

---

# Ausgewählte Kuriositäten der Quanteninformation

Von Albert Einstein bis Wigners Freund: ein kleines Glossar zur Reportage «Die Physiker».

Von [Anja Konzett](#) und Dr. Paul Erker, 07.09.2019

Um den Haupttext «[Die Physiker](#)» noch besser zu verstehen und um ihn nicht mit Informationen zu überhäufen, haben wir die Erklärung einiger Begriffe in dieses Glossar ausgelagert. Wobei «einiger» eine schwere Unter-treibung ist. Und Tausende mehr wären möglich. Aber dann wäre dieser Artikel in frühestens einem Jahr fertig; wahrscheinlicher aber erst in tausend Jahren. Also nutzen Sie dieses Glossar als erste Inspiration, als Einstieg und forschen Sie weiter – als Starthilfe finden Sie am Ende ☒ [neun Lesetipps](#).

## ... and everything goes to shit

Die letzte Konsequenz des zweiten Hauptsatzes der Thermodynamik in einer nicht ☒ [superdeterministischen](#) Welt.

## Anthropomorphismus

Zusammengesetzt aus dem Griechischen *anthropos* für Mensch und *morphe* für Gestalt. Beschreibt im Kontext dieses *brainfucks* namens Quantenphysik einen seiner liebsten und intuitivsten Aspekte – das angewandte Bedürfnis nach Vermenschlichung dessen, das weit jenseits der menschlichen Wahrnehmung liegt. Das heisst: Die Quantenphysiker sprechen über abstrakte Systeme gern so, als wären es selbstbewusste Lebewesen. Etwa: «Dann entscheidet sich das Teilchen ...». Oder: «Das Photon isch än geile Siech ...» Oder: «Ui, diä Teili hend sich grad härt disst!»

## Bell, John Stewart

Geboren 1928 in Belfast, gestorben 1990 in Genf. Physiker, der trotz bahnbrechender Erkenntnisse nie einen Nobelpreis erhielt. Unter der Woche war er Quanteningenieur – unter anderem am Cern, wo er ☒ [Reinhold Bertlmann](#) traf. Am Wochenende hatte er Prinzipien. Mit seiner Freizeitbeschäftigung verhalf er der Quantenphysik zu einem neuen goldenen Zeitalter, seit dessen Beginn Physiker sich wieder Gedanken über fundamentale (philosophische) Probleme machen und diese teilweise sogar in Experimenten testen können.

## Benasque

Benasque wird in der Gemeinschaft der Quanteninformation als Synonym für die Konferenz verwendet, die dort stattfindet. Es finden zwar jährlich mehrere Konferenzen im Bereich der Quantenphysik statt, aber keine hat die Bedeutung der beschriebenen, weshalb Benasque hier auch als Synonym für diese spezifische Konferenz verwendet wird.

## Bertlmann, Reinhold

Geboren 1945 in Reutte (Tirol), Lehrer und Physiker, bei Schülern wie Kollegen ausserordentlich beliebt. Arbeitete fürs Cern und ist nun Professor für Physik an der Universität Wien im Ruhestand. Held der Sowjetunion, der noch nie mit einem Paar gleicher Socken gesehen wurde – was ihm unter anderem weltweite Berühmtheit verschaffte.

☒ John S. Bell, der sich einst metaphysisch mit ☒ Einstein anlegte und gewann (☒ EPR), schrieb zu Ehren des eigentümlichen Kleidungsstils seines Kollegen einen Aufsatz. Anhand von «Bertlmanns Socken» philosophiert Bell über die Natur der Realität und veranschaulicht damit den Unterschied zwischen klassischen und ☒ Quantenkorrelationen. Die Abhandlung ist nicht formelfrei, daher für Laien nur schwer bekömmlich, aber das soll kein Hindernis sein.

## Bohmianer

Es passiert, was passiert. Bohmianer klingt nach ausserirdischen Bobos (in Wien beliebtes Schimpfwort, das Boheme und Bourgeoisie kombiniert, *Oida!*), sind sie aber nicht. Bevor wir dazu kommen, zuerst ein wenig Geschichte: die bohmsche Mechanik beziehungsweise die De-Broglie-Bohm-Theorie. Diese basiert einerseits auf den Ideen von Louis de Broglie, die damals jedoch verworfen wurden. In den 1950er-Jahren entwickelte David Bohm, ohne Kenntnis von de Broglies Ideen, den gleichen Formalismus. Bedeutend ist dieser Formalismus, da er eine Beschreibung der Quantenphysik ermöglicht, in der Messwerte schon vor der Messung bestehen. Dies funktioniert dadurch, dass eine Pilotwelle oder auch das Quantenpotenzial eingeführt werden, diese kann sich instantan (unendlich schnell) über beliebige Distanzen ändern und sorgt dafür, dass passiert, was passiert. Auch hier kann Information nicht überlichtgeschwindigkeitsschnell (superluminal) übertragen werden, denn das Quantenpotenzial ist uns prinzipiell nicht zugänglich. Es kann nur im Nachhinein, basierend auf dem, was passiert ist, nachvollzogen werden, wie sich diese Pilotwelle verhalten hat.

☒ John S. Bell wurde von der bohmschen Mechanik zu seiner Arbeit inspiriert und war auch derjenige, der sie in der Welt bekannt machte. Für viele Quantenphysiker ist dieser Formalismus zu kompliziert und ausschweifend, das heisst zu wenig praktikabel, um mit ihm zu arbeiten.

Die Anhänger dieser superdeterministischen Interpretation der Quantenphysik sind für ihren harten bis harschen Diskussionsstil berüchtigt. Innerhalb der Quanteninformationsgemeinschaft geniesst dieses Grüppchen einen, sagen wir mal, sehr eigenen Ruf.

