When does a problem have a solution: A logician and computability-theorist’s view

Rod Downey
Victoria University
Wellington
New Zealand

Wellington, May 2009
THANKS

- Supported by the Marsden Fund of New Zealand.
- The New Zealand Institute of Mathematics and its Applications.
From a set of basic instructions (ingredients) specify a mechanical method to obtain the desired result.

Already you can see that I plan to be sloppy, but you should try to get the feel of the subject.

I will try to have a general overview but will talk about some of my own work. Not to say that my work is the most important, but that I actually know something about it!
When does a problem have a solution: A logician and computability-theorist’s view
When does a problem have a solution: A logician and computability-theorist's view

Cream Fritters

READY TRAY

Serves 4 to 6

4 egg yolks
¼ cup sugar
½ cup flour
Salt to taste
4 cups milk, scalded
1 teaspoon grated orange or lemon rind
1 egg, beaten

Breadcrumbs
2 tablespoons oil
2 tablespoons butter
Powdered sugar
2 tablespoons brandy or rum

Beat egg yolks and sugar in top of double boiler. Cook over low heat, stirring with wooden spoon until slightly thickened. Mix in ¼ cup flour, salt and gradually add milk. Simmer, stirring, until very thick. At no time allow to boil. Blend in rind.

Rinse a square dish or pan with cold water and pour in mixture to a depth of 2 inches. Chill until firm. Cut into squares or rectangular pieces 2 inches long. Dip in remaining flour, in egg and then in breadcrumbs. Brown gently on both sides in hot oil and butter. Serve sprinkled with sugar, and flame with heated brandy or rum.

Fried Ricotta

READY TRAY

Serves 8

½ pound macaroons
1 pound ricotta cheese
Pinch cinnamon
3 eggs

Breadcrumbs
¾ pound butter
Powdered sugar
Brandy
From a set of basic instructions (ingredients) specify a mechanical method to obtain the desired result.
The greatest common divisor of two numbers \( x \) and \( y \) is the biggest number that is a factor of both.

For instance, the greatest common divisor, \( \text{gcd}(4,8) \) is 4. \( \text{gcd}(6,10)=2; \text{gcd}(16,13)=1. \)

Euclid, or perhaps Team Euclid, (around 300BC) devised what remains the “best” algorithm for determining the gcd of two numbers.
Euclid’s Algorithm

To find gcd(1001, 357).

$1001 = 357 \cdot 2 + 287$

$357 = 287 \cdot 1 + 70$

$287 = 70 \cdot 4 + 7$

$70 = 7 \cdot 10$

$7 = \text{gcd}(1001, 357)$. 
Ingredients: numbers, $+, -, \times, \div$, division.
Operations: Combine in sensible ways.
Another Example

At school one sees the following algorithm for solving the quadratic equation.

\[ ax^2 + bx + c = 0. \]

The solutions are \( \frac{-b + \sqrt{b^2 - 4ac}}{2a} \) and \( \frac{-b - \sqrt{b^2 - 4ac}}{2a} \).

Example 4 \( x^2 - 5x + 1 = 0 \) gives \( \frac{5 + \sqrt{5^2 - 4 \cdot 1}}{2 \cdot 4} \) which equals 1; and \( \frac{5 - \sqrt{5^2 - 4 \cdot 4}}{2 \cdot 4} \) which equals \( \frac{1}{4} \).
Ingredients: numbers, $+, -, \times, \div, \sqrt{\cdot}$, maybe cube roots, powers etc.

Operations: Combine in sensible ways.
Can we do the same for degree 3, the “cubic”

\[ ax^3 + bx^2 + cx + d = 0, \]

what about degree 4, etc.

This was one of the many questions handed to us by the Greeks.

