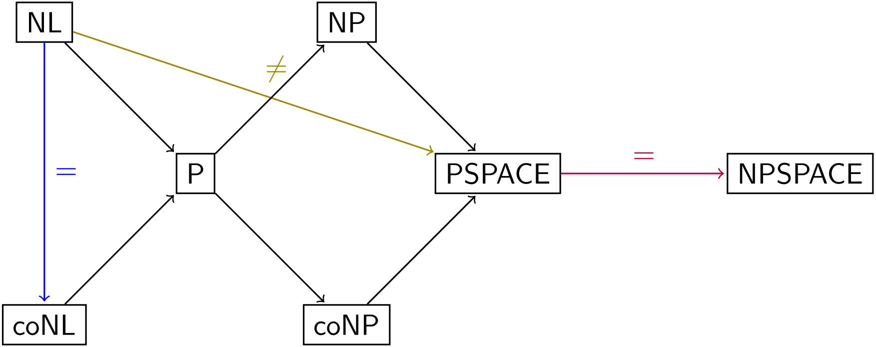
Advanced Complexity : Fundamentals

Marius

October 2021

A brief overview



Immerman-Szelepscényi theorem

Strict hierarchy theorem

Savitch theorem

Definitions

Fonction propre

Fonction croissante et calculable en temps $\mathcal{O}(n + f(n))$ et en espace $\mathcal{O}(f(n))$.

Machine alternantes

L'espace des états finaux est partitionné entre *existentiel* et *universel*
Une machine accepte un mot depuis un état existentiel s'il existe une exécution acceptante
Une machine accepte un mot depuis un état universer si toute exécution accepte.

Intuition

Une machine alternante peut-ête vue comme un jeu à deux joueurs.
Un mot est accepté ssi le joueur existentiel dispose d'une stratégie gagnante.

C-complete problems

A few complete-problems

$REACH$ is **NL**-complete
QBF is **PSPACE**-complete
$HORN - SAT$ is **P**-complete
$CIRCUIT\ VALUE$ is **P**-complete
$MONOTONE\ CIRCUIT\ VALUE$ is **P**-complete

Reminders

A *Horn clause* contains at most one positive literal.
A *Circuit value* is a DAG labelled with $\wedge, \vee, \overline{\wedge}, \overline{\vee}$
A *Monoton circuit value* is a DAG labelled with $\wedge, \vee$

Usual classes of complexity : Major theorems

Savitch theorem

For any proper function $f > \log$, $\mathbf{NSPACE}(f(n)) \subseteq \mathbf{SPACE}(f^2(n))$

Immerman-Szelepscényi theorem

$REACH$ is **coNL**

Corollaries (more important)

$\mathbf{NPSPACE} = \mathbf{PSPACE}$

$\mathbf{NL} = \mathbf{coNL}$

Relation between TM and ATM

A few results

$\mathbf{AP} = \mathbf{PSPACE}$ (Chandra-Kozen-Stockmeyer I)
$\mathbf{AL} = \mathbf{P}$ (Chandra-Kozen-Stockmeyer II)
$\mathbf{APSPACE} = \mathbf{EXPTIME}$

Corollaries (more important)

Le temps alternant, c'est de l'espace !
L'espace alternant, c'est du temps exponentiel !

Polynomial hierarchy

Σ_n^p and $\prod_n^p$

$\Sigma_0^p = \prod_0^p = \mathbf{P}$
Σ_{n+1}^p la classe des langages $L = \{x | \exists y \in A*$ de taille $p(n), x \# y \in L\}$
$\prod_{n+1}^p$ la classe des langages $L = \{x | \forall y \in A*$ de taille $p(n), x \# y \in L\}$

Advanced Complexity : Probabilistic classes of complexity

Marius

October 2021

Randomized TM

Randomized TM

A TM augmented with a random tape on read-only and never read twice.

RP

A language L is in **RP** if there is a polynomial RTM such that :

- If $x \in L$ then $\mathbb{P}(M(x,r)\ accepts) > \frac{1}{2}$
- Otherwise the machine always rejects.

A language L is in **co-RP** if $L^c \in \mathbf{RP}$

RP : A few remarks

$PRIMALITY$ is in $co-RP$ (Miller-Rabbin)

$\forall \epsilon \in]0,1[, \mathbf{RP} = \mathbf{RP}(\epsilon)$

$\rightarrow$ Simulate (x,r) for various r and answer the disjunction.

Better : $\forall q(n), \mathbf{RP} = \mathbf{RP}(2^{-q(n)})$

P $\subseteq$ **RP** $\subseteq$ **NP**

Zero Probability of error Polynomial-time

ZPP

ZPP$=$ **RP** $\cap$ **co-RP**

ZPP also languages decidable in average polynomial time with $\mathbb{P}(M\ errs) = 0$.

Bounded Probability of error Polynomial time

BPP

A language L is in **BPP** if there is a polynomial RTM such that :

- If $x \in L$ then $\mathbb{P}(M(x,r)\ accepts) > \frac{2}{3}$
- Otherwise $\mathbb{P}(M(x,r)\ accepts) < \frac{1}{3}$

BPP

It would have been good to have an example :)

$\mathbf{BBP} = \mathbf{co} - \mathbf{BPP}$

$\forall \epsilon \in]0, \frac{1}{2}[\ \mathbf{BPP} = \mathbf{BPP}(\epsilon)$

$\rightarrow$ Simulate (x, r) for various r and answer the majority.

