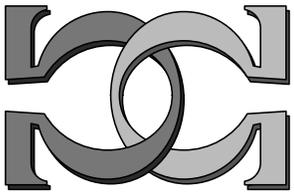
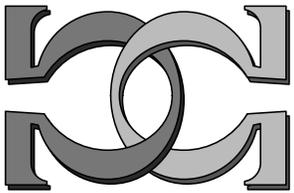
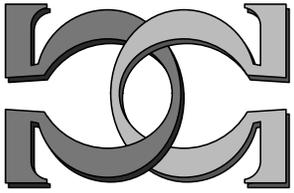
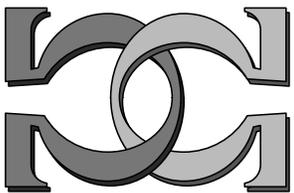


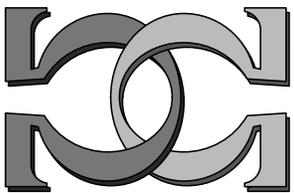
**CDMTCS  
Research  
Report  
Series**



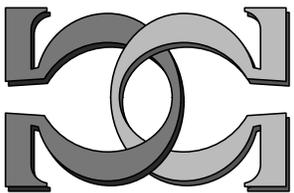
**How Much Information Can  
There Be in a Real Number?**



**G. J. Chaitin**  
IBM Research, Yorktown Heights, USA



CDMTCS-294  
January 2007



Centre for Discrete Mathematics and  
Theoretical Computer Science

# How Much Information Can There Be in a Real Number?

Gregory Chaitin\*

## Abstract

This note gives some information about the magical number  $\Omega$  and why it is of interest. Our purpose is to explain the significance of recent work by Calude and Dinneen attempting to compute  $\Omega$ . Furthermore, we propose measuring human intellectual progress (not scientific progress) via the number of bits of  $\Omega$  that can be determined at any given moment in time using the current mathematical theories.  
*Keywords:* halting problem, halting probability.

## 1 Introduction

A real number corresponds to the length of a line segment that is measured with infinite precision. A rational number has a periodic decimal expansion. For example,

$$\frac{1}{3} = 0.3333333 \dots$$

The decimal expansion of an irrational real number is not periodic. Here are three well-known irrational reals that everyone encounters in high school and college mathematics:  $\sqrt{2}$ ,  $\pi$ , and  $e$ .

Each of these numbers would seem to contain an infinite amount of information, because they have an infinite decimal expansion that never repeats. For example,

$$\pi = 3.1415926 \dots$$

---

\*IBM T. J. Watson Research Center, P. O. Box 218, Yorktown Heights, NY 10598, U.S.A., [chaitin@us.ibm.com](mailto:chaitin@us.ibm.com).

However,  $\pi$  actually only contains a finite amount of information, because there is a small computer program for computing  $\pi$ . Instead of sending someone the digits of  $\pi$ , we can just explain to them how to compute as many digits as they want.

Are there any real numbers that contain an infinite amount of information? Well, clearly, if the successive decimal digits are chosen at random, the resulting stream of digits has no structure, each digit is a complete surprise, and there cannot be an algorithm for computing the number digit by digit.

However, this random sequence of digits is not **useful** information, not at all. It's an infinite amount of completely useless information.

## 2 Borel's Know-It-All Real Number

In 1927, the French mathematician Emile Borel pointed out that there are real numbers which contain an infinite amount of extremely **useful** information. The particular example that he gave is defined like this: Its  $N$ th digit answers the  $N$ th yes/no question in an infinite list of all possible yes/no questions, questions about the weather, the stock market, history, the future, physics, mathematics... Here I am talking about the  $N$ th digit after the decimal point. Borel's number is between zero and one; there is nothing before the decimal point, only stuff after the decimal point. And we can assemble this list of questions because the set of all possible questions is what mathematicians call a countable or a denumerable set.

## 3 Using a Real Number as an Oracle for the Halting Problem

Borel's real number may seem rather unreal, rather fantastic, even though it exists in some Platonic, ideal, conceptual sense. How about a more realistic example, and now let's use base two, not base ten. Well, there is a real  $\Theta$  whose  $N$ th bit tells us whether or not the  $N$ th computer program ever halts. This time we imagine an infinite list of all possible self-contained computer programs—not yes/no questions—and ask which programs will eventually finish running. This is Alan Turing's famous 1936 halting problem.

$\Theta$  doesn't tell us anything about the stock market or history, but it does tell us a great deal about mathematics. Why? Because knowing this number

$\Theta$  would automatically enable us to resolve famous mathematical problems like Fermat's so-called last theorem, which asserts that there are no positive integer solutions for

$$x^N + y^N = z^N$$

with the power  $N$  greater than two.

How can  $\Theta$  enable us to decide if Fermat was right and this equation has no solutions? There is a simple computer program for systematically searching for a solution of Fermat's equation. This program will fail to halt precisely if Fermat's conjecture that there are no solutions is correct.

However, in the case of Fermat's conjecture there is no need to wait for the number  $\Theta$ ; Andrew Wiles now has a proof that there are no solutions. But  $\Theta$  would enable us to answer an infinite number of such conjectures, more precisely, all conjectures that can be refuted by a single counter example that we can search for using a computer.

