

RANDOMNESS AND GÖDEL'S THEOREM

Mondes en Développement,
No. 54–55 (1986), pp. 125–128

G. J. Chaitin

IBM Research Division

Abstract

Complexity, non-predictability and randomness not only occur in quantum mechanics and non-linear dynamics, they also occur in pure mathematics and shed new light on the limitations of the axiomatic method. In particular, we discuss a Diophantine equation exhibiting randomness, and how it yields a proof of Gödel's incompleteness theorem.

Our view of the physical world has certainly changed radically during the past hundred years, as unpredictability, randomness and complexity have replaced the comfortable world of classical physics. Amazingly enough, the same thing has occurred in the world of pure mathematics,

in fact, in number theory, a branch of mathematics that is concerned with the properties of the positive integers. How can an uncertainty principle apply to number theory, which has been called the queen of mathematics, and is a discipline that goes back to the ancient Greeks and is concerned with such things as the primes and their properties?

Following Davis (1982), consider an equation of the form

$$P(x, n, y_1, \dots, y_m) = 0,$$

where P is a polynomial with integer coefficients, and x, n, m, y_1, \dots, y_m are positive integers. Here n is to be regarded as a parameter, and for each value of n we are interested in the set D_n of those values of x for which there exist y_1 to y_m such that $P = 0$. Thus a particular polynomial P with integer coefficients in $m+2$ variables serves to define a set D_n of values of x as a function of the choice of the parameter n .

The study of equations of this sort goes back to the ancient Greeks, and the particular type of equation we have described is called a polynomial Diophantine equation.

One of the most remarkable mathematical results of this century has been the discovery that there is a “universal” polynomial P such that by varying the parameter n , the corresponding set D_n of solutions that is obtained can be any set of positive integers that can be generated by a computer program. In particular, there is a value of n such that the set of prime numbers is obtained. This immediately yields a prime-generating polynomial

$$x \left[1 - (P(x, n, y_1, \dots, y_m))^2 \right],$$

whose set of positive values, as the values of x and y_1 to y_m vary over all the positive integers, is precisely equal to the primes. This is a remarkable result that surely would have amazed Fermat and Euler, and it is obtained as a trivial corollary to a much more general theorem!

The proof that there is such a universal P may be regarded as the culmination of Gödel’s original proof of his famous incompleteness theorem. In thinking about P , it is helpful to regard the parameter n as the Gödel number of a computer program, and to regard the set of solutions x as the output of this computer program, and to think

of the auxiliary variables y_1 to y_m as a kind of multidimensional time variable. In other words,

$$P(x, n, y_1, \dots, y_m) = 0$$

if and only if the n th computer program outputs the positive integer x at time (y_1, \dots, y_m) .

Let us prove Gödel's incompleteness theorem by making use of this universal polynomial P and Cantor's famous diagonal method, which Cantor originally used to prove that the real numbers are more numerous than the integers. Recall that D_n denotes the set of positive integers x for which there exist positive integers y_1 to y_m such that $P = 0$. I.e.,

$$D_n = \{x | (\exists y_1, \dots, y_m) [P(x, n, y_1, \dots, y_m) = 0]\}.$$

Consider the "diagonal" set

$$V = \{n | n \notin D_n\}$$

of all those positive integers n that are not contained in the corresponding set D_n . It is easy to see that V cannot be generated by a computer program, because V differs from the set generated by the n th computer program regarding the membership of n . It follows that there can be no algorithm for deciding, given n , whether or not the equation

$$P(n, n, y_1, \dots, y_m) = 0$$

has a solution. And if there cannot be an algorithm for deciding if this equation has a solution, no fixed system of axioms and rules of inference can permit one to prove whether or not it has a solution. For if there were a formal axiomatic theory for proving whether or not there is a solution, given any particular value of n one could in principle use this formal theory to decide if there is a solution, by searching through all possible proofs within the formal theory in size order, until a proof is found one way or another. It follows that no single set of axioms and rules of inference suffice to enable one to prove whether or not a polynomial Diophantine equation has a solution. This is a version of Gödel's incompleteness theorem.

