Speed-up theorems and their impact on mathematics

Sakaé Fuchino (渕野 昌)

fuchino@diamond.kobe-u.ac.jp

2019 年 10 月 10 日 (09:38 JST) 版

This slide is downloadable as:

http://fuchino.ddo.jp/slides/tokuron2019-07-pf.pdf

Set theory is the theory of everything (in mathematics)

- The axiom system of standard set theory (Zermelo Fraenkel set theory with Axiom of Choice, abbr: ZFC) provides a framework in which all known mathematical theories (and their proofs) can be formulated.
- Set theory also provides powerful meta-mathematical tools to analyze the interrelation between mathematical theorems and theories (mostly in terms of consistency strength but also in other ways).
- ▷ If some mathematical statement φ is shown to be unprovable in ZFC, (e.g. by using the method of forcing) then it should be regarded that φ is not provable in the (conventional) mathematics.
- ▷ If it is shown that a mathematical theorem φ unprovable in a fragment $\mathcal{F}$ of ZFC (e.g. $\mathcal{F} =$ Zermelo's set theory Z without the Axiom of Choice), this may be interpreted either that φ is a result outside the classical mathematics, or that this is an example showing the mathematical necessity of those axioms of set theory used in the proof.

Naïve axiomatic set theory

- The axioms of ZFC are built on the single predicate "$\in$" where "$x \in y$" means x belongs to y as an element.
  - We do not introduce a predicate for expressing "x is a set" since everything is a set in set theory. If we say "for all x ..." in an axiom of set theory, what is meant is "for all set x, ...".
- In the following, The axiom system ZFC of set theory is formulated with certain redundancy. This formulation is chosen on purpose so that some important subtheories of ZFC are subsets of the system.

Naïve axiomatic set theory (2/4)

- The axioms of Zermelo's set theory Z are the following statements:

Extensionality: If we have $u \in x$ if and only if $u \in y$ for any u, then $x = y$.

Empty Set: There is x s.t. $u \notin x$ for any u (such set x is denoted by $\emptyset$).

Pair: For x and y there is z s.t., for any u, $u \in z$ if and only if $u = x$ or $u = y$ (notation: $z = \{x, y\}$).

Union: For any x, there is y s.t., for any u, $u \in y$ if and only if $u \in z$ for some $z \in x$ (notation: $y = \bigcup x$).

Separation: If $\Phi(\cdot)$ is a property expressed by using only "$\in$" and "$=$" then for any x there is y s.t. $u \in y$ if and only if $u \in x$ and $\Phi(u)$ holds. (notation: $y = \{u \in x \ : \ \Phi(u)\}$).

Power Set: For any x, there is y s.t., for any u, $u \in y$ if and only if all elements of u are elements of x (notation: $y = \mathcal{P}(x)$).

Naïve axiomatic set theory (3/4)

Infinity: There is x s.t. $\emptyset \in x$ and, for any $y \in x$, $\bigcup\{y, \{y, y\}\}$ $(= y \cup \{y\}) \in x$.

▷ Zermelo's axiom system of set theory consists of all the axioms introduced sofar.

▶ Most of classical mathematics can be developed in the axiom system Z (see the argument in the next slide but one). The next Axiom of Choice (abbr.: AC) is often used in modern mathematics (there are even a couple of theorems in Calculus and Linear Algebra in which we need this axiom):

AC: For any x s.t. $\emptyset \notin x$ and s.t. any distinct y, $y' \in x$ have empty intersection (i.e. there is no u with $u \in y$ and $u \in y'$), there is z s.t. for each $y \in x$ there is the unique $u \in z$ s.t. $u \in y$.

▶ The axiom system which is obtained by adding AC to Z is denoted by ZC.

