Über erkenntnistheoretische Implikationen der algorithmischen Informationstheorie

Joachim Bromand, Bonn

Seit den Unvollständigkeitssätzen Kurt Gödels ist wahrscheinlich kaum einem Resultat im Bereich der Logik so viel Aufmerksamkeit zuteil geworden wie den Ergebnissen Gregory J. Chaitins, welcher neben A. N. Kolmogorov und R. J. Solomonoff zu den Begründern der *algorithmischen Informationstheorie* zählt. Die für das Folgende relevanten Ergebnisse Chaitins beweisen wie Gödels Theoreme die Unvollständigkeit bestimmter formaler Systeme. Im Gegensatz zu Gödels Beweisen spielt bei denjenigen Chaitins allerdings der Begriff der *computational complexity* bzw. der Kolmogorov-Komplexität eine zentrale Rolle. Unbestritten haben Chaitins Ergebnisse viel zum Interesse an diesem Begriff und der auf ihm aufbauenden algorithmischen Informationstheorie beigetragen. Sehr wohl umstritten sind demgegenüber aber der tatsächliche mathematische Gehalt und die philosophische Bedeutung von Chaitins Theoremen.

Aus der Perspektive traditioneller philosophischer Fragestellungen besteht die interessanteste Behauptung Chaitins wohl darin, Fragen aufgeworfen zu haben, welche Grenzen des (mathematischen) Wissens aufzeigen: „These questions are completely beyond the power of human reasoning. Mathematics cannot deal with them“ (Chaitin 1987, 163). Ausgerechnet dieser Behauptung ist aber in den kritischen Repliken auf Chaitins Thesen so gut wie keine Beachtung zuteil geworden. Dies ist umso verwunderlicher, bedenkt man das gegenwärtige Interesse an der Frage nach etwaigen Begrenzungen unseres Wissens; vgl. etwa (Priest 2002) und (Williamson 2000). Das Folgende will daher der Frage nachgehen, ob erfolgreich für Chaitins erkenntnistheoretische These argumentiert werden kann oder nicht.

Argumentationsversuche für die Begrenztheit unseres Wissens sind selbstverständlich keine Seltenheit. Geht man etwa davon aus, dass alles, was wir wissen können, sprachlich formulierbar sein muss, zeigt etwa Patrick Grim mit einem einfachen Diagonalargument, dass es mehr Tatsachen geben muss als die, von denen wir wissen können (Grim 1991). Auch das *Paradox of Unknowability*, welches erstmals von Fitch veröffentlicht wurde (Fitch 1963), scheint prinzipielle Grenzen des Wissens aufzuzeigen, ohne dass Genaueres darüber gesagt werden könnte, wo diese Grenzen verlaufen; vgl. die ausführliche Diskussion in (Williamson 2000). Gemeinsam ist diesen Ansätzen, dass sie für die Begrenztheit von Wissen argumentieren, aber nicht spezifizieren können, *inwiefern* unser Wissen begrenzt sein sollte. Ein interessanter Beitrag zur Debatte bestünde nun darin, zumindest etwas genauer anzugeben, *wo genau* die besagten Grenzen verlaufen. Tatsächlich scheinen Chaitins Überlegungen in dieser Beziehung über die erwähnten Argumentationen hinauszuführen, insofern er eine Problematik namhaft machen kann, von der er dann zu zeigen versucht, dass sie letztlich unerforschlich ist. Chaitins Ansatz scheint somit durchaus spezifizieren zu können, *wo* (unter anderem) Grenzen unseres Wissens verlaufen.

Chaitins Idee, erkenntnistheoretisches Kapital aus seinen Unvollständigkeitsresultaten zu schlagen, liegt nicht so fern, berücksichtigt man die Vielzahl der Versuche, erkenntnistheoretische Konsequenzen aus Gödels Unvollständigkeitstheoremen zu ziehen. Insbesondere hinsichtlich der Grenzen unseres Erkenntnisvermögens wurde erst kürzlich ausgehend von Gödels Resultat ein solcher Versuch von Haim Gaifman unternommen (Gaifman 2000).

