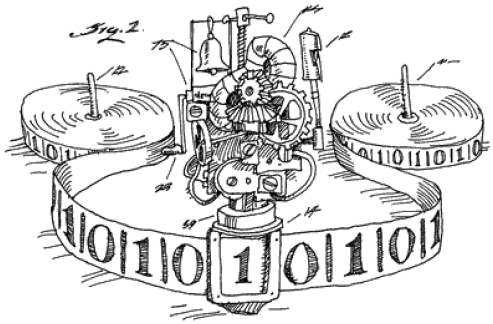
What is Turing's Halting Problem?

Cristian S. Calude
University of Auckland

Turing's Halting Problem

Turing's halting problem (THP), i.e. the problem to decide whether an arbitrary Turing machine (TM)



halts on an arbitrary input, is arguably the most (in)famous unsolvable (by any TM) mathematical problem.

Indeed, assume, for the sake of contradiction, that there exists a TM `HALT` which can decide whether a TM T (given by its code #T) eventually stops on input x:

$$\texttt{HALT}(\#T, x) = \begin{cases} 1, & \text{if } T(x) \text{ stops,} \\ 0, & \text{otherwise.} \end{cases}$$

Construct a TM Q

$$Q(x) = \begin{cases} 1, & \text{if } \texttt{HALT}(x, x) = 0, \\ \text{loops forever}, & \text{otherwise,} \end{cases}$$

and deduce the contradiction:

$$\texttt{HALT}(\#Q, \#Q) = 1 \text{ iff } \texttt{HALT}(\#Q, \#Q) = 0.$$

Why THP Would Be of Any Interest to Mathematicians?

- The negative solution of Hilbert's tenth problem discovered by Matiyasevich (there is no TM deciding whether an arbitrary Diophantine equation has or has not a solution in integers) follows from the undecidability of THP.
- Gödel's incompleteness theorem is another notable consequence.
- Pour-El & Richards theorem (roughly, any closed unbounded operator on any Hilbert space takes some computable input to some uncomputable output) is rooted in the undecidability of THP.
- If one could solve THP, then many mathematical problems would be automatically solved, e.g., Goldbach's conjecture or Riemann's hypothesis.

How Difficult is THP?

Take a universal (self-delimiting TM) U and, instead of asking whether $U(x)$ stops on an arbitrary input x, look at the probability that $U(x)$ stops when x is randomly chosen according to the Lebesgue measure. The result is Chaitin's Omega Number

$$\Omega_U = \sum_{U(x) \text{ halts}} 2^{-|x|}.$$

The number Ω_U is not only uncomputable (a direct consequence of the undecidability of THP), but also algorithmically random (its expansion in any base is not contained in any "constructive null set" with respect to the Lebesgue measure).

Knowing the first N bits of Ω_U allows us to decide which program of less than N bits halts, but the converse is not necessary true.

Interesting recursion-theoretical results have been recently obtained in this area by Downey and his colleagues.

In 1975 Chaitin has proved that *if we assume that ZFC is arithmetically sound, then ZFC can determine the value of only* finitely *many bits of* Ω_U.

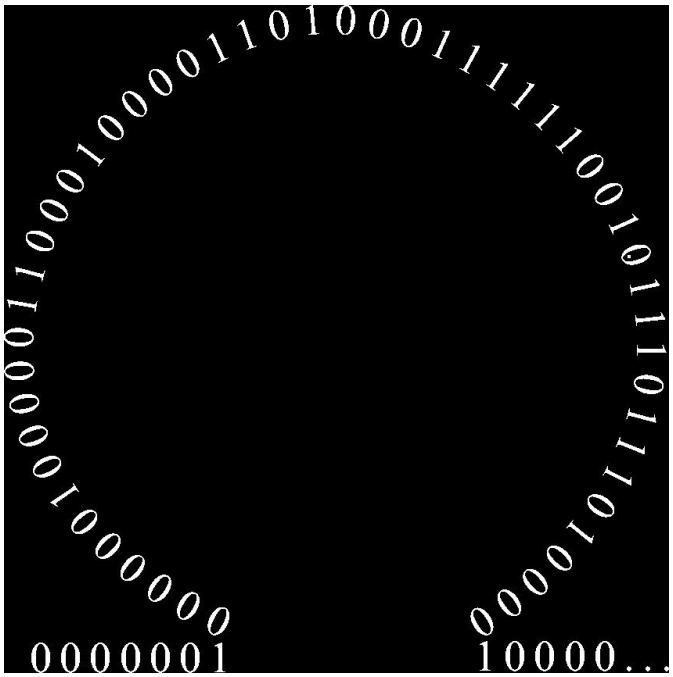
In 1999 Solovay *has effectively constructed a self-delimiting* TM U *such that ZFC, if arithmetically sound, cannot determine* any *bit of the* Ω_U.

