The Berry Paradox

(Originally appeared in Complexity 1, No. 1, (1995))

G. J. Chaitin

IBM Research Division,
P. O. Box 704, Yorktown Heights, NY 10598, USA,
chaitin @ watson.ibm.com

In early 1974, I was visiting the Watson Research Center and I got the idea of calling Gödel on the phone. I picked up the phone and called and Gödel answered the phone. I said, "Professor Gödel, I'm fascinated by your incompleteness theorem. I have a new proof based on the Berry paradox that I'd like to tell you about." Gödel said, "It doesn't matter which paradox you use." He had used a paradox called the liar paradox. I said, "Yes, but this suggests to me an information-theoretic view of incompleteness that I would very much like to tell you about and get your reaction." So Gödel said, "Send me one of your papers. I'll take a look at it. Call me again in a few weeks and I'll see if I give you an appointment."

I had had this idea in 1970, and it was 1974. So far I had only published brief abstracts. Fortunately I had just gotten the galley proofs of my first substantial paper on this subject. I put these in an envelope and mailed them to Gödel.

I called Gödel again and he gave me an appointment! As you can imagine I was delighted. I figured out how to go to Princeton by train. The day arrived and it had snowed and there were a few inches of snow everywhere. This was certainly not going to stop me from visiting Gödel! I was about to leave for the train when the phone rang. It was Gödel's secretary, who said that Gödel was very careful about his health and because of the snow he wasn't coming to the Institute that day. Therefore, my appointment was canceled.

And that's how I had two phone conversations with Gödel but never met him. I never tried again.

I'd like to tell you what I would have told Gödel. What I wanted to tell Gödel is the difference between what you get when you study the limits of mathematics the way Gödel did, using the paradox of the liar, and what I get using the Berry paradox instead.

What is the paradox of the liar? Well, the paradox of the liar is

"This statement is false!"

Why is this a paradox? What does "false" mean? Well, "false" means "does not correspond to reality." This statement says that it is false. If that doesn't

correspond to reality, it must mean that the statement is true, right? On the other hand, if the statement is true it means that what it says corresponds to reality. But what it says is that it is false. Therefore the statement must be false. So whether you assume that it's true or false, you must conclude the opposite! So this is the paradox of the liar.

Now let's look at the Berry paradox. First of all, why "Berry"? Well it has nothing to do with fruit! This paradox was published at the beginning of this century by Bertrand Russell. Now there's a famous paradox which is called Russell's paradox and this is not it! This is another paradox that he published. I guess people felt that if you just said the Russell paradox and there were two of them it would be confusing. And Bertrand Russell when he published this paradox had a footnote saying that it was suggested to him by an Oxford University librarian, a Mr G. G. Berry. So it ended up being called the Berry paradox even though it was published by Russell.

Here is a version of the Berry paradox:

"the first positive integer that cannot
be specified in less than a billion words".

This is a phrase in English that specifies a particular positive integer. Which positive integer? Well, there are an infinity of positive integers, but at any given time there are only a finite number of words in English. Therefore, if you have a billion words, there's only going to be a finite number of expressions of any given finite length. But there's an infinite number of positive integers. Therefore most positive integers require more than a billion words to describe. So let's just take the first one. But wait a second. By definition this integer is supposed to take a billion words to specify, but I just specified it using much less than a billion words! That's the Berry paradox.

What does one do with these paradoxes? Let's take a look again at the liar paradox:

"This statement is false!"

The first thing that Gödel does is to change it from "This statement is false" to "This statement is unprovable":

"This statement is unprovable!"

What do we mean by "unprovable"?

In order to be able to show that mathematical reasoning has limits you've got to say very precisely what the axioms and methods of reasoning are that you have in mind. In other words, you have to specify how mathematics is done with mathematical precision so that it becomes a clear-cut question. Hilbert put it this way: The rules should be so clear, that if somebody gives you what they claim is a proof, there is a mechanical procedure that will check whether the proof is correct or not, whether it obeys the rules or not. This proof-checking algorithm is the heart of this notion of a completely formal axiomatic system.

