Acceptable Complexity Measures of Theorems

Bruno Grenet

Bruno.Grenet@ens-lyon.fr
http://perso.ens-lyon.fr/bruno.grenet/

École Normale Supérieure de Lyon, France

Bloomington – October 31, 2008

Historical Overview

Historical Overview

- 1931: Gödel publishes his Incompleteness Theorem

Historical Overview

- 1931: Gödel publishes his Incompleteness Theorem

Some true mathematical statements are unprovable.

Historical Overview

- 1931: Gödel publishes his Incompleteness Theorem

Some true mathematical statements are unprovable.

  - Are there many such statements?

Historical Overview

- 1931: Gödel publishes his Incompleteness Theorem

Some true mathematical statements are unprovable.

  - Are there many such statements?
  - Are there natural such statements?

Historical Overview

- 1931: Gödel publishes his Incompleteness Theorem

Some true mathematical statements are unprovable.

  - Are there many such statements?
  - Are there natural such statements?
  - Why are they unprovable?

Historical Overview

- 1931: Gödel publishes his Incompleteness Theorem

Some true mathematical statements are unprovable.

  - Are there many such statements?
  - Are there natural such statements?
  - Why are they unprovable?

- 1974: Chaitin proposes his “heuristic principle”

Historical Overview

- 1931: Gödel publishes his Incompleteness Theorem

Some true mathematical statements are unprovable.

  - Are there many such statements?
  - Are there natural such statements?
  - Why are they unprovable?

- 1974: Chaitin proposes his "heuristic principle"

The theorems of a finitely-specified theory cannot be significantly more complex than the theory itself.

Historical Overview

- 1931: Gödel publishes his Incompleteness Theorem

Some true mathematical statements are unprovable.

  - Are there many such statements?
  - Are there natural such statements?
  - Why are they unprovable?

- 1974: Chaitin proposes his “heuristic principle”

The theorems of a finitely-specified theory cannot be significantly more complex than the theory itself.

- 2005: Calude and Jürgensen prove the “heuristic principle”

Goal

- $\delta(x) = H(x) - |x|$ where H is the *program-size* complexity.

Goal

- $\delta(x) = H(x) - |x|$ where H is the *program-size* complexity.
- Is it the only measure satisfying the heuristic principle?

Outline

Outline

Aphabets and strings

For $i \geq 2$,

- X_i: alphabet with i elements

Aphabets and strings

For $i \geq 2$,

- X_i: alphabet with i elements
- X_i^*: set of finite strings on X_i, including the empty string λ

Aphabets and strings

For $i \geq 2$,

- X_i: alphabet with i elements
- X_i^*: set of finite strings on X_i, including the empty string λ
- $|w|_i$: length of w

Aphabets and strings

For $i \geq 2$,

- X_i: alphabet with i elements
- X_i^*: set of finite strings on X_i, including the empty string λ
- $|w|_i$: length of w
- Gödel numbering for the language L: computable one-to-one function $g : L \to X_2^*$

Aphabets and strings

For $i \geq 2$,

- X_i: alphabet with i elements
- X_i^*: set of finite strings on X_i, including the empty string λ
- $|w|_i$: length of w
- Gödel numbering for the language L: computable one-to-one function $g : L \to X_2^*$
- G: set of all the Gödel numberings

Self-delimiting Turing Machines

- Prefix-free set: $u \in S$ implies that $uv \notin S$ $(v \neq \lambda)$

Self-delimiting Turing Machines

- Prefix-free set: $u \in S$ implies that $uv \notin S$ $(v \neq \lambda)$
- $PROG_T = \{x \in X_i^* : T(x) \downarrow\}$

Self-delimiting Turing Machines

- Prefix-free set: $u \in S$ implies that $uv \notin S$ $(v \neq \lambda)$
- $PROG_T = \{x \in X_i^* : T(x) \downarrow\}$