In 2000 Calude has shown that *for every self-delimiting* TM U *we can effectively construct a self-delimiting* TM U' *such that*

- $\Omega_U = \Omega_{U'}$,
- *ZFC, if arithmetically sound, cannot determine more than the* initial block of 1's *of the binary expansion of* Ω_U.

In 2002 Calude, Dinneen and Shu *have computed the first 64 bits of the self-delimiting* TM U constructed in 1987 by Chaitin using the following register machine instructions:

```
L:  GOTO  L2
L:  JUMP  R  L2
L:  GOBACK  R
L:  EQ  R1  R2  L2
L:  NEQ  R1  R2  L2
L:  RIGHT  R
L:  LEFT  R1  R2
L:  SET  R1  R2
L:  HALT
L:  OUT  R
L:  DUMP
```



Is it Possible to Break Turing's Barrier?

Turing's proof shows that, in general (i.e. for an arbitrary pair $(\mathtt{T}, x)$), there is no algorithmic procedure capable of answering in a *finite* time the *infinite* set of questions

"does $\mathtt{T}(x)$ stop in t steps", for $t = 1, 2, \ldots$

It is essential that `HALT` *is a* TM, *so* Q *is itself a* TM.

So, what about trying to prove that `HALT` is "computable by some other type of machine"?

Taking into account that TMs are not only mathematical objects, but also "physical devices" two natural ideas come to mind:

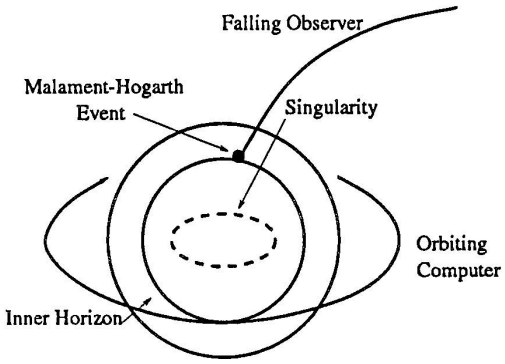
- relativistic machines
- quantum machines

Relativistic Computing

Accelerate machines, which execute their n-th instruction in 2^{-n} seconds, may not be impossible as the same physical theory which limits the speed of information processing by the velocity of light maintains that time is relative to the observer.

So, if a satellite revolving with instantaneous tangential velocity $c(1-e^{-2t})^{\frac{1}{2}}$ (c is the speed of light, t is the earth time scale) and local time scale T, the time interval $dT = e^{-t}dt$, then one second in the satellite's time scale corresponds to an eternity on earth as $\int_0^\infty e^{-t}dt = 1$.

In 2002 Etesi and Németi observed that in Malament-Hogarth space-times, due to infinite time contraction, it may be possible for a computer to receive, in *finite* time, the answer to a *yes-or-no question* from an *infinite* computation.



In 2002 Wiedermann and van Leeuwen have introduced the *relativistic* TM and showed that *RTMs whose relativistic phases can solve the THP for* TMs em recognize exactly the Δ_2-sets.

Quantum Computing

Consider the Merchant's Problem: *A merchant learns than one of his five stacks of coins contains only false coins, γ grams heavier than normal ones. Can he find the odd stack by a single "weighing"?*

- Take one coin from the first stack, two coins from the second stack, ..., five coins from the last stack.
- Measure the weight of the combination of coins and obtain the number $15 + \gamma \times n$.
- The n-th stack contains false coins.

The above solution is, in spirit, "quantum". It consists of the following steps:

a) *preparation*,
b) *measurement*,
c) *classical calculation*.

