On Toda's Theorem in structural communication complexity

Henning Wunderlich

Universität Ulm, Institut für Theoretische Informatik,
Oberer Eselsberg, D-89069 Ulm, e-mail: henning.wunderlich@uni-ulm.de

SOFSEM 2009,
Hotel Arnika, Špindlerův Mlýn, Czech Republic,
January 27, 2009

Outline

Yao's Model

Definition (Yao's Model)

- Two almighty players Alice and Bob

Yao's Model

Definition (Yao's Model)

- Two almighty players Alice and Bob
- They want to compute $f(x, y)$ for function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$, where $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ are finite sets

Yao's Model

Definition (Yao's Model)

- Two almighty players Alice and Bob
- They want to compute $f(x, y)$ for function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$, where $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ are finite sets
- Distributed inputs: Alice $x \in \mathcal{X}$, Bob $y \in \mathcal{Y}$

Yao's Model

Definition (Yao's Model)

- Two almighty players Alice and Bob
- They want to compute $f(x, y)$ for function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$, where $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ are finite sets
- Distributed inputs: Alice $x \in \mathcal{X}$, Bob $y \in \mathcal{Y}$
- Players send messages (bits);
  communication is specified by a protocol

Protocol variants

Analogously to Turing machines, protocols can be

- deterministic : messages depend only on the player's input and the messages sent before
- randomized
- guess protocols
- alternating
- ...

Protocol variants

Analogously to Turing machines, protocols can be

- deterministic
- randomized :
  - players have random source
  - messages may also depend on random source
  - output is a random variable $\rightsquigarrow$ we may allow error
- guess protocols
- alternating
- ...

Protocol variants

Analogously to Turing machines, protocols can be

- deterministic
- randomized
- guess protocols :
  - output is 0 (rejecting) or 1 (accepting)
  - players may guess bits (guess strings)
  - players accept input (x, y) if $C(acc(x, y), rej(x, y))$ holds
    - $C(acc, rej)$ accepting mode
    - $acc(x, y) :=$ number of guess strings leading to an accepting output
    - analogously for $rej(x, y)$
- alternating
- ...

Protocol variants

Analogously to Turing machines, protocols can be

- deterministic
- randomized
- guess protocols
- alternating :
  - output is 0 (rejecting) or 1 (accepting)
  - players may guess bits existentially $\exists$ or universally $\forall$
  - input acceptance defined analogously to TM
- ...

What is "Structural complexity theory"?

First of all, for every computation model there exists a structural theory!

Computation models

- Turing machine/Register machine.

Resources

- Time, Space.

What is "Structural complexity theory"?

First of all, for every computation model there exists a structural theory!

Computation models

- Turing machine/Register machine.
- Branching program/Circuit/OBDD.

Resources

- Time, Space.
- Size, Depth, Width.

What is "Structural complexity theory"?

First of all, for every computation model there exists a structural theory!

Computation models

- Turing machine/Register machine.
- Branching program/Circuit/OBDD.
- Communication protocol.

Resources

- Time, Space.
- Size, Depth, Width.
- Number of communicated bits.

What is "Structural complexity theory"?

First of all, for every computation model there exists a structural theory!

Computation models

- Turing machine/Register machine.
- Branching program/Circuit/OBDD.
- Communication protocol.
- ...

Resources

- Time, Space.
- Size, Depth, Width.
- Number of communicated bits.
- ...

What is "Structural complexity theory"?

Variants

What is "Structural complexity theory"?

Variants

- Randomization

What is "Structural complexity theory"?

Variants

- Randomization
- Guess strings + accepting modes

What is "Structural complexity theory"?

Variants

- Randomization
- Guess strings + accepting modes
- Alternation

What is "Structural complexity theory"?

Variants

- Randomization
- Guess strings + accepting modes
- Alternation
- ...

What is "Structural complexity theory"?

Some features/recurring themes . . .

- Definition of complexity classes containing
  - decision problems
  - functions
  - optimization problems

.

What is "Structural complexity theory"?

Some features/recurring themes ...

- Definition of complexity classes .
- Comparisons of classes (Inclusion relations).

Example

- $\mathbf{P} \neq \mathbf{NP}$?
- $\mathbf{BPP} \subseteq \mathbf{PSPACE}$.
- $\mathbf{PH}^{cc} = \mathbf{PSPACE}^{cc}$?
- ...

What is "Structural complexity theory"?

Some features/recurring themes ...

- Definition of complexity classes .
- Comparisons of classes (Inclusion relations).
- Reductions, hardness/completeness.