So "This statement is unprovable" doesn't mean unprovable in a vague way. It means unprovable when you have in mind a specific formal axiomatic system *FAS* with its mechanical proof-checking algorithm. So there is a subscript:

"This statement is unprovable$_{FAS}$!"

And the particular formal axiomatic system that Gödel was interested in dealt with the positive integers and addition and multiplication, that was what it was about. Now what happens with "This statement is unprovable"? Remember the liar paradox:

"This statement is false!"

But here

"This statement is unprovable$_{FAS}$!"

the paradox disappears and we get a theorem. We get incompleteness, in fact. Why?

Consider "This statement is unprovable". There are two possibilities: either it's provable or it's unprovable.

If "This statement is unprovable" turns out to be unprovable within the formal axiomatic system, that means that the formal axiomatic system is incomplete. Because if "This statement is unprovable" is unprovable, then it's a true statement. Then there's something true that's unprovable which means that the system is incomplete. So that would be bad.

What about the other possibility? What if

"This statement is unprovable$_{FAS}$!"

is provable? That's even worse. Because if

"This statement is unprovable$_{FAS}$!"

is provable and it says of itself that it's unprovable, then we're proving something that's false.

So Gödel's incompleteness result is that if you assume that only true theorems are provable, then this

"This statement is unprovable$_{FAS}$!"

is an example of a statement that is true but unprovable.

But wait a second, how can a statement deny that it is provable? In what branch of mathematics does one encounter such statements? Gödel cleverly converts this

"This statement is unprovable$_{FAS}$!"

into an arithmetical statement, a statement that only involves positive integers and addition and multiplication. How does he do this?

The idea is called gödel numbering. We all know that a string of characters can also be thought of as a number. Characters are either 8 or 16 bits in binary. Therefore, a string of N characters is either $8N$ or $16N$ bits, and it is also

the base-two notation for a large positive integer. Thus every mathematical statement in a formal axiomatic system is also a number. And a proof, which is a sequence of steps, is also a long character string, and therefore is also a number. Then you can define this very funny numerical relationship between two numbers X and Y, which is that X is the gödel number of a proof of the statement whose gödel number is Y. Thus

"This statement is unprovable$_{FAS}$!"

ends up looking like a very complicated numerical statement.

There is another serious difficulty. How can this statement refer to itself? Well you can't directly put the gödel number of this statement inside this statement; it's too big to fit! But you can do it indirectly. This is how Gödel does it: The statement doesn't refer to itself directly. It says that if you perform a certain procedure to calculate a number, this is the gödel number of a statement which cannot be proved. And it turns out that the number you calculate is precisely the gödel number of the entire statement

"This statement is unprovable$_{FAS}$!"

That is how Gödel proves his incompleteness theorem.

What happens if you start with this

"the first positive integer that cannot
be specified in less than a billion words"

instead? Everything has a rather different flavor. Let's see why.

The first problem we've got here is what does it mean to specify a number using words in English? This is very vague. So instead let's use a computer. Pick a standard general-purpose computer, in other words, pick a universal Turing machine (UTM). Now the way you specify a number is with a computer program. When you run this computer program on your UTM it prints out this number and halts. So a program is said to specify a number, a positive integer, if you start the program running on your standard UTM, and after a finite amount of time it prints out one and only one great big positive integer and it says "I'm finished" and halts.

Now it's not English text measured in words, it's computer programs measured in bits. This is what we get. It's

"the first positive integer that cannot
be specified$_{UTM}$ by a computer program
with less than a billion bits".

By the way the computer program must be self-contained. If it has any data, the data is included in the program as a constant.

Next we have to do what Gödel did when he changed "This statement is false" into "This statement is unprovable." So now it's

> "the first positive integer that can be proved$_{FAS}$
> to have the property that it cannot
> be specified$_{UTM}$ by a computer program
> with less than a billion bits".