Das Theorem Chaitins, auf welches sich seine erkenntnistheoretischen Behauptungen stützen, hat die bemerkenswerte reelle Zahl Ω zum Gegenstand. Ω kann aufgefasst werden als Haltewahrscheinlichkeit eines universellen Computers. Im Folgenden legen wir uns auf einen universellen Computer *U* fest, welcher nur binäre prefixfreie Programme akzeptiert (eine (Programmier-)Sprache *L* wird *prefix-frei* genannt gdw. kein Wort von *L* ein Prefix eines anderen Wortes von *L* ist). $|p|$ bezeichne die Länge eines Programms *p*. Die *Haltewahrscheinlichkeit* von *U* ist nun

$$\Omega = \sum_{U(p)\ \text{hält}} 2^{-|p|}$$

Dieser Definition liegt die Intuition zugrunde, dass Ω die Wahrscheinlichkeit ist, dass *U* hält, wenn sein Programm durch eine Folge von Münzwürfen generiert wurde. Zentral hinsichtlich Ω ist, dass seine binäre Darstellung eine nicht komprimierbare Folge bildet; vgl. etwa (Li und Vitanyi 1997, 217–218). Ausgehend von dieser Tatsache kann das folgende Unvollständigkeitstheorem Chaitins bewiesen werden, welches als Ω-*Theorem* bezeichnet werden soll. Was hinsichtlich Ω gezeigt werden kann, ist, dass Ω eine reelle Zahl ist, so dass $0 < \Omega < 1$ gilt (der Einfachheit halber wird mit „Ω“ im Folgenden sowohl die reelle Zahl $0{,}a_1a_2a_3$ ... als auch die Folge $a_1a_2a_3$ ... bezeichnet). Chaitins Ω-Theorem zeigt jedoch, dass die Anzahl der Bits von Ω, welche wir im Rahmen einer Theorie bestimmen können, begrenzt ist:

> **Ω-Theorem.** Jede rekursiv axiomatisierbare formale Theorie erlaubt lediglich endlich viele (unzusammenhängende) Bits von Ω zu bestimmen.

Der Beweis findet sich etwa in (Chaitin 1987, 150–151) oder (Calude 1994, 195–196).

Chaitin argumentiert nicht explizit für die Unerforschlichkeit von Ω, sondern scheint Letztere auf die Zufälligkeit von Ω zurückführen zu wollen (wobei er die Zufälligkeit einer Folge mit deren Nicht-Komprimierbarkeit identifiziert) (Chaitin 1987, 164): „Ω is about as random, patternless, unpredictable and incomprehensible as possible; the pattern of its bit sequence defies understanding.“ Ein solcher Argumentationsansatz ist allerdings nicht unproblematisch, da eben fraglich ist, ob Chaitins Begriff eine gelungene Formalisierung des umgangssprachlichen Zufallsbegriffes ist. Dies ist nicht unumstritten, so dass van Lambalgen etwa gegen Chaitins informationstheoretische Charakterisierung von Zufälligkeit einwendet (van Lambalgen 1989, 1398):

> „The randomness of a quantum mechanical phenomenon such as electron spin does not disappear as soon as we decide to adopt a different definition of randomness, whereas in cases such as the above we seem to observe an artifact of the particular definition chosen.

Of course other (arithmetical) definitions of random sequences would yield new examples of "randomness in mathematics" constructed with the help of a suitable basis theorem; but one looks in vain for examples which are stable under a change of definition. Hence the *robustness* which is present in the physical examples that Chaitin mentions is lacking here."

Selbst wenn also gezeigt werden könnte, dass Zufälligkeit im umgangssprachlichen Sinne Unerforschlichkeit impliziert, bliebe noch zu zeigen, dass Chaitins Definition der Zufälligkeit dem umgangssprachlichen Begriff entspricht (was, wie die zuletzt zitierte Passage vermuten lässt, nicht unproblematisch ist).

Im Folgenden soll daher ein alternativer Versuch unternommen werden, ein Argument für die Unerforschlichkeit von Ω auf der Grundlage von Chaitins Ω-Theorem zu rekonstruieren, ohne auf Chaitins umstrittene Explikation des Begriffes der Zufälligkeit zurückzugreifen. Vielmehr basiert der folgende Versuch auf der erwähnten Nicht-Komprimierbarkeit von Ω.

