Knoten zur Realisierung von Quantenrechnern

Eine Anwendung der Topologie?

Martin Schottenloher

Die Idee für einen Quantencomputer (oder Quantenrechner, wie es im Folgenden heißt) wird schon seit einigen Jahrzehnten verfolgt. Dass etwas „Neues“ zu erwarten ist, wenn Berechnungen von einem Quantensystem ausgeführt werden, lässt sich bereits aus verschiedenen Bemerkungen von R. Feynman (um 1980) herauslesen.

Als solides theoretisches Konzept gibt es den Quantenrechner inzwischen seit gut 20 Jahren [3], – und in der Tat, die Umsetzung des Konzeptes in einen konkreten Rechner verspricht viel, zum einen wesentlich mehr an Rechenkraft und zum anderen den Einsatz von neuen Algorithmen, mit denen es z.B. möglich wäre, die zur Zeit gebräuchlichen Sicherheitscodes (RSA) zu knacken.

Es gibt noch weitere wichtige Gründe, sich mit der Entwicklung von Quantenrechnern zu beschäftigen. Die fortschreitende Miniaturisierung der Bauteile von herkömmlichen Rechnern bedeutet zum einen, dass dabei schon bald (schätzungsweise vor 2020) in Größenordnungen vorgestoßen wird, bei denen Quanteneffekte eine maßgebliche Rolle spielen. Zum anderen wird die Wärmeentwicklung zu einem Problem. Denn unterhalb einer festen Größenordnung ist es nach dem Stand der Technik nicht mehr möglich, die (durch Informationsverlust) entstehende Wärme in den integrierten Schaltungen der zukünftigen Computer überhaupt abzuleiten und die betroffenen Teile davor zu schützen, dass sie verglühen. Hier gibt das Quantenrechnen eine Perspektive, weil es sich so gestalten lässt, dass im Prinzip kaum Wärme entsteht.

Die Herstellung eines Quantenrechners wäre daher sicherlich auch mit einem ökonomischen Erfolg verbunden. Warum also gibt es solch ein Wunderding eines Quantenrechners noch nicht?

Es fehlt ganz einfach die zündende Idee einer Realisierung des Quantenrechners. Die Realisierung als konkretes physikalisches System (also als ein gebautes Gerät) hat vor allem mit dem Umstand zu kämpfen, dass ein Quantensystem mit seiner unmittelbaren Umgebung interagiert, und daher die Rechenoperationen auf dem Quantenniveau nicht stabil ablaufen, sondern von den genannten Interaktionen gestört werden (*Dekohärenz*). Es gilt also ein Gerät zu schaffen, welches das Quantensystem, das die Rechnungen ausführt, genügend gut abschirmt, und das dennoch Inputs (durch Präparation von geeigneten Zuständen) und Outputs (durch Messung) zulässt.

Vorschläge zum Bau eines Quantenrechners sind das Thema von vielen interessanten Arbeiten der letzten 15 Jahre. Die meisten Vorschläge konzentrieren sich darauf, lokal ein Quantensystem zu konstruieren, das genügend abgeschirmt ist, zum Beispiel durch große Kühlung (und weiteren Aufwand). In diesem Artikel möchte ich stattdessen auf einen Vorschlag von A. Kitaev eingehen, der die Topologie ins Spiel bringt, und zwar die Topologie der Knoten und Zöpfe. In der von M. Freedman[1] weiterentwickelten Idee von A. Kitaev [4] sind bestimmte Quasiteilchen, die so genannten Anyonen, von Bedeutung. Anyonen kann man sich als Teilchen vorstellen, die sich auf zweidimensionalen Flächen bewegen, und deren „Bahnen“ dann im dreidimensionalen Raumzeitdiagramm zu Verknotungen (genauer: zu Zöpfen) führen.

[1] M. Freedman erhielt 1986 die Fieldsmedaille und forscht jetzt – wie auch A. Kitaev – bei Microsoft am „Project Q“.

Prinzip des Quantenrechnens

R. Feynman hat 1982 dargelegt, dass die (zeitliche) Evolution eines Quantensystems sich nicht effizient mit einem klassischen Computer simulieren lässt, auch wenn stochastische Effekte einbezogen werden. Der Grund dafür ist, dass die Informationsmenge, die benötigt wird, um ein sich zeitlich entwickelndes Quantensystem mit klassischen Mitteln zu beschreiben, in der Regel zu schnell wächst, sie nimmt nämlich exponentiell zu. Diese Tatsache nicht als Schwäche der klassischen Beschreibung zu werten, sondern als eine Chance für neue Rechenkraft zu sehen, ist das Wesen des Quantenrechnens. Wenn es denn klar ist, dass in großem Umfang Berechnungen nötig sind, um klassisch darzustellen, was in einem Mehrteilchen-Interferenz-Experiment auf Quantenniveau passieren wird, dann kann im Prinzip umgekehrt die Durchführung des Experiments mit anschließender Messung eine komplexe Berechnung ersetzen. Das ist die grundsätzliche Idee des Quantenrechnens!

D. Deutsch zeigte im Jahre 1985 [3], dass ein universeller Quantenrechner existiert, der in der Lage ist, beliebige andere Quantenrechner zu simulieren. Das entspricht im Klassischen der universellen Turingmaschine, weshalb dieser universelle Quantenrechner auch *Quantenturingmaschine* genannt wird. In weiteren Forschungen wurde bewiesen, dass Details und Umfang des zu simulierenden Quantensystems den Aufwand des universellen Quantencomputers nicht exponentiell wachsen lässt.

