Nano-Qubits für Quantencomputer

Gerd Schön und Yuriy Makhlin

Quantencomputer können gewisse Aufgaben sehr viel schneller bewältigen als klassische Computer. Während die theoretischen Konzepte hierzu schon weit entwickelt sind, stecken die physikalischen Realisierungen noch in den Anfangsstadien. Für logische Operationen und Speicher sowie die Integration in elektronische Schaltungen erscheinen nanoelektronische Bauelemente am besten geeignet. Josephson-Kontakte mit kleiner Kapazität kombinieren die Phasenkohärenz des Supraleiters mit den Kontrollmöglichkeiten von Einzelelektronensystemen.

Die Miniaturisierung elektronischer Bauelemente brachte enorme Gewinne an Rechen- und Speicherleistung. Es ist jedoch absehbar, dass die traditionellen Halbleitertechnologien in wenigen Jahren an Grenzen stoßen, unterhalb derer klassische Beschreibungen nicht mehr ausreichen. In Schaltungen mit kleinen Kapazitäten werden Einzelelektroneneffekte sichtbar, während in metallischen Leitern mit Längen unterhalb einiger Mikrometer die quantenmechanische Kohärenz der Elektronenbewegung wichtig wird. Für Forschungszwecke werden bereits heute routinemäßig elektronische Schaltungen mit Abmessungen bis hinab zu 10 Nanometern hergestellt, und die genannten Effekte werden daran intensiv untersucht.

Diese Untersuchungen sind auch durch die Perspektive technischer Anwendungen motiviert. Davon sind einige inzwischen realisiert. Beispielsweise werden Einzelelektronen-Transistoren als äußerst empfindliche Elektrometer verwendet. Von Anfang an war es auch ein Ziel, diese Bauelemente, bei denen der Schaltvorgang durch ein einzelnes Elektron bewirkt wird, für digitale Anwendungen zu nutzen. Offensichtlich stellen sie die kleinst möglichen elektronischen Speicher dar. Allerdings macht ihre extreme Empfindlichkeit sie auch sehr anfällig gegenüber Störungen wie zufällig verteilte Ladungen in der Umgebung. Dies und die anhaltenden Fortschritte bei klassischen Technologien schränkt die Bedeutung von Einzelelektronensystemen für *klassische* digitale Anwendungen stark ein.

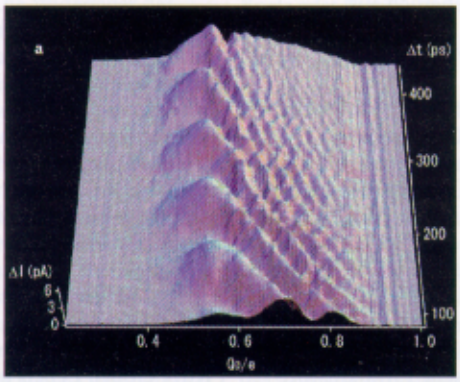


Abb. 8. Oszillationen des Stromes aufgrund der kohärenten Oszillationen des Quantenzustands, der durch einen Schaltprozess der Gatterspannung auf einen Wert $CV = Q_0$ der Dauer Δt gesteuert ist (mit Genehmigung von Nature und Y. Nakamura).

Elektronische Elemente mit Abmessungen von wenigen Nanometern können auch als Bausteine von Quanteninformationssystemen dienen. Hier spielen die quantenmechanische Kohärenz und die Kontrolle der Quantenfreiheitsgrade eine wesentliche Rolle, und klassische Technologien bieten keine Alternative. Das Interesse an dieser neuartigen Technologie ist groß, da Quantencomputer Aufgaben durchführen könnten, die kein klassischer Computer in akzeptabler Zeit bewältigen kann [1, 2, 3]. Die Quantenkommunikation würde auf der anderen Seite eine abhörsichere Übertragung von Nachrichten ermöglichen [4]. Die wohl bekannteste Anwendung eines potentiellen Quantencomputers ist das von Shor [5] entwickelte Verfahren zur Faktorisierung sehr großer ganzer Zahlen (siehe „Faktorisierung großer Zahlen", Seite 36). Dies ist für die Kryptographie – die Verschlüsselung von Nachrichten – von großer Bedeutung (siehe „Das RSA-Verfahren zur Verschlüsselung von Daten", Seite 36)

Ein Quantencomputer, der eine Überlagerung aus vielen quantenmechanischen Zuständen parallel bearbeitet, kann diese Aufgabe außerordentlich wirkungsvoll durchführen [5] (siehe „Der Shorsche Algorithmus" Seite 37). Die Rechenzeit steigt nur wie eine Potenz ($\propto L^3$) mit der Zahl der Stellen L und nicht – wie beim klassischen Computer – exponentiell ($\propto L^2$). Was dies praktisch bedeutet, wird durch das folgende Zahlenbeispiel verdeutlicht: Während eine Zahl mit 130 Stellen mit einem Cluster moderner Computer in ungefähr einem Monat faktorisiert werden kann, würde es bei einer Zahl mit 400 Stellen 10^{10} Jahre dauern, also so lange wie das Alter unseres Universums. Dagegen dauerte es bei einem hypothetischen Quantencomputer für die längere Zahl *nur* ungefähr dreißig Monate!

Während beim klassischen Computer das Bit die elementare Einheit darstellt, die zwei Zustände 0 und 1 annehmen kann, benötigt man für einen Quantencomputer ein Quantenbit (Qubit). Ein Qubit ist nichts anderes als ein quantenmechanisches Zwei-Niveau-System. Qubits verhalten sich quantenmechanisch phasenkohärent, bleiben also in ihrer zeitlichen Entwicklung in einer festen

0031-9252/00/0101-0034 $ 17.50 + .50/0

Phasenbeziehung zueinander. Gleichzeitig müssen sie aber auch kontrolliert manipuliert und gekoppelt werden können. Verschiedene physikalische Realisierungen wurden als mögliche Qubits vorgeschlagen. Wir beschreiben hier Josephson-Kontakte mit Abmessungen von wenigen Nanometern, bei denen Ladungen einzelner Cooper-Paare [6, 7] kontrolliert werden können. Bei einem verwandten Vorschlag ist der relevante Freiheitsgrad der Fluss in einer supraleitenden Ringgeometrie [8]. Andere Beispiele sind Ionen in Ionenfallen mit zwei quantenmechanischen Niveaus, die durch einen Laser angeregt werden können [9, 10], Kernspins in geeigneten Molekülen [11, 12], quantenoptische Systeme [13] sowie Spins von Elektronen in Quantenpunktstrukturen, die sich ebenfalls mit modernen Nanostrukturierungsverfahren herstellen lassen [14]. Erste kontrollierte Quantenmanipulationen sind bereits an einigen dieser Systeme durchgeführt worden.

