ersten Stern-Gerlach schon nach dem Spin in $+z$-Richtung sortiert wurde, erwartet man nach den Prinzipien der klassischen Physik dass er nun nicht mehr aufspaltet, da ja im 1. Versuch nur $|\uparrow_3\rangle$ ausgewählt wurden.

Die QM liefert aber ein anderes Resultat. Nach dem Durchgang durch durch den 1. Stern Gerlach befindet sich $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ im Zustand $\mathbf{P}_{\uparrow 3}|\psi\rangle = \begin{pmatrix} \alpha \\ 0 \end{pmatrix}$. Nachdem durchgang durch den 2. Stern-Gerlach, der nach $\mathbf{J}_1$ sortiert, ist der Teil, dessen Spin in $+x$ Richtung zeigt nach dem Messaxiom im Zustand

$$\mathbf{P}_{\uparrow 1} \cdot \mathbf{P}_{\uparrow 3}|\psi\rangle = \tfrac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} \alpha \\ 0 \end{pmatrix} = \tfrac{1}{2}\alpha\begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{2.49}$$

enthält also wieder eine $|\downarrow_3\rangle$ Komponente und zwar mit der gleichen Intensität wie die $|\uparrow_3\rangle$ Komponente,Siehe Abb. 2.3. stern-b

Dass der Zustand nach der 2. Messung eine kleine $|\downarrow_3\rangle$ Komponente enthält, könnte man klassisch ja noch als Verunreinigung durch die 2. Messung verstehen, aber beobachtet ist genau die quantenmechanische Vorhersage.

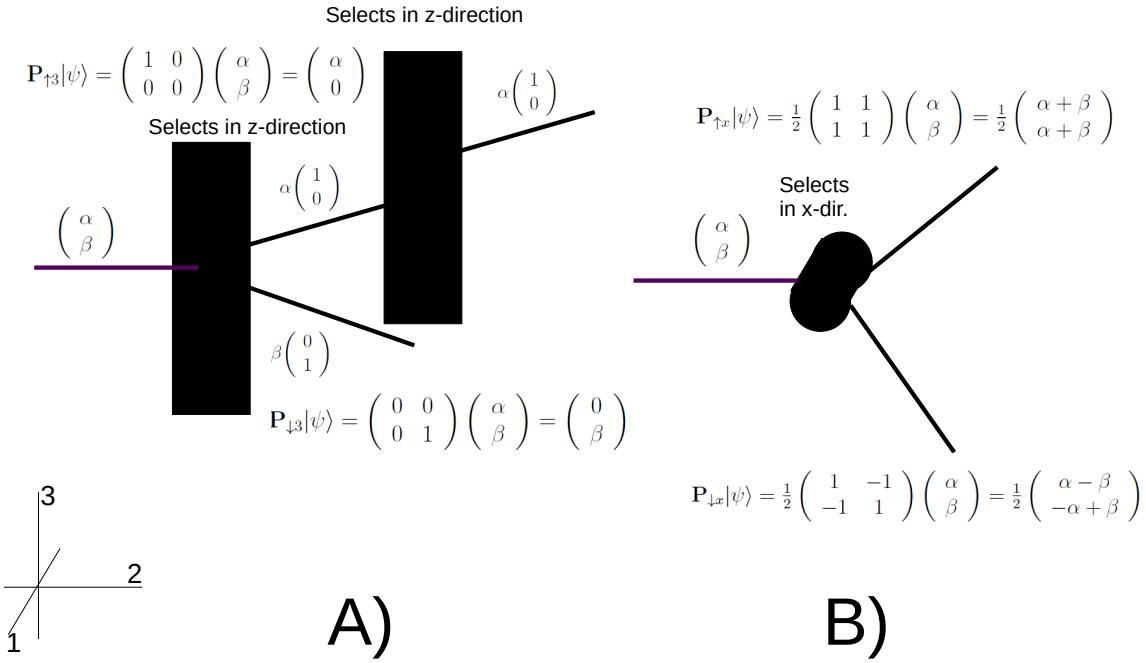


Abbildung 2.2: stern-a

Dieses Ergebnis, inclusive der Intensität, wird von der QM voehergasagt und ist in vielen Fällen bestätigt. Dennoch ist es keine direkte Widerlegung der klassischen Vorstellung, denn man kann sich ja immer noch vorstellen, dass bei der Messung durch eine noch unbekannten Parameter die Aufspaltung beeinflusst wird. Dies wird in der Bohm'schen Formulierung der QM versucht.

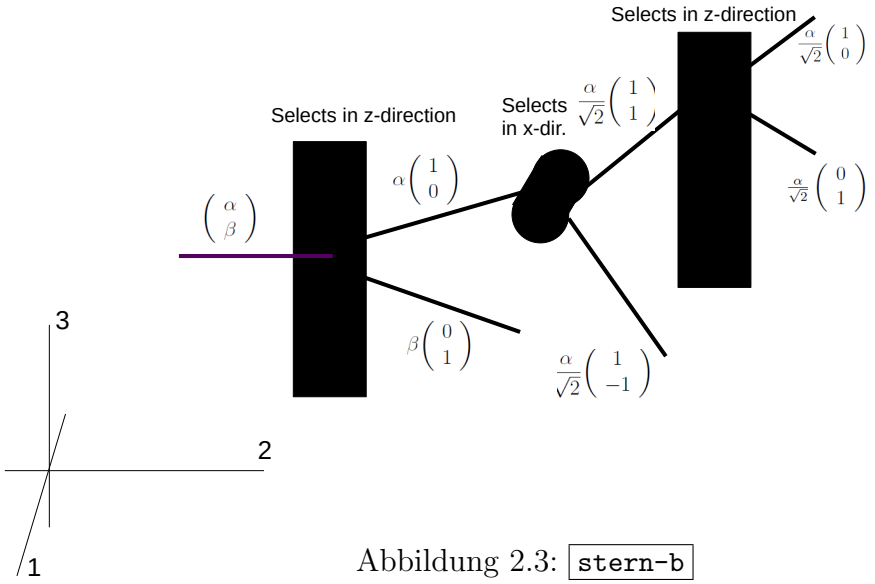


Abbildung 2.3: stern-b

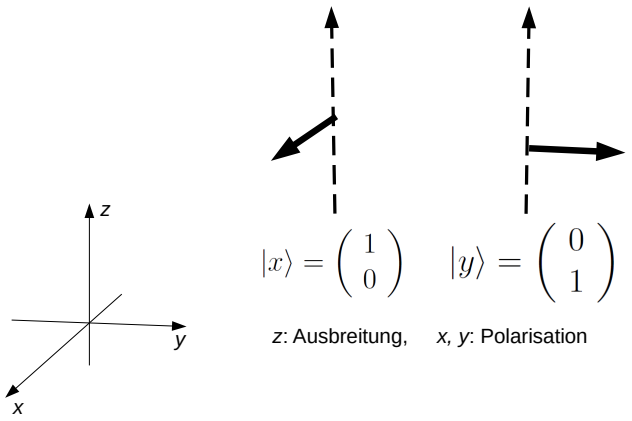
2.2.2.0.1 Stern-Gerlach als Prototyp einer Präparation oder eines Gatters Ein einzelnes Teilchen, das durch einen Stern-Gerlach in z Richtung in $+z$ Richtung abgelenkt wurde, ist sicher im Zustand $\begin{pmatrix}1\\0\end{pmatrix}$. Wird dieses Teilchen um die y Achse um 90 Grad gedreht, z.b. in dem man es durch einen x-gerichteten Stern-Gerlach schickt und idas $+x$ Richtung abgelenkte selektiert, befindet es sich sicher im Zustand $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$. Drehen wir diesen Spinor, beispielsweise um die y-Achse um den Winkel θ, so ist er, danach im Zustand, s.(2.21)

$$\mathbf{U}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}=\begin{pmatrix}\cos\frac{\theta}{2} & -\boldsymbol{i}\sin\frac{\theta}{2}\\ \boldsymbol{i}\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}e^{-\boldsymbol{i}\frac{\theta}{2}}\\ e^{\boldsymbol{i}\frac{\theta}{2}}\end{pmatrix}=\frac{e^{-\boldsymbol{i}\frac{\theta}{2}}}{\sqrt{2}}\begin{pmatrix}1\\ e^{\boldsymbol{i}\theta}\end{pmatrix} \tag{2.50}$$

2.2.2.1 Polarisierte Photonen

Mögliche wichtige Realisierungen von Qubits sind Photonen, die Quanten des em Feldes. Sie haben zwar den Gesamtspin 1, aber da die Felder einer elektromagnetischen Welle steht senkrecht zur Ausbreitungsrichtung stehen, gibt es nur zwei linear unabhängige Polarisationsrichtungen. Daher haben die Photonen 2 Polarisationszustände senkrecht zu IHilberträumer Ausbreitungsrichtung. Sie sind deswegen auch mögliche Realisierungen eines Qubits. Im folgenden sei die Ausbreitungsrichtung die 3-Richtung, die z-Achse, dann zeigen die Polarisationen in die 1 oder 2-Richtung, die x und die y Achse. Wir wollen diese beiden Zustände mit $|x\rangle$ und $|y\rangle$ bezeichnen, die wir wider durch Spinoren darstellen können

$$|x\rangle\equiv\begin{pmatrix}1\\0\end{pmatrix};\qquad |y\rangle\equiv\begin{pmatrix}0\\1\end{pmatrix} \tag{2.51}$$



Bei einer Drehung um die Ausbreitungs (z) Richtung gilt":

$$|x\rangle \rightarrow \cos\theta|x\rangle + \boldsymbol{i}\,\sin\theta|y\rangle \tag{2.52}$$
$$|y\rangle \rightarrow -\boldsymbol{i}\,\sin\theta|x\rangle + \cos\theta|y\rangle \tag{2.53}$$

Die unitäre Darstellung dieser Drehung ist also

$$\mathbf{U}(\theta) = \begin{pmatrix} \cos\theta & \boldsymbol{i}\,\sin\theta \\ -\boldsymbol{i}\,\sin\theta & \cos\theta \end{pmatrix} \tag{2.54}$$

Die bei einem Emissionsprozess erzeugten Photonen sind i. A. Eigenzustände dieser Matrix, die sog. rechts und links-polarisierten Photonen:

$$|R\rangle = \sqrt{\tfrac{1}{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}; \quad |L\rangle = \sqrt{\tfrac{1}{2}}\begin{pmatrix} i \\ 1 \end{pmatrix} \tag{2.55}$$

mit

$$\mathbf{U}(\theta)|R\rangle = e^{i\theta}|R\rangle;\ \mathbf{U}(\theta)|L\rangle = e^{-i\theta}|L\rangle \tag{2.56}$$

$|R\rangle$, $|L\rangle$ sind Eigenvektoren zu dem Generator der Rotation um die z-Achse: $\mathbf{J} = \boldsymbol{\sigma}_2$ mit den Eigenwerten ± 1.

2.3 2 und mehr Qubits

2.3.1 Notation

Wir wählen für Qubits generell die Notation:

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |+\tfrac{1}{2}\rangle; \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |-\tfrac{1}{2}\rangle \tag{2.57}$$

und für mehrere Qubits:

$$|m\,n\,r,\cdots\rangle \equiv |m\rangle \otimes |n\rangle \otimes |r\rangle \otimes \cdots \quad m,n,r \in 0,1 \tag{2.58}$$

Wollen wir die Basisvektoren abzählen, hilft das Dualsystem. Jede Zahl j kann eindeutig als Dualzahl dargestellt werden $j = \sum_k m_k\, 2^k$. Für den ℓ-Qubit Zustand $|m_\ell\, m_{\ell-1}\, \cdots m_0\rangle$ können wir abgekürzt schreiben:

$$|m_\ell\, m_{\ell-1}\, \cdots m_0\rangle = |j\rangle_d \quad \text{wobei} \;\; j = m_\ell \cdot 2^\ell + m_{\ell-1} \cdot 2^{\ell-1} + \cdots + m_0 \cdot 2^0$$

Das Subskript d wird von den an das Dualsystem gewöhnten Informatikern oft weggelassen, wenn eine Zahl grösser als 1 im $|\rangle$ oder $\langle$ steht, wird diese als Dualzahl interpretiert. z.B.

$$|1\rangle_A \otimes |0\rangle_B \otimes |1\rangle_C \equiv |1\,0\,1\rangle \equiv |5\rangle_d \quad \text{in Cartesischer Basis} \equiv \begin{pmatrix} 0\\0\\0\\0\\0\\1\\0\\0 \end{pmatrix}$$

2.3.2 Quantenteleportation

Der Zustand aus 2 Spins mit dem Gesamtspin 0 hat die Form:

$$\frac{1}{\sqrt{2}}\big(|\uparrow_3\rangle_A \otimes |\downarrow_3\rangle_B - |\downarrow_3\rangle_A \otimes |\uparrow_3\rangle_B\big) \equiv \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{2.59}$$ ver

$$\text{d.h. } \vec{\mathbf{J}}^2_{AB}\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = 0; \text{ mit } \quad \vec{\mathbf{J}}^2_{AB} = (\frac{1}{4}(\vec{\boldsymbol{\sigma}}_A \otimes \mathbf{I}_B + \mathbf{I}_A \otimes \vec{\boldsymbol{\sigma}}_B)^2 \tag{2.60}$$

Informatiker lassen zwar meist die Indices $_{A,B}$ weg, sprechen aber gern vom ersten Hilbertraum mit der Beobachterin Alice und vom zweiten mit dem Beobachter Bob. In einer Vorlesung über QC ist es sinnvoll, sich dieser Konvention anzuschliessen.

Angenommen, Alice und Bob bbefinden auf zwei Raumstationen die weit auseinander liegen. In der Mitte zerfällt ein Zustand mit dem Gesamtspin 0 in zwei Spin $\frac{1}{2}$ Teilchen. Der Zustand ist also:

$$|\psi(t)\rangle = A(y_1,t)\,B(y_2,t)(|\uparrow_3\rangle_A \otimes |\downarrow_3\rangle_B - |\downarrow_3\rangle_A \otimes |\uparrow_3\rangle_B) \equiv A(y_1,t)\,B(y_2,t)(|01\rangle - |10\rangle)$$

Die Wellenpakete $A(y,t)\,B(y,t)$ überlappen zur Zeit $t = 0$, $\phi_A(y,t)$ fliegt nach links zu Alice, $\psi_B(y,t)$ nach rechts zu Bob, zu einem späteren Zeitpunkt haben A und B weit entfernte Träger.

Auf beiden Raumstationen sind Stern Gerlachs installiert, die beide streng parallel in z Richting ausgerichtet sind. Allice und Bob messen also beide die Observable $\mathbf{J}_3 = \frac{1}{2}\boldsymbol{\sigma}_3$.