## Bohr, Niels

Geboren 1885 in Kopenhagen, gestorben 1962 ebenda, einer der Urväter der Quantenphysik, Nobelpreisträger für Physik des Jahres 1922, Namensgeber des Elements Bohrium sowie eines Mondkraters; beteiligt an der Gründung des Cern; kämpfte im dänischen Widerstand gegen die Nazis und sein Leben lang energisch dagegen, dass seine bahnbrechenden Entdeckungen im Bereich der Atomphysik (bohresches Atommodell) entgegen dem Wohl der Menschheit gebraucht werden. Mehr oder weniger erfolgreich.

## Church of the Larger Hilbert Space

Alle Zustände können rein sein, wenn der Zustandsraum (Hilbertraum) gross genug gemacht wird. John Smolin prägte diesen Begriff, er steht für den Erweiterungsansatz mithilfe des Stinespring-Theorems, eines der mächtigsten und nützlichsten Werkzeuge in der Quanteninformationstheorie. Manche harten Kirchgänger verwenden das Theorem nicht als mathematisches Werkzeug, sondern normativ, was für Konflikte sorgen kann.

## Cluster(ing)

In der Physik: ☒ mesoskopische Ansammlung von Atomen oder Molekülen. Wird auch in der Chemie, Biologie und der Informatik verwendet, bezeichnet dort aber andere Dinge. Im Lauftext bezieht sich der Begriff auf eine Ansammlung von Ähnlichkeiten.

## Einstein, Albert

Hoffentlich der überflüssigste Glossareintrag aller Zeiten, *but here we go*: geboren 1879 in Ulm, gestorben 1955 in Princeton, Nobelpreisträger des Jahres 1921. Physikgott, der hin und wieder auch mal falsch lag (☒ EPR-Paradoxon). Projektionsfläche zur Bestätigung wissenschaftlicher Minderwertigkeitskomplexe schlechthin und heutzutage vor allem eins: ultimative Popikone.

## EPR-Paradoxon

Ein Gedankenexperiment von ☒ Einstein, Boris Podolsky und Nathan Rosen, mit dem zu beweisen versucht wurde, dass die Quantenphysik unvollständig ist. Seine jetzige Relevanz gewann diese Arbeit erst durch die Arbeit von ☒ John S. Bell, die das Paradoxon auflöste, die Arbeit von Einstein und Co. damit berichtigte – und sie ironischerweise erst wichtig machte. Dies zeigt sich auch anhand der Verweise auf diesen Artikel: Bis 1980 verwiesen nur 34 Arbeiten auf EPR, doch diese Zahl explodierte in den darauffolgenden Jahrzehnten, sodass 2003 schon 456 Arbeiten Bezug darauf nahmen. Heute sind es mehr als 5000. Mittlerweile so unvorstellbar wie die Quantenphänomene selbst: ein Artikel zur Verschränkung ohne Verweis auf den zu EPR (☒ Verschränkung). Also, *here we go again*.

## Feyerabend, Paul

Geboren 1924 in Wien, gestorben 1994 in Genolier VD. Feyerabend war ein kriegsversehrter und darum nicht schwanzgesteuerter Philosophieprofessor, vermutlich auch deshalb ein so guter Denker. Lässt Popper alt aussehen und füllte an der ETH Zürich Hörsäle, in einer Zeit, als diese

noch einen kulturellen Anspruch verfolgte. Er zeigte mittels eines Ad-absurdum-Beweises, dass es nur eine sinnvolle Schlussfolgerung auf der Suche nach einer einzigen Methode gibt, die immerwährenden Fortschritt bringt. Nämlich: «*Anything goes*», «alles geht». Oft falsch verstanden als Aufruf zum absoluten Relativismus, brachte es ihm den Ruf des wissenschaftsphilosophischen Anarchisten ein. Dabei hat er nur drauf hingewiesen, dass jede feste Methode ihre Grenzen hat.

## **Feynman, Richard**

Geboren 1918 in Queens NY, gestorben 1988 in Los Angeles, Nobelpreisträger der Physik im Jahr 1965. Dachte als einer der Ersten über den Zusammenhang zwischen Physik und Komputation nach. Bongotrommler, Atombombenbauer und Lebemensch – der Oscar Wilde der Quantenphysik und als solcher Urheber unzähliger Zitate und Aphorismen, die man teilweise getrost ignorieren, aber nur schlecht vergessen kann.

## **Freiheitsgrad**

Streng mechanisch genommen, bezeichnet dies die Bewegungsmöglichkeiten, die ein System hat. Hier steht es allgemein für (innere und äussere) Parameter, die unabhängig voneinander variieren können. Freiheitsgrade eines Quantensystems können unter anderem der Ort, der Impuls, der Spin oder der Bahndrehimpuls sein.

## **Glauber, Roy J.**

Geboren 1925 in New York, gestorben 2018 in Newton (Massachusetts), Nobelpreisträger für Physik des Jahres 2005, war erst 18 Jahre alt, als er für das Manhattan-Projekt rekrutiert wurde – und 20, als die Bomben, die er mitbaute, über Hiroshima und Nagasaki niedergingen. Im Dokumentarfilm, der anlässlich seines Besuchs in Benasque im Jahr 2017 entstand, stellt er sich die Frage, was geschehen wäre, wenn die Bombe vor dem Untergang des Dritten Reichs fertig geworden wäre. Wäre sie über Europa niedergegangen? «Wahrscheinlich.»