Im Ergebnis: Die Quantenmechanik setzt dem klassischen Rechnen keine Grenzen, sie liefert dagegen im Prinzip neue Berechnungsmethoden. Und der universelle Quantenrechner kann wesentlich mehr als der klassische Rechner.

Qubits

Basiselement des Quantenrechners ist das *Quantenbit* (kurz: *Qubit*) in Verallgemeinerung der Bits. Während ein Bit nur zwei Zustände, etwa 0 und 1, annehmen kann, ist der Zustand eines Qubits eine *Superposition* zweier Elementarzustände. Qubits werden durch zweidimensionale komplexe Hilberträume $\mathbb{H} = \mathbb{C}^2$ repräsentiert und ihre Zustände durch Vektoren aus $\mathbb{H}$ der Länge 1. Wir notieren einen Zustandsvektor mit $|\psi\rangle \in \mathbb{H}$ und die Elemente einer Orthonormalbasis von $\mathbb{H}$ mit $|0\rangle$ und $|1\rangle$. $|\psi\rangle$ hat dann die eindeutige Darstellung

$$|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle \text{ mit } \||\psi\rangle\| = 1\,,$$

wobei $\omega_0, \omega_1 \in \mathbb{C}$ und $\omega_0\overline{\omega}_0 + \omega_1\overline{\omega}_1 = |\omega_0|^2 + |\omega_1|^2 = 1$. Die Zustände des Qubits werden daher durch die Koeffizienten (ω_0, ω_1) auf der dreidimensionalen Sphäre $\mathbb{S}^3 \subset \mathbb{C}^2$ parametrisiert. Zwei Zustandsvektoren $|\psi\rangle$ und $|\phi\rangle$ beschreiben dabei den gleichen Zustand, wenn sie sich um eine komplexe Zahl $\lambda = e^{i\theta} \in \mathbb{S}^1$ vom Betrag 1 unterscheiden, d.h. wenn $|\psi\rangle = \lambda|\phi\rangle$ ist. Man spricht von der *Phase* θ, um die sich die beiden Zustandsvektoren zum gleichen Zustand unterscheiden. Es folgt, dass die Zustände eines Qubits eineindeutig parametrisiert werden durch Punkte auf der komplex-projektiven Geraden $\mathbb{P}_1 := \mathbb{S}^3/\mathbb{S}^1$, das ist der Raum aller komplexen Geraden im $\mathbb{C}^2$. $\mathbb{P}_1$ ist die Riemannsche Zahlensphäre und ist in natürlicher Weise mit der zweidimensionalen Sphäre $\mathbb{S}^2$ identifizierbar. Insgesamt ergibt sich daher als Raum der Zustände eines Qubits die Sphäre $\mathbb{S}^2$. Die durch die Einheitsvektoren $|0\rangle$ bzw. $|1\rangle$ repräsentierten Zustände entsprechen dabei auf $\mathbb{S}^2$ dem Nord- bzw. Südpol, und ein allgemeiner Zustand wird als Punkt auf der Sphäre $\mathbb{S}^2$ gegeben. Dieses Bild entspricht der Polarisierung eines Photons oder dem Spin eines Elektrons.

Ein wichtiger Unterschied – der auch das klassische Rechnen und das Quantenrechnen so verschieden macht – ist die Tatsache, dass ein klassisches Bit nur zwei, ein Qubit dagegen unendlich viele verschiedene Zustände einnehmen kann.

Quantenregister

Eine Reihe von n Qubits wird *Quantenregister* der Größe n genannt. Das Register wird gleichgesetzt mit dem n-fachen Tensorprodukt $\mathbb{H}^{\otimes n} := \mathbb{H}_1 \otimes \mathbb{H}_2 \otimes \ldots \otimes \mathbb{H}_n$ von n Kopien des Hilbertraumes $\mathbb{H}_j = \mathbb{H} = \mathbb{C}^2$. Informationen werden in binärer Form verwendet. Z.B. hat 5 die Darstellung $|1\rangle \otimes |0\rangle \otimes |1\rangle$ wegen der Entwicklung von 5 als $5 = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$. Allgemein wird für $a \in \{0,1\}^n$ die Abkürzung

$$|a\rangle := |a_{n-1}\rangle \otimes |a_{n-2}\rangle \ldots |a_1\rangle \otimes |a_0\rangle\,,$$

$a = (a_0, a_1, \ldots, a_{n-1}) = a_0 \ldots a_{n-1}$, $a_i \in \{0,1\}$, verwendet. $|a\rangle$ repräsentiert den Zustand zum Wert ${}^*a \in \mathbb{N}$, ${}^*a := 2^0 a_0 + 2^1 a_1 + \ldots + 2^{n-1} a_{n-1}$, und wir schreiben auch $|{}^*a\rangle$ statt $|a\rangle$. Es gibt 2^n Zustände von diesem Typ, welche die natürlichen Zahlen ${}^*a$ zwischen 0 und $2^n - 1$ repräsentieren. Zugleich bilden die $|a\rangle$, $a \in \{0,1\}^n$, eine Orthonormalbasis von $\mathbb{H}^{\otimes n}$.

