MCU 2007

Information Hiding and Incompleteness

Klaus Sutner

Carnegie Mellon University
www.cs.cmu.edu/~sutner

or

Breaking the Turing Barrier, Downward

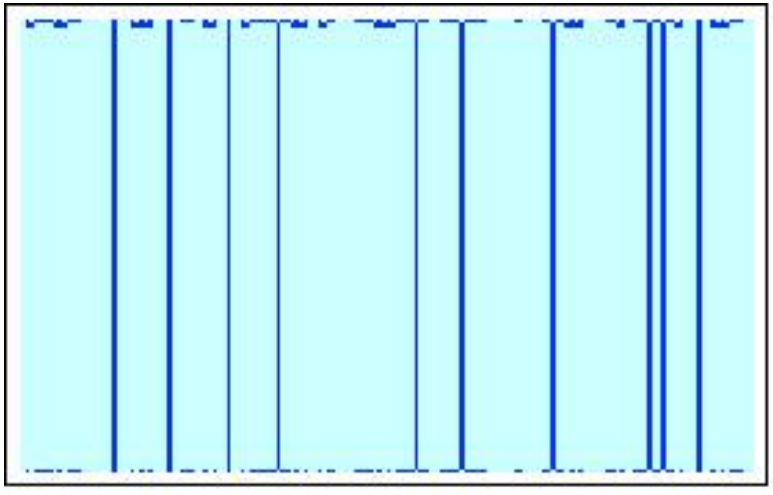
Outline

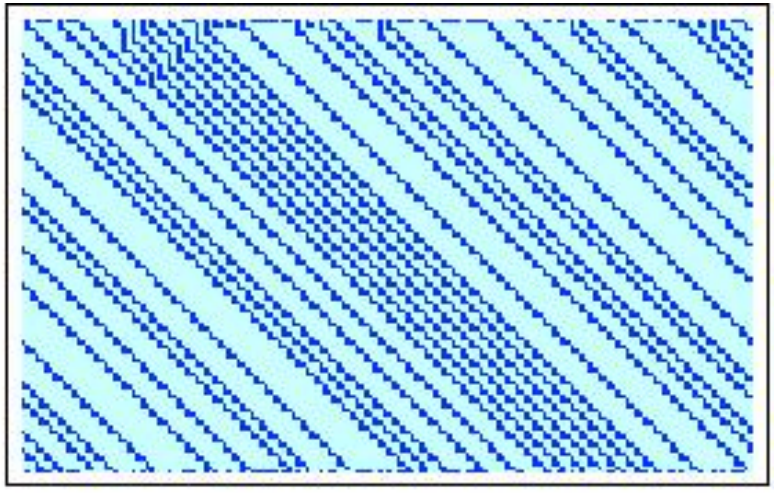
Outline

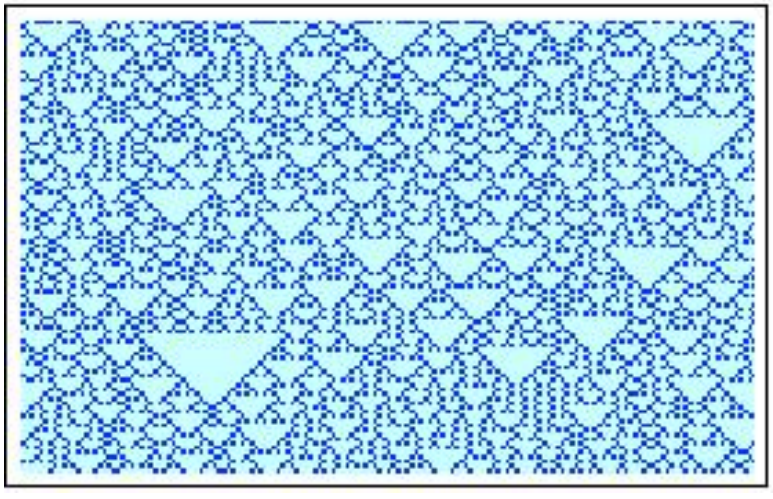
Outline

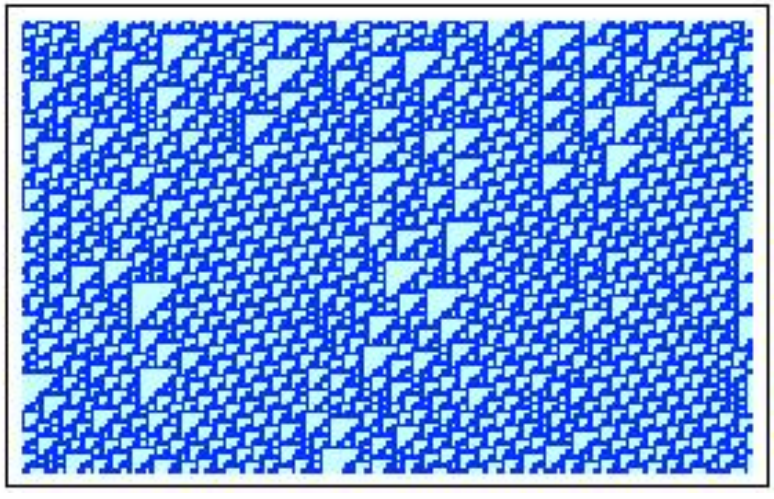
Outline

Pretty Pictures

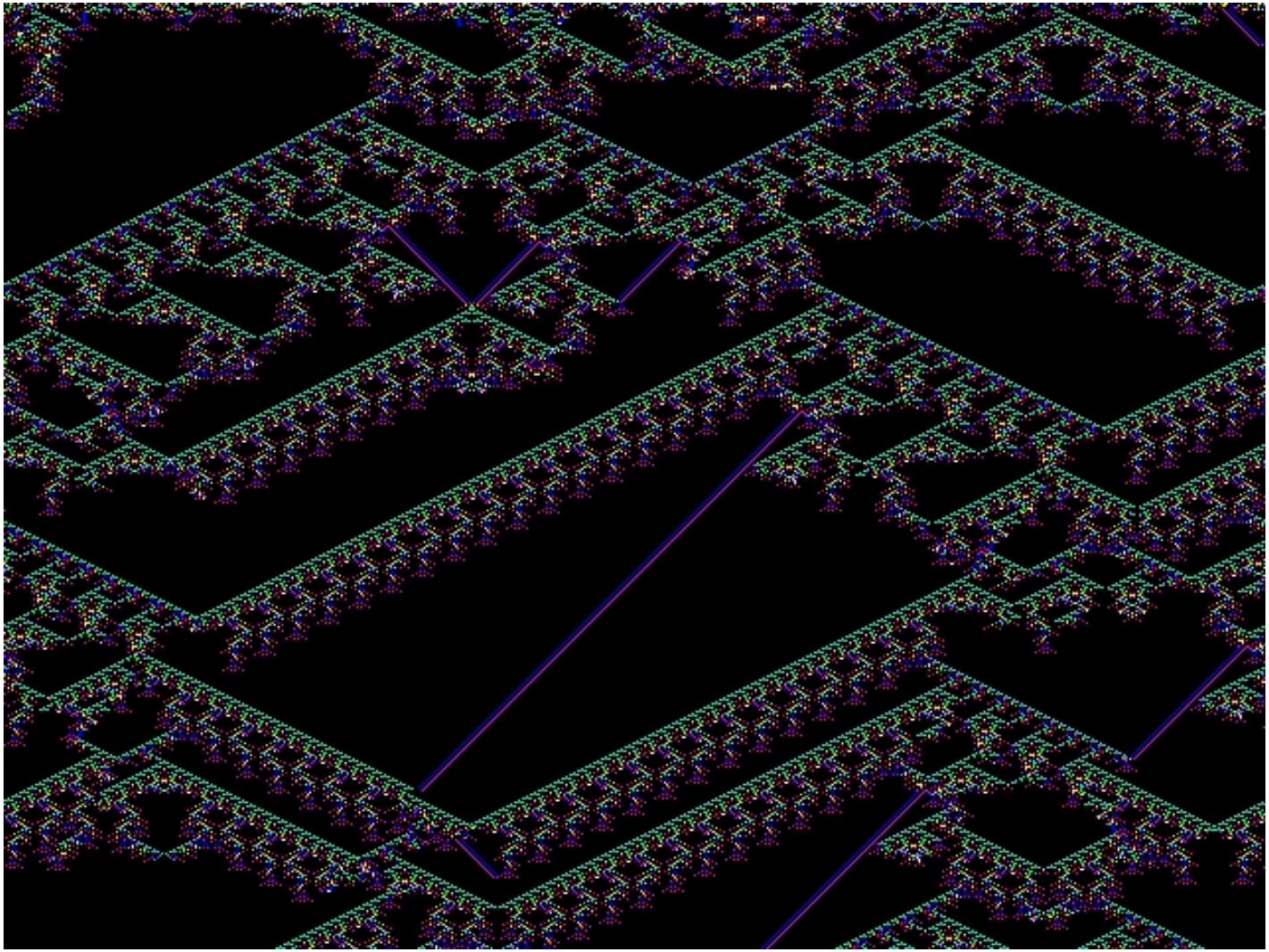








A Langton CA



Wolfram's Classes

Long term behavior of certain discrete dynamical systems (cellular automata, continuous shift-invariant maps on Σ^{∞}).

- *W1*: Evolution leads to homogeneous fixed points.
- *W2*: Evolution leads to periodic configurations.
- *W3*: Evolution leads to chaotic, aperiodic patterns.
- *W4*: Evolution produces persistent, complex patterns of localized structures.

Justification: Appeal to visual characteristics of the orbits.

Entscheidungsproblem

- What is computable?
- Classify the non-computable part.

Caveat Emptor

We only use classical recursion theory which requires simple finitary descriptions.

Often one considers only

$$\mathcal{C}_{\text{fin}} = \text{all configurations with finite support} \subseteq \Sigma^{\infty}$$

or minor modifications such as backgrounds.

Minor atrocity from the perspective of classical dynamics.

The Good News

A few elementary properties are decidable – and then only in dimension one.

Theorem (Amoroso, Patt 1972)

Reversibility and surjectivity in dimension one is decidable.

$$\forall\, x, y, z\, (x \to z \wedge y \to z \Rightarrow x = y)$$

$$\forall\, x\, \exists\, y\, (y \to x)$$

$$\forall\, x, y, z\, (x \to z \wedge y \to z \wedge x \stackrel{*}{=} y \Rightarrow x = y)$$

The Good News

A few elementary properties are decidable – and then only in dimension one.

