ALGORITHME ET PROGRAMMATION
CIRM - 2 au 6 mai 2016
F. Dorra & L. Albert

Lundi 2 mai

10h30. F. Dorra & L. Albert : *Bienvenue à tous*

10h45. Emeric Tourniaire : *Internet, comment ça marche ?*

Internet est le plus vaste réseau d'information au monde, utilisé par plus de trois milliards d'utilisateurs. Ce réseau est en évolution permanente, à la fois dans son fonctionnement et dans ses utilisations ; c'est également un sujet de conflits politiques (neutralité du réseau, protection de la vie privée, liberté d'expression, etc.). L'objectif de cet exposé est de présenter les aspects techniques d'Internet, de se familiariser avec quelques acronymes (TCP, HTTP, DNS) et de découvrir, en bref, comment ça marche. Dans une deuxième partie, nous parlerons de fiabilité du réseau, d'attaques possibles, et de comment ça ne marche pas.

14h. Gilles Dowek : *Calculabilité, réécriture, lambda-calcul, automates cellulaires, ... comment s'abstraire d'un langage de programmation particulier ?*

15h30. Stéphane Gonnord **:** *Un record du monde comme défi collectif*

Présentation d'un problème combinatoire pour lequel la solution n'est connue que jusqu'à n=12. Avec la mise en commun des idées, des connaissances de l'assistance... et quelques centaines d'ordis, le but sera de décrocher la timbale !

Mardi 3 mai

9h. Olivier Bournez : *Calculer avec des modèles où le temps est continu.*

Quelle est la puissance des machines de calculs analogiques (vs digitales)? Que peut-on calculer avec des équations différentielles? Que cela nous apprend-t'il sur la physique et ses modèles de notre monde physique?

10h45. Frédéric Vivien : *Algorithmes d'approximation (1)*

De nombreux problèmes d'optimisation sont NP-complets. Nous ne connaissons pas de problème NP-complet qui admette un algorithme optimal de résolution s'exécutant en temps polynomial en la taille de l'instance (sinon P=NP serait établi), et l'intuition commune est que P =/= NP. Pour ces problèmes, la recherche de solutions optimales peut donc être prohibitive. Les algorithmes d'approximation offrent un compromis intéressant: par définition, ils s'exécutent en temps polynomial et fournissent des solutions dont la qualité est garantie. Nous introduirons la notion d'algorithme d'approximation et de schéma d'approximation en temps polynomial, et nous illustrerons ces notions sur de nombreux exemples. Nous montrerons également comment établir qu'un problème n'admet pas d'algorithme d'approximation (à

moins que P=NP), ou comment établir une borne inférieure au facteur d'approximation de tout algorithme d'approximation (sauf si P=NP).

14h. Frédéric Vivien : *Algorithmes d'approximation (2)*

Dans la deuxième partie de ce cours nous considérerons un problème lié, celui des algorithmes compétitifs. Dans le cadre de l'algorithmique « en-ligne », les caractéristiques d'une instance d'un problème ne sont découvertes qu'au fur et à mesure du traitement de l'instance (comme on ne découvre l'histoire d'un livre qu'au fur et à mesure où on en lit des pages). Ne pas connaître à l'avance toutes les caractéristiques d'une instance interdit souvent - mais pas toujours - de construire un algorithme optimal. Nous montrerons, entre autres, comment utiliser la technique de l'adversaire pour établir une borne inférieure au facteur de compétitivité de tout algorithme en-ligne (cette fois-ci en dehors de toute notion de complexité).

15h30. Yann Salmon // François Boisson

Yann Salmon : *Quel Caml pour l'option informatique ?*

Nous avons tourné le dos à Pascal en 2013, mais les documents officiels restent à la fois contraignants (Caml Light imposé) et flous (aucune indication sur le fragment à étudier). J'explorerai l'intérêt pédagogique et pratique de faire le cours avec OCaml et l'importance de choisir un langage vivant pour développer les inscriptions en option informatique, puis la nécessité d'une évolution réglementaire pour permettre son usage tout en délimitant plus précisément les éléments syntaxiques et de la bibliothèque standard exigibles et autorisés aux concours.