Wenn Alice zur Zeit τ bei der Messung einen nach oben abgelenkten Zustand findet (d.h. $|\uparrow_3\rangle$), so ist der Zustand zu $B(y,\tau)(|\uparrow_3\rangle_A \otimes |\downarrow_3\rangle_B)$ kollabiert:

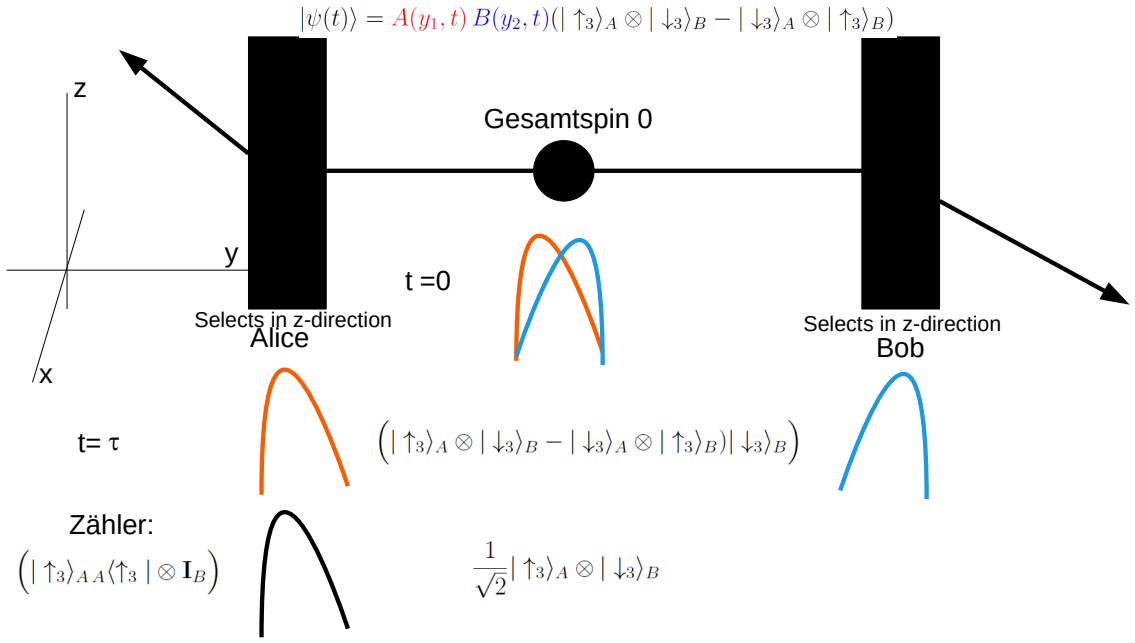
$$|\psi(\tau)\rangle \;\rightarrow\; \overbrace{\int dy_1 Z_A(y_1)\, A(\tau, y_1)}^{\approx 1}\; B(\tau, y_2)) \tag{2.61}$$

$$\Big(|\uparrow_3\rangle_{A\,A}\langle\uparrow_3| \otimes \mathbf{I}_B\Big)\Big(|\uparrow_3\rangle_A \otimes |\downarrow_3\rangle_B - |\downarrow_3\rangle_A \otimes |\uparrow_3\rangle_B)|\downarrow_3\rangle_B\Big) \tag{2.62}$$

$$= B(\tau, y^{(2)})\,|\downarrow_3\rangle_B \tag{2.63}$$

und sie weiss in dem Augenblick der Mewssung, dass Bob, wenn er die Messung auch zum gleichem Augenbklick durchführt, den Spin seines Teilchens nach unten gerichtet messen muss. Allerdings wird damit keine Information und keine Materie transportiert!

Etwas realistischer ist das analoge Gedankenexperiment mit links und rechtspolarisierten Photonen.



I

Obwohl die Änderung (Kollaps) der Wellenfunktion instantan ist, lassen sich damit keine Signale mit Überlichtgeschwindigkeit übermitteln, da ja Bob nicht das Ergebnis der Messung von Alice kennt.

2.3.3 Zeitliche Entwicklung in einem Produktraum

Seien $\mathcal{H}_A$ und $\mathcal{H}_B$ zwei isomorphe Hilberträume (gleiche Dimension). Wir wollen zeigen, dass es keine zeitliche Entwicklung (oder allgemein keine unitäre Entwicklung) gibt, die beliebigen einen Zustand von $\mathcal{H}_A$ nach $\mathcal{H}_B$ kopiert.

NB: $(\mathbf{A}|\lambda\rangle)^\dagger = \langle\lambda|\mathbf{A}^\dagger|$; $\quad$ $\mathbf{U}$ unitär: $\mathbf{U}^\dagger\mathbf{U} = \mathbf{I}$; z. B. $\mathbf{U} = e^{i\mathbf{H}t}$;

Seien $|\psi\rangle$, $|\phi\rangle$, $|\eta\rangle$ drei Quantenzustände (d.h. normierte Vektoren) aus $\mathcal{H}_A$ oder $\mathcal{H}_B$. Die unitäre Transformation $\mathbf{U}$ in $\mathcal{H}_A \otimes \mathcal{H}_b$ soll Zustände von $\mathcal{H}_A$ nach $\mathcal{H}_B$ "kopieren", dh. es soll gelten:

$$\mathbf{U}\left(|\psi\rangle \otimes |\eta\rangle\right) = \left(|\psi\rangle \otimes |\psi\rangle\right); \qquad \mathbf{U}\left(|\phi\rangle \otimes |\eta\rangle\right) = \left(|\phi\rangle \otimes |\phi\rangle\right) \tag{2.64}$$ hyp

Daraus (2.64) folgt:

$$\langle\left(\langle\psi| \otimes \langle\eta|\right)\mathbf{U}^\dagger|\mathbf{U}\left(|\phi\rangle \otimes |\eta\rangle\right)\rangle = \langle\left(\langle\psi| \otimes \langle\psi|\right)|\left(|\phi\rangle \otimes |\phi\rangle\right)\rangle = \langle\psi|\phi\rangle\,\langle\psi|\phi\rangle \tag{2.65}$$ hyp2

aus der Unitarität folgt:

$$\langle\left(\langle\psi| \otimes \langle\eta|\right)\mathbf{U}^\dagger|\mathbf{U}\left(|\phi\rangle \otimes |\eta\rangle\right)\rangle = \langle\left(\langle\psi| \otimes \langle\eta|\right)|\left(|\phi\rangle \otimes |\eta\rangle\right)\rangle = \langle\psi|\phi\rangle\,\langle\eta|\eta\rangle \tag{2.66}$$ hyp3

d.h. aus (2.65) und (2.66) folgt $\langle\psi|\phi\rangle^2 = \langle\psi|\phi\rangle$ (2.67)

Daraus folgt, dass entweder $\langle\psi|\phi\rangle = 1$ oder $\langle\psi|\phi\rangle = 0$ sein muss. Die Transformation (2.64) gilt also nichttrivial nur, wenn $|\psi\rangle \perp$ auf $|ph\rangle$ steht. Damit ist gezeigt, dass es keine allgemeine unitäre "Kopiertransformation" für Quantenzustände gibt.

William Wootters und Wojciech Zurek (1982)

2.3.4 Die Bellschen Ungleichungen

Grob gesagt: Die Bell'schen Ungleichungen gälten, wenn die Physik so realistisch wäre, wie Einstein es sich vorstellte. Ihre Verletzung besagt: Selbst wenn man neben den beobachtbaren Grössen noch verborgene Paramter einführt, so müssen diese die selben spukhaften, d.h. nichtlokalen Eigenschaften haben, die Einstein (und viele andere) an der QM kritisierten. Schon sehr bald wurden Experimente durchgeführt, die die Verletzung der Bell'schen Ungleichungen belegen.

Wenn wir das Experiment von Alice und Bob nach Einstein interpretieren, dann ist die Tatsache, dass der Zustand bei Bob **sicher** nach unten abgelenkt wird, wenn er bei Alice nach oben abgelenkt wird, ein Zeichen dafür, dass diese Ablenkung des Spins nach unten auf eine feste physikalische Eigenschaft zurückgef'ührt werden kann. Sie kommt ihm zu, egal was Alice an ihrem Stern-Gerlach macht. Die Unsicherheit, dass er nämlich manchmal nach oben, manchmal nach unten abgelenkt wird, muss an verborgenen Parametern liegen, die wir noch nicht kennen.

Wenn wir die Ergebnisse der QM nicht infrage stellen, so ist es ziemlich egal, ob die oben angeführtten Axiome endgültig sind, oder ob es noch irgendwelche verborgene Parameter gibt. Von daher gesehen, sind die Bell'schen Ungleichungen für das Quantenrechnen nicht

von grosser Bedeutung. Da aber in der Literatur oft ein verschiedener Standpunkt vertreten wird, sein diese Ungleichungen hier kurz behandelt, zumal sie wesentlich zum Verständnis der Besonderheiten der QM beitragen.

Bei vorher dem beschriebenen Experimenten sind die Stern-Gerlachs stets in die selbe Richtung $\vec{a}$ ausgerichtet. Beim Experiment misst Alice den (doppelten) Spin in diese Richtung $\vec{a}$, d.h. manchmal $+1$ manchmal -1, der resultierende Erwartungswert ist 0: $\langle\vec{\boldsymbol{\sigma}}\cdot\vec{a}\rangle = 0$, genauso ist es bei Bob. Wenn aber beide den gleichen Zustand mit Gesamtspin 0 untersuchen, dann ist das Ergebnis stets -1:

$$\langle \mathbf{J}_{AB}=0|((\vec{\boldsymbol{\sigma}}_A\cdot\vec{a})\otimes(\vec{\boldsymbol{\sigma}}_B\cdot\vec{a})|\mathbf{J}_{AB}=0\rangle = -1, \tag{2.68}$$

denn wenn Alice $+1$ misst dann Bob -1 und umgekehrt. Bells originelle Idee war, die Stern Gerlachs von A und B in verschiedene Richtungen zeigen zu lassen, d.h. den quantenmechanischen Erwartungswert von $((\vec{\boldsymbol{\sigma}}_A\cdot\vec{a})\otimes(\vec{\boldsymbol{\sigma}}_B\cdot\vec{b})$ messen zu lassen, der sich leicht berechnen lässt.

$$\begin{aligned}
P_{QM}(\vec{a},\vec{b}) &= \langle \mathbf{J}_{AB}=0|((\vec{\boldsymbol{\sigma}}_A\cdot\vec{a})\otimes(\vec{\boldsymbol{\sigma}}_B\cdot\vec{b})|\mathbf{J}_{AB}=0\rangle \\
&= \tfrac{1}{2}\langle(\langle 10|-\langle 01|)(\vec{\boldsymbol{\sigma}}_A\cdot\vec{a})\otimes(\vec{\boldsymbol{\sigma}}_B\cdot\vec{b})(|10\rangle-|01\rangle)\rangle \\
&= \tfrac{1}{2}\Big(\langle 1|\vec{\boldsymbol{\sigma}}_A\cdot\vec{a}|1\rangle\ \langle 0|\vec{\boldsymbol{\sigma}}_B\cdot\vec{b}|0\rangle - \langle 1|\vec{\boldsymbol{\sigma}}_A\cdot\vec{a}|0\rangle\ \langle 0|\vec{\boldsymbol{\sigma}}_B\cdot\vec{b}|1\rangle \\
&\qquad \langle 0|\vec{\boldsymbol{\sigma}}_A\cdot\vec{a}|1\rangle\ \langle 1|\vec{\boldsymbol{\sigma}}_B\cdot\vec{b}|0\rangle - \langle 0|\vec{\boldsymbol{\sigma}}_A\cdot\vec{a}|1\rangle\ \langle 0|\vec{\boldsymbol{\sigma}}_B\cdot\vec{b}|1\rangle\Big) \\
&= \tfrac{1}{2}\Big(-a_3\,b_3-(a_1+\boldsymbol{i}b_y)(a_1-\boldsymbol{i}b_y)-a_3\,b_3\Big) \\
&= -\vec{a}\cdot\vec{b}
\end{aligned}$$

wobei wir benutzt haben:

$$\langle 0|\vec{\boldsymbol{\sigma}}\cdot\vec{a}|0\rangle = a_3;\ \langle 1|\vec{\boldsymbol{\sigma}}\cdot\vec{a}|1\rangle = -a_3;\ \langle 0|\vec{\boldsymbol{\sigma}}\cdot\vec{a}|1\rangle = a_1+\boldsymbol{i}a_y;\ \langle 1|\vec{\boldsymbol{\sigma}}\cdot\vec{a}|0\rangle = a_1-\boldsymbol{i}a_y \tag{2.69}$$

also erhalten wir das quantenmechanische Resultat

$$P_{QM}(\vec{a},\vec{b}) = -\vec{a}\cdot\vec{b} = \cos\theta_{\vec{a}\vec{b}}. \tag{2.70}$$

bell-qm

Im Sinne von EPR können die Eigenschaften der von A und B gemessenen Zustände noch von einem verborgenen Parametern λ abhängen, der zur Beschreibung notwendig ist, der aber inhärent den beiden Zuständen ist, also unabhängig von der Einstellung der Stern-Gerlach Richtungen $\vec{a}$ und $\vec{b}$. Das Resultat der Messung von $\vec{\boldsymbol{\sigma}}\cdot\vec{a}$ und $\vec{\boldsymbol{\sigma}}\cdot\vec{b}$ sei $A(\vec{a},\lambda)$ und $B(\vec{b},\lambda)$, resp.

Die entscheidende Annahme in der EPR Argumentation ist, dass Resultat der Messung von der Messung von Bob, $B(\vec{b},\lambda)$ nicht von der Einstellung von Alice, $\vec{a}$ abhängt, es kann aber sehr wohl noch von einem (oder auch mehreren) verborgenen Parametern abhängen. Das Ergebnis vieler Messungen ist dann gegeben durch das Integral über die Verteilung der Parameter $\rho(\lambda)$, mit $\int d\lambda\rho(\lambda) = 1$. Der klassische Erwartungswert der Messung von $\vec{\boldsymbol{\sigma}}_A\cdot\vec{a}\quad\vec{\boldsymbol{\sigma}}_B\cdot\vec{b}$ ist dann

$$\langle\vec{\boldsymbol{\sigma}}_A\cdot\vec{a}\quad\vec{\boldsymbol{\sigma}}_B\cdot\vec{b}\rangle_{\rm class} = P_{\rm class}(\vec{a},\vec{b}) = \int d\lambda\rho(\lambda)A(\vec{a},\lambda)\,B(\vec{b},\lambda) \tag{2.71}$$

Nun berücksichtigen wir, dass bei jedem Versuch, bei dem die Magnete in die gleich Richtung eingestellt sind (d.h. $\vec{a} = \vec{b}$) die Strhlen in jeweils entgegengesetzt Richtung abgelenkt werden, also

$$A(\vec{a}, \lambda) = -B(\vec{a}, \lambda) \tag{2.72}$$ ab

Es spielt ja keine Rolle, welche Richtung wir die z-Richtung nennen.