Wissen wir um die Beschaffenheit einer unendlichen Folge wie Ω, sollten wir in der Lage sein, den Wert von Ω an jeder beliebigen Stelle zu spezifizieren. Als endliche Wesen können wir natürlich nur um die Wahrheit endlich vieler Propositionen wissen, welche die Werte von Ω beschreiben. Daher kann unser Wissen um Ω bestenfalls in der Kenntnis eines Algorithmus bestehen oder zumindest in der Kenntnis einer Theorie, welche es (wenigstens prinzipiell) erlaubt, Theoreme herzuleiten, welche alle Stellen der Folge wahrheitsgemäß beschreiben. Aufgrund der algorithmischen Nicht-Komprimierbarkeit von Ω kann es allerdings keinen solchen Algorithmus geben und Chaitins Ω-Theorem zeigt zudem, dass es auch eine entsprechende Theorie im Falle von Ω nicht geben kann. Alle in Frage kommenden Theorien erlauben lediglich, endlich viele Stellen von Ω zu bestimmen; in jeder solchen Theorie werden demnach unendlich viele Sätze über die Beschaffenheit von Ω unentscheidbar sein.

Ist damit aber bereits gezeigt, dass unser Wissen um die Beschaffenheit von Ω notwendigerweise begrenzt ist? Eingewendet werden könnte etwa, dass wir um den Wahrheitswert von unentscheidbaren Propositionen wissen können (wie derjenigen, welche die Werte von Ω beschreiben). Tatsächlich ist die Unentscheidbarkeit eines Satzes in *einem* formalen System aus erkenntnistheoretischer Sicht nicht unbedingt problematisch. Insbesondere zeigt der Nachweis der Unentscheidbarkeit bestimmter Sätze nicht, dass es unmöglich ist, den Wahrheitswert der unentscheidbaren Sätze in Erfahrung zu bringen. Dies kann verdeutlicht werden durch den Vergleich mit dem erkenntnistheoretischen Status anderer unentscheidbarer Probleme bzw. Sätze wie etwa Gödels erstem Unvollständigkeitstheorem oder der durch Gödel und Cohen nachgewiesenen Unentscheidbarkeit der Kontinuumshypothese (CH) im Rahmen von ZFC. Zum Nachweis der Unvollständigkeit der Arithmetik konstruiert Gödel einen Satz *G*, der unentscheidbar in PA ist. Dennoch haben wir aufgrund von metatheoretischen Erwägungen gute Gründe, an die Wahrheit von *G* zu glauben, da *G* gerade besagt, dass *G* in PA nicht nachweisbar ist, und wir zudem gute Gründe haben daran zu glauben, dass aus den Axiomen von PA nichts Falsches herleitbar ist. Demgegenüber stellt die Frage nach Wahrheit oder Falschheit von CH ein wesentlich gravierenderes Problem dar. CH ist unentscheidbar in ZFC und damit unentscheidbar relativ zur stärksten weitestgehend anerkannten und gegenwärtig zur Verfügung stehenden mathematischen Theorie. Zudem helfen in diesem Fall nicht metatheoretische Erwägungen wie im Falle von Gödels Satz. Allerdings besteht die Möglichkeit, ZFC durch weitere Axiome zu ergänzen, so dass CH auf der Basis der somit erweiterten Theorie entscheidbar ist. Solche Erweiterungen einer Theorie um neue Axiome bzw. (im Falle von Gödels Satz) um metatheoretische Feststellungen stellen dabei bislang die einzigen kaum umstrittenen Möglichkeiten dar, den Wahrheitswert eines unentscheidbaren Satzes zu eruieren. Problematisch im Falle von Ω ist nun, dass keine der beiden Methoden signifikant weiterhilft, die Beschaffenheit von Ω zu bestimmen. Da es nach Chaitins Ω-Theorem in *jeder* Theorie unendlich viele unentscheidbare Sätze geben wird, welche die Beschaffenheit von Ω betreffen, kann auch der Übergang zu einer umfassenderen (rekursiv axiomatisierbaren) Theorie nicht zur Lösung des Problems führen. Weder das Hinzuziehen metatheoretischer Überlegungen (wie im Falle von *G*) noch das Hinzuziehen weiterer Axiome (wie eventuell im Fall von CH) helfen daher zur Bestimmung der Beschaffenheit von Ω deutlich weiter. Letztere stellt demnach ein Problem dar, welches in *keiner* von uns überschaubaren (d. h. rekursiv axiomatisierbaren) Theorie vollständig gelöst werden kann. Die Frage nach der Beschaffenheit von Ω scheint demnach von uns prinzipiell nicht beantwortet werden zu können – unabhängig davon, in welcher Theorie sich unsere fortschreitenden Bemühungen, unser mathematisches Wissen zu erweitern, auch niederschlagen mögen. Damit deuten Chaitins Ergebnisse hinsichtlich Ω zumindest auf die Existenz von Grenzen unseres (mathematischen) Wissens hin.