## 4 $N$ Cases of the Halting Problem is Only $\log_2 N$ Bits of Information

So knowing the answers to individual cases of the halting problem can be valuable information, and  $\Theta$  enables us to answer **all** such problems, but unfortunately not in an optimal way.  $\Theta$  isn't optimal, it is highly redundant, we're wasting lots of bits. Individual answers to the halting problem aren't independent, they're highly correlated.

Why? Because if we are given  $N$  programs, we can determine which ones halt and which ones don't if we merely know **how many** of these  $N$  programs halt, and to know that is only about  $\log_2 N$  bits of information. (Run all  $N$  programs in parallel until precisely the correct number have stopped; the remaining programs will never stop.)

Furthermore,  $\log_2 N$  is much smaller than  $N$  for all sufficiently large values of  $N$ .

So what is the best we can do? Is there an oracle for the halting problem that isn't redundant, that doesn't waste any bits?

## 5 The Halting Probability $\Omega$ is the Most Compact Oracle for the Halting Problem

The best way to pack information about the halting problem into a real number is to know a great many bits of the numerical value of the probability that a program chosen at random will eventually halt. Precisely how do I define this halting probability? Well, the exact definition is a little complicated, and in fact the numerical value of  $\Omega$  depends on the particular computer and the programming language that you pick.

The general idea is that the computer that we are using flips a fair coin to generate each bit of the program, a heads yields a 1, a tails yields a 0, successive coin tosses are independent, and the computer starts running the program right away as it generates these bits.  $\Omega$  is the probability that this process will eventually halt.

More precisely, each  $K$ -bit program  $p$  that halts contributes precisely  $1/2^K$  to the halting probability  $\Omega$ :

$$\Omega = \sum_{p \text{ halts}} 2^{-(\text{the size of } p \text{ in bits})}.$$

Furthermore, to avoid having this sum diverge to infinity, the set of meaningful programs must be a prefix-free set, in other words, no extension of a valid program is a valid program. Then what information theorists call the Kraft inequality applies to the set of all programs and  $\Omega$  is necessarily less than one.

$\Omega$  is a very valuable oracle, because knowing the first  $N$  bits of  $\Omega$  would enable us to resolve the halting problem for all programs up to  $N$  bits in size. No oracle for the halting problem can do better than this.  $\Omega$  is so valuable precisely because it is the most compact way to represent this information. It's the best possible oracle for the halting problem. You get the biggest bang for your buck with each bit!

And because this information is so valuable,  $\Omega$  is maximally unknowable, maximally uncomputable: An  $N$ -bit computer program can compute at most  $N$  bits of  $\Omega$ , and a mathematical theory with  $N$  bits of axioms can enable us to determine at most  $N$  bits of  $\Omega$ . In other words, the bits of  $\Omega$  are incompressible, irreducible information, both logically irreducible and computationally irreducible.

Paradoxically, however, even though  $\Omega$  is packed full of useful information, its successive bits **appear** to be totally unstructured and random, totally

chaotic, because otherwise  $\Omega$  would not be the most compact oracle for the halting problem. If one could predict future bits from past bits, then  $\Omega$  would not be the best possible compression of all the answers to individual cases of Turing's halting problem.

## 6 Measuring Mathematical or Human Intellectual Progress in Terms of Bits of $\Omega$

Counting how many bits of  $\Omega$  our current mathematical theories permit us to know, gives us a way to measure the complexity of our mathematical knowledge as a function of time.  $\Omega$  is infinitely complex, and at any given moment our theories capture at most a finite amount of this complexity. Our minds are finite, not infinitely complex like  $\Omega$ .

But what if we bravely try to compute  $\Omega$  anyway?

## 7 Storming the Heavens: Attempting to Compute the Uncomputable Bits of $\Omega$

This amounts to a systematic attempt to increase the complexity of our mathematical knowledge, and it is precisely what Calude and Dinneen try to do in [1]. As they show, you can start off well enough and indeed determine a few of the initial bits of  $\Omega$ . But as I have tried to explain, the further you go, the more creativity, the more ingenuity is required. To continue making progress, you will eventually need to come up with more and more complicated mathematical principles, novel principles that are not consequences of our current mathematical knowledge.

Will mathematics always be able to advance in this way, or will we eventually hit an insurmountable obstacle? Who knows! What is clear is that  $\Omega$  can never be known in its entirety, but if the growth of our mathematical knowledge continues unabated, each individual bit of  $\Omega$  can eventually be known.

I hope that this note gives some idea why [1] is of interest. (See also [2].) For more on  $\Omega$ , please see my article in *Scientific American* [3] or my book [4]. A more recent paper is my Enriques lecture at the University of Milan in 2006 [5].

## References

- [1] C. S. Calude, M. J. Dinneen, “Exact approximations of  $\Omega$  numbers,” to appear.
- [2] C. S. Calude, E. Calude, M. J. Dinneen, “A new measure of the difficulty of problems,” *Journal of Multiple-Valued Logic and Soft Computing*, in press.
- [3] G. Chaitin, “The limits of reason,” *Scientific American* **294**, No. 3 (March 2006), pp. 74–81.
- [4] G. Chaitin, *Meta Math!*, Pantheon, New York, 2005, *Meta Maths*, Atlantic Books, London, 2006.
- [5] G. Chaitin, “The halting probability  $\Omega$ : Irreducible complexity in pure mathematics,” *Milan Journal of Mathematics* **75** (2007), in press.