Seminar 2, June 12, 2013

Characterising Complexity Classes by Fixed Point Axioms

Naohi Eguchi

Institute of Computer Science, University of Innsbruck

Introduction 1/3

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

Introduction 2/3

- $\mathbf{P}$: the class of polynomial-time computable funcs.
- $\mathbf{PSPACE}$: the class of polynomial-space computable functions.

Facts

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

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

Any strict inclusion is not known.

Introduction 3/3

- It is not known if $\mathbf{P} \subsetneq \#\mathbf{P} \subsetneq \mathbf{PSPACE}$, e.g.
  1. $\mathbf{PSPACE}$ is closed under *summation*:

     If $g \in \mathbf{PSPACE}$, then $f \in \mathbf{PSPACE}$, where

     $$f(x, \vec{y}) = \sum_{i=0}^{x} g(i, \vec{y})$$
  2. It is not known if $\mathbf{P}$ is closed under summation.
- To know more about complexity classes:

  Machine-independent logical characterisations.

  (Recursion-theoretic, Model-theoretic,

  Proof-theoretic, Term-rewriting, ...)

Outline

- There may be many characterisations of one class.
- What is the most essential principle to uniformly defines functions in a complexity class?

Outline

- There may be many characterisations of one class.
- What is the most essential principle to uniformly defines functions in a complexity class?

  Given a complexity class $\mathcal{F}$ find an axiom Ax s.t.

  1. $f \in \mathcal{F} \implies \mathbf{T} + \mathrm{Ax} \vdash \forall x \exists ! y f(x) = y$.
  2. $\mathbf{T} + \mathrm{Ax} \vdash \forall x \exists ! y f(x) = y \implies f \in \mathcal{F}$.

  ($\mathbf{T}$: a base axiomatic system)

Outline

- There may be many characterisations of one class.
- What is the most essential principle to uniformly defines functions in a complexity class?

  Given a complexity class $\mathcal{F}$ find an axiom Ax s.t.

  1. $f \in \mathcal{F} \implies \mathbf{T} + \text{Ax} \vdash \forall x \exists ! y f(x) = y$.
  2. $\mathbf{T} + \text{Ax} \vdash \forall x \exists ! y f(x) = y \implies f \in \mathcal{F}$.

  ($\mathbf{T}$: a base axiomatic system)
- This work: $\mathcal{F} = \mathbf{P}$ or $\mathcal{F} = \mathbf{PSPACE}$,

  Ax is Fixed Point axiom.

Fixed Point principle

Let $F : S \to S$ $(\#S < \omega)$.

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

Fixed Point principle

Let $F : S \to S$ ($\#S < \omega$).

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

- $\exists k < 2^{\#S}$, $\exists l > 0$ 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^l denotes the tape description at the lth step in computing $f(x)$;

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

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

Connection to time-complexity

Suppose:

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

   TAPE^0 =

B	i_1	$\cdots$	$i_{\|x\|}$	B	$\cdots$	B

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

Connection to time-complexity

Suppose:

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

   $\text{TAPE}^0 =$

B	i_1	$\cdots$	$i_{\vert x\vert}$	B	$\cdots$	B

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

Then

- $\text{TAPE}^{T(x)+1} = \text{TAPE}^{T(x)}$.
- Further $\forall l \geq T(x)$, $\text{TAPE}^l = \text{TAPE}^{T(x)}$.

Finite model theory

Model-theoretic characterisations of $\mathbf{P}$, $\mathbf{PSPACE}$.

Thm (N. Immerman et al.)

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

Bounded arithmetic 1/2

- Introducing a fixed point axiom (FP) s.t.
  1. $f \in \mathcal{F} \implies \mathbf{T} + (\text{FP}) \vdash \forall x \exists! y f(x) = y$.
  2. $\mathbf{T} + \text{FP} \vdash \forall x \exists! y f(x) = y \implies f \in \mathcal{F}$.

  where $\mathcal{F} = \mathbf{P}$ or $\mathcal{F} = \mathbf{PSPACE}$.
- The base system $\mathbf{T}$ must be weak: $\mathbf{T} \nvdash$ (FP).
- Bounded arithmetic seems suitable for $\mathbf{T}$.

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

Fixed point axiom

Def $\forall x, \exists X, Y$ s.t. $|X|, |Y| \leq x$, $Y \neq \emptyset$ and

1. $\forall j < x(P_\varphi^{\emptyset}(j) \leftrightarrow \emptyset(i))$ ($\emptyset$: empty string)
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_φ^X: 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. $F^{k+l} = F^k$

Fixed point axiom

Def $\forall x, \exists X, Y$ s.t. $|X|, |Y| \leq x$, $Y \neq \emptyset$ and

1. $\forall j < x(P_\varphi^{\emptyset}(j) \leftrightarrow \emptyset(i))$ ($\emptyset$: empty string)
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_φ^X: 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. $F^{k+l} = F^k$

Fixed point axiom

Def $\forall x, \exists X, Y$ s.t. $|X|, |Y| \leq x$, $Y \neq \emptyset$ and

1. $\forall j < x(P_\varphi^{\emptyset}(j) \leftrightarrow \emptyset(i))$ ($\emptyset$: empty string)
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_φ^X: 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

Def (FO-FP): Fixed point axiom for some FO φ.

