

Episode 1

HINTERGRUNDWISSEN QUANTENCOMPUTING

VERSCHRÄNKUNG

Qubizz | Wissen

Wie sich das Phänomen der Verschränkung für das Quantencomputing nutzen lässt.

Anders als klassische Computer nutzen Quantencomputer keine Transistor-basierten Chips zur Informationsverarbeitung, sondern Quantensysteme. Oder anders ausgedrückt: Die Rechenpower wird auf Basis der kleinsten Teilchen, wie etwa Photonen, Ionen oder Elektronen erzeugt. Bei der Programmierung solcher Rechner werden physikalische Phänomene der Quantenwelt ausgenutzt. In dem folgenden Artikel wollen wir den Effekt der Verschränkung genauer betrachten.

Um das Phänomen der Verschränkung etwas genauer zu beleuchten, machen wir uns zunächst nochmals mit der grundlegenden Funktionsweise eines Quantencomputers vertraut: Damit ein Quantenrechner arbeiten kann, benötigt er, genau wie herkömmliche Rechner auch, eine Informationseinheit. Im klassischen Fall wird diese Informationseinheit als Bit bezeichnet und ist die kleinstmögliche Unterscheidung, die ein digitaltechnisches System treffen kann. Es besitzt entweder den Zustand 0 („Strom aus“) oder 1 („Strom an“).

Quantencomputer arbeiten jedoch auf Basis von sogenannten Qubits. Als eine Art abstraktes Konstrukt machen sie es möglich, quantenmechanisch ein Bit zu kodieren. Darüber hinaus verfügen Qubits über besonders bemerkenswerte Eigenschaf-

ten, denn sie können „zeitgleich“ in mehreren Zuständen existieren. Man spricht dabei vom Superpositionsprinzip. (Wir werden das Thema Superposition in Kürze in einer eigenen Qubizz-Episode ausführlich behandeln). Das bedeutet, dass sie nicht nur in den „reinen“ Zuständen 0 und 1, sondern

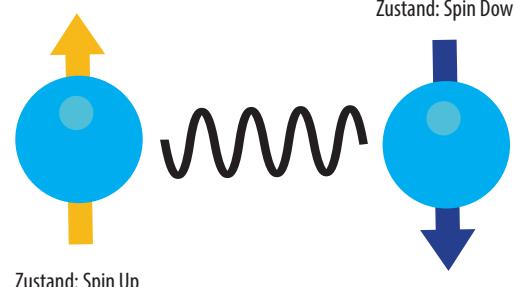


Abbildung: Zwei paarweise verschränkte Quanten.

Wird der Spin eines Teilchens beeinflusst (z.B. durch eine Messung), passt sich dadurch auch instantan der Spin des anderen Teilchens an. Das gilt auch dann, wenn die beiden Teilchen weit voneinander entfernt sind. Die Verschränkung kann auch zwischen mehreren Teilchen erfolgen.

auch in einer Überlagerung dieser vorliegen können. Solch unterschiedliche Überlagerungszustände lassen sich vereinfacht als verschiedene Wahrscheinlichkeiten für die Zustände 0 oder 1 interpretieren.

Ohne an dieser Stelle zu tief ins Detail zu gehen, lassen sich die Zustände 0 und 1 beispielsweise als Spin eines Elektrons betrachten. Der Spin kann als klassische Analogie ähnlich einer Art Rotationsbewegung von quantenmechanischen Teilchen betrachtet werden. Bei Elektronen hat dieser Spin zwei Ausprägungen: „Spin down“ (Zustand 0) und „Spin up“ (Zustand 1). Solange der Spin des Elektrons nicht gemessen wurde, liegt er jedoch in einer Überlagerung der beiden „reinen“ Zustände vor. Solch eine „Superposition“ ist ein neuer Zustand, der sich physikalisch auch anders verhält als die einzelnen reinen Zustände. Zugegeben: Mit unserer Alltags erfahrung ist dieses Phänomen nur schwer zu erfassen. Quantencomputer machen sich diese Effekte jedoch zu Nutze und beziehen sie in ihre Rechenoperationen mit ein. Kommt jetzt mit der sogenannten Verschränkung noch ein weiteres Quantenphänomen ins Spiel, offenbart sich das immense Potential eines Quantencomputers.

Die Quantenverschränkung

Bei der Verschränkung werden einzelne quantenmechanische Teilchen zu einem Quantensystem zusammengeführt. Das bedeutet, sie sind dann wechselseitig miteinander verbun-

den und müssen als ein einziges, untrennbares System betrachtet werden. Wird nun der Zustand eines Qubit verändert, beeinflusst dies immer auch alle anderen Qubits, welche mit diesem verschärkt wurden. Dies geschieht unmittelbar und unabhängig von der Entfernung der verschärkten Teilchen zueinander – als ob sie durch eine unsichtbare Kraft miteinander verbunden wären.