Example

- Many-one reduction $A \leq_m B$ defined by

  $\exists$ reduction f such that $x \in A \Leftrightarrow f(x) \in B$ for all x.

- ...

What is "Structural complexity theory"?

Some features/recurring themes ...

- ...
- Reductions, hardness/completeness.
- Closure properties.

Example

- set theoretic operations: $A, B \in \mathcal{C} \Rightarrow A \cup B \in \mathcal{C}$?
- closure under reductions: $A \leq_m B$ and $B \in \mathcal{C} \Rightarrow A \in \mathcal{C}$?
- closure under class operators: $\mathrm{BP} \cdot \mathcal{C} \subseteq \mathcal{C}$?
- ...

What is "Structural complexity theory"?

Some features/recurring themes ...

- Definition of complexity classes .
- Comparisons of classes (Inclusion relations).
- Reductions, hardness/completeness.
- Closure properties.
- Relativization.

Example

- there exist A, B with $\mathbf{PH}^A = \mathbf{PSPACE}^A$ and $\mathbf{PH}^B \neq \mathbf{PSPACE}^B$.
- $\mathbf{BPP}(\mathbf{BPP}) = \mathbf{BPP}$.
- ...

What is "Structural complexity theory"?

Some features/recurring themes . . .

- Definition of complexity classes .
- Comparisons of classes (Inclusion relations).
- Reductions, hardness/completeness.
- Closure properties.
- Relativization.
- . . .

Definition of complexity classes

The definition of a complexity class is often based on ...

- Variant of a computation model

Definition of complexity classes

The definition of a complexity class is often based on ...

- Variant of a computation model
- Resource complexity (defined for each variant)

Definition of complexity classes

The definition of a complexity class is often based on ...

- Variant of a computation model
- Resource complexity (defined for each variant)
- A notion of efficiency: poly(n), polylog(n)

Definition of complexity classes

The definition of a complexity class is often based on ...

- Variant of a computation model
- Resource complexity (defined for each variant)
- A notion of efficiency: poly(n), polylog(n)

Definition (Class "P")

"P": class of decision problems that can be decided efficiently deterministically

Definition of complexity classes

The definition of a complexity class is often based on ...

- Variant of a computation model
- Resource complexity (defined for each variant)
- A notion of efficiency: poly(n), polylog(n)

Definition (Class "P")

"P": class of decision problems that can be decided efficiently deterministically

Definition (Class "BPP")

"BPP": class of decision problems that can be decided efficiently randomized with bounded error

Definition of classes

Definition (Class "PSPACE")

"PSPACE": class of decision problems that can be decided efficiently with an efficient number of alternations

Definition of classes

Definition (Class "PSPACE")

"PSPACE": class of decision problems that can be decided efficiently with an efficient number of alternations

Definition ("Polynomial Hierarchy")

Definition of classes

Definition (Class "PSPACE")

"PSPACE": class of decision problems that can be decided efficiently with an efficient number of alternations

Definition ("Polynomial Hierarchy")

- "Σ_k": class of decision problems that can be decided efficiently with $k-1$ alternations starting in $\exists$-state

Definition of classes

Definition (Class "PSPACE")

"PSPACE": class of decision problems that can be decided efficiently with an efficient number of alternations

Definition ("Polynomial Hierarchy")

- "Σ_k": class of decision problems that can be decided efficiently with $k-1$ alternations starting in $\exists$-state
- "PH" $:= \cup_{k \geq 0} \Sigma_k$ = constant number of alternations

Definition of classes

Definition ("Counting classes")

"μP": class of decision problems that can be decided efficiently using guess strings and accepting mode μ. Especially, we have

"NP": $N(acc, rej) := (acc > 0)$ (nondeterministic)

Definition of classes

Definition ("Counting classes")

"μP": class of decision problems that can be decided efficiently using guess strings and accepting mode μ. Especially, we have

"NP": $N(acc, rej) := (acc > 0)$ (nondeterministic)

"co-NP": $co\text{-}N(acc, rej) := (rej = 0)$ (co-nondeterministic)

Definition of classes

Definition ("Counting classes")

"μP": class of decision problems that can be decided efficiently using guess strings and accepting mode μ. Especially, we have

"NP": $N(acc, rej) := (acc > 0)$ (nondeterministic)

"co-NP": $co\text{-}N(acc, rej) := (rej = 0)$ (co-nondeterministic)

