Characterising Complexity Classes by Inductive Definitions in Bounded Arithmetic

Naohi Eguchi

Institute of Computer Science
University of Innsbruck
Austria

CiE 2013, July 2, 2013, Milano

Introduction (1/2)

- Many of computable functions can be already computed with some realistic computation resources (in realistic time, with realistic space).
- Attempts to find limits of realistic computations have given rise to open problems about complexity classes, e.g. $\mathrm{P} \neq ?\mathrm{NP}$.
- In many cases it is difficult to compare complexity classes.

Introduction (2/2)

- P: the class of polynomial-time computable functions.
- PSPACE: the class of polynomial-space computable functions.

Fact

1. $\mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PH} \subseteq \mathrm{PSPACE}$.
2. $\mathrm{P} \subseteq \#\mathrm{P} \subseteq \mathrm{PCH} \subseteq \mathrm{PSPACE}$.

(PH: Polynomial hierarchy, $\#\mathrm{P}$: Polynomial counting, PCH: Counting hierarchy)

No strict inclusion is known.

Outline

- There can be many characterisations of one complexity class. (Recursion-theoretic, Model-theoretic, Proof-theoretic, ...)
- What is the most essential principle to uniformly define functions in a given complexity class?
  Given a complexity class $\mathcal{F}$, find an axiom Ax s.t.

  $$f \in \mathcal{F} \iff \mathrm{T} + \mathsf{Ax} \vdash \forall x \exists ! y f(x) = y.$$

  (T: a base axiomatic system)
- This work: $\begin{cases} \mathcal{F} = \mathrm{P} \text{ or } \mathcal{F} = \mathrm{PSPACE}, \\ \text{Ax is Axiom of Inductive Definitions.} \end{cases}$

Finitary inductive definitions

Let $F : \mathcal{P}(S) \to \mathcal{P}(S)$ $(\#S < \omega)$.

- Define F^m by $\begin{cases} F^0 & := \emptyset \\ F^{m+1} & := F(F^m) \end{cases}$
- If F is inflationary, i.e., $X \subseteq F(X)$ for any $X \subseteq S$, then $\exists k \leq \#S$ such that $F^{k+1} = F^k$.
- $\exists k$ s.t. $F^{k+1} = F^k$ does not hold in general.
- However $\exists k < 2^{\#S}$, $\exists l \neq 0$ such that

$$\forall n \geq k, \ F^{n+l} = F^n.$$

  - Otherwise there exist $2^{\#S} + 1$ subsets of S.
  - This contradicts $\#\{M \mid M \subseteq S\} = 2^{\#S}$.

Connection to time-complexity

Suppose:

1. A function $f(x)$ is computable in $T(x)$ steps.
2. TAPE^k denotes the tape description at the kth step in computing $f(x)$;

$$\text{TAPE}^0 = \boxed{B \mid i_1 \mid \cdots \mid i_{|x|} \mid B \mid \cdots \mid B}$$

$(x = i_1 \cdots i_{|x|}$ (input), $i_1, \dots, i_{|x|} \in \{0, 1\})$

- Then $\text{TAPE}^{T(x)+1} = \text{TAPE}^{T(x)}$.

$$\text{TAPE}^{T(x)} = \boxed{B \mid i_1 \mid \cdots \mid i_{|f(x)|} \mid B \mid \cdots \mid B}$$

$(f(x) = i_1 \cdots i_{|f(x)|}$ (output), $i_1, \dots, i_{|f(x)|} \in \{0, 1\})$

- Further $\forall k \geq T(x)$, $\text{TAPE}^k = \text{TAPE}^{T(x)}$.

Finite model theory

Model-theoretic characterisations of P, PSPACE.

Theorem (Immerman et al.)

1. *A predicate $L \in \mathrm{P} \Leftrightarrow L$ can be expressed by the first order predicate logic (FO) with the fixed point predicate of a FO definable inflationary operator, i.e. $X \subseteq F(X)$.*
2. *A predicate $L \in \mathrm{PSPACE} \Leftrightarrow L$ can be expressed by FO with the fixed point predicate of a FO definable non-inflationary operator.*

Bounded arithmetic (1/2)

- Introducing an axiom (ID) of inductive definitions such that

$$f \in \mathcal{F} \iff \mathrm{T} + (\mathrm{ID}) \vdash \forall x \exists ! y f(x) = y.$$

  where $\mathcal{F} = \mathrm{P}$ or $\mathcal{F} = \mathrm{PSPACE}$.
- The base system T must be weak: $\mathrm{T} \nvdash (\mathrm{ID})$.
- Bounded arithmetic seems suitable for T.
- A system of bounded arithmetic is:
  - a weak subsystem of Peano arithmetic PA;
  - suitable for finitary mathematics.