Ein Quantenregister der Größe 3 kann daher natürliche Zahlen wie z.B. 7 darstellen bzw. speichern, nämlich durch

$$|1\rangle \otimes |1\rangle \otimes |1\rangle = |111\rangle = |7\rangle$$

($7 = {}^*111$). Der springende Punkt im Vergleich zur klassischen Situation ist allerdings, dass ein Quantenregister auch zwei Zahlen zugleich als Superposition speichern kann. Etwa durch

$$\alpha|011\rangle + \beta|111\rangle \text{ mit } |\alpha|^2 + |\beta|^2 = 1\,,$$

$\alpha \neq 0 \neq \beta$. Das Register lässt sich sogar in einer Superposition von allen 8 Basiselementen präparieren, z.B. als $|\eta\rangle = 2^{-\frac{3}{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) = 2^{-\frac{3}{2}} \sum_{k=0}^{7} |k\rangle$. Man beachte, dass sich dieser Zustand ergibt, indem jedes der drei Qubits in den Zustand $2^{-\frac{1}{2}}(|0\rangle + |1\rangle)$ versetzt wird: $|\psi\rangle = 2^{-\frac{1}{2}}(|0\rangle + |1\rangle) \otimes 2^{-\frac{1}{2}}(|0\rangle + |1\rangle) \otimes 2^{-\frac{1}{2}}(|0\rangle + |1\rangle)$. Ein beliebiger Zustandsvektor hat die Form $\sum_{k=0}^{7} \omega_k |k\rangle$ mit $\omega_k \in \mathbb{C}$, $\sum |\omega_k|^2 = 1$. Im Falle n anstelle von 3 haben wir analoge Formeln und sehen, dass die Zustände eines Quantenregisters der Größe n über die Koeffizienten ω_k durch die Sphäre $\mathbb{S}^{2m-1} \subset \mathbb{C}^m$ parametrisiert werden, wobei $m = 2^n = \dim_{\mathbb{C}} \mathbb{H}^{\otimes n}$ ist. Stellt man noch die Mehrfachbeschreibung durch Faktoren $\lambda \in \mathbb{S}^1$ in Rechnung, so ist der eigentliche Parameterraum der komplex-projektive Raum $\mathbb{P}_{m-1} := \mathbb{S}^{2m-1}/\mathbb{S}^1$ der komplexen Geraden im $\mathbb{C}^m$. Das ist eine Mannigfaltigkeit der reellen Dimension $2m - 2 = 2^{n+1} - 2$ mit dem Potential, entsprechend viel an Information vorzuhalten.

Zeitentwicklung

Um Rechenoperationen mit Quantenregistern durchzuführen, muss man die Quantenregister verändern. Die zeitliche Entwicklung eines Quantensystems wird durch eine Grundgleichung beschrieben, die darauf hinausläuft, dass eine unitäre Transformation U auf das System wirkt, d.h. auf den Hilbertraum $\mathbb{H}$, dessen Einheitsvektoren die Zustände des Systems repräsentieren. Für einen Anfangszustand $|\psi\rangle \in \mathbb{H}$ ist $U(|\psi\rangle) \in \mathbb{H}$ der Endzustand zu einem (vorher festgelegten) späteren Zeitpunkt. Das kann man sich als verallgemeinerte Rotation eines Zustandsvektors vorstellen. Wichtig ist, dass U linear ist, d.h.

$$U(\alpha|\phi\rangle + \beta|\psi\rangle) = \alpha U(|\phi\rangle) + \beta U(|\psi\rangle)$$

für $\alpha, \beta \in \mathbb{C}$ und $|\phi\rangle, |\psi\rangle \in \mathbb{H}$, und dass $\|U(|\psi\rangle)\| = \||\psi\rangle\|$. Das gilt für alle Hilberträume $\mathbb{H}$, und trifft insbesondere für

Qubits und Quantenregister zu. Eine typische unitäre Transformation U_A auf dem Qubit ist z.B. durch lineare Fortsetzung von

$$U_A(|0\rangle) := 2^{-\frac{1}{2}}(|0\rangle + |1\rangle)\,,$$
$$U_A(|1\rangle) := 2^{-\frac{1}{2}}(|0\rangle - |1\rangle)\,,$$

gegeben. $|\eta\rangle$ findet sich dann wieder als

$$(U_A \otimes U_A \otimes U_A)(|000\rangle) = |\eta\rangle\,.$$

Quantenparallelismus

Die Zeitentwicklung hängt von den physikalischen Gegebenheiten ab. Es ist daher prinzipiell möglich, z.B. durch Anlegen von magnetischen und elektrischen Feldern, eine gewünschte Transformation maßzuschneidern. Damit wird der Vorteil, den die Quantentheorie bietet, deutlich: Ist der Anfangszustand eine Superposition, so wirkt die Zeitentwicklung ja zugleich auf alle Summanden. Auf diese Weise wird z.B. eine Funktion wegen der Linearität der Zeitentwicklung für alle diejenigen Basiszustände gleichzeitig „berechnet“, die in der anfänglichen Superposition relevant sind. Das ist der *Quantenparallelismus*, der als Erklärung dienen kann, warum im Prinzip das Quantenrechnen schneller ist als das klassische Rechnen. Die Anzahl der Basiszustände ($|a\rangle\,,\ a \in \{0,1\}^n$) wächst exponentiell mit n, sie ist 2^n. Es können also in einem Register der Größe n bis zu 2^n Informationseinheiten parallel verarbeitet werden.