Ferner gilt: Bei jeder Einzel-Messung, gleichgültig in welche Richtung, wird der Strahl nach oben oder unten abgelenkt, d.h

$$A(\vec{a}, \lambda) = \pm 1; \quad B(\vec{b}, \lambda) = \pm 1 \tag{2.73}$$ sab

Damit erhalten wir

$$\begin{aligned} P_{\text{class}}(\vec{a}, \vec{b}) - P_{\text{class}}(\vec{a}, \vec{c}) &= \int d\lambda \rho(\lambda)(A(\vec{a}, \lambda)\, B(\vec{b}, \lambda) - A(\vec{a}, \lambda)\, B(\vec{c}, \lambda)) \\ &= -\int d\lambda \rho(\lambda)[A(\vec{a}, \lambda)\, A(\vec{b}, \lambda) - A(\vec{a}, \lambda)\, A(\vec{c}, \lambda)] \\ &= -\int d\lambda \rho(\lambda) A(\vec{a}, \lambda)\, A(\vec{b}, \lambda)[1 - A(\vec{b}, \lambda)\, A(\vec{c}, \lambda)] \end{aligned}$$

since $A(\vec{b}, \lambda)^2 = 1$, see (2.73) Using the triangle inequality we obtain:

$$\begin{aligned} |P_{\text{class}}(\vec{a}, \vec{b}) - P_{\text{class}}(\vec{a}, \vec{c})| &\leq \int d\lambda \rho(\lambda) |\, A(\vec{a}, \lambda)\, A(\vec{b}, \lambda)[1 + A(\vec{b}, \lambda)\, B(\vec{c}, \lambda)] \\ &\leq \int d\lambda \rho(\lambda)[1 + A(\vec{b}, \lambda)\, B(\vec{c}, \lambda)] = 1 + P_{\text{class}}(\vec{b}, \vec{c}) \end{aligned}$$ bell-cl

where we have used (2.72), (2.73) und $\rho(\lambda) \geq 0$.

Die Ungleichung

$$|P_{\text{class}}(\vec{a}, \vec{b}) - P_{\text{class}}(\vec{a}, \vec{c})| \leq \int d\lambda \rho(\lambda)[1 + A(\vec{b}, \lambda)\, B(\vec{c}, \lambda)] = 1 + P_{\text{class}}(\vec{b}, \vec{c}) \tag{2.74}$$ bell-u

ist eine Form der Bell'schen Ungleichungen, die aus der klassische Wahrscheinlichkeitsverteilungen der verborgenen Parameter folgt.

Diese Ungleichung (2.74) ist incompatibel mit dem quantenmechanischen Resultat (2.70), wie mann an Fig. 2.4 sieht: Setzt man in der aus klassischen Überlegungen gewonnene Ungleichung (2.74) für P_{class} das aus der Quantenmechanik gewonnene Resultat (2.70) ein so sieht mann, dass es nahe $\theta = 0$ und $\theta = 2\pi$ Bereiche gibt, in dene die Ungleichung verletzt ist.

Die wichtigsten Schritte der Ableitung der Ungleichung und ihre Verletzung durch die QM sind in Abb. 2.5 zusammengefasst.

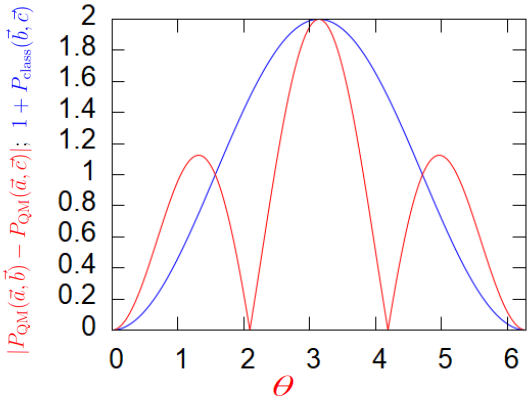
Es hat nur sehr wenige Physiker verwundert, dass die Experimente zeigten, dass die Bellschen Ungleichungen verletzt sind. John Bell antwortete auf die Frage, ob er erwartet habe, dass seine Ungleichungen erfüllt seien:

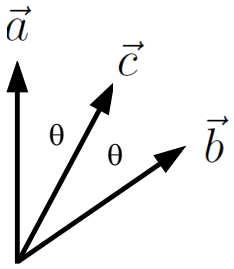
> You must distinguish between "expected" and "hoped for".

$$|P_{\rm class}(\vec{a},\vec{b}) - P_{\rm class}(\vec{a},\vec{c})| \le 1 + P_{\rm class}(\vec{b},\vec{c})$$

$$P_{\rm QM} = -\vec{a}\cdot\vec{b} = -\cos\theta_{ab}$$

$$|\cos 2\theta - \cos\theta| > 1 - \cos\theta$$





Drei coplanare Vectoren $\vec{a}$, $\vec{b}$, $\vec{c}$ mit $|\vec{a}| = |\vec{b}| = |\vec{c}| = 1$, $\theta_{ac} = \theta_{cb} = \frac{1}{2}\theta_{ab}$

bell-fig

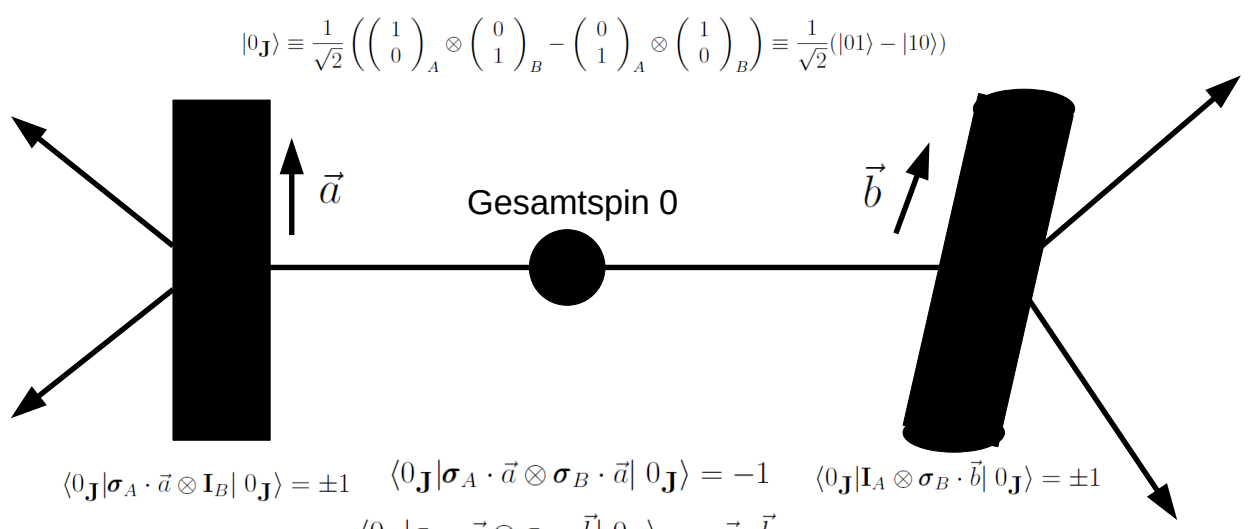
Abbildung 2.4: Unvereinbarkeit der Bell'schen Ungleichung (2.74), das aud klassischen überlegungen nach EPR basiert, mit dem Ergebnis der QM , (2.70), das experimentell bestätigt ist. Setzt man (2.70) in die Ungleichung (2.74) ein, so sieht man dass es nahe $\theta = 0$ und $\theta = 2\pi$ Bereiche gibt, in dene die Ungleichung (2.74) verletzt ist. $\vec{a}$, $\vec{b}\,vecc$ sind drei Vektoren in einer Ebene mit $\theta_{\vec{a}\vec{c}} = \theta_{\vec{c}\vec{b}} = \theta$; $\theta_{\vec{a}\vec{b}} = 2\theta$

Der Mathematiker Yu.I.Manin hat eine recht originelle Interpretation:

> With hindsight, one recognizes in Bell's setup the first example of the game-like situation where quantum players can behave demonstrably more efficiently than the classical ones.

2.3.5 Fouriertransformation mit Qubits*

wird am 8.6. behandelt.



ern-bell

Abbildung 2.5: Die wichtigsten Schritte der Ableitung der Bellschen Ungleichung in einer Einstein-realistischen" Theorie und ihre Verletzung durch die QM

Kapitel 3

Grundsätzliches

3.1 Superposition und Gemisch

Für das QC ist der reiche Informationsgehalt der Qubits entscheidend, deshalb ist die Superposition verschiedener (reiner) Zustände, die wieder zu einem (reinen) Zustand führtt, so wichtig. Deshalb ist es nötig zwischen Superposition (Überlagerung) und Mischung streng zu unterscheiden. Der Zustand, der durch einen Spinor

$$\frac{1}{\sqrt{2}}\left(|\uparrow_3\rangle + |\downarrow_3\rangle\right) = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix}\right) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = |\uparrow_1\rangle$$

beschrieben wird, ist wieder ein reiner Zustand, nämlich ein in $+x$ Richtung polarisierter Zustand. Auf die Phase zwischen den beiden Summanden kommt es entscheidend an: Der Zustand, der durch einen Spinor

$$\frac{1}{\sqrt{2}}\left(|\uparrow_3\rangle - |\downarrow_3\rangle\right) = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix}\right) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = |\downarrow_1\rangle$$

beschrieben wird, ist zwar auch wieder ein reiner Zustand, aber, wie man leicht nacHilberträumechnet, in ein in $-x$ Richtung polarisierter.

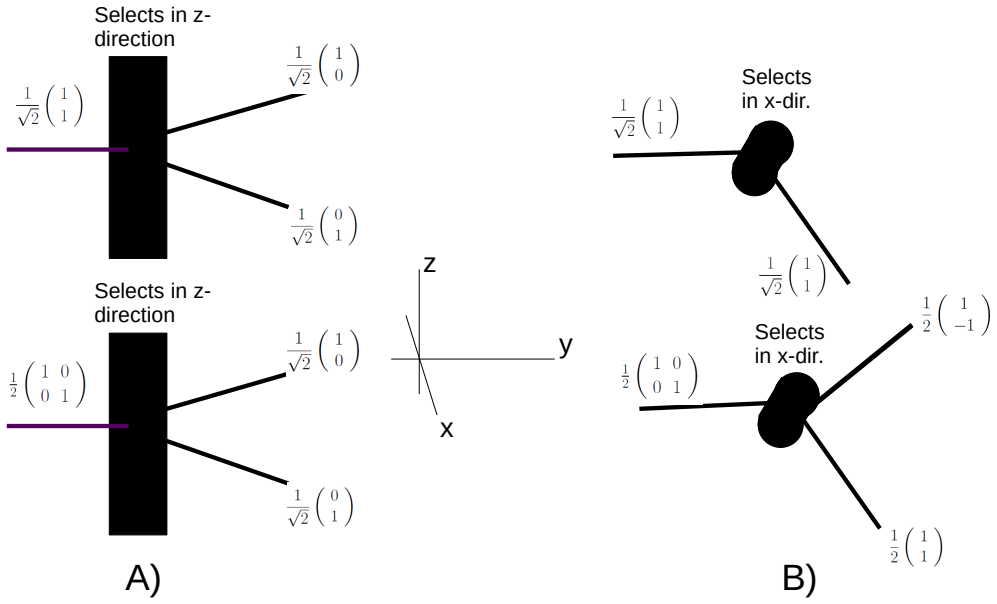
Hat man einen Strahl von Teilchen mit Spin $\frac{1}{2}$, bei dem die keine Phasenbeziehung zwischen den einzelnen Zustäne besteht, so spricht man von einem Gemisch. Nehmen wir an wir haben einen Strahl von Teilchen, der zu gleichen Teilen aus solchen mit Spin $+\frac{1}{2}$ und $-\frac{1}{2}$ besteht, so heisst dieses unpolarisiertes Gemisch Es wird durch die Dichtematrix

$$\rho = \tfrac{1}{2}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \tag{3.1}$$

beschrieben . Bei einem teilpolarisierten Strahl hat die Dichtematrix die Form

$$\rho = \begin{pmatrix}a & \alpha^*\\ \alpha & 1-a\end{pmatrix} = \tfrac{1}{2}(1 + \vec{P}\cdot\vec{\boldsymbol{\sigma}}). \tag{3.2}$$

wobei $\vec{P}$ die (Teil-) Polarisationsrichtung ist.



gemisch

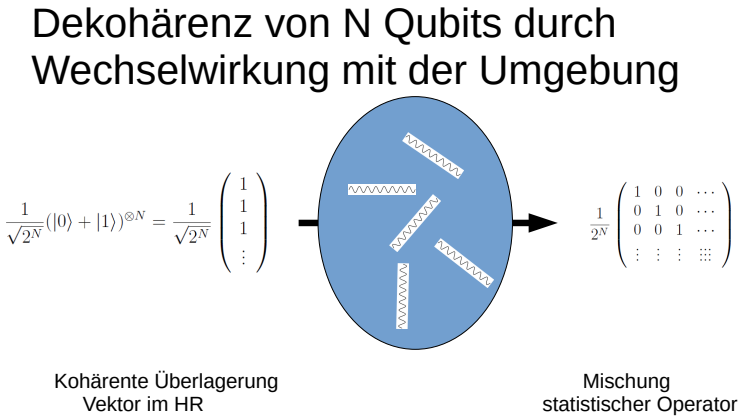
Abbildung 3.1: Die kohärente Überlagerung von $\frac{1}{\sqrt{2}}(|\uparrow_3\rangle + |\downarrow_3\rangle) = \frac{1}{\sqrt{2}}|\uparrow_1\rangle$ spaltet im nach z sortierenden Stern-Gerlach A) in zwei gleichstarke Teilchenstrahlen auf, genauso wie das durch die Dichtematrix $\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ beschriebene Gemsch (unpolarisierter Strahl). Im nach der x Richtung sortierenden Stern-Gerlach B) spaltet die kohärente Überlagerung nicht auf, wohl aber ein unpolarisierter Strahl.

Ein unpolarisierter Strahl ($\vec{P} = 0$) wird in einem Stern-Gerlach Versuch immer in 2 gleich starke Strahlen aufspalten, gleichgültig, nach welcher Richtung der Magnet gerichtet is s. Abb. gemisch 3.1.