Def (FO-IFP): (FO-FP) and additionally $\forall X, \forall i < |X|(i \in X \rightarrow \varphi(i, X))$ holds.

Main results

Def (FO-FP): Fixed point axiom for some FO φ.

Def (FO-IFP): (FO-FP) and additionally $\forall X, \forall i < |X|(i \in X \rightarrow \varphi(i, X))$ holds.

Let $\mathbf{T_0}$ be a base system of bounded arithmetic.

Thm 1 $f \in \mathbf{P}$ if and only if $\mathbf{T_0}$ + (FO-IFP) $\vdash \forall X \exists ! Y f(X) = Y$.

Thm 2 $f \in \mathbf{PSPACE}$ if and only if $\mathbf{T_0}$ + (FO-FP) $\vdash \forall X \exists ! Y f(X) = Y$.

Connection to time-complexity

Suppose:

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

   TAPE^{0} =

B	i_1	$\cdots$	$i_{\lvert x \rvert}$	B	$\cdots$	B

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

Then

- TAPE$^{T(x)+1}$ = TAPE$^{T(x)}$.
- Father $\forall l \geq T(x)$, TAPE^{l} = TAPE$^{T(x)}$.

Proof of "only if" of Theorem 2

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

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

See: $\mathsf{TAPE}^L \mapsto \mathsf{TAPE}^{L+1}$: FO-definable.

By ($\exists^2$FO-FP) $\exists K, \exists L$ s.t. $\mathsf{TAPE}^{K+L} = \mathsf{TAPE}^K$

See: TAPE^K must be in the accepting state.

So $f(X) = Y \Leftrightarrow \exists K, L$ s.t. $|K|, |L| \leq p(|X|)$,
$\mathsf{TAPE}^{K+L} = \mathsf{TAPE}^K \wedge Y = \mathsf{output}(\mathsf{TAPE}^K)$

Hence $\mathbf{T_0}$ + (FO-FP) $\vdash \forall X \exists! Y\, f(X) = Y$.

Proof of “only if” of Theorem 2

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

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

See: $\mathsf{TAPE}^L \mapsto \mathsf{TAPE}^{L+1}$: FO-definable.

By ($\exists^2$FO-FP) $\exists K, \exists L$ s.t. $\mathsf{TAPE}^{K+L} = \mathsf{TAPE}^K$

See: TAPE^K must be in the accepting state.

So $f(X) = Y \Leftrightarrow \exists K, L$ s.t. $|K|, |L| \leq p(|X|)$,

$\mathsf{TAPE}^{K+L} = \mathsf{TAPE}^K \wedge Y = \mathsf{output}(\mathsf{TAPE}^K)$

Hence $\mathbf{T_0} + (\text{FO-FP}) \vdash \forall X \exists! Y f(X) = Y$.

Proof of "only if" of Theorem 2

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

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

See: $\mathsf{TAPE}^L \mapsto \mathsf{TAPE}^{L+1}$: FO-definable.

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

See: TAPE^K must be in the accepting state.

So $f(X) = Y \Leftrightarrow \exists K, L$ s.t. $|K|, |L| \leq p(|X|)$,

$\mathsf{TAPE}^{K+L} = \mathsf{TAPE}^K \wedge Y = \mathsf{output}(\mathsf{TAPE}^K)$

Hence $\mathbf{T_0} +$ (FO-FP) $\vdash \forall X \exists! Y f(X) = Y$.

Proof of "only if" of Theorem 2

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

$\exists p$: poly $\begin{cases} f(X) \text{ is computable in } 2^{p(|X|)} \text{steps} \\ |\mathsf{TAPE}^{L}| \le p(|X|) \end{cases}$

See: $\mathsf{TAPE}^{L} \mapsto \mathsf{TAPE}^{L+1}$: FO-definable.

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

See: TAPE^{K} must be in the accepting state.

So $f(X) = Y \Leftrightarrow \exists K, L$ s.t. $|K|, |L| \le p(|X|)$,

$\quad \mathsf{TAPE}^{K+L} = \mathsf{TAPE}^{K} \wedge Y = \mathsf{output}(\mathsf{TAPE}^{K})$

Hence $\mathbf{T_0} + \text{(FO-FP)} \vdash \forall X \exists! Y f(X) = Y$.

“if” of Theorem 1 & 2

Proof of “if” direction of Thm 1 & 2 are based on:

Thm (Zambella ’96) $\boldsymbol{f} \in \mathbf{P}$ if and only if

$\mathbf{T_0} + (\exists^{\mathbf{2}}\text{FO-IND}) \vdash \forall \boldsymbol{X} \exists ! \boldsymbol{Y} \boldsymbol{f}(\boldsymbol{X}) = \boldsymbol{Y}$.

