Characterising Complexity Classes by Fixed Point Axioms

Naohi Eguchi

Institute of Computer Science
University of Innsbruck
Austria

19 September 2013, Swansea University

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.

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.

Introduction (2/2)

Definition

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

- It is not known if $\mathrm{P} \subsetneq \#\mathrm{P} \subsetneq \mathrm{PSPACE}$, e.g.
  1. PSPACE is closed under summation:
  $$f(x, \vec{y}) = \sum_{i=0}^{x} g(i, \vec{y}).$$
  2. It is not known if P is closed under summation.
- To know much about complexity classes: Machine-independent logical characterisations.

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: $\begin{cases} \mathcal{F} = \mathrm{P} \text{ or } \mathcal{F} = \mathrm{PSPACE}, \\ \text{Ax is Axiom of Inductive Definitions.} \end{cases}$

Inductive definition (monotone case)

Example

$\mathbb{N}$ is the smallest set containing 0 closed under $x \mapsto x + 1$.
More precisely: define an operator $F : \mathcal{P}(V) \to \mathcal{P}(V)$ by
$x \in F(X) :\Leftrightarrow x = 0 \lor \exists y \in X(x = y + 1)$.

See:

- $\mathbb{N}$ is the least fixed point of F:
  - $F(\mathbb{N}) \subseteq \mathbb{N}$ (Fixed point)
  - $\forall X \subseteq V[F(X) \subseteq X \to \mathbb{N} \subseteq X]$ (Leastness)
- The least fixed point exists since F is monotone:

$$X \subseteq Y \Rightarrow F(X) \subseteq F(Y)$$

Inductive definition (general case)

Let α: an ordinal number.

Definition

$$\begin{cases} F^0 & := & \emptyset \\ F^{\alpha+1} & := & F(F^\alpha) \\ F^\gamma & := & \bigcup_{\alpha<\gamma} F^\alpha \quad (\gamma : \text{limit}) \end{cases}$$

See: $\exists \alpha_0 < \#\mathcal{P}(V)$ such that $F^{\alpha_0+1} = F(F^{\alpha_0}) = F^{\alpha_0}$.

Example

$x \in F(X) :\Leftrightarrow x = 0 \vee \exists y \in X(x = y + 1)$.
See: $\mathbb{N} = F^{\alpha_0}$ for $\alpha_0 = \min\{\alpha\colon \text{ordinal} \mid F^{\alpha+1} = F^\alpha\}$.

Finitary inductive definitions

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

Define F^m by $\begin{cases} F^0 & := & \emptyset \\ F^{m+1} & := & F(F^m) \end{cases}$

Definition

If F is inflationary if $X \subseteq F(X)$ for any $X \subseteq S$.

- $\exists k \leq \#S$ such that $F^{k+1} = F^k$ if F is inflationary.
- $\exists k \leq \#S$ 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 $f(X)$;

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

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

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

Motivation: Finite model theory

Model-theoretic characterisations of P, PSPACE.

Theorem (Immerman '82, Vardi '82)

Over finite structures, the following are equivalent.

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

Theorem (Immerman et al.)

Over finite structures, the following are equivalent.

1. *A predicate* $L \in \mathrm{PSPACE}$.
2. *L can be expressed by FO with the fixed point predicate of a FO definable non-inflationary operator.*

Bounded arithmetic (1/3)

- 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 (2/3)

Second order bounded arithmetic:

- Language $\mathcal{L}^2_{\mathsf{BA}}$: 0, 1, $+$, $\cdot$ and $|X|$.
- First order elements $x, y, z, \dots$: natural numbers with upper bounds of $\mathcal{L}^2_{\mathsf{BA}}$-terms, i.e. polynomials.
- Second order elements $X, Y, Z, \dots$: 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.

Bounded arithmetic (3/3)

Question. Why second order formulation?
Reason. To avoid inessential string encoding.

- (Turing) computations are "rewriting of finite strings".
- In classical formulation: encoding finite strings with exponentials e.g. $\ulcorner a_1 a_2 \cdots a_k \urcorner = 2^{\ulcorner a_1 \urcorner} \cdot 3^{\ulcorner a_2 \urcorner} \cdot \cdots \cdot p_k^{\ulcorner a_k \urcorner}$.
- Conversely: numerical functions can be regarded as functions over $\{0, 1\}$-strings.

Question. Why first order elements necessary?
Reason. To rewrite strings without encoding but with:

$$\forall X \exists Y (\forall i < |Y|)(i \in Y \leftrightarrow \varphi(i, X)) \qquad \text{(Comprehension)}$$

Meaning: $i \in X \iff$ the ith element of X is 1
($i \notin X \iff$ the ith element of X is 0)

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_1^{B}.

Theorem

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

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), $i_1, \ldots, i_{|X|} \in \{0, 1\})$

- 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), $i_1, \ldots, i_{|f(X)|} \in \{0, 1\})$

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

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. $\begin{cases} f(X) \text{ is computable in } 2^{p(|X|)} \text{steps} \\ |\mathrm{TAPE}^L| \leq p(|X|) \end{cases}$

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

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

See: TAPE^K denotes the final tape description.

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

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

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

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 $\mathrm{V}^0 + (\exists^2 FO\text{-}IND) \vdash \forall X \exists ! Y f(X) = Y$ 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 to 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.