Self-delimiting Turing Machine: $PROG_T$ is prefix-free

Program-size complexity

Definition

$H_{i,T}(x) = \min\{|y|_i : y \in X_i^* \text{ and } T(y) = x\}$

Program-size complexity

Definition

$H_{i,T}(x) = \min \{|y|_i : y \in X_i^* \text{ and } T(y) = x\}$

Invariance Theorem

There exists a universal machine U_i such that for every T, there exists c such that

$$H_{i,U_i}(x) \leq H_{i,T}(x) + c$$

Program-size complexity

Definition

$H_{i,T}(x) = \min \{|y|_i : y \in X_i^* \text{ and } T(y) = x\}$

Invariance Theorem

There exists a universal machine U_i such that for every T, there exists c such that

$$H_{i,U_i}(x) \leq H_{i,T}(x) + c$$

$$H_i \triangleq H_{i,U_i}$$

Outline

Definitions

Definition

$$\delta_i(x) = H_i(x) - |x|_i \, , i \geq 2$$

Definitions

Definition

$$\delta_i(x) = H_i(x) - |x|_i \,, i \geq 2$$

Definition

$$\delta_g(u) = H_2(g(u)) - \lceil \log_2(i) \cdot |x|_i \rceil \,,$$

where g is a Gödel numbering.

Invariance of the measure

Theorem

There exists a constant c such that

$$|H_2(g(u)) - \log_2(i) \cdot H_i(u)| \leq c.$$

Invariance of the measure

Theorem

There exists a constant c such that

$$|H_2(g(u)) - \log_2(i) \cdot H_i(u)| \leq c.$$

Corollary

- With the same constant c as in the theorem, it holds that

$$|\delta_g(u) - \log_2(i) \cdot \delta_i(u)| \leq c + 1.$$

Invariance of the measure

Theorem

There exists a constant c such that

$$|H_2(g(u)) - \log_2(i) \cdot H_i(u)| \leq c.$$

Corollary

- With the same constant c as in the theorem, it holds that

$$|\delta_g(u) - \log_2(i) \cdot \delta_i(u)| \leq c + 1.$$

- For every g and g', there exists a constant d such that

$$\left|H_2(g(u)) - H_2(g'(u))\right| \leq d \text{ and } \left|\delta_g(u) - \delta_{g'}(u)\right| \leq d + 1.$$

Main results about δ_g

- $\mathcal{F}$: finitely-specified, arithmetically sound and consistent theory, strong enough to formalize arithmetic.

Main results about δ_g

- $\mathcal{F}$: finitely-specified, arithmetically sound and consistent theory, strong enough to formalize arithmetic.
- $\mathcal{T}$: set of theorems that $\mathcal{F}$ proves.

Main results about δ_g

- $\mathcal{F}$: finitely-specified, arithmetically sound and consistent theory, strong enough to formalize arithmetic.
- $\mathcal{T}$: set of theorems that $\mathcal{F}$ proves.

Theorem

There exists a constant $N_{\mathcal{F}}$ such that for all $x \in \mathcal{T}$, $\delta_g(x) < N_{\mathcal{F}}$.

Main results about δ_g

- $\mathcal{F}$: finitely-specified, arithmetically sound and consistent theory, strong enough to formalize arithmetic.
- $\mathcal{T}$: set of theorems that $\mathcal{F}$ proves.

Theorem

There exists a constant $N_{\mathcal{F}}$ such that for all $x \in \mathcal{T}$, $\delta_g(x) < N_{\mathcal{F}}$.

Proposition

$\forall N > 0, \lim_{n\to\infty} i^{-n} \cdot \mathrm{card}\,\{x \in X_i^* : |x|_i = n, \delta_g(x) \leq N\} = 0$

Outline

Complexity Measure Builder

Definition

Let $\hat{\rho}_i : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}$ be a computable function. Then we define the *complexity measure builder* ρ by

$$\begin{aligned} \rho : G &\to [X_i^* \to \mathbb{Q}] \\ g &\mapsto \rho_g \end{aligned}$$

where $\rho_g(u) = \hat{\rho}_i(H_2(g(u)), |u|_i)$.

Complexity Measure Builder

Definition

Let $\hat{\rho}_i : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Q}$ be a computable function. Then we define the *complexity measure builder* ρ by

$$\begin{aligned} \rho : G &\rightarrow [X_i^* \rightarrow \mathbb{Q}] \\ g &\mapsto \rho_g \end{aligned}$$

where $\rho_g(u) = \hat{\rho}_i(H_2(g(u)), |u|_i)$.

- $\hat{\rho}_i$: *witness* of the builder

Complexity Measure Builder

Definition

Let $\hat{\rho}_i : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}$ be a computable function. Then we define the *complexity measure builder* ρ by

$$\begin{aligned} \rho : G &\to [X_i^* \to \mathbb{Q}] \\ g &\mapsto \rho_g \end{aligned}$$

where $\rho_g(u) = \hat{\rho}_i(H_2(g(u)), |u|_i)$.