($\exists^{\mathbf{2}}$FO: $\exists \boldsymbol{X} \varphi$ for some FO φ)

Thm (Skelley ’06) $\boldsymbol{f} \in \mathbf{PSPACE}$ if and only if

$\mathbf{T_0} + (\exists^{\mathbf{3}}\text{SO-IND}) \vdash \forall \boldsymbol{X} \exists ! \boldsymbol{Y} \boldsymbol{f}(\boldsymbol{X}) = \boldsymbol{Y}$.

($\exists^{\mathbf{3}}$SO: third order $\exists \boldsymbol{\mathcal{X}} \varphi$ for some second order φ)

“if” of Theorem 1 & 2

Proof of “if” direction of Thm 1 & 2 are based on:

Thm (Zambella ’96) $\boldsymbol{f} \in \mathbf{P}$ if and only if

$\mathbf{T_0} + (\exists^{\mathbf{2}}\text{FO-IND}) \vdash \forall \boldsymbol{X} \exists! \boldsymbol{Y} \, \boldsymbol{f}(\boldsymbol{X}) = \boldsymbol{Y}$.

($\exists^{\mathbf{2}}$FO: $\exists \boldsymbol{X} \varphi$ for some FO φ)

Show: $\mathbf{T_0} \vdash (\exists^{\mathbf{2}}\text{FO-IND}) \to (\text{FO-IFP})$.

Thm (Skelley ’06) $\boldsymbol{f} \in \mathbf{PSPACE}$ if and only if

$\mathbf{T_0} + (\exists^{\mathbf{3}}\text{SO-IND}) \vdash \forall \boldsymbol{X} \exists! \boldsymbol{Y} \, \boldsymbol{f}(\boldsymbol{X}) = \boldsymbol{Y}$.

($\exists^{\mathbf{3}}$SO: third order $\exists \boldsymbol{\mathcal{X}} \varphi$ for some second order φ)

Show: $\mathbf{T_0} \vdash (\exists^{\mathbf{3}}\text{SO-IND}) \to (\text{FO-FP})$.

Concluding remarks

It is not clear yet if:

1. $\mathbf{T_0} \vdash (\text{FO-IFP}) \rightarrow (\exists^{\mathbf{2}}\text{FO-IND})$.
2. $\mathbf{T_0} \vdash (\text{FO-FP}) \rightarrow (\exists^{\mathbf{3}}\text{SO-IND})$.

Concluding remarks

It is not clear yet if:

1. $\mathbf{T_0} \vdash$ (FO-IFP) $\rightarrow$ ($\exists^{\mathbf{2}}$FO-IND).
2. $\mathbf{T_0} \vdash$ (FO-FP) $\rightarrow$ ($\exists^{\mathbf{3}}$SO-IND).

Thm (Zambella '96) $\boldsymbol{f} \in \mathbf{P}$ if and only if $\mathbf{T_0} +$ ($\exists^{\mathbf{2}}$FO-IND) $\vdash \forall \boldsymbol{X} \exists ! \boldsymbol{Y} \boldsymbol{f}(\boldsymbol{X}) = \boldsymbol{Y}$.

Proof is based on a recursion-theoretic characterisation of $\mathbf{P}$ by A. Cobham ('64). (If $\boldsymbol{f}(\boldsymbol{X})$ is defined by recursion on $|\boldsymbol{X}|$, then $\exists ! \boldsymbol{Y} \boldsymbol{f}(\boldsymbol{X}) = \boldsymbol{Y}$ is inferred by ($\exists^{\mathbf{2}}$FO-IND) on $|\boldsymbol{X}|$)

Summary

Fixed point axioms (FO-IFP), (FO-FP) are introduced.

- New proof-theoretic characterisations of $\mathbf{P}$ and $\mathbf{PSPACE}$.
- Classical recursion-theoretic characterisations of $\mathbf{P}$ and $\mathbf{PSPACE}$ are connected to model-theoretic characterisations.

Further research

Connection to rewriting characterisations of $\mathbf{P}$ by termination orders (Avanzini-Moser '08, Avanzini-E.-Moser '12)?

- Example: For a termination order $\succ$, $f \in \mathbf{P}$ if and only if $\mathbf{T_0} + \mathrm{WF}(\succ) \vdash \forall X \exists! Y\, f(X) = Y$. (WF($\succ$): "There is no infinite descending sequence $t_0 \succ t_1 \succ \cdots$")
- If so: $\mathbf{T_0} \vdash$ (FO-IFP) $\leftrightarrow$ WF($\succ$)?

  $\mathbf{T_0} \vdash$ ($\exists^2$FO-IND) $\leftrightarrow$ WF($\succ$)?

Thank you for your attention!

Speaker is supported by JSPS postdoctoral fellowships for young scientists.