Ganz so toll ist die Situation – ganz abgesehen von den Schwierigkeiten der Realisierung – dann doch nicht. Der Endzustand enthält zwar alle Funktionswerte, aber bei einer einzelnen Messung kann man nur einen Messwert ermitteln. Eine weitere Messung ist unmöglich, weil die durchgeführte Messung den Zustand verändert und die weiteren Informationen daher zerstört. Die Vorteile der Quantenmechanik werden also durch die Eigenheiten der Quantenmechanik gleich wieder zunichte gemacht? Nein, denn mit den richtigen Ideen kann die Informationsmenge, die in dem superponierten Endzustand steckt, genutzt und teilweise ausgelesen werden, so dass aus dem Quantenparallelismus doch noch ein Vorteil gezogen wird. Dazu das Beispiel:

Algorithmus von Deutsch

Es geht darum, bei einer nicht bekannten Funktion $f : \{0,1\} \to \{0,1\}$ herauszufinden, ob sie konstant ist oder nicht. Im Klassischen bleibt einem nichts übrig, als die Funktion zweimal aufzurufen, also die beiden Werte $f(0), f(1)$, zu berechnen, um diese Aufgabe zu lösen. Im Quantenrechnen reicht eine Rechenoperation mit f:

Es werden zwei Qubits verwendet. Das erste wird zu Beginn in den Zustand $|0\rangle$ und das zweite in $|1\rangle$ versetzt. Wir beginnen also mit dem Zustand $|01\rangle$. Auf jeden der beiden Zustände wird die unitäre Transformation U_A (s.o.) angewendet, also $U_A \otimes U_A$ auf $|01\rangle$. Das Ergebnis ist

$$\frac{1}{2}\left(|0\rangle + |1\rangle\right) \otimes \left(|0\rangle - |1\rangle\right) =$$
$$\frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right).$$

Die vorgegebene Funktion f definiert durch $U_f(|a_0a_1\rangle) = |b_0b_1\rangle$ mit $b_0 := a_0\,,\ b_1 := a_1 \oplus f(a_0)$ und durch lineare Fortsetzung die unitäre Transformation U_f. Dabei ist $x \oplus y$ die Addition „modulo“ 2, also $1 \oplus 1 = 0 = 0 \oplus 0, 0 \oplus 1 = 1 \oplus 0 = 1$. U_f angewandt auf unser Ergebnis von $U_A \otimes U_A(|01\rangle)$ liefert einen Zustand, der abschließend wieder durch $U_A \otimes U_A$ gedreht wird. Der Endzustand $|\phi\rangle := (U_A \otimes U_A) \circ U_f \circ (U_A \otimes U_A)(|01\rangle)$ kann elementar ausgerechnet werden. Für die konstanten Funktionen $f_1 = 0\,,\ f_2 = 1$, ergibt sich für $|\phi\rangle$:

$$|01\rangle \text{ bzw. } -|01\rangle\,.$$

Für die Identität f_3 und die Vertauschung $f_4 : 0 \mapsto 1\,,\ 1 \mapsto 0\,,$ ergibt sich

$$|11\rangle \text{ bzw. } -|11\rangle\,.$$

Eine Messung des ersten Qubits zeigt dann 0 oder 1, je nachdem ob f konstant ist oder nicht. Das Problem wird also mit nur einem Aufruf der Funktion f gelöst.

Quantengatter und Quantenrechner

Wir kommen jetzt zu dem Konzept eines Quantenrechners, und zwar als Modell eines Schaltplans (oder Schaltkreises oder Netzwerks; im Englischen „circuit“ oder „network“). Sämtliche Manipulationen an Qubits oder Quantenregister müssen unitäre Transformationen sein, wie wir oben festgestellt haben. Ein *Quantengatter* ist eine Schaltung, die eine festgelegte unitäre Operation auf einer fest ausgewählten (endlichen) Menge von Qubits in einem definierten Zeitintervall durchführt. Ein bereits eingeführtes Beispiel ist die unitäre Transformation U_A, die „Hadamard-Gatter“ genannt wird.

Ein *Quantenschaltplan* besteht aus mehreren Quantengattern, die hintereinander geschaltet sind, und für die festgelegt ist, in welcher Reihenfolge jedes einzelne Gatter auf welche Qubits wirkt. Schließlich besteht ein *Quantenrechner* aus einem solchen Schaltplan, bzw. aus einer fehlerfreien physikalischen Realisierung eines solchen Schaltplans. Mehr dazu findet man in [7].

Analog zur klassischen Situation gibt es einige wenige Quantengatter (bezeichnet als *universelle Quantengatter*), mit denen alle Quantengatter beschrieben werden können. Das läuft daraus hinaus, für die unitäre Gruppe $U(2^n)$ einen übersichtlichen Satz von Transformationen aus $U(2)$ und $U(4)$ auszuwählen, durch den $U(2^n)$ erzeugt wird. Z.B. ist das Hadamard-Gatter zusammen mit den Phasengattern ausreichend, um alle unitären Transformationen U eines Qubits, also $U \in U(2)$, darzustellen. Das *Phasengatter* zu $\theta \in \mathbb{R}$ ist durch $|0\rangle \mapsto |0\rangle$, $|1\rangle \mapsto e^{i\theta}|1\rangle$ und lineare Fortsetzung gegeben.

Wunder dauern etwas länger

Die Realisierung eines Quantenrechners steht noch aus. In gewisser Weise kann man sich die heutige Situation in etwa analog zu der Zeit um 1940 vorstellen, als die Grundprinzipien des maschinellen Rechnens durch die Turingmaschine (1936) etabliert waren, aber noch kein Computer mit seinen Röhren und Schaltungen vollständig entwickelt worden war.

Beim Bau eines Quantenrechners nach den gerade formulierten Prinzipien sind eine Vielzahl von Problemen zu überwinden. Die Dekohärenz durch die Interaktion der Bauteile mit der Umgebung ist bereits genannt worden. Ein weiteres Thema stellt die notwendige Fehlerkorrektur dar. Die Fehlerkorrektur aus der klassischen Praxis ist nicht direkt übertragbar, weil man in der Quantentheorie keine Kopien von Zuständen herstellen kann (No-Cloning-Theorem). Diese Hürde wurde aber genommen, wie z.B. in [7] nachgelesen werden kann. Ebenso ist bekannt, dass fehlertolerantes Quantenrechnen möglich ist. Allerdings ist der technische Aufwand, der getrieben werden muss, um die Schwelle an Fehlern geeignet niedrig zu halten, außerordentlich hoch.

