CoCo (PH)

amir yehudayoff

recall

NP	$\exists P$	$\exists\varphi$
coNP	$\forall P$	$\forall\varphi$
PSPACE	*TQBF*	$\forall\exists\forall\exists\cdots\varphi$

alternations

$$P \subset \exists P \subset \forall\exists P \subset \exists\forall\exists P \subset \cdots$$

$$P \subset \forall P \subset \exists\forall P \subset \forall\exists\forall P \subset \cdots$$

Σ's

for an integer i the class Σ_i^p comprises all $L \subseteq \{0,1\}^*$ such that there is a poly-time TM M and $C > 0$ such that

$$x \in L \quad \Leftrightarrow \quad \exists w_1 \forall w_2 \dots Q_i w_i M(x, w_1, \dots, w_i) = 1$$

where $|w_1, \dots, w_i| \leq C|x|^C$

$$x \notin L \quad \Rightarrow \quad \forall w_1 \exists w_2 \dots Q_i' w_i M(x, w_1, \dots, w_i) = 0$$

Π's

$$\Pi_i^p = co\Sigma_i^p$$

$\exists M, C$ such that

$$x \in L \quad \Leftrightarrow \quad \forall w_1 \exists w_2 \ldots Q_i w_i M(x, w_1, \ldots, w_i) = 1$$

where $|w_1, \ldots, w_i| \leq C|x|^C$

in a nutshell

Σ_i^p higher analog of *NP*

Π_i^p higher analog of *coNP*

PH

observation for all i

$$\Pi_i^p \subseteq \Pi_{i+1}^p \cap \Sigma_{i+1}^p \supseteq \Sigma_i^p$$

definition **(+claim)**

$$PH = \bigcup_i \Sigma_i^p = \bigcup_i \Pi_i^p$$

collapses

theorem for all i

$$\Sigma_i^p = \Sigma_{i+1}^p \Rightarrow PH = \Sigma_{i+1}^p$$

$$\Sigma_i^p = \Pi_i^p \Rightarrow PH = \Sigma_i^p$$

if $\Sigma_1^p = \Pi_1^p$ then $\Sigma_2^p = \Sigma_1^p$

for $L \in \Sigma_2^p$ there is M such that[1]

$$x \in L \Leftrightarrow \exists w_1 \forall w_2 M(x, w_1, w_2) = 1$$

[1] running times and lengths of witnesses are poly

if $\Sigma_1^p = \Pi_1^p$ then $\Sigma_2^p = \Sigma_1^p$

for $L \in \Sigma_2^p$ there is M such that[1]

$$x \in L \Leftrightarrow \exists w_1 \forall w_2 M(x, w_1, w_2) = 1$$

$$\Rightarrow \quad L_* := \{(x, w_1) : \forall w_2 \; M(x, w_1, w_2) = 1\} \in \Pi_1^p = \Sigma_1^p$$

[1] running times and lengths of witnesses are poly

if $\Sigma_1^p = \Pi_1^p$ then $\Sigma_2^p = \Sigma_1^p$

for $L \in \Sigma_2^p$ there is M such that[1]

$$x \in L \Leftrightarrow \exists w_1 \forall w_2 M(x, w_1, w_2) = 1$$

$$\Rightarrow \quad L_* := \{(x, w_1) : \forall w_2 \ M(x, w_1, w_2) = 1\} \in \Pi_1^p = \Sigma_1^p$$

$\Rightarrow$ there is M_* such that $(x, w_1) \in L_* \Leftrightarrow \exists w_* M_*(x, w_1, w_*) = 1$

[1] running times and lengths of witnesses are poly

if $\Sigma_1^p = \Pi_1^p$ then $\Sigma_2^p = \Sigma_1^p$

for $L \in \Sigma_2^p$ there is M such that[1]

$$x \in L \Leftrightarrow \exists w_1 \forall w_2 M(x, w_1, w_2) = 1$$

$\Rightarrow \quad L_* := \{(x, w_1) : \forall w_2 \; M(x, w_1, w_2) = 1\} \in \Pi_1^p = \Sigma_1^p$

$\Rightarrow$ there is M_* such that $(x, w_1) \in L_* \Leftrightarrow \exists w_* M_*(x, w_1, w_*) = 1$

$\Rightarrow \quad L \in \Sigma_1^p$ because $x \in L$ iff $\exists w_1, w_* \; M_*(x, w_1, w_*) = 1$

