# Can everything be computed? On the Solvability Complexity Index and towers of algorithms

Anders C. Hansen (Cambridge)

Joint work with:

J. Ben-Artzi (Cambridge)
O. Nevanlinna (Aalto)
M. Seidel (Chemnitz)

Chicheley Hall, July 1, 2014

# Gödel's Incompleteness Theorem

"Any effectively generated theory capable of expressing elementary arithmetic cannot be both consistent and complete. In particular, for any consistent, effectively generated formal theory that proves certain basic arithmetic truths, there is an arithmetical statement that is true, but not provable in the theory"

- Gödel suggests that there are things that are not possible to compute.
- Do we know about an example?
- Need to specify the "tools" or operations allowed.

# Examples

- Let $A = \{a_{ij}\}_{i,j\in\mathbb{N}} \in \mathcal{B}(\ell^2(\mathbb{N}))$.
  - Problem: Compute the spectrum $\mathrm{Sp}(A)$.
  - Tools allowed: arithmetic operations and radicals of $a_{ij}$, and taking limits.
- Let $A = \{a_{ij}\}_{i,j\in\mathbb{N}} \in \mathcal{B}(\ell^2(\mathbb{N}))$.
  - Problem: Solve $Ax = y$.
  - Tools allowed: arithmetic operations and radicals of $a_{ij}$ and $y_i$, and taking limits.
- Let $H = -\Delta + V$, $V \in L^\infty(\mathbb{R}) \cap C(\mathbb{R})$, $\mathcal{D}(H) = W^{2,2}(\mathbb{R})$.
  - Problem: Compute the spectrum $\mathrm{Sp}(H)$.
  - Tools allowed: arithmetic operations and radicals of $V(t), t \in \mathbb{R}$, and taking limits.
- Let $p \in \mathbb{P}_n$, $n > 4$.
  - Problem: Compute a root of $p$.
  - Tools allowed: iterations of a rational map $R$, and taking one limit.

# Examples

- Let $p \in \mathbb{P}_n$, $n > 4$.
  - Problem: Compute a root of $p$.
  - Tools allowed: iterations of a rational map $R$, and taking one limit.

Smale: " Does there exist, for any $n \in \mathbb{N}$, a map $R : \mathbb{P}_n \to \mathrm{rat}(\mathbb{C})$ such that for all $p \in \mathbb{P}_n$, $R_p^k(\omega) \to \lambda$ as $k \to \infty$ and $\lambda$ is a root of $p$, where $\omega$ is in an open dense set of $\mathbb{C}$?"

# Examples

- Let $p \in \mathbb{P}_n$, $n > 4$.
  - Problem: Compute a root of $p$.
  - Tools allowed: iterations of a rational map $R$, and taking one limit.

Smale: " Does there exist, for any $n \in \mathbb{N}$, a map $R : \mathbb{P}_n \to \mathrm{rat}(\mathbb{C})$ such that for all $p \in \mathbb{P}_n$, $R_p^k(\omega) \to \lambda$ as $k \to \infty$ and $\lambda$ is a root of $p$, where $\omega$ is in an open dense set of $\mathbb{C}$?"

Theorem (McMullen, Annals of math '87)

*No!*

Theorem (Doyle and McMullen, Acta Math '89)

*There exists maps* $R_i : \mathbb{P}_5 \to \mathrm{rat}(\mathbb{C})$, $i = 1, 2, 3$ *such that for all* $\omega$ *in a dense open set of* $\mathbb{C}$ *we get that*

$$\begin{aligned} \lambda_1 &= \lim_{k\to\infty} R^k_{1,p}(\omega), \qquad p \in \mathbb{P}_5, \\ \lambda_2 &= \lim_{k\to\infty} R^k_{2,f_1(\lambda_1)}(\omega) \\ \lambda_3 &= \lim_{k\to\infty} R^k_{3,f_2(\lambda_1,\lambda_2)}(\omega) \end{aligned}$$

*where the evaluation of* $f_i : \mathbb{C}^{n_i} \to \mathbb{C}^5$ *requires finitely many arithmetic operations, and* $\lambda_3$ *is a root of* $p$.

# Examples

- Let $A = \{a_{ij}\}_{i,j\in\mathbb{N}} \in \mathcal{B}(\ell^2(\mathbb{N}))$.
  - Problem: Compute the spectrum $\sigma(A)$.
  - Tools allowed: arithmetic operations and radicals of $a_{ij}$, and taking limits.
- The problem has been open for a long time, however, E. B. Davies, expressed his concern in "A defence of mathematical pluralism", *Philos. Math* (2005), and suggested that the answer could very well be negative.