Unter dem Gesichtspunkt möglicher Anwendungen sind die nanoelektronischen Realisierungen am interessantesten, da sie in elektronische Schaltkreise integriert werden können und die nötige Erweiterung auf vielkomponentige Systeme am ehesten ermöglichen. Josephson-Kontakte mit Abmessungen im Bereich von 100 nm und darunter und entsprechend kleinen Kapazitäten von weniger als 10^{-15} F (1 Femtofarad) kombinieren die Phasenkohärenz des supraleitenden Zustands mit den Kontrollmöglichkeiten von Einzelelektronensystemen [6, 7]. Ihre Phasenkohärenzzeit ist lang genug, um eine große Zahl der benötigten Operationen durchzuführen. Anschließend an die Quantenmanipulationen muss der Endzustand ausgelesen werden. Dies ist ein quantenmechanischer Messprozess, den man durch Ankoppeln von Einzelelektronentransistoren an die Qubits bewerkstelligen kann [15].

Die benötigten Josephson-Kontakte lassen sich mit verfügbaren Technologien herstellen (Abbildung 1), und es ist schon experimentell gezeigt worden, dass sie sich unter geeigneten Umständen wie quantenmechanische Zwei-Niveau-Systeme verhalten. So ließ sich nachweisen, dass die Eigenzustände Superpositionen von Ladungszuständen sind [16, 17]. Und in jüngster Zeit hat ein Forscherteam in Japan [18] an einem Josephson-Qubit die so genannten kohärenten Quantenoszillationen, die ein in einer Superposition von Eigenzuständen präpariertes Quantensystem zeigen

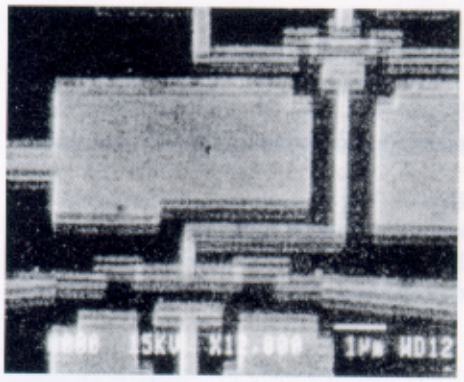


Abb. 1. Bild eines supraleitenden Elektronenkastens (oben) gekoppelt an einen Einzelelektronentransistor (unten). Die Strukturen werden mittels Schattenbedampfung durch eine Maske in mehreren Schritten unter verschiedenen Winkeln hergestellt. Dadurch können in den Bereichen, wo verschiedene Lagen überlappen, Kontakte mit sehr kleiner Fläche (100 nm × 100 nm und kleiner) und entsprechend kleiner Kapazität erzeugt werden [16].

sollte, zeitaufgelöst beobachtet. Dies ist das erste erfolgreiche Experiment dieser Art an einem Festkörpersystem. Nach diesem Durchbruch ist damit zu rechnen, dass in naher Zukunft weitere Fortschritte in Richtung des „Quantum State Engineering" gemacht werden.

Die Physik von Qubits

Um die Funktionsweise eines Quantencomputers zu verstehen, müssen wir uns etwas genauer mit der Physik von quantenmechanischen Zwei-Niveau-Systemen auseinandersetzen. Dazu ist es zweckmäßig, ein konkretes physikalisches Modell zu betrachten, nämlich den Spin, der eine wichtige Rolle in der Quantenphysik spielt.

Elektronen, Protonen und Neutronen besitzen einen internen Freiheitsgrad, einen Eigendrehimpuls, der als Spin (Spin-1/2) bezeichnet wird. Er wird durch sogenannte Pauli-Matrizen $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ dargestellt. Dieser rein quantenmechanische Freiheitsgrad kann in zwei Basiszuständen, „Spin nach oben" $|\uparrow\rangle = \binom{1}{0}$ oder „Spin nach unten" $|\downarrow\rangle = \binom{0}{1}$ vorkommen, insofern besitzt er Eigenschaften wie ein klassisches Bit mit den Zuständen 0 und 1. Beide Schreibweisen, Pfeil oder zweikomponentiger Vektor, werden im Folgenden verwendet. Der Quantenspin kann aber auch in einer Superposition der beiden Basiszustände sein $|\psi\rangle = a\,|\uparrow\rangle + b\,|\downarrow\rangle = \binom{a}{b}$ mit zwei komplexwertigen, normierten Amplituden $|a|^2 + |b|^2 = 1$. Verbunden mit dem Spin ist ein magnetisches Moment $\mu\vec{\sigma}$ (μ Bohrsches Magneton). Seine Energie in einem Magnetfeld $\vec{B} = (B_x, B_y, B_z)$ wird durch den Hamilton-Operator $H = -\mu\vec{B} \cdot \vec{\sigma}$ dargestellt.

Stellen wir uns nun vor, dass der Spin anfänglich in einem Zustand $|\psi(0)\rangle$ präpariert ist und dass wir zur Zeit $t = 0$ das Feld plötzlich für eine gewisse Dauer τ in x-Richtung schalten können. Die Gesetze der Quantenmechanik sagen uns dann, dass der Spin rotiert. Dies wird mathematisch durch eine unitäre Transformation beschrieben,

$$|\psi(\tau)\rangle = U_x(\alpha)|\psi(0)\rangle \qquad (1)$$

mit dem unitären Drehoperator

$$U_x(\alpha) = \begin{pmatrix} \cos\alpha & i\sin\alpha \\ i\sin\alpha & \cos\alpha \end{pmatrix}, \qquad (2)$$

wo $\alpha = \mu B_x \tau/\hbar$. Wenn wir also vom Grundzustand für ein homogenes Magnetfeld in z-Richtung ausgehen, $|\uparrow\rangle = \binom{1}{0}$, ist nach der Drehung $|\psi(\tau)\rangle = \binom{\cos\alpha}{i\sin\alpha}$. Wir können durch die Kontrolle des Feldes und der Zeitdauer τ, während der es in x-Richtung geschaltet ist, einen neuen Zustand – er entspricht der Richtung des Spins – kontrolliert einstellen.

Ein idealer Quantencomputer

Für einen Quantencomputer benötigen wir nun viele, man sagt auch Register von L Qubits. Im obigen Beispiel wären dies L Spin-1/2-Systeme. Ein ideales Modell unseres Quantencomputers wäre dann etwa durch den folgenden Hamilton-Operator für Spins auf Gitterplätzen $i = 1, \ldots, L$ zu beschreiben

$$H = -\sum_{i=1}^{L}\left[\mu B_z^i(t)\,\sigma_z^i + \mu B_x^i(t)\,\sigma_x^i\right] + \sum_{i\neq j} J^{ij}(t)\,\sigma_+^i\sigma_-^j + H_{mess}(t) + H_{diss}. \qquad (3)$$

Eine wichtige Bedingung ist dabei, dass das Magnetfeld für jeden einzelnen Spin individuell kontrollierbar ist. Für unsere Zwecke genügt es, Magnetfelder in der x-z-Ebene, $B_x^i(t)$ und $B_z^i(t)$, zu betrachten, die aber beide separat ein- und ausschaltbar sein sollten. Weiterhin müssen die Spins untereinander gekoppelt werden können. Verschiedene physikalische Wechselwirkungen bewirken ein paarweises Umklappen der Spins, wie es durch das Produkt der Matrizen $\sigma_+ = \binom{01}{00}$

und $\sigma_- = \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$ in (3) ausgedrückt wird. Zur Kontrolle dieser wichtigen Quantenmanipulation müssen die Kopplungsparameter $J^{ij}(t)$ für das gewählte Paar von Qubits ein- und ausschaltbar sein.