The answer is yes for degree 3 and degree 4.
For degree 3 this was first proven by Ferro (1500).
Ferro left it to his son-in-law Nave and pupil Fiore.
Fiore challenged Tartaglia (in 1535) who then re-discovered the solution with a few days to spare, leaving Foire in ignomy.
Galo Fontana (Tartaglia), who discovered how to solve cubic
For degree 3 this was first proven by Ferro (1500).
Ferro left it to his son-in-law Nave and pupil Fiore.
Fiore challenged Tartaglia (in 1535) who then re-discovered the solution with a few days to spare, leaving Foire in ignomy.
Tartaglia also kept it secret, but told Cardano, who promised by his Christian faith to keep it secret, but....
in 1545 Cardano published it in his great text *Ars Magna*
Additionally Cardano published how to extend to degree 4, being discovered by a student Ferrari, (of whom the car company is surely named).
Figure 4: Title page of Cardano's *Ars Magna*.
square roots being chosen so that
\[ \forall -y_1 \times \forall -y_2 \times \forall -y_3 = -q. \]

22 Cardano, the first to publish solutions of cubic and quartic equations.
Finally, in 1823, a young Norwegian mathematician, Abel proved that there is no recipe using the given ingredients for the degree 5 case, the quintic.
When does a problem have a solution: A logician and computability-theorist's view
Finally, in 1823, a young Norwegian mathematician, Abel proved that there is no recipe using the given ingredients for the degree 5 case, the quintic.

(The paper was called “Memoir on algebraic purifications...” rather than “Memoir on algebraic equations...” due to a typsetting error.)

(My favourite error in one of my own papers referred to a journal “Annals of Mathematical Logic” as “Animals of Mathematical Logic.” It made me think of some of my colleagues!)

Nobody believed him, for a long time. (There had been an earlier announcement by Ruffini, which contained “gaps”.)
Evariste Galois (1811-32) eventually gave a general methodology for deciding if a given degree $n$ equation admits a solution with the ingredients described.
When does a problem have a solution: A logician and computability-theorist's view
**Figure 8:** "I have no time" (*je n’ai pas le temps*) above deleted paragraph in lower left corner. But consider the context.
Evariste Galois (1811-32) eventually gave a general methodology for deciding if a given degree $n$ equation admits a solution with the ingredients described.

This work laid the basis for group theory.

Galois method is to associate a group with each equation, so that the equation is solvable in terms of the given ingredients (arithmetic operations and radicals) iff the group has a certain structure on its subgroups. This is one of the gems of mathematics.
It is not true to say that the quintic has no solution, just none with the given ingredients.

We can add some new operations “elliptic functions” and show that there is a method of solving the general degree \( n \) equation.

These operations are “mechanical” so there is an algorithm for solving all such equations.
David Hilbert, 1900, working from a background of 19th century determinism basically asked the question of whether mathematics could be finitely “mechanized”.
When does a problem have a solution: A logician and computability-theorist's view
The first three problems concerned the foundations of mathematics:

1. To prove Cantor’s “continuum hypothesis” that any set of real numbers can be put into one-to-one correspondence either with the set of natural numbers or with the set of all real numbers (i.e., the continuum).
2. To investigate the consistency of the arithmetic axioms.
3. To axiomatize those physical sciences in which mathematics plays an important role.
4. “So far we have considered only questions concerning the foundations of the mathematical sciences. Indeed, the study of the foundations of a science is always particularly attractive, and the testing of these foundations will always be among the foremost problems of the investigator. Weierstrass said, ‘The final objective always to be kept in mind is to arrive at a correct understanding of the foundations. . . . But to make any progress in the sciences the study of individual problems is, of course, indispensable.’ In fact, a thorough understanding of its special theories is necessary to the successful treatment of the foundations of the science. Only that architect is in the position to lay a sure foundation for a structure who knows its purpose thoroughly and in detail.”

The next four problems were selected from arithmetic and algebra:

5. To establish the transcendence, or at least the irrationality, of certain numbers.
6. To prove the correctness of an extremely important statement by Riemann that the zeros of the function known as the “zeta function” all have the real part 1/2, except the well known negative integral real zeros.
7. To show the impossibility of the solution of the general equation of the 7th degree by means of functions of only two arguments.
8. To conduct a thorough investigation of the relative position of the separate branches which a plane algebraic curve of 8th order can have when their number is the maximum . . . and the corresponding investigation as to the number, form, and position of the sheets of an algebraic surface in space.

The last three problems came from the theory of functions:

9. To determine whether the solutions of “regular” problems in the calculus of variations are necessarily analytic.
10. To show that there always exists a linear differential equation of the Fuchsian class with given singular points and monodromic group.
11. To generalize a theorem proved by Poincaré to the effect that it is always possible to uniformize any algebraic relation between two variables by the use of automorphic functions of one variable.

