Recursion Theory

Joost J. Joosten

Institute for Logic Language and Computation
University of Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam
Room P 3.26, +31 20 5256095
jjoosten@phil.uu.nl
www.phil.uu.nl/~jjoosten
Natural examples of incomputability

- Incomputable sets:
Natural examples of incomputability

- Incomputable sets: $K$, 
Natural examples of incomputability

Incomputable sets: $K$, $K_0$, 
Natural examples of incomputability

Incomputable sets: $K$, $K_0$, Simple sets
Natural examples of incomputability

- Incomputable sets: $K$, $K_0$, Simple sets
- Are there mathematical examples?
Natural examples of incomputability

- Incomputable sets: $K$, $K_0$, Simple sets
- Are there mathematical examples?
- Hilbert’s tenth problem
Natural examples of incomputability

- Incomputable sets: $K$, $K_0$, Simple sets
- Are there mathematical examples?
- Hilbert’s tenth problem
- Diophantine equations (Alexandria, +- 250 AD) have solutions?
Natural examples of incomputability

- Incomputable sets: $K$, $K_0$, Simple sets
- Are there mathematical examples?
- Hilbert’s tenth problem
- Diophantine equations (Alexandria, +- 250 AD) have solutions?
- $\{n \mid x^n + y^n = z^n \text{ for some natural numbers } x, y, z\}$ undecidable?
Natural examples of incomputability

- Incomputable sets: $K$, $K_0$, Simple sets
- Are there mathematical examples?
- Hilbert’s tenth problem
- Diophantine equations (Alexandria, +- 250 AD) have solutions?
  \[ \{ n \mid x^n + y^n = z^n \text{ for some natural numbers } x, y, z \} \text{ undecidable?} \]
- General definition of a Diophantine set (we can interpret the integers into the natural numbers)
Natural examples of incomputability

- Incomputable sets: $K$, $K_0$, Simple sets
- Are there mathematical examples?
- Hilbert’s tenth problem
- Diophantine equations (Alexandria, +- 250 AD) have solutions?
  \[ \{ n \mid x^n + y^n = z^n \text{ for some natural numbers } x, y, z \} \]
  undecidable?
- General definition of a Diophantine set (we can interpret the integers into the natural numbers (and also the other way around) )
Example: \( \{ x \mid x \neq 2(4) \} \) is Diophantine
Example: \( \{ x \mid x \neq 2(4) \} \) is Diophantine

The polynomial that does it is: \( y_1^2 - y_2^2 - x \) by some non-trivial number theory
Example: \( \{ x \mid x \neq 2(4) \} \) is Diophantine

The polynomial that does it is: \( y_1^2 - y_2^2 - x \) by some non-trivial number theory

Conjecture of Martin Davis (1950): every c.e. set is Diophantine.
Example: \( \{x \mid x \neq 2(4)\} \) is Diophantine

The polynomial that does it is: \( y_1^2 - y_2^2 - x \) by some non-trivial number theory

Conjecture of Martin Davis (1950): every c.e. set is Diophantine.

Together with Putnam and Julia Robinson: almost proved, provided there exists an exponential set which is Diophantine.
Matiasevich

Matiasevich, 1970: The Fibonacci sequence is Diophantine. Chudnovsky claims to have simultaneously solved it.

)
Matiasevich, 1970: The Fibonacci sequence is Diophantine (Chudnovsky claims to have simultaneously solved it.)
Matiasevich, 1970: The Fibonacci sequence is Diophantine (Chudnovsky claims to have simultaneously solved it (Post (21)/Gödel (31)) )
Matiasevich, 1970: The Fibonacci sequence is Diophantine (Chudnovsky claims to have simultaneously solved it (Post (21)/Gödel (31)))

Matiasevich calls it the DPRM-theorem!
Matiasevich, 1970: The Fibonacci sequence is Diophantine (Chudnovsky claims to have simultaneously solved it (Post (21)/Gödel (31)));

Matiasevich calls it the DPRM-theorem!

Fibonacci sequence grows about as

\[ \frac{1}{\sqrt{5}} \left[ \frac{1}{2} (1 + \sqrt{5}) \right]^{n+1} \]
Matiasevich

• Matiasevich, 1970: The Fibonacci sequence is Diophantine (Chudnovsky claims to have simultaneously solved it (Post (21)/Gödel (31)) )
• Matiasevich calls it the DPRM-theorem!
• Fibonacci (Liber Abaci, 1202, Leonardo Pisano) sequence grows about as

\[ \frac{1}{\sqrt{5}} \left[ \frac{1}{2} \left(1 + \sqrt{5}\right) \right]^{n+1} \]
Matiasevich, 1970: The Fibonacci sequence is Diophantine (Chudnovsky claims to have simultaneously solved it (Post (21)/Gödel (31))

Matiasevich calls it the DPRM-theorem!