3.1.1 Dekohärenz

Ein Hauptproblem bei der Konstruktion von QCn besteht darin, die Kohärenz einer Superposition zu erhalten. Durch Wechselwirkung mit der Umwelt (das sind effektiv Messungen) werden gehen die Phasenbeziehungen zwischen den Komponenten einer Überlagerung verloren und wir landen nach einer gewissen Zeit bei einem Gemisch, s. Abb. deko 3.2 uns dko^q ??.

Dieser Effekt der "Dekohärenz", (H.D. Zeh) führt zu einer Zunahme der Entropie eines Systems (s. Abschn. ent ??)



deko Abbildung 3.2: Durch die Wechselwirkung mit der Umgebung kann die Kohärenz einer Überlagerung verloren gehen, sie wird i. A. zu einem Gemisch. Bei makroskopischen Körpern reicht schon die Wechselwirkung mit der kosmischen Hintergrundstrahlung aus, um Dekohärenz in kürzester Zeit zu bewirken

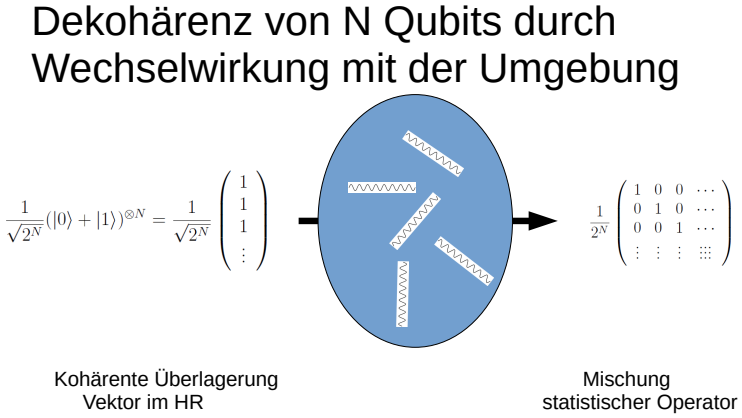
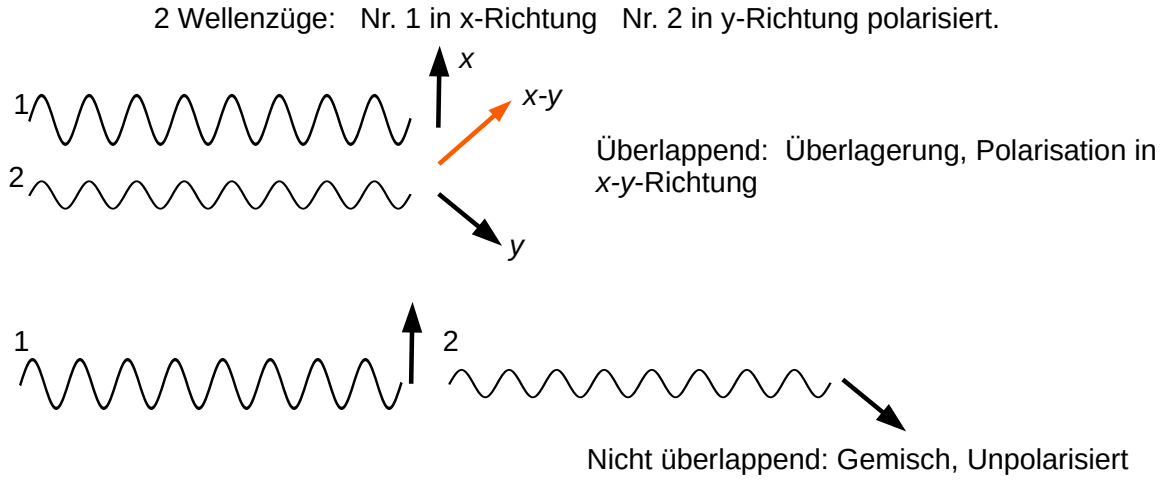


Abbildung 3.3: Dekohärenz eines N-Qubit Zustandes

Bei makroskopischen Körpern ist die Wechselwirkung mit der Umgebung so stark, dass die "Kohärenzzeit" im Sub-Nanosekunden Bereich liegt. Deshalb hat noch niemand die (kohärente) Überlagerumg einer wachen und schlafenden Katze beobachtet.

3.1.1.1 Kohärenz und Dekohärenz in der Optik

Da unsre Vorstellung von rein elektromagnetischen Vorgängen durch die klassische E-dynamik geprägt ist, entspricht hier die Kohärenz sehr viel eher unsrer Vorstellung, als das Gemisch. Haben wir zwei Strahlungsquellen, bei denen die eine Licht, das in x-Richtung polarisiert ist, ausstrahlt, die andere Licht, das in y-Richtung polarisiert ist, dann ist die Lösung für das Gesamtsystem eine Überlagerung der beiden Lösungen, da die Maxwell-Gleichungen linear



pol Abbildung 3.4: Überlagerung und Gemisch in der Optik. Nur wenn zwei Photonen eine feste Phasenbeziehung haben, bilden sie eine Überlagerung. Dies ist z.B. beim Laser der Fall. Bei einem gewöhnlichen Leuchtmittel (z.B. LED) werden die Photonen unkorreliert ausgesandt, sie bilden ein Gemisch.

in den Feldern sind. Daher erhalten wir eine in $x - y$ Richtung polarisierte Welle. So wie es ungewohnt ist in der Punktmechanik die Superposition zu verstehen, so schwer ist es in der E-Dynamik zu verstehen, warum Licht i. A. unpolarsiert ist.

Der Grund für die Mischung liegt darin, dass normalerweise Lichtquanten in atomaren Prozessen entstehen und deswegen der klassische Wellenzug, dem ein Photon entspricht, nur eine endliche Länge hat ($c \times \tau$). Unpolariesertes Licht ist also in der klassischen E-dynamik eine Mischung von nicht überlappenden Wellenzügen mit verschiedenen Polarisationsrichtungen.

Die Situation ist beim Laser verschieden, da hier die Wellenzüge kohäerent sind und sehr lang sein können.

Kapitel 4

Die "Quanten" Fourier Transformation

4.1 Fourier Transformation und Fourier Reihe

Die Fourier-Transformation ist eine harmonische Analysis, d.h. eine Darstellung einer Funktion durch —Überlagerung periodische Funktionen. Sie ist daher z. B. in der Akustik bedeutend. Unser Ohr führt eine Art Fourieranalyse des Schalldrucks durch und sie spielt bei Sprachanalyse, bei der akustischer Kompression (MP3), und auch der Signalübermittlung allgemein (G5) eine wichtige Rolle. Algorithmen zur schnellen Durchführung der Fourieranalyse waren daher schon im klassische Computing wichtig (FFA fast Fourier analysis, s. nächste Vorlesung Marquard).

Auch in der QM ist die Fourier Transformation sehr bedeutend. Sie erlaubt den Übergang zwischen der Ortsdarstellung, in dem die Observable Ort eine Multiplikation und der Impuls eine Ableitung ist, d.h. Ortsoperator ist $\mathbf{Q}_i$ und Impulsoperator $P_i = \frac{\hbar}{i}\partial_{Q_i}$ und der Impulsdarstellung in dem die Observable Impuls eine Multiplikation und die Observable Ort eine Ableitung ist. Der Übergang von der "Ortsdarstellung" $f(q)$ zur Impulsdarstellung $\tilde{f}(p)$ ist:

$$\tilde{f}(p) = \frac{1}{\mathcal{N}} \int dq\, e^{\boldsymbol{i}pq}\, f(q) \tag{4.1}$$

In numerischen Anwendumgen muss das Integral durch eine Summe ersetzt werden. Im Hinblick auf Anwendungen im QC wählen wir als Intgrationsgrenzen 0 und 2π und wählen 2^N Stützpunkte:

$$\tilde{f}_k = \frac{1}{\sqrt{2^N}} \sum_{\ell=0}^{2^N-1} e^{(\boldsymbol{i}2\pi\, k\, \ell)/2^N} f_\ell, \quad \text{mit} \quad \tilde{f}_k = \tilde{f}(\frac{k}{2^N}),\ f_\ell = f(\frac{\ell}{2^N}) \tag{4.2}$$

fdis

d.h. die diskrete FT is eine Matrix, die die Vektoren $\{f_0, f_1, \cdots, f_{2^N-1}\}$ in die Vektoren $\{\tilde{f}_0, \tilde{f}_1, \cdots, \tilde{f}_{2^N-1}\}$ abbildet.

$$\tilde{f}_k = \sum_{\ell=0}^{M-1} F_{k\ell}\, f_\ell; \quad \text{mit} \quad F_{k\ell} = \frac{1}{\sqrt{M}} e^{(\boldsymbol{i}2\pi\, k\, \ell)/M} \tag{4.3}$$

fdismat

Die Matrix $\mathbf{F}$ ist unitär:

$$\begin{aligned}(\mathbf{F}'^{\dagger}\,\mathbf{F})_{k\ell} &= \frac{1}{M}\sum_{k'=0}^{M-1}(e^{(-\boldsymbol{i}2\pi\,k'\,k)/M}e^{(\boldsymbol{i}2\pi\,k'\,\ell)/M} \\ &= \frac{1}{M}\sum_{k'=0}^{M-1}(e^{\boldsymbol{i}2\pi\,k'\,(\ell-k)/M} = \delta_{k\ell}\end{aligned}$$

Die letzte Gleichheit basiert auf der Gleichung

$$\sum_{k'=0}^{M-1}(e^{\boldsymbol{i}2\pi\,k'\,(\ell-k)/M} = M\,\delta_{k\ell}, \quad M = 2^N \tag{4.4}$$ zaub

Diese wichtige Relation basiert auf den periodischen Eigenschaften der e-Funktion, z. B. $e^{i\pi\,2n} = 1;\ e^{i\pi\,(2n+1)} = -1$

Zum Beweis von (4.4) zeigt man, dass in der Summe $a = \sum_{k'=0}^{M-1}(e^{\boldsymbol{i}2\pi\,k'\,(\ell-k)/M}$ mit $0 < |\ell - k| \leq M-1$ für jedes $e^{\boldsymbol{i}2\pi\,k'\,(\ell-k)/M}$ ein Term $b = e^{\boldsymbol{i}2\pi\,k'+(M*s/2)\,(\ell-k)/M} =$ mit ungeradem s auftritt. d.h. $a = -b$.

Die QFT ist nichts anderes als eine Übertragung der diskreten FT (4.2) auf Qubits unter ganz wesentlicher Ausnutzung der CB. Es ist daher nochmals wichtig, sich die etwas ungewohnte Form der CB und ihre Darstellung durch Zahlen im Dualsystem zu verinnerlichen.

4.2 Wiederholung: computatorische Basis

Dieser Abschnitt ist eine Erweiterung von Sect. 2.3.

Seien $|q\rangle_k$ computatorische Qubit Basen von n Hilbert-räumen,

$$|0\rangle_k = \begin{pmatrix} 1 \\ 0 \end{pmatrix};\ |1\rangle_k = \begin{pmatrix} 0 \\ 1 \end{pmatrix};$$

Dann besteht die computatorische Basis im N-Qubit Raum: aus den 2^N orthonormalen Vektoren

$$|q_1\rangle_1 \otimes |q_2\rangle_2 \cdots \otimes |q_N\rangle_N \equiv |q_1\,q_2, \cdots q_N\rangle; \quad q_k = 0,\ 1 \tag{4.5}$$

Ein bra-vektor ist

$$\langle p_1\,p_2, \cdots p_N| \equiv \langle p_1|_1 \otimes \langle p_2|_2 \cdots \otimes \langle p_N|_N$$

d.h. wir haben

$$\langle p_1\,p_2, \cdots p_n|q_1\,q_2, \cdots q_N\rangle = \prod_{k=1}^{N}\langle p_k|q_k\rangle \tag{4.6}$$

Da jede ganze Zahl q eindeutig im Dualsystem dargestellt werden kann

$$q = q_1 \cdot 2^{N-1} + q_2 \cdot 2^{N-2} + \cdots + q_N \cdot 2^0 \tag{4.7}$$ dubas

1235 können wir jeden Vektor $|q_1\, q_2\, \cdots q_N\rangle$ eindeutig bezeichnen als

$$|q_1\, q_2\, \cdots q_N\rangle \equiv |q_d\rangle \tag{4.8}$$ dual

1236 wobei der Index $_d$ andeuted, dass hier die Dualstellen von q stehen.

Wegen der Eindeutigkeit der Dualzerlegung gilt:

$$\langle p_d|q_d\rangle = \delta_{pq}$$

1237 Es muss q_d stets als N-stellige Dualzahl geschrieben werden, also gegebenenfalls müssen links
1238 Nullen aufgefüllt werde Haben wir etwa 3 Qubit-Räume, so ist $|1_d\rangle \equiv |001\rangle$

1239 Der allgemeine N-Qubit Zustand ist

$$\big(\alpha_{0,1}|0\rangle_N + \alpha_{1,1}|1\rangle_1\big) \otimes \big(\alpha_{0,2}|0\rangle_2 + \alpha_{1,2}|1\rangle_2\big) \otimes \cdots \otimes \big(\alpha_{0,N}|0\rangle_N + \alpha_{1,N}|1\rangle_N\big) = \tag{4.9}$$

$$= \begin{pmatrix} \alpha_{0,1} \\ \alpha_{1,1} \end{pmatrix} \otimes \begin{pmatrix} \alpha_{0,2} \\ \alpha_{1,2} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} \alpha_{0,N} \\ \alpha_{1,N} \end{pmatrix}$$

$$= \sum_{\{q_k=0,1\}} \prod_{k=1}^{N} \alpha_{q_k,k} \cdots \alpha_{q_N,N}\, |q_1, q_2, \cdots q_N\rangle \tag{4.10}$$

$$= \sum_{\{q_k=0,1\}} \prod_{k=1}^{N} \alpha_{q_k,k} \cdots \alpha_{q_N,N}\, |q_d\rangle \quad \text{mit} \quad q = q_1 \cdot 2^{N-1} + q_2 \cdot 2^{N-2} + \cdots + q_N \cdot 2^0 \tag{4.11}$$

1240 wobei die Summe über alle die 2^N möglichen Anordnungen von Nullen und Einsen in einem
1241 N-tupel geht.

1242 Wird ein Hadamard Gate $\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, d.h. $\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ auf jedes der N
1243 Qubits des Zustandes $|0_d\rangle$ angewandt, so erhalten wir

$$\mathbf{H}^{\otimes N}|0, 0, \ldots 0\rangle = 2^{-N/2}\big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle + |1\rangle\big) \otimes \cdots \big(|0\rangle + |1\rangle\big) \tag{4.12}$$

$$= 2^{-N/2}\Big(|00\cdots0\rangle + |10\cdots0\rangle + \cdots + |101\cdots0\rangle + |111\cdots1\rangle\Big) \tag{4.13}$$

$$= 2^{-N/2}\Big(|0_d\rangle + |1_d\rangle + \cdots |2^N - 1_d\rangle\Big) \tag{4.14}$$

1244 4.2.1 Definition der FT in der CB

1245 Die Quanten-Fouriertransformation ist analog (4.2) definiert , doch erfordert sie etwas Um-
1246 denken, da wir hier die Zahlen $f_\ell, \tilde{f}_\ell$ in (4.2) die als Elemente der CB in einem N-Qubit
1247 Raum auffassen.