In der Realität ist die Kontrolle der Felder separat für jeden Spin und der Kopplungsenergien kaum möglich. Deshalb werden für die Realisierung eines Quantencomputers äquivalente Zwei-Niveau-Quantensysteme gesucht, die mehr oder weniger gut durch Modelle wie (3) beschrieben sind. Zur Erläuterung der Ideen kann man aber das obige ideale Modell gut verwenden.

Die wichtigen Schritte und Bedingungen für die Nutzung eines solchen Systems als Quantencomputer sind folgende:

(1) Restwechselwirkungen mit weiteren, verlustbringenden Freiheitsgraden der Umgebung, die in H_{diss} stecken, müssen schwach sein, da sie die notwendige Phasenkohärenz zerstören. Dies ist die Voraussetzung dafür, dass eine große Zahl der im folgenden beschriebenen Ein- und Zweibit-Operationen phasenkohärent ablaufen können.

(2) Um einen wohldefinierten Anfangszustand zu schaffen, schalten wir bei tiefen Temperaturen alle B_z-Felder auf große Werte, so dass die thermische Energie vernachlässigbar ist, $k_B T \ll \mu B_z^i$, während $B_x^i = J^{ij} = 0$. Nach genügend langem Abwarten ist dann das Spinsystem auf Grund der Restwechselwirkungen mit der Umgebung, H_{diss}, in den Grundzustand $|\uparrow\uparrow\uparrow \ldots\rangle$ relaxiert. Dann schalten wir das Magnetfeld wieder aus.

(3) Um eine Drehung des Spins i durchzuführen, schalten wir das jeweilige Feld B_x^i für eine Zeitdauer τ ein. Der Spin am Gitterplatz i dreht sich dann aus der z-Richtung heraus, beschrieben durch die unitäre Transformation $U_x(\alpha)$ in (2). Abhängig von dem Produkt aus Feldstärke und Zeitdauer $\alpha = \mu B_x \tau/\hbar$ erfolgt eine $\pi/2$- oder eine $\pi/4$-Rotation, was einen Spin-Flip (NOT-Operation) oder eine Überlagerung der zwei Spinzustände mit gleichem Gewicht erzeugt. Letztere entspricht einer $\sqrt{\text{NOT}}$-Operation; denn erst die zweifache sukzessive Anwendung produziert ein NOT. Diese Operation ist in der Quantenmechanik möglich. Sie hat offensichtlich *kein* Analogon beim klassischen Computer.

Anschalten eines Feldes B_z in z-Richtung ergibt eine weitere Operation, nämlich

$$U_z(\beta) = \begin{pmatrix} \exp(i\beta) & 0 \\ 0 & \exp(-i\beta) \end{pmatrix}.$$

Sie bewirkt eine Phasenverschiebung zwischen $|\uparrow\rangle$ und $|\downarrow\rangle$ um den Winkel $\beta = \mu B_z \tau/\hbar$.

Beide Einbit-Operationen, die jeweils nur einen einzigen Spin betreffen, sind elementare Manipulationen, die im Rahmen der Quantenrechnung benötigt werden. Zurück im Ruhezustand, wo alle Felder und Kopplungen ausgeschaltet sind, also $\vec{B} = 0$, entwickelt sich die relative Phase der Zustände nicht mehr weiter.

(4) Zur Kopplung zweier verschiedener Spins, i und j, schalten wir die entsprechende Kopplung J^{ij} für eine gewisse Zeit τ ein. In der Basis der Zwei-Spinzustände für das Paar i, j, $|\uparrow\uparrow\rangle$, $|\uparrow\downarrow\rangle$, $|\downarrow\uparrow\rangle$, $|\downarrow\downarrow\rangle$, bewirkt dies ebenfalls

Faktorisierung großer ganzer Zahlen

Die Dauer für die Zerlegung einer großen ganzen Zahl in ihre Primzahlfaktoren $N = P \cdot Q$ wächst exponentiell mit der Zahl der Stellen und ist praktisch nicht möglich für Zahlen mit mehr als 100–150 Stellen. Das ist äquivalent zu einem anderen Problem, dem Finden der Periode r der Funktion

$$f_{a,N}(j) \equiv a^j|_{\text{mod } N} \quad \text{für } j = 1, 2, 3, \ldots$$

mit einer beliebigen ganzen Zahl a. Dies ist auf einem klassischen Computer ebenso zeitraubend, kann aber [5] auf einem Quantencomputer innerhalb einer Zeit, die nur wie eine Potenz mit der Zahl der Stellen wächst, gelöst werden.

Nachdem r gefunden ist mit r gerade und $r|_{\text{mod } N} \neq -1$, erhält man P und Q als größten gemeinsamen Teiler

$$P, Q = \text{ggt}\,(a^{r/2} \pm 1, N).$$

Für diesen Schritt erfand Euklid bereits 300 v. Chr. einen effizienten Algorithmus.

Zur Erläuterung betrachten wir ein Beispiel, die Faktorisierung der Zahl $N = 15$. Wir wählen $a = 2$, dann gilt für $j = 1, 2, 3, 4, 5, 6, 7, 8, \ldots$

$$f_{2,15}(j) = 2^j|_{\text{mod } 15} = 2, 4, 8, 1, 2, 4, 8, 1, \ldots$$

Die Periode ist $r = 4$ und $a^{r/2} = 4$. Also soll $P = \text{ggt}\,(5, 15) = 5$ gelten und $Q = \text{ggt}\,(3, 15) = 3$.

Die RSA-Methode der Verschlüsselung

Netscape, Banken, aber auch der CIA verschlüsseln Daten mit dem von Rivest, Shamir und Adleman (RSA) vorgeschlagenen Verfahren. Dies geht so

– „Alice" will „Bob" eine Botschaft M chiffriert senden.
– Bob bildet das Produkt $N = P \cdot Q$ von zwei großen Primzahlen P und Q von etwa 100–150 Dezimalstellen Länge, und er wählt eine Zahl $E > 1$ mit der Eigenschaft, mit $P-1$ und $Q-1$ teilerfremd zu sein. Weiterhin berechnet er die Zahl D, für die gilt

$$ED|_{\text{mod } (P-1)(Q-1)} = 1.$$

– Bob sendet den „öffentlichen Schlüssel" (N, E) über einen öffentlichen Kanal (etwa über das Internet) an Alice. Sein geheimer Schlüssel ist (N, D).

