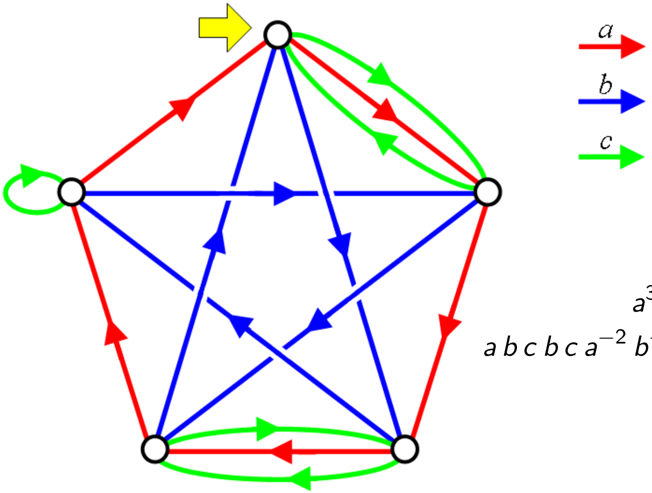
Decidability: The Entscheidungsproblem

Robin Whitty

London South Bank University

Turing's Worlds, Rewley House, 23 June 2012

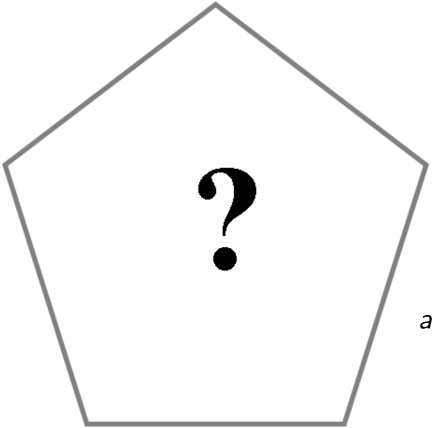
A Word Problem



$$\begin{aligned} a^5 &= 1 \\ a^3\, b &= 1 \\ a\, b\, c\, b\, c\, a^{-2}\, b^{-1} &= 1 \end{aligned}$$

What about $a^2\, b^2\, c^2\, b^{-1}\, c^2\, a^{-1}\, c^{-1}\, b^3\, c\, b^2\, a^3\, c^{-2}\, a^{-2}\, b^3 c^2 a^{-1} b^4$?

A Word Problem



$$\begin{aligned} a^5 &= 1 \\ a^3\,b &= 1 \\ a\,b\,c\,b\,c\,a^{-2}\,b^{-1} &= 1 \end{aligned}$$

What about $a^2\,b^2\,c^2\,b^{-1}\,c^2\,a^{-1}\,c^{-1}\,b^3\,c\,b^2\,a^3\,c^{-2}\,a^{-2}\,b^3c^2a^{-1}b^4$?

The Word Problem

Max Dehn, 1912

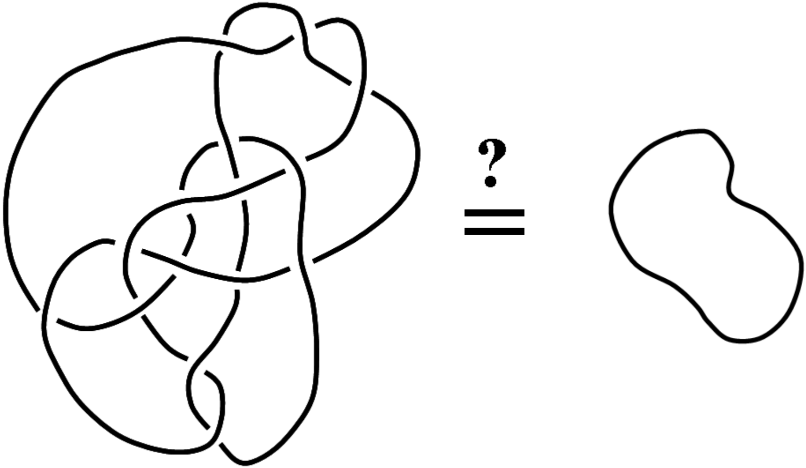
Let G be a group given by a finite presentation

$$G =< X \mid R > .$$

Is there an algorithm which decides whether or not any given X-word w represents the identity in G, i.e., whether or not $w = 1_G$?