Naïve axiomatic set theory (3/4)

- Finally, the axiom system ZFC is the system obtained by adding the following axioms to the axioms of ZC:

  Replacement: For any x, if $\Phi(\cdot,\cdot)$ is a property expressed by using only "$\in$" and "$=$" s.t., for any $u \in x$ there is the unique v s.t. $\Phi(u,v)$ holds, then there is y s.t. $v \in y$ if and only if $\Phi(u,v)$ for some $u \in x$ (notation: $y = \{v : \Phi(u,v) \text{ for some } u \in x\}$).

  Foundation: For any non empty x, there is $y \in x$ s.t. there is no $y' \in x$ with $y' \in y$.

The whole mathematics can be developed in ZFC

- Most of the classical mathematics can be developed in Z!
- All the usual set operations and relations can be defined in Z.
- For example, we can define $x \cup y = \bigcup\{x, y\}$,
  $x \cap y = \{u \in x : u \in y\}$, $x \setminus y = \{u \in x : u \notin y\}$,
  $\langle x, y\rangle = \{\{x, x\}, \{x, y\}\}$,
  $x \times y = \{\langle u, v\rangle \in \mathcal{P}(\mathcal{P}(x \cup y)) : u \in x,\ v \in y\}$

  $x \subseteq y \;\Leftrightarrow\; z \in y$ holds for all $z \in x$,

  f is a function from x to y $\;\Leftrightarrow\;$ $f \subseteq x \times y$ and for any $u \in x$ there is a unique $v \in y$ s.t. $\langle u, v\rangle \in f$

  $f(u) = v \;\Leftrightarrow\; \langle u, v\rangle \in f$, etc.
- For a set x as in the Axiom of Infinity, let

$$\begin{aligned}\omega = \{y \in x : y \in z \text{ for all } z \text{ s.t. } \emptyset \in z \text{ and}\\ u \cup \{u\} \in z \text{ for all } u \in z\}\\ = \bigcap\{z : \emptyset \in z \text{ and } \bigcap\{y, \{y, y\}\} \in z \text{ for all } y \in z\}.\end{aligned}$$

The whole mathematics can be developed in ZFC (2/2)

- Most of the classical mathematics can be developed in Z!
- ω can be seen as the set of all $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, etc. Thus ω can be considered as the set of natural numbers. We distinguish between meta-mathematical natural numbers and natural numbers in set theory and the collection of the former is denoted by $\mathbb{N}$.
- We can introduce basic operations like addition and multiplication on ω which satisfy all the properties these functions should satisfy.
- Starting from ω with the basic operations, we can define the set of rational numbers $\mathbb{Q}$ and the set of real numbers $\mathbb{R}$. The Axiom of Power Set is used to define $\mathbb{R}$ over $\mathbb{Q}$ as a set.
- Using the notion of function as a set, introduced earlier, We can reformulate AC as:

  AC: (Reformulated) For any x s.t. $\emptyset \notin x$, there is $f : x \to \bigcup x$ s.t., for each $y \in x$, $f(y) \in y$.

Meta-mathematics

- The axiom systems of Z, ZFC etc. formulated as above are still highly inaccurate in many ways. They can be made precise by reformulating them on basis of the predicate logic.
- In the following, we work in "meta-mathematics". In particular any set-theoretic notation in the following is just for convenience. No set theory is assumed.

Predicate logic

- A language $\mathcal{L}$ is a collection of constant, function and relation symbols $\{c_i, f_j, r_k\}_{i\in I, j\in J, k\in K}$. We keep an (potentially infinite) list of symbols for variables x_0, x_1,... in stock.

- $\mathcal{L}$-terms are defined recursively by:

  (1) a variable is an $\mathcal{L}$-term; (2) a constant symbol of $\mathcal{L}$ is an $\mathcal{L}$-term; (3) if t_0,..., t_{n-1} are $\mathcal{L}$-terms, and f is an n-ary function symbol of $\mathcal{L}$, then $f(t_0, \dots, t_{n-1})$ is an $\mathcal{L}$-term; (4) nothing else.

- If all the variables, which appear in a term t, are in the list $x_0, \dots, x_{k-1}$, we write $t = t(x_0, \dots, x_{k-1})$.