– Alice sendet nun Bob die chiffrierte Botschaft über den öffentlichen Kanal

$$F(M) = M^E|_{\text{mod } N}.$$

– Bob kann die Botschaft leicht dechiffrieren; denn elementare Zahlentheorie besagt, dass

$$F(M)^D|_{\text{mod } N} = M.$$

Alle oben genannten Schritte sind mit effizienten Algorithmen durchführbar. Die Sicherheit des RSA-Verfahrens beruht darauf, dass kein Algorithmus bekannt ist, mit dem die Zahl N mit genügend großer Anzahl von Stellen in akzeptabler Zeit in Primzahlfaktoren zerlegt werden kann. Somit ist es für einen Lauscher praktisch nicht möglich, die Zahl D zu berechnen.

eine unitäre Transformation, die aber jetzt durch eine 4×4 – Matrix dargestellt wird,

$$U_{2b}(\gamma) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\gamma & i\sin\gamma & 0 \\ 0 & i\sin\gamma & \cos\gamma & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad (4)$$

mit $\gamma = J^{ij}\tau/\hbar$. Für $\gamma = \pi/2$ ist das Resultat ein Spin-Austausch, $|\uparrow\downarrow\rangle \rightarrow |\downarrow\uparrow\rangle$, ein sogenannter SWAP, während $\gamma = \pi/4$ die nichtklassische Operation $\sqrt{\text{SWAP}}$ liefert. Diese transformiert den Zustand $|\uparrow\downarrow\rangle$ in einen verschränkten Zustand $(|\uparrow\downarrow\rangle + i|\downarrow\uparrow\rangle)/\sqrt{2}$. Die Zweibit-Operation $\sqrt{\text{SWAP}}$, kombiniert mit Einbit-Operationen, erlaubt es, eine „controllednot" Operation (CNOT) durchzuführen, und in der Tat alle logischen Operationen, die für Quantencomputer nötig sind [19].

(5) Nachdem nun alle Quantenmanipulationen durchgeführt sind, sollte der Endzustand der Qubits ausgelesen werden können. Dazu muss ein Messgerät an die Qubits angekoppelt werden. Da die Messung im allgemeinen zu einem raschen Verlust an Phasenkohärenz führt, ist es wichtig, dass man dieses Messgerät, formal den Term $H_{\text{mess}}(t)$ in (3), ebenfalls kontrolliert ein- und ausschalten kann.

Rechnen mit Quantencomputern

Wie mit konventionellen Bits kann man mit L Qubits mit den Zuständen $|\uparrow\rangle$ und $|\downarrow\rangle$ ganze Zahlen zwischen 0 und $2^L - 1$ binär darstellen,

$$\begin{aligned} |0\rangle &= |\uparrow \ldots \uparrow\uparrow\uparrow\rangle \\ |1\rangle &= |\uparrow \ldots \uparrow\uparrow\downarrow\rangle \\ |2\rangle &= |\uparrow \ldots \uparrow\downarrow\uparrow\rangle \\ &\vdots \\ |2^L - 1\rangle &= |\downarrow \ldots \downarrow\downarrow\downarrow\rangle. \end{aligned}$$

Im klassischen Rechner ist der Anfangszustand durch *eine* Zahl charakterisiert, am Ende wird dieser *ein* Endzustand zugeordnet. Im Gegensatz dazu kann man bei Quantensystemen aber auch eine beliebige Superposition aller Zahlen erzeugen,

$$|\psi\rangle = \sum_{j=0}^{2^L-1} c_j |j\rangle, \quad (5)$$

und diese Superposition, das heißt alle Zustände parallel, entsprechend den Regeln des Programmes manipulieren. Dieses Parallelisieren ist der Grund für die Überlegenheit von Quantencomputern im Vergleich zu klassischen. Außer bei speziellen Algorithmen, wie etwa beim Shorschen zur Faktorisierung [5], geht dieser Vorteil aber wieder verloren, wenn wir am Ende der Rechnung durch eine quantenmechanische Messung wieder nur *einen* Zustand herausprojizieren.

Die oben beschriebenen unitären Transformationen stellen einen universellen Satz von Operationen dar: Sie erlauben es, alle notwendigen logischen Operationen durchzuführen [19]. Die unitären Transformationen, und daher alle Quantenrechenschritte, sind aufgrund der Kohärenz immer reversibel, während beim klassischen Computer gewöhnlich auch irreversible Schritte verwendet werden.

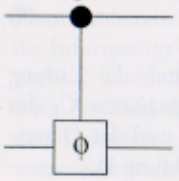
Eine in den Algorithmen häufig verwendete Operation ist das sogenannte Hadamard-Gatter, das auf einzelne Qubits wirkt,

$$-\boxed{\text{H}}- = \text{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (6)$$

Diese Transformation kann durch eine Kombination der oben beschriebenen Einbit-Operationen erzeugt werden nach $\text{H} = -iU_z(\pi/4)U_x(\pi/4)U_z(\pi/4)$, oder durch gleichzeitiges Einschalten von $B_x = B_z$ für eine geeignete Zeitdauer $\text{H} = -iU_{x+z}(\pi/2)$. Durch Anwenden jeweils eines Hadamard-Gatters für jedes Qubit können wir aus dem Grundzustand eine Superposition von allen Basiszuständen mit gleichen Amplituden erzeugen, schematisch etwa

$$\text{H}^1 \otimes \ldots \otimes \text{H}^L |\uparrow \ldots \uparrow\rangle = \frac{1}{\sqrt{2^L}} \sum_{j=0}^{2^L-1} |j\rangle. \quad (7)$$

Eine andere wichtige Zweibit-Operation ist die „kontrollierte Phasenverschiebung" des zweiten Qubits, abhängig vom Zustand des ersten. Die Darstellung in einem Diagramm, das die Entwicklung der beiden Qubits repräsentiert, sowie als Matrix in der Basis der Zwei-Spin-Zustände hat folgende Form



$$\text{R}(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix}$$

Der Shorsche Algorithmus

Der Shorsche Algorithmus [5] zur Faktorisierung großer ganzer Zahlen N beruht auf dem äquivalenten Problem, dem Finden der Periode der Funktion $f_{a,N}(j) \equiv a^j|_{\text{mod } N}$ als Funktion der ganzen Zahlen $j = 1, 2, 3, \ldots$ Es wird eine genügende Anzahl L von Qubits benötigt, um $N < 2^L$ darstellen zu können. Eine gleich große Zahl von Qubits wird für die Funktion $f_{a,N}(j)$ vorgesehen. Dann werden die folgenden Schritte durchgeführt:

(1) Als Ausgangszustand wird der Zustand $|\{j\}\rangle|\{0\}\rangle$ gewählt. Im ersten Register ist eine Superposition $|\{j\}\rangle$ aller ganzen Zahlen $1 \leq j \leq 2^L - 1$, erzeugt durch Anwenden von L Hadamard-Transformationen (7) auf den Grundzustand. Das zweite Register ist im Grundzustand.

(2) Die Exponentiation $f_{a,N}(j) \equiv a^j|_{\text{mod } N}$ kann durch eine Serie von Quantenoperationen durchgeführt werden [21]. Der Vorteil des Quantencomputers ist, dass dies parallel für die Superposition aller Zahlen j durchgeführt werden kann. Das Ergebnis ist $|\{j\}\rangle\,|\{f_{a,N}(j)\}\rangle$. Wir erwarten, dass die Funktion $f_{a,N}(j)$, die in den dafür vorgesehenen Qubits als Superposition gespeichert wird, periodisch ist.