Bounded arithmetic (2/2)

Second order bounded arithmetic:

- Language $\mathcal{L}^2_{\mathrm{BA}}$: 0, 1, $+$, $\cdot$ and $|X|$.
- First order elements $x, y, z, \ldots$: natural numbers with upper bounds of $\mathcal{L}^2_{\mathrm{BA}}$-terms, i.e. polynomials.
- Second order elements $X, Y, Z, \ldots$: finite sets of naturals. Interpretable into $\{0, 1\}$-strings, i.e. exponentials.
- $|X|$ denotes the number of elements of X, or equivalently the binary length of X.
- Axioms: Induction, Comprehension, ..., Inductive definitions.

Axiom of Inductive Definitions

Definition (Axiom of Inductive Definitions)

$\forall x, \exists X, Y$ s.t. $|X|, |Y| \leq x$, $Y \neq \emptyset$ ($\emptyset$: empty string) and

1. $\forall j < x(P_{\varphi}^{\emptyset}(j) \leftrightarrow i \in \emptyset)$
2. $\forall Z, \forall j < x(P_{\varphi}^{S(Z)}(j) \leftrightarrow \varphi(j, P_{\varphi}^{Z}))$
3. $\forall j < x(P_{\varphi}^{X+Y}(j) \leftrightarrow P_{\varphi}^{X}(j))$

($P_{\varphi}^{X}(j)$: fresh predicate, S: string successor $X \mapsto X + 1$)
Recall:

1. $F^0 = \emptyset$
2. $F^{m+1} = F(F^m)$
3. $\exists k < 2^{\#S}$, $\exists l \neq 0$ s.t. $F^{k+l} = F^k$

Main results

Definition

1. (FO-ID): Axiom of inductive definitions for some FO φ.
2. (FO-IID): (FO-ID) if additionally φ is inflationary, i.e., if $\forall X, \forall i < |X|(i \in X \to \varphi(i, X))$ holds.

Let V^0 be a base system of bounded arithmetic.
$\exists^2$FO formula: $\exists X(|X| \leq t \wedge \psi)$ and ψ FO formula, known as Σ^{B}_1.

Theorem

1. *$f \in \mathrm{P}$ if and only if $\mathrm{V}^0 + (\text{FO-IID}) \vdash \forall X \exists! Y f(X) = Y$ and "$f(X) = Y$" can be expressed by a $\exists^2$FO formula with P^X_φ.*
2. *$f \in \mathrm{PSPACE}$ if and only if $\mathrm{V}^0 + (\text{FO-ID}) \vdash \forall X \exists! Y f(X) = Y$ & "$f(X) = Y$" can be expressed by a $\exists^2$FO formula with P^X_φ.*

Connection to time-complexity

Suppose:

1. A function $f(x)$ is computable in $T(x)$ steps.
2. TAPE^k denotes the tape description at the kth step in computing $f(x)$;

$$\mathrm{TAPE}^0 = \boxed{B \mid i_1 \mid \cdots \mid i_{|x|} \mid B \mid \cdots \mid B}$$

$(x = i_1 \cdots i_{|x|}$ (input), $i_1, \ldots, i_{|x|} \in \{0, 1\})$

- Then $\mathrm{TAPE}^{T(x)+1} = \mathrm{TAPE}^{T(x)}$.

$$\mathrm{TAPE}^{T(x)} = \boxed{B \mid i_1 \mid \cdots \mid i_{|f(x)|} \mid B \mid \cdots \mid B}$$

$(f(x) = i_1 \cdots i_{|f(x)|}$ (output), $i_1, \ldots, i_{|f(x)|} \in \{0, 1\})$

- Further $\forall k \geq T(x)$, $\mathrm{TAPE}^k = \mathrm{TAPE}^{T(x)}$.

Proof of “only if” of Theorem 2

Theorem 2

$f \in \mathrm{PSPACE}$ if and only if $\mathrm{V}^0 + (\text{FO-ID}) \vdash \forall X \exists ! Y f(X) = Y$ and "$f(X) = Y$" can be expressed by a $\exists^2$FO formula with some P_φ^X.

Proof of “only if” of Theorem 2.

Suppose: $f \in \mathrm{PSPACE}$.

$\exists p$: polynomial s.t. $\begin{cases} f(X) \text{ is computable in } 2^{p(|X|)} \text{steps} \\ |\mathsf{TAPE}^L| \leq p(|X|) \end{cases}$

See: $\mathsf{TAPE}^L \mapsto \mathsf{TAPE}^{L+1}$: expressed by a FO formula.

By (FO-ID) $\exists K, \exists L$ s.t. $\mathsf{TAPE}^{K+L} = \mathsf{TAPE}^K$

See: TAPE^K denotes the final tape description.

$$f(X) = Y \Leftrightarrow \exists K, L \text{ s.t.} \begin{cases} |K|, |L| \leq p(|X|), \mathsf{TAPE}^{K+L} = \mathsf{TAPE}^K \\ \& Y = \mathsf{output}(\mathsf{TAPE}^K). \end{cases}$$

Hence $\mathrm{V}^0 + (\text{FO-ID}) \vdash \forall X \exists ! Y f(X) = Y$. □

“If” of Theorem 1 & 2 (1/2)

Proofs of “if” direction of Theorem 1 & 2 are based on:

Theorem (Zambella ’96)

$f \in \mathrm{P}$ if and only if $\mathrm{V}^0 + (\exists^2$FO-IND$) \vdash \forall X \exists! Y f(X) = Y$ and “$f(X) = Y$” can be expressed by a $\exists^2$FO formula.