Theorem (Amoroso, Patt 1972)

Reversibility and surjectivity in dimension one is decidable.

$$\forall\, x, y, z\, (x \to z \wedge y \to z \Rightarrow x = y)$$

$$\forall\, x\, \exists\, y\, (y \to x)$$

$$\forall\, x, y, z\, (x \to z \wedge y \to z \wedge x \stackrel{*}{=} y \Rightarrow x = y)$$

The Good News

A few elementary properties are decidable – and then only in dimension one.

Theorem (Amoroso, Patt 1972)

Reversibility and surjectivity in dimension one is decidable.

$$\forall\, x, y, z\, (x \to z \wedge y \to z \Rightarrow x = y)$$

$$\forall\, x\, \exists\, y\, (y \to x)$$

$$\forall\, x, y, z\, (x \to z \wedge y \to z \wedge x \stackrel{*}{=} y \Rightarrow x = y)$$

Glory/Misery of Automata Theory

Theorem (J. Kari 1990)

Reversibility and surjectivity are undecidable in dimension two.

Theorem

Reversibility, openness and surjectivity are quadratic time.

Can one exploit automata theory a bit more?

Pushing The Good News

Consider first order logic $\mathcal{L}(\rightarrow, =)$ with a one-step predicate and equality. Think of a cellular automaton as a relational structure

$$\mathfrak{A}_\rho = \langle \mathcal{C}, \rightarrow \rangle$$

Theorem

Model checking for one-dimensional cellular automaton and FOL is decidable.

Model Checking CA

So how do we decide, say, injectivity:

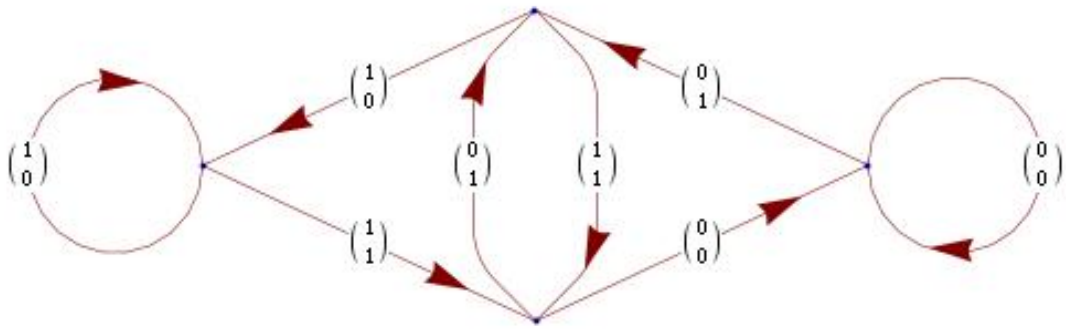
$$\mathfrak{A}_\rho \models \forall x, y, z\,(x \to z \wedge y \to z \Rightarrow x = y)$$

We need to deal with

- predicates $x \to y$ and $x = y$,
- boolean connectives $\wedge$, $\vee$, $\neg$ and $\Rightarrow$,
- quantifiers $\forall$ and $\exists$.

Basic Relation: $x \to y$

$\ldots$	x_{-3}	x_{-2}	x_{-1}	x_0	x_1	x_2	x_3	$\ldots$
$\ldots$	y_{-3}	y_{-2}	y_{-1}	y_0	y_1	y_2	y_3	$\ldots$



The canonical automaton $\mathcal{A}_\rho(x, y)$ for the local map $\rho(\mathbf{x}) = x_0 \oplus x_1$.

No Coordinates

Bi-infinite words are less well-behaved than finite or one-way infinite ones: there is no natural coordinate systems.

Two distinct bi-infinite words can be indistinguishable by an finite state machine.

In fact they will be indistinguishable iff they are shifts of each other or are recurrent and have the same set of finite factors.

Comments

- Need to glue Büchi automata together to obtain an automaton for bi-infinite words.
- Boolean operations are "easy": disjoint union for logical or, complementation for logical not.
- Existential quantification is almost free: simply drop the corresponding variable from the input.

Comments

- Need to glue Büchi automata together to obtain an automaton for bi-infinite words.
- Boolean operations are "easy": disjoint union for logical or, complementation for logical not.
- Existential quantification is almost free: simply drop the corresponding variable from the input.

Comments

- Need to glue Büchi automata together to obtain an automaton for bi-infinite words.
- Boolean operations are "easy": disjoint union for logical or, complementation for logical not.
- Existential quantification is almost free: simply drop the corresponding variable from the input.

More Comments

- The complexity of this algorithm is not elementary: we need nested complementation which uses determinization (Safra's algorithm)

$$\text{Büchi} \longrightarrow \text{Rabin}: \qquad 2^{O(n \log n)}$$

- But: For simple queries one obtains efficient algorithms.

- Useful in classification for finite grids (spectra are rational).

More Comments

- The complexity of this algorithm is not elementary: we need nested complementation which uses determinization (Safra's algorithm)

$$\text{Büchi} \longrightarrow \text{Rabin}: \qquad 2^{O(n \log n)}$$

- But: For simple queries one obtains efficient algorithms.

- Useful in classification for finite grids (spectra are rational).