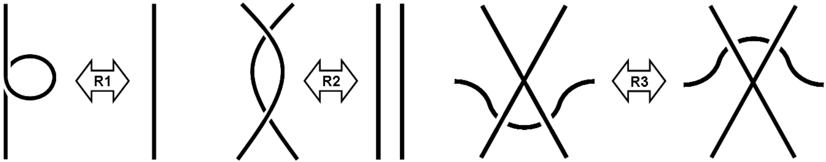
E.g. $G = \langle a, b, c \mid a^5 = 1,\ a^3\, b = 1,\ a\, b\, c\, b\, c\, a^{-2}\, b^{-1} = 1 \rangle$,
$w = a^2\, b^2\, c^2\, b^{-1}\, c^2\, a^{-1}\, c^{-1}\, b^3\, c\, b^2\, a^3\, c^{-2}\, a^{-2}\, b^3 c^2 a^{-1} b^4$

The Unknot Problem



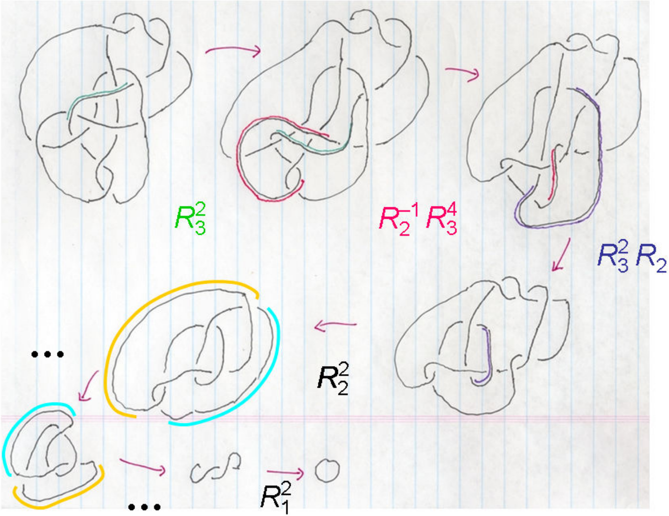
Is there an algorithm to determine whether any given knot (embedding of S_1 in 3-space) is continuously deformable to the unknot?

The Reidemeister Moves



Kurt Reidemeister, Königsberg, 1926

The Reidemeister Moves



$$R_3^2\ R_2^{-1}\ R_3^4\ R_3^2\ R_2\ R_2^2\ \ldots\ R_1^2 = 1$$

Hilbert's Tenth Problem, 1900

Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Attention focuses on the restricted problem: find **nontrivial, nonnegative integer** solutions.

E.g. (1) $16(k+1)^3(k+2)(n+1)^2+1-f^2=0$ is solved by

$$\begin{array}{lll} k=0 & n=2 & f=17, \\ k=1 & n=244 & f=4801, \\ k=2 & n=87814 & f=3650401, \quad \textit{etc} \end{array}$$

(2) The **Pell Equation:** $x^2-k(y+1)^2=1$ may be solved for x and y if and only if k is not a positive square.

The Hilbert Programme, 1900–1931

Given a mathematical system $\mathcal{S}$ (e.g. first order predicate logic) to establish that, for any proposition P,

Completeness: either P or **not** P is provable in $\mathcal{S}$.

Consistency: P and **not** P cannot both be provable in $\mathcal{S}$.

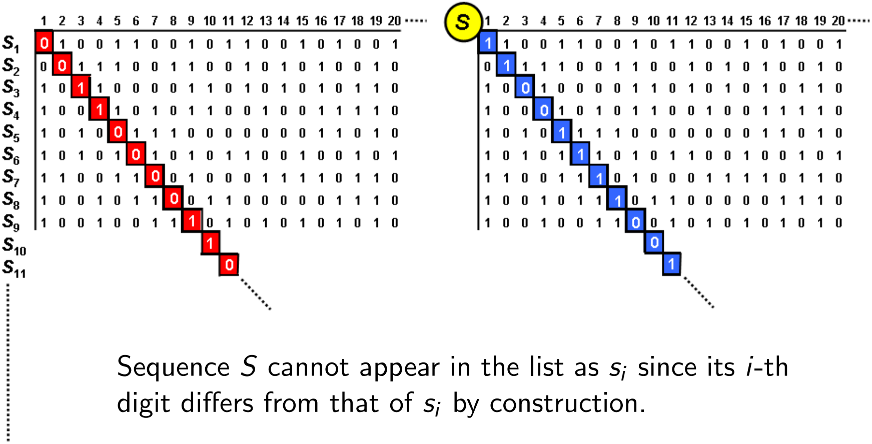
Decidability: (the Entscheidungsproblem) there is a process for deciding in finite time whether P is provable in $\mathcal{S}$.