“The problems mentioned,” Hilbert told his audience, “are merely samples of problems; yet they are sufficient to show how rich, how manifold and how extensive the mathematical science is today; and the question is urged upon us whether mathematics is doomed to the fate of those other
David Hilbert, 1900, working from a background of 19th century determinism basically asked the question of whether mathematics could be finitely “mechanized”.

Can we create an algorithm, a machine, into which one feeds a statement about mathematics or at least in a reasonable “formal system” and from the other end a decision emerges: true or false.

Or, for a given formal system, can we produce a machine that would eventually emit all the “truths” of that system.

Hilbert also proposed that we should prove the consistency of various formal systems of mathematics.
It is not important what this is, save to say the type envisioned would be a bunch of axioms, saying things like

- for all numbers $x$, $x+1$ exists,
- for all numbers $x$ and $y$ $x + y = y + x$,
- and other “obvious truths.”
- plus rules of inference, like “if whenever $P$ is true then $Q$ is true, and whenever $Q$ is true then $R$ is true; then whenever $P$ is true $R$ is true.”
- induction.
Hilbert’s dreams were forever shattered by a young mathematician, Kurt Gödel.
When does a problem have a solution: A logician and computability-theorist’s view
Hilbert’s dreams were forever shattered by a young mathematician, Kurt Gödel.

He proved the two *incompleteness* theorems.

The first incompleteness theorem says that any sufficiently rich formal system has statements expressible in the system true of the system, but cannot be proven in the system.

Secondly no sufficiently rich formal system can prove its own consistency.

The collective intuition of a generation of mathematicians was wrong.
Some rich systems are decidable by mechanical methods.

For example, Euclidian geometry. (Tarski, using quantifier elimination, and inventing model theory).
Gödel’s results had only weak penetration into the consciousnesses of so-called “working mathematicians”, and far too much penetration into that of would-be philosophers and physicists.

There are definitely now known “mathematical incompleteness of various systems”

Here is one example: Kruskal’s Theorem says that finite trees are well-partially ordered by topological embedding. (No infinite antichain)

(Harvey Friedman) For all $k$ there is an $n$ so large that if \( \{ T_i : i \leq n \} \) are trees with $|T_i| < k \cdot i$ then for some $i < j$, $T_i$ topologically embeds into $T_j$.

This is statable in PA but not provable in any system that essentially does not prove the existence of uncountable sets. Friedman has examples equivalent to the existence of “Mahlo Cardinals” (i.e. their truth is equivalent to deciding what colour cheese the moon is made of).
Around the same time, various people were working on formalizing what we might mean by “mechanical method.” (such as the above)
Plate 3. The analytical engine
Around the same time, various people were working on formalizing what we might mean by “mechanical method.” (such as the above)

There were various models proposed, “lambda calculus” (Church) “partial recursive functions (Kleene)”

The convincing model was that of Turing which are now called Turing Machines.

Church’s Thesis “All mechanically computable processes on the numbers can be simulated on a Turing Machine”
Worked on Code cracking in the 2nd world war. (Enigma machine)
The Enigma Machine, employed by the Germans to encrypt classified and sensitive messages during World War II. (HultonArchive/Getty Images)
When does a problem have a solution: A logician and computability-theorist's view
The von Neumanns starting the descent into the Grand Canyon on an excursion in the late 1940s: Klari, with visor, is fourth from front; Johnny, bareheaded and in city suit, is last, on the only mule facing the wrong way.
Worked on Code cracking in the 2nd world war. (Enigma machine)
His fundamental paper, was part of the inspiration for the first computers, and strongly influenced John von Neumann.
Much work e.g. on Colossus only recently declassified.
Also the foundations of numerical analysis and ill-conditioning.
Using the fact that all Turing machines can be enumerated we can use a beautiful argument of Cantor about differing sizes of infinite sets(!) to show that there is no algorithm to decide to following question.

INPUT Turing machine number $x$ and an input $y$.
QUESTION Does the machine $x$ halt on input $y$. 