## **Heisenberg, Werner**

Geboren 1901 in Würzburg, gestorben 1976 in München, einer der Urväter der Quantenphysik, Nobelpreisträger für Physik des Jahres 1932, war der einzige grosse Quantenphysiker der ersten Hälfte des letzten Jahrhunderts, der sich nicht gegen Nazideutschland stellte, sondern ihm die Treue hielt. Dies, obwohl die Nazis Heisenbergs Quantenphysik als «Judenphysik» verdammt und der jüdischstämmige ☒ *Einstein* einer seiner engsten Freunde war. Heisenberg wurde von den Nazis zwar unentwegt angefeindet, aber wegen Bekanntschaften seiner Familie zu Heinrich Himmler geschont. Die Geschichtsschreibung war gnädig mit Heisenberg – statt als feiger Nazi-freund ist er heute vor allem als brutaler Drogenbaron bekannt. Der Grund dafür ist die TV-Serie «*Breaking Bad*», in der ein Chemielehrer an Krebs erkrankt und Crystal Meth kocht, um seine Behandlung zu bezahlen. Der Lehrer gibt sich den Strassennamen Heisenberg als Hommage an Heisenbergs ☒ *Unschärferelationen*.

## Heisenberg-Cut

Hypothetische Grenze zwischen der Quantenwelt und der klassischen Welt. Erhielt seinen Namen durch ☒ Werner Heisenberg, weil dieser lieber über eine Trennlinie als über einen ☒ Kollaps (☒ Measurement-Problem) philosophierte.

**Achtung:** *Hic sunt leones!* Ob die Grenze überhaupt existiert, ist so unmöglich wie möglich.

## Klassische Physik

Alles, was keine Quantenphysik braucht, um es zu beschreiben.

## Kollaps (der Wellenfunktion)

Prozess, in dem ein quantenmechanisches System sich für einen definitiven Zustand entscheidet (☒ Anthropomorphismus), also das Zustandekommen des Messwerts. Was das bedeutet oder wie es funktioniert, ist völlig unklar. Der Begriff stammt aus der Zeit der Entwicklung der Quantenphysik und wurde so schwammig formuliert, dass er sich perfekt zum Unter-den-Teppich-Kehren von Problemen eignet (☒ Measurement-Problem). Zentral für die ☒ Shut up and Calculate-Interpretation und vermutlich der Grund, warum sich der Kollapsbegriff bis heute gehalten hat. Zu ernst genommen (☒ Kollapsmodell), führt er zu sehr unphysikalischen Konsequenzen.

## Kollapsmodelle, objektive

Der Glaube, dass ☒ Kollaps einen (tatsächlichen) physikalischen Prozess beschreibt. Alle bisherigen Versuche, einen solchen Prozess zu beobachten, scheiterten. Ein solcher Prozess wird meistens durch eine Erweiterung der Schrödinger-Gleichung eingeführt. Solche Erweiterungen bringen jedoch oft unerwünschte Nebeneffekte mit sich. Konkret: Sollten die Anhänger des Kollapsmodells recht behalten, wäre ein Perpetuum mobile nicht mehr ausgeschlossen.

## Kontextualität

Phänomen in der Quantenphysik, das zeigt, dass die Ergebnisse einer Messung davon abhängen, welche Messungen noch vorgenommen werden (könnten). Dieses Phänomen steht im krassen Gegensatz zur ☒ klassischen Physik, die nicht kontextuell ist. Die meisten Quantenphysiker leiten von der Kontextualität den Schluss ab, dass Quantenmessung nicht einfach das Herausfinden schon bestehender Werte ist. Also eigentlich so ziemlich alle Quantenphysiker bis auf jene aus den weltanschaulichen Lagern der Superdeterministen (☒ Superdeterminismus, ☒ Many Worlds, ☒ Bohmianer).

## Laser

*Light Amplification by Stimulated Emission of Radiation*. Maschine, die kohärentes Licht produziert. Zufallsentdeckung. Heutzutage allgegenwärtig.

## Makroskopisch

Gross. In diesem Kontext: gross genug, um Teil der ☒ klassischen Welt zu sein.

## Many Worlds

Alles, was passieren kann, passiert. Vereinfacht: Wenn ein Auto in dieser Welt links abbiegt, biegt es in einer zweiten rechts ab, fährt in einer dritten geradeaus in ein Reh und löst so eine Kettenreaktion aus, die zum Untergang des dritten Universums führt. Many Worlds ist eine Möglichkeit für Menschen, die in der Kirche des grösseren Hilbertraums (☒ Church of the Larger Hilbert Space) zu Hause sind, dem Zustand des Universums Bedeutung beizumessen. Scheint bei Protestanten beliebter zu sein als bei Katholiken, schaffte es aus der Physik in die Popkultur und wieder zurück (siehe «Dark» auf Netflix oder die Kultserie «Rick and Morty»). Geht auf die Einführung eines Formalismus zur Beschreibung der Quantenphysik von Hugh Everett III. (1930–1982) zurück, Kettenraucher und Vater von «Eels»-Sänger Mark Oliver. ([Hier gelangen Sie zur Physiker-Playlist bei Spotify](#)).

Everetts Arbeit erfuhr erst 20 Jahre später Wertschätzung, als er sich längst frustriert von der Physik abgewandt hatte. Die Ursprünge der Interpretation anhand vieler Welten liegen aber nicht bei Everett selbst, der ist nur für mathematischen Formalismus verantwortlich, sondern sind eher bei [Bryce DeWitt](#) oder [David Deutsch](#) zu suchen.