# Examples

- Let $A = \{a_{ij}\}_{i,j \in \mathbb{N}} \in \mathcal{B}(\ell^2(\mathbb{N}))$.
  - Problem: Compute the spectrum $\sigma(A)$.
  - Tools allowed: arithmetic operations and radicals of $a_{ij}$, and taking limits.

**Theorem (H, J. Amer. Math. Soc. '11)**

*The above problem can be solved.*

Problem: The computation requires 3 limits. Is this sharp?

# The Solvability Complexity Index

The Solvability Complexity Index is the smallest number of limits needed to compute a problem.

# The Setup

(i) $\Omega$ is some set, called the *primary* set,

(ii) $\Lambda$ is a set of complex valued functions on $\Omega$, called the *evaluation* set,

(iii) $(\mathcal{M}, d)$ is a pseudo metric space,

(iv) $\Xi : \Omega \to \mathcal{M}$, called the *problem* function.

### Example

- Let $\Omega = \mathcal{B}(\mathcal{H})$, the set of all bounded linear operators on a separable Hilbert space $\mathcal{H}$
- the problem function $\Xi$ be the mapping $A \mapsto \mathrm{sp}(A)$ (the spectrum of $A$),
- $(\mathcal{M}, d)$ is the set of all compact subsets of $\mathbb{C}$ provided with the Hausdorff metric.
- The evaluation functions in $\Lambda$ could for example consist of the family of all functions $f_{i,j} : A \mapsto \langle Ae_j, e_i \rangle$, $i, j \in \mathbb{N}$, which provide the entries of the matrix representation of $A$ w.r.t. an orthonormal basis $\{e_i\}_{i\in\mathbb{N}}$

# Computational Problem

**Definition (Computational problem)**

Given a primary set $\Omega$, an evaluation set $\Lambda$, a (pseudo) metric space $\mathcal{M}$ and a problem function $\Xi : \Omega \to \mathcal{M}$ we call the collection $\{\Xi, \Omega, \mathcal{M}, \Lambda\}$ a computational problem.

### Definition (General Algorithm)

Given a computational problem $\{\Xi, \Omega, \mathcal{M}, \Lambda\}$, a *general algorithm* is a mapping $\Gamma : \Omega \to \mathcal{M}$ such that for each $A \in \Omega$

(i) there exists a finite subset of evaluations $\Lambda_\Gamma(A) \subset \Lambda$ ,

(ii) the action of $\Gamma$ on $A$ only depends on $\{A_f\}_{f \in \Lambda_\Gamma(A)}$ where $A_f := f(A)$,

(iii) for every $B \in \Omega$ such that $B_f = A_f$ for every $f \in \Lambda_\Gamma(A)$, it holds that $\Lambda_\Gamma(B) = \Lambda_\Gamma(A)$.

## Definition (Tower of algorithms)

Given a computational problem $\{\Xi, \Omega, \mathcal{M}, \Lambda\}$, a *tower of algorithms of height $k$ for* $\{\Xi, \Omega, \mathcal{M}, \Lambda\}$ is a family of sequences of functions

$$\begin{aligned} \Gamma_{n_k} &: \Omega \to \mathcal{M}, \\ \Gamma_{n_k, n_{k-1}} &: \Omega \to \mathcal{M}, \\ &\vdots \\ \Gamma_{n_k, \ldots, n_1} &: \Omega \to \mathcal{M}, \end{aligned}$$

where $n_k, \ldots, n_1 \in \mathbb{N}$ and the functions $\Gamma_{n_k, \ldots, n_1}$ at the lowest level in the tower are general algorithms in the sense of Definiton 6. Moreover, for every $A \in \Omega$,

$$\begin{aligned} \Xi(A) &= \lim_{n_k \to \infty} \Gamma_{n_k}(A), \\ \Gamma_{n_k}(A) &= \lim_{n_{k-1} \to \infty} \Gamma_{n_k, n_{k-1}}(A), \\ &\vdots \\ \Gamma_{n_k, \ldots, n_2}(A) &= \lim_{n_1 \to \infty} \Gamma_{n_k, \ldots, n_1}(A), \end{aligned} \tag{1}$$

where $S = \lim_{n \to \infty} S_n$ means convergence $S_n \to S$ in the metric space $\mathcal{M}$.