(3) Eine Messung am zweiten Register produziert einen der möglichen Werte von $f_{a,N}(j)$, etwa die Zahl k. Gleichzeitig wird der Gesamtzustand auf den entsprechenden Unterraum projiziert. Im ersten Register finden sich nur noch genau die Zahlen j mit $f_{a,N}(j) = k$. Diese sollten periodisch angeordnet sein.

(4) Eine diskrete Fourier-Transformation des Inhalts des ersten Registers, wie oben beschrieben, erlaubt es, diese Periode zu finden und daraus nach dem bekannten Verfahren die Faktoren von N.

Alle Schritte können mit einer Zahl von Rechenoperationen durchgeführt werden, die nur wie eine Potenz, aber nicht exponentiell mit der Größe der Zahl steigt. Dieser enorme Zeitgewinn ist der wichtige Aspekt des Shorschen Algorithmus und bedingt unter anderem die große Attraktivität des Quantencomputers.

Auch dieses Gatter lässt sich aus einer Serie der oben beschriebenen Ein- und Zweibit-Operationen erzeugen.

Die in Abbildung 2 dargestellte Kombination von Hadamard-Gattern und kontrollierter Phasenverschiebung bewirkt eine diskrete Fourier-Transformation [1]

$$\sum_{j=0}^{2^L-1} c_j|j\rangle \rightarrow \sum_{k=0}^{2^L-1} \tilde{c}_k|k\rangle.$$

Der Eingangszustand mit den Amplituden c_j der Basiszustände $|j\rangle$, $j = 0, \ldots 2^L-1$ entwickelt sich dabei zum Ausgangszustand mit den neuen Amplituden $\tilde{c}_k$. Sie sind die Fourier-Transformierten der Eingangskoeffizienten

$$\tilde{c}_k = \frac{1}{2^L} \sum_{j=0}^{2^L-1} \exp\left(\frac{2\pi i k j}{2^L}\right) cj.$$

Während die Rechenzeit der Fourier-Transformation beim klassischen Computer mit der Zahl der Bits mit $L\,2^{L-1}$, exponentiell zunimmt, wächst sie beim Quantencomputer nur mit L^2 [20]. Dieser Zeitgewinn wird beim Shorschen Algorithmus zur Faktorisierung großer Zahlen genutzt (siehe „Der Shorsche Algorithmus", Seite 37).

Josephson-Kontakte als Qubits

Josephson-Kontakte mit Abmessungen von wenigen Nanometern stellen Realisierungen von Qubits dar. Das einfachste Beispiel [6] ist der supraleitende Elektronenkasten (Abbildung 3a). Die wesentlichen Variablen sind dabei die Ladung $Q = 2ne$ im Kasten, wobei n die Anzahl der überschüssigen Cooper-Paare relativ zu einem ladungsneutralen Ausgangszustand bezeichnet, und die supraleitende Phasendifferenz φ über den Josephson-Kontakt. Beides sind quantenmechanisch konjugierte Variable. Sie verhalten sich wie Impuls und Ort eines quantenmechanischen Teilchens und erfüllen eine Unschärferelation. Wenn die supraleitende Energielücke genügend groß und die Temperatur genügend tief sind, wird das Tunneln von einzelnen Elektronen unterdrückt. Die Energie des Kontaktes ist dann eine Summe von Ladungs- und Josephson-Energie

$$H = H_{ch} + H_J. \qquad (8)$$

Die Ladungsenergie ist durch die Ladung Q im Kasten und die Kapazitäten C_J des Josephson-Tunnelkontaktes und der Gatterkapazität C bestimmt (Abbildung 3),

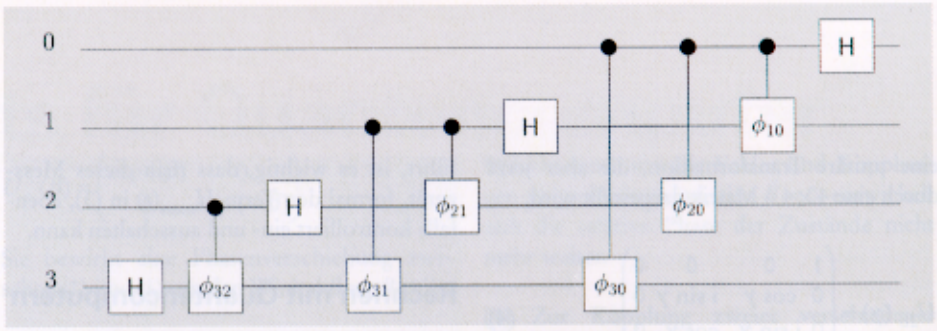


Abb. 2. Eine Realisierung der diskreten Fourier-Transformation für vier Qubits, das sind $2^4 = 16$ Koeffizienten. Die Phasenverschiebungen der kontrollierten Phasenverschiebungsgatter sind $\Phi_{jk} = \pi/2^{|j-k|}$, $j, k = 1 \ldots 6$.

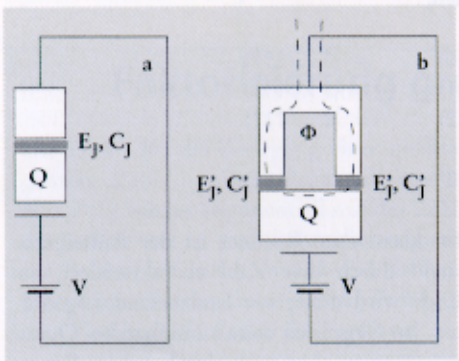


Abb. 3. Josephson-Qubits: (a) Die einfachste Realisierung, bei der die Gatterspannung, das heißt B_z^i im idealen Modell (3) kontrolliert wird. (b) Realisierung, bei der die Gatterspannung und der magnetische Fluss (durch den Strom in der gestrichelt gezeichneten Induktionsschleife) durch den Ring, das heißt B_z^i und B_x^i in (3) kontrolliert wird. Dies erlaubt auch, die Zweibit-Kopplungen zu kontrollieren.

$$H_{ch} = \frac{(Q - CV)^2}{2(C + C_J)} \cdot \qquad (9)$$

Sie ist durch eine extern kontrollierte Gatterspannung V, die an das Qubit angekoppelt ist, modulierbar. Der Josephson-Term

$$H_J = -E_J \cos\varphi \qquad (10)$$

beschreibt das Tunneln der Cooper-Paare.

Wir betrachten Kontakte, bei denen die Kapazität des Gatters klein gegen die des Tunnelkontaktes ist, $C \ll C_J$, und die resultierende Ladungsenergie $E_C = e^2/2C_J$ größer ist als die Energie der Josephson-Kopplung E_J. Im Gleichgewicht bei tiefen Temperaturen, $k_B T \ll E_C$, ist das System in dem Zustand der niedrigsten Energie, repräsentiert durch die jeweils niedrigste Parabel in Abbildung 4. Jedoch in der Nähe der Spannungen, die ungeradzahlige Vielfache von e/C sind, sind zwei benachbarte Ladungszustände, der mit n und der mit $n+1$ Cooper-Paarladungen im Ka-

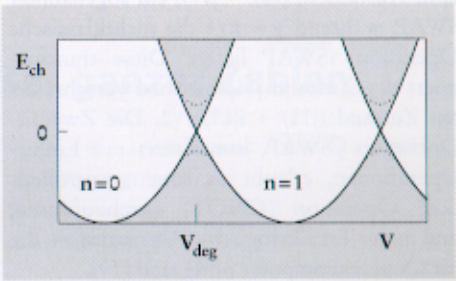


Abb. 4. Die Eigenenergie der verschiedenen Ladungszustände der supraleitenden Elektronenschachtel als Funktion der Kontrollspannung.