## Measurement-Problem

Tritt schon bei ☒ Schrödingers berühmtem Büsi auf, dessen Skurrilität aus der Anwendung von quantenmechanischen Konzepten (☒ Superposition) auf ☒ makroskopische Objekte/Subjekte herrührt. Die grosse Frage, die wir hier besprechen wollen, ist jedoch nicht, ob das Büsi tot oder lebendig ist, sondern wie es zu dieser makroskopischen Welt kommt, in der wir leben. Ab wann verschwinden die seltsamen Phänomene der Quantenphysik, und ab wann hat wieder Gültigkeit, was wir im Alltag erfahren können (☒ Heisenberg-Cut)? Die Quantenphysik liefert darauf von sich aus keine Antwort. Einige winden sich aus dem Problem einfach damit heraus, indem sie die Quantenphysik auf alles anwenden, womit sich die Frage gar nicht mehr stellt (☒ Many Worlds, ☒ Bohmianer).

## Mesoskopisch

Nicht makroskopisch genug für die ☒ klassische Physik und nicht ☒ mikroskopisch genug für die der Quanten.

## Mikroskopisch

Hier: klein genug, um Teil der Quantenwelt zu sein.

## Moore's Law

Besagt, dass sich die Anzahl von ☒ Transistoren pro Flächeneinheit alle zwei Jahre verdoppelt. Bis jetzt empirisch zutreffend. Zeigt das exponentielle Wachstum der uns zur Verfügung stehenden Rechenleistung über den Verlauf der letzten Jahrzehnte.

Dieses Gesetz lässt sich nicht einfach auf  $\boxtimes$  Quantencomputer übertragen, da nicht klar ist, auf welche Grösse es sich beziehen sollte, ob dies nun die Anzahl der kontrollierbaren  $\boxtimes$  Qbits, die maximale Anzahl an applizierbaren Gattern oder die maximale Anzahl von Qbits ist, auf die ein Gatter anwendbar ist. Noch befindet sich die Industrie rund um den Bau eines Quantencomputers in den Kinderschuhen, die Beobachtung des Physikers und Chemikers Gordon Moore ist aber bedingt dadurch, dass es eine Industrie gibt und diese möglichst viele Bauteile auf einen Computerchip quetschen will und kann.

## No-Cloning

Theorem, in welchem bewiesen wurde, dass es unmöglich ist, einen beliebigen unbekanntem  $\boxtimes$  Quantenzustand perfekt zu reproduzieren. Das erlaubt uns nicht nur, grundlegende Aussagen über die Welt zu treffen und andere auszuschliessen, sondern hat noch dazu eine interessante Geschichte. Und ja, sie hat mit Hippies zu tun (siehe «How the Hippies Saved Physics»).

Einer der Proponenten der Fundamental Fysics Group, Nick Herbert, versuchte, seine theoretischen Überlegungen zur Konstruktion superluminaler Kommunikationsgeräte – das heisst zu Geräten, die schneller als Licht Information austauschen können – namens Flash in einer anerkannten Physikzeitschrift zu publizieren. Die Publikation des einen Artikels wurde von einem der Reviewer, Giancarlo Ghirardi, abgelehnt. Mit der für Ghirardi trivialen Überlegung, mit der er die Absage begründete, erbrachte er beiläufig einen Beweis für das No-Cloning-Theorem. Da die Berichte der Reviewer solcher Zeitschriften nicht öffentlich sind, wurde dieser erst Jahre später gefunden.

Die Hippies hatten sich zu dieser Zeit ein riesiges, die ganze USA und Teile der Welt umspannendes Verteilernetz für Informationen aufgebaut (siehe «How the Hippies Saved Physics»). Durch dieses landete eine Version des Flash-Artikels in den Händen der beiden damals jungen Physiker William Wootters und Wojciech Zurek. Diese fackelten nicht lange und publizierten einen Artikel mit dem unmissverständlichen Titel «A Single Quantum Cannot Be Cloned».

Etwa zur gleichen Zeit war Nick Herbert auf Europatournee und gab Vorträge über seine scheinbar revolutionäre Entdeckung. Einen dieser Vorträge hielt er in Amsterdam, wo er von Dennis Dieks gehört wurde. Dieser schenkte Herbert jedoch keinen Glauben und schrieb kurz darauf, unabhängig von Wootters und Zurek, einen Aufsatz, der das No-Cloning-Theorem ebenfalls behandelte.

Der Irrtum also, man könne Geräte bauen, die schneller als Licht kommunizieren, und seine Korrektur rückten den Fokus der Quantenphysik wieder auf fundamentale Überlegungen, die der Quanteninformation schliesslich mit den Weg bereiteten – *and that's how the hippies saved physics*.

## No-Signalling-Prinzip

Ein Theorem, das besagt, Informationen können sich nicht schneller als Licht ausbreiten. Aus ihm kann auch das  $\boxtimes$  No-Cloning-Theorem abgeleitet werden. Es beschränkt die mögliche Stärke von Korrelationen ( $\boxtimes$  Quantenkorrelationen). Es macht Korrelationen, die teilweise stärker sind als in der Quantenwelt, eigentlich möglich. Zumindest theoretisch. Bis jetzt haben wir noch keinen Hinweis in der Natur gefunden, dass solche Korre-

