Fermat's Last Theorem and Chaoticity

Elena Calude (Massey University)

July 2010

Aim

We apply the computational method we developed in two recent articles to show that proving the chaoticity of a dynamical system is equivalent to proving the Fermat's last theorem, which is a low complexity computational problem.

Dynamic systems

The dynamical system concept is a mathematical formalisation for any fixed "rule" which describes the time dependence of a point's position in its ambient space.

In an abstract setting, a dynamic system on a space X is a function

$$f : X \to X.$$

The orbit of a point $x \in X$ is given by the sequence

$$x, f(x), f^2(x) = f(f(x)), \ldots, f^n(x), \ldots$$

Chaotic dynamic systems

A dynamic system is chaotic if small differences in initial conditions may yield widely diverging outcomes, making long-term prediction impossible in general.

Chaotic behaviour was observed in a variety of systems including electrical circuits, lasers, oscillating chemical reactions, fluid dynamics, and mechanical and magneto-mechanical devices, etc.

Observations of chaotic behaviour in nature include changes in weather, the dynamics of satellites in the solar system, and population growth in ecology.

Fermat's last theorem

There are no positive integers x, y, z satisfying the equation $x^n + y^n = z^n$, for any integer value $n > 2$.

The result was conjectured by Pierre de Fermat in 1637, and it was proven in 1995 by A. Wiles.

Da Costa, Doria and Amaral theorem

One can effectively construct the expression describing a two-dimensional Hamiltonian system $\mathcal{H}$ such that proving that $\mathcal{H}$ is chaotic is equivalent to proving Fermat's last theorem.

Cavines, Richardson, Wang lemma

For every polynomial $P(x_1, x_2, \ldots, x_n) \in \mathcal{P}_n$ there exists $f_P(x_1, x_2, \ldots, x_n) \in F(\mathcal{E}_n)$ (the set of functions represented by the expressions in $\mathcal{E}_n$) such that the following conditions are equivalent.

1. There are naturals $x_1, x_2, \ldots, x_n$ such that $P(x_1, x_2, \ldots, x_n) = 0$.
2. There are reals $x_1, x_2, \ldots, x_n$ such that $f_P(x_1, x_2, \ldots, x_n) = 0$.
3. There are reals $x_1, x_2, \ldots, x_n$ such that $f_P(x_1, x_2, \ldots, x_n) \leq 1$.

The complexity

To every Π_1–problem $\pi = \forall n P(n)$ we associate the algorithm

$$\Pi_P = \inf\{n \,:\, P(n) = \text{ false}\}$$

which systematically searches for a counter-example for π.

There are many programs (for a universal self-delimiting Turing machine U) which implement Π_P; without loss of generality, any such program will be denoted also by Π_P.

The complexity (with respect to U) of a Π_1–problem π is defined by the length of the smallest-length program (for U) Π_P—defined as above—where minimisation is calculated for all possible representations of π as $\pi = \forall n P(n)$:

$$C_U(\pi) = \min\{|\Pi_P| \,:\, \pi = \forall n P(n)\}.$$

Complexity classes

Because the complexity C_U is incomputable, we can work only with upper bounds for C_U. As the exact value of C_U is not important, we classify Π_1–problems into the following classes:

$$\mathfrak{C}_{U,n} = \{\pi \,:\, \pi \text{ is a } \Pi_1\text{–problem}, C_U(\pi) \leq n \text{ kbit}\}.$$

Fermat's last theorem is a Π_1–problem.

Complexity of Fermat's last theorem

0. =a,a,14 1. &e,0 2. &d,1 3. +e,1 4. &f,0 5. &g,0 6. +f,1 7. +g,a 8. =f,d,10 9. =a,a,6 10. &d,g 10. &d,g 11. =e,b,13 12. =a,a,3 13. =a,a,c 14. &B,4 15. +B,1 16. &n,3 17. +n,1 18. =n,B,15 19. &z,3 20. +z,1 21. =z,B,17 22. &x,3 23. +x,1 24. =x,z,20 25. &y,3 26. +y,1 27. =y,z,23 28. &b,n 29. &a,x 30. &c,32 31. =a,a,1 32. &E,d 33. &a,y 34. +c,4 35. =a,a,1 36. +E,d 37. &a,z 38. +c,4 39. =a,a,1 40. =E,a,42 41. =a,a,26 42. %

The size of the register machine program for Fermat's last theorem is 597 bits Fermat's last theorem is in $\mathfrak{C}_{U,1}$.

One can effectively construct the expression describing a two-dimensional Hamiltonian system $\mathcal{H}$ such that proving that $\mathcal{H}$ is chaotic is equivalent to proving a problem in class $\mathfrak{C}_{U,1}$.

Fermat's last theorem complexity revisited

Is the excruciating long proof of the Fermat's last theorem a good indication that the corresponding two-dimensional Hamiltonian system is extremely complex?

The result proven in Hartmanis which shows that one can (effectively) find infinite sets of trivially true theorems which require as long proofs as the hardest theorems—indicates that the length of a proof may not be an adequate complexity measure in this case.

In Hartmanis' words of:

> *In every formalization, infinite sets of trivial theorems will require very long proofs. . . . It also gives a warning that a necessarily long proof in a formal system does not certify that the result is non-trivial.*

References

C. S. Calude, E. Calude. Evaluating the Complexity of Mathematical Problems. Part 1 *Complex Systems*, 18, 3 (2009), 267–285.

C.S. Calude, Elena Calude. Evaluating the Complexity of Mathematical Problems. Part 2, *Complex Systems* 18, 4 (2010), 387–401.

C. S. Calude, E. Calude, M. J. Dinneen. A new measure of the difficulty of problems, *Journal for Multiple-Valued Logic and Soft Computing* 12 (2006), 285–307.

N. C. A. da Costa, F. A. Doria, A. F. Furtado do Amaral. Dynamical system where proving chaos is equivalent to proving Fermat's conjecture, *International Journal of Theoretical Physics* 32, 11 (1993), 2187–2206.

J. Hartmanis. On effective speed-up and long proofs of trivial theorems in formal theories, *Informatique Théorique et Applications* 10 (1976), 29–38.