More Comments

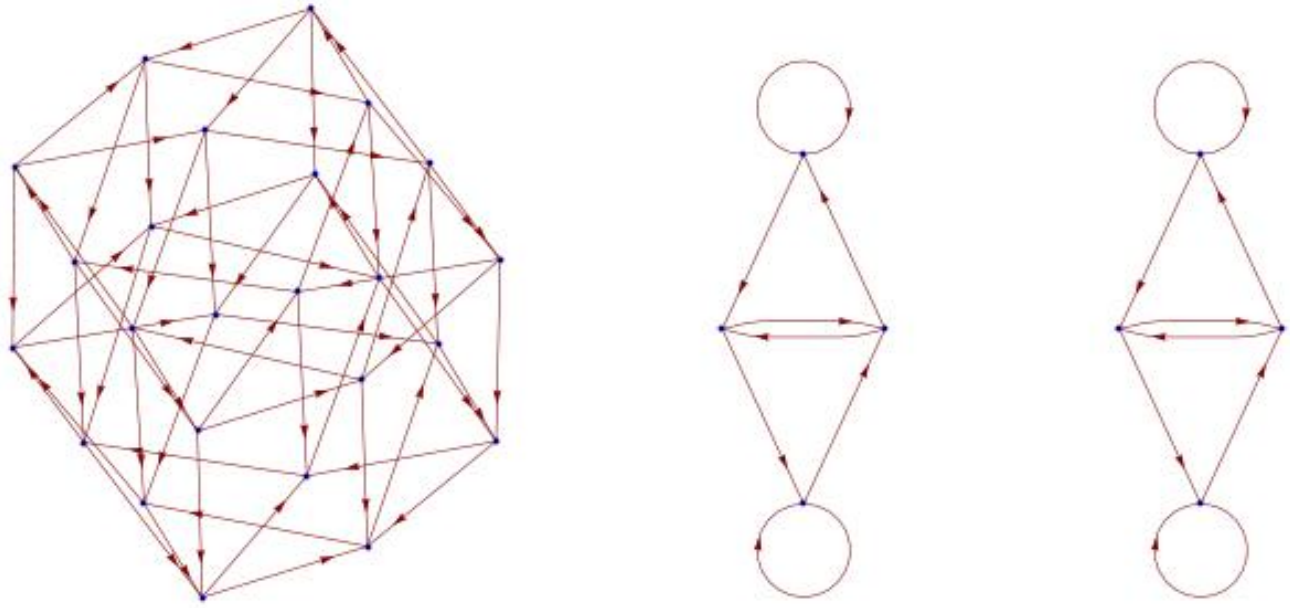
- The complexity of this algorithm is not elementary: we need nested complementation which uses determinization (Safra's algorithm)

$$\text{Büchi} \longrightarrow \text{Rabin}: \qquad 2^{O(n \log n)}$$

- But: For simple queries one obtains efficient algorithms.

- Useful in classification for finite grids (spectra are rational).

Frivolous Picture



Minor Extensions

- Can easily deal with nondeterministic cellular automata.
- Can add unary predicates describing recognizable sets of configurations (as sets of bi-infinite words).
  - configurations of finite support

$$^{\omega}0\,\Sigma^{\star}\,0^{\omega}$$

  - backgrounds (almost periodic configurations)

$$^{\omega}u\,\Sigma^{\star}\,v^{\omega}$$

Not So Minor Extensions

Describing local structures in phasespace is not terribly interesting; we need stronger logics to make assertions about long term behavior.

- add Reachability as a basic predicate $\mathcal{L}(\overset{*}{\rightarrow}, =)$,
- use monadic second order logic,
- use transitive closure logic.

Too messy, corresponding theories way too complicated.

Lots of Bad News

Theorem
It is Π_2-complete to test if all orbits end in fixed points.

Theorem
It is Σ_3-complete to test if all orbits are decidable.

Theorem
It is Σ_4-complete to test if a CA is computationally universal.

Hardness Is Hard

Note that "ending in fixed point" is Π_2^0:

$$\forall\, x\, \exists\, y\, (x \stackrel{*}{\to} y \wedge y \to y)$$

Classical models of computation are meaningful only on a few select configurations.

Some care is required to deal with "meaningless" configurations of the cellular automaton, configurations that do not correspond to computations of the simulated Turing machines.

The Root of All Evil

The Reachability Problem

$$x \overset{*}{\to} y$$

is undecidable.

For obvious reasons: it is straightforward to code Turing machines (or cyclic tag systems), so orbits are not necessarily decidable.

Early History of Unsolvability

1936 Kleene: Halting Set K is r.e. but no recursive

1939 Turing: oracle Turing machines

1943 Kleene: again, no completeness

1943 Kleene: arithmetic hierarchy

1944 Post: K is complete

$$A \text{ re} \quad \Rightarrow \quad A \leq_T K$$

Early History of Unsolvability

1944 Post: degrees of unsolvability

$$A \equiv_T B \iff A \leq_T B \leq_T A$$

1947 Mostowski: arithmetic hierarchy

1948 Post: definability and Turing reducibility

1952 Kleene: the jump A' is complete for A

$$A' = \left\{ e \mid \{e\}^A(e) \downarrow \right\}$$

1954 Kleene, Post: jump well-defined on degrees

Degree-Based Classification

$$\deg(\rho) = \deg\left(\left\{ (x, y) \in \mathcal{C}_{\text{fin}} \times \mathcal{C}_{\text{fin}} \mid x \overset{*}{\to} y \right\}\right)$$

Clearly $\deg(\rho)$ is an r.e. degree and it is straightforward to produce examples where $\deg(\rho) = \emptyset'$.