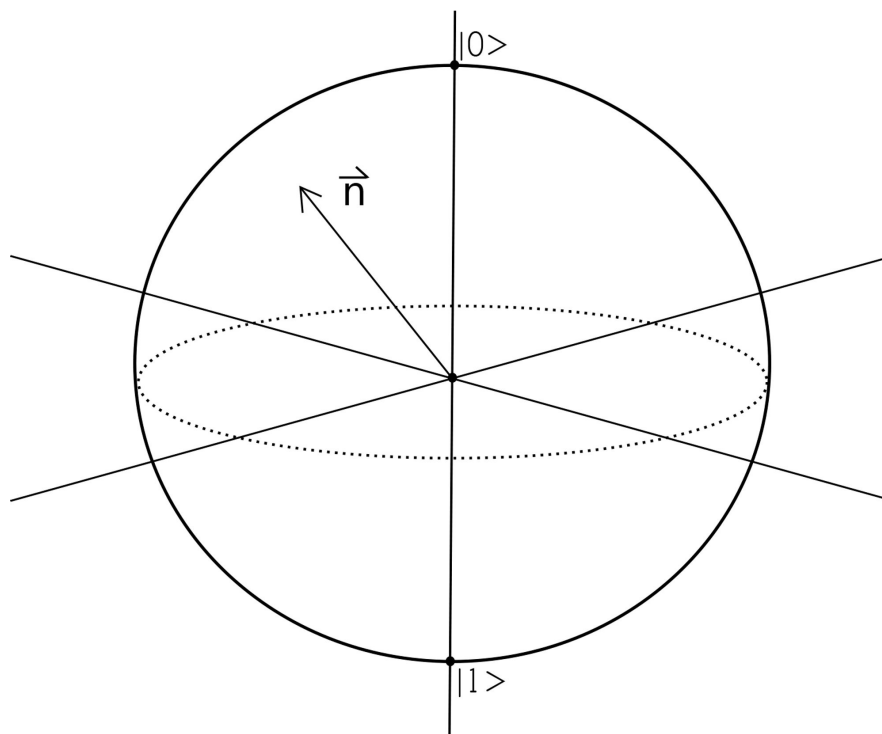
lationen existieren. Würden sie aber vorkommen, könnte man mit ihnen das im Eintrag Quantenkorrelationen beschriebene Spiel immer gewinnen, also mit 100 Prozent. Da die mathematische Handhabung dieser Stärker-als-Quanten-Korrelationen oder Supraquantenkorrelationen leichter ist als die der Quantenkorrelationen selbst, wird beim Beweis der Sicherheit der  $\boxtimes$  Quantenkryptografie eine Spionin angenommen, die mehr Macht besitzt, als die Quantenphysik erlaubt. (Diese Spionin heisst in der Quanteninformatik übrigens immer Eve, in Anlehnung an das englische Wort für «lauschen»: *to eavesdrop*.) Die Spionin Eve wird beim Nachweisen der Sicherheit als so mächtig angenommen, dass sie alles machen kann, was Supraquantenkorrelationen erlauben. Das heisst, dass in dieser Art überprüfte Quantenkryptografie selbst dann noch sicher ist, wenn eines Tages Supraquantenkorrelationen in der Natur doch noch gefunden werden. Mit anderen Worten: Wenn Eve die Verschlüsselung nicht knacken kann, kann es keiner.

## QBismus

Subjektivität ist die neue Objektivität. Klingt weniger nach Wissenschaft als nach Kubismus, ist es aber nicht. «Q» steht für Quantum. «Bismus» für Bayesianismus (eine Interpretationsform für Wahrscheinlichkeiten). Das Erstaunliche: Es scheint sich auszugehen!

## Quantenbit, Qubit oder Qbit

Quantenversion des Bits. Grundeinheit der Quanteninformatik. Anstatt entweder 0 oder 1 zu sein, kann sich das Qbit in jeder denkbaren  $\boxtimes$  Superposition zweier  $\boxtimes$  Zustände befinden. Der Zustandsraum ist visuell als Bloch-Kugel gut veranschaulicht. Jeder Punkt dieser Kugel (beschrieben durch den dreidimensionalen Vektor) ist ein möglicher Zustand des Qbits.



Paul Erker



## Quantencomputer, universeller

Ein auf den Gesetzen der Quantenphysik basierender Computer. Wichtig: Quantencomputer werden bestehende Computer nicht vollständig ersetzen, sondern im Idealfall als modulare Bausteine fungieren, die man, ähnlich einer Grafikkarte, zu klassischen Computern dazuschalten kann.

Der Vorteil des Quantencomputers besteht darin, dass er gewisse Probleme effizienter lösen kann als ein klassischer Computer. Die Probleme sind im Speziellen das Durchsuchen grosser Datenbanken und das Faktorisieren von Zahlen. Da Zweites eine Möglichkeit ist, die heute gängige RSA-Verschlüsselung zu knacken, interessieren sich Geheimdienste für eine solche Maschine (oder sie interessierten sich eben früher dafür, dass nie eine gebaut wird). Universell bezieht sich auf die Möglichkeit, alle Algorithmen auf einem solchen Gerät ausführen zu können.

Der erste als Quantencomputer angekündigte Prozessor (von D-Wave Systems) löste Kontroversen aus, da es sich dabei um einen nicht universellen Quantencomputer handelt, der nur zur Lösung eines bestimmten Optimierungsproblems verwendet wird. Die erste Version dieser Maschine wurde an den Rüstungskonzern Lockheed Martin verkauft, die zweite Generation ging an die Nasa und Google. Da dieser Maschine bis heute kein Vorteil beim Berechnen irgendeines Problems nachgewiesen werden konnte, stellt sich die Frage: Ist dieser glorifizierte tiefgekühlte Computerchip mit seiner guten PR-Kampagne der Anfang der Quabble, der Quanten-Bubble?

## Quantencomputing

Ein Feld der Quanteninformation, welches sich mit den theoretischen Grenzen sowie der praktischen Umsetzung eines  $\boxtimes$  Quantencomputers sowie den Algorithmen zur Anwendung darauf beschäftigt.