---

[1] running times and lengths of witnesses are poly

if $\Sigma_1^p = \Pi_1^p$ then $\Sigma_2^p = \Sigma_1^p$

for $L \in \Sigma_2^p$ there is M such that[1]

$$x \in L \Leftrightarrow \exists w_1 \forall w_2 M(x, w_1, w_2) = 1$$

$\Rightarrow \quad L_* := \{(x, w_1) : \forall w_2 \ M(x, w_1, w_2) = 1\} \in \Pi_1^p = \Sigma_1^p$

$\Rightarrow$ there is M_* such that $(x, w_1) \in L_* \Leftrightarrow \exists w_* M_*(x, w_1, w_*) = 1$

$\Rightarrow \quad L \in \Sigma_1^p$ because $x \in L$ iff $\exists w_1, w_* \ M_*(x, w_1, w_*) = 1$

$\Rightarrow \quad \Sigma_2^p \subseteq \Sigma_1^p$

---

[1] running times and lengths of witnesses are poly

collapses: high level

if $\forall\exists\forall\varphi$ can be replaced by $\exists\forall\exists\psi$ then

$$\exists\forall\exists\forall\exists\forall\varphi = \exists\forall\exists(\forall\exists\forall\varphi) \to \exists\forall\exists(\exists\forall\exists\psi) = \exists\forall\exists\forall\exists\psi$$

completeness

theorem

for all i the language Σ_i-SAT of all true TQBF of the form[2] $\exists x_1 \forall x_2 \ldots Q_i x_i \varphi$ is Σ_i^p-complete

remarks

—poly-time (and log-space) reductions

—similarly for Π_i^p

[2] here $x_1, \ldots, x_i$ are vectors

completeness for PH

theorem

if PH has a complete problem then PH collapses

completeness for PH

theorem

if PH has a complete problem then PH collapses

idea

if L is PH-complete then $L \in \Sigma_i^p$ for some i ...

PSPACE

corollary

if PH = PSPACE then PH collapses

PSPACE

corollary

if PH = PSPACE then PH collapses

proof

if PH = PSPACE then TQBF is PH-complete

oracles: alternative definition

a class of functions $\mathcal{O}$

denote by $NP^{\mathcal{O}}$ the collection of languages that can be decided by poly-time NTM with oracle access to some $O \in \mathcal{O}$

can define Σ_2^p as $NP^{NP} = NP^{SAT}$ ...

counting

a set A

decision: is A empty

counting: $|A| =?$

counting problems

$\#$*SAT* number of satisfying assumptions of CNF formula

$\#$*BIPARTITE-PM* number of perfect matchings in bipartite graph

$\#$*SPAN-TREE* number of spanning trees in graph

counting classes

poly-time TM M input (x, y) so that $|y| = p(|x|)$ for polynomial p

define $\#_M : \{0,1\}^* \to \mathbb{N}$ as

$$\#_M(x) = \big|\{y : M(x,y) = 1\}\big|$$

the class $\#P$ comprises all such functions[3]

[3] not decision

counting is powerful

P, NP, $coNP$ are all contained in $P^{\#P}$

counting is powerful

P, NP, $coNP$ are all contained in $P^{\#P}$

theorem **[Toda]**

$$PH \subseteq P^{\#P}$$

counting is powerful

P, NP, $coNP$ are all contained in $P^{\#P}$

theorem **[Toda]**

$$PH \subseteq P^{\#P}$$

ideas

—randomized reduction from TQBF to $\oplus SAT$

—reduction from $\oplus SAT$ to $\# SAT$

counting versus decision

BIPARTITE-PM is in *P*

#*BIPARTITE-PM* is ?

counting versus decision

BIPARTITE-PM is in *P*

$\#$*BIPARTITE-PM* is ?

theorem **[Valiant]**

$\#$*BIPARTITE-PM* is $\#$*P*-complete

ideas

—reduce $\#$*SAT* to integer permanent

—reduce integer permanent to zero-one permanent

permanent versus determinant

$\#$*BIPARTITE-PM* is

$$perm(A) = \sum_{\pi} \prod_{i} A_{i,\pi(i)}$$

permanent versus determinant

$\#$*BIPARTITE-PM* is

$$perm(A) = \sum_{\pi} \prod_{i} A_{i,\pi(i)}$$

similar to

$$det(A) = \sum_{\pi} sign(\pi) \prod_{i} A_{i,\pi(i)}$$

DET in poly-time but PERM is probably not

summary

alternating classes

polynomial hierarchy

counting classes

perm versus det