Degree Theorem

Theorem

For any r.e. degree $\mathbf{d}$ *there is a cellular automaton with degree* $\mathbf{d}$.

Technical point: the hard part is to pin down the degree $\deg(\rho) \leq \mathbf{d}$, pushing it up is easy.

Two-Degree Theorem

Arguably the second most important notion after Reachability is Confluence (leading to the same limit cycle):

$$x, y \text{ confluent} \iff \exists z \, (x \overset{*}{\to} z \wedge y \overset{*}{\to} z)$$

Theorem

For any two r.e. degrees $\mathbf{d}_1$ *and* $\mathbf{d}_2$*, there is a cellular automaton whose Reachability Problem has degree* $\mathbf{d}_1$*, and whose Confluence Problem has degree* $\mathbf{d}_2$*.*

Degree Theorem for Reversible CA

Theorem

For any r.e. degree $\mathbf{d}$ *there is a reversible cellular automaton whose Reachability Problem has degree* $\mathbf{d}$.

Technical point: proof seems to require finite configurations: they provide an opportunity for signal bits to escape to infinity (which makes it feasible to deal with undesirable configurations).

But of course . . .

Note that for reversible cellular automata the Confluence Problem has the same degree as Reachability:

$$x, y \text{ confluent} \iff x \overset{*}{\to} z \vee y \overset{*}{\to} z$$

Hence the Two-Degree Theorem fails miserably for reversible CA.

Post's Problem

Are there intermediate r.e. degrees?
Is there an r.e. set A such that

$$\emptyset <_T A <_T \emptyset'$$

Theorem (Friedberg, Muchnik 1956/7)

There are intermediate r.e. sets.

Construction quite complicated and very different from previous methods in recursion theory, so-called priority argument.

All Hell Brakes Lose

Theorem (Sack's Density theorem)

Given r.e. sets $A <_T B$ there is another r.e. set C such that $A <_T C <_T B$.

The Theory of r.e. Degrees

The Turing degrees of all r.e. sets form an upper semi-lattice $\mathcal{D}$ (meet is partial).

How about deciding the validity of sentences over $\mathcal{D}$. For example:

$$\exists\, x_1, x_2, \ldots, x_n\, \varphi(x_1, x_2, \ldots, x_n)$$

where is φ is quantifier-free in $\mathcal{L}(\leq, \sqcup)$ over $\mathcal{D}$, the structure of the r.e. degrees?

A Glimmer of Hope

Theorem (Folklore)

The Σ_1 theory of $\mathcal{D}$ is decidable.

Alas, the reason is that one can embed all countable partial orders into $\mathcal{D}$.

So a Σ_1 sentence in true in $\mathcal{D}$ simply if it is consistent: it cannot make any obviously contradictory assertions.

. . . Followed by Despair

Theorem (Harrington, Shelah, Slaman)

The Entscheidungsproblem for $\mathcal{D}$ is highly undecidable (more precisely, it has degree $\emptyset^{(\omega)}$).

Isn't This All Perversion?

All known examples of intermediate degrees are artificial: their construction produces an intermediate degree but has no other purpose.

Of course, it is not so easy to define what a natural degree is.

Martin Davis:

> *. . . but one can be quite precise in stating that no one has produced an intermediate r.e. degree about which it can be said that it is the degree of a decision problem that had been previously studied and named.*

Dana Scott, 2004

70 years of research on Turing degrees has shown the structure to be extremely complicated. In other words, the hierarchy of oracles is worse than any political system. No one oracle is all powerful.

J. Myhill, 1961

The heavy symbolism used in the theory of recursive functions has perhaps succeeded in alienating some mathematicians from this field, and also in making mathematicians who are in this field too embroiled in the details of their notation to form as clear an overall picture of their as is desirable. In particular the study of degrees of recursive unsolvability by Kleene, Post, and their successors has suffered greatly from this defect, . . .

Hao Wang, 1977

The study of degrees seems to be appealing only to some special kind of temperament since the results seem to go into many different directions. Methods of proof are emphasized to the extent that the main interest in this area is said to be not so much the conclusions proved as the elaborate methods of proof.

Lastly: H. Poincaré

Formerly, when one invented a new function, it was to further some practical purpose; today one invents them in order to make incorrect the reasoning of our fathers, and nothing more will ever be accomplished by these inventions.

Jeanne d'Arc of Recursion Theory

In 2002 Wolfram proposed a vaguely worded Principle of Computational Equivalence (PCE):

> *There are various ways to state the Principle of Computational Equivalence, but probably the most general is just to say that almost all processes that are not obviously simple can be viewed as computations of equivalent sophistication.*

Comment

Scratch the "obvious".

There are many decision problems that are very far from obvious, yet the underlying problem is considered simple in this context.

Typical example: Tarski's quantifier elimination argument for the theory of the reals:

$$\langle \mathbb{R}, +, \times \rangle$$

The Evidence?

Evidence: very impressive collection of simulations on various systems such as Turing machine, register machines, tag systems, rewrite systems, combinators, cellular automata.