## Quantenkorrelation

Stellen Sie sich ein Spiel vor, bei dem in mehreren Räumen, isoliert voneinander, zufällig zusammengestellte Multiple-Choice-Tests beantwortet werden müssen und die richtigen Antworten von den Fragen der anderen Testteilnehmerinnen abhängen. Der Einfachheit halber besteht der Test nur aus zwei verschiedenen Fragen mit jeweils zwei möglichen Antworten zur Auswahl, und wir beschränken uns auf zwei Spieler – in der Quanteninformation heissen diese immer Alice und Bob. Um das Spiel zu gewinnen, müssen Alice und Bob die gleiche Antwort geben (vollkommen gleichgültig, was die Antwort ist), es sei denn, beide bekommen Frage 2, dann müssen die Antworten unterschiedlich ausfallen. Bevor sie in getrennte Räume gesetzt werden, dürfen sie eine gemeinsame Strategie ausmachen. Ausserhalb des Reichs der Quantenphysik würden Alice und Bob abmachen, immer die gleiche Antwort zu geben, also zum Beispiel Antwort 1, unabhängig davon, welche Frage gestellt wird. Dadurch wäre ihre Gewinnchance 75 Prozent, da bei dem zufällig zusammengestellten Test die Wahrscheinlichkeit, dass beide Frage 2 bekommen, bei einem Viertel liegt. Hätten Alice und Bob sich vorher mit verschränkten Teilchen ( $\boxtimes$  Verschränkung) ausgerüstet, könnten sie ihre Gewinnchancen auf etwa 85 Prozent steigern. Dies zeigt, dass Korrelationen in der Quantenwelt stärker sein können als in der klassischen Welt.

## Quantenkryptografie

Beginn und bis jetzt grösster Erfolg der Quanteninformation. Sie löst ein jahrtausendealtes Problem der Kryptografie. Zur Veranschaulichung: Wenn Cäsar, bekannt dafür, seine Befehle zu kodieren, seinem Heerführer eine verschlüsselte Nachricht schickte, brauchte dieser einen Schlüssel, um die Nachricht zu entziffern. Dieser Schlüssel wurde vorher ausgehandelt. Mit jeder Nachricht, die zwischen den beiden hin- und hergeht, wird die Wahrscheinlichkeit aber grösser, dass der Schlüssel vom Feind geknackt wird. Um wirklich sicher kommunizieren zu können, wäre für jede Nachricht ein eigener Schlüssel nötig, mindestens so lang wie die Nachricht selbst. Hier präsentiert sich das alte Problem, dass der sichere Austausch eines geheimen Schlüssel genauso schwierig ist wie der sichere Austausch der geheimen Nachricht. Dieses Problem nennt sich das Problem des Schlüsselaustausches und wird von der Quantenkryptografie gelöst. Sie erlaubt es, beliebig viele dieser geheimen Schlüssel abfangsicher auszutauschen. Dies ist zum Beispiel mithilfe von  $\otimes$  Verschränkung möglich. Diese Methode wurde von einem der beiden Organisatoren der Quanteninformations-Konferenz in Benasque, Artur Ekert, Anfang der 1990er-Jahre entwickelt.

## (Quanten-)Zustand

Auch Wellenfunktion. Sie beschreibt das Verhalten eines physikalischen Systems bezüglich eines gewissen  $\otimes$  Freiheitsgrades. Ein reiner Zustand wird als  $\Psi$  (Psi) nach dem 23. Buchstaben im griechischen Alphabet, ein allgemeiner Zustand als  $\rho$  (Rho) nach dem 17. Buchstaben bezeichnet.

Im Unterschied zur klassischen Physik, wo ein Zustand schon alle Messergebnisse enthält – beziehungsweise äquivalent zu den Messergebnissen ist –, sind  $\Psi$  und  $\rho$  für sich genommen in der Quantenphysik noch nicht sehr aufschlussreich. Erst aus dem Duett von Zustand und Observable (der Frage, die wir bezüglich eines gewissen Freiheitsgrades an das System stellen) lassen sich Schlüsse ziehen. Zwar können wir nicht die Antworten (Messergebnisse) selbst berechnen, sehr wohl aber die Wahrscheinlichkeiten aller möglichen Antworten.

## Random Numbers

Zufallsgeneratoren sind bis jetzt der grösste Verkaufsschlager aus der Reihe der kommerzialisierten Quantentechnologien. Denn wirklich zufällige Zahlen zu produzieren, ist verdammt schwer, und dem Quantenzufall ist bis jetzt noch niemand auf die Schliche gekommen. Gebraucht werden *Random Numbers* in Unmengen von Banken, Versicherungen, Casinos, und auch das Internet will mit ihnen gefüttert werden. Die Wissenschaft braucht Zufallszahlen für Simulationen, im Speziellen Monte-Carlo-Simulationen. Daher gab es bis zur Verbreitung des Computers in jeder naturwissenschaftlichen Bibliothek Bücher voll mit nichts weiterem als zufälligen Zahlenfolgen, so absurd das auch klingen mag.