Definition (Solvability complexity index)

- Given a computational problem $\{\Xi, \Omega, \mathcal{M}, \Lambda\}$, it is said to have *Solvability Complexity Index* $\mathrm{SCI}(\Xi, \Omega, \mathcal{M}, \Lambda)_\alpha = k$ with respect to a tower of algorithms of type $\alpha$ if $k$ is the smallest integer for which there exists a tower of algorithms of type $\alpha$ of height $k$.
- If no such tower exists then $\mathrm{SCI}(\Xi, \Omega, \mathcal{M}, \Lambda)_\alpha = \infty$.
- If there exists a tower $\{\Gamma_n\}_{n\in\mathbb{N}}$ of type $\alpha$ and height one such that $\Xi = \Gamma_{n_1}$ for some $n_1 < \infty$, then we define $\mathrm{SCI}(\Xi, \Omega, \mathcal{M}, \Lambda)_\alpha = 0$.

### Definition (Radical towers)

Given a computational problem $\{\Xi, \Omega, \mathcal{M}, \Lambda\}$ we define the following:

(ii) A *Radical tower of algorithms* of height $k$ for $\{\Xi, \Omega, \mathcal{M}, \Lambda\}$ is a tower of algorithms where the lowest functions $\Gamma = \Gamma_{n_k,\ldots,n_1} : \Omega \to \mathcal{M}$ satisfy the following: For each $A \in \Omega$ the action of $\Gamma$ on $A$ consists of only performing finitely many arithmetic operations on and extracting radicals of $\{A_f\}_{f \in \Lambda_\Gamma(A)}$.

# The $n$-pseudospectrum

Definition

Let $T$ be a closed operator on a Hilbert space $\mathcal{H}$ such that $\sigma(T) \neq \mathbb{C}$, and let $n \in \mathbb{Z}_+$ and $\epsilon > 0$. The $(n, \epsilon)$-pseudospectrum of $T$ is defined as the set

$$\mathrm{Sp}_{n,\epsilon}(T) = \sigma(T) \cup \{z \notin \sigma(T) : \|(T - z)^{-2^n}\|^{1/2^n} > \epsilon^{-1}\}.$$

# Computing spectra and pseudospectra of bounded infinite matrices

**Theorem**

*Let* $\Omega = \mathcal{B}(\ell^2(\mathbb{N}))$ *and* $\Xi_1 : A \mapsto \mathrm{Sp}(A)$. *Define also, for* $n \in \mathbb{N}$ *and* $\epsilon > 0$,

$$\Xi_2 : A \mapsto \mathrm{Sp}_{n,\epsilon}(A).$$

*Then*

$$\mathrm{SCI}(\Xi_1)_{\mathrm{G}} = \mathrm{SCI}(\Xi_1)_{\mathrm{R}} = 3, \qquad \mathrm{SCI}(\Xi_1)_{\mathrm{G}} = \mathrm{SCI}(\Xi_1)_{\mathrm{R}} = 2.$$

**Theorem**

*Let*

$$\Omega = \{A \in \mathcal{B}(\ell^2(\mathbb{N})) : A = A^*\}$$

*and define*

$$\Xi : A \mapsto \mathrm{Sp}(A).$$

*Then*

$$\mathrm{SCI}(\Xi)_{\mathrm{G}} = \mathsf{SCI}(\Xi)_{\mathrm{R}} = 2. \tag{2}$$

# The SCI and the impossibility of error control

- We want to control the convergence

$$\Gamma_{n_k} \to \Xi, \ldots, \Gamma_{n_k,\ldots,n_1} \to \Gamma_{n_k,\ldots,n_2}.$$

- For $\epsilon > 0$, how big does $n_k, \ldots, n_1$ have to be such that

$$d(\Gamma_{n_k,\ldots,n_1}(v), \Xi(v)) \leq \epsilon, \qquad \forall\, v \in \Omega.$$

**Theorem**

*Given a computational problem $\{\Xi, \Omega, \mathcal{M}, \Lambda\}$ with $\mathrm{SCI}(\Xi, \Omega, \mathcal{M}, \Lambda)_{\mathrm{G}} \geq 2$. Let $\{\epsilon_m\}_{m\in\mathbb{N}}$ be a sequence such that $\epsilon_m \to 0$ as $m \to \infty$. Then there do NOT exist integers $n_k = n_k(m), \ldots, n_1 = n_1(m)$ (depending on $m$) such that*

$$d(\Gamma_{n_k,\ldots,n_1}(A), \Xi(A)) \leq \epsilon_m, \qquad \forall\, A \in \Omega, \quad \forall\, m \in \mathbb{N}.$$

