Über Zufall und Wahrscheinlichkeit

ARMIN UHLMANN*

Für Günter Vojta zum 80. Geburtstag

Es ist schon mehr als vierzig Jahre her. GÜNTER VOJTA war in „Permosien", dem damaligen Leipziger Zweig der Deutschen Akademie der Wissenschaften, beschäftigt und Professor für Theoretische Physik an Leipzigs Universität. Letzteres „Im Nebenamt", wie man damals sagte. Was die universitären Aufgaben wie Vorlesungen, Prüfungen, Konsultationen und dergleichen betraf, war vom „Neben" im „Amt" nichts zu bemerken. Ich weiß, wovon ich rede, unsere Zimmer lagen nebeneinander. Seit dieser Zeit fühle ich mich mit dem Jubilar freundschaftlich verbunden. Die profunden Kenntnisse des Jubilars in Statistischer Physik und Thermodynamik habe ich stets bewundert. Daher erschien es mir passend, etwas über den Zufall und sein Maß aus einer anderen Perspektive aufzuschreiben.

Der allgemeine Sprachgebrauch verbindet „Zufall" oft mit Ereignissen, die unerwartet auftreten oder deren Eintreffen sich genaueren Vorhersagen verschließt. Es werden dann meist begriffliche Substitute wie „Schicksal", „Fügung", „Wunder" und anderes mehr verwendet. Denn es fällt unserem vorwiegend kausal und an Regeln geschulten Denken schwer, Zufall als natürlich zu akzeptieren.

Aber schon im Altertum findet sich der Gedanke, dass die Naturgesetze durch eine riesige Zahl zufälliger Ereignisse zur Geltung kommen (LUKREZ, *Über die Natur der Dinge*). Mitte des siebzehnten Jahrhunderts erkannte man, dass Aussagen über Erwartungswerte sehr nützlich für Versicherungen und bei der Berechnung von Renten sein können. Man weiß nicht genau, ob der Beginn systematischer wissenschaftlicher Untersuchungen hiervon beeinflusst wurde. Letztere, die mit einem Briefwechsel zwischen FERMAT und PASCAL (etwa 1654) ihren Anfang nahmen, stützten sich auf Glücksspiele. Das war eine sehr gute Wahl; denn hier hat man die Möglichkeit beliebiger Wiederholungen. Man kann *experimentell* ermitteln, wie gut Voraussagen eintreffen.

Obwohl seitdem Berechnungen von Wahrscheinlichkeiten und darauf aufbauenden Größen effektiv durchgeführt werden konnten, entzogen sie sich lange einer klaren mathematischen Definition. Diese Lücke konnte erst 1933 durch KOLMOGOROV [1] geschlossen werden. Seine Ergebnisse wurden zur Basis der sich rasch

* Prof. Dr. Armin Uhlmann, Institut für Theoretische Physik, Universität Leipzig

entwickelnden Wahrscheinlichkeitstheorie und der Theorie der stochastischen Prozesse.

Bereits bloßes Würfeln lässt die Problematik erkennen. Würfeln wir z. B. 60-mal. Bei dieser Tätigkeit erwarten wir eine „zufällige" Sequenz von 60 Zahlen. Fragen wir uns, was hier das Wort „zufällig" wohl bedeutet.

Eine physikalische Antwort ist die Unmöglichkeit, diese 60 Zahlen vorauszusagen. Wir müssen sie erst erwürfeln. In der Tat, wenn wir diese Sequenz geheimhalten, könnten wir sie zur Verschlüsselung eines Textes benutzen. Wir können umso mehr Information verstecken, je „typischer" die Sequenz, je „regelloser" unsere 60 Zahlen sind.[1] Anders gesagt, wäre unsere erwürfelte Sequenz hinreichend typisch, so wären nur diejenigen imstande, den verschlüsselten Text zu dekodieren, die den Schlüssel besitzen. Man sieht es einem gut kodierten Text nicht an, dass er ein Doppelleben führt: als neue zufällige Sequenz und als Träger (geheimer) Information. Ohne Schlüssel besitzt der kodierte Text keine Information!