Fibonacci (Liber Abaci, 1202, Leonardo Pisano) sequence grows about as

$$\frac{1}{\sqrt{5}} \left[ \frac{1}{2} (1 + \sqrt{5}) \right]^{n+1}$$

There is a nice exercise in Terwijn’s reader to the effect that

$$a_n := \frac{1}{\sqrt{5}} \left[ \frac{1}{2} (1 + \sqrt{5}) \right]^{n+1} - \frac{1}{\sqrt{5}} \left[ \frac{1}{2} (1 - \sqrt{5}) \right]^{n+1}$$
More on Hilbert 10

- Fibonacci numbers are Diophantine with degree 3
More on Hilbert 10

- Fibonacci numbers are Diophantine with degree 3
- Every c.e. set has at most degree 9
More on Hilbert 10

- Fibonacci numbers are Diophantine with degree 3
- Every c.e. set has at most degree 9
- It is not known if this can be lowered
More on Hilbert 10

- Fibonacci numbers are Diophantine with degree 3
- Every c.e. set has at most degree 9
- It is not known if this can be lowered
- Corollary: there is a polynomial enumerating the primes
More on Hilbert 10

- Fibonacci numbers are Diophantine with degree 3
- Every c.e. set has at most degree 9
- It is not known if this can be lowered
- Corollary: there is a polynomial enumerating the primes
- No polynomial for $K$ has yet been found
More on Hilbert 10

- Fibonacci numbers are Diophantine with degree 3
- Every c.e. set has at most degree 9
- It is not known if this can be lowered
- Corollary: there is a polynomial enumerating the primes

- No polynomial for $K$ has yet been found
- Hilbert over algebraic fields is unknown
More on Hilbert 10

- Fibonacci numbers are Diophantine with degree 3
- Every c.e. set has at most degree 9
- It is not known if this can be lowered
- Corollary: there is a polynomial enumerating the primes

- No polynomial for $K$ has yet been found
- Hilbert over algebraic fields is unknown
- In particular: is $\mathbb{Z}$ Diophantine over $\mathbb{Q}$?
Natural simple sets

Randomness and Kolmogorov complexity (7.3 of reader Terwijn)
Natural simple sets

Randomness and Kolmogorov complexity (7.3 of reader Terwijn)

Fix a universal TM $U$
Natural simple sets

- Randomness and Kolmogorov complexity (7.3 of reader Terwijn)
- Fix a universal TM $U$
- Kolm. Compl. of a string $\sigma$ is $\pm$ the length of the shortest TM program that on empty input outputs $\sigma$
Natural simple sets

- Randomness and Kolmogorov complexity (7.3 of reader Terwijn)
- Fix a universal TM $U$
- Kolm. Compl. of a string $\sigma$ is +- the length of the shortest TM program that on empty input outputs $\sigma$
- Is dependent on $U$
Natural simple sets

- Randomness and Kolmogorov complexity (7.3 of reader Terwijn)
- Fix a universal TM $U$
- Kolm. Compl. of a string $\sigma$ is +- the length of the shortest TM program that on empty input outputs $\sigma$
- Is dependent on $U$ but only in a $O(1)$ sense
Natural simple sets

- Randomness and Kolmogorov complexity (7.3 of reader Terwijn)

- Fix a universal TM $U$

- Kolm. Compl. of a string $\sigma$ is $\pm$ the length of the shortest TM program that on empty input outputs $\sigma$

- Is dependent on $U$ but only in a $O(1)$ sense

- A string $\sigma$ is $k$-random if $C(\sigma) \geq |\sigma| - k$
Natural simple sets

- Randomness and Kolmogorov complexity (7.3 of reader Terwijn)
- Fix a universal TM $U$
- Kolm. Compl. of a string $\sigma$ is +- the length of the shortest TM program that on empty input outputs $\sigma$
- Is dependent on $U$ but only in a $O(1)$ sense
- A string $\sigma$ is $k$-random if $C(\sigma) \geq |\sigma| - k$
- The set of non-$k$-random strings is simple
Comparing incomputability

Compare the incomputable sets
Comparing incomputability

- Compare the incomputable sets
- Are some sets less computable than others
Comparing incomputability

- Compare the incomputable sets
- Are some sets less computable than others
- Notion of *many-one reducability*
Comparing incomputability

- Compare the incomputable sets
- Are some sets less computable than others
- Notion of *many-one reducability*
- Important features:
Comparing incomputability

- Compare the incomputable sets
- Are some sets less computable than others
- Notion of *many-one reducability*
- Important features:
  - $B \leq_m A$ and $A$ decidable, then $B$ decidable
Comparing incomputability

- Compare the incomputable sets
- Are some sets less computable than others
- Notion of many-one reducability

