LABORATOIRE DE RECHERCHE EN INFORMATIQUE

Algorithmes Complexité

Cours 2-11
Master MPRI

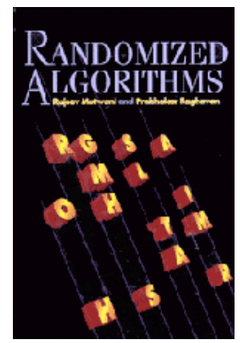
2-11-1 (24h) Algorithmique avancée et complexité

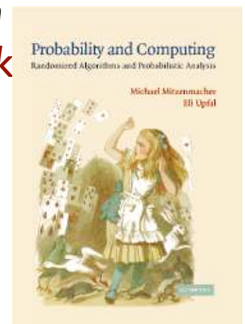
Michel de Rougemont
Adi Rosen

2-11-2 (24h) Information quantique et applications

Iordanis Kerenidis
Miklos Santha

Partie 1. Vérification probabiliste

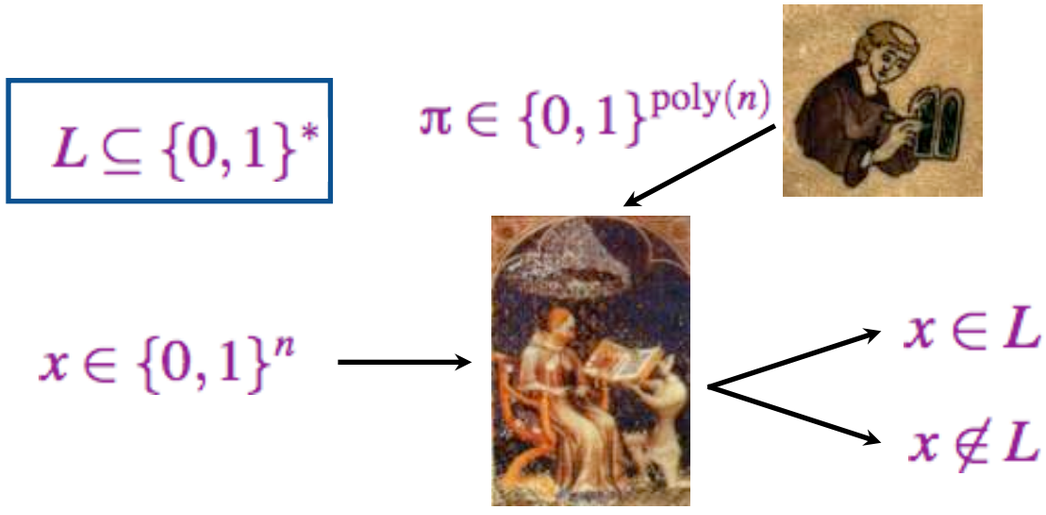




- Pourquoi probabilistes ?

  "For many applications, a randomized algorithm is the simplest algorithm available, or the fastest, or both."
  "Randomization and probabilistic techniques play an important role in modern computer science, with applications ranging from combinatorial optimization and machine learning to communication network and secure protocols."

- Un exemple : différentes preuves, différents langages



Bits lus / Vérificateur	polynomial	constant
Déterministe	$L \in NP$	
Probabiliste	$L \in MA$	$L \in P$

$L \in NP$

Théorème PCP (Godel prize 2001): Chaque énoncé de NP admet une preuve vérifiable de manière probabiliste, telle que la preuve peut être localement vérifiée en n'en observant qu'un nombre constant de bits.

Partie 2. Algorithmes en ligne

- Why online?

  We have to take decisions without knowing the future (calls for taxis; exchange rates; downloads of files)
  Nevertheless we want to have algorithms that have low costs
  We compare the cost of the online algorithm to the cost of the utopian algorithm that knows the future.

- Example: Two servers on the line

  Two servers p,q travel on the line ; requests are points on the line ; one of p or q must immediately move to the request. cost - total distance travelled

Greedy (= move the closest server) is bad

Cover: Move the servers at the same distance towards the request -

The cost of Cover is at most twice the optimal (i.e. the cost if we know the future)

Dates

- Cours + examen(s) : 14/09 - 06/11

Plan (8 cours)

- Probabilistic verification

  Probabilistic Verification: IP and MIP, Protocol for the permanent and QBF, IP=PSPACE.