If we still have five stacks of coins, but a few (maybe none) may contain false coins, then a possible solution is to choose 1, 2, 4, 8, 16 coins from each stack, and use the uniqueness of base two representation.

Variants of the Merchant's Problem

- *The Finite Problem:* We have N stacks of coins and we know that *at most one stack may contain false coins*. We are allowed to take just one coin from each stack and have a single "weighing". Can we determine whether there is a stack containing false coins, and in the affirmative, which?
- *The Infinite Problem:* We now have countable many stacks, all of them, except at most one, containing true coins only. Can we determine whether there is a stack containing false coins?

A Quantum Strategy

We are given $\theta = 2^{-n}$ and we assume that we work with a quantum "device" with sensitivity $\varepsilon = 2^{-m}$.

- First, we *compute classically* a time $T = T_{\theta,\varepsilon}$,
- Then, we run the "device" on a random input for the time T.

The quantum "device" may or may not produce a click.

- If we get a click, then the system has false coins (in the finite case the stack containing false coins can be located).
- If we don't get a click, then with probability greater than $1 - \theta$ all coins are true.

An essential part of the method is the requirement that the time limit T is *computable* in a classical way.

The Finite Problem

We consider the space $\mathbf{R}^N$ and denote by q_i the weight of a coin in the i-th stack; if the i-th stack contains true coins, then $q_i = 1$, otherwise, $q_i = 1 + \gamma$ (γ is a rational in $(0, 1)$).

Consider the operator $\mathbf{Q} = \sum_{i=1}^{N} q_i \mathbf{P}_i$, where $\mathbf{P}_i(\mathbf{x}) = (0, 0, \ldots, x_i, 0, \ldots, 0)$:

$$\mathbf{Q}(\mathbf{x}) = (q_1\mathbf{P}_1, \ldots, q_N\mathbf{P}_N)(\mathbf{x}) = (q_1x_1, \ldots, q_Nx_N),$$

and the quadratic form induced by the t-th iteration of the operator $\mathbf{Q}$, $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle$. Note that:

- if all coins are true $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle = \| \mathbf{x} \|^2$, for all $\mathbf{x} \in \mathbf{R}^N$;
- if there are false coins in some stack, for some $\mathbf{x} \in \mathbf{R}^N$, $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle > \| \mathbf{x} \|^2$, and the value increases with every new iteration.

We work with a "weighted Lebesgue measure" with proper non-negative continuous density ρ, for example, the Gaussian distribution

$$\rho(\mathbf{x}) = \frac{1}{\pi^{N/2}} \, e^{-\sum_{s=1}^{N} |x_s|^2}.$$

Hence the probability of the event $\{\mathbf{x} \mid x_1 \in \Omega\}$ is the integral $\mathrm{Prob}(\Omega) = \int_{\Omega \times \mathbf{R}^{N-1}} \rho dm$.

Assume that time is discrete, $t = 1, 2, \ldots$. Choose a "test" vector $\mathbf{x} \in \mathbf{R}^N$ and assume that we have a quantum "device" which measures the quadratic form and clicks at time T on $\mathbf{x}$ when

$$\langle \mathbf{Q}^T(\mathbf{x}), \mathbf{x} \rangle > (1 + \varepsilon) \parallel \mathbf{x} \parallel^2 . \tag{1}$$

In this case we say that the quantum "device" has sensitivity ε.

Two cases may appear:

1. If $\langle \mathbf{Q}^T(\mathbf{x}), \mathbf{x} \rangle > (1 + \varepsilon) \parallel \mathbf{x} \parallel^2$, then the "device" has clicked at time T and we know for *sure* that there exist false coins in the system.
2. If by the time $T > 0$ the "device" hasn't (yet?) clicked, then either all coins are true, i.e., $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle = \parallel \mathbf{x} \parallel^2$, for all $t > 0$, or at time T the growth of $\langle \mathbf{Q}^T(\mathbf{x}), \mathbf{x} \rangle$ hasn't yet reached the threshold $(1 + \varepsilon) \parallel \mathbf{x} \parallel^2$.

In the first case the "device" will *never* click, so at each stage t the test-vector $\mathbf{x}$ produces "true" information; we can call $\mathbf{x}$ a "true" vector.