- $\hat{\rho}_i$: *witness* of the builder
- ρ_g: complexity measure

Acceptable Builder

(i) If $\mathcal{F} \vdash x$, then $\rho_{\mathbf{g}}(x) < N_{\mathcal{F}}$.

Acceptable Builder

(i) If $\mathcal{F} \vdash x$, then $\rho_g(x) < N_{\mathcal{F}}$.

- Heuristic principle

Acceptable Builder

(i) If $\mathcal{F} \vdash x$, then $\rho_g(x) < N_{\mathcal{F}}$.

- Heuristic principle

(ii) $\lim_{n\to\infty} i^{-n} \cdot \mathrm{card}\,\{x \in X_i^* : |x|_i = n \text{ and } \rho_g(x) \leq N\} = 0$

Acceptable Builder

(i) If $\mathcal{F} \vdash x$, then $\rho_g(x) < N_{\mathcal{F}}$.

- Heuristic principle

(ii) $\lim_{n\to\infty} i^{-n} \cdot \mathrm{card}\,\{x \in X_i^* : |x|_i = n \text{ and } \rho_g(x) \leq N\} = 0$

- Lower bound on the complexity

Acceptable Builder

(i) If $\mathcal{F} \vdash x$, then $\rho_g(x) < N_{\mathcal{F}}$.

- Heuristic principle

(ii) $\lim_{n\to\infty} i^{-n} \cdot \mathrm{card}\left\{x \in X_i^* : |x|_i = n \text{ and } \rho_g(x) \leq N\right\} = 0$

- Lower bound on the complexity

(iii) $\left|\rho_g(x) - \rho_{g'}(x)\right| \leq c$

Acceptable Builder

(i) If $\mathcal{F} \vdash x$, then $\rho_g(x) < N_{\mathcal{F}}$.

- Heuristic principle

(ii) $\lim_{n\to\infty} i^{-n} \cdot \mathrm{card}\left\{x \in X_i^* : |x|_i = n \text{ and } \rho_g(x) \leq N\right\} = 0$

- Lower bound on the complexity

(iii) $\left|\rho_g(x) - \rho_{g'}(x)\right| \leq c$

- Independence on the Gödel numbering

Acceptable Builder

(i) If $\mathcal{F} \vdash x$, then $\rho_g(x) < N_{\mathcal{F}}$.

- Heuristic principle

(ii) $\lim_{n\to\infty} i^{-n} \cdot \mathrm{card}\left\{x \in X_i^* : |x|_i = n \text{ and } \rho_g(x) \leq N\right\} = 0$

- Lower bound on the complexity

(iii) $\left|\rho_g(x) - \rho_{g'}(x)\right| \leq c$

- Independence on the Gödel numbering

Proposition

The function δ_g is an acceptable complexity measure.

Acceptable Builder

(i) If $\mathcal{F} \vdash x$, then $\rho_g(x) < N_{\mathcal{F}}$.

- Heuristic principle

(ii) $\lim_{n\to\infty} i^{-n} \cdot \mathrm{card}\,\{x \in X_i^* : |x|_i = n \text{ and } \rho_g(x) \leq N\} = 0$

- Lower bound on the complexity

(iii) $\left|\rho_g(x) - \rho_{g'}(x)\right| \leq c$

- Independence on the Gödel numbering

Proposition

The function δ_g is an acceptable complexity measure.

Proposition

The program-size complexity is not an acceptable complexity measure.

Outline

Definitions

Definition

- $$\hat{\rho}_i^1(x,y) = \begin{cases} x/y, & \text{if } y \neq 0, \\ 0, & \text{else.} \end{cases}$$

Definitions

Definition

- $$\hat{\rho}^1_i(x,y) = \begin{cases} x/y, & \text{if } y \neq 0, \\ 0, & \text{else.} \end{cases}$$
- $$\rho^1_g(x) = \begin{cases} \frac{H_2(g(x))}{|x|_i}, & \text{if } x \neq \lambda, \\ 0, & \text{else.} \end{cases}$$

Definitions

Definition

- $$\hat{\rho}_i^1(x, y) = \begin{cases} x/y, & \text{if } y \neq 0, \\ 0, & \text{else.} \end{cases}$$

