Gödel's Speed-up Theorem
and its impacts on Mathematics

Sakaé Fuchino (渕野 昌)

Graduate School of System Informatics
Kobe University
(神戸大学大学院 システム情報学研究科)

http://fuchino.ddo.jp/index-j.html

情報基礎特論 2017

(2017 年 07 月 05 日 (09:38 JST) version)

2017 年 06 月 12 日

This presentation is typeset by pLaTeX with beamer class.
These slides are downloadable as
http://fuchino.ddo.jp/slides/speed-up-theorem-2017-pf.pdf

A rough statement of the theorem

For a concretely given (recursive) theory T with the property that the elementary arithmetic can be developed in T, and any computable (recursive) function $f : \mathbb{N} \to \mathbb{N}$, there is a formula $\varphi = \varphi(x)$ in the language of the theory T s.t. for each $n \in \mathbb{N}$, $\varphi(\underline{n})$ is provable from T but the simplest proof of $\varphi(\underline{n})$ has the degree (of complexity) $\geq f(n)$. In contrast, $T + consis(\ulcorner\ulcorner T\urcorner\urcorner)$ proves $\forall x\varphi(x)$ and thus there is a linear function g s.t. the degree of the proof of $\varphi(\underline{n})$ from $T + consis(\ulcorner\ulcorner T\urcorner\urcorner)$ is $\leq g(n)$.

- $\underline{n}$ denotes the numeral (in the language of T) representing n.
- $consis(\ulcorner\ulcorner T\urcorner\urcorner)$ denotes the formula in the language of T asserting "the theory T is consistent". We put the strange double quotation mark around T since, strictly speaking, the formula does not talk about the theory (which is a meta-mathematical object) but rather the object in the theory which corresponds to the theory T.
- The assertion above varies according to the exact choice of (the range of) theories and the degree (of complexity).

History of the theorem

- Kurt Gödel (1906–1978 (明治 39 年–昭和 53 年)) mentioned the statement of his Speed-up Theorem in an seminar report in 1936 (昭和 11 年).
- The proof of Gödel's Incompleteness Theorems were obtained in 1930. The Speed-up Theorem can be seen as a spin-off of the results around the Incompleteness Theorems — actually we show later that the Second Incompleteness Theorem follows from our version of the Speedup Theorem.
  - Both of the terms "incompleteness theorems" and "speed-up theorem" were not coined by Gödel himself but introduced by other people soon after these results were public.
- Gödel never published his proof of the Speed-up Theorem.
- Samuel Buss' paper in 1995 contains one of the first explicit proof of some versions of the Gödel's theorem.

History of the theorem (2/2)

- The original statement of the theorem was as follows:

> Sei nun S_i das System der Logik i-ter Stufe, wobei die natürlichen Zahlen als Individuen betrachtet werden. ... Zu jeder in S_i berechenbaren Funktion ϕ gibt es unendlich viele Formeln f von der Art, daß, wenn k die Länge eines kürzesten Beweises für f in S_i und ℓ die Länge eines kürzesten Beweises für f in S_{i+1} ist, $k > \phi(\ell)$.
>
> K. Gödel [1936]

> English translation (by S.F.): Now let S_i be the system of the ith order logic where the natural numbers are considered to be the basic objects. ... To each computable function ϕ in S_i, there are infinitely many formulas f s.t., if k is the length of a shortest proof of f in S_i and ℓ the length of a shortest proof of f in S_{i+1}, then we have $k > \phi(\ell)$.

Another version of the Speed-up Theorem

- The version of the Speed-up Theorem with

  degree = the length of the proof (= number of the letters contained in the proof),

  as in the original formulation of the theorem by Gödel, is dependent on the system of the proof.

  - It can be even false in some artificially set deduction system!

- The version of the theorem with

  degree = the sum of the lengths of the formulas appearing in the proof

  is independent of the choice of the deduction system (as far as the language of the theory contains only finitely many non logical sysmbols):

Another version of the Speed-up Theorem (2/3)

- Let $\mathcal{L}_{\{\}}$ be the language consisting of $\emptyset$, $\{.,.\}$, $\cdot \cup \cdot$, $\cdot \in \cdot$. Let $\mathsf{ZF}_{\{\}}$ be the Zermelo-Fraenkel set theory formulated in $\mathcal{L}_{\{\}}$.
- Note that all concretely given hereditarily finite sets can be represented by some closed terms in this language.
- For a theory T and a formula ψ, we denote with $T \vdash \psi$ the assertion "there is a (formal) proof of ψ from the theory T." If P is such a proof we write $T \vdash^{P} \psi$.