1248 Wir führen im N-Qubit Raum 2 Basissysteme ein: $|\tilde{p_d}\rangle,\ p = 0, 1, \ldots 2^N - 1$ und $|q_d\rangle,\ p =$
1249 $0, 1, \ldots 2^N - 1$

1250 Sie sind durch die Matrix der FT, (4.3) verknüpft:

$$|q_d\rangle \to \mathcal{F}(|q_d\rangle) = |\tilde{p_d}\rangle = \frac{1}{2^{N/2}} \sum_{q=0}^{2^N-1} e^{2\pi \boldsymbol{i}\, q\, p/2^N]}|q_d\rangle \tag{4.15}$$ defqft

Haben wir einen Zustand

$$|\phi\rangle = \sum_{q=1}^{2^N-1} \phi_q |q_d\rangle \tag{4.16}$$

wird dieser durch die FT linear abgebildet:

$$|\phi\rangle \to \mathcal{F}(|\phi\rangle) = |\tilde{\phi}\rangle = \sum \tilde{\phi}_p |\tilde{p}\rangle = \frac{1}{2^{N/2}} \sum_{q=0}^{2^N-1} \phi_q \, e^{2\pi \boldsymbol{i}\, q\, p/2^N} |q_d\rangle \tag{4.17}$$

d.h. die Fourier transformierte von ϕ_q ist:

$$\phi_q \to \tilde{\phi}_p = \frac{1}{2^{N/2}} \sum_{q=0}^{2^N-1} e^{2\pi \boldsymbol{i}\, q\, p/2^N} \, \phi_q \tag{4.18}$$

Wenn wir also ein Verfahren hätten, um eine Funktion $\phi(q)$ leicht in eine Summe von CB-Vektoren $|\phi\rangle = \sum_{q=1}^{2^N-1} \phi_q |q_d\rangle$ zu bringen, so könnten wir den Fouriertransformierten Zustand leicht erzeugen. Leider ist offenbar ein generelles Verfahren für eine solche reversible Zuordnung für periodisch Funktionen unmöglich. Wir betrachten z. B. die Zuordnung

$$\mathbf{A} : |q_d\rangle \to \phi(q)|\phi(q)_d\rangle. \tag{4.19}$$

Wenn die Funktion nicht umkehrbar eindeutig ist, wie z.B eine periodische Funktion mit $\phi(q) = \phi(q+T)$, dann könnten die Urbilder vom Zustand $\phi(q_0)|\phi(q_0)_d\rangle$ alle die Vektoren $|q_{0d}\rangle$, $|q_0 + T_d\rangle$, $|q_0 + 2T_d\rangle, \ldots$ sein, d.h. die Zuordnung ist nicht reversibel.

Erweitern wir den Hilbertraum $\mathcal{H}$ zu einem Produkt $\mathcal{H} \otimes \mathcal{H}$, dann können wir eine reversible (unitäre) Abbildung leicht konstruieren:

$$\mathbf{\Phi} : |q_d\rangle \otimes |0_d\rangle \to |q_d\rangle \otimes |\phi(q)_d\rangle, \tag{4.20}$$

ph

da hier die direkte Information über den Wert von q im Abbild, nämlich im ersten Faktor des Produktraumes, enthalten ist. Die Situation ist ähnlich wie beim CNOT gate.

Die Fouriertransformation eines einzelnen Basisvektors (4.15) ist als unitäre Transformation durch Quantengatter zu erreichen. Bevor wir zu einer klassischen Anwendung der FT schreiten, nämlich der Frequenzanalyse, wollen wir diese Realisierung der Fourieranalyse, die der Architektur eines Quanten Computers besonders angebracht ist, behandeln.

4.2.2 Auf Qubits adaptierte Form der Fourier-Transformierten

Wir gehen zurück zur Definition des CBasisvektor $|q_d\rangle$ als direktes Produkt der Basisvektoren eines Qubits, $|0\rangle$, $|1\rangle$

$$|q_d\rangle \equiv \bigotimes_{k=1}^{N} |q_k\rangle_k \quad \text{sowie } q = q_1 \cdot 2^{N-1} + \cdots q_N \cdot 2^0$$

Damit schreiben wir die rechte Seite von (4.15) defqft um

$$\begin{aligned}
\mathcal{F}(|q\rangle) = |\tilde{p_d}\rangle &= \frac{1}{2^{N/2}} \sum_{q=0}^{2^N-1} e^{2\pi \boldsymbol{i}\, q\, p/2^N} |q_d\rangle = && (4.21)\\
&= \frac{1}{2^{N/2}} \sum_{q_1=0}^{1} \cdots \sum_{q_N=0}^{1} e^{\frac{2\pi \boldsymbol{i}\, p}{2^N}\,(q_1\cdot 2^{N-1}+\cdots q_k\cdot 2^{-k}+\cdot q_N\cdot 2^0)} \bigotimes_{k=1}^{N} |q_k\rangle_k && (4.22)\\
&= \frac{1}{2^{N/2}} \bigotimes_{k=1}^{N} \sum_{q_k=0}^{1} e^{2\pi \boldsymbol{i}\, p\, q_k\cdot 2^{-k}} |q_k\rangle_k && (4.23)\\
&= \frac{1}{2^{N/2}} \bigotimes_{k=1}^{N} \Big(|0\rangle + e^{2\pi \boldsymbol{i}\, p\cdot 2^{-k}} |1\rangle\Big)_k && (4.24)\\
&\quad \text{wir setzen ein } p = \textstyle\sum_{\ell=1}^{N} p_\ell \cdot 2^{N-\ell} \\
|\tilde{p_d}\rangle &= \frac{1}{2^{N/2}} \bigotimes_{k=1}^{N} \Big(|0\rangle + e^{2\pi \boldsymbol{i}\left(\sum_{l=1}^{N} p_l\cdot 2^{N-l-k}\right)} |1\rangle\Big)_k && (4.25)\\
&\quad \text{wir können vereinfachen, da } e^{2\pi \boldsymbol{i}(N-l-k)} = 1 \text{ für } l+k \le N \\
&= \frac{1}{2^{N/2}} \bigotimes_{k=1}^{N} \Big(|0\rangle + e^{2\pi \boldsymbol{i}\left(\sum_{l=N-k+1}^{N} p_l\cdot 2^{N-l-k}\right)} |1\rangle\Big)_k && (4.26)\\
&= \frac{1}{2^{N/2}} \bigotimes_{k=1}^{N} \Big(|0\rangle + e^{2\pi \boldsymbol{i}\left(\sum_{r=1}^{k} p_{N-r-k}\cdot 2^{-r}\right)} |1\rangle\Big)_k && (4.27)
\end{aligned}$$

Es ist üblich, die folgende Dualbruch-Notation einzuführen:

$$\begin{aligned}
0.p_N &\equiv p_N \cdot 2^{-1} && (4.28)\\
0.p_{N-1}p_N &\equiv p_{N-1}2^{-1} + p_N \cdot 2^{-2} && (4.29)\\
0.p_{N-k}p_{N-k+1}\cdots p_N &\equiv p_{N-k}\cdot 2^{-1} + p_{N-k+1}\cdot 2^{-2} + \cdots + p_N \cdot 2^{-k} && (4.30)
\end{aligned}$$

Die Indizes $1 \cdots N$ indizieren die Qubits.

Damit erhalten wir schliesslich:

$$\begin{aligned}
|\tilde{p_d}\rangle = \frac{1}{2^{N/2}} \Big[&\Big(|0\rangle + e^{2\pi \boldsymbol{i}\, 0.p_N}|1\rangle\Big)_1 \otimes \Big(|0\rangle + e^{2\pi \boldsymbol{i}\, 0.p_{N-1}p_N}|1\rangle\Big)_2 \otimes \\
&\cdots \otimes \Big(|0\rangle + e^{2\pi \boldsymbol{i}\, 0.p_1 p_2 \ldots p_N}|1\rangle\Big)_N \Big] && (4.31)
\end{aligned}$$

Diese Form der QFT ist für QC sehr bequem, da sie zeigt wie jedes der N Qubits des Rechneres durch ein unitäres Matrix-Gatter der Form

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi \boldsymbol{i}\alpha} \end{pmatrix} \qquad (4.32)$$

with $\alpha = .p_{N-k}\, p_{N-k+1} \cdots p_N$ transformiert wird.

Ein Beispiel: Sei $N = 3$ und $p = 3$. Die Dualdarstellung ist $3 = 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$, d.h. $|\tilde{3_d}\rangle = |\tilde{011}\rangle$; oder $p_1 = 0,\ p_2 = 1,\ p_3 = 1$ und damit $0.p3 = 2^{-1},\ 0.p_2p_3 = 2^{-1} + 2^{-2},\ 0.p_1p_2p_3 = 0 \cdot 2^{-1} + 2^{-2} + 2^{-3}$ und damit erhalten wir:

$$|\tilde{3_d}\rangle = (|0\rangle + e^{\boldsymbol{i}\,\pi}) \otimes (|0\rangle + e^{\boldsymbol{i}\,\pi\cdot 3/2}) \otimes (|0\rangle + e^{\boldsymbol{i}\,\pi\cdot 3/4}) \tag{4.33}$$

4.3 Anwendung: Periodenbestimmung durch QFT

Eine wichtige Anwendung der üblichen FT ist die Frequenzbestimmung einer periodischen Funktion. Sei $\phi(q)$ eine Funktion mit ganzzahligen Argumenten und ganzzahligen Werten, $\mathbb{Z} \to \mathbb{Z}$ mit der Periode T d.h.

$$\phi(q) = \phi(q + n\,T),\ n \in \mathbb{Z} \tag{4.34}$$ ph1

Da wir schon die Schwierigkeiten mit der Zuordnung $|q_d\rangle \to \phi(k)|\phi(q)_d\rangle$ gesehen hatten, gehen wir gleich zu einer Darstellung der Funktion im Produktraum.

Die allgemeine Sprachregelung ist: Ein Zustand in einem direkten Produkt zweier Qubit-Hilberträume $\mathcal{H}_1 \otimes \mathcal{H}_2$, mit jeweils den Dimensionen 2^M bzw. 2^N, heisst Quantenregister. Der Faktor aus $\mathcal{H}_1$ heisst Quantenregister QR1, der aus aus $\mathcal{H}_2$ heisst Quantenregister QR2

Im nun betrachteten Falle sei QR1 der Zustand $\frac{1}{2^{M/2}}(|0_d\rangle + |1_d\rangle + \cdots |(2^M-1)_d\rangle)$ [1] , QR2 sei der Basisvektor $|0_d\rangle$ d.h. unser Zustand im Quantenregister ist:

$$|A\rangle \equiv \frac{1}{2^{M/2}} \underbrace{\left(\sum_{q=0}^{2^M-1} |q_d\rangle\right)}_{QR1} \otimes \underbrace{|0_d\rangle}_{QR2} \tag{4.35}$$ A

Die Schmidtzahl N_{Sch} dieses Zustands is 1.

Nun benutzen wir die reversible Zuordnung (4.20):

$$\boldsymbol{\Phi}\Big(|q_d\rangle \otimes |0_d\rangle\Big) = |q_d\rangle \otimes |\phi(q)_d\rangle \tag{4.36}$$

Dieses Zuordung wenden wir auf unser ganzes QR an und erhalten den Zustand:

$$|Z\rangle \equiv \frac{1}{2^{M/2}} \sum_{q=1}^{2^M-1} |q_d\rangle \otimes |\phi(q)_d\rangle \tag{4.37}$$ pf1

Hier ist die Schmidtzahl $N_{Sch} = T$.

Jetzt berücksichtigen wir die Periodizität der Funktion $\phi(q) = \phi(q + n\,T)$, aus der folgt:

[1] Ein solcher Zustand läst sich durch das Hadamard Gatter, (4.12) aus einem "leeren"Basisvektor $|0_d\rangle$ erzeugen

Jedem Basisvektor $|q_d\rangle$ der Summe in QR1, der die Form $|q_d\rangle = |(m\,T + q')_d\rangle$ hat, ist der gleiche Basisvektor aus QR2, nämlich $|\phi(q')_d\rangle$ zugeordnet. Damit faktorisiert $|Z\rangle$ (4.37):

$$|Z\rangle = \frac{1}{2^{M/2}} \sum_{q'=0}^{T-1} \Big(\sum_{m=0}^{A} |(m\,T + q')_d\rangle \Big) \otimes |\phi(q')_d\rangle + R \tag{4.38}$$

wobei $(A+1)\,T - 1 \leq 2^M - 1 < (A+2)\,T$ und $\frac{1}{\sqrt{2^M}} \sum_{q=A\,(T+1)}^{2^M-1} |q_d\rangle \otimes |\phi(q)_d\rangle$

Der Einfachheit halber vernachlässigen wir den Rest R von der Ordnung $O\left(\frac{1}{2^{M/2}}\right)$ oder nehmen, um Fallunterscheidungen zu vermeiden an, dass $2^M/T \in \mathbb{Z}$, d.h. dass garkein Rest auftritt.

Als nächstes messen wir im $\mathcal{H}_2$. Dabei wird die kohärente Summe in $\mathcal{H}_1 \otimes \mathcal{H}_2$ auf einen Summanden $q' = q_0,\ 0 \leq q_0 \leq T-1$, kollabieren. Sei der resultierende Zustand (das Resultat der Messung):

$$|B\rangle \equiv \left(\sum_{m=0}^{A} |(m\,T + q_0)_d\rangle \right) \otimes |\phi(q_0)_d\rangle \tag{4.39}$$

Der Wert von $q_0 \in \mathbb{Z}$ spielt im folgenden keine Rolle, d.h. es genügt eine Messung.

Um die Periode T, die in der Summe der Basiszustände

$$|\Psi\rangle = \sum_{m=0}^{A} |(r_m)_d\rangle \quad \text{mit} \quad |(r_m)_d\rangle = |(m\,T + q_0)_d\rangle \tag{4.40}$$

enthalten ist, bestimmen wir die Fourierzerlegung von $|\Psi\rangle$.