## Shut up and Calculate

*Heb d Schnurre und tue rächne!* Selbsterklärender Ansatz zum Verständnis der Quantenphysik, der Ende der 1930er-Jahre als Folge einer Welt im Krieg mit sich entwickelt wurde. Der Zweite Weltkrieg und die Anfänge des Kalten Kriegs liessen wenig Raum für die philosophischen Fragen, die  $\otimes$  Ein-

stein, ☒ Heisenberg, ☒ Bohr, ☒ Schrödinger, Grete Hermann und Wolfgang Pauli noch so leidenschaftlich diskutierten, dass man sich gegenseitig bis ans Bett verfolgte (sic). Im Krieg wurden die Physiker zur Ressource im Wettrüsten um die neusten Tötungs- und Abhörtechnologien. Staaten wie die USA butterten Millionen in die Subvention von Physikstudenten. Das sorgte nicht nur für eine gigantische Inflation von Physikern in den Sechzigern, sondern auch zu einem Stillstand im Bereich der Quantenphysik, wo es mit Rechnen und Schweigen offenbar nicht getan ist (Siehe «How the Hippies Saved Physics»).

## Schrödinger, Erwin

Geboren 1887 in Wien, gestorben 1961 in Wien, einer der Urväter der Quantenphysik, Nobelpreisträger der Physik des Jahres 1933. Da er sich nicht eindeutig zu den Nazis bekannte, verlor er seinen Lehrstuhl und ging nach Dublin ins Exil, 1956 kehrte er zurück nach Wien. Bekannt ist er für sein vermaledaites Büsi, weniger bekannt für seinen polyamorösen Lebensstil. In Österreich wurde er als Blauer verewigt – nicht wegen einer Affinität zum Rechtsextremismus, sondern auf der 1000-Schilling-Note.

## Spooky Action at a Distance

Zu Deutsch: spukhafte Fernwirkung. Begriff, der von ☒ Einstein geprägt wurde. Beruht auf einem falschen Verständnis von ☒ Verschränkung, da es dort eben zu keiner Wirkung über die Ferne kommt – also auch zu keinem Spuk. Das zweite Postulat von Einsteins spezieller Relativitätstheorie behält auch in der Quantenphysik und -information seine Gültigkeit; Informationsübertragung (und damit auch Wirkung) kann höchstens mit Lichtgeschwindigkeit stattfinden (☒ No-Signalling-Prinzip).

## Superdeterminismus

Superdeprimierende und superlangweilige Weltanschauung: Alles passiert, wie es passieren muss. Im Grunde genommen also einfach Determinismus, wie man ihn kennt; da der Begriff selbst aber schon belegt war, wird er in der Quantenwelt einfach potenziert verwendet. Determinismus per se ist populär bei gewissen Weltreligionen und gewissen Naturwissenschaftlern gleichermassen. In der Quantenwelt vor allem bei den Anhängern der ☒ Many-Worlds-Theorie und den ☒ Bohmianern.

## Superposition

Eigentlich ganz einfach: Superposition meint die Überlagerung verschiedener ☒ Zustände. Um dies zu veranschaulichen, stellen wir uns zwei sich aufeinander zubewegende Wasserwellen vor. Die Höhen der Wellenberge können sich bei ihrem Aufeinandertreffen überlagern. Dies geschieht, ohne dass sie sich dabei gegenseitig stören. Sind die Wellen aneinander vorbeigezogen, haben sie wieder dieselbe Form wie vor ihrem Treffen. In der Quantenwelt gibt es diese Überlagerung bezüglich jedes ☒ Freiheitsgrades, also auch des Orts. Etwa so, wie ein Ehepaar, das sich trotz Zusammenlebens nie und nimmer auf den Sack geht.

Unvorstellbar? Genau. Und das ist der Moment, in dem es alles andere als einfach wird: Diese Möglichkeit der Überlagerung von Zuständen führt zu einer der Eigenheiten des ☒ Quantencomputers (☒ Quantencomputing). Statt

nur mit einer Eingabe kann er mit einer Überlagerung aller möglichen Eingaben gefüttert werden. Genannt wird dies Quantenparallelismus.

So weit, so gut. Zurück zu den Wellen. Während in der klassischen Physik schon das Muster der Überlagerung selbst Interferenz genannt wird, tritt ein Interferenzmuster in der Quantenwelt erst nach der Messung auf (☒ *Measurement-Problem*). Dieses zeigt sich nicht nur bei Wellen, sondern entgegen der klassischen Vorstellung auch bei Teilchen. Doch solche binären Vorschreibungen sind in der Quantenwelt sehr unangebracht, denn hier sind alle *queer* (☒ *Anthropomorphismus*).

## Stringtheorie

Mathematische Collage physikalischer Theorien. Wie ein Sonnenuntergang – nichtssagend, aber wunderschön.

## Transistor

Essenzielles elektronisches Bauteil, das als Schalter oder Verstärker von elektrischen Strömen benutzt wird. Transistoren sind als aktive Schlüsselbauteile in allen modernen elektronischen Geräten verbaut (☒ *Moore's Law*).

## Unschärferelationen

Jede Messung, die uns Information über ein Quantensystem gibt, stört dieses auch. Ähnlich wie ein Gespräch zwischen zwei Menschen unweigerlich anders verläuft, wenn sie wissen, dass sie dabei aufgezeichnet werden. Mit dem Unterschied, dass es einem Quantensystem sehr wahrscheinlich scheissegal ist (☒ *Anthropomorphismus*), was die Konsequenz einer Beobachtung ist. Unschärferelation bedeutet, dass wir die Eigenschaften eines Quantensystems nicht beliebig genau simultan bestimmen können. Diese Austauschbeziehung zwischen Information und Störung ist ein eigenes Forschungsfeld innerhalb der Quanteninformation. Gängiges Beispiel dafür ist die heisenbergsche Unschärferelation.

## Verschränkung oder Entanglement

Phänomen in der Quantenphysik zwischen zwei oder mehr Systemen. Es zeichnet sich dadurch aus, dass Teilsysteme minimale Information über ihr Verhalten beinhalten, während das gesamte System maximale Information beinhaltet. In einfachen Worten: Zwei oder mehrere Teilchen, die verschränkt sind, verhalten sich so, als wären sie eins. Die Systeme sind dadurch stärker korreliert als klassisch möglich (☒ *Quantenkorrelation*).