Nach EINSTEIN können sich raumartig getrennte Ereignissen nicht unmittelbar kausal beeinflussen, Wirkungen können sich nicht mit Überlichtgeschwindigkeit ausbreiten. Da der Begriff der Kausalität von diffiziler Art ist, sagt man auch, dass Signalübertragung nicht schneller als mit Lichtgeschwindigkeit stattfinden kann. Das ist die EINSTEIN'sche „non-signaling condition". Aber auch hier ist Vorsicht geboten: Die Übertragung eines „informationslosen" Textes ist nicht notwendig eine Signalübertragung! Freilich kann die Gewissheit, dass ein Text keine Information enthält, nur die Quantenphysik liefern. Klassisch ist derartiges schlicht unmöglich. Doch dazu später.

Aussagen über den Zufall sind asymptotischer Natur. Wir sehen nicht voraus, was aus unsere Sequenz bei fortgesetztem Würfeln entstehen wird. Wir nähern uns KOLMOGOROV, indem wir nicht *eine* etwaige Fortsetzung, sondern *alle nur möglichen Fortsetzungen* unserer Sequenz betrachten. Für ihre eventuelle Länge bietet sich offensichtlich keine natürliche Begrenzung an. Daher bietet sich ganz natürlich die Menge aller unendlichen Folgen an, die, für das Beispiel des Würfelns, aus den Zahlen Eins bis Sechs gebildet werden können. Die Zufälligkeiten beim Würfeln können aus einem Maß auf dieser Folgenmenge abgeleitet werden. Das KOLMOGOROV'sche Wahrscheinlichkeitsmaß beschreibt unsere Intuition vom Würfeln mathematisch exakt. Es tut dies, indem es all ihren wichtigen Teilmengen ein Volumen zuordnet. Beispielsweise ordnet es der Menge aller Folgen, deren zweite Zahl eine 3 und deren zehnte Zahl eine 1 ist, das Volumen gleich 6^{-2} zu. Der Menge der Folgen, bei denen entweder die zweite Zahl eine 3 oder die zehnte Zahl eine 1 ist oder beides zutrifft, kommt das Volumen ⅓ zu. Nachdem man nach diesem Rezept einer respektablen Familie von Folgenmengen Volumina zuerkannt hat, ist es mathematische Routine, aus diesen Vorgaben ein Maß zu erzeugen. Mit

[1] Die Typizität kann mit der Entropie abgeschätzt werden.

diesen Andeutungen lassen wir es bewenden und gehen auf eine weiteres Problem zu.

Einen idealen Würfel gibt es im Makroskopischen nicht. Wenn jemand behauptete, einen solchen zu besitzen, er könnte es nicht beweisen.

Dagegen sind radioaktive Atomkerne ideale „Würfel": Die Zeit, die zwischen ihrer Herstellung und ihrem Zerfall vergeht, ist für einzelne Kerne unvorhersehbar, unterliegt aber als Massenphänomen streng den Gesetzen des Zufalls. Auch der Ort, an dem der jeweils nächste Zerfall in einer radioaktiven Substanz stattfindet, ist ein unvorhersehbar zufälliges Ereignis.

Makroskopischer Objekte können aus 10^{19}–10^{24} und mehr Atomen (Molekülen) bestehen. Auf Grund ihrer Komplexität sind sie individuell und besitzen eine Geschichte. Aus ihre gegenwärtigen Struktur kann ihre Herkunft erschlossen werden, wenngleich meist nur im Prinzip. Das steht im Gegensatz zu den Eigenschaften elementaren Teilchen, von Atomen und Molekülen in definierten Zuständen. Sie haben keine Individualität. Sie sind ohne Geschichte: Werden sie erzeugt, so ist alles vergessen, was vorher war und nicht durch allgemeine Erhaltungssätze (Energie, Impuls, Ladung, usw.) gesichert bleibt.