Die Fourierreihe für einen einzelnen Basisvektor $|(r_m)_d\rangle$ ist:

$$|\tilde{(r_m)}_d\rangle = \frac{1}{2^{N/2}} \sum_{p=0}^{2^M-1} e^{2\pi \boldsymbol{i}\, r_m\, p/2^M} |p_d\rangle \tag{4.41}$$

Die Fourierreihe für den Zustand $\frac{1}{\sqrt{A}}|\Psi\rangle$ ist damit:

$$\begin{aligned} \frac{1}{\sqrt{A}}|\tilde{\Psi}\rangle &= \frac{1}{\sqrt{A\,2^M}} \sum_{m=0}^{A} \sum_{p=0}^{2^{M-1}} e^{2\pi \boldsymbol{i}\,(m\,T+q_0)\,p/2^M} |p_d\rangle \\ &= \frac{1}{\sqrt{A\,2^M}} \sum_{p=0}^{2^{M-1}} \underbrace{e^{2\pi \boldsymbol{i}\, q_0\, p/2^M} \sum_{m=0}^{A} e^{2\pi \boldsymbol{i}\, m\, T\, p/2^M}}_{\alpha(p)} |p_d\rangle \end{aligned} \tag{4.42}$$

Führen wir in der Fourier-Darstellung von $|\Psi\rangle$ eine Messung durch, in der der Zustand als Überlagerung von Basisvektoren $|p_d\rangle$ dargestellt ist und projizieren durch eine Messung auf einen solchen Vektor, so ist die Wahrscheinlichkeit Prob(p_0), dass wir auf den den speziellen

ket $|p_0\rangle$ projezieren, d.h. das Resultat unsrer Messung, gegeben durch das Betragsquadrat des Koeffizienten von $|\tilde{p_{0_d}}\rangle$, also $|\alpha(p)|^2$.

$$\mathrm{Prob(p_0)} = \frac{1}{A\,2^M}|e^{2\pi \boldsymbol{i}\, q_0\, p_0/2^M}|^2 \,|\sum_{m=0}^{A} e^{2\pi \boldsymbol{i}\, m\, T\, p_0/2^M}|^2 \tag{4.43}$$

Die Terme der Summe $\sum_{m=0}^{m} Ae^{2\pi \boldsymbol{i}\, mTp_0/N}$ heben sich wegen der Oszillationen der e-Funktion weitgehend auf, nur wenn $p_0 = p_R$ mit

$$\frac{p_R\, T}{2^M} \in \mathbb{Z} \tag{4.44}$$ resfin

ist, addieren sie sich alle und nur der Term mit $|p_{R_d}\rangle$ hat einen grossen Koeffizienten. Bei einer Messung an $\frac{1}{\sqrt{A}}|\tilde{\Psi}\rangle$ wird also mit sehr grosser Wahrscheinlichkeit auf den Zustand $|(p_R)_d\rangle$ projiziert. Damit haben wir P_R bestimmt, und aus (4.44) folgt, dass die Periode T ein ganzzahliges Vielfaches von $\frac{2^M}{p_R}$ ist.

Möglicherweise ist allerdings $\frac{2^M}{p_R}$ keine ganze Zahl und mit mehreren Tests muss eine ganze Zahle in der Nähe von $n \cdot \frac{2^M}{p_R}$ ein ganzzahliges Vielfaches gesucht werden.

Wichtig bei dem ganzen Vorgehen ist, dass man sehr leicht prüfen kann (in von der Zahl 2^N unabhängigen Schritten), ob T tatsächlich die gesuchte Periode ist, d.h. ob $\phi(q) = \phi(q+T)$ ist.

4.3.1 Zusammenfassung

Wir fassen die Schritte zusammen, besonders im Hinblick auf die durch die QM relevanten Punkte, s. auch Abb. 4.1 scheme

Der erste Schritt ist die Herstellung eines Quantenregisters $\in \mathcal{H}_1 \otimes \mathcal{H}_2$. Es ist der Zustandsvektor $|A\rangle$, s. (4.35) A. Dieser (reine) ist das Produkt zweier Zustandsvektoren aus $\mathcal{H}_1$ bzw. $\mathcal{H}_2$, die Schmidtzahl ist also $N_{Sch} = 1$, es liegt keinerlei Verschränkung vor. Eine Messung in einem der beiden Räume hat also keinerlei Konsequenzen für den Zustand im anderen.

Beim beim 2. Schritt wird durch die reversible Transformation $\mathbf{\Phi}$ der Zustand $|A\rangle$ in $|\Psi\rangle$ überführt s. (4.37) pf1. Durch Ausnuzung der Periodizität der Funktion $\phi(q)$ (s. (4.34)) ph1 lässt sich $|\Psi\rangle$ in eine Schmidt-Darstellung bringen: (4.38) pf2; die Schmidtzahl hat für $|\Psi\rangle$ den Wert $N_{Sch} = T$. Hier liegt nun Verschränkung vor: der Zustand $|\phi(q_0)_d\rangle\mathcal{H}_2$ ist verschränkt mit dem Zustand $\sum_m |(q_0 + mT)_d\rangle$ und eine Messung in $\mathcal{H}_2$ führt zu einer Projektion auf den Verschränkten Partner in $\mathcal{H}_1$.

Im dritten Schritt wird eine solce Messung in $\mathcal{H}_2$ durchgeführt, und wir haben in $\mathcal{H}_1$ den Verschränkungspartner des gemessenen Zustands in $\mathcal{H}_2$.

Im vierten Schritt wird eine Fouriertransformation in cH_1 durchgeführt, sie ist ein Übergang von den Basisvektoren $|q_d\rangle$ zu $|\tilde{p_d}\rangle$, s. (4.42) ftpsi.

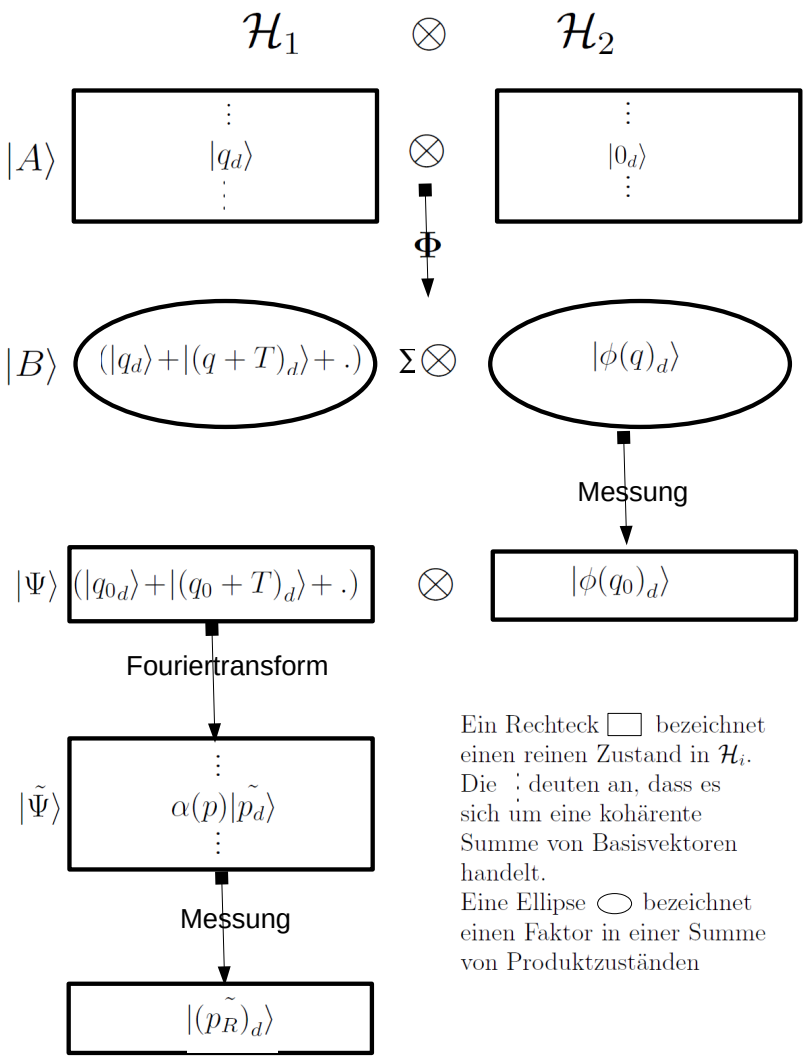


Abbildung 4.1: Die Schritte bei der Periodenbestimmung

mfourier

4.3.2 Numerisches Beispiel

Im 5. Schritt wird dann eine Messung als Projektion auf die Basisvektoren $|\tilde{p_d}\rangle$ durchgeführt. Diese Messung reultiert mit grosser Wahrscheinlichkeit mit einem Basisvektor $|\tilde{p_{Rd}}\rangle$, und die gesuchte Periode ist ein ganzzahliges Vielfaches von p_R.

Wir sehen, dass bei jedem Schritt die kohärente Überlagerung von Zuständen wesentlich ist, die Verschränkung spielt im 3. Schritt die entscheidende Rolle.

Wir betrachten die Funktion $\phi(q) = \mathrm{mod}(7^q, 247)$, die uns später bei der Priemzahlzerlegung nochmals begegnen wird.

$\mathcal{H}_1$: q	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	$\cdots$
$\mathcal{H}_2$: $\phi(q)$	1	7	49	96	178	11	77	45	68	229	121	106	1	7	49	96	178	11	77	45	68	229	121	106	1	7	49	96	$\cdots$

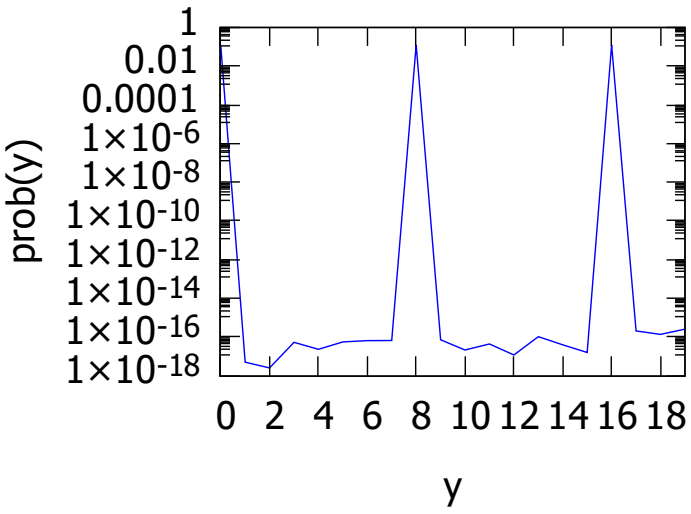


Abbildung 4.2: Die Betragsquadrate der Koeffizienten von $|y_d\rangle$

.

Für $\mathcal{H}_2$ muss N so gross sein, dass $2^N \geq 229$, d.h. $N = 8$

Messung in in $\mathcal{H}_2$ durchgeführt. Haben wir etwa als Resultat von der Messung im $\mathcal{H}_2$ die auf den Basisvektor $|49_d\rangle$ projiziert erhalten, ist der resultierende Zustand:

$$\frac{1}{\sqrt{8}}\left(|2_d\rangle+|14_d\rangle+|26_d\rangle+|38_d\rangle+|50_d\rangle+|62_d\rangle+|74_d\rangle+|86_d\rangle\right)\otimes|49_d\rangle = \left(\frac{1}{\sqrt{8}}\sum_{n=0}^{7}|(2+12\,n)_d\rangle\right)\otimes|49_d\rangle \tag{4.45}$$

Wir fouriertransformieren den Teil aus $\mathcal{H}_1$ $\frac{1}{\sqrt{8}}\sum_{n=0}^{7}|(2+12\,n)_d\rangle$ z. B. mit 5 Qubits: $Q = 2^5 = 32$

$$\frac{1}{\sqrt{8}}\sum_{n=0}^{7}\widetilde{|2+12\,n_d\rangle} = \frac{1}{\sqrt{8\cdot 32}}\sum_{y=0}^{31}\sum_{n=0}^{7}e^{2\pi i\,y\,(2+12\,n)/32}|y_d\rangle$$

Die Betragsquadrate der Koeffizienten von $|y_d\rangle$ sind in Abb. 4.2 aufgetragen. Daraus sehen wir, dass wir mit einer grossen Wahrscheinlichkeit die Werte $y = 8,\ 16, \cdots$ messen.

Also wissen wir dass $T \cdot y/2^5 = T \cdot 8/32 \in \mathbb{Z}$ oder $T = n \cdot \frac{32}{y} = n \cdot \frac{32}{8} = n \cdot 4$

also ist $T = 4, 8, 12, 16 \cdots$ in übereinstimmung mit der tatsächlichen Periode $T = 12$.

Kapitel 5

Basis des Shore'schen Algorithmus.

Es ist noch nicht klar, in wievielen Bereichen ein QC einem klassischen PC wesentlich überlegen ist. Wir hatten ja in der letzten Stunde von Herrn Marquard gehört, wie wenig die Quanten-Komplexitätstheorie entwickelt ist.

Die teilweise recht reisserischen Aussagen über die eminente Überlegenheit eines Quantencomputers über einen klassischen sind meist mit der Übersetzungsvorschrift zu lesen:

A typical example is .... ⇒ The best example I can think of

So wäre z.B. der folgende Satz korrekt:

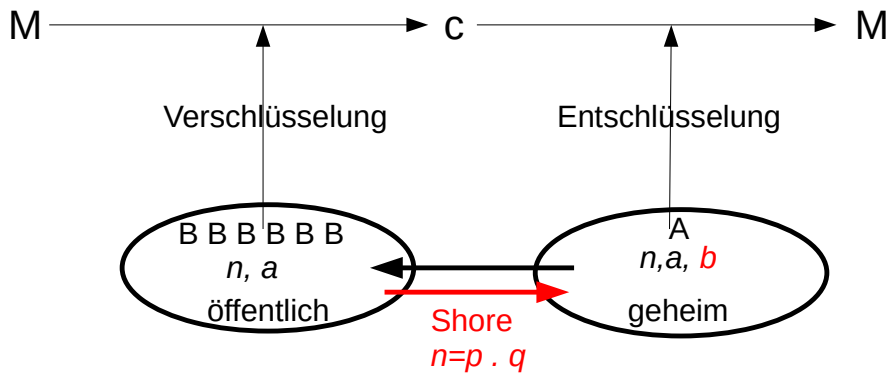
> Mit Hilfe eines Quantencomputers ist es möglich innerhalb von Millisekunden Vorgänge darzustellen, die auch der schnellste Supercomputer niemals generieren könnte.

Es handelt sich dabei um eine Reihe von echten Zufallsevents, die Herr Marquard öfters erwähnt hat und die mit dem inhärent stochstischem Charakter der QM zusammenhängen.

Eines der wenigen Beispiele für die drastische Überlegenheit eines Quantencomputers über einen klassischen ist die Zerlegung einer (riesig grossen) Zahl in Primzahlen mit Hilfe des Shore'schen Algorithmus. Sie ist nach gegenwärtigem Stand auf einem klassischen Computer nur mit exponentiell ansteigendem Aufwand durchfürbar, während sie über die Quanten FT mit polynomial anwachsendem Aufwand lösbar ist.