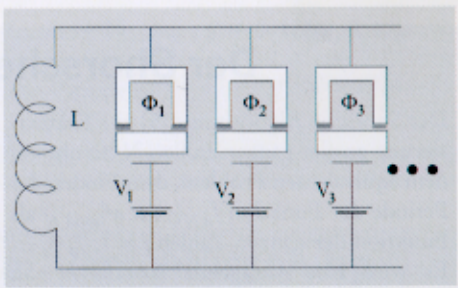


Abb. 5. Qubits werden in einem LC-Kreis gekoppelt.

sten, nahezu entartet und werden stark durch die Josephson-Kopplung gemischt.

In der Nähe dieser Entartungspunkte können wir uns auf die zwei benachbarten Ladungszustände konzentrieren. Das System reduziert sich hier auf ein quantenmechanisches Zwei-Niveau-System mit einem Freiheitsgrad, der so etwas wie einen „künstlichen Spin" darstellt. Entsprechend können wir den Zustand mit n Ladungen durch $|\uparrow\rangle$ und den mit $n+1$ Ladungen durch $|\downarrow\rangle$ bezeichnen und den Hamilton-Operator durch Pauli-Matrizen ausdrücken

$$H = -\frac{1}{2}\Delta E_{ch}(V)\,\sigma_z - \frac{1}{2}E_J\,\sigma_x. \qquad (11)$$

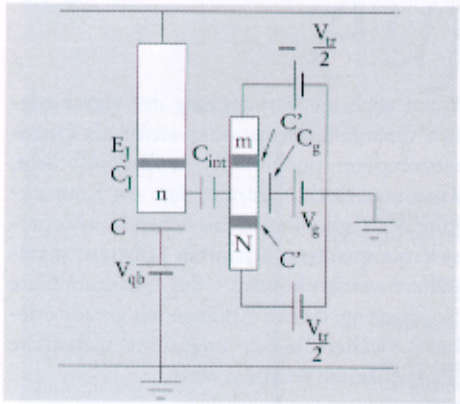


Abb. 6. Der Zustand des Qubits (links) kann durch einen Einzelelektronentransistor (rechts) ausgelesen werden. Dieser wird über eine kleine Kapazität C_{int} angekoppelt und durch eine Transportspannung V_{tr} kontrolliert. Die Zahl der Elektronen auf der Insel ist N, die Zahl derer, die durch den Transistor getunnelt sind, ist m. V_g ist die Gate-Spannung am Transistor, C' und C_g Kapazitäten, die den Transistor charakterisieren.

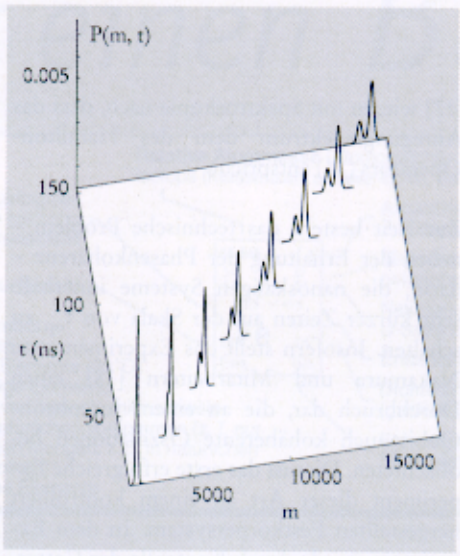


Abb. 7. Die Wahrscheinlichkeitsverteilung, dass m Elektronen in der Zeit t durch den Transistor geflossen sind. Bei dem Beispiel ist angenommen, dass das Qubit bei $t = 0$ in einer Superposition von Zuständen mit Amplitudenquadraten 1/4 und 3/4 war.

Der Unterschied in der Ladungsenergie der beiden Zustände $\Delta E_{ch}(V)$ hängt von der angelegten Kontrollspannung ab. Die Josephson-Kopplung E_J bewirkt Übergänge zwischen den beiden Zuständen.

Das System, das durch (11) beschrieben wird, mit der Möglichkeit den Koeffizienten von σ_z zu kontrollieren – das entspricht einem Magnetfeld in z-Richtung – reicht schon aus, um alle Einbit-Operationen durchzuführen [6]. Die Flexibilität und die Präzision der Operationen wird aber deutlich verbessert, wenn der Josephson-Kontakt des Qubits noch durch ein SQUID (Superconducting Quantum Interference Device) ersetzt wird [7] (Abbildung 3b). Ein SQUID besteht aus zwei Josephson-Kontakten, die in einem Ring angeordnet sind, der einen magnetischen Fluss Φ einschließt. Dieser Fluss kann extern durch den Strom kontrolliert werden, der durch eine Induktionsschleife fließt. Die effektive Josephson-Kopplungsenergie $E_J(\Phi) = 2E_J' \cos(2\pi\,\Phi/\Phi_0)$ im Hamilton-Operator (11) ist dann durch einen Faktor reduziert, der vom Fluss Φ in Einheiten des Flussquants $\Phi_0 = h/2e$ im Ring abhängt.

Das bedeutet, dass durch die angelegte Spannung am Gatter und den Strom durch die Induktionsschleife sowohl der Koeffizient von σ_z (entsprechend der z-Komponente des Feldes B_z im idealen Modell (3)) als auch der Koeffizient von σ_x (entsprechend B_x) kontrolliert werden kann. Mit diesen beiden „Knöpfen" können wir nun alle Einzelbit-Operationen wie oben beschrieben separat durchführen sowie im Ruhezustand zwischen Operationen $B = 0$ setzen und so jede weitere Zeitentwicklung abschalten.

Bei L Qubits brauchen wir entsprechend L Kontrollspannungen und L Kontrollströme. Wir erreichen damit aber, dass wir jedes Qubit einzeln ansprechen können, was für Spins im Magnetfeld kaum möglich ist. Zur Kopplung der Qubits verbinden wir sie parallel mit einer gemeinsamen Induktivität (Abbildung 5). Die Schwingungen in dem so entstandenen LC-Oszillator koppeln die Qubits. Bei geeigneter Wahl der Parameter sind die Kopplungen von der Form wie im idealen Modell (3), wobei die Kopplungsenergie zweier Spins durch

$$J^{ij} = \frac{E_J(\Phi^i)\,E_J(\Phi^j)}{E_L}, \qquad (12)$$

gegeben ist und $E_L \propto (C_J/C)^2\,\Phi_0^2/L$. Durch die Erweiterung auf die SQUIDs haben wir erreicht, dass auch die Zweibit-Kopplung kontrolliert werden kann. Sie wirkt nur dann, wenn für zwei Qubits die Josephson-Kopplung gleichzeitig eingeschaltet ist.