Hier eine etwas lockere Illustration (nach WALLACE): Ist es wahr, dass wir mit jedem Atemzug ein paar Moleküle des letzten Seufzers von CÄSAR einatmen? Diese Frage ist inkorrekt: Die Moleküle, die wir einatmen, können prinzipiell nicht von denen unterschieden werden, die CÄSAR ausgestoßen hat. (Wären sie unterscheidbar, wäre die Antwort „Ja".)

Mancher wird sich noch an CHRUSTCHOVS flotten Spruch erinnern: „Was nicht verboten ist, ist erlaubt." Die Hochenergiephysiker haben ihn verschärft zu: „Was nicht verboten ist, findet statt!" Wenn also unter Milliarden registrierter Stöße von Protonen an Protonen bestimmte, nach den wenigen Erhaltungssätzen erlaubte Ereignisse *nicht* stattfinden, dann muss, so ist der Schluss, ein noch unbekanntes Gesetz dies verhindern. In der Tat: Bei hinreichend vielen Ereignissen muss sich jedes erlaubte zeigen.

Wir gewinnen besonders klare Verhältnisse, wenn wir uns an „kleinen" Quantensystemen orientieren, deren HILBERT-Räume von niedriger Dimension sind. Augenscheinlicher Vorteil gegenüber Zerfallsprozessen ist ihre weitgehende Manipulierbarkeit. Ist besagte Dimension gleich zwei, so sagt man, es beschreibe ein *Quantenbit.*

Wie viele andere 2-Niveau-Systeme ist die Polarisation des Photons für die Informatik ein konkretes physikalisches Modell für ein Qubit. Zudem ist es, wegen der Proportionalität zwischen PAULI-LUBANSKI- und Energie-Impuls-Vektor, ein relativistisch invariantes. Zur Illustration sehen wir es uns etwas genauer an.

In diesem „Modell" wird jeder Zustand eines Qubits durch genau eine dem Photon erlaubte Polarisation realisiert. Diese Zustände können eindeutig den Punkten einer Kugel, der *Bloch-Kugel,* zugeordnet werden. Wählt man als Nord- bzw. Südpol die beiden zirkularen Polarisationen, so finden wir entlang des Äqua-

tors die linearen Polarisationen. Die anderen Punkte der Oberfläche der BLOCH-Kugel, also der *Bloch-Sphäre,* gehören zu elliptischen Polarisationen. Die BLOCH-Sphäre beschreibt die reinen Zustände.

Im Inneren der Kugel findet man die mehr oder weniger depolarisierten, also gemischten Zustände. Ihnen kann eine eindeutige Polarisation nicht zugeordnet werden. Sie können die mittlere Polarisation eines Ensembles von Photonen anzeigen. Sie können aber auch, und das ist für das Folgende entscheidend, die Polarisation eines einzelnen Photons beschreiben. Besonders interessant ist der Mittelpunkt der BLOCH-Kugel, der zu einem vollkommen depolarisierten Photon gehört, einem Qubit ohne Eigenschaften. Im übertragenen Sinne ist es „weißes Quantenpapier", auf dem eine Quanteninformation eingeschrieben werden kann, ohne dabei eine andere zu löschen.

Alle VON-NEUMANN'schen Messungen der Polarisation eines Photons sind Ja-Nein-Fragen: Man fragt, ob ein vorgegebener Zustand ξ auf der BLOCH-Sphäre vorliegt, „Ja", oder nicht vorliegt, „Nein". Im letzteren Fall wurde die zu ξ orthogonale Polarisation, der zu ξ antipodalen Zustand $\xi^{\perp}$, identifiziert. Nun kommt der Zufall ins Spiel: Ob die Messapparatur zu einem einlaufendes Photon „Ja" oder „Nein" sagt, ist rein zufällig!