"PP": $P(acc, rej) := (acc > rej)$

Definition of classes

Definition ("Counting classes")

"μP": class of decision problems that can be decided efficiently using guess strings and accepting mode μ. Especially, we have

"NP": $N(acc, rej) := (acc > 0)$ (nondeterministic)

"co-NP": $co\text{-}N(acc, rej) := (rej = 0)$ (co-nondeterministic)

"PP": $P(acc, rej) := (acc > rej)$

"$\oplus$P": $\oplus(acc, rej) := (acc \mod 2 = 1)$ (parity)

Inclusion relations

Observation (true for every model)

- "P" $\subseteq$ "BPP" $\subseteq$ "PP" $\subseteq$ "PSPACE"
- "P" $\subseteq$ "NP", "co-NP" $\subseteq$ "PH" $\subseteq$ "PSPACE"
- "P" $\subseteq$ "PP", "$\oplus$P" $\subseteq$ "PSPACE"

Inclusion relations

Observation

- $\mathbf{P} \subsetneq (?)\ \mathbf{BPP} \subsetneq (?)\ \mathbf{PP} \subsetneq (?)\ \mathbf{PSPACE}$
- $\mathbf{P} \subsetneq (?)\ \mathbf{NP}, \mathbf{co\text{-}NP} \subsetneq (?)\ \mathbf{PH} \subsetneq (?)\ \mathbf{PSPACE}$
- $\mathbf{P} \subsetneq (?)\ \mathbf{PP}, \oplus\mathbf{P} \subsetneq (?)\ \mathbf{PSPACE}$
- $\mathbf{NP}$ vs. $\mathbf{co\text{-}NP}(?)$; $\mathbf{NP}$ vs. $\mathbf{PP}(?)$; $\mathbf{NP}$ vs. $\oplus\mathbf{P}(?)$; $\mathbf{PP}$ vs. $\oplus\mathbf{P}(?)$; ...

Two examples

- Turing machine model: we don't know anything ...

Inclusion relations

Observation

- $\mathbf{P}^{cc} \subsetneq \mathbf{BPP}^{cc} \subsetneq \mathbf{PP}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$
- $\mathbf{P}^{cc} \subsetneq \mathbf{NP}^{cc}, \mathbf{co\text{-}NP}^{cc} \subsetneq \mathbf{PH}^{cc}$;
- $\mathbf{P}^{cc} \subsetneq \mathbf{PP}^{cc}, \oplus\mathbf{P}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$
- $(\mathbf{NP}^{cc}, \mathbf{co\text{-}NP}^{cc})$, $(\mathbf{NP}^{cc}, \mathbf{PP}^{cc})$, $(\mathbf{NP}^{cc}, \oplus\mathbf{P}^{cc})$, $(\mathbf{PP}^{cc}, \oplus\mathbf{P}^{cc})$ incomparable, ...

Two examples

- Turing machine model: we don't know anything ...
- Yao's model: we know a lot ...

Inclusion relations

Observation

- $\mathbf{P}^{cc} \subsetneq \mathbf{BPP}^{cc} \subsetneq \mathbf{PP}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$
- $\mathbf{P}^{cc} \subsetneq \mathbf{NP}^{cc}, \mathbf{co\text{-}NP}^{cc} \subsetneq \mathbf{PH}^{cc}$; $\mathbf{PH}^{cc} \subsetneq (?)\ \mathbf{PSPACE}^{cc}$
- $\mathbf{P}^{cc} \subsetneq \mathbf{PP}^{cc}, \oplus\mathbf{P}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$
- $(\mathbf{NP}^{cc}, \mathbf{co\text{-}NP}^{cc})$, $(\mathbf{NP}^{cc}, \mathbf{PP}^{cc})$, $(\mathbf{NP}^{cc}, \oplus\mathbf{P}^{cc})$, $(\mathbf{PP}^{cc}, \oplus\mathbf{P}^{cc})$ incomparable, ...

Two examples

- Turing machine model: we don't know anything ...
- Yao's model: we know a lot , but not everything ...

Inclusion relations

Long-standing open problem

Do we have $\mathbf{PH}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$?

Inclusion relations

Long-standing open problem

Do we have $\mathbf{PH}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$?

Recall

Theorem (Toda)

$\mathbf{PH} \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}$

- $\mathbf{PH}^{cc}$ and $\mathbf{PSPACE}^{cc}$ based on alternations
- $\mathrm{BP} \cdot \oplus\mathbf{P}^{cc}$ NOT based on alternations

Inclusion relations

Long-standing open problem

Do we have $\mathbf{PH}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$?