Phasenkohärenz

Die externen Spannungsquellen sind über Zuleitungen mit einem effektiven Widerstand R an die Qubits angekoppelt. Die damit verbundenen Johnson-Nyquist-Spannungsschwankungen zerstören die Phasenkohärenz und beenden damit die für den Quantencomputer so wesentliche kohärente Zeitenwicklung. Die Stärke der Fluktuationen kann aber durch Wahl geeigneter Systemparameter in gewissem Maße kontrolliert werden.

Bei tiefen Temperaturen ist die Phasenkohärenzzeit [6, 7, 22]

$$\tau_\varphi \approx \frac{R_K}{R}\left(\frac{C_J}{C}\right)^2 \frac{\hbar}{E_J}. \qquad (13)$$

Sie ist durch das Verhältnis zwischen dem Quantenwiderstand, Von-Klitzing-Konstante $R_K = h/e^2 \approx 25{,}8\ \mathrm{k\Omega}$, und dem klein zu wählenden Widerstand der Zuleitungen R bestimmt. Weiterhin hilft die kleine Gatterkapazität C, das Qubit von der Umgebung abzukoppeln. Da die Zeitskala für die typischen Einbit-Operationen von der Ordnung $\tau_{op} \sim \hbar/E_J$ ist, lassen sich für realistische Parameter eine vergleichsweise große Zahl von $\tau_\varphi/\tau_{op} \geq 10^4$ Rechenoperationen kohärent durchführen. Eine ähnlich günstige Abschätzung gilt für die Fluktuationen durch die Ströme in den Induktionsschleifen, die an die SQUIDs koppeln.

Der Messprozess

Auch der schnellste Computer ist nutzlos, wenn es nicht gelingt, die Information, die er erzeugt, auszulesen. Beim Quantencomputer entspricht dies einem quantenmechanischen Messprozess. Zum Auslesen des Zustandes eines Qubits koppeln wir einen Einzelelektronen-Transistor (Single Electron Transistor, SET) kapazitiv an das Qubit (Abbildung 6). Zur Beschreibung des Messprozesses ist es nötig, sich die zeitliche Entwicklung des gekoppelten Systems zu betrachten [15]. Man findet, dass, so lange die Transportspannung V_{tr} ausgeschaltet bleibt, der Transistor wie eine ideale Kapazität wirkt, also die kohärente Phasenentwicklung nicht stört.

Dies ändert sich schlagartig, wenn die Transportspannung eingeschaltet wird und im Transistor ein dissipativer Tunnelstrom fließt. Dann wird innerhalb sehr kurzer Zeit die Phasenkohärenz zerstört. Die Messgröße, die die Information über den Zustand des Qubits enthält, ist der Strom durch den Transistor, oder die Zahl der Elektronen m, die durch den Transistor geflossen sind (und beispielsweise eine Referenzkapazität aufgeladen ha-

ben). Bei einer Superposition von zwei Zuständen misst man den einen oder anderen Wert entsprechend einer gewissen Wahrscheinlichkeitsverteilung (Abbildung 7). Aufgrund des Schrotrauschens dauert es allerdings einige Zeit, bis die zwei Maxima der Verteilung, die den beiden Zuständen des Qubits entsprechen, getrennt sichtbar werden. Nach noch längeren Zeiten zerstört der Einfluss des Messgerätes auf das Qubit die Information über dessen Zustand, und man findet wieder nur ein Maximum.

Qubit-Design

Die hier diskutierten Systeme können mit moderner Technologie hergestellt werden. Dies soll jetzt durch ein Zahlenbeispiel quantitativ veranschaulicht werden. Für das Qubit wählen wir Tunnelkontakte mit Kapazität $C_J = 4 \cdot 10^{-16}$ F. Die Gatterkapazität wird kleiner gewählt mit $C = 2 \cdot 10^{-18}$ F, um so die Kopplung an die Umgebung schwach zu halten. Die Ladungsenergie des Qubits (in Temperatureinheiten nach Division durch k_B) ist dann $E_C \approx 2\,\mathrm{K}$. Die supraleitende Energielücke muss größer sein, um das Tunneln von Quasiteilchen zu unterdrücken. Eine geeignete Josephson-Kopplungsenergie ist $E_J = 100\,\mathrm{mK}$. Damit liegt die Arbeitstemperatur im Bereich von $T = 50\,\mathrm{mK}$, was nicht unrealistisch niedrig ist. Die Zeitdauer von Einbit-Operationen ist damit $\tau_{op} = \hbar/E_J \approx 7 \cdot 10^{-11}$ s. Die Phasenkohärenzzeit ist durch den Widerstand der Zuleitungen begrenzt. Für $R = 50\,\Omega$ haben wir also Zeit für $\tau_\varphi/\tau_{op} \approx 8 \cdot 10^5$ kohärente Einbit-Operationen. Die Dauer der Zweibit-Operationen ist auch durch die Induktivität bestimmt. Für $L = 3\,\mu\mathrm{H}$ gilt $\tau_\varphi/\tau_{2bit} = 650$. Mit der Induktivität können wir 10 bis 100 Qubits koppeln.

Die Fabrikation von Josephson-Qubits gemäß dieser Spezifikationen ist also mit existierender Nanotechnologie möglich. In der Tat wurden auch schon in Experimenten ihre quantenmechanischen Eigenschaften, so wie sie aus dem Hamilton-Operator (11) folgen, nachgewiesen. Die Forschergruppe in Saclay in Frankreich [16] demonstrierte an der Probe von Abbildung 1, dass der Grundzustand eine von der Gatterspannung abhängige Superposition $|\psi_0(V_x)\rangle = a(V)\,|\uparrow\rangle + b(V)\,|\downarrow\rangle$ von verschiedenen Ladungszuständen ist. Dazu veränderten sie die Gatterspannung kontinuierlich und zeigten, dass der Erwartungswert der Ladung $\langle Q\rangle = 2e\,[|a(V)|^2\,n + |b(V)|^2\,(n+1)]$ sich entsprechend kontinuierlich verändert. Die Forscher bei NEC in Tsukuba in Japan [17] wiesen mit Spektroskopie nach, dass das Anregungsspektrum dem des Hamilton-Operators (11) entspricht.