Theorem 1 Let T be a concretely given (recursive) theory containing a large enough fragment of the theory $\mathsf{ZF}_{\{\}}$. Suppose that $f : \mathbb{N} \to \mathbb{N}$ is a computable (recursive) function. Then there is an $\mathcal{L}_{\{\}}$-formula $\varphi(x)$ s.t., for each $n \in \mathbb{N}$, we have $T \vdash \varphi(\underline{n})$ but, if $T \vdash^{P} \varphi(\underline{n})$ for a proof P in T, then $T \vdash rank(\ulcorner P \urcorner) \geq f(\underline{n})$.

In contrast we have
$T + consis(\ulcorner\ulcorner T \urcorner\urcorner) \vdash (\forall n \in \omega)\ \varphi(n)$.

Another version of the Speed-up Theorem (3/3)

Theorem 1 Let T be a concretely given (recursive) theory containing a large enough fragment of the theory $\mathsf{ZF}_{\{\}}$. Suppose that $f : \mathbb{N} \to \mathbb{N}$ is a computable (recursive) function. Then there is an $\mathcal{L}_{\{\}}$-formula $\varphi(x)$ s.t., for each $n \in \mathbb{N}$, we have $T \vdash \varphi(\underline{n})$ but, if $T \vdash^{P} \varphi(\underline{n})$ for a proof P in T, then $T \vdash \mathit{rank}(\ulcorner P \urcorner) \geq f(\underline{n})$.

In contrast we have
$T + \mathit{consis}(\ulcorner\ulcorner T \urcorner\urcorner) \vdash (\forall n \in \omega)\ \varphi(n)$.

- The "rank" in Theorem 1 above is in the sense of von Neumann hierarchy:
  - In (a large enough fragment of) $\mathsf{ZF}_{\{\}}$, let $V_0 = \emptyset$ and $V_{n+1} = \mathcal{P}(V_n)$ for $n \in \omega$ (ω is the set of natural numbers defined inside set-theory). $H = \bigcup_{n\in\omega} V_n$ is the "set" of all hereditarily finite sets.
  - For $x \in H$, $\mathit{rank}(x)$ is the first $n \in \omega$ s.t. $x \in V_{n+1}$.

A proof of the Second Incompleteness Theorem

- The Second Incompleteness Theorem can be easily obtained as a Corollary to Theorem 1:

Theorem 2 (The Second Incompleteness Theorem) Let T be a concretely given (recursive) theory containing a large enough fragment of the theory $\mathsf{ZF}_{\{\}}$. If T is consistent then $T \nvdash \mathit{consis}(\ulcorner\ulcorner T\urcorner\urcorner)$.

Proof of Theorem 2 from Theorem 1: Suppose that $f : \mathbb{N} \to \mathbb{N}$ is an exponentially growing computable (i.e. recursive) function and let $\varphi(x)$ be as in Theorem 1. If $T \vdash \mathit{consis}(\ulcorner\ulcorner T\urcorner\urcorner)$, let P^* be s.t. $T \vdash^{P^*} \mathit{consis}(\ulcorner\ulcorner T\urcorner\urcorner)$. We can extend P^* to a P_n with $T \vdash^{P_n} \varphi(\underline{n})$ for each $n \in \mathbb{N}$ s.t. $T \vdash \mathit{rank}(P_n) \leq p(\underline{n})$ for some polynomial function p. This is a contradiction to the choice of φ. $\square$

- Suppose that $f : \mathbb{N} \to \mathbb{N}$ is a fast growing computable function s.t., say, $f(8)$ exceeds the number of atoms in the whole universe.
  - ▷ Let T be as in Theorem 1 and $\varphi = \varphi(x)$ be as in Theorem 1 for these f and T. Then we know (by meta-mathematical arguments on the formula φ) that $T \vdash \varphi(\underline{8})$ but it is impossible to write down the proof (as far as T is consistent).
  - ▷ In $T + consis(\ulcorner T \urcorner)$ we obtain a proof of $\varphi(\underline{8})$ of reasonable length!
- Let T and φ be as above (and assume that T is consistent).
  - ▷ The theory $\tilde{T} = T + \neg\varphi(\underline{8})$ is inconsistent but there is no feasible proof of the inconsistency!
  - ▷ The inconsistency of $\tilde{T} = T + \neg\varphi(\underline{8})$ can be only recognized in $T + consis(\ulcorner T \urcorner)$.

Mathematical and philosophical consequences of the Speed-up Theorem (2/2)

- Two contrasting standpoints

> $\boxed{\text{A}}$ We should restrict our mathematics to the weakest possible framework so that any possible inconsistency of the system (which cannot be totally exluded by the Second Incompleteness Theorem) can be avoided as much as possible.