Proof strategy for open problem (milestones)

- Show Toda's Theorem in cc

Inclusion relations

Long-standing open problem

Do we have $\mathbf{PH}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$?

Proof strategy for open problem (milestones)

- Show Toda's Theorem in cc
- Develop measure ν for $\mathrm{BP} \cdot \oplus\mathbf{P}^{cc}$

Inclusion relations

Long-standing open problem

Do we have $\mathbf{PH}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$?

Proof strategy for open problem (milestones)

- Show Toda's Theorem in cc
- Develop measure ν for $\mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$
- Show strict inclusion using ν:

$$\mathrm{BP} \cdot \oplus \mathbf{P}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$$

Inclusion relations

Long-standing open problem

Do we have $\mathbf{PH}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$?

Proof strategy for open problem (milestones)

- Show Toda's Theorem in cc ✓
- Develop measure ν for $\mathrm{BP} \cdot \oplus\mathbf{P}^{cc}$
- Show strict inclusion using ν:

$$\mathrm{BP} \cdot \oplus\mathbf{P}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$$

Inclusion relations

Long-standing open problem

Do we have $\mathbf{PH}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$?

Proof strategy for open problem (milestones)

- Show Toda's Theorem in cc ✓
- Develop measure ν for $\mathrm{BP} \cdot \oplus\mathbf{P}^{cc}$ ✓
- Show strict inclusion using ν:

$$\mathrm{BP} \cdot \oplus\mathbf{P}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$$

Inclusion relations

Long-standing open problem

Do we have $\mathbf{PH}^{cc} \subsetneq \mathbf{PSPACE}^{cc}$?

Proof strategy for open problem (milestones)

- Show Toda's Theorem in cc ✓
- Develop measure ν for $\mathrm{BP} \cdot \oplus\mathbf{P}^{cc}$ ✓
- Show strict inclusion using ν:

$$\mathrm{BP} \cdot \oplus\mathbf{P}^{cc} \subsetneq \mathbf{PSPACE}^{cc} \text{ (not yet)}$$

Complexity classes

Formal languages

Definition

- $\{0,1\}^{**} := \{(x,y) \mid x,y \in \{0,1\}^*, |x| = |y|\}$
- Formal language $L \subseteq \{0,1\}^{**}$
- $L_n := L \cap \{(x,y) \in \{0,1\}^{**} \mid |x| = |y| = n\}$

Complexity classes

Formal languages

Definition

- $\{0,1\}^{**} := \{(x,y) \mid x,y \in \{0,1\}^*, |x| = |y|\}$
- Formal language $L \subseteq \{0,1\}^{**}$
- $L_n := L \cap \{(x,y) \in \{0,1\}^{**} \mid |x| = |y| = n\}$

Definition

A protocol family $(\Pi_n)_{n\in\mathbb{N}}$ decides a language L if each Π_n decides L_n.

Complexity classes

Formal languages

Definition

- $\{0,1\}^{**} := \{(x,y) \mid x,y \in \{0,1\}^*, |x| = |y|\}$
- Formal language $L \subseteq \{0,1\}^{**}$
- $L_n := L \cap \{(x,y) \in \{0,1\}^{**} \mid |x| = |y| = n\}$

Definition

A protocol family $(\Pi_n)_{n\in\mathbb{N}}$ decides a language L if each Π_n decides L_n.

Definition (**poly**)

poly := class of functions with polynomial growth.

Complexity classes

Reductions

Definition (Reductions)

Languages L and L'

- L is many-one reducible to L' iff
  - $\exists$bound $b \in \mathbf{poly}$
  - $\exists$family $\{(f_n, g_n)\}_{n\in\mathbb{N}}$, $f_n, g_n \colon \{0,1\}^n \to \{0,1\}^{\lceil 2^{b(\log n)} \rceil}$
  - $(x, y) \in L \iff (f_n(x), g_n(y)) \in L'$ for all (x, y)

Complexity classes

Reductions

Definition (Reductions)

Languages L and L'

- L is many-one reducible to L' iff
  - $\exists$bound $b \in \mathbf{poly}$
  - $\exists$family $\{(f_n, g_n)\}_{n\in\mathbb{N}}$, $f_n, g_n \colon \{0,1\}^n \to \{0,1\}^{\lceil 2^{b(\log n)} \rceil}$
  - $(x, y) \in L \iff (f_n(x), g_n(y)) \in L'$ for all (x, y)
- Turing reduction
- Majority reduction
- Conjunctive reduction
- ...