Entsprach die Polarisation des Photons dem Punkt ρ der BLOCH-Kugel, so wird die Wahrscheinlichkeit p, dass unsere Apparatur „Ja" sagt, wie folgt berechnet: Wir fällen das Lot von ρ auf die durch ξ und $\xi^{\perp}$ gehende Achse und erhalten einen neuen Punkt ρ'. Wenn wir den Durchmesser der BLOCH-Kugel auf 1 normieren, so ist die Wahrscheinlichkeit des „Ja-Sagens" gleich dem Abstand zwischen ρ' und $\xi^{\perp}$. Lassen wir im Gedanken[2] Photonen der Polarisation ρ auf unser Messinstrument fallen und setzen wir 1, wenn es „Ja" sagt, und -1 sonst. Dann erhalten wir eine Zufallsfolge. Es gibt keinen Schlüssel, nichts, was einer so generierten Folge eine zusätzliche Information entreißen könnte. (Das ist ein Beispiel für die Nichtexistenz sogenannter verborgener Parameter.) Nach und nach approximiert das Experiment die Wahrscheinlichkeit p für „Ja" und $1-p$ für „Nein". Damit kann ρ' bestimmt werden, nicht aber ρ.

Ehe man in der Geschichte des mathematischen Zufalls von Wahrscheinlichkeiten gesprochen hat, hat man *Erwartungswerte* berechnet. HUYGENS, der die FERMAT-PASCAL'schen Resultate beschreibt (1658 *Über die bei Glücksspielen möglichen Berechnungen*), nennt ihn den „Wert der Hoffnung". Kehren wir wieder zum Photon zurück und ordnen wir unserem Messinstrument eine Observable A zu: Wir richten es so ein, dass bei „Ja" die Zahl +1 und bei „Nein" -1 ausgegeben wird. Das ist besonders einfach und symmetrisch. Der Erwartungswert $< A >$ von A im Zustand ρ ist dann $p + (1-p)(-1) = 2p - 1$.

---

[2] Das Experimentieren mit einzelnen Photonen ist hohe experimentelle Kunst!

Photonen, deren Polarisation im Inneren der BLOCH-Kugel liegt, können aus 2-Photonen-Systemen gewonnen werden. Die Polarisationen von 2-Photonen-Zuständen sind ein konkretes 2-Qubit-System. Diese Zustände lassen sich auf eine komplizierte 15-parametrische Mannigfaltigkeit abbilden. Physikalisch besonders interessant sind die *maximal verschränkten* Zustände. Die Benutzung des Wortes „Verschränkung" (entanglement) in der Quantentheorie stammt von SCHRÖDINGER [2], der es zur Analyse der berühmten Arbeit [3] von EINSTEIN, PODOLSKI und ROSEN einführte. Maximal verschränkt ist ein 2-Photon-Polarisationszustand, wenn er rein ist und jedes der beiden Photonen total depolarisiert ist.[3] Die beiden Photonen verhalten sich also wie das oben apostrophierte „weiße Quantenpapier". Gesetzt den Fall, eines der beiden Photonen wird vollständig polarisiert und somit „beschrieben". Dann, so sagt die Theorie, wird instantan auch das andere Photon polarisiert. Bei korrekter Justierung der beiden BLOCH-Kugeln sind die beiden entstandenen Polarisationen identisch. Wurden die beiden Photonen vor den Messungen hinreichend räumlich getrennt, so entstehen bei Wiederholung nach und nach zwei identische, absolut zufällige Sequenzen von Messwerten. So als hätten wir zwei Würfel, sagen wir in Dresden und Leipzig, und jeder simultane Wurf ergäbe die gleiche Zahl. Die Quantenphysik erlaubt eine derartige, klassisch unvorstellbare Korrelation.

Eine besonders beeindruckende experimentelle Bestätigung [4] verdanken wir einer Genfer Gruppe um GISIN und ZBINDEN, die diesem Problem mit immer größerer Genauigkeit und Raffinesse nachgegangen ist. Von ihrem Genfer Labor sendeten sie je ein Photon eines maximal verschränkten Photonenpaares[4] durch zwei je 17,5 km lange optische Fasern der Swisscom nach den Orten Satigny und Jussy. Letztere sind 18 km voneinander entfernt. Theoretisch sollten sich die Quantenkorrelationen ohne Zeitverzug einstellen. Experimentell konnte die untere experimentelle Schranke in den Jahren 2000 bis 2008 von 4-facher auf die 10 000-fache Lichtgeschwindigkeit angehoben werden.