"Sophisticated" systems can be quite small. Not new, but still: the complexity of many apparently simple systems is surprising.

Nota bene: All systems under consideration here are quite limited in size, one cannot search in any systematic way over spaces of larger systems.

Degree Theorem versus PCE

Wolfram's Rejoinder (non-verbatim):

> *You are cheating. You are constructing a CA whose behavior has intermediate degree in some technical sense, but underneath it all there is a universal Turing machine. The real computational process is universal.*

Strawman: Computational Process

How can one make the vague notion of computational process precise?

π one-step relation

ρ the observer

Given an initial state $X_0 \in \Sigma^\star$ define the corresponding computation to be

$$X_{n+1} = \pi(X_n)$$

and the corresponding output as

$$\bigcup \rho(X_n)$$

Allocating Blame

Constraints on the complexity of π and ρ:

π	primitive recursive
ρ	rational transducer

It's not the observer's fault if the output is complete.

Information Hiding

So the observer uncovers some part of the computation but does not increase the complexity. Moreover, he may hide the details.

A computational process is universal if there is some observer that yields r.e.-complete output.

A computational process is intermediate if it fails to be complete and there is some observer that yields non-recursive output.

Transfer?

Burning Question:
Of all the known constructions of intermediate degrees, is there any that can be construed as an intermediate computational process?