- $$\rho_g^1(x) = \begin{cases} \frac{H_2(g(x))}{|x|_i}, & \text{if } x \neq \lambda, \\ 0, & \text{else.} \end{cases}$$

- $$\hat{\rho}_i^2(x, y) = \begin{cases} x/\left\lceil \log_i y \right\rceil, & \text{if } y > 1, \\ 0, & \text{else.} \end{cases}$$

Definitions

Definition

- $$\hat{\rho}_i^1(x,y) = \begin{cases} x/y, & \text{if } y \neq 0, \\ 0, & \text{else.} \end{cases}$$

- $$\rho_g^1(x) = \begin{cases} \frac{H_2(g(x))}{|x|_i}, & \text{if } x \neq \lambda, \\ 0, & \text{else.} \end{cases}$$

- $$\hat{\rho}_i^2(x,y) = \begin{cases} x/\left\lceil \log_i y \right\rceil, & \text{if } y > 1, \\ 0, & \text{else.} \end{cases}$$

- $$\rho_g^2(x) = \begin{cases} \frac{H_2(g(x))}{\left\lceil \log_i |x|_i \right\rceil}, & \text{if } |x|_i > 1, \\ 0, & \text{else.} \end{cases}$$

ρ_g^1 is not acceptable

Lemma

ρ_g^1 is bounded.

ρ_g^1 is not acceptable

Lemma

ρ_g^1 is bounded.

Proposition

(i) If $\mathcal{F} \vdash x$, then $\rho_g^1(x) < N_{\mathcal{F}}$.

ρ_g^1 is not acceptable

Lemma

ρ_g^1 is bounded.

Proposition

(i) ✓ The bound is always valid.

ρ_g^1 is not acceptable

Lemma

ρ_g^1 is bounded.

Proposition

(i) ✓ The bound is always valid.

(ii) $\lim_{n\to\infty} i^{-n} \cdot \mathrm{card}\left\{x \in X_i^* : |x|_i = n \text{ and } \rho_g^1(x) \leq N\right\} = 0$

ρ_g^1 is not acceptable

Lemma

ρ_g^1 is bounded.

Proposition

(i) ✓ The bound is always valid.

(ii) ✗ $\{x \in X_i^* : |x|_i = n, \rho_g^1(x) \leq N\} = X_i^n$ for N big enough.

ρ_g^1 is not acceptable

Lemma

ρ_g^1 is bounded.

Proposition

(i) ✓ The bound is always valid.

(ii) ✗ $\left\{x \in X_i^* : |x|_i = n, \rho_g^1(x) \leq N\right\} = X_i^n$ for N big enough.

(iii) $\left|\rho_g^1(x) - \rho_{g'}^1(x)\right| \leq c$

ρ_g^1 is not acceptable

Lemma

ρ_g^1 is bounded.

Proposition

(i) ✓ The bound is always valid.

(ii) ✗ $\{x \in X_i^* : |x|_i = n, \rho_g^1(x) \leq N\} = X_i^n$ for N big enough.

(iii) ✓ As for δ.

ρ_g^2 is not acceptable either

Proposition

(i) If $\mathcal{F} \vdash x$, then $\rho_g^2(x) < N_{\mathcal{F}}$.

ρ_g^2 is not acceptable either

Proposition

(i) ✗ Cardinality argument.

ρ_g^2 is not acceptable either

Proposition

(i) ✗ Cardinality argument.

(ii) $\lim_{n\to\infty} i^{-n} \cdot \mathrm{card}\left\{x \in X_i^* : |x|_i = n \text{ and } \rho_g^2(x) \leq N\right\} = 0$

ρ_g^2 is not acceptable either

Proposition

(i) ✗ Cardinality argument.

(ii) ✓ Long proof...

ρ_g^2 is not acceptable either

Proposition

(i) ✗ Cardinality argument.

(ii) ✓ Long proof...

(iii) $\left|\rho_g^2(x) - \rho_{g'}^2(x)\right| \leq c$

ρ_g^2 is not acceptable either

Proposition

(i) ✗ Cardinality argument.

(ii) ✓ Long proof. . .

(iii) ✓ *Cf* previous slide.

Intuitive Results and Independence

- ρ^1 is "too small" and ρ^2 is "too big".

Intuitive Results and Independence

- ρ^1 is "too small" and ρ^2 is "too big".