Die bei der gesamten Digitalisierung gegenwärtig eminent wichtige asymmetrische Verschlüsselung hängt ganz stark an der "praktischen Unlösbearkeit" der Primzahlzerlegung sehr grosser Zahlen ab. Daher die mögliche Entschlüsselung der bisher als sicher eingestufter Verschlüsselungen das QC im Augenblick besonders aktuell.

Das Schema der Ver- und Entschlüsselung nach Rivest, Shamir, and Adleman (RSA) ist in Abb. 5.1 dargestellt. fig-versch



Asymmetrische Verschlüsselung

Abbildung 5.1: A konstruiert aus dem Produkt zweier Primzahlen $n = p \cdot q$ das Schloss a, das er, zusammen mit der Zahl n der Öffentlichkeit mitteilt. Dadurch wird eine Botschaft M verschlüsselt, als $c = M^a \bmod n$. Mithilfe des Schlüssels b, der geheim bleibt, kann A die von B verschlüsselte Nachricht leicht entschlüsseln, nämlich $M = c^b \bmod n$. Der Schlüssel b ist das inverse Element des Schlosses, des Elements $[a]_{(p-1)\cdot(q-1)}$ der primen Restklasse, $(Z/Z_{(p-1)\cdot(q-1)})^*$. Durch Auffinden der Faktoren p und q der Zahl n mit Hilfe der Quanten Fourier-Transformation kann ein Hacker aus a, p und q den Schlüssel b mit polynomialen Aufwand finden.

g-versch

Wie aus der Erklärung der Figur fig-versch 5.1 deutlich erkennbar, spielt bei der Verschlüsselung die Zahlentheorie, der scheinbar esoteristschste Zweig der Mathematik, die entscheidende Rolle. Daher beschäftigt sich der erste Abschnitt etwas ausführlicher mit den relevanten Aspekten der Zahlentheorie.

5.1 Für Verschlüsselung und Entschlüsselung wichtige Elemente der Zahlentheorie

5.1.1 Notation und Begriffe

Allgemein gebräuchlichem Begriffe wie Primzahl, Primzahlzerlegung etc werden vorausgestezt.

Nichtnegative ganze Zahlen:	$\{0, 1, 2 \cdots\}$	$\mathbb{N}$
Positive ganze Zahlen:	$\{1, 2 \cdots\}$	$\mathbb{N}^*$
ganze Zahlen:	$\{\cdots -2, -1, 0, 1, 2 \cdots\}$	$\mathbb{Z}$

natürliche Zahlen: Notation etwas uneinheitlich, entweder $\mathbb{N}$ oder $\mathbb{N}^*$

Wenn nicht anders angegeben: römische Buchstaben; (mindestens) ganze Zahlen.

Zwei ganze Zahlen a, b heissen **coprim** oder relativ prim:
ihr **grösster gemeinsamer Teiler (gcd)** ist $1 : a, b$ coprim $\Leftrightarrow \gcd(a, b) = 1$

Kongruenz
a kongruent b modulo n : $\quad a \equiv b \bmod n \Leftrightarrow\ a - b$ teilbar durch n d.h. $b = a + k \cdot n, \quad k \in \mathbb{Z}$

Äquivalenzklasse Alle Zahlen $b \equiv a \bmod n$ bilden eine Äquivalenzklasse $[\mathbf{a}]_\mathbf{n}$. D.h. $[a]_n = [b_n] \Leftrightarrow a \equiv b \bmod n$.

I. A dient die kleinste nichtnegative Zahl der Äquivalenzklasse als Repräsentant dieser Klasse.

Restklassenring $\mathcal{Z}/n\mathcal{Z}$
Die Äquivalenzklasen $[r]_n,\ 0 \leq r < n$ bilden den Restklassenring $\mathcal{Z}/n\mathcal{Z}$. Jedes Element der Restklasse : $a \in [r]_n$ hat damit die Zerlegung $a = r + k \cdot n$

Man rechnet leicht nach dass in ihm Addition und Multiplikation definiert sind:

$$\begin{array}{ll} \bullet\text{Addition und Subtraktion:} & [a]_n \pm [b]_n = [a \pm b]_n \\ \bullet\text{Multiplikation:} & [a]_n \cdot [b]_n = [a \cdot b]_n \end{array} \tag{5.1}$$ add-mult

Bew. für Multiplikation:

$a \in [a]_n,\ b \in [b]_n\ \Rightarrow (a + k \cdot n)(b + k' \cdot n) = a \cdot b + n \cdot (a \cdot k' + b \cdot k + k \cdot k' \cdot n) = a \cdot b + n \cdot k''$
$\rightarrow a \cdot b \in [a \cdot b]_n$

Division i. A. nicht definiert

Prime Restklassen oder Einheitsgruppe des Restklassenrings
Die Äquivalenzklassen $[a]_n$ aus $\mathcal{Z}/n\mathcal{Z}$ bei denen a und n coprim sind.

$$(\mathcal{Z}/n\mathcal{Z})^* \ni \{[a]_n, \gcd(a, n) = 1\} \tag{5.2}$$ prk

In primen Restklassen ist ein Inverses definiert; wie unten gezeigt. Für den Beweis brauchen wir allerdings den "Urahn aller Algorithmen", das ist der

Euklidischer Algorithmus:

Da coprime Zahlenpaare und prime Äquivalenzklassen in der Verschlüsselung eine grosse Rolle spielen, sei der Euklidische Algorithmus, mit denen man den gcd findet, hier kurz beschriebenbeschrieben. Er ist einer der ältesten Algorithmen [1] und ein wesentliches Element des vielleicht aktuellsten Algorithmus, nämlich des Shore'schen.

Sei $a > b$; beim Euklidische Algorithmus werden erst a und b ganzzahlig geteilt und dann

[1] Elemente,VII, 1 und 2; 1. Teil: Nimmt man bei Vorliegen zweier ungleicher Zahlen immer die kleinere von der grösseren weg, so müssen, wenn niemals ein Rest die vorhergehende Zahl genau misst, bis die Einheit übrig bleibt, die ursprüngliche Zahlen gegeneinander prim sein. 3. Jh. v. Chr. Der Algorithmus ist wahrscheinlich älter (Schule des Pythagoras)

fortlaufend die nichtnegativen Reste:

$$\begin{aligned} a - q_1 \cdot b &= r_1; & r_1 < b \\ b - q_2 \cdot r_1 &= r_2; & r_2 < r_1 \\ r_1 - q_3 \cdot r_2 &= r_3; & r_3 < r_2 \\ &\vdots & \\ r_{k-3} - q_{k-1} \cdot r_{k-2} &= r_{k-1}; & r_{k-1} < r_{k-2} \\ r_{k-2} - q_k \cdot r_{k-1} &= r_k; & r_k = 0 \end{aligned}$$

Das Verfahren ist beendet, wenn $r_k = 0$ ist.

Dann gilt: r_{k-1} teilt alle vorigen r_{k-i}, $i \geq 2$ und damit auch a und b; r_{k-2} teilt aber schon nicht mehr r_{k-3}. Damit ist r_{k-1} der grösste gemeinsame Teiler von a, b

$$\mathbf{r_{k-1} = gcd(a, b)}$$

Durch Rückeinsetzen der Werte von r_i erhält man, dass der $\gcd(a, b) = r_{k-1}$ eine ganzzahlige Linearkombination von a und b ist $r_{k-1} = r_{k-3} - q_{k-3} \cdot r_{k-2}$; $r_{k-2} = \ldots$

$$\gcd(a, b) = r_{k-1} = q \cdot a + q' \cdot b, \quad q, q' \in \mathbb{Z} \tag{5.3}$$ cop

Der Euklidischen Logarithmus ist mit dem algebraischen Programm Maxima (LISP-basiert, public domain) schon auf einem gewöhnlichem PC sehr schnell.

5.1.2 Theoreme

5.1.2.1 Inversee Restklasse:

Zu jeder primen Äquivalenzklasse $[a]_n$,(5.2), gibt es eine inverses Äquivalenzklasse $[b]_n$, d.h.

$$\forall a \in (\mathcal{Z}/n\mathcal{Z})^* \; \exists \, b \text{ mit} \quad a \cdot b \equiv 1 \mod n \tag{5.4}$$ inv

Für dieses wichtige Resultat ist der Beweis sehr einfach: $[a]_n$ ist prim, d.h. a and n sind coprim oder $\gcd(a, n) = 1$. Es gilt daher nach (5.3)

$$\gcd(a, n) = 1 = q \cdot a + q' \cdot n \tag{5.5}$$ cop3

d.h

$$q \cdot a \equiv 1 \bmod n; \quad \text{bzw.} \quad [q \cdot a]_n = [1]_n \tag{5.6}$$

d.h. das q aus (5.5) ist das gesuchte Inverse b.

5.1.2.2 Kleiner Fermat:

Ist p prim, dann gilt [2]

$$a^p \equiv a \bmod p \quad \text{bzw} \;\; a^p - a = k \cdot p; \qquad k \in \mathbb{Z} \tag{5.7}$$ kf

[2]Fermat, Brief 1640, ohne Beweis

Normalerweise bringen wir keine mathematischen Beweise, doch der kleine Fermat ist so berühmt und der Beweis durch vollständige Induktion ist so einfach, dass wir hier eine Ausnahme machen:

$a^p \equiv a \bmod p$ gilt für $a = 1$.

Er gelte für a, d.h. $a^p - a = k \cdot p$

Nach Binomi gilt

$$(a+1)^p - (a+1) = \left(a^p + \sum_{k=1}^{p-1} \left(\begin{array}{c} p \\ k \end{array} \right) a^{p-k} + 1 \right) - (a+1) = a^p - a + \sum_{k=1}^{p-1} \left(\begin{array}{c} p \\ k \end{array} \right) a^{p-k}$$

Die Summe

$$\sum_{k=1}^{p-1} \left(\begin{array}{c} p \\ k \end{array} \right) a^{p-k} = \sum_{k=1}^{p-1} \frac{p\,(p-1)\cdots(p-k+1)}{k!} a^{p-k}$$

ist für $0 < k < p$ stets durch p teilbar, da der Faktor p im Zähler steht und er stets coprim zum Nenner ist (p ist prim) kann er nicht gekürzt werden. Daher gilt:

$$(a+1)^p - (a+1) = a^p - a + k \cdot p \quad k \in \mathbb{Z}$$

Nach Induktionsvoraussetzung ist $a^p - a = k \cdot p$, d.h.

$$(a+1)^p - (a+1) = k' \cdot p \quad k \in \mathbb{Z}$$

bzw:

$$(a+1)^p \equiv (a+1) \bmod p$$

qed

5.1.2.3 Euler-Fermat

Der kleine Fermat wurde 1736 von Euler bewiesen und erweitert: [3]

$$a^{\phi(n)} \equiv 1 \bmod n \tag{5.8}$$ ef

wobei a coprim zu n ist und $\phi(n)$ ist die **Eulersche Funktion**:

$$\phi(n) = \text{ Anzahl der zu } n \text{ coprimen Zahlen, die kleiner als } n \text{ sind, incl. der 1 !} \tag{5.9}$$ euler-n

Eigenschaften der Euler Funktion ϕ:

- Ist p prim, dann $\phi(p) = p - 1$
- Sind p_1, p_2 coprim, dann $\phi(p_1 \cdot p_2) = \phi(p_1) \cdot \phi(p_2)$

Beispiele:

$\phi(15) = 8 : \supset \{14, 13, 11, 8, 7, 4, 2, 1\} \quad \phi(5) = 4 : \supset \{4, 3, 2, 1\}; \quad \phi(3) = 2 : \supset \{2, 1\}$

$15 = 3 \cdot 5 : \; p_1 = 3, e_1 = 1;\; p_2 = 5, e_2 = 1; \phi(15) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 2 \cdot 4 = 8$

Der kleine Fermat (5.7) folgt aus Euler-Fermat (5.8) durch Multiplikation mit $[a]_n$.

[3] Euler, St. Petersburg 1736, Leibniz, unveröffentlicht, vor 1683

period

5.1.2.4 Periodizität T

Wenn $a^T \equiv 1 \mod n$ ist, dann ist die Funktion $f_{a,n}(s) : \; s \to a^s \bmod n$ periodisch mit der Periode T.

Dies ist einfach zu sehen:

$$\begin{aligned} a^T \equiv 1 \bmod n \to a^T - 1 &= k \cdot n \\ a^{T+s} - a^s &= k \cdot n \cdot a^s \\ a^{T+s} &= a^s + k' \cdot n \\ a^s &\equiv a^{T+s} \bmod n \end{aligned} \tag{5.10}$$

Daraus folgt: Die Funktion $f_{a,n}(s) : (s \to a^s \mod n)$ ist sicher periodisch wenn a, n coprim sind. Auf jeden Fall nach (5.8) mit der Periode $T' = \phi(n)$, aber möglicherweise auch mit einem Teiler von $\phi(n)$, denn mit T ist auch ein vielfaches von T eine Periode.

Umgekehrt, gilt für $s = 0$

$$a^T \equiv 1 \mod n \tag{5.11}$$

period-2

Die Periode T zu finden ist (gegenwärig) der einzige Algorithmus der über die Quanten Fourier Transformation das QC so überlegen gegen dem klassischen Rechnen macht.

5.2 RSA-Verschlüsselung

Eine asymetrische Verschlüsselung ist eine Verschlüsselung mit einem öffentlichem Schlüssel, Die Dechifrieren ist aber praktisch nur mit einem geheimen Schlussel möglich

Die Basis der gebräuchlichen RSA [4] Verschlüsselung ist:

1) Der kleine Fermat in der Eulerschen Form, (5.8)

2) Die Existenz inverser Restklassen

3) Die Quanten-FT als Basis des schneller Algorithmus

5.2.1 Chiffrierung

B veröffentlicht den Chiffriercode:

n (sehr gross) und a, nicht so gross.

Sei die ganze positive Zahl M die Nachricht (hier ausnahmsweise mit grossem Buchstaben bezeichnet, der ASCI code für einen Buchstaben), dann chifriert A diese message mit Hilfe der öffentlichen Schlüssel zu dem Chiffrat:

$$c \equiv M^a \bmod n$$

[4] RL Rivest, A Shamir, L Adleman, Communications of the ACM, 1978 - dl.acm.org
http://people.csail.mit.edu/rivest/Rsapaper.pdf

Obwohl der Chiffriercode a öffentlich ist, ist es ohne weitere Kenntnisis sehr schwer, aus c die Nachricht n zu gewinnen, man mus lösen

$$M = (c - k\,n)^{1/a}$$

wobei k eine unbekannte ganze Zahl ist.

