The Complexity of Mathematical Problems

C. S. Calude (UoA) and E. Calude (Massey U)

In Honour of Eric Goles 60th Birhday

Valparaiso, November 2011

Do the following statements

Do the following statements

- the four colour theorem,

Do the following statements

- the four colour theorem,
- Fermat's great theorem,

Do the following statements

- the four colour theorem,
- Fermat's great theorem,
- the Riemann hypothesis,

Do the following statements

- the four colour theorem,
- Fermat's great theorem,
- the Riemann hypothesis,
- the Collatz's conjecture?

Do the following statements

- the four colour theorem,
- Fermat's great theorem,
- the Riemann hypothesis,
- the Collatz's conjecture?

share a common mathematical property?

Do the following statements

- the four colour theorem,
- Fermat's great theorem,
- the Riemann hypothesis,
- the Collatz's conjecture?

share a common mathematical property?

And, if there is such a property, how can we use it for a better understanding of these statements?

Universality theorem. There exists (and can be constructed) a (Turing) machine U—called *universal*—such that for every machine V there exists a constant $c = c_{U,V}$ such that for every program σ there exists a σ' for which the following two conditions hold:

- $U(\sigma') = V(\sigma)$,
- $|\sigma'| \leq |\sigma| + c$.

The **halting problem** for a machine V is the function Λ_V defined by

$$\Lambda_V(\sigma) = \begin{cases} 1, & \text{if } V(\sigma) = \infty, \\ 0, & \text{otherwise}. \end{cases}$$

The **halting problem** for a machine V is the function Λ_V defined by

$$\Lambda_V(\sigma) = \begin{cases} 1, & \text{if } V(\sigma) = \infty, \\ 0, & \text{otherwise} . \end{cases}$$

Undecidability theorem. If U is universal, then Λ_U is incomputable, i.e. the halting problem for a universal machine is undecidable.

Π_1–problems

A problem π of the form

$$\forall \sigma P(\sigma),$$

where P is a computable predicate is called a Π_1–*problem*.

Π_1–problems

A problem π of the form

$$\forall \sigma P(\sigma),$$

where P is a computable predicate is called a Π_1–*problem*.

- Any Π_1–problem is finitely refutable.

Π_1–problems

A problem π of the form

$$\forall \sigma P(\sigma),$$

where P is a computable predicate is called a Π_1–*problem*.

- Any Π_1–problem is finitely refutable.
- For every Π_1–problem $\pi = \forall \sigma P(\sigma)$ we associate the program

$$\sigma_\pi = \inf\{n : P(n) = \text{ false}\}$$

which satisfies:

$$\pi \text{ is true iff } U(\sigma_\pi) = \infty.$$

Π_1–problems

A problem π of the form

$$\forall \sigma P(\sigma),$$

where P is a computable predicate is called a Π_1–*problem*.

- Any Π_1–problem is finitely refutable.
- For every Π_1–problem $\pi = \forall \sigma P(\sigma)$ we associate the program

  $$\sigma_\pi = \inf\{n : P(n) = \text{ false}\}$$

  which satisfies:

  $$\pi \text{ is true iff } U(\sigma_\pi) = \infty.$$

- Solving the halting problem for U solves all Π_1–problems.

Examples

The problems

- the four colour theorem,

Examples

The problems

- the four colour theorem,
- Fermat's great theorem,

Examples

The problems

- the four colour theorem,
- Fermat's great theorem,
- the Riemann hypothesis,

Examples

The problems

- the four colour theorem,
- Fermat's great theorem,
- the Riemann hypothesis,
- the Collatz's conjecture

Examples

The problems

- the four colour theorem,
- Fermat's great theorem,
- the Riemann hypothesis,
- the Collatz's conjecture

are all Π_1–problems.

Examples

The problems

- the four colour theorem,
- Fermat's great theorem,
- the Riemann hypothesis,
- the Collatz's conjecture

are all Π_1–problems.

Of course, not all problems are Π_1–problems. For example, the twin prime conjecture.

Complexity

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

Complexity

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

Invariance theorem. If U, U' are universal, then there exists a constant $c = c_{U,U'}$ such that for all $\pi = \forall n P(n)$, P computable:

$$|C_U(\pi) - C_{U'}(\pi)| \leq c.$$

Complexity

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

Invariance theorem. If U, U' are universal, then there exists a constant $c = c_{U,U'}$ such that for all $\pi = \forall n P(n)$, P computable:

$$|C_U(\pi) - C_{U'}(\pi)| \leq c.$$

Incomputability theorem. If U is universal, then C_U is incomputable.

Because of the incomputability theorem, we work 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:

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

Some Results

- $\mathfrak{C}_{U,1}$: *Legendre's conjecture* (there is a prime number between n^2 and $(n+1)^2$, for every positive integer n), *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 $n > 2$) and *Goldbach's conjecture* (every even integer greater than 2 can be expressed as the sum of two primes)

Some Results

- $\mathfrak{C}_{U,1}$: *Legendre's conjecture* (there is a prime number between n^2 and $(n+1)^2$, for every positive integer n), *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 $n > 2$) and *Goldbach's conjecture* (every even integer greater than 2 can be expressed as the sum of two primes)
- $\mathfrak{C}_{U,2}$: *Dyson's conjecture* (the reverse of a power of two is never a power of five)