Hier kommt das *topologische* Quantenrechnen (s.u.) zum Tragen, das grundsätzlich weniger von der Umgebung beeinflusst wird und daher weniger fehleranfällig ist.

Identische Teilchen

Ein zentrales Thema der Quantenphysik ist die Theorie der *identischen* Teilchen, das

sind Teilchen, die sich nicht durch physikalische Eigenschaften unterscheiden lassen. Zum Beispiel sind alle Elektronen in diesem Sinne identisch. Daher wird in einem System von mehreren Elektronen durch den Austausch von zwei Elektronen die Physik des Gesamtsystems nicht verändert. Das bedeutet, dass der Austausch eine Symmetrie des Systems ist, die durch eine unitäre Transformation U auf dem Hilbertraum $\mathbb{H}$ (der Wellenfunktionen) des Gesamtsystems repräsentiert wird.

Im dreidimensionalen Raum ergeben sich genau zwei solche Symmetrien, die Identität $U = \mathrm{id}$ bei den Bosonen (z.B. ist das Photon ein Boson) und die Transformation $U = -\mathrm{id}$ bei den Fermionen (z.B. ist das Elektron ein Fermion). Weitere Teilchen im Dreidimensionalen kann es in der derzeit gültigen Formulierung der Quantentheorie nicht geben. Das gilt auch für Teilchen, die sich in höherdimensionalen Räumen bewegen. Dass es nur diese zwei Möglichkeiten gibt, hat nicht zuletzt auch topologische Gründe, wie wir hier darlegen wollen:

Konfigurationsraum

Der *Konfigurationsraum* K_n von n identischen Teilchen im d-dimensionalen $X = \mathbb{R}^d$, $d \geq 2$, kann wie folgt beschrieben werden: Man bildet den Raum $K_n^\sim$ aller n-Tupel $(x_1, x_2, \ldots, x_n)$ von Punkten (bzw. Positionen) $x_j \in X$, die sich unterscheiden, d.h. $x_j \neq x_k$ für $j \neq k$, und identifiziert dann alle n-Tupel aus $K_n^\sim$, die durch Permutationen auseinander hervorgehen. Der dadurch gegebene Raum ist der Konfigurationsraum $K_n := K_n^\sim / S_n$, wobei S_n die Permutationsgruppe von n Elementen bezeichnet. Im Falle $d \geq 3$ kann man vergleichsweise leicht sehen, dass $K_n^\sim$ einfach zusammenhängend ist, also sich jede Schleife kontinuierlich innerhalb $K_n^\sim$ auf einen Punkt zusammenziehen lässt. Die Fundamentalgruppe von K_n ist daher gerade die Permutationsgruppe S_n, und diese hat genau zwei nichtäquivalente unitäre skalare Darstellungen (bzw. Charaktere, s.u.), die der Bosonen- bzw. Fermionenstatistik entsprechen.

Im Falle $d = 2$ ist die Fundamentalgruppe von K_n weitaus komplizierter, weil die Räume $K_n^\sim$ nicht einfach zusammenhängend sind. Die Fundamentalgruppe von K_n ist die *Zopfgruppe* B_n und die von $K_n^\sim$ ist die Gruppe P_n der reinen Zöpfe mit n Strähnen. Es gilt $B_n / P_n \cong S_n$. Die möglichen unitären skalaren Darstellungen von B_n lassen sich durch $\lambda \in \mathbb{S}^1$ parametrisieren, wie sich mit Hilfe einer geeigneten Beschreibung der Zopfgruppe zeigen lässt:

Zöpfe und Knoten

Um Zöpfe mit n Strähnen zu beschreiben, fixiere man im $\mathbb{R}^3$ zwei Reihen von je n Punkten $A_1, A_2, \ldots, A_n$ und $E_1, \ldots, E_n$ (z.B. $A_j := (j, 0, 0)$, $E_j := (j, 0, 1)$). Eine *Strähne* ist eine Kurve (oder Polygonzug), der einen der Punkte A_j (Anfangspunkt) mit einem der E_k (Endpunkt) ohne Überschneidungen verbindet (d.h. die zugehörige Parametrisierung kann injektiv gewählt werden)[2]. Ein *Zopf σ mit n Strähnen* wird durch n Strähnen repräsentiert, die sich nirgends schneiden (je zwei Strähnen sind ohne gemeinsame Punkte). Es wird daher der Punkt A_j mit genau einem Punkt $E_{s(j)}$ verbunden und damit zu σ eine Permutation $s \in S_n$ definiert. Wenn diese Permutation die Identität ist, also A_j mit E_j verbindet für $1 \leq j \leq n$, so spricht man von einem *reinen Zopf* mit n Strähnen. Zwei Zöpfe gelten als *äquivalent*, wenn sie sich

[2] Die Kurven müssen außerdem noch stückweise regulär sein, d.h. dass sie in einer geeigneten Parametrisierung, abgesehen von endlich vielen Punkten, stets einen nichtverschwindenden Geschwindigkeitsvektor haben.

kontinuierlich (durch eine sogenannte Homotopie) so ineinander deformieren lassen, dass sie stets punktfremde injektive Strähnen als Zwischenstufen haben. Für den Fall $n = 4$ seien drei typische Zöpfe skizziert:

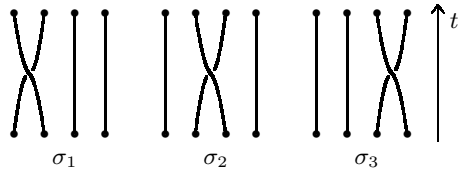

Abb. 1: Drei Zöpfe mit $n = 4$ Strähnen

Offensichtlich sind die in Abb. 1 skizzierten Zöpfe keine reinen Zöpfe.