In the second case, the test-vector $\mathbf{x}$ is "lying" at time T as we *do* have false coins in the system, but they were not detected at time T; we say that $\mathbf{x}$ produces "false" information at time T.

Of course, the second case may be *dangerous*, and indeed, classically we cannot say anything in this case.

If the system has false coins and they are located in the j-th stack, then each test-vector $\mathbf{x}$ whose j-th coordinate is 0 produces "false" information at any time.

If the system has false coins and they are located in the j-th stack, $x_j \neq 0$, but

$$\| \mathbf{x} \|^2 + ((1+\gamma)^T - 1)|x_j|^2 \leq (1+\varepsilon) \| \mathbf{x} \|^2,$$

then $\mathbf{x}$ produces "false" information at time T. If $|x_j| \neq 0$, then $\mathbf{x}$ produces "false" information for only a finite period of time, that is, only for

$$T \leq \log_{1+\gamma} \left(1 + \frac{\varepsilon \| \mathbf{x} \|^2}{|x_j|^2} \right);$$

after this time the quantum "device" starts clicking.

Consider now the *indistinguishable set at time* t

$$\mathcal{F}_{\varepsilon,t} = \{ \mathbf{x} \in \mathbf{R}^N \mid \langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle \leq (1+\varepsilon) \| \mathbf{x} \|^2 \}.$$

If the system contains only true coins, then $\mathcal{F}_{\varepsilon,t} = \mathbf{R}^N$, for all $\varepsilon > 0, t \geq 1$. If there is one stack (say, the j-th one) containing false coins, then $\mathcal{F}_{\varepsilon,t}$ is a cone $\mathcal{F}_{\varepsilon,t,j}$ centered at the "false" plane $x_j = 0$:

$$((1+\gamma)^t - 1)\, |x_j|^2 \leq \varepsilon \| x \|^2 .$$

A direct calculation shows that

$$\mathrm{Prob}(\mathcal{F}_{\varepsilon,t}) \leq \frac{3N^{3/4}\varepsilon^{1/4}}{\sqrt{\pi}((1+\gamma)^t - 1)^{1/4}} \tag{2}$$

hence,

$$\lim_{t\to\infty} \mathrm{Prob}(\mathcal{F}_{\varepsilon,t}) = 0. \tag{3}$$

In fact, the limit (3) is *constructive*, that is, for every $S > 0$ we can construct the computable bound

$$T_{S,\varepsilon} = \log_{1+\gamma}\left(\frac{2^{4S}3^4N^3\varepsilon}{\pi^2} + 1\right)$$

such that *if the system contains false coins and* $t \geq T_{S,\varepsilon}$, *then* $\mathrm{Prob}(\mathcal{F}_{\varepsilon,t}) \leq 2^{-S}$.

Let us now denote by $\mathcal{N}$ the event "the system contains no false coins" and by $\mathcal{Y}$ the event "the system contains false coins". By $P(\mathcal{N})$ ($P(\mathcal{Y})$) we denote the *a priori* probability that the system contains no false coins (the system contains false coins).

In the simplest case $P(\mathcal{Y}) = \frac{N}{N+1}, P(\mathcal{N}) = 1 - P(\mathcal{Y}) = \frac{1}{N+1}$. We can use Bayes' formula to obtain the *a posteriori probability that the system contains only true coins when at time t the quantum "device" didn't click*:

$$P_{\text{non-click}}(\mathcal{N}) = \frac{P(\mathcal{N})}{P(\mathcal{N}) + (1 - P(\mathcal{N}))\text{Prob}(\mathcal{F}_{\varepsilon,t})}$$

$$\geq 1 - N \cdot \text{Prob}(\mathcal{F}_{\varepsilon,t}).$$

When $t \to \infty$, $\text{Prob}(\Omega_{\varepsilon,t}) \to 0$, so $P_{\text{non-click}}(\mathcal{N})$ goes to 1. More precisely, if $t \geq T_{S,\varepsilon}$, and $S > \log_2 N$, then

$$P_{\text{non-click}}(\mathcal{N}) \geq 1 - N2^{-S}.$$

In conclusion,

for every integer $S > \log_2 N$ we can construct a computable time $T = T_{S,\varepsilon}$ such that picking up a test-vector $\mathbf{x} \in \mathbf{R}^N \setminus \{\mathbf{0}\}$ at random and using a quantum "device" with sensitivity ε up to time T either:

- ◇ *we get a click at some time $t \leq T$, so the system contains false coins; the j-th stack, where j is the unique coordinate such that $(Q^T(\mathbf{x})/((1+\gamma)^T - 1))_j > x_j$, contains false coins;*

- ◇ *or we don't get a click in time T, so with probability greater than $1 - N2^{-S}$ all coins are true.*

The Infinite Problem

"Approximating" the Infinite Problem using the solution of the Finite Problem doesn't work.