Completeness and Consistency $\Rightarrow$ truth and provability are synonymous. They are not (Gödel, 1931).

Completeness also $\Rightarrow$ Decidability since we can **enumerate** all proofs; eventually either P or **not** P will appear as a proved proposition.

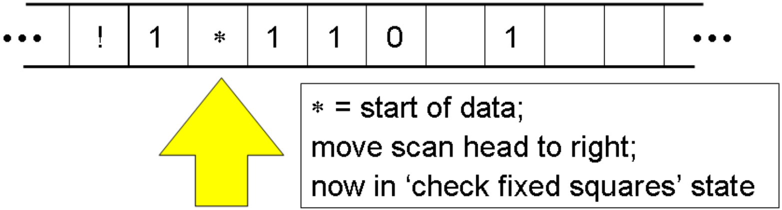
Cantor and Diagonalisation

We cannot enumerate all infinite 0-1 sequences.



Sequence S cannot appear in the list as s_i since its i-th digit differs from that of s_i by construction.

Turing's machine



Circle-free machine: prints an infinite number of 0-1 symbols

Description number: a numerical encoding of the definition of a machine

Satisfactory number: one which describes a circle-free machine

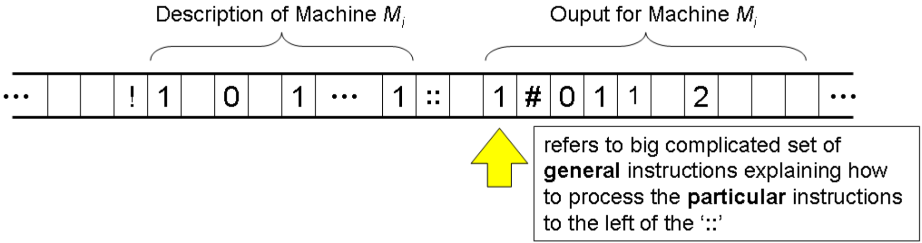
Computable sequence: output of a circle-free machine (infinite 0-1 sequence)

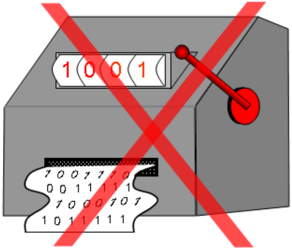
enumerated by enumerating satisfactory numbers

Uncomputable sequence: one which is the output of no machine

must exist by diagonalisation

Turing's universal computing machine





N.B.: no distinction between machine and input data!

Satisfactoriness not decidable

Why does the following customised universal machine **H** fail to output the uncomputable sequence S?

```
do forever
    k:= next machine description number
    if k is satisfactory then
        write M_k on tape
    simulate M_k until k-th digit reached
    write reverse of k-th digit on tape
loop
```

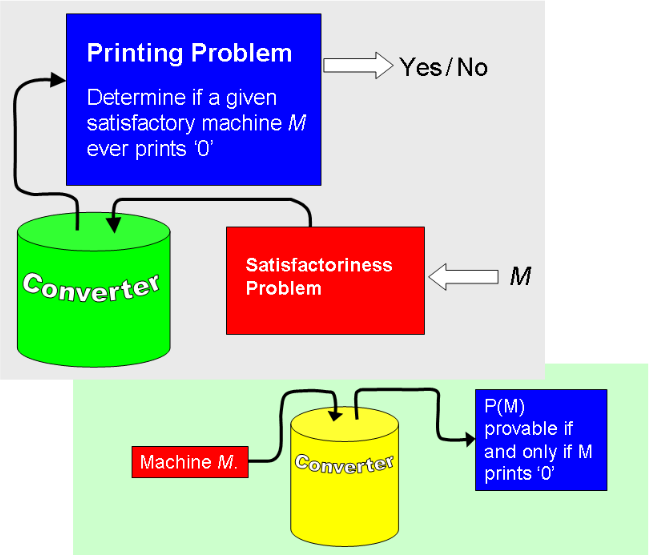
If **H** is a valid machine then it has a description number $k_{\mathbf{H}}$.

What happens when the loop reaches $k_{\mathbf{H}}$?

H can never print the $k_{\mathbf{H}}$-th digit of S.

Every task done by **H** has been implemented except checking satisfactoriness which must therefore defy implementation.

The Entscheidungsproblem unsolvable



Undecidability of the word problem

The decidability of the word problem for finitely presented groups was settled in the negative by Petr Sergeevich Novikov in 1954.