Die Abbildung soll auch zeigen, dass Zöpfe als Bewegung des Systems von n Punkten in der Ebene $F = \mathbb{R}^2$ (als *Raum*) verstanden werden können, die zu einer Vertauschung führt: Die Bewegung hängt ab von dem Zeitparameter t (siehe Abb. 1) und sie vollzieht sich in der Ebene F, welche die Anfangspunkte A_j enthält und die senkrecht zur Zeichenebene steht. Zum Zeitpunkt $t = 0$ beginnt die Bewegung in den Anfangspunkten, zwischendurch müssen die Punkte stets in getrennten Positionen auf F sein und zu einem festen Zeitpunkt $t = T$, z.B. $T = 1$, endet die Bewegung in den Endpunkten. Die Strähnen sind dann die Weltlinien und die Skizze in Abb. 1 zeigt die Bewegung in einem Raumzeitdiagramm. Bewegungen gelten als gleich, wenn sie sich überschneidungsfrei stetig ineinander überführen lassen.

Die Menge B_n' (der Äquivalenzklassen) der Zöpfe wird zu einer Gruppe durch die Definition einer Verknüpfung, in der die jeweiligen Verzopfungen hintereinander ausgeführt werden: Für Zöpfe σ und τ sei σ^1 die Strähne von σ, die A_1 mit $E_{s(1)}$ verbindet und $\tau^{s(1)}$ die Strähne von τ, die $A_{s(1)}$ mit $E_{t(s(1))}$ verbindet (t ist die zu τ gehörige Permutation der Indizes). Dann liefert die Hintereinanderdurchlaufung der Kurve σ^1 und dann der Kurve $\tau^{s(1)}$, deren Beginn man jetzt bei $E_{s(1)}$ ansetzt, nach geeigneter Stauchung eine Kurve von A_1 nach $E_{t(s(1))}$, welche die erste Strähne von $\tau\sigma$ definiert. Genauso werden die weiteren Strähnen von $\tau\sigma$ definiert, um einen wohldefinierten Zopf $\tau\sigma$ zu erhalten.

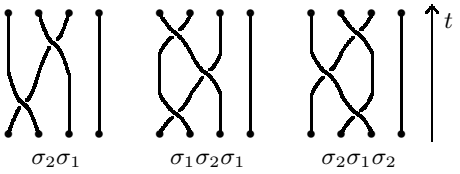

Abb. 2: Verknüpfungen

Es erfordert keine große Mühe nachzuweisen, dass B_n' mit dieser Verknüpfung zu einer Gruppe – der *Artinschen Zopfgruppe* – wird. Die Abb. 2 zeigt, dass $\sigma_1\sigma_2\sigma_1$ und $\sigma_2\sigma_1\sigma_2$ übereinstimmen, weil sie sich stetig ineinander deformieren lassen. Analog gilt $\sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3$. Außerdem ist offensichtlich $\sigma_1\sigma_3 = \sigma_3\sigma_1$. Das sind alle Relationen der σ_j, und die Gruppe B_4' wird von den σ_i erzeugt. B_n' erweist sich ganz analog als isomorph zur Gruppe in $n - 1$ Erzeugern σ_j mit den Relationen $\sigma_j\sigma_{j+1}\sigma_j = \sigma_{j+1}\sigma_j\sigma_{j+1}$, $1 \leq j \leq n - 2$ und $\sigma_j\sigma_k = \sigma_k\sigma_j$ für $|j - k| \geq 2$. Es folgt: ${B_2}' \cong \mathbb{Z}$ und alle weiteren B_n' , $n \geq 3$, sind ebenfalls unendlich.

Wir haben uns den Zöpfen etwas ausführlicher zugewandt, weil sie für das topologische Quantenrechnen eine wichtige Rolle spielen. Außerdem geben sie eine Realisierung der Fundamentalgruppen der oben behandelten Konfigurationsräume, denn die Gruppe B_n' erweist sich als isomorph zu der weiter oben definierten Fundamentalgruppe B_n des Konfigurationsraumes von n identischen Teilchen im $\mathbb{R}^2$. Ferner können

wir mit der expliziten Beschreibung auch sofort die unitären skalaren Darstellungen von B_n angeben, es sind dies die Homomorphismen $\rho : B_n \to \mathbb{S}^1$. Diese sind festgelegt durch $\rho(\sigma_j) = e^{i\theta_j}$ mit $e^{\theta_j} = e^{\theta_k}$ für alle $1 \leq j, k \leq n-1$, weil die $\rho(\sigma_j)$ die Relationen erfüllen müssen. Umgekehrt liefert jede Vorgabe von $\theta_j = \theta \in \mathbb{R}$ einen solchen Homomorphismus.