Complexity classes

Class operators

Definition (Class operators I)

Language L, bound $p \in \mathbf{poly}$

$$\forall^p(L) := \{(x,y) \in \{0,1\}^{**} \mid \forall w \in \{0,1\}^{\lceil p(\log|x|)\rceil} : (\langle x,w\rangle, \langle y,w\rangle) \in L\} \ ,$$

$$\exists^p(L) := \{(x,y) \in \{0,1\}^{**} \mid \exists w \in \{0,1\}^{\lceil p(\log|x|)\rceil} : (\langle x,w\rangle, \langle y,w\rangle) \in L\} \ ,$$

$$\oplus^p(L) := \{(x,y) \in \{0,1\}^{**} \mid |\{w \in \{0,1\}^{\lceil p(\log|x|)\rceil} \mid (\langle x,w\rangle, \langle y,w\rangle) \in L\}| \mod 2 = 1\} \ .$$

Complexity classes

Class operators

Definition (Class operators II)

Class $\mathcal{C}$

$$\begin{aligned}
\mathrm{co} \cdot \mathcal{C} &:= \{\overline{L} \mid L \in \mathcal{C}\} \ , \\
\forall \cdot \mathcal{C} &:= \{\forall^p(L) \mid L \in \mathcal{C}, p \in \mathbf{poly}\} \ , \\
\exists \cdot \mathcal{C} &:= \{\exists^p(L) \mid L \in \mathcal{C}, p \in \mathbf{poly}\} \ , \\
\oplus \cdot \mathcal{C} &:= \{\oplus^p(L) \mid L \in \mathcal{C}, p \in \mathbf{poly}\} \ .
\end{aligned}$$

Complexity classes

Class operators

Definition (Class operators II)

Language L is in $\mathrm{BP} \cdot \mathcal{C}$ iff

- $\exists$language $L' \in \mathcal{C}$ and $\exists$bound $q \in \mathbf{poly}$
- for all (x, y) we have

$$(x, y) \in L \Rightarrow \frac{|\{r \in \{0,1\}^{\lceil q(\log n) \rceil} \mid (\langle x, r \rangle, \langle y, r \rangle) \in L'\}|}{2^{\lceil q(\log n) \rceil}} \geq \frac{2}{3}$$

Complexity classes

Class operators

Definition (Class operators II)

Language L is in $\mathrm{BP} \cdot \mathcal{C}$ iff

- $\exists$language $L' \in \mathcal{C}$ and $\exists$bound $q \in \mathbf{poly}$
- for all (x, y) we have

$$(x, y) \notin L \Rightarrow \frac{|\{r \in \{0,1\}^{\lceil q(\log n) \rceil} \mid (\langle x, r \rangle, \langle y, r \rangle) \in L'\}|}{2^{\lceil q(\log n) \rceil}} \leq \frac{1}{3}$$

Complexity classes

Class operators

Observation (Compatibility)

$$\begin{aligned}
\mathbf{NP}^{cc} &= \exists \cdot \mathbf{P}^{cc} \ , \\
\mathbf{co\text{-}NP}^{cc} &= \forall \cdot \mathbf{P}^{cc} \ , \\
\oplus\mathbf{P}^{cc} &= \oplus \cdot \mathbf{P}^{cc} \ , \\
\mathbf{BPP}^{cc} &= \mathrm{BP} \cdot \mathbf{P}^{cc} \ .
\end{aligned}$$

Complexity classes

Classes based on alternations

Definition (Polynomial hierarchy)

$$\mathbf{PH}^{cc} := \bigcup_{k \geq 0} \Sigma_k^{cc} \ ,$$

$$\Sigma_0^{cc} := \mathbf{P}^{cc} \ ,$$
$$\Sigma_{k+1}^{cc} := \exists \cdot \mathrm{co} \cdot \Sigma_k^{cc} \ .$$

Remark

New and old definition of $\mathbf{PH}^{cc}$ *are equivalent.*

Valiant-Vazirani-Lemma

Classical result in structural (time) complexity:

Lemma (Valiant-Vazirani)

$\mathbf{NP} \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}$.

Valiant-Vazirani-Lemma

Classical result in structural (time) complexity:

Lemma (Valiant-Vazirani)

$\mathbf{NP} \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}$.

Idea:

Valiant-Vazirani-Lemma

Classical result in structural (time) complexity:

Lemma (Valiant-Vazirani)

$\mathbf{NP} \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}$.