We follow the same strategy but use more sophisticated mathematical tools: the "device" (with sensitivity ε) will distinguish the values of the iterated quadratic form

$$\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle = \sum_{i=1}^{\infty} q_i^t \, |x_i|^2$$

by observing the difference between the non-perturbed and perturbed sequences t_l, $\tilde{t}_l$ corresponding to two discrete stochastic processes. We will work with the intersections of l_2 with the discrete Sobolev class l_2^1 of summable sequences with the square norm

$$| \, \mathbf{x} \, |_1^2 \; = \sum_{m=1}^{\infty} |x_{_m} - x_{_{m-1}}|^2,$$

and the discrete Sobolev class $\tilde{l}_2^1$ of weighted-summable sequences with the square norm

$$\| \, \mathbf{x} \, \|_1^2 \; = \sum_{m=1}^{\infty} \frac{1 - \tilde{\delta}_m}{\tilde{\delta}_m} \; |x_{_m} - x_{_{m-1}}|^2.$$

We consider two discrete stochastic processes corresponding to the *equidistant sequence* of moments of time $t_l = l,\ l = 0, 1, \ldots,\ \delta_s = 1$ and to the *perturbed sequence* of moments of time $\tilde{t}_l = \sum_{m=0}^{l} \tilde{\delta}_m,\ \tilde{\delta}_m < 1$.

By natural extension from cylindrical sets we can define the Wiener measures $\tilde{W}$ and W on these spaces and use the following relation between $\tilde{W}$ and W: for every W–measurable set Ω,

$$\tilde{W}(\Omega) = \frac{1}{\prod_{l=1}^{\infty} \sqrt{\delta_l}} \int_{\Omega} e^{-\sum_{m=1}^{\infty} \frac{1-\tilde{\delta}_m}{\tilde{\delta}_m} |x_m - x_{m-1}|^2} dW.$$

The *indistinguishable set* becomes

$$\mathcal{F}_{\varepsilon,T} = \{\mathbf{x} \in l_2 \cap l_2^1 \mid \langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle < \| \mathbf{x} \|^2 + \varepsilon \| \mathbf{x} \|_1^2 .$$

In 2002 Calude and Pavlov proved that *if we assume that there exist false coins in the system, say at stack j, then*

$$\tilde{W}(\mathcal{F}_{\varepsilon,T}) \leq \left(\frac{\varepsilon}{((1+\gamma)^T - 1 - \varepsilon) \cdot \prod_{m=1}^{\infty} \tilde{\delta}_m} \right)^{1/2}.$$

In fact,

$$\tilde{W}(\mathcal{F}_{\varepsilon,T}) \leq 2^{-S},$$

provided

$$t > \log_{1+\gamma} \left(\frac{\varepsilon 2^{-2S}}{\prod_{m=1}^{\infty} \tilde{\delta}_m} + 1 + \varepsilon \right).$$

Hence

$$P_{\text{non-click}}(\mathcal{N}) > 1 - \frac{1 - P(\mathcal{N})}{P(\mathcal{N})} \cdot \frac{\sqrt{\varepsilon}}{\sqrt{(1+\gamma)^T - 1 - \varepsilon}\sqrt{\prod_{m=1}^{\infty} \tilde{\delta}_m}}.$$

Final Comments

- The undecidability of THP can be seen not only as a fundamental barrier, but as a result showing that mathematics is inexhaustible.
- Recent attempts to attack THP by mixing mathematics and physics, thought in infancy, have succeeded to shed more light on the problem, i.e. by clarifying the distinction between halting and unending computations.
- THP is far from being completely understood; much more work, inspiration and talent is needed in this quest.