Über die Gruppenisomorphie $B_n/P_n \cong S_n$ lassen sich schließlich auch die unitären skalaren Darstellungen der Permutationsgruppe S_n bestimmen, die ja die Fundamentalgruppe der Konfigurationsräume K_n in den Dimensionen $d \geq 3$ ist: Es gibt nur zwei solche Darstellungen. Denn jeder Homomorphismus $\rho : B_n \to \mathbb{S}^1$, der von einem Homomorphismus $r : S_n \to \mathbb{S}^1$ kommt, muss auf der Untergruppe P_n der reinen Zöpfe konstant gleich dem neutralen Element 1 sein. Wegen $\sigma_j^2 \in P_n$ folgt $\rho(\sigma_j)^2 = 1$, und damit $\rho(\sigma_j) = \pm 1$. Wegen der Relation $\sigma_j\sigma_{j+1}\sigma_j = \sigma_{j+1}\sigma_j\sigma_{j+1}$ folgt entweder stets $\rho(\sigma_j) = 1$ oder stets $\rho(\sigma_j) = -1$. Der erste Fall entspricht den Bosonen und der zweite den Fermionen.

Aus Zöpfen werden Knoten, wenn man die Anfangspunkte mit den Endpunkten durch Kurven überschneidungsfrei (im $\mathbb{R}^3$) miteinander verbindet. Ein wesentliches Resultat besagt, dass umgekehrt jeder Knoten auf diese Weise vorkommt. Knoten und Zöpfe, wie auch Verknotungen und Verzopfungen, können daher in diesem Sinne als gleichwertig angesehen werden.

Anyonen

Teilchen, die sich nur in zwei Dimensionen bewegen, also z.B. in der Ebene $F = \mathbb{R}^2$, in der 2-Sphäre $F = \mathbb{S}^2$ oder im Torus $F = \mathbb{S}^1 \times \mathbb{S}^1$, verhalten sich bei Vertauschung fundamental anders als solche in höheren Dimensionen: Es gibt nicht nur Fermionen und Bosonen, sondern es treten weitere unitäre Symmetrietransformationen auf, die durch Teilchenaustausch entstehen. Das passt zur Beschreibung der unitären skalaren Darstellungen von B_n (s.o.), kann aber auch in Verbindung gebracht werden mit denjenigen projektiven Darstellungen der Gruppe $\mathrm{SO}(2,1)$, die nicht durch eine lineare Darstellung induziert werden.

Man nennt die Teilchen, die nicht Fermionen oder Bosonen sind, *Anyonen*[3], da jede beliebige („any") Phase zugelassen ist (vgl. [9] für eine elementare Einführung). Im Experiment lassen sich tatsächlich Konfigurationen realisieren, die zu Anyonen führen könnten. Dazu werden Elektronen zwischen zwei Halbleitern eingefangen, so dass eine Bewegung senkrecht zur Grenzfläche nicht möglich ist. Anregungen des so präparierten Elektronengases verhalten sich bei geeigneten Bedingungen wie Systeme von Teilchen in der Grenzfläche. Bekannt geworden ist das Beispiel des Experiments zum fraktionalen Quantum-Hall-Effekt, bei dem sich die Anregungen wie Teilchen verhalten, die einen Bruchteil der Elektronenladung tragen. Ob sich auch Anyonen erzeugen lassen, die die Eigenschaften haben, wie sie für den topologischen Quantenrechner benötigt werden, ist aber bisher nicht geklärt.

Was sind diese „Anyonen-Eigenschaften"? Wir wollen noch einmal auf das Vertauschen von Teilchen zurückkommen. Man kann sich bei einem System von zum Beispiel 4 Teilchen den Austausch von Teilchen 1 und Teilchen 2 durch das erste Diagramm in Abb. 1 veranschaulichen. Dabei entspricht unsere Skizze dem Vertauschen im Uhrzeigersinn. Eine Vertauschung im Gegenuhrzeigersinn führt gerade zu dem inversen Zopf σ_1^{-1}, für den in einer zu Abb. 1 analogen Skizze bei der Überkreuzung die

[3] nicht zu verwechseln mit Anionen

Strähne von 1 nach 2 im Vordergrund liegt. Beliebige Vertauschungen führen so zu allen möglichen Zöpfen.

Jede Sequenz von Vertauschungen bedeutet auf dem Niveau der Zustände eine Symmetrie, d.h. eine unitäre Transformation des jeweiligen Quantenregisters.

Für das topologische Quantenrechnen müssen die Anyonen *nichtabelsch* sein, das heißt, dass nicht alle diese unitären Operatoren miteinander vertauschen, dass sie also von einer nichtabelschen und daher höherdimensionalen Darstellung der Zopfgruppe B_n kommen. Solche Anyonen treten in theoretischen Überlegungen auf, wenn man von Quantenfeldtheorien mit einer nichtabelschen Eichgruppe (z.B. $\mathrm{SU}(2)$) ausgeht.

Es ist schließlich erforderlich, dass es verschiedene Arten von Anyonen gibt, so dass zu jedem Teilchen auch ein Antiteilchen gehört. Zwischen diesen Teilchen gibt es feste Regeln der Fusion und der Spaltung (s.u.).

Topologisches Quantenrechnen

Bevor wir auf weitere Eigenschaften der Anyonen eingehen, soll erst einmal das Grundprinzip des topologischen Quantenrechnens mit Anyonen dargelegt werden (vgl. [8]).

1. Im ersten Schritt werden eine endliche Anzahl von Anyon–Antianyon Paaren erzeugt und in einer Reihe angeordnet. Sie stellen die Qubits der Eingabe der Berechnung dar.

2. Die präparierten Anyonen werden in einem zweiten Schritt durch Einwirkung von elektrischen und magnetischen (und evtl. weiteren) Feldern vertauscht. Sie erzeugen dabei einen Zopf und weiterhin eine unitäre Transformation des Gesamtsystems. Diese wirkt sich auf die Fusion der Anyonen aus.

3. Im Endzustand werden benachbarte Teilchen fusioniert und es wird festgehalten, ob die Teilchen vollständig verschwinden oder nicht. Diese Daten stellen das Ergebnis der Berechnung dar.