Idea:

- randomised reduction of SAT to $\oplus\mathrm{SAT}$

Valiant-Vazirani-Lemma

Classical result in structural (time) complexity:

Lemma (Valiant-Vazirani)

$\mathbf{NP} \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}$.

Idea:

- randomised reduction of SAT to $\oplus\mathrm{SAT}$
- CNF $\phi \mapsto$ CNF $f(\phi) := \phi \wedge \psi(R)$

Valiant-Vazirani-Lemma

Classical result in structural (time) complexity:

Lemma (Valiant-Vazirani)

$\mathbf{NP} \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}$.

Idea:

- randomised reduction of SAT to $\oplus\mathrm{SAT}$
- CNF $\phi \mapsto$ CNF $f(\phi) := \phi \wedge \psi(R)$
- ϕ unsatisfiable $\Rightarrow$ $f(\phi)$ unsatisfiable

Valiant-Vazirani-Lemma

Classical result in structural (time) complexity:

Lemma (Valiant-Vazirani)

$\mathbf{NP} \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}$.

Idea:

- randomised reduction of SAT to $\oplus\mathrm{SAT}$
- CNF $\phi \mapsto$ CNF $f(\phi) := \phi \wedge \psi(R)$
- ϕ unsatisfiable $\Rightarrow$ $f(\phi)$ unsatisfiable
- ϕ satisfiable $\Rightarrow$ with non-negligible probability:

$$\#\text{satisfying assignments}(f(\phi)) = 1 \ .$$

Valiant-Vazirani-Lemma

This relativizes:

Lemma (Valiant-Vazirani (relativized))

$\mathbf{NP}^A \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}^A$ *for every oracle* A.

Valiant-Vazirani-Lemma

This relativizes:

Lemma (Valiant-Vazirani (relativized))

$\mathbf{NP}^A \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}^A$ *for every oracle A.*

Problem

Transferring the respective proof to the cc-setting is not possible because of seemingly non-relativizing reductions.

Valiant-Vazirani-Lemma

This relativizes:

Lemma (Valiant-Vazirani (relativized))

$\mathbf{NP}^A \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}^A$ *for every oracle* A.

Problem

Transferring the respective proof to the cc-setting is not possible because of seemingly non-relativizing reductions.

Open question

Do we have $\mathbf{NP}^{cc}(A) \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}^{cc}(A)$ in structural communication complexity?

Valiant-Vazirani-Lemma

This relativizes:

Lemma (Valiant-Vazirani (relativized))

$\mathbf{NP}^A \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}^A$ *for every oracle* A.

Problem

Transferring the respective proof to the cc-setting is not possible because of seemingly non-relativizing reductions.

Open question

Do we have $\mathbf{NP}^{cc}(A) \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}^{cc}(A)$ in structural communication complexity?

Remark

Relativized version of V.V.-Lemma is used in the original proof of Toda's Theorem.

Valiant-Vazirani-Lemma

Question

How can we show Toda's Theorem without a relativized Valiant-Vazirani-Lemma?

Valiant-Vazirani-Lemma

Question

How can we show Toda's Theorem without a relativized Valiant-Vazirani-Lemma?

Solution

1. There is a version of the V.V.-Lemma using class operators that can be transferred to the cc-setting due to Lance Fortnow using ideas of Harry Buhrman.
2. There is a proof of Toda's Theorem using class operators due to Uwe Schöning.

Valiant-Vazirani-Lemma

Lemma (Valiant-Vazirani (cc-version))

Class $\mathcal{C}$ normal and closed under conjunctive reductions. Then

$$\exists \cdot \mathcal{C} \subseteq \mathrm{BP} \cdot \oplus \cdot \mathcal{C} \ .$$

Definition (Normal)

Class $\mathcal{C}$ is normal iff

- $\mathbf{P}^{cc} \subseteq \mathcal{C}$
- $\mathcal{C}$ closed under $\mathbf{P}^{cc}$-intersection
- $\mathcal{C}$ closed under $\mathbf{P}^{cc}$-union

Valiant-Vazirani-Lemma

Idea

Valiant-Vazirani-Lemma

Idea

- let $L = \exists^p(L') \in \exists \cdot \mathcal{C}$

Valiant-Vazirani-Lemma

Idea

- let $L = \exists^p(L') \in \exists \cdot \mathcal{C}$
- randomly choose field $F := \mathrm{GF}(2^m)$