Allerdings sind auch einige einschränkende Bemerkungen zur Bedeutung von Chaitins Theorem zu erörtern. Zunächst sind die Voraussetzungen zu erwähnen, auf welchen Chaitins erkenntnistheoretische Deutung seiner Theoreme beruht. So besteht die vielleicht wesentlichste Voraussetzung für die obige Argumentation in einer realistischen Grundhaltung, zumindest im Festhalten an der These, mathematischen Aussagen käme *objektiv* ein Wahrheitswert zu. Wäre dies aber etwa bei unentscheidbaren Problemen wie im Falle der Bits von Ω nicht der Fall, gäbe es mathematische Fragen, die keine Antwort besitzen und demnach auch nicht beantwortet werden können. Demzufolge gäbe es aber auch keine Antworten, von denen wir wissen könnten, so dass hier nicht von Grenzen unseres Wissens gesprochen werden könnte. Eine realistische Haltung, derzufolge mathematischen Aussagen objektiv ein Wahrheitswert zukommt, ist natürlich keine Selbstverständlichkeit und wird selbst im Rahmen von Positionen abgelehnt, welche dem klassischen Platonismus nahe stehen wie etwa Fields *plenitudinous platonism* (Field 1998). Sicherlich auch aus einer intuitionistischen Perspektive ist der Glaube an die Objektivität mathematischer Aussagen nicht zu halten. Entsprechend weist van Lambalgen darauf hin, dass insbesondere Chaitins erstes Unvollständigkeitstheorem[1] wesentlich auf die Verwendung klassischer Logik (und die ihr zugrunde liegenden Annahmen) angewiesen ist und nicht etwa auf intuitionistische Systeme übertragen werden kann (van Lambalgen 1989, 1395). Und selbstverständlich kann auch Chaitins Ω-Theorem nicht auf der Grundlage einer beliebigen Alternative zur klassischen Logik hergeleitet werden. So berechtigt solche relativierenden Hinweise auch sein mögen, rütteln sie aufgrund der doch weitgehend unangefochtenen Stellung der klassischen Logik (und der ihr

[1] Chaitins erstes Unvollständigkeitstheorem, von welchem bislang nicht die Rede war, besagt dabei, dass es für jede formale Theorie *T* eine Konstante *m* gibt, so dass *T* nur dann wahre Sätze der Form „Die Komplexität der Folge *s* ist größer als *n*" beweist, wenn *n* kleiner als *m* ist. Ein Beweis findet sich etwa in (Chaitin 1987, 147–149).

zugrunde liegenden Annahmen) nicht unbedingt an dem erkenntnistheoretischen Interesse an Chaitins Theorem.