A BASIC UNDECIDABLE QUESTION
(Proof. Suppose that we could decide this algorithmically. We can then use the decision procedure to construct a machine $M$ that halts on input $n$ if $T_n$ does not halt on input $n$, and our machine $M$ does not halt if machine $T_n$ does halt on input $n$. Then $M$ would be some machine $T_m$, but then $T_m(m)$ halts if and only if $M(m)$ halts iff $T_m(m)$ does not halt....)

We code this problem into others.
Example- Conways Theorem

- Collatz-type functions. $f(x) = \frac{x}{2}$ if $x$ is even, and $f(x) = 3x + 1$ if $x$ odd.

- e.g. $f(3) = 10$ $f(f(3)) = 5$, get the sequence, 3,10,5,16,8,4,2,1

- Do you always get to 1? (Still open)

- General type of question: e.g $g(x) = \frac{1}{2}x$ if $x$ divisible by 4, $g(x) = 5x - 1$ if $x$ has remainder 1 when divided by 4, etc.

- John Conway (1980’s) showed that there is no general algorithm to decide

INPUT A system like the above, and a number $x$.

QUESTION Does $x$ get back to 1?
WANG TILES

- INPUT a set of square coloured tiles of the same size. Only same colour borders next to one another.
- QUESTION Can an initial configuration be extended to colour the plane?
- Wang in the 60’s showed that there is no algorithm to decide this.
Hilbert’s 10th problem

- INPUT A polynomial $P$ in variables $x_1, \ldots, x_n$
- QUESTION Is there a positive solution to the equation $P = 0$?
- Matijasevich, after Julia Robinson in the 70’s showed there is no algorithm to decide such questions.
- But there is now a polynomial whose only positive rational zeroes are the primes!
This shows myself, Julia Robinson, Raphael Robinson, and my wife.
\[ Q(a, \ldots, z) = (k + 2) \{ 1 - [wz + h + j - q]^2 \} \]
- \[ (gk + 2g + k + 1)(h + j) + h - z \]^2
- \[ 2n + p + q + z - e \]^2 - \[ 16(k + 1)^3(k + 2)(n + 1)^2 + 1 - f^2 \]^2
- \[ e^3(e + 2)(a + 1)^2 + 1 - o^2 \]^2 - \[ (a^2 - 1)y^2 + 1 - x^2 \]^2
- \[ 16r^2y^4(a^2 - 1) + 1 - u^2 \]^2
- \[ ((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2 \]^2
- \[ n + 1 + v - y \]^2
- \[ (a^2 - 1)l^2 + 1 - m^2 \]^2 - \[ ai + k + 1 - l - i \]^2
- \[ p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m \]^2
- \[ q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x \]^2
- \[ z + pl(a - p) + t(2ap - p^2 - 1) - pm \]^2 \].
Hilbert’s 10th problem

- **INPUT** A polynomial $P$ in variables $x_1, ..., x_n$
- **QUESTION** Is there a positive solution to the equation $P = 0$?
- Matijasevich, after Julia Robinson in the 70’s showed there is no algorithm to decide such questions.
- **But** there is now a polynomial whose only rationals zeroes are the primes!
Recently it was shown by Braverman and Yampolsky (STOC, 2007) that Julia sets can be noncomputable, any halting problem being codable. (Also Blum-Smale-Shub, but that’s another story.)

Julia set: $z \mapsto z^2 + \alpha z$, where $\alpha = e^{2\pi i \theta}$.

Nabutovsky and Weinberger (Geometria Dedicata, 2003) showed that basins of attraction in differential geometry faithfully emulated certain computations. Refer to Soare Bull. Symbolic Logic.

Remark: Earlier and ignored work by Lee Rubel on universal PDE’s.
Figure 1: Examples of quadratic Julia sets $J_p$ (black), and filled Julia sets $K_p$ (gray); orbits that originate at white points escape to $\infty$; note that on picture (c) $K_p = J_p$, since $K_p$ has empty interior.
The answer is inescapable: these diverse mathematical objects, tiles, Conway sequences, and polynomials can be used to simulate computations.
Much of mathematics is concerned with **classification** of structures (groups, rings, DE’s etc) by **invariants**.