Important features:
- $B \leq_m A$ and $A$ decidable, then $B$ decidable
- $B \leq_m A$ and $B$ undecidable, then $A$ undecidable
Comparing incomputability

- Compare the incomputable sets
- Are some sets less computable than others
- Notion of *many-one reducability*
- Important features:
  - $B \leq_m A$ and $A$ decidable, then $B$ decidable
  - $B \leq_m A$ and $B$ undecidable, then $A$ undecidable
  - $B \leq_m A$ and $A$ c.e, then $B$ c.e.
Comparing incomputability

- Compare the incomputable sets
- Are some sets less computable than others
- Notion of many-one reducability

Important features:
- \( B \leq_m A \) and \( A \) decidable, then \( B \) decidable
- \( B \leq_m A \) and \( B \) undecidable, then \( A \) undecidable
- \( B \leq_m A \) and \( A \) c.e., then \( B \) c.e.

Application: \( K_0 \) is undecidable (not computable)
Comparing incomputability

- Compare the incomputable sets
- Are some sets less computable than others
- Notion of *many-one reducability*
- Important features:
  - $B \leq_m A$ and $A$ decidable, then $B$ decidable
  - $B \leq_m A$ and $B$ undecidable, then $A$ undecidable
  - $B \leq_m A$ and $A$ c.e., then $B$ c.e.
- Application: $K_0$ is undecidable (not computable)
- Actually $K \leq_1 K_0$
Comparing incomputability

- Compare the incomputable sets
- Are some sets less computable than others
- Notion of *many-one reducability*

Important features:
- \( B \leq_m A \) and \( A \) decidable, then \( B \) decidable
- \( B \leq_m A \) and \( B \) undecidable, then \( A \) undecidable
- \( B \leq_m A \) and \( A \) c.e, then \( B \) c.e.

Application: \( K_0 \) is undecidable (not computable)
- Actually \( K \leq_1 K_0 \)
- \( A \) is c.e. iff \( A \leq_m K_0 \)
Index sets

\( \mathcal{A} \) is an index set if \( e \in \mathcal{A} \) and \( W_e = W_{e'} \) implies \( e' \in \mathcal{A} \)
Index sets

- $\mathcal{A}$ is an index set if $e \in \mathcal{A}$ and $W_e = W_{e'}$ implies $e' \in \mathcal{A}$
- Examples: Tot and $K_1$
Index sets

- $A$ is an index set if $e \in A$ and $W_e = W_{e'}$ implies $e' \in A$
- Examples: $\text{Tot}$ and $K_1$
- $K_1 := \{ x \mid W_x \neq \emptyset \}$
Index sets

- \( A \) is an index set if \( e \in A \) and \( W_e = W_{e'} \) implies \( e' \in A \)

- Examples: \( \text{Tot} \) and \( K_1 \)

- \( K_1 := \{ x \mid W_x \neq \emptyset \} \)

- Theorem: \( K \) is not an index set
Index sets

- \( \mathcal{A} \) is an index set if \( e \in \mathcal{A} \) and \( W_e = W_{e'} \) implies \( e' \in \mathcal{A} \)

Examples: Tot and \( K_1 \)

\( K_1 := \{ x \mid W_x \neq \emptyset \} \)

Theorem: \( K \) is not an index set

Proof idea: make a singleton set consisting only of its code \( e \), using the padding lemma, find another code \( e' \) of this set. Then, \( e \in K \) and \( e' \notin K \).
Rice’s Theorem

If $A$ is an index set – not equal to $\emptyset$ or $\mathbb{N}$ –, then $A$ is incomputable
Rice’s Theorem

If $A$ is an index set – not equal to $\emptyset$ or $\mathbb{N}$ –, then $A$ is incomputable.

First step: it is sufficient to show that either $K \leq_m A$ or $K \leq_m \overline{A}$. 
Rice’s Theorem

- If $A$ is an index set – not equal to $\emptyset$ or $\mathbb{N}$ –, then $A$ is incomputable.

- First step: it is sufficient to show that either $K \leq_m A$ or $K \leq_m \overline{A}$.

- Case distinction $\emptyset$ has no code in $A$, or it has
Rice’s Theorem

- If $A$ is an index set – not equal to $\emptyset$ or $\mathbb{N}$ –, then $A$ is incomputable.
- First step: it is sufficient to show that either $K \leq_m A$ or $K \leq_m \overline{A}$.
- Case distinction $\emptyset$ has no code in $A$, or it has.
- By assumption, there is some $e \in A$ and some $e' \in \overline{A}$. 