Zur Zeit besteht das technische Problem – neben der Erhaltung der Phasenkohärenz – darin, die nanoskaligen Systeme innerhalb sehr kurzer Zeiten auf der Skala von τ_{op} zu schalten. Insofern stellt das Experiment von Nakamura und Mitarbeitern [18] einen Durchbruch dar, die an einem Josephson-Qubit auch kohäherente Oszillationen beobachteten. Dies ist das erste erfolgreiche Experiment dieser Art an einem kontrolliert hergestellten Festkörpersystem. In dem Experiment wurde durch Kontrolle der Gatterspannung ein Josephson-Qubit in eine Superposition von Grund- und angeregtem Zustand (ψ_0 und ψ_1) gebracht, die sich dann mit verschiedenen Frequenzen entsprechend der Energie von Grund- und angeregtem Zustand (E_0 und E_1) entwickeln, $|\psi(t)\rangle = a\,\exp(-iE_0 t/\hbar)\,|\psi_0\rangle + b\,\exp(-iE_1 t/\hbar)\,|\psi_1\rangle$. Die sich daraus ergebenden Oszillationen der Ladung mit einer Frequenz, die der Energiedifferenz der beiden Zustände entspricht, $\hbar\omega = E_1 - E_0$, wurde zeitaufgelöst nachgewiesen, indem der Strom zu einer Probe gemessen wurde. Das Ergebnis zeigt Abbildung 8. Man erkennt die Periode der Oszillationen von ungefähr 50 ps. Aus der Abklingdauer kann die Phasenkohärenzzeit von $\tau_\varphi = 2$ ns abgeschätzt werden. Die wichtigste Quelle der Dekohärenz im vorliegenden Experiment ist die einfache Messprobe. Verbesserungen an dieser Stelle sollten τ_φ deutlich verlängern.

Als nächstes Ziel sollten nun an gekoppelten Qubits durch Zweibit-Operationen verschränkte Zustände erzeugt und nachgewiesen werden. Damit wären die fundamentalen Experimente zum Nachweis der quantenmechanischen Gesetze (etwa der Bellschen Ungleichungen), die zum Teil schon in der Quantenoptik demonstriert wurden, nun auch mit kontrolliert hergestellten Festkörpersystemen möglich.

Eine Phasenkohärenzzeit, wie wir sie für Josephson-Systeme finden, sollte ausreichen, um eine recht große Zahl der benötigten Manipulationen kohärent durchführen zu können. Für die interessanten Algorithmen werden aber noch weit mehr Operationen benötigt. Eine wichtige Entwicklung der letzten Jahre sind die „Error-correcting codes" [23], mit deren Hilfe auftretende Fehler, sofern sie nicht zu häufig sind, wieder korrigiert werden können.

Wenn auch die Verwendung der verschiedenen Quanteninformationssysteme als Quantencomputer noch in ferner Zukunft liegt, kann man doch erwarten, dass die Entwicklung der Technologien mit denen Festkörpersysteme quantenmechanisch kohärent manipuliert werden können – das Quantum State Engineering, dessen Anfänge wir gerade erleben – weitere bisher ungeahnte technische Möglichkeiten eröffnen wird.

Literatur

[1] S. Lloyd, *Science* 261, 1589 (1993); C. H. Bennett, *Physics Today* **48** (10), 24 (1995); D. P. DiVincenzo, *Science* **269**, 255 (1995); A. Barenco, *Contemp. Phys.* **37**, 375 (1996); A. M. Steane, *Reports on Progress in Physics* **61**, 117 (1998).

[2] C. P. Williams and S. H. Clearwater, *Explorations in Quantum Computation*, Springer-Verlag (1998).

[3] Verschiedene Artikel in *Fortschritte der Physik* 46 (1998).

[4] Siehe z. B. H.-J. Briegel, I. Cirac and P. Zoller, Physikalische Blätter **55**, 37 (1999).

[5] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, IEEE Press, Los Alamitos, CA 1994, pp. 124–134.

[6] A. Shnirman, G. Schön, and Z. Hermon, Phys. Rev. Lett. **79**, 2371 (1997).

[7] Yu. Makhlin, G. Schön, and A. Shnirman, *Nature* 398, 305 (1999).

[8] J. E. Mooij, T. P. Orlando, L. Levitov, L. Tian, C. H. van der Waal, and S. Lloyd, Science **285**, 1036 (1999).

[9] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).

[10] B. E. King et al., Phys. Rev. Lett. **81**, 1525 (1998); Q. A. Turchette et al., ibid. **81**, 3631 (1998).

[11] I. L. Chuang, N. A. Gershenfeld, and M. Kubinec, Phys. Rev. Lett. **80**, 3408 (1998); N. A. Gershenfeld and I. L. Chuang, Spektr. d. Wissenschaft **8**, 54 (1998).

[12] D. G. Cory et al., Phys. Rev. Lett. **81**, 2152 (1998).

[13] Q. A. Turchette et al., Phys. Rev. Lett. **75**, 4710 (1995); E. Hagley et al., Phys. Rev. Lett. **79**, 1 (1997).

[14] D. Loss and D. P. DiVincenzo, Phys. Rev. A **57**, 120 (1998); B. E. Kane, Nature **393**, 133 (1998).

[15] A. Shnirman and G. Schön, Phys. Rev. B **57**, 15400 (1998); G. Schön, A. Shnirman, and Yu. Makhlin, cond-mat/9811029.

[16] V. Bouchiat, D. Vion, P. Joyez, D. Esteve, and M. H. Devoret, Physica Scripta **T76**, 165 (1998).

[17] Y. Nakamura, C. D. Chen, and J. S. Tsai, Phys. Rev. Lett. **79**, 2328 (1997).

[18] Y. Nakamura, Yu. A. Pashkin, and J. S. Tsai, *Nature* 398, 786 (1999).

[19] A. Barenco et al., Phys. Rev. *A* **52**, 3457 (1995).

[20] D. Coppersmith, IBM Research Report No. RC19642 (1994). Siehe auch T. Beth, *Verfahren der schnellen Fourier-Transformation*, Verlag Teubner (1984).

[21] V. Vedral, A. Barenco, and A. Ekert, Phys. Rev. A **54**, 147 (1996).

[22] A. J. Leggett et al., Rev. Mod. Phys. 59, 1 (1987); U. Weiss, *Quantum dissipative systems*. World Scientific, Singapore, 1993.

[23] P. W. Shor, Phys. Rev. **A 52**, 2493 (1995); D. P. DiVincenzo, Proc. R. Soc. London A (1996) (quant-ph/9705009); T. Beth and M. Grassl, in Ref. [3] und weitere Referenzen darin.

Die Autoren:

Gerd Schön, geb. 1948, Physikstudium an den Universitäten Karlsruhe und Dortmund (Diplom 1972) und der Stanford University. 1996 Promotion über ein Thema der Nichtgleichgewichtssupraleitung. Es folgen Assistententätigkeit in Karlsruhe und Forschungsaufenthalte am FZ Jülich, der Cornell University, UC Berkeley und UC Santa Barbara. Von 1986–1991 Professor an der TU Delft. Seither Professor an der Universität Karlsruhe. Aktuelle Forschungsaktivitäten im Bereich des Elektronentransports und Supraleitung in Nanostrukturen.

Yuriy Makhlin, geb. 1969. Physikstudium in Moskau. 1995 Promotion am Landau-Institut für Theoretische Physik über superfluides ^{3}He. 1996/97 Post-doc an der University of Illinois at Urbana-Champaign. Seit 1997 als Alexander-von-Humboldt-Stipendiat und Assistent an der Universität Karlsruhe. Aktuelle Forschungsaktivitäten im Bereich der Quantencomputer und Josephson-Netzwerke.

Anschrift:

Institut für Theoretische Festkörperphysik, Universität Karlsruhe, 76128 Karlsruhe.