> $\boxed{\text{B}}$ We should do mathematics in any strong frameworks as far as the mathematics developed there is coherent and interesting.

- The Gödel Speedup Theorem (e.g. Theorem 1 above) tells us that even if the final objective of our mathematical research is along the line of the standpoint $\boxed{\text{A}}$, there are theorems in a given weak theory which can be understood only if we work from the point of view of $\boxed{\text{B}}$.

Instances of infinitely many times speed-up

- In Zermelo Fraenkel set theory (ZF) the von Neumann hierachy can be extnded for all transfinite ordinals by defining $V_0 = \emptyset$ $V_{\alpha+1} = \mathcal{P}(V_\alpha)$ and $V_\gamma = \bigcup_{\alpha<\gamma} V_\alpha$ for a limit ordinal γ.
- In ZFC (ZF with the Axiom of Choice), V_γ is a model of the Zermelo set theory with the Axiom of Choice (ZC = ZFC − Axiom of Replacement) for all limit ordinals $\gamma > \omega$. It follows that $\mathsf{ZFC} \vdash \mathit{consis}(\ulcorner \mathsf{ZC} \urcorner)$.
  - Most of the results in modern mathematics can be fromulated in ZC as far as the set theory is not deeply involved.
  - This means that the set theory (ZFC) has a possible speedup over the conventional mathematics (whose proofs can be reformulated as proofs from ZC).

Instances of infinitely many times speed-up (2/3)

- A cardinal κ is said to be inaccessible if it is regular and closed with respect to the cardinal exponentiation (i.e $\alpha < \kappa$ always implies $2^\alpha < \kappa$)
  - For an inaccessible κ we have $V_\kappa \models \mathsf{ZFC}$. Thus:
  - ZFC + "there is an inaccessible cardinal" $\vdash$ *consis*($\ulcorner\ulcorner$ZFC$\urcorner\urcorner$).
- ZFC + "there is an inaccessible cardinal" is thought to be the framework of the mathematics which employs the notion of Grothendieck universe.
  - This means that the mathematical arguments using Grothendieck universe can have a possible speedup over the ZFC set theory.

Instances of infinitely many times speed-up (3/3)

- For $T_0 = \mathrm{ZC}$ and $T^* = \mathrm{ZFC}$ or for $T_0 = \mathrm{ZFC}$ and $T^* = \mathrm{ZFC} +$ there is an inaccessible cardinal we even have the following (for a inaccessible cardinal we can see this by applying the Löwenheim-Skolem Theorem):
- There are (recursive) theories T_i, $i < \omega_1^{CK}$ s.t. T_0, $\langle Th(T_i) \, : \, i < \omega_1^{CK} \rangle$ is continuously increasing $T_{i+1} \vdash consis(\ulcorner\ulcorner T_i \urcorner\urcorner)$ for all $i < \omega_1^{CK}$ and $Th(\bigcup_{i<\omega_1^{CK}} T_i) \subseteq T^*$
- ▷ Here ω_1^{CK} denotes the upper bound of all definable countable ordinals.
- Similar assertion holds between two extensions of set theory T, T' where the stronger theory T' include a large cardinal axiom which transcends the weaker set theory T.
- There are transfinite repetition of possible speedup between such T_0 and T^*.

An incomplete list of literature

- Samuel R. Buss, On Gödel's theorems on lengths of proofs I: Number of lines and speedups for arithmetic, Journal of Symbolic Logic 39 (1994), 737–756.
- 渕野 昌，集合論 (= 数学) の未解決問題，現代思想 2016 年 10 月臨時増刊号 総特集=未解決問題集 (2016 年 9 月 7 日発売)
- 渕野 昌，美は一本の毛で男をひつぱるだろう，現代思想 2017 年 3 月臨時増刊号，Vol.45-5, 総特集＝知のトップランナー 50 人の美しいセオリー，102–108, (2017).
- 渕野 昌, 数学と集合論 — ゲーデルの加速定理の視点からの考察，submitted.
- George A. Miller, The magical number seven, plus or minus two: some limits on our capacity for processing information, Psychological Review, vol.63 (1956), 81–97.

Report

- For a theory T as in Theorem 1 show that there is always a formula $\varphi(x)$ s.t. $T \vdash \varphi(\underline{n})$ for all $n \in \mathbb{N}$ but $T \nvdash (\forall x \in \omega)\varphi(x)$.
  - Deadline: June 30, 2017 (either by email to `fuchino@diamond.kobe-u.ac.jp` or directly to me at my office on the 4th floor of 3 号館 there will be also an envelope for the submission hang on the door of my office)