Better : $\forall q(n), \mathbf{BPP} = \mathbf{BPP}(2^{-q(n)})$

The Sipser-Gàcs-Lautemann Theorem

SGC Theorem

$\mathbf{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p$

A few reminders

$\Sigma_2^p = \exists \cdot \mathbf{coNP} = \exists \cdot \forall \cdot \mathbf{NP}$
$\Pi_2^p = \mathbf{co} - \mathbf{\Sigma_2^p} = \forall \cdot \mathbf{\Sigma_2^p} = \forall \cdot \exists \cdot \forall \cdot \mathbf{NP}$

Proof draft

• $\mathbf{BPP} \subseteq \Sigma_2^p$
Lautemann's trick :
$x \in L$ iif $\{0,1\}^{p(n)}$ coverable by translations of $\{r|M(x,r)accepts\}$
This means $x \in L$ if and only if $\exists t_1..t_n \forall r$, one of the $M(x, r + t_i)$ accepts
Hence the result.
• $\mathbf{BPP} \subseteq \Pi_2^p$
This is a direct consequence of $\mathbf{BPP} = \mathbf{co} - \mathbf{BPP}$

P/Poly

Uniform P/Poly

A langage L is in **Uniform P/Poly** if for every $n \in \mathbb{N}$, one can build C_n

- in space $O(\log n)$
- s.t $\forall x$ of size n, $\in L$ iff $C_n[x] = 1$

P/Poly

A langage L is in **P/Poly** if for every $n \in \mathbb{N}$, There is a circuit C_n

- of polynomial size in n
- s.t $\forall x$ of size n, $\in L$ iff $C_n[x] = 1$

The circuits does not need to be actually buildable anymore.

Two remarks

P=Uniform P/Poly

There are **undecidable problems** in **P/Poly**.

Adleman's Theorem

Adleman's Theorem

BPP $\subseteq$ P/Poly

Proof Draft

$L \in \mathbf{P/Poly}$ iff $\exists$ $\mathcal{M}$ and $(w_n)_{n \in \mathbb{N}}$ s.t

- advice strings w_n are of polynomial sizes
- $\forall x$ of size n, $x \in L$ iff $\mathcal{M}(x, w_n)$ accepts

First, we prove that there exists r_n such that $\mathcal{M}(x, r_n)$ always returns the correct answer

Then, we use r_n as advice strings.

Karp-Lipton Theorems

Karp-Lipton Theorems

I. If **NP** $\subseteq$ **P/Poly**, **PH** collapses at level 2.
II. If **NP** $\subseteq$ **P/Poly**, **PH** $\subseteq$ **P/Poly**

Reminders

PH collapsing at level 2 means that $\Sigma_2^p = \Pi_2^p = ...$
By properties of the **co** operator, it is equivalent to $\Sigma_2^p \subseteq \Pi_2^p$
Using Adleman's theorem, **NP** $\subseteq$ **BPP** would be a sufficient condition.

Arthur-Merlin Games (I)

AM

L is in **AM** iff

$\forall g, \exists$ poly-time $\mathcal{A}$, Merlin map M with poly size outputs and $D \in$ **P** s.t

- if $x \in L$, $\mathbb{P}(x\#\mathcal{A}(x,r)\#r\#M(x\#q\#r) \in \mathbf{D}) \leq 1 - \frac{1}{2^{g(n)}}$
- if $x \notin L$, then $\forall M', \mathbb{P}(x\#\mathcal{A}(x,r)\#r\#M'(x\#q\#r) \in \mathbf{D}) \leq \frac{1}{2^{g(n)}}$

Intuition

Arthur asks a question to Merlin depending on x and r.
Merlin tries to convince Arthur that $x \in L$ with a polynomial answer.
Finally, a polynomial referee must decide wether Merlin was convincing with exponentially low-error.

Arthur-Merlin Games : A few results

We can define different classes depending on how many times Arthur and Merlin can interact and the order.

$\epsilon = \mathbf{P}$

$\mathbf{A} = \mathbf{BPP}$

$\mathbf{M} = \mathbf{NP}$

MA,**AM**...

IP

L is in **IP** iff

$\forall g, \exists$ poly-time $\mathcal{A}$, Merlin map with poly size outputs M and $D \in$ **P** s.t

- if $x \in L$, $\mathbb{P}(x\#\mathcal{A}(x,r)\#r\#M(x\#q) \in \mathbf{D}) \leq 1 - \frac{1}{2^{g(n)}}$
- if $x \notin L$, then $\forall M', \mathbb{P}(x\#\mathcal{A}(x,r)\#r\#M'(x\#q) \in \mathbf{D}) \leq \frac{1}{2^{g(n)}}$

Intuition

We proceed in the same fashion as before but Merlin does not have access to the random tape r anymore.

Note that Arthur can still send r as part of the question, hence **AM** $\subseteq$ **IP**

The Graph Isomorphism Problem

GI

D : Two graphs G and G'

Q : Are they isomorphic ?

GNI = coGI $\in \mathbf{IP}$

BP operator

BP·$\mathcal{C}$

As a generalisation of **BPP**, we define **BP**·$\mathcal{C}$
A language L is in **BP**·$\mathcal{C}$ if there is a $\mathcal{C}$ RTM such that
$\mathbb{P}(M(x,r)\ errs) < \frac{1}{3}$

If $\mathcal{C}$ is closed under $\{w_1\#...\#w_k|$a majority of w_i is in $L\}$,
we may replace $\frac{1}{3}$ with $\frac{1}{2^{g(n)}}$ for any polynom g

Main interest

BPP.NP=**AM**

Intuition

$\supseteq$ The NDTM guess the random tape and the answer of Merlin
$\subseteq$ If the NDTM has found a certificate, so can Merlin

MA as expectation/maximizer

Intuition

MA $\subseteq$ **AM**...

...but the proof uses expectation maximizer X)