Existing Constructions

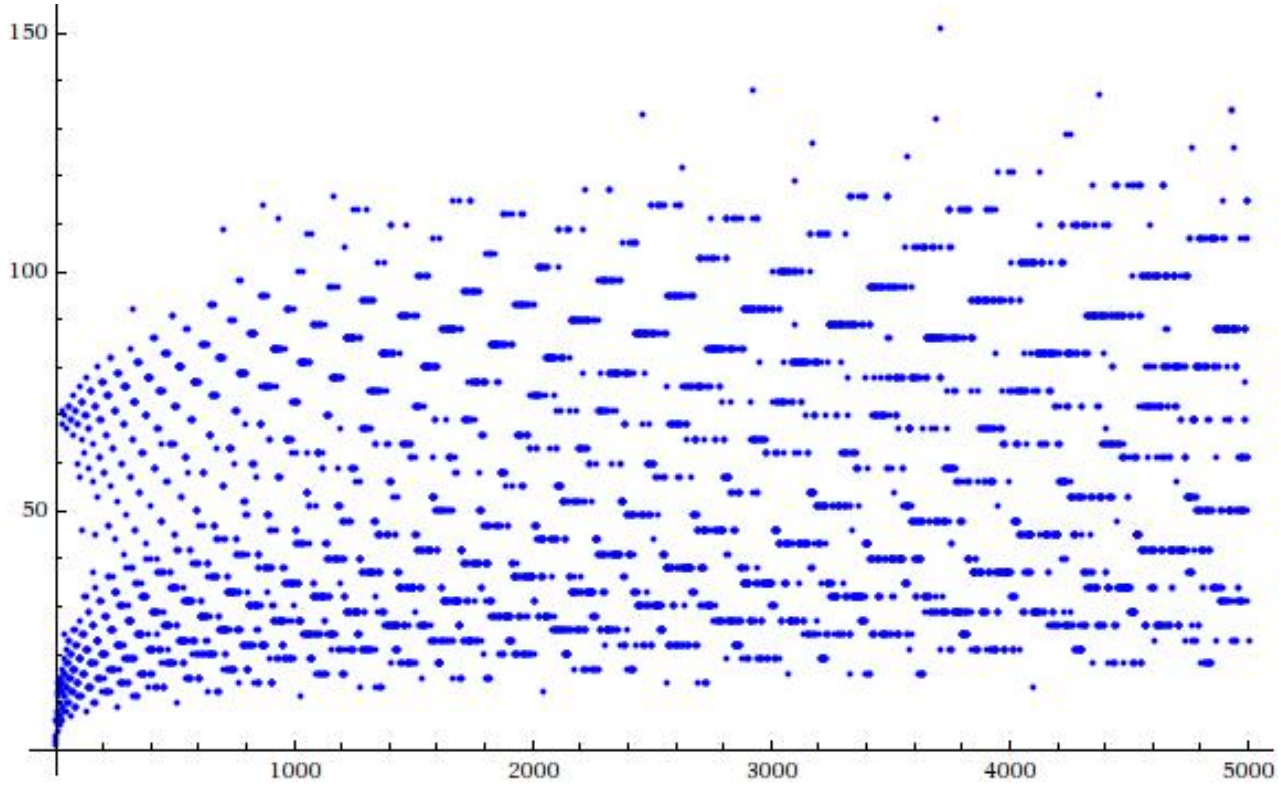
Essentially only two choices

- Friedberg-Muchnik priority construction
- Kucera priority-free construction

▸ Priority Arguments

▸ Priority-Free Arguments

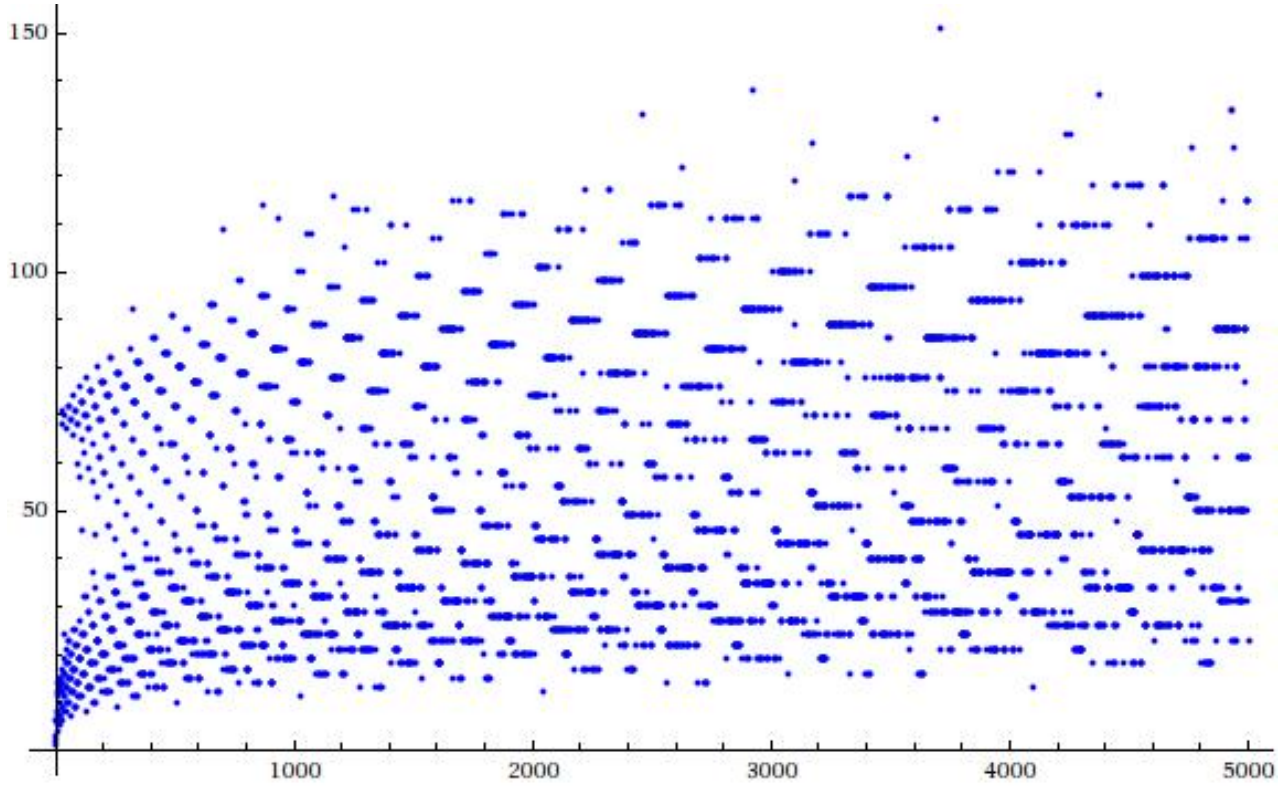
Is This Hopeless?



Mathematics is not ready for this kind of problem.

Pal Erdös

Is This Hopeless?



Mathematics is not ready for this kind of problem.

Pal Erdös

The Logic Angle

Theorem (Feferman 1957)

For every r.e. degree $\mathbf{d}$ *there exists an axiomatizable theory whose degree is exactly* $\mathbf{d}$.

Interestingly, Feferman's constructions uses $\mathcal{L}(=)$, the theory of equality, there are no function symbols, no relation symbols.

In essence, one can only say "there are exactly 17 elements", see Hilbert and Bernays.

H. Friedman's Suggestion

Consider the language $\mathcal{L}(+, \times, <, 0, 1)$ of Peano arithmetic.

Conjecture:

$\mathrm{Th}(\varphi)$ has degree $\emptyset$ or $\emptyset'$

when $|\varphi| \leq 20$

Another One

Consider language $L = \mathcal{L}(R)$ of first order logic with one binary predicate R.

How many quantifiers are needed in a single axiom φ to obtain an intermediate theory:

$$\mathsf{Th}(\varphi) = \{\, \psi \in L \mid \varphi \vdash \psi \,\}$$

Conjecture: 8.

Questions

- Does PCE hold for elementary CA?
- Does PCE hold for all small Turing machines?
- What is the least size where PCE fails?
- How about reversible systems?

Questions

- Does PCE hold for elementary CA?
- Does PCE hold for all small Turing machines?
- What is the least size where PCE fails?
- How about reversible systems?

Questions

- Does PCE hold for elementary CA?
- Does PCE hold for all small Turing machines?
- What is the least size where PCE fails?
- How about reversible systems?

Questions

- Does PCE hold for elementary CA?
- Does PCE hold for all small Turing machines?
- What is the least size where PCE fails?
- How about reversible systems?

More Questions

- What happens to the degree of the sets constructed by Friedberg-Muchnik when the enumeration is changed?
- Can one dispense of a whole class of constructions (say, finite injury priority arguments or the low basis theorem)?
- Again: Is there an intermediate computational process?

More Questions

- What happens to the degree of the sets constructed by Friedberg-Muchnik when the enumeration is changed?
- Can one dispense of a whole class of constructions (say, finite injury priority arguments or the low basis theorem)?
- Again: Is there an intermediate computational process?