And to make things clearer let's replace "a billion bits" by "N bits". So we get:

> "the first positive integer that can be proved$_{FAS}$
> to have the property that it cannot
> be specified$_{UTM}$ by a computer program
> with less than N bits".

The interesting fact is that there is a computer program of length

$$\log_2 N + c_{FAS}$$

bits for calculating this number that supposedly cannot be calculated by any program that is less than N bits long. And

$$\log_2 N + c_{FAS}$$

is much much smaller than N for sufficiently large N. Thus for such N our FAS cannot enable us to exhibit any numbers that require programs more than N bits long. This is my information-theoretic incompleteness result that I wanted to discuss with Gödel.

Why does there have to exist a program that is

$$\log_2 N + c_{FAS}$$

bits long for calculating

> "the first positive integer that can be proved$_{FAS}$
> to have the property that it cannot
> be specified$_{UTM}$ by a computer program
> with less than N bits" ?

Well here is how you show it.

You start running through all possible proofs in the formal axiomatic system in size order. You apply the proof-checking algorithm to each proof. And after filtering out all the invalid proofs, you search for the first proof that a particular positive integer requires at least an N-bit program.

The algorithm that I've just described is very slow but it is very simple. It's basically just the proof-checking algorithm, which is c_{FAS} bits long, and the number N, which is $\log_2 N$ bits long. So the total number of bits is just

$$\log_2 N + c_{FAS},$$

as was claimed. That concludes the proof of my incompleteness result that I wanted to discuss with Gödel.

Over the years, I've continued to do research on my information-theoretic approach to incompleteness. Here are the three most dramatic results that I've obtained thus far:

1) Call a program "elegant" if no smaller program produces the same output. You can't prove that a program is elegant. More precisely, N bits of axioms are needed to be able to prove that an N-bit program is elegant.
2) Consider the binary representation of the halting probability Ω, which is the probability that a program chosen at random halts. You can't prove what one of the bits of Ω is. More precisely, N bits of axioms are needed to be able to determine N bits of Ω.
3) I have constructed a perverse algebraic equation

$$P(K, X, Y, Z, \ldots) = 0.$$

Vary the parameter K and ask whether this equation has finitely or infinitely many whole-number solutions. In each case, this turns out to be equivalent to determining one of the bits of Ω. Therefore N bits of axioms are needed to be able to settle N cases.

These striking examples show that sometimes you have to put more into a set of axioms in order to get more out. Results (2) and (3) are extreme cases. They are accidental mathematical assertions that are true for no reason at all. In other words, the questions considered in (2) and (3) are irreducible; essentially the only way to prove them is to assume them as new axioms. So in this extreme case, what you get out of a set of axioms is only what you put in.

How do I prove these incompleteness results (1), (2) and (3)? As before, the basic idea is the paradox of "the first positive integer that cannot be specified in less than a billion words." For (1) the connection with the Berry paradox is obvious. For (2) and (3) it was obvious to me only in the case where one is talking about determining the first N bits of Ω. In the case where the N bits of Ω are scattered about, my original proof of (2) and (3) (the one given in my Cambridge University Press monograph) is decidedly not along the lines of the Berry paradox. But a few years later I was happy to discover a new and more straightforward proof of (2) and (3) that is along the lines of the Berry paradox!

In addition to working on incompleteness, I have also devoted a great deal of thought to the central idea that can be extracted from my version of the Berry paradox, which is to define the program-size complexity of something to be the size in bits of the smallest program that calculates it. I have developed a general theory dealing with program-size complexity that I call algorithmic information theory (*AIT*).

AIT is an elegant theory of complexity, perhaps the most developed of all such theories. But as von Neumann said, pure mathematics is easy compared to the real world! *AIT* provides the correct complexity concept for metamathematics, but not necessarily for other more practical fields.