5.2.2 Dechiffrierung

A hat aber eine einfache Möglichkeit die Nachricht M aus dem c Chifrat wiedrerzugewinnen, nämlich einen Schlüssel, die Zahl b, die er nur mit Wissen über die Struktur von n bestimmen kann: Mit diesem diesen Schlüssel b gilt:

$$c^b \equiv M \bmod n. \tag{5.12}$$ schl

Um mit Wissen über die Struktur von n und a den Schlüssel b zu bestimmen,wählt B $n = p \cdot q$ wobei p und q grosse, nicht zu sehr benachbarte und nicht zusehr verschiedene Primzahlen sind und seinen geheimen Schlüssel b, der coprim zu $\phi(n) = (p-1)(q-1)$ ist. Da b und $\phi(n) = (p-1)(q-1)$ coprim sind (s. (5.4)) gibt es ein multiplikatives Inverses a im Ring der ganzen Zahlen modulo $\phi(n)$:

$$a \cdot b \equiv 1 \bmod \phi(n) \tag{5.13}$$ dd0

Daher gilt:

$$a \cdot b = 1 + k \cdot \phi(n) \tag{5.14}$$ dd1

Aus (5.8) folgt für jedes m das p nicht als Faktor enthält:

$$M^{p-1} \equiv 1 \bmod p$$

Aus der Multiplikationsregel (5.1) folgt: $A \equiv B \bmod n \Rightarrow A^r \equiv B^r \bmod n; \quad \forall r > 0$ d.h.

$$M^{r\cdot(q-1)\cdot(p-1)} \equiv 1 \bmod p \quad \text{ sowie } M^{r\cdot\phi(n)+1} \equiv M \bmod p$$

Da $\phi(n) = (q-1)\cdot(p-1)$

$$M^{r\cdot\phi(n)+1} \equiv M \bmod p; \quad \Leftrightarrow \quad M^{r\cdot\phi(n)+1} - M = k \cdot p$$

Genauso zeigt man:

$$M^{r\cdot\phi(n)+1} \equiv M \bmod q \quad \Leftrightarrow \quad M^{r\cdot\phi(n)+1} - M = \ell \cdot q$$

Da p und q sicher coprim sind, sind die beiden letzen Gl. nur verträglich, wenn

$$k = k' \cdot q, \quad \ell = \ell' \cdot p$$

$$M^{r\cdot\phi(n)+1} - M = k' \cdot \underbrace{p \cdot q}_{n} \quad \Leftrightarrow \quad M^{r\cdot\phi(n)+1} \equiv M \bmod n$$

wegen (5.14) gilt also:

$$M^{a\cdot b} = M^{r\cdot\phi(n)+1} \equiv M \bmod n \tag{5.15}$$

dd2

Das Chiffrat war $c = M^a \bmod n$, also gilt nach (5.14) und (5.15) :

$$c^b \equiv (M^a)^b \equiv M^{a\cdot b} \equiv M^{k\cdot\phi(n)+1} \equiv M \bmod n$$

Die Entschlüsselung über $M \equiv c^b \bmod n$ ist also nur sehr einfach, wenn man, ausser den öffentlich zugänglichen Verschlüsselunsparametern, n und a auch die Zerlegung von $n = p \cdot q$ kennt und damit den Schlüssel b als modular inverses von a in der Restklass $[k]_{\phi(n)}$ bestimmen kann. Deswegen ist die Primzahlzerlegung so wichtig und die grösste Hoffnung für bzw Gefahr durch das QC.

5.3 Berechnung des Schlüssels aus dem öffentlichen n

5.3.1 Faktorzerlegung von n

erlegung2

1) Man wähle eine ganze Zahl, d die coprim zu n ist. Die Fuktion

$$f_{d,n}(x) : x \to (d^x \bmod n)$$

ist dann periodisch, s. (5.1.2.4). Die Fouriertransformation (??) erlaubt, die Periode T zu bestimmen. Haben wir T bestimmt, so können wir damit Faktoren von n bestimmen, mit folgendem Algorithmus:

Erhalten wir wir, z.B. mit hilfe der QFT die Periode T und sei T gerade (wenn T ungerade, versuchen wir es mit einem anderen d) dann gilt ((5.11))

$$a^T = (a^{T/2})^2 \equiv 1 \bmod n \tag{5.16}$$

Daraus folgt

$$a^+ \cdot a^- = a^T - 1 = 0 + k \cdot n; \quad \text{mit } a^\pm = a^{T/2} \pm 1 \tag{5.17}$$

best

Wir betrachten nun den interessanten Fall, dass $n = p_1 \cdot p_2$ mit p_ℓ prim. Dann muss das Produkt $a^+ \cdot a^-$ die Faktoren p_ℓ enthalten. Wir suchen also die grössten gemeinsamen Teiler von a^+ und a^+ und erhalten damit p_ℓ. Natürlich ist sehr leicht festzustellen ob die do gewonnenen p_ℓ tatsächlich das Produkt $p_1 \cdot p_2 = n$ ergeben.

5.3.2 Numerisches Beispiel

5.3.2.0.1 Verschlüsselung A geht bei der Konstruktion von der Zahl $n = 13 \cdot 19 = 247$ aus. Damit ist $\phi(247) = 12 \cdot 18 = 216$.

Der (öffentliche) Chiffrierschlüssel a und der geheime Dechiffrierschlüssel b müssen nach (5.14) erfüllen:

$$a \cdot b = 1 + r \cdot 216.$$

Für $r = 3$ z.B. erhalten wir
factor$(1 + 3 \cdot 216) = 11 \cdot 59$;
A kann also $n = 247$ und $a = 11$ veröffentlichen, sein geheimer Schlüssel ist dann $b = 59$
Das Ciffrat von $M = 23$ ist $c =$ mod $(23^{11}, 247) = 952809757913927 + k \cdot 247$

Bei Empfang dieser Nachricht kann A sie mit dem geheimen Schlüssel $b = 59$ keicht entziffern:

$$\text{mod}(c^b, 247) = \text{mod}(952809757913927^{59}, 247) = 23$$

Allerdings wäre ein Hacker auf dieses Ergebnis auch mit den öffentlichen Schlüssel gekommen:

$$M = c^a \Rightarrow M = c^{1/a}; \quad M = 952809757913927^{1/11} = 23$$

Aber: Zu dem kleinsten Repräsentanren derRestgruppe $M^a \bmod 247$ auch noch ein beliebiges ganzzahliges Produkt $k \cdot 247$ zufügt werden, wobei k etwa durch einen Zufallsgenerator bestimmt wird. Dann wirkt der Schlüssel b immer noch:
. z.B. $c1 = 23^{11} + 200^{11} * 247$; $\text{mod}(23^{11} + 7 * 247)^{59}, 247) = 23$
aber der Trick mit der öffentlich zugänglichen Wurzel funktioniert natürlich nicht mehr:
$(c1 + 200^{11} * 247)^{1/11} = 330.02\ldots$

Allerdings muss man schon klotzen, denn wenn k zu klein ist die Wurzel zu nahe an der message M=23. Mit $k = 10000$ erhält man: $(c1 + 10000 * 247)^{1/11} = 23.00000000542033$

5.3.2.0.2 Angriff der Hacker Die Hacker (H) kennen $n = 247$ und das Schloss $a = 11$. Sie nutzen den Shor'schen Algorithmus: Die einzelnen Schritte sind:

1) Periodenbestimmung der Funktion

$$f(j) = (d^j \bmod 247)$$

mit Hilfe der FT.

2) Primzahlzerlegung mit Hilfe der Periode, s. Abschn. factorzerlegung 5.3.1

3) Berechnung des Schlüssels b aus der Faktorzerlegung und Kenntnis und des Schlosses a. Sie suchen

1. Schritt: Periodenbestimmung

Dazu bilden sie zunächst das Quantenregister:

$$|QR_1\rangle \otimes |QR_2\rangle = \sum_j |j\rangle \otimes |7^j \bmod 247\rangle =$$

d.h. sie haben $d = 7$ gewählt.

Wir hatten dieses QR in sect. numfourier 4.3.2 bereits berechnet und gefunden:

QR_1: j	0	1	2	3	4	5	6	7	8	9	10	11	$\cdots$	255
QR_2: $f_{7,247}(j)$	1	7	49	96	178	11	77	45	68	229	121	106	$\cdots$	96

Dann wird eine Messung im QR2 durch geführt. Messung im QC heisst, wenn nicht ausdrücklich anders festgestellt, immer : **Projektion auf einen Basiszustand der CB**.

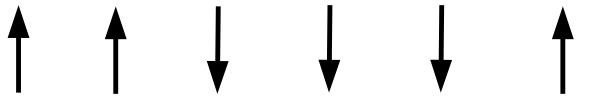
das Resultat der Messung sei z.B. 49, es wird also auf den Zustand

$$\underbrace{(\frac{1}{\mathcal{N}}\sum_{\ell}|k_\ell\rangle)}_{QR_1}\otimes\underbrace{|49\rangle}_{QR_2};\quad \text{mit}\ \ 7^{k_\ell} \bmod 247 = 49$$

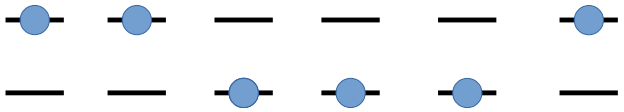
projeziert

$$\left(\frac{1}{\mathcal{N}}(\sum_{\ell}|k_\ell\rangle)\right)\otimes|1\rangle\otimes|1\rangle\otimes|0\rangle\otimes|0\rangle\otimes|0\rangle\otimes|1\rangle$$

z.B. Spin in z-Richtung:



z.B. Grundzustand oder angeregter Z.



Wir fouriertransformieren den Teil aus QR_1,

$$\frac{1}{\mathcal{N}}\widetilde{\sum_\ell|k_\ell\rangle} = \frac{1}{\mathcal{N}\sqrt{\cdot 32}}\sum_{y=0}^{31}\sum_\ell e^{2\pi \boldsymbol{i}\, y\, k_\ell/32}|y_d\rangle$$

Die Betragsquadrate der Koeffizienten von $|y_d\rangle$ sind in Abb. ftnum 5.2 aufgetragen.

An eingen Werten der Fourier-Variable y addieren sich die Koeffizienten konsruktiv, aber an den meisten "oszilieren sie sich weg". mit grosser Wahrscheinlichkeit wird also der Wert den Zustand $|8_d\rangle = |0\rangle\otimes|1\rangle\otimes|0\rangle\otimes|0\rangle\otimes|0\rangle$; $|16_d\rangle = |1\rangle\otimes|0\rangle\otimes|0\rangle\otimes|0\rangle\otimes|0\rangle$; oder $|24_d\rangle = |1\rangle\otimes|1\rangle\otimes|0\rangle\otimes|0\rangle\otimes|0\rangle$ gemessen.

Dies ergibt eine Periode in den "Fouriervariablen" y von $y_m = 8$.

Die konstruktiven Iterferenzen ergeben sich, wenn für die Periode T in $\frac{1}{\mathcal{N}}\sum_\ell|k_\ell\rangle$ und damit in in $f(\ell) = (|7^\ell\rangle \bmod 247)$ wenn $T\cdot y_m/2^5 \in \mathbb{Z}$.

Die von den Hackern gesuchte Periode muss in diesem Beispiel erfüllen:

$$T\cdot 8/32 \in \mathbb{Z} \quad \text{oder } T = n\cdot 4.$$

Daraus können die Hacker schliessen, dass die Periode T ein vielfaches von 4 sein muss: $T = k\cdot 4$. In unserem Trivialbeispiel mit den recht kleinen Zahlen wussten wir das schon vorher, aber bei 100 und mehrstelligen Zahlen ist der Überblick schon schwerer :).

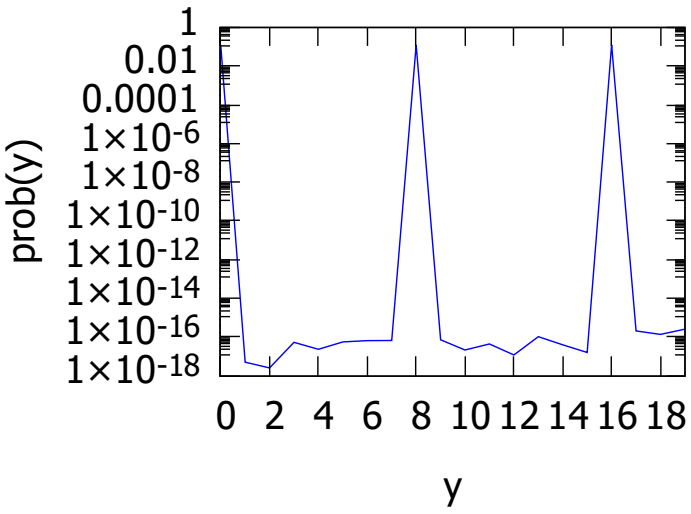


Abbildung 5.2: Betragsquadrat der Fouriercoeffizienten des Zustands (??) auf 5 Qubits

2. Schritt. Primzahlzerlegung

Die Hacker hatten $d = 7$ gewählt und $T = k * 4$ gefunden. Also wissen sie nach (5.17) dass $d^{\pm} = 7^{4k/2} \pm 1$ die Faktoren von n enthalten muss. Also versuchen sie:

$$k = 1; \quad \gcd(7^2 - 1,\ 247) = 1; \quad \gcd(7^2 + 1,\ 247) = 1 \tag{5.18}$$

$$k = 2; \quad \gcd(7^4 - 1,\ 247) = 1; \quad \gcd(7^4 + 1,\ 247) = 1 \tag{5.19}$$

$$k = 3; \quad \gcd(7^6 - 1,\ 247) = 19; \quad \gcd(7^6 + 1,\ 247) = 13 \tag{5.20}$$

und damit haben sie mit $k = 3$ die Zerlegung

$$247 = 13 \cdot 19$$

gefunden. Damit haben Sie das gleiche Wissen wie A und können jede so verschlüsselte Nachricht dechiffrieren.

3. Schritt. Bestimmung des Schlüssels

Der Schlüssel muss bei bekannten Schloss 11 und $n = 247$ Lösung der modulare Gleichung sein:

$$(b \cdot 11) \equiv 1 \mod \underbrace{\phi(13 \cdot 19)}_{12 \cdot 18 = 216}$$

z.B.

$$\begin{aligned} 216/11 &= 19 + 7/11 \\ 3 \cdot 216/11 &= 57 + 21/11 \\ (3 \cdot 216 + 1)/11 &= 57 + 22/11 = 59 \\ &\Downarrow \\ 11 \cdot 59 &= 1 + 3 \cdot 216 \\ 11 \cdot 59 &\equiv 1 \bmod 216 \end{aligned} \tag{5.21}$$

d.h. 59 ist der gesuchte Schlüssel