Etwas locker, aber zu einer präzisen Aussage formulierbar, kann man sagen: Quantenkorrelationen bauen sich instantan auf. Sie können keine klassische Information übertragen. Das hat zu der Vermutung geführt, quantale Korrelationen könnten höchstens so stark sein, dass die EINSTEIN-Kausalität gerade noch respektiert wird. Diese attraktive Hypothese ist jedoch falsch! POPESCU und ROHRLICH haben mit der nach ihnen genannten „PR-Box" [5, 6] gezeigt, dass es Korrelationen zwischen zwei Systemen geben könnte, die keine Information übertragen können, also kein Problem für unser kausales Verständnis bilden, jedoch quantenphysikalisch nicht realisierbar sind.

---

[3] Für zwei Elektronenspins, einem anderen 2-Qubit-System, tritt maximale Verschränkung bei der Berechnung des Heliumspektrums sowie des H_2-Moleküls auf.

[4] Genutzt wurde die Verschränkung von Zeit und Energie.

Um zu sehen, worum es sich handelt, nehmen wir an, im Genfer Labor würden Photonenpaare mit der Polarisation ω erzeugt und jeweils eines nach Satigny und Jussy geschickt. In jedem dieser Orte würden zwei Polarisationen gewählt und an jedem je eine abgefragt. Indem wir „Ja" mit +1 und „Nein" mit –1 bewerten, hätten wir vier Observable: A_1, A_2 seien die in Satigny und B_1, B_2 die in Jussy gewählten. Wegen der räumlichen Trennung kommutiert jedes A_i mit jedem B_j. Daher sind A_iB_j Observable, die das Produkt der Messwerte der Faktoren ausgeben. Wenn ständig Photonenpaare der Polarisation ω für die Messungen bereitgestellt werden, können die Erwartungswerte $< A_iB_j >$ immer genauer bestimmt werden. Hierzu kommt zufällig an jedem der beiden Orte eine der beiden Messungen zum Zuge.

Es war die Fortführung einer genialen Einsicht von BELL [7] durch CLAUSER, HORNE, SHIMONY und HOLT [8], dass der Wert von Ausdrücken der Art

$$b(\omega) = | < A_1B_1 > + < A_2B_1 > + < A_2B_2 > - < A_1B_2 > |$$

empfindlich auf die Stärke der Korrelation reagiert, die durch die Polarisation ω zwischen den in den beiden Orten eintreffenden Photonen besteht. Diese Größe bewertet die Gesamtkorrelation, die sich aus klassischen und quantalen Bestandteilen zusammensetzt. Nimmt man an, dass die zu messenden Werte von vornherein feststehen, so muss $b(\omega) \leq 2$ sein. Das ist die nach ihren Erfindern benannte „CHSH-Ungleichung".

Eine Annahme vorbestimmter Messwerte widerspricht der Quantentheorie. Denn mit maximal verschränkten Zuständen kann man $b(\omega) = 2\sqrt{2}$ erreichen. Daher ist es unmöglich, dass die Werte bereits vor der Messung feststanden. Sie müssen durch den Akt der Messung zufällig erzeugt worden sein. Die wichtige Einsicht, dass innerhalb der Quantenphysik stets $b(\omega) \leq 2\sqrt{2}$ gelten muss, verdankt man TSIRELSON [9]. Sein Resultat eröffnet die Möglichkeit, über die Grenzen der Quantentheorie in elementarer Weise nachzudenken. Denn der Ausdruck $b(\omega)$ ist theorieunabhängig. Er ist ein Vorschlag für Experimente und Modelle.