Des Weiteren ist festzuhalten, dass die obigen erkenntnistheoretischen Überlegungen auch an bereits bekannte limitative Theoreme von Church, Gödel und Turing anknüpfen könnten und nicht auf Chaitins Unvollständigkeitsresultat hinsichtlich Ω angewiesen sind. Zahlen mit einem Ω vergleichbaren erkenntnistheoretischen Status stellen etwa die von Turing erörterten *nicht-berechenbaren Zahlen* dar; siehe (Turing 1936–7). Um ein weiteres Beispiel anzuführen, betrachten wir zunächst eine vollständige Aufzählung aller Sätze der Sprache der Arithmetik S_1, S_2, S_3, ... Die Zahl A sei nun identisch mit $0{,}a_1a_2a_3$ ..., wobei $a_i = 1$, falls S_i wahr in der Standard-Interpretation der Arithmetik ist, sonst sei $a_i = 0$. Es kann leicht gezeigt werden, dass es uns wie im Falle von Ω nicht möglich ist, die Zahl A *vollständig* zu bestimmen. Allerdings zeigt Chaitins Resultat die Grenzen unserer Möglichkeiten drastischer auf, da im Falle von Ω – im Gegensatz zu A – nur endlich viele Stellen bestimmt werden können; eine ausführlichere Diskussion vergleichbarer reeller Zahlen wird vorgelegt in (Löwe und Bromand 200?).

Schließlich ist anzumerken, dass die obigen Überlegungen lediglich zeigen, dass wir über die genaue Beschaffenheit von Ω nichts in Erfahrung bringen können, sofern wir die bislang gebräuchlichen Methoden verwenden, um etwas über die Wahrheitswerte unentscheidbarer Sätze zu erfahren (wie diejenigen, welche die Bits von Ω betreffen). Demgegenüber könnte für Chaitins Behauptung erst dann lückenlos argumentiert werden, wenn ausgeschlossen werden könnte, dass es (neben dem Hinzuziehen metatheoretischer Erwägungen oder weiterer Axiome) alternative, bislang unbekannte Methoden gibt, durch welche wir Wissen über den Wahrheitswert formal unentscheidbarer Sätze erlangen könnten. Dieses Problem ist verwandt mit der Frage, ob sich die Gesamtheit unseres mathematischen Wissens in einer rekursiv axiomatisierbaren Theorie erschöpft. Gegenwärtig wird ZFC als eine solche Grundlagentheorie verstanden, in welcher nahezu alle mathematischen Argumentationen formalisiert werden können. Um ausgehend vom obigen Argumentationsansatz eine lückenlose Argumentation für Chaitins erkenntnistheoretische These zu erhalten, wäre es notwendig, zunächst zu zeigen, dass die Gesamtheit unseres mathematischen Wissens (zumindest unser Wissen von reellen Zahlen) stets in Form einer rekursiv axiomatisierbaren Theorie darstellbar ist (was selbstverständlich nicht unumstritten ist). Um dies zeigen oder widerlegen zu können, wissen wir allerdings längst noch nicht genug über den Begriff des mathematischen Wissens.

Literatur

Calude, C. 1994 *Information and Randomness. An algorithmic Perspective*, Berlin, Heidelberg & New York: Springer.

Chaitin, G. 1987 *Algorithmic Information Theory*, Cambridge: Cambridge University Press.

Field, H. 1998 „Which Undecidable Mathematical Sentences Have Determinate Truth Values?“, in H.G. Dales und G. Oliveri (eds.), *Truth in Mathematics*, Oxford: Oxford University Press, 291-310.

Fitch, F.B. 1963 „A Logical Analysis of some Value Concepts“, *Journal of Symbolic Logic* 28, 135-142.

Gaifman, H. 2000 „What Gödel's Incompleteness Result does and does not show“, *The Journal of Philosophy* 97, 462-470.

Grim, P. 1991 *The Incomplete Universe*, Cambridge (MA): MIT-Press.

Li, M. und Vitanyi, P. 1997 *An Introduction to Kolmogorov Complexity and its Applications*, 2. Aufl., New York: Springer.

Löwe, B. und Bromand, J. 200? „(Formally) Unknowable Reals and Theorems of Essential Incompleteness“, in Vorbereitung.

Priest, G. 2002 *Beyond the Limits of Thought*, 2. Aufl., Oxford: Oxford University Press.

Turing, A.M. 1936–7 „On Computable Numbers, with an Application to the Entscheidungsproblem“, *Proceedings of the London Mathematical Society* 42, ser. 2, 230-265.

van Lambalgen, M. 1989 „Algorithmic Information Theory“, *Journal of Symbolic Logic* 54, 1389-1400.

Williamson, T. 2000 *Knowledge and its Limits*, Oxford: Oxford University Press.