Valiant-Vazirani-Lemma

Idea

- let $L = \exists^p(L') \in \exists \cdot \mathcal{C}$
- randomly choose field $F := \mathrm{GF}(2^m)$
- randomly choose $(a, b) \in F^2$

Valiant-Vazirani-Lemma

Idea

- let $L = \exists^p(L') \in \exists \cdot \mathcal{C}$
- randomly choose field $F := \mathrm{GF}(2^m)$
- randomly choose $(a, b) \in F^2$
- interpret witness $w = w_0 \dots w_{l-1}$ for input (x, y) as polynomial $p_w(X) := \sum_i w_i X^i$

Valiant-Vazirani-Lemma

Idea

- let $L = \exists^p(L') \in \exists \cdot \mathcal{C}$
- randomly choose field $F := \mathrm{GF}(2^m)$
- randomly choose $(a, b) \in F^2$
- interpret witness $w = w_0 \dots w_{l-1}$ for input (x, y) as polynomial $p_w(X) := \sum_i w_i X^i$
- for "many" (a, b) there is exactly one polynomial p_w with $p_w(a) = b$

Valiant-Vazirani-Lemma

Idea

- let $L = \exists^p(L') \in \exists \cdot \mathcal{C}$
- randomly choose field $F := \mathrm{GF}(2^m)$
- randomly choose $(a, b) \in F^2$
- interpret witness $w = w_0 \dots w_{l-1}$ for input (x, y) as polynomial $p_w(X) := \sum_i w_i X^i$
- for "many" (a, b) there is exactly one polynomial p_w with $p_w(a) = b$
- $\rightsquigarrow$ define $L'' \in \mathcal{C}$ by

$$L'' := \{(\langle\langle x, r\rangle, w\rangle, \langle\langle y, r\rangle, w\rangle) \mid r = \langle m, a, b\rangle; a, b \in \mathrm{GF}(2^m); \\ p_w(a) = b; (\langle x, w\rangle, \langle y, w\rangle) \in L'\}$$

Toda's Theorem

In time complexity we have

Theorem (Toda)

$\mathbf{PH} \subseteq \mathrm{BP} \cdot \oplus\mathbf{P}$

Toda's Theorem

Analogously, in the cc-setting we have

Theorem (Toda)

$\mathbf{PH}^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$

What does this tell us?

Randomization+computing parity is as powerful as every constant number of alternations

Toda's Theorem

Proof sketch of $\Sigma_k^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$:

Proof by induction on k: *Case* $k \to k+1$:

$$\Sigma_{k+1}^{cc} = \exists \cdot \mathrm{co} \cdot \Sigma_k^{cc}$$

Toda's Theorem

Proof sketch of $\Sigma_k^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$:

Proof by induction on k: *Case* $k \to k+1$:

$$\begin{aligned} \Sigma_{k+1}^{cc} &= \exists \cdot \mathrm{co} \cdot \Sigma_k^{cc} \\ &\subseteq \exists \cdot \mathrm{co} \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \end{aligned}$$

Toda's Theorem

Proof sketch of $\Sigma_k^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$:

Proof by induction on k: *Case* $k \to k+1$:

$$\begin{aligned} \Sigma_{k+1}^{cc} &= \exists \cdot \mathrm{co} \cdot \Sigma_k^{cc} \\ &\subseteq \exists \cdot \mathrm{co} \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\ &= \exists \cdot \mathrm{BP} \cdot \mathrm{co} \cdot \oplus \cdot \mathbf{P}^{cc} \end{aligned}$$

Toda's Theorem

Proof sketch of $\Sigma_k^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$:

Proof by induction on k: *Case* $k \to k+1$:

$$\begin{aligned}
\Sigma_{k+1}^{cc} &= \exists \cdot \mathrm{co} \cdot \Sigma_k^{cc} \\
&\subseteq \exists \cdot \mathrm{co} \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \exists \cdot \mathrm{BP} \cdot \mathrm{co} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \exists \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc}
\end{aligned}$$

Toda's Theorem

Proof sketch of $\Sigma_k^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$:

Proof by induction on k: *Case* $k \to k+1$:

$$\begin{aligned}
\Sigma_{k+1}^{cc} &= \exists \cdot \mathrm{co} \cdot \Sigma_k^{cc} \\
&\subseteq \exists \cdot \mathrm{co} \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \exists \cdot \mathrm{BP} \cdot \mathrm{co} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \exists \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&\subseteq \mathrm{BP} \cdot \oplus \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \text{ (Valiant-Vazirani)}
\end{aligned}$$