Bases for vector spaces, Ulm invariants for abelian groups.

How can we show that **no** invariants are possible?

A computability theorist’s view.
The halting problem is called $\Sigma^0_1$ in that $\varphi_x(y)$ halts iff

$$\exists t \in \mathbb{N} \varphi_x(y)$$

halts in $t$ steps. (And $\varphi_x(y)$ halts in $t$ steps is computable.) This is arithmetic, where the quantifier searches over $\mathbb{N}$.

- Almost all problems in normal mathematics are analytic.
- A is analytic or $\Sigma^1_1$ iff deciding $x \in A$ entails asking if there is a function $f$ from $\mathbb{N}$ to $\mathbb{N}$ such that some computable relation holds for all $f(n)$.
- E.g. isomorphism is typically in $\Sigma^1_1$. 
Many problems in $\Sigma_1$ are much easier. E.g. isomorphism for finitely presented groups is $\Sigma_3^0$. (Is there a matching of generators for which every equation in the first holds in the second?)

If some problem is shown to be $\Sigma_1$ complete, then no simpler set of invariants is possible.

E.g. (Downey and Montalbán) the problem of deciding if two finitely presented groups have $H_i(G) \cong H_i(\hat{G})$ for $i \leq 3$ is $\Sigma_1$ complete.

Uses the result that the isomorphism problem for computable torsion free Abelian groups is $\Sigma_1$ complete. (DM)
How to prove such a result?

- A tree is a downward subset of $\mathbb{N}^\subset \mathbb{N}$, the set of finite strings of natural numbers.
- A tree is well-founded if it has no infinite path.
- Core problem: Deciding of a tree is well-founded is $\Sigma^1_1$ complete. Deciding if two trees are isomorphic is $\Sigma^1_1$ complete. (Essentially Kleene, Harrison)

**Theorem (DM)**

There is a computable operator $G$, that assigns to each tree $T$ a torsion-free group $G(T)$, in a way that

1. if $T_0 \cong T_1$, then $G(T_0) \cong G(T_1)$,
2. if $T_0$ is well-founded and $T_1$ is not, then $G(T_0) \not\cong G(T_1)$. 
Borel cardinality theory: equivalence relations (such as isomorphism) $E_1 \leq_B E_2$ iff there is a Borel mapping $f : E_1 \to E_2$ with $x \approx_{E_1} y$ iff $f(x) \approx_{E_2} f(y)$.

Their idea is that any reasonable translation should be at least Borel.

Invariants? e.g. finite rank torison free Abelian groups. $E_{\text{rank } i} <_B E_{\text{rank } i + 1}$. Complete?

From a computability point of view, all the same $\Sigma_3^0$.

Structure largely unknown.
Another example is provided by extending partial orderings.

A linear extension \((P, \leq_L)\) of a partial ordering \((P, \leq_P)\) is a linear ordering such that whenever \(x \leq_P y, x \leq_L y\).

Theorem (Szpilrajn) every partial order has a linear extension.

A well-partial ordering has a well ordered extension. (Bonnet, Corominas, Fraïssé, Jullien, and Pouzet, Galvin, Kostinsky, and McKenzie, etc for extendible types)

Theorem (Slaman and Woodin) The collection of computable partial orderings with dense extensions is co-\(\Sigma^1_1\) complete, and hence there are no reasonable invariants, answering a question of Łoś.
One of the greatest theorems in mathematics is not widely known, and is due to Saharon Shelah.

The realization is that orderings are very complex and if one can code them into a structure then that structure will have so many models in its isomorphism type that it will be impossible to “classify”

Shelah proved the Dichotomy Theorem which says very very roughly, that either a class of models resembles a vector space and has a decent set of invariants “like a basis” generated by a relation called “forking” or it resembles a linear ordering and is unclassifiable.

“Why am I so happy?” (AMS notices), Classification Theory and the Number of Non-isomorphic Models.

There is a nice user friendly discussion of this in a Bull LMS paper by Wilfred Hodges “What is structure theory?” (1987)
One modern incarnation of this story is to only look at efficient solutions to problems. The title would be *A complexity-theorists view*.

See e.g. Wigderson’s ICM article.

But I have run out of time, so that is another story.
Thanks for your attention.