Predicate logic (2/2)

- $\mathcal{L}$-formulas are defined recursively by:

  (1) if t_0 and t_1 are $\mathcal{L}$-terms then $t_0 \equiv t_1$ is an $\mathcal{L}$-formula; (2) if $t_0, \ldots, t_{n-1}$ are $\mathcal{L}$-terms and r is an n-ary relation symbol in $\mathcal{L}$, then $r(t_0, \ldots, t_{n-1})$ is an $\mathcal{L}$-formula; (3) if φ and ψ are $\mathcal{L}$-formulas, then $\neg\varphi$ and $(\varphi \to \psi)$ are $\mathcal{L}$-formulas; (4) if φ is an $\mathcal{L}$-formula and x a variable, then $\exists x\, \varphi$ is an $\mathcal{L}$-formula; (5) nothing else.

- a variable x in an $\mathcal{L}$-formula φ is said to be free in φ if there is no subformula of the form $\exists x\, \psi$ containing the appearance of the variable x in ψ. We write $\varphi = \varphi(x_0, \ldots, x_{k-1})$, if all free variables of φ are among $x_0, \ldots, x_{k-1}$.

- An $\mathcal{L}$-formula without any free variable is called an $\mathcal{L}$-sentence.

Predicate logic (3/3)

- The intended reading of $\neg\varphi$, $(\varphi \to \psi)$, $\exists x\, \varphi$ is "φ does not hold", "φ implies ψ", and "there exists x s.t. φ", respectively.

- We can also express $(\varphi \vee \psi)$ ["φ or ψ"], $(\varphi \wedge \psi)$ ["φ and ψ"], $(\varphi \leftrightarrow \psi)$ ["φ if and only if ψ"], $\forall x\, \varphi$ ["for all x we have φ"] by $(\neg\varphi \to \psi)$, $\neg(\neg\varphi \vee \neg\psi)$, $((\varphi \to \psi) \wedge (\psi \to \varphi))$, and $\neg\exists x \neg\varphi$ respectively.

- With the intended reading of the logical symbols in mind, we can reformulate the formal axioms of ZFC. Let $\mathcal{L}_\varepsilon$ be the language consisting of the single binary relation symbol ε (whose intended interpretation is the set-theoretic element relation).

Empty Set: $\exists x\, \forall y\, (\neg y \;\varepsilon\; x)$

$\vdots$

Separation: for each $\mathcal{L}_\varepsilon$-formula $\varphi = \varphi(y, x_0, \dots, x_{k-1})$,
$\forall x_0 \cdots \forall x_{k-1} \forall u \exists v\, \forall y\, (y \;\varepsilon\; v \leftrightarrow (y \;\varepsilon\; u \wedge \varphi))$

$\vdots$

A formal deduction system of the predicate logic

- We can introduce a formal deduction system for the predicate logic which encompasses all logical deduction in mathematics —— The completeness of the system is "guaranteed" by Gödel's completeness theorem.

- For a language $\mathcal{L}$ and an $\mathcal{L}$-theory (concretely given collection of $\mathcal{L}$-sentences) T, a proof $\mathcal{P}$ of an $\mathcal{L}$-formula φ from T is a sequence $\varphi_0, \ldots, \varphi_n$ of $\mathcal{L}$-formulas s.t. $\varphi_n = \varphi$, and each φ_i in the sequence is either an element of T, or one of the following logical axioms, or φ_i is deduced from earlier formulas in the sequence by one of the deduction schemes below.

- If there is a proof $\mathcal{P}$ of φ from T, we write $T \vdash^{\mathcal{P}} \varphi$. If there is a proof of φ from T, we write $T \vdash \varphi$.

Axioms and deduction rules of the formal system

Axioms of equality: $\forall x\, x \equiv x$, $\forall x \forall y\, (x \equiv y \to y \equiv x)$,...