What does this have to do with randomness, uncertainty and unpredictability? The point is that the solvability or unsolvability of the equation

$$P(n, n, y_1, \dots, y_m) = 0$$

in positive integers is in a sense mathematically uncertain and jumps around unpredictably as the parameter n varies. In fact, it is possible to construct another polynomial P' with integer coefficients for which the situation is much more dramatic.

Instead of asking whether $P' = 0$ can be solved, consider the question of whether or not there are infinitely many solutions. Let D'_n be the set of positive integers x such that

$$P'(x, n, y_1, \dots, y_m) = 0$$

has a solution. P' has the remarkable property that the truth or falsity of the assertion that the set D'_n is infinite, is completely random. Indeed, this infinite sequence of true/false values is indistinguishable from the result of successive independent tosses of an unbiased coin. In other words, the truth or falsity of each of these assertions is an independent mathematical fact with probability one-half! These independent facts cannot be compressed into a smaller amount of information, i.e., they are irreducible mathematical information. In order to be able to prove whether or not D'_n is infinite for the first k values of the parameter n , one needs at least k bits of axioms and rules of inference, i.e., the formal theory must be based on at least k independent choices between equally likely alternative assumptions. In other words, a system of axioms and rules of inference, considered as a computer program for generating theorems, must be at least k bits in size if it enables one to prove whether or not D'_n is infinite for $n = 1, 2, 3, \dots, k$.

This is a dramatic extension of Gödel's theorem. Number theory, the queen of mathematics, is infected with uncertainty and randomness! Simple properties of Diophantine equations escape the power of any particular formal axiomatic theory! To mathematicians, accustomed as they often are to believe that mathematics offers absolute certainty, this may appear to be a serious blow. Mathematicians often deride the non-rigorous reasoning used by physicists, but perhaps they have something to learn from them. Physicists know that new

experiments, new domains of experience, often require fundamentally new physical principles. They have a more pragmatic attitude to truth than mathematicians do. Perhaps mathematicians should acquire some of this flexibility from their colleagues in the physical sciences!

Appendix

Let me say a few words about where P' comes from. P' is closely related to the fascinating random real number which I like to call Ω . Ω is defined to be the halting probability of a universal Turing machine when its program is chosen by coin tossing, more precisely, when a program n bits in size has probability 2^{-n} [see Gardner (1979)]. One could in principle try running larger and larger programs for longer and longer amounts of time on the universal Turing machine. Thus if a program ever halts, one would eventually discover this; if the program is n bits in size, this would contribute 2^{-n} more to the total halting probability Ω . Hence Ω can be obtained as the limit from below of a computable sequence $r_1 \leq r_2 \leq r_3 \leq \dots$ of rational numbers:

$$\Omega = \lim_{k \rightarrow \infty} r_k;$$

this sequence converges very slowly, in fact, in a certain sense, as slowly as possible. The polynomial P' is constructed from the sequence r_k by using the theorem that “a set of tuples of positive integers is Diophantine if and only if it is recursively enumerable” [see Davis (1982)]: the equation

$$P'(k, n, y_1, \dots, y_m) = 0$$

has a solution if and only if the n th bit of the base-two expansion of r_k is a “1”. Thus D'_n , the set of x such that

$$P'(x, n, y_1, \dots, y_m) = 0$$

has a solution, is infinite if and only if the n th bit of the base-two expansion of Ω is a “1”. Knowing whether or not D'_n is infinite for $n = 1, 2, 3, \dots, k$ is therefore equivalent to knowing the first k bits of Ω .

References

- G. J. Chaitin (1975), “Randomness and mathematical proof,” *Scientific American* 232 (5), pp. 47–52.
- M. Davis (1978), “What is a computation?” , *Mathematics Today: Twelve Informal Essays*, L. A. Steen, Springer-Verlag, New York, pp. 241–267.
- D. R. Hofstadter (1979), *Gödel, Escher, Bach: an Eternal Golden Braid*, Basic Books, New York.
- M. Gardner (1979), “The random number Ω bids fair to hold the mysteries of the universe,” Mathematical Games Dept., *Scientific American* 241 (5), pp. 20–34.
- G. J. Chaitin (1982), “Gödel’s theorem and information,” *International Journal of Theoretical Physics* 22, pp. 941–954.
- M. Davis (1982), “Hilbert’s Tenth Problem is Unsolvable,” *Computability & Unsolvability*, Dover, New York, pp. 199–235.