Program-size complexity in *AIT* is analogous to entropy in statistical mechanics. Just as thermodynamics gives limits on heat engines, *AIT* gives limits on formal axiomatic systems.

I have recently reformulated *AIT*. Up to now, the best version of *AIT* studied the size of programs in a computer programming language that was not actually usable. Now I have obtained the correct program-size complexity measure from a powerful and easy to use programming language. This language is a version of *LISP*, and I have written an interpreter for it in *C*. I have written a book employing this new approach that is entitled *The Limits of Mathematics*. To automatically obtain this book in LaTeX, send e-mail to "`chao-dyn @ xyz.lanl.gov`" with "`Subject: get 9407003`" or with "`Subject: get 9407009`". For an extended abstract of the book, request "9407010".

So this is what I would like to discuss with Gödel, if I could speak with him now. Of course this is impossible! But thank you very much for giving me the opportunity to tell you about these ideas!

Questions for Future Research

- Find questions in algebra, topology and geometry that are equivalent to determining bits of Ω.
- What is an interesting or natural mathematical question?
- How often is such a question independent of the usual axioms? (I suspect the answer is "Quite often!")
- Show that a classical open question in number theory, such as the Riemann hypothesis, is independent of the usual axioms. (I suspect that this is often the case, but that it cannot be proven.)
- When doing mathematics, should we take incompleteness seriously or is it a red herring? (I believe that we should take incompleteness very seriously indeed.)
- Is mathematics quasi-empirical? In other words, should mathematics be done more like physics is done? (I believe the answer to both questions is "Yes.")

Bibliography

Books:

- G. J. Chaitin, *Information, Randomness & Incompleteness*, second edition, World Scientific, 1990. Errata: on page 26, line 25, "quickly that" should read "quickly than"; on page 31, line 19, "Here one" should read "Here once"; on page 55, line 17, "RI, p. 35" should read "RI, 1962, p. 35"; on page 85, line 14, "1. The problem" should read "1. The Problem"; on page 88, line 13, "4. What is life?" should read "4. What is Life?"; on page 108, line 13, "the table in" should read "in the table in"; on page 117, Theorem 2.3(q), "$H_C(s,t)$" should read "$H_C(s/t)$"; on page 134, line 7, "$\#\{n|H(n) \leq n\} \leq 2^n$" should read "$\#\{k|H(k) \leq n\} \leq 2^n$"; on page 274, bottom line, "n_{4p+4}" should read "$n_{4p'+4}$".

- G. J. Chaitin, *Algorithmic Information Theory,* fourth printing, Cambridge University Press, 1992. Erratum: on page 111, Theorem I0(q), "$H_C(s,t)$" should read "$H_C(s/t)$".
- G. J. Chaitin, *Information-Theoretic Incompleteness,* World Scientific, 1992. Errata: on page 67, line 25, "are there are" should read "are there"; on page 71, line 17, "that case that" should read "the case that"; on page 75, line 25, "the the" should read "the"; on page 75, line 31, "$-\log_2 p - \log_2 q$" should read "$-p\log_2 p - q\log_2 q$"; on page 95, line 22, "This value of" should read "The value of"; on page 98, line 34, "they way they" should read "the way they"; on page 99, line 16, "exactly same" should read "exactly the same"; on page 124, line 10, "are there are" should read "are there".

Recent Papers:

- G. J. Chaitin, "On the number of n-bit strings with maximum complexity," *Applied Mathematics and Computation* **59** (1993), pp. 97–100.
- G. J. Chaitin, "Randomness in arithmetic and the decline and fall of reductionism in pure mathematics," chao-dyn/9304002, *Bulletin of the European Association for Theoretical Computer Science,* No. 50 (June 1993), pp. 314–328.
- G. J. Chaitin, "The limits of mathematics—Course outline & software," chao-dyn/9312006, *IBM Research Report RC-19324,* 127 pp., December 1993.
- G. J. Chaitin, "Randomness and complexity in pure mathematics," *International Journal of Bifurcation and Chaos* **4** (1994), pp. 3–15.
- G. J. Chaitin, "Responses to 'Theoretical Mathematics...'," *Bulletin of the American Mathematical Society* **30** (1994), pp. 181–182.
- G. J. Chaitin, "The Limits of Mathematics," chao-dyn/9407003, IBM Research Report RC-19646, July 1994, 270 pp.
- G. J. Chaitin, "The Limits of Mathematics IV," chao-dyn/9407009, IBM Research Report RC-19671, July 1994, 231 pp.
- G. J. Chaitin, "The Limits of Mathematics (Extended Abstract)," chao-dyn/9407010, IBM Research Report RC-19672, July 1994, 7 pp.

See Also:

- M. Davis, "What is a computation?," in L.A. Steen, *Mathematics Today,* Springer-Verlag, 1978.
- R. Rucker, *Infinity and the Mind,* Birkhäuser, 1982.
- T. Tymoczko, *New Directions in the Philosophy of Mathematics,* Birkhäuser, 1986.
- R. Rucker, *Mind Tools,* Houghton Mifflin, 1987.
- H.R. Pagels, *The Dreams of Reason,* Simon & Schuster, 1988.
- D. Berlinski, *Black Mischief,* Harcourt Brace Jovanovich, 1988.
- R. Herken, *The Universal Turing Machine,* Oxford University Press, 1988.
- I. Stewart, *Game, Set & Math,* Blackwell, 1989.
- G.S. Boolos and R.C. Jeffrey, *Computability and Logic,* third edition, Cambridge University Press, 1989.

- J. Ford, "What is chaos?," in P. Davies, *The New Physics,* Cambridge University Press, 1989.
- J.L. Casti, *Paradigms Lost,* Morrow, 1989.
- G. Nicolis and I. Prigogine, *Exploring Complexity,* Freeman, 1989.
- B.-O. Küppers, *Information and the Origin of Life,* MIT Press, 1990.
- J.L. Casti, *Searching for Certainty,* Morrow, 1991.
- J.A. Paulos, *Beyond Numeracy,* Knopf, 1991.
- L. Brisson and F.W. Meyerstein, *Inventer L'Univers,* Les Belles Lettres, 1991. (English edition in press)
- J.D. Barrow, *Theories of Everything,* Oxford University Press, 1991.
- D. Ruelle, *Chance and Chaos,* Princeton University Press, 1991.
- T. Nørretranders, *Mærk Verden,* Gyldendal, 1991.
- M. Gardner, *Fractal Music, Hypercards and More,* Freeman, 1992.
- P. Davies, *The Mind of God,* Simon & Schuster, 1992.
- J.D. Barrow, *Pi in the Sky,* Oxford University Press, 1992.
- N. Hall, *The New Scientist Guide to Chaos,* Penguin, 1992.
- H.-C. Reichel and E. Prat de la Riba, *Naturwissenschaft und Weltbild,* Hölder-Pichler-Tempsky, 1992.
- I. Stewart, *The Problems of Mathematics,* Oxford University Press, 1992.
- A.K. Dewdney, *The New Turing Omnibus,* Freeman, 1993.
- A.B. Çambel, *Applied Chaos Theory,* Academic Press, 1993.
- K. Svozil, *Randomness & Undecidability in Physics,* World Scientific, 1993.
- J.L. Casti, *Complexification,* HarperCollins, 1994.
- M. Gell-Mann, *The Quark and the Jaguar,* Freeman, 1994.
- T. Nørretranders, *Verden Vokser,* Aschehdoug, 1994.
- S. Wolfram, *Cellular Automata and Complexity,* Addison-Wesley, 1994.
- C. Calude, *Information and Randomness,* Springer-Verlag, 1994.
- J.L. Casti and A. Karlqvist, *Cooperation and Conflict in General Evolutionary Processes,* Wiley, 1995.