  PCP model, Holographic proofs. NP= PCP(n^3, 1), Non approximability of Maxclique and Maxsat,

  NP= PCP(log n, 1), Key lemmas and Proof of the PCP theorem

  Property Testing: graphs, trees and words: regular properties are testable.

- Online algorithms

  Motivation and introduction

  Paging (cache replacement)

  The k-server problem

  Search problems: "the cow problem"; Navigation in unknown terrain

  Metrical task systems

  The power of randomness: relative power of adversaries versus randomized online algorithms

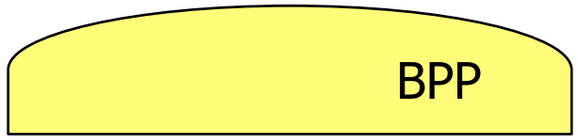
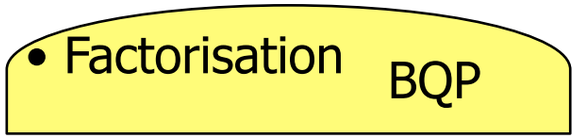
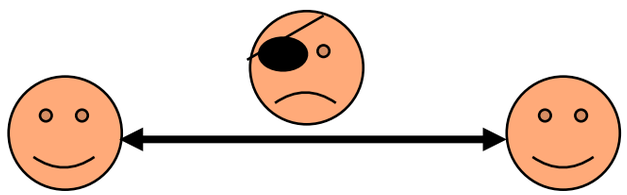
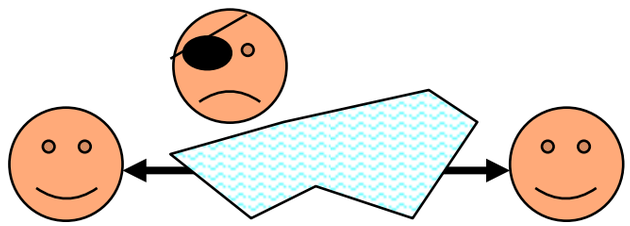
  Online load balancing algorithms

  Online algorithms in communication networks

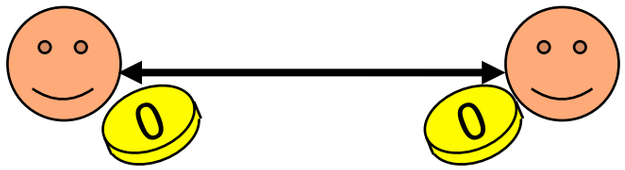
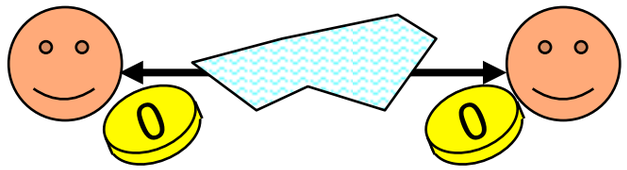
Dates

- Cours + examen(s) : 14/09 - 06/11

Contenu

Informatique actuelle classique	**Informatique utilisant la mécanique quantique**
Complexité calculatoire	
On pense que • 3SAT • Factorisation 	On pense (sait) que • 3SAT • Factorisation 
Cryptographie	
 La sécurité de la distribution de clés repose sur une hypothèse de complexité	 La sécurité de la distribution de clés repose sur un axiome physique

Contrairement aux ordinateurs quantiques, la cryptographie quantique existe déjà !

Recherche non structurée dans N éléments	
Demande $\Theta(N)$ accès	Demande $\Theta(\sqrt{N})$ accès
Communication	
Egalité: O(N) sans aléa partagé	O(log N) sans aléa partagé
DISJ : N	$\sqrt{N}$
Tirer à pile ou face	
	
impossible (ou repose sur une hypothèse de complexité)	Possible avec un biais de ¼

etc...