Logical axioms: All tautology of propositional logic (for example, all $\mathcal{L}$-formulas of the form $(\varphi \to (\psi \to \varphi))$)

▷ Note that there is an algorithm to decide if a given formula is a tautology.

Existential axioms: All $\mathcal{L}$-formulas of the form $(\varphi(t/x) \to \exists x\, \varphi)$ for an $\mathcal{L}$-formula φ and $\mathcal{L}$-term t where the substitution $\varphi(t/x)$ is appropriate (i.e., without any conflict of the variables in φ and t)

Deduction schemes:

$$\frac{\varphi,\ (\varphi \to \psi)}{\psi}$$ (Modus Ponens)

$$\frac{(\varphi \to \psi)}{(\exists x \varphi \to \psi)}$$ where x is not free in ψ (Rule of Existential Quantification)

Significance of the strict axiomatization

- By the strict axiomatization of set theory over the predicate logic, we can say definitively if a proof is correct or not. Theoretically, this can be even checked mechanically (-> proof checking, automated theorem proving ATP)

- ZFC over predicate logic gives the superset of the range of conventional mathematics.

- Foundational questions about consistency and relative consistency can be asked first after the strict axiomatization has been done.

- After the strict axiomatization has been done, meta-mathematical methods can be applied to obtain mathematical results (even inside ZF).

Meta-mathematics translated into the set theory

- Let $\mathcal{L}_{\{\}}$ be the language $\mathcal{L}_{\varepsilon}$ extended by adding the constant and function symbols $\emptyset$, $\{\cdot,\cdot\}$, $\cdot \cup \cdot$. Let $\mathsf{Z}_{\{\}}$, $\mathsf{ZFC}_{\{\}}$, etc. be the expansion of the axiom systems Z, ZFC, etc. in $\mathcal{L}_{\{\}}$ obtained by adding the axioms saying the expected definitions of the new symbols (e.g., $\forall x\,(\neg x \mathrel{\varepsilon} \emptyset)$ is one of such definitions).

- Let Z_0 be the minimal subtheory of $\mathsf{Z}_{\{\}}$ containing all the axioms needed in the following arguments.

- In Z_0, finite sequences can be defined as mapping t from some $n \in \omega$ (with $n = \{0, ..., n-1\}$) where n is the length of the sequence and the ith component of t is $t(i)$. The set ${}^{\omega>}X$ of all finite sequences of elements of X can be also considered in Z_0. In the following T, T' etc. are concretely given $\mathcal{L}_{\{\}}$-theories extending Z_0.

Meta-mathematics translated into the set theory (2/3)

- For a concretely given language $\mathcal{L}$ all the symbols which appear in $\mathcal{L}$-formulas can be coded by elements of $\omega \times \omega$. For example, variables x_0, x_1,... are coded by $\langle 0, 0\rangle$, $\langle 1, 0\rangle$,..., symbols '$\rightarrow$', '$\neg$', '$\exists$',... by $\langle 0, 1\rangle$, $\langle 1, 1\rangle$, $\langle 2, 1\rangle$,... etc.

- Further in Z_0, we can define sets $\mathit{Term}_{\mathcal{L}_{\{\}}}$, $\mathit{Fml}_{\mathcal{L}_{\{\}}}$, $\ulcorner\ulcorner \mathsf{ZFC}_{\{\}} \urcorner\urcorner$, $\ulcorner\ulcorner T \urcorner\urcorner \subseteq {}^{\omega>}\omega \times \omega$ which correspond to the collections of $\mathcal{L}_{\{\}}$-terms, $\mathcal{L}_{\{\}}$-formulas, axioms of ZFC and axioms of T respectively, by corresponding recursive definition which can be done in Z_0.