**Theorem**

*Let* $\mathcal{B}_{\mathrm{inv}}(l^2(\mathbb{N}))$ *denote the set of bounded invertible operators and define the domain* $\Omega = \mathcal{B}_{\mathrm{inv}}(l^2(\mathbb{N})) \times l^2(\mathbb{N})$*. Then*

$$\mathrm{SCI}(\Xi)_{\mathrm{G}} = \mathrm{SCI}(\Xi)_{\mathrm{R}} = 2, \tag{3}$$

# Finding roots of polynomials

- Let $\Omega = \mathbb{P}_s$, the set of polynomials of degree $s$ over $\mathbb{C}$.
- Let the problem function $\Xi$ be the mapping $p \mapsto \{\alpha \in \mathbb{C} | \, p(\alpha) = 0\}$ (the roots of $p$).
- Let $(\mathcal{M}, d)$ denote the collection of finite sets of points in $\mathbb{C}$ equipped with the pseudo metric $d : \mathcal{M} \times \mathcal{M} \to [0, \infty]$, defined by $d(x, y) = \min_{1 \leq i \leq n, 1 \leq j \leq m} |x_j - y_i|$, where $x = \{x_1, \ldots, x_n\}, y = \{y_1, \ldots, y_m\} \in \mathcal{M}$.

# Doyle-McMullen Tower

### Definition (Doyle-McMullen tower)

A tower of algorithms is a finite sequence of generally convergent algorithms, linked together serially, so the output of one or more can be used to compute the input to the next. The final output of the tower is a single number, computed rationally from the original input and the outputs of the intermediate generally convergent algorithms.

The result of Doyle and McMullen's work

$$\mathrm{SCI}(\Xi)_{\mathrm{DM}} \begin{cases} = 1 & s \leq 3, \\ \in \{2, 3\} & s = 4, 5, \\ = \infty & s \geq 6. \end{cases}$$

Let

$$\Omega := \{V : V \in \mathrm{L}^\infty(\mathbb{R}^d) \cap \mathrm{BV}_\phi(\mathbb{R}^d)\},$$

where $\phi : [0,\infty) \to [0,\infty)$ is some increasing function and

$$\mathrm{BV}_\phi(\mathbb{R}^d) = \{f : \mathrm{TV}(f_{[-a,a]^d}) \leq \phi(a)\},$$

($f_{[-a,a]^d}$ means $f$ restricted to the box $[-a,a]^d$).

**Theorem**

*Let $\mathcal{D}(H) = \mathrm{W}^{2,2}(\mathbb{R}^d)$ and define $\Xi_1(V) = \mathrm{sp}(H)$ and, for $\epsilon > 0$, let $\Xi_2(V) = \mathrm{sp}_\epsilon(H)$. Then*

$$\mathrm{SCI}(\Xi_1, \Omega)_{\mathrm{R}} \leq 2, \qquad \mathrm{SCI}(\Xi_2, \Omega_1)_{\mathrm{R}} \leq 2.$$

Let

$$\Psi(x) = \frac{i(\exp(-2\pi i x) - 1)}{2\pi x}, \qquad x \in \mathbb{R},$$

and consider the following Gabor basis for $L^2(\mathbb{R})$:

$$e^{2\pi i m x}\chi_{[0,1]}(x - n), \qquad m, n \in \mathbb{Z}.$$

(where $\chi$ is the characteristic function) and then chosen some enumeration of $\mathbb{Z} \times \mathbb{Z}$ into $\mathbb{N}$ to obtain a basis $\{\psi_j\}$ that is just indexed over $\mathbb{N}$. To get our basis we let $\varphi_j = \mathcal{F}\psi_j$, where $\mathcal{F}$ is the Fourier Transform. Let

$$a(i, j) = \langle \Psi(Q)\varphi_j, \varphi_i \rangle.$$

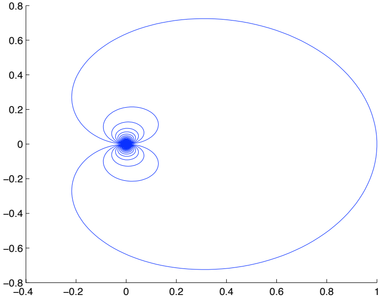
Now we can use

$$\Gamma_{n_3,n_2,n_1}(a)$$

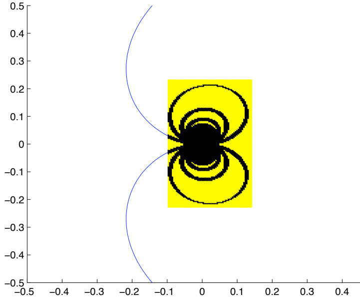
to estimate $\sigma(\Psi(Q))$.

# Tests with the Operator $\Psi(Q)$ for $\Psi \in L^\infty(\mathbb{R})$

$\sigma(\Psi(Q))$




$\Gamma_{n_3,n_2,n_1}(a)$




$n_3 = 100, \qquad n_2 = 10000, \qquad n_1 = 15000.$