(i) Upper bound: the complexity of the theorems has to be bounded.

Intuitive Results and Independence

- ρ^1 is "too small" and ρ^2 is "too big".

(i) Upper bound: the complexity of the theorems has to be bounded.

(ii) Lower bound: avoid trivial measures.

Intuitive Results and Independence

- ρ^1 is "too small" and ρ^2 is "too big".

(i) Upper bound: the complexity of the theorems has to be bounded.
(ii) Lower bound: avoid trivial measures.
(iii) Independence from the chosen language.

Intuitive Results and Independence

- ρ^1 is “too small” and ρ^2 is “too big”.

(i) Upper bound: the complexity of the theorems has to be bounded.

(ii) Lower bound: avoid trivial measures.

(iii) Independence from the chosen language.

Theorem

The three conditions are independent from each other.

Outline

Introduction

Can we find other acceptable measures of complexity?

Introduction

Can we find other acceptable measures of complexity?

Proposition

Suppose that ρ_g is acceptable. Then so is $\alpha \cdot \rho_g + \beta$, $\alpha, \beta \in \mathbb{Q}$, $\alpha > 0$.

Results

Proposition

Let $\hat{\rho}_i : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}$ be a computable function, linear in both variables. If it defines an acceptable complexity measure, then

$$\hat{\rho}_i(x, y) = a \cdot (x - \varepsilon \cdot \lceil \log_2(i) \cdot y \rceil) + b,$$

where $1/2 \leq \varepsilon \leq 1$.

Results

Proposition

Let $\hat{\rho}_i : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}$ be a computable function, linear in both variables. If it defines an acceptable complexity measure, then

$$\hat{\rho}_i(x, y) = \qquad x - \varepsilon \cdot \lceil \log_2(i) \cdot y \rceil \qquad ,$$

where $1/2 \leq \varepsilon \leq 1$.

Results

Proposition

Let $\hat{\rho}_i : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}$ be a computable function, linear in both variables. If it defines an acceptable complexity measure, then

$$\hat{\rho}_i(x, y) = \qquad x - \varepsilon \cdot \lceil \log_2(i) \cdot y \rceil \qquad ,$$

where $1/2 \leq \varepsilon \leq 1$.

Proposition

Let $\rho_g(x) = H_2(g(x))/f(|x|_i)$ where f is computable. Then ρ_g is not acceptable.

Summary of the work

- Studying the results about δ_g

Summary of the work

- Studying the results about δ_g
  - Some corrections

Summary of the work

- Studying the results about δ_g
  - Some corrections
  - Key elements in the proofs

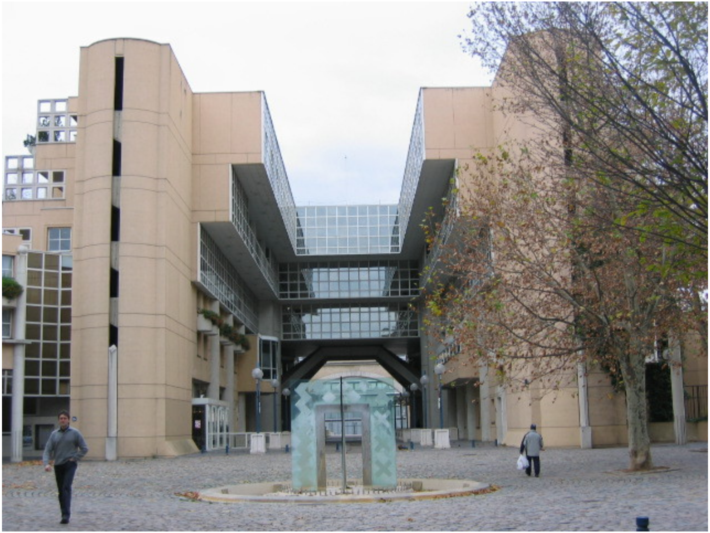
Summary of the work

- Studying the results about δ_g
  - Some corrections
  - Key elements in the proofs
- Proposition of a general definition of *acceptable complexity measure of theorems*

Summary of the work

- Studying the results about δ_g
  - Some corrections
  - Key elements in the proofs
- Proposition of a general definition of *acceptable complexity measure of theorems*
- Studying those acceptable measures to find other ones (in progress)

Thank you for your attention!



École Normale Supérieure de Lyon