Some Results

- $\mathfrak{C}_{U,1}$: *Legendre's conjecture* (there is a prime number between n^2 and $(n+1)^2$, for every positive integer n), *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 $n > 2$) and *Goldbach's conjecture* (every even integer greater than 2 can be expressed as the sum of two primes)
- $\mathfrak{C}_{U,2}$: *Dyson's conjecture* (the reverse of a power of two is never a power of five)
- $\mathfrak{C}_{U,3}$: *the Riemann hypothesis* (all non-trivial zeros of the Riemann zeta function have real part 1/2)

Some Results

- $\mathfrak{C}_{U,1}$: *Legendre's conjecture* (there is a prime number between n^2 and $(n+1)^2$, for every positive integer n), *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 $n > 2$) and *Goldbach's conjecture* (every even integer greater than 2 can be expressed as the sum of two primes)
- $\mathfrak{C}_{U,2}$: *Dyson's conjecture* (the reverse of a power of two is never a power of five)
- $\mathfrak{C}_{U,3}$: *the Riemann hypothesis* (all non-trivial zeros of the Riemann zeta function have real part 1/2)
- $\mathfrak{C}_{U,4}$ *the four colour theorem* (the vertices of every planar graph can be coloured with at most four colours so that no two adjacent vertices receive the same colour)

More Results and Open Questions

- $\mathfrak{C}_{U,5}$: ?

More Results and Open Questions

- $\mathfrak{C}_{U,5}$: ?
- $\mathfrak{C}_{U,6}$: ?

More Results and Open Questions

- $\mathfrak{C}_{U,5}$: ?
- $\mathfrak{C}_{U,6}$: ?
- $\mathfrak{C}_{U,7}$: *Euler's integer partition theorem* (the number of partitions of an integer into odd integers is equal to the number of partitions into distinct integers).

- $\mathfrak{C}_{U,5}$: ?
- $\mathfrak{C}_{U,6}$: ?
- $\mathfrak{C}_{U,7}$: *Euler's integer partition theorem* (the number of partitions of an integer into odd integers is equal to the number of partitions into distinct integers).
- In which class is *the Collatz conjecture*? (given any positive integer a_1 there exists a natural N such that $a_N = 1$, where

$$a_{n+1} = \begin{cases} a_n/2, & \text{if } a_n \text{ is even,} \\ 3a_n + 1, & \text{otherwise}. \end{cases} \Bigg)$$

Inductive Complexity and Complexity Classes of First Order

By transforming each program Π_P for U into a program $\Pi_P^{ind,1}$ for U^{ind} (U working in "inductive mode") we can define the inductive complexity of first order by

$$C_U^{ind,1}(\pi) = \min\{|\Pi_P^{ind,1}| : \pi = \forall n P(n)\},$$

By transforming each program Π_P for U into a program $\Pi_P^{ind,1}$ for U^{ind} (U working in "inductive mode") we can define the inductive complexity of first order by

$$C_U^{ind,1}(\pi) = \min\{|\Pi_P^{ind,1}| : \pi = \forall n P(n)\},$$

the inductive complexity classes of order one by

$$\mathfrak{C}_{U,n}^{ind,1} = \{\pi : \pi \text{ is a } \Pi_1\text{–statement}, C_U^{ind,1}(\pi) \le n \text{ kbit}\},$$

By transforming each program Π_P for U into a program $\Pi_P^{ind,1}$ for U^{ind} (U working in "inductive mode") we can define the inductive complexity of first order by

$$C_U^{ind,1}(\pi) = \min\{|\Pi_P^{ind,1}| : \pi = \forall n P(n)\},$$

the inductive complexity classes of order one by

$$\mathfrak{C}_{U,n}^{ind,1} = \{\pi : \pi \text{ is a } \Pi_1\text{–statement}, C_U^{ind,1}(\pi) \leq n \text{ kbit}\},$$

and prove that

$$\mathfrak{C}_{U,n} = \mathfrak{C}_{U,n}^{ind,1}.$$

Inductive Complexity and Complexity Classes of Higher Orders

By allowing inductive programs of order 1 as routines we get inductive programs of order 2, so we can define the inductive complexity of second order (for more complex problems)

$$C_U^{ind,2}(\rho) = \min\{|M_R^{ind,2}| \,:\, \rho = \forall n \exists i R(n,i)\},$$

By allowing inductive programs of order 1 as routines we get inductive programs of order 2, so we can define the inductive complexity of second order (for more complex problems)

$$C_U^{ind,2}(\rho) = \min\{|M_R^{ind,2}| : \rho = \forall n \exists i R(n,i)\},$$

and the inductive complexity class of second order:

$$\mathfrak{C}_{U,n}^{ind,2} = \{\rho : \rho = \forall n \exists i R(n,i), C_U^{ind,2}(\rho) \leq n \text{ kbit}\}.$$

Inductive Complexity and Complexity Classes of Higher Orders

By allowing inductive programs of order 1 as routines we get inductive programs of order 2, so we can define the inductive complexity of second order (for more complex problems)

$$C_U^{ind,2}(\rho) = \min\{|M_R^{ind,2}| : \rho = \forall n \exists i R(n,i)\},$$

and the inductive complexity class of second order:

$$\mathfrak{C}_{U,n}^{ind,2} = \{\rho : \rho = \forall n \exists i R(n,i), C_U^{ind,2}(\rho) \leq n \text{ kbit}\}.$$

The Collatz conjecture is in the class $\mathfrak{C}_{U,3}^{ind,2}$.

Two open problems

What is the complexity of

Two open problems

What is the complexity of

- P vs NP problem?

Two open problems

What is the complexity of

- P vs NP problem?
- Poincaré's conjecture?

Thank you

Thank you

VIVE ERIC!