Toda's Theorem

Proof sketch of $\Sigma_k^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$:

Proof by induction on k: *Case* $k \to k+1$:

$$\begin{aligned}
\Sigma_{k+1}^{cc} &= \exists \cdot \mathrm{co} \cdot \Sigma_k^{cc} \\
&\subseteq \exists \cdot \mathrm{co} \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \exists \cdot \mathrm{BP} \cdot \mathrm{co} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \exists \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&\subseteq \mathrm{BP} \cdot \oplus \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \text{ (Valiant-Vazirani)} \\
&\subseteq \mathrm{BP} \cdot \mathrm{BP} \cdot \oplus \cdot \oplus \cdot \mathbf{P}^{cc}
\end{aligned}$$

Toda's Theorem

Proof sketch of $\Sigma_k^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$:

Proof by induction on k: *Case* $k \to k+1$:

$$
\begin{aligned}
\Sigma_{k+1}^{cc} &= \exists \cdot \mathrm{co} \cdot \Sigma_k^{cc} \\
&\subseteq \exists \cdot \mathrm{co} \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \exists \cdot \mathrm{BP} \cdot \mathrm{co} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \exists \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&\subseteq \mathrm{BP} \cdot \oplus \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \text{ (Valiant-Vazirani)} \\
&\subseteq \mathrm{BP} \cdot \mathrm{BP} \cdot \oplus \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \mathrm{BP} \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc}
\end{aligned}
$$

Toda's Theorem

Proof sketch of $\Sigma_k^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$:

Proof by induction on k: *Case* $k \to k+1$:

$$
\begin{aligned}
\Sigma_{k+1}^{cc} &= \exists \cdot \mathrm{co} \cdot \Sigma_k^{cc} \\
&\subseteq \exists \cdot \mathrm{co} \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \exists \cdot \mathrm{BP} \cdot \mathrm{co} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \exists \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&\subseteq \mathrm{BP} \cdot \oplus \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \text{ (Valiant-Vazirani)} \\
&\subseteq \mathrm{BP} \cdot \mathrm{BP} \cdot \oplus \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \mathrm{BP} \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc}
\end{aligned}
$$

Toda's Theorem

Proof sketch of $\Sigma_k^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$:

Proof by induction on k: *Case* $k \to k+1$:

$$
\begin{aligned}
\Sigma_{k+1}^{cc} &= \exists \cdot \mathrm{co} \cdot \Sigma_k^{cc} \\
&\subseteq \exists \cdot \mathrm{co} \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \exists \cdot \mathrm{BP} \cdot \mathrm{co} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \exists \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&\subseteq \mathrm{BP} \cdot \oplus \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \text{ (Valiant-Vazirani)} \\
&\subseteq \mathrm{BP} \cdot \mathrm{BP} \cdot \oplus \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \mathrm{BP} \cdot \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc} \\
&= \mathrm{BP} \cdot \oplus \cdot \mathbf{P}^{cc}
\end{aligned}
$$

□

Concluding remarks

We have seen Toda's Theorem: $\mathbf{PH}^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$.

We haven't seen (recent developments):

Concluding remarks

We have seen Toda's Theorem: $\mathbf{PH}^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$.

We haven't seen (recent developments):

- Approximate rank is a measure for the BP-parity-complexity

Concluding remarks

We have seen Toda's Theorem: $\mathbf{PH}^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$.

We haven't seen (recent developments):

- Approximate rank is a measure for the BP-parity-complexity
- connection between approximate rank and matrix rigidity
  $\rightsquigarrow$ most functions have high BP-parity-complexity

Concluding remarks

We have seen Toda's Theorem: $\mathbf{PH}^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$.

We haven't seen (recent developments):

- Approximate rank is a measure for the BP-parity-complexity
- connection between approximate rank and matrix rigidity
  $\rightsquigarrow$ most functions have high BP-parity-complexity
- using Ramsey theory one can show:
  (almost) superregular function families have high approximate rank

Concluding remarks

We have seen Toda's Theorem: $\mathbf{PH}^{cc} \subseteq \mathrm{BP} \cdot \oplus \mathbf{P}^{cc}$.

We haven't seen (recent developments):

- Approximate rank is a measure for the BP-parity-complexity
- connection between approximate rank and matrix rigidity
  $\rightsquigarrow$ most functions have high BP-parity-complexity
- using Ramsey theory one can show:
  (almost) superregular function families have high approximate rank

Conjecture

$\mathbf{PH}^{cc} \neq \mathbf{PSPACE}^{cc}$