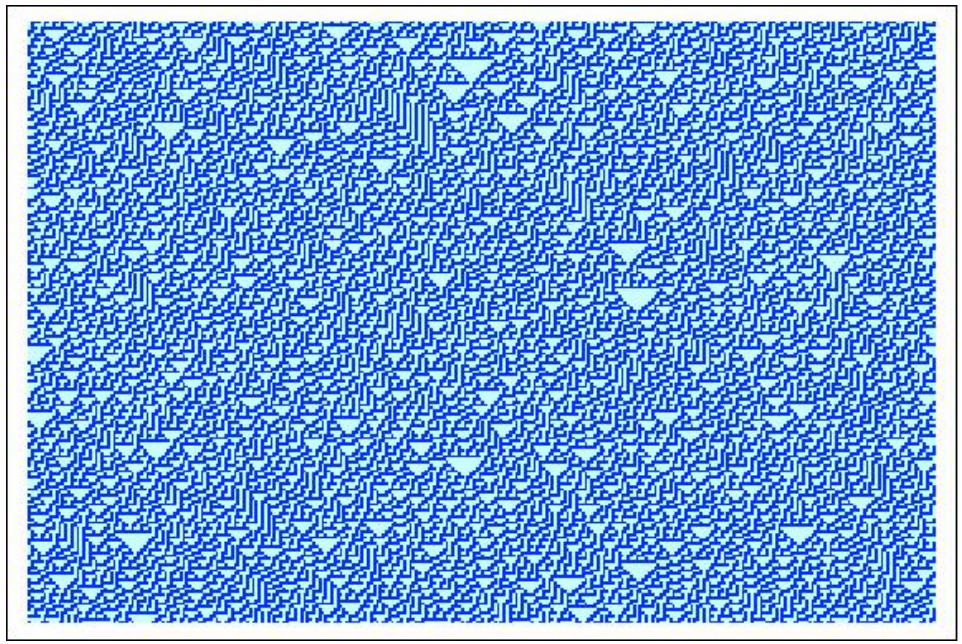
More Questions

- What happens to the degree of the sets constructed by Friedberg-Muchnik when the enumeration is changed?
- Can one dispense of a whole class of constructions (say, finite injury priority arguments or the low basis theorem)?
- Again: Is there an intermediate computational process?

A Rumination on Randomness

Work by Simpson et.al. suggests that natural examples of intermediate degrees can be found if one adopts a different notion of reduction (Muchnik degrees). One of the natural examples is based on randomness (Martin-Löf).

So how about rule 30?



Thank You!

Priority Arguments

Construct two r.e. sets A and B that are incomparable with respect to Turing reducibility.

So the goal is

$$A \not\leq_T B \qquad \text{and} \qquad B \not\leq_T A.$$

Intermediate as a side-effect, almost an accident.

The Construction

Construct sets in stages: $A = \bigcup A^\sigma$ and $B = \bigcup B^\sigma$ where $\sigma < \omega$. At each stage, add elements to A and B trying to satisfy the following requirements:

R_e: $A \neq \{e\}^B$

R'_e: $B \neq \{e\}^A$

Idea: if $\{e\}^B(x) = 0$ then throw x into A.

Injuries

Big Problem: There are infinitely many requirements, and they clash.

Suppose at stage σ we work on R_e: we place x into A so that

$$A(x) = 1 \neq 0 = \{e\}^B(x)$$

But that will in general change the result of some computation $\{e'\}^A(z)$ since the oracle $A^{<\sigma}$ is different from $A^{\leq\sigma}$.

So we may have ruined $R'_{e'}$.

Priorities

The solution is to order the requirements and prefer a higher-priority requirement over a lower-priority one.

$$R_0, R'_0, R_1, R'_1, R_2, R'_2, R_3, R'_3, \ldots$$

A requirement may get clobbered by a higher-priority requirement.
But: this can happen only a finite number of times, ultimately it will be satisfied.

- We get an artificial, non-structural solution; the raison d'être of A (or B) is just to get a solution to Post's Problem.
- As a computational process, observing either A or B produces an intermediate set.
- But observing both at the same time yields a complete set.

◀ Return

- We get an artificial, non-structural solution; the raison d'être of A (or B) is just to get a solution to Post's Problem.
- As a computational process, observing either A or B produces an intermediate set.
- But observing both at the same time yields a complete set.

◀ Return

- We get an artificial, non-structural solution; the raison d'étre of A (or B) is just to get a solution to Post's Problem.
- As a computational process, observing either A or B produces an intermediate set.
- But observing both at the same time yields a complete set.

◀ Return

Fixed Point Free Functions

A total function f is fixed point free (FPD) if $f(e) \neq \{e\}(e)$ for all e.

Theorem (Kucera 1986)

Let f be fixed point free, $f \leq_T \emptyset'$. Then there exists a simple set S such that $S \leq_T f$.

An r.e. set S is simple if $\mathbb{N} - S$ is infinite but $(\mathbb{N} - S) \cap W_e$ is finite for all e.

The Low Basis Theorem

A Π^0_1-class of sets is given by a recursive tree $T \subseteq \mathbf{2}^{<\omega}$. The class consists of all infinite branches in the tree.

Theorem

The low degrees form a basis for Π^0_1-classes of sets.

Kucera's Construction

Break up the problem into two natural parts:

- Use his theorem to obtain a simple (and thus non-recursive) set,
- use the Low Basis Theorem to insure that the set is non-complete.

Alas, as a computational process Kucera's construction is also complete.

Return