Der wesentliche Unterschied zu einem Quantenrechner im Schaltplan-Modell, wie wir ihn oben vorgestellt haben, ist die Tatsache, dass auf Grund von quantentheoretischen Eigenschaften die (globalen) topologischen Konfigurationen gegen kleine Störungen unempfindlich sind, die Berechnung also weitaus weniger störanfällig ist (vgl. [2, 8]).

Äquivalenz

M. Freedman hat in Kooperation mit anderen Forschern zeigen können, dass die hier vorgestellten Modelle des Quantenrechnens äquivalent sind. Einerseits kann jeder Quantenrechner im Schaltplan-Modell durch einen topologischen Quantenrechner simuliert werden, andererseits gilt das auch umgekehrt. Dahinter steckt möglicherweise ein Prinzip, wie es im Klassischen durch die Church-Turing-These formuliert wird: Alle Konzepte des Quantenrechnens sind letztlich äquivalent.

Knoteninvarianten

Im Grundsatz gibt das Konzept des topologischen Quantenrechnens mit Hilfe von Anyonen auch die Möglichkeit, Knoteninvarianten direkt zu ermitteln, indem der entsprechende Knoten (bzw. Zopf, s.o.) über die Anyonenbahnen realisiert und dann einfach gemessen wird. Dieser Ansatz steht in einer engen Beziehung zu den Ideen von E. Witten[4], der in der Arbeit [11] eine Grundlage für die Existenz einer großen Klasse von Knoteninvarianten durch Quantenfeldtheorien (hier die Chern-

[4] Fieldsmedaille 1990

Simons-Theorie) liefert und in diesem Kontext den Anstoß zu einer neuen Theorie, der *topologischen Feldtheorie*, gegeben hat.

Fusion und Spaltung

Welche Eigenschaften der Anyonen für das Quantenrechnen sinnvoll und erforderlich sind, wird in der Beschreibung von verschiedenen Anyonenmodellen dargelegt. Eine Einführung dazu findet sich in [8], und ein spezielles, exakt lösbares Modell, das dem Ising-Modell der Statistischen Physik entspricht, wurde von A. Kitaev [5] ausgearbeitet. Im Kern geht es darum, die Fusion von je zwei Anyonen zu beschreiben. Die Quintessenz ist eine Fusionsregel von dem Typ

$$\mu \times \nu = \sum_{\lambda} N_{\mu\nu}^{\lambda} \lambda \,.$$

Dabei bezeichnen λ, μ, ν Teilchensorten, $\times$ steht für Fusion, und auf der rechten Seite stehen die bei der Fusion von μ, ν entstehenden Teilchen der Sorte λ mit ihrer Vielfachheit $N_{\mu\nu}^{\lambda}$. Die Gleichung kann auch von rechts nach links gelesen werden und beschreibt dann die Spaltung von Anyonen.

Die Fusionsregeln (mit zusätzlichen Bedingungen) beinhalten eine reiche algebraische Struktur. Fusionsregeln treten in vielen Bereichen der Mathematik und Physik auf, u.a. bei Kategorien von Darstellungen einer Gruppe, bei Quantengruppen und Hopf-Algebren, bei der Verlinde-Formel [1], bei topologischen Feldtheorien [11] und konformen Feldtheorien [6], und bei modularen Kategorien. In [8] wird behauptet, dass die Fusionsregeln des dort dargestellten Anyonenmodells eine unitäre modulare Kategorie festlegen, und der Beweis dazu wird in [10] erbracht. Aus allgemeinen Resultaten über solche Kategorien folgt, dass diese Anyonenmodelle deshalb eine topologische Feldtheorie bestimmen.

Viele Details zu dem Thema „topologisches Quantenrechnen“ mussten fortgelassen werden, insbesondere zur physikalischen Realisierung, aber auch zum Quantenrechnen überhaupt, wie z.B. die Nutzung der Verschränkung von quantentheoretischen Zuständen. Sie können in der angegebenen Literatur nachgelesen werden.

Literatur

[1] Blau, M./Thompson, G.: *Derivation of the Verlinde Formula from Chern-Simons Theory and the G/G model.* `http://arxiv.org/hep-th/9305010` (1993).

[2] Collins, G.P.: Quantenknoten in der Raumzeit. *Spektrum d. Wiss.* (Juli 2006), 35–41.

[3] Deutsch, D.: Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. Roy. Soc. London, Ser A* **400** (1985), 97–117.

[4] Freedman, M./Kitaev, A./Larsen, M./Wang, Z.: *Topological quantum computation.* `http://arxiv.org/quant-ph/0101025` (2002).

[5] Kitaev, A.: *Anyons in an exactly solved model and beyond.* `http://arxiv.org/cond-mat/0506438` (2005)

[6] Moore, G./Seiberg, N.: Classical and quantum conformal field theory. *Comm. Math. Phys.* **123** (1989), 171– 254.

[7] Nielsen, M.A. / Chuang, I.L.: *Quantum Computation and Quantum Information.* Cambridge Univ. Press (2000).

[8] Preskill, J.: *Topological Quantum Computation.* `http://www.theory.caltech.edu/~preskill/ph219/topological.pdf`

[9] Rao, S.: *An Anyon Primer.* `http://arxiv.org/abs/hep-th/9209066` (1992).

[10] Schaffry, M.: *Knoteninvarianten und topologisches Quantenrechnen.* Diplomarbeit (2006), LMU München.

[11] Witten, E.: Quantum Field Theory and the Jones Polynomial. *Comm. Math. Phys.* **121** (1989), 351–399.