Theorem (Skelley ’06)

$f \in \mathrm{PSPACE}$ if and only if $\mathrm{V}^0 + (\exists^3$SO-IND$) \vdash \forall X \exists! Y f(X) = Y$ and “$f(X) = Y$” can be expressed by a $\exists^3$SO formula.
($\exists^3$SO: third order $\exists \mathcal{X} \psi$ for some second order ψ known as $\Sigma_1^{\mathcal{B}}$)

Proof of “if” of Theorem 1 & 2.

Theorem 1: Show $\mathrm{V}^0 \vdash (\exists^2\text{FO-IND}) \to (\text{FO-IID})$.
Theorem 2: Show $\mathrm{V}^0 \vdash (\exists^3\text{SO-IND}) \to (\text{FO-ID})$. □

"If" of Theorem 1 & 2 (2/2)

Proof of "if" of Theorem 1 & 2.

Theorem 1: Show $\mathrm{V}^0 \vdash (\exists^2\text{FO-IND}) \to (\text{FO-IID})$.
Theorem 2: Show $\mathrm{V}^0 \vdash (\exists^3\text{SO-IND}) \to (\text{FO-ID})$. □

This is not enough.

Lemma (Eliminating fixed point predicates)

1. *If* $\mathrm{V}^0 + (\textit{FO-IID}) \vdash \psi$: $\exists^2$*FO with* P_φ, *then* $\exists\ \psi'$: $\exists^2$*FO without* P_φ *such that* $\mathrm{V}^0 + (\exists^2\textit{FO-IND}) \vdash \psi'$ *and* $\psi \Leftrightarrow \psi'$ *under a standard interpretation.*
2. *If* $\mathrm{V}^0 + (\textit{FO-ID}) \vdash \psi$: $\exists^2$*FO with* P_φ, *then* $\exists\ \psi'$: $\exists^3$*SO without* P_φ *such that* $\mathrm{V}^0 + (\exists^3\textit{SO-IND}) \vdash \psi'$ *and* $\psi \Leftrightarrow \psi'$ *under a standard interpretation.*

Remarks

Theorem (Zambella '96)

$f \in \mathrm{P}$ if and only if $\mathrm{V}^0 + (\exists^2\mathit{FO\text{-}IND}) \vdash \forall X \exists! Y f(X) = Y$ and "$f(X) = Y$" can be expressed by a $\exists^2 FO$ formula.

Proof is based on a recursion-theoretic characterisation of P by A. Cobham ('64).

- E.g. if $f(X)$ is defined by (bounded) recursion on $|X|$, then $\underbrace{\exists Y f(X) = Y}_{\exists^2\text{FO formula}}$ is inferred by $\exists^2$FO-IND on $|X|$.

Conclusion

Summary: Axioms of inflationary/non-inflationary inductive definitions are introduced.

- New machine-independent characterisations of P & PSPACE.
- P vs. PSPACE problem can be reduced the distinction between inflationary/non-inflationary inductive definitions.
- Classical recursion-theoretic characterisations of P & PSPACE are connected to model-theoretic characterisations.

Observation:

- In contrast to infinitary ones, the axiom of finitary inductive definitions is logically close to Pigeon Hole Principle.
  (If $n + 1$ pigeons in n holes, then there is a pair of pigeons)
- Indeed (FO-ID) implies a specific form of PHP.

Further research

Possible extension:

- It seems possible to extend the characterisation of P to the polynomial hierarchy, e.g., NP.
- Extension to EXP would be also possible.
(Recall it is not known if $\mathrm{NP} \subsetneq \mathrm{PSPACE} \subsetneq \mathrm{EXP}$)

In terms of bounded reverse mathematics:

- $\mathrm{V}^0 \vdash$ (FO-IID) $\rightarrow$ ($\exists^2$FO-IND)?
Equivalently $\mathrm{V}^0 \vdash$ (FO-IID) $\rightarrow$ ($\exists^2$FO-CA)?
- $\mathrm{V}^0 \vdash$ (FO-ID) $\rightarrow$ ($\exists^3$SO-IND)?
Equivalently $\mathrm{V}^0 \vdash$ (FO-ID) $\rightarrow$ ($\exists^3$SO-CA)?

References

Characterising Complexity Classes by Inductive Definitions in Bounded Arithmetic
Naohi Eguchi
Technical report, arXiv: 1306.5559 [math.LO], 2013.

Thank you for your attention!

Speaker is supported by JSPS postdoctoral fellowships for young scientists.