Albert Einstein bezeichnete dieses Phänomen deshalb auch als „spukhafte Fernwirkung“. Die Tatsache, dass zwei räumlich voneinander getrennte Teilchen Informationen über ihre Eigenschaften, scheinbar instantan und ohne ein messbares Signal austauschen können, widerspricht allen Gesetzen der klassischen Physik.

Also doch Hexerei? Sicher nicht. Vielmehr beruht das Phänomen auf der intrinsischen Beschreibung von Quantensystemen über eine Wellenfunktion, was eine anschauliche Erklärung kaum möglich macht. Die Effekte sind jedoch messbar und lassen sich in der Praxis auch ohne Zauberstab reproduzieren. So ist die Quantenverschränkung ein elementares Grundkonzept, um universelles Quantencomputing zu ermöglichen. Denn nur durch Verschränkung können überhaupt alle möglichen Zustände eines Quantencomputers mit mehreren Qubits gezielt erreicht und beeinflusst werden. Diese Tatsache macht das Rechnen mit Quantenalgorithmen möglich. Durch Ausnutzung von Verschränkung und Superposition können solche Algorithmen genutzt werden, um bestimmte Proble-

Informationsübertragung in Überlichtgeschwindigkeit?

Durch die instantane Beeinflussung verschärkter Teilchen untereinander, liegt es nahe, dass das Phänomen der Verschränkung auch zur Übertragung von Informationen in Überlichtgeschwindigkeit genutzt werden könnte. Dies ist leider ein Trugschluss. Denn auf der Quantenebene bedeutet dies, dass selbst wenn Partei A ihr Teilchen durch eine Messung „beeinflusst“ hat, Partei B keine Kenntnis davon besitzt, wenn sie ihr Teilchen misst. Nur durch den klassischen Austausch von Informationen können sich beide Parteien darüber im Klaren sein, wer wann das eigene Teilchen beeinflusst hat. Auf den ersten intergalaktischen Instant Messenger Dienst müssen wir also noch etwas warten.

me exponentiell schneller lösen zu können, als alle bekannten klassischen Algorithmen. Denn Quantenalgorithmen sehen oftmals vor, dass alle möglichen Zustände sich gegenseitig beeinflussen können und die Wahrscheinlichkeit der „richtigen“ Lösung maximiert wird. Stark vereinfacht gesagt bedeutet das, dass ein Quantencomputer demnach so programmiert

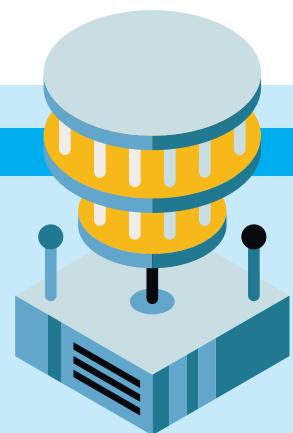
werden kann, dass er nahezu simultan alle möglichen Lösungswege „testet“. Dies hat gerade bei kombinatorisch anspruchsvollen „Multi-Dimensions-Aufgaben“ hohe Relevanz. Also immer dann, wenn für die Lösung eines Problems viele verschiedene Möglichkeiten in Betracht gezogen werden müssen. Ohne die Nutzung der Quantenverschränkung wäre das kaum möglich.



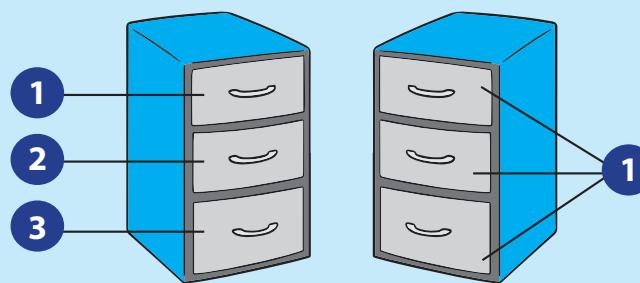
Auf Lösungssuche

So unterscheidet sich die Arbeitsweise eines Quantencomputers von einem klassischen Computer

In diesem Beispiel ist die gesuchte Lösung sinnbildlich in einer der Schubladen versteckt.



Ein herkömmlicher Rechner rechnet sequentiell – also Schritt für Schritt. Um die versteckte Lösung zu finden, würde er zunächst Schublade 1 durchsuchen. Im Anschluß dann Schublade 2 und daran anschließend Schublade 3. Durch die Erhöhung der Rechenpower (zum Beispiel durch den Zusammenschluss mehrerer Rechner) lässt sich dieser Prozess zwar parallelisieren, aber schlechter skalieren als bei einem Quantencomputer. Denn für die Verdopplung der Rechenpower wären demnach immer eine Verdopplung der Rechner erforderlich.



Ein Quantenrechner würde alle Schubladen zum gleichen Zeitpunkt öffnen und gleichzeitig den Inhalt durchsuchen. Die Wahrscheinlichkeit für die Ausgabe der richtigen Schublade wird durch einen Quantenalgorithmus maximiert. Entsprechend der Aufgabenstellung lässt sich die Rechenpower verhältnismäig einfach erhöhen. Zur Verdopplung der Rechenpower genügt es, ein weiteres Qubit hinzuzufügen.