Die Hippies («*How the Hippies Saved Physics*») haben daraus den Fehlschluss gezogen, durch dieses Phänomen schneller als Licht kommunizieren zu können – also telepathisch. Sie hätten richtig gelegen, wenn man Quanteninformation klonen könnte. Kann man aber nicht (☒ *No-Cloning-Theorem*).

Die Hippies lagen aber insofern richtig, als man durch Einflussnahme auf ein einziges Teilchen tatsächlich Einfluss auf alle mit ihm verschränkten Teilchen nehmen kann – das Problem ist nur, dass die Information dieses Einflusses für die Empfängerin erst dann wahrnehmbar wird, wenn sie weiss, worin genau die Einflussnahme bestand. Mit anderen Worten: Wir

müssen immer noch schnell telefonieren, um zu sagen, was wir da gemacht haben.

## Wigners Freund

Ein Gedankenexperiment, bei dem es um die (quantenphysikalische) Beobachtung eines (quantenphysikalischen) Beobachters geht. Dazu muss man wissen: Anders als in der klassischen Welt gibt es in der Welt der Quantenphysik zwei Formalismen, also zwei Arten, etwas zu berechnen (siehe auch [Everett](#)). Welche man wählt, spielt keine Rolle; das Resultat ist immer das Gleiche – bis auf einen einzigen Fall: Wigners Freund, benannt nach dem Physiker und Nobelpreisträger [Eugene Wigner](#). In diesem Gedankenexperiment führen die zwei unterschiedlichen mathematischen Beschreibungen der Quantenphysik zu unterschiedlichen Vorhersagen, jede für sich genommen konsistent. Wenigstens in der Theorie.

---

## Und jetzt die Lesetipps

Wenn der Wissensdurst in Bezug auf Quanteninformation noch immer nicht gestillt ist, empfehlen wir, sich in ein Physikstudium einzuschreiben – oder Folgendes:

### Für physikfremde Feingeister

Ralph Leighton, Richard P. Feynman: «[Surely You're Joking, Mr. Feynman!](#). [Adventures of a Curious Character](#)». W. W. Norton 1985, 400 Seiten, ca. 20 Franken. Hier geht es unter anderem um Safe-Knacken in Los Alamos.

### Für anspruchsvolle Kinder und Comicfans

Thibault Damour, Mathieu Burniat: «[Das Geheimnis der Quantenwelt](#)». Knesebeck 2017, 168 Seiten, ca. 30 Franken.

### Für einen federleichten Einstieg mit viel Pop Culture

David Kaiser: «[How the Hippies Saved Physics: Science, Counterculture, and the Quantum Revival](#)». W. W. Norton 2011, 416 Seiten, ca. 23 Franken.

### Für History Buffs und Englisch-Fortgeschrittene

Scott Aaronson: «[Quantum Computing Since Democritus](#)». Cambridge University Press 2013, 398 Seiten, ca. 56 Franken.

### Für Wissenschaftstheoriker und Politnerds

Paul Feyerabend: «[Against Method. Outline of an Anarchistic Theory of Knowledge](#)». Verso 2010, 336 Seiten, ca. 10 Franken. Paul Feyerabend: «[Wider den Methodenzwang](#)». Aus dem Englischen von Hermann Vetter. Suhrkamp 1986, 432 Seiten, ca. 32 Franken.

### Für naturwissenschaftlich Bewanderte oder jene, die es wirklich, wirklich wissen wollen

Dagmar Bruss: «Quanteninformation». Fischer 2003, 130 Seiten, ca. 30-Franken. [Der Verlag bietet eine Leseprobe](#).

### Für Physikstudis und solche, die es werden wollen

Isaac L. Chuang, Michael Nielsen: «[Quantum Computation and Quantum Information](#)». Cambridge University Press 2010, 702 Seiten, ca. 70 Franken.

### **Für Vollständigkeitsfanatiker und Masochisten**

Mark M. Wilde: «Quantum Information Theory». Cambridge University Press 2017, 776 Seiten, ca. 65 Franken.

### **Fürs Grosse, fürs Ganze – für alle**

Hannah Arendt: «Vita activa oder Vom tätigen Leben». Piper 2007, 496 Seiten, ca. 22 Franken.

Erwin Schrödinger: «Was ist Leben? Die lebende Zelle mit den Augen des Physikers betrachtet». Piper 1989, 160 Seiten, ca. 16 Franken.

---

### **Zum Haupttext**

Sie haben sich durchs gesamte Glossar gearbeitet, Sie sind zufrieden, wissender, vielleicht auch ein wenig ermattet und wissen nicht mehr so genau, wie Sie hierhergeiangt sind: [Hier gehts zurück zum Haupttext «Die Physiker»](#).

---

### **Zum Co-Autor**

Dr. Paul Erker, 1987 in Klagenfurt geboren, ist Quanteninformatiktheoretiker. Er besitzt den Bachelor in Physik (Uni Wien), den Master in Physik (ETH in Zürich) sowie den Dokortitel in Physik (Uni Barcelona) in Verbindung mit dem Dokortitel in Informatik (Uni Lugano). Erker spricht Deutsch, Englisch, Spanisch, Portugiesisch und Küchen-Italienisch; er flucht fließend in Bergslowenisch, Bosnisch/Kroatisch/Serbisch. Sein Lebensziel: Hausphysiker (das ist so etwas wie Hausmann, aber mit Physik). Er lebt in Wien.