Various restrictions are decidable, notably the word problem for **one-relator groups**: groups having presentation $G =< X \,|\, r >$, where r is a single relation.

E.g. $< a, b \,|\, ba^m b^{-1} a^{-n} = 1 >$, the so-called Baumslag–Solitar group $BS(m, n)$.

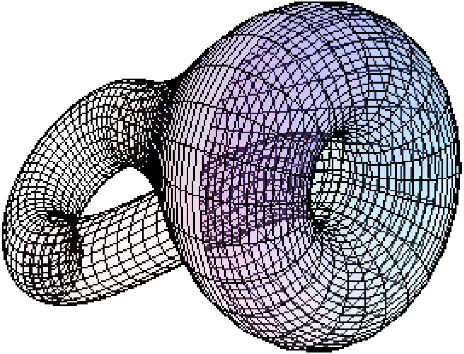
But that does not mean one-relator groups are easy; a big open problem is:

Is it decidable to determine whether two one-relator presented groups are the same (isomorphic)?

E.g. $< a, b \,|\, b^2 a^{-2} = 1 >$ is the same group as $B(1, -1)$. But is there an algorithm which guarantees to tell us this?

Undecidability in 4-space knots

The decidability of the unknot questions was settled in the affirmative by Wolfgang Haken in 1961.



The Klein bottle: a 2-dimensional surface embedded in 4 dimensions. (By the way the two isomorphic one-relator groups we just looked at are the fundamental group of the Klein bottle).

A knotted embedding of S_2 in 4-space may or may not be deformable to the unknot. The decidability is unknown. For higher dimensions the question is undecidable.

Hilbert's 10th Problem

There exist enumerable sets for which membership is undecidable.

E.g. the set of provable propositions of first order logic can be enumerated but has no membership test (this is precisely the Entscheidungsproblem).

Conjecture (Martin Davis, 1950) A set is enumerable if and only if it is Diophantine (e.g. the Pell equation confirms that the non-square positive integers form a Diophantine set).

E.g. (James P. Jones, 1975) the Fibonacci numbers, $0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$ are Diophantine: k is Fibonacci if and only if the following equation has a positive integer solution in x:

$$\left(k^2 - kx - x^2\right)^2 = 1.$$

(Exercise: what positive x solves the equation for $k = 3$?)

The DPRM Theorem

Theorem (Davis, Putnam, Robinson, Matiasevich, 1970) Davis' 1950 conjecture is true: enumerable sets and Diophantine sets are the same thing.

Consequences: (1) there is a *universal Diophantine equation* $U(k, K, u_1, \ldots, u_N) = 0$ which simulates any given Diophantine equation $D(k, x_1, \ldots, x_n) = 0$ by making a suitable choice of K.

(2) For any enumerable set E there is a Diophantine equation $D_E(k, x_1, \ldots, x_n) = 0$ which has a solution in the x_i if and only if k belongs to E. (E.g. $E =$ set of counterexamples to Goldbach's conjecture, set of twin primes, ...)

A Prime Generating Polynomial

$$
\begin{aligned}
(k+2)\Big[\, 1 &- (wz+h+j-q)^2 \\
&- \big((gk+2g+k+1)(h+j)+h-z\big)^2 \\
&- \left(16\,(k+1)^3(k+2)(n+1)^2+1-f^2\right)^2 \\
&- (2n+p+q+z-e)^2 - \left(e^3(e+2)(a+1)^2+1-o^2\right)^2 \\
&- \left(\left(a^2-1\right)y^2+1-x^2\right)^2 - \left(16\,r^2y^4\left(a^2-1\right)+1-u^2\right)^2 \\
&- \left(\left(\left(a+u^2\left(u^2-a\right)\right)^2-1\right)(n+4dy)^2+1-(x+cu)^2\right)^2 \\
&- \left(\left(a^2-1\right)l^2+1-m^2\right)^2 - \big((a-1)i+k-l+1\big)^2 - (n+l+v-y)^2 \\
&- \left(p+l(a-n-1)+b\left(2an+2a-n^2-2n-2\right)-m\right)^2 \\
&- \left(q+y(a-p-1)+s\left(2ap+2a-p^2-2p-2\right)-x\right)^2 \\
&- \left(z+pl(a-p)+t\left(2ap-p^2-1\right)-pm\right)^2 \,\Big]
\end{aligned}
$$

(Jones, Sato, Wada, Wiens, 1976)