- The predicate "$\mathcal{P}$ is a proof of φ from $\ulcorner\ulcorner T \urcorner\urcorner$" can be also introduced in Z_0 as an appropriate $\mathcal{L}_{\{\}}$-formula which we abbreviate as $\mathit{proof}(\mathcal{P}, \ulcorner\ulcorner T \urcorner\urcorner, \varphi)$. The $\mathcal{L}_{\{\}}$-formula $\exists\mathcal{P}\, \mathit{proof}(\mathcal{P}, \ulcorner\ulcorner T \urcorner\urcorner, \varphi)$ then expresses that "φ is provable from $\ulcorner\ulcorner T \urcorner\urcorner$". This formula is abbreviated as $\mathit{prov}(\ulcorner\ulcorner T \urcorner\urcorner, \varphi)$.

Meta-mathematics translated into the set theory (3/3)

- We define $Th(\ulcorner\ulcorner T\urcorner\urcorner) = \{\varphi \in Fml_{\mathcal{L}_{\{\}}} : prov(\ulcorner\ulcorner T\urcorner\urcorner, \varphi)\}$. $Th(T)$ denotes the meta-theoretical original of $Th(\ulcorner\ulcorner T\urcorner\urcorner)$.

- The predicate *consis*$(\ulcorner\ulcorner T\urcorner\urcorner)$ is defined by $Th(\ulcorner\ulcorner T\urcorner\urcorner) \not\equiv Fml_{\mathcal{L}_{\{\}}}$. Intuitively the predicate claims that "T is consistent".

- The following surprising result is a variation of Gödel's Second Incompleteness Theorem. Remember that T is a concretely given $\mathcal{L}_{\{\}}$-theory with $T \supseteq Z_0$.

Theorem 1.

(a) If T is consistent then *consis*$(\ulcorner\ulcorner T\urcorner\urcorner)$ is not provable in T.

(b) any concretely given extension T' of T is not decidable, that is, $Th(T')$ is not recursive (computable), as far as T' is consistent.

Speed-up theorems

- For a proof $\mathcal{P}$, let the length $L(\mathcal{P})$ of the proof $\mathcal{P}$ be defined as the sum of of the length of formulas in $\mathcal{P}$. For an $\mathcal{L}_{\{\}}$-formula φ, let $W_T(\varphi)$ be the smallest possible length of a proof of φ from T, if φ is provable; undefined otherwise.

Theorem 2. (Ehrenfeucht and Mycielski, 1971) Suppose that φ_0 is an $\mathcal{L}_{\{\}}$-formula independent from T (i.e., neither φ_0 nor $\neg\varphi_0$ is provable from T). Then there is no recursive function $S : \mathbb{N} \to \mathbb{N}$ s.t.

$$W_T(\tau) \leq S(W_{T+\varphi_0}(\tau)) \text{ holds for all } \tau \in Th(T).$$

Theorem 3. (Gödel, 1936) Suppose that T' is a consistent extension of T s.t. $T' \vdash consis(\ulcorner\ulcorner T \urcorner\urcorner)$. Then, for any recursive function $S : \mathbb{N} \to \mathbb{N}$, there is an $\mathcal{L}_{\{\}}$-formula $\varphi = \varphi(x)$ s.t. (1) $T' \vdash \varphi(\underline{n})$ for all $n \in \mathbb{N}$, (2) $W_T(\varphi(\underline{n})) \geq S(n)$ for all $n \in \mathbb{N}$, but (3) $T' \vdash (\forall n \,\varepsilon\, \omega)\varphi(n)$.

Significance of the Speed-up Theorems

- Speed-up theorems are nods to the intuition that we obtain shorter proofs in a stronger axiomatic framework.

- ZFC is very much stronger than what we need to develop the conventional mathematics.

  - ▷ There is a research field called “Reverse Mathematics” in which very weak systems of set theory are studied in connection with the question which part of mathematics can be already done in which weak fragment of the set theory. Some of these researchers want to see in (full) set theory an unbalancedly strong theory irrelevant to the every day mathematics.

  - ▷ Speed-up theorems shows that, even if the final objective of these people is to formulate the “reasonable” mathematics in a possible weak framework, the study of set theory and its extensions are indispensable for (research in) mathematics.

Thank you for your attention.