Recursion Theory – p.9/11
Rice’s Theorem

- If $A$ is an index set – not equal to $\emptyset$ or $\mathbb{N}$ –, then $A$ is incomputable.
- First step: it is sufficient to show that either $K \leq_m A$ or $K \leq_m \overline{A}$.
- Case distinction $\emptyset$ has no code in $A$, or it has.
- By assumption, there is some $e \in A$ and some $e' \in \overline{A}$.
- First idea: Define $f(x) := e$ if $x \in K$ and
Rice’s Theorem

- If $A$ is an index set – not equal to $\emptyset$ or $\mathbb{N}$ –, then $A$ is incomputable

- First step: it is sufficient to show that either $K \leq_m A$ or $K \leq_m \overline{A}$

- Case distinction $\emptyset$ has no code in $A$, or it has

- By assumption, there is some $e \in A$ and some $e' \in \overline{A}$

- First idea: Define $f(x) := e$ if $x \in K$ and

- $f(x) := e'$ if $x \notin K$
Rice’s Theorem

- If $A$ is an index set – not equal to $\emptyset$ or $\mathbb{N}$ –, then $A$ is incomputable
- First step: it is sufficient to show that either $K \leq_m A$ or $K \leq_m \overline{A}$
- Case distinction $\emptyset$ has no code in $A$, or it has
- By assumption, there is some $e \in A$ and some $e' \in \overline{A}$
- First idea: Define $f(x) := e$ if $x \in K$ and $f(x) := e'$ if $x \notin K$
- Then: $K \leq_m A$
Rice’s Theorem

- If $A$ is an index set – not equal to $\emptyset$ or $\mathbb{N}$ –, then $A$ is incomputable.

- First step: it is sufficient to show that either $K \leq_m A$ or $K \leq_m \overline{A}$.

- Case distinction $\emptyset$ has no code in $A$, or it has.

- By assumption, there is some $e \in A$ and some $e' \in \overline{A}$.

- First idea: Define $f(x) := e$ if $x \in K$ and $f(x) := e'$ if $x \notin K$.

- Then: $K \leq_m A : x \in K \iff f(x) \in A$. 

Recursion Theory – p.9/11
Rice’s Theorem

- If $A$ is an index set – not equal to $\emptyset$ or $\mathbb{N}$ –, then $A$ is incomputable
- First step: it is sufficient to show that either $K \leq_m A$ or $K \leq_m \overline{A}$
- Case distinction $\emptyset$ has no code in $A$, or it has
- By assumption, there is some $e \in A$ and some $e' \in \overline{A}$
- First idea: Define $f(x) := e$ if $x \in K$ and $f(x) := e'$ if $x \notin K$. 
- Then: $K \leq_m A : x \in K \iff f(x) \in A$
- Alas: $f$ is not computable
Rice’s Theorem

Second idea: Define $f(x) := e$ if $x \in K$ and
Rice’s Theorem

- Second idea: Define $f(x) := e$ if $x \in K$ and undefined otherwise.
Rice’s Theorem

Second idea: Define $f(x) := e$ if $x \in K$ and undefined otherwise.

Now $f$ is partially computable.
Rice’s Theorem

- Second idea: Define \( f(x) := e \) if \( x \in K \) and
- and undefined otherwise.
- Now \( f \) is partially computable.
- and: \( x \in K \iff f(x) \downarrow \in A \)
Rice’s Theorem

- Second idea: Define \( f(x) := e \) if \( x \in K \) and
- and undefined otherwise.
- Now \( f \) is partially computable.
- and: \( x \in K \iff f(x) \downarrow \in A \)
- But \( f \) is not total, so no reduction
Rice’s Theorem

- Second idea: Define $f(x) := e$ if $x \in K$ and undefined otherwise.
- Now $f$ is partially computable.
- and: $x \in K \iff f(x) \downarrow \in A$
- But $f$ is not total, so no reduction
- Final idea: $W_f(x) := W_e$ if $x \in K$
Rice’s Theorem

Second idea: Define \( f(x) := e \) if \( x \in K \) and undefined otherwise.

Now \( f \) is partially computable.

and: \( x \in K \iff f(x) \downarrow \in A \)

But \( f \) is not total, so no reduction

Final idea: \( W_{f(x)} := W_e \) if \( x \in K \)

and \( \emptyset \) otherwise.
Rice’s Theorem

- Second idea: Define \( f(x) := e \) if \( x \in K \) and
- and undefined otherwise.
- Now \( f \) is partially computable.
- and: \( x \in K \iff f(x) \downarrow \in A \)
- But \( f \) is not total, so no reduction
- Final idea: \( W_f(x) := W_e \) if \( x \in K \)
- and \( \emptyset \) otherwise.
- The case that \( \emptyset \) has a code in \( A \) goes similar (misprint)
Rice applications

Fin
Rice applications

- Fin
- Inf
Rice applications

- Fin
- Inf
- Cof
Rice applications

- Fin
- Inf
- Cof
- Virus scanner does not exist and \textit{cannot} exist!!!
Rice applications

- Fin
- Inf
- Cof
- Virus scanner does not exist and *cannot* exist!!!
- and much more