Nun sind wir hinreichend vorbereitet, um uns noch dem Gedankenexperiment „PR-Box" zuzuwenden. Diese Blackbox hat zwei Eingänge, A_1, A_2, und zwei Ausgänge, B_1, B_2, die Zahlen ±1 ein- und ausgeben. Mit jedem Eingabepaar reagiert die Box mit einer zufälligen Ausgabe. Diese beiden ausgegebenen Zufallsfolgen seien nun wie folgt untereinander und mit der Eingabe korreliert: Sind die Werte von A_1, B_1 gleich $\{1, 1\}$, so geben A_2, B_2 mit Wahrscheinlichkeit ½ entweder $\{1, -1\}$oder $\{-1, 1\}$aus. Ist aber A_1, B_1 gleich $\{1, -1\}$, so wird A_2, B_2 mit Wahrscheinlichkeit ½ entweder $\{1, 1\}$oder $\{-1, -1\}$. Die übrigen Fälle entstehen, indem alle Vorzeichen geändert werden. Offenbar erhalten wir b(PR-Box) = 4, ein Wert, der durch kein quantenphysikalisches Arrangement erreichbar ist. Trotzdem können A_1, B_1 beziehungsweise A_2, B_2 an verschiedenen Orten gedacht werden: Da jede der ausgegebenen Folgen für sich eine Zufallsfolge ist, kann mit der PR-Box

keine Information übertragen werden. Non-signaling reicht daher nicht aus, um den CHSH-Wert auf den quantalen Wert $2\sqrt{2}$ zu beschränken.

Die POPESCU-ROHRLICH-Box ist eine neue, vermutlich fundamentale Idee [10, 11]. Eine der unerwarteten Konsequenzen hat VAN DAM [12], siehe auch [13], offengelegt: Würde die PR-Box in der Natur existieren, so wäre, beliebige lokale Ressourcen an Rechenleistung und maximal verschränkten Zuständen vorausgesetzt, die Komplexität von verteilten Rechnungen (die „complexity of distributed computation") trivial. Man weiß nicht, ob diese Konsequenz bereits zutrifft, wenn der quantenphysikalische Wert $2\sqrt{2}$ nur wenig übertroffen wird. Sind quantale Korrelationen gerade so stark, dass es zu keiner Trivialisierung der Komplexität verteilter Berechnungen kommt, oder ist dem nicht so? Noch ist die Antwort nicht gefunden.

Literatur

[1] A. N. Kolmogorov: *Grundbegriffe der Wahrscheinlichkeitsrechnung*. Springer, Berlin, 1933.

[2] E. Schrödinger: *Die gegenwärtige Situation in der Quantenmechanik*. Naturwissenschaften, 23:807–812,823–828,844–849, 1935.

[3] A. Einstein, B. Podolsky, and N. Rosen: *Can quantum-mechanical description of physical reality be considered complete ?* Phys.Rev., 47:777–780, 1935.

[4] S. Salart, A. Baas, C. Branciard, N. Gisin, and H. Zbinden: *Testing spooken action at distance*. Nature, 2008.

[5] S. Popescu and D. Rohrlich: *Quantum nonlocality as an axiom*. Foundation of Physics, 24:379, 1994.

[6] S. Popescu and D. Rohrlich: *Action and passion at a distance. An Essay in Honor of Professor Abner Shimony*. 1996. arXiv: quant-ph/9605004.

[7[J. Bell: *On the problem of hidden variables in quantum mechanics*. Rev. Mod. Phys., 38:447–452, 1966.

[8] J. F. Clausner, M. A. Horne, A. Shimony, and R. A. Holt: *Proposed experiment to test local hidden-variable theories*. Phys.Rev.Lett., 49:1804, 1969.

[9] B. S. Tsirelson: *Quantum generalizations of Bell's inequality*. Lett.Math.Phys., 4:93, 1980.

[10] J. Barrett, N. Linden, S. Massar, S. Popescu, and D. Roberts:. *Non-local correlations as an information theoretic resource*. Phys.Rev., A 71:022101, 2005.

[11] F. Dupuis, N. Gisin, A. Hasidim, A. A. Method, and H. Pilpel:. *No nonlocal box is universal*. 2007. arXiv: quant-ph/0701142.

[12] W. van Dam: *Implausible consequences of superstrong nonlocality*. 2005. arXiv: quant-ph/0201041.

[13] G. Brassard and H. Buhrman, N. Linden, A. A. Method, A. Trapp, and F. Unger: *A limit on non-local correlations in any world where communication complexity is not trivial*. Phys.Rev.Lett., 96:205401, 2006.