François Boisson : *Buffer Overflow ou explication de «une faille de type bufferoverflow peut permettre à un code malicieux d'être éxécuté»*

Explication de ce qu'est un buffer overflow, de la façon de l'exploiter, des protections possibles et des contournements...

Mercredi 4 mai

9h. Claude Gomez et Jean Sequeira : *Étendre le logiciel Scilab. Exemple en traitement d'images.*

Lorsque l'on utilise un logiciel de calcul numérique comme Scilab, on a souvent besoin de créer ses propres fonctions. Mais parfois il faut faire plus comme créer une application complète ou lier à Scilab des programmes écrits dans un autre langage. Nous allons montrer comment le faire et nous donnerons comme exemple un programme de traitement d'images écrit en C++.

10h45. Jean Sequeira : *Mathématiques "anciennes" pour l'imagerie numérique*

Quelques domaines des mathématiques ne sont plus enseignés en classes préparatoires car ils sont moins prioritaires que d'autres. Pourtant, ils ont fait l'objet d'un regain d'intérêt, au point de devenir parfois incontournables, avec l'émergence de l'imagerie numérique (représentation de l'image dans l'ordinateur), que ce soit en matière de visualisation, d'analyse d'images ou de modélisation géométrique. Dans cette présentation, il sera fait essentiellement référence à la pertinence de leur

utilisation, et nous en donnerons quelques exemples à travers l'apport des espaces projectifs et des quaternions en imagerie.

14h. Sylvie Bonnet , Luc Bougé : *Table Ronde*

L'informatique en CPGE. Les concours. La nouvelle épreuve de Tipe. L'informatique au Capes. Les ENS…

15h30. Ballade aux calanques suivie de la traditionnelle Bouillabaisse…

Jeudi 5 mai

9h. Florent Capelli : *Complexité paramétrée : comprendre finement la difficulté d'un problème.*

Un voyageur souhaite visiter toutes les villes d'un pays. Il voudrait savoir si ce serait possible en parcourant moins de mille kilomètres. Ce problème, dans toute sa généralité, est supposé difficile à résoudre par l'informatique. Cependant, les routes qu'il pourra emprunter n'ont pas été construites au hasard : on peut donc imaginer qu'elles reposent sur une structure implicite susceptible d'être exploitée pour une résolution plus rapide. Le but de la complexité paramétrée est de fournir les outils qui permettront de repérer lesquelles parmi celles-ci ne seront d'aucune utilité. Dans cette présentation, je reviendrai sur la théorie de la NP-complétude qui explique la difficulté de nombreux problèmes dans toute leur généralité. Je montrerai ensuite des exemples où la structure sous-jacente de l'entrée permet d'accélérer significativement le calcul. Enfin, nous verrons comment la théorie de la complexité paramétrée peut aider à comprendre finement où réside la difficulté du problème.

10h45. Richard Lassaigne : *La méthode des poids multiplicatifs: un méta-algorithme d'approximation pour l'apprentissage et l'optimisation*

Il s'agit de la version unifiée d'une méthode probabiliste utilisée pour l'approximation dans des domaines aussi divers que l'apprentissage automatique, la théorie des jeux, l'optimisation linéaire,...
En outre, cette méthode, qui a un intérêt pédagogique certain, commence à être présente dans la plupart des cours d'algorithmique.

14h. Luc Bougé : *Big Data: Large Challenges, Great Solutions*

L'apparition des "Big Data" est en train de modifier profondément notre compréhension du traitement algorithmique de l'information. Le centre de gravité s'est déplacé du calcul vers les données, et le passage à l'échelle est devenu une notion centrale. En particulier, la prise en compte de la localisation géographique des données, du coût de leur déplacement et de leur disponibilité sont devenus des facteurs majeurs de la conception des applications.
Cette nouvelle vision "centrée sur les données" et "consciente de l'échelle" (data-centric, scaling-aware) renouvelle complètement la problématique de l'algorithmique et de la programmation, à la fois dans les outils théoriques utilisés et aussi dans les méthodologies pratiques mises en oeuvre. Cet exposé présentera quelques-uns des aspects ainsi touchés et proposera des pistes pour adapter l'enseignement de l'informatique à ce nouveau paysage.

Vendredi 6 mai

9h. Patrice Séébold : *Quelques questions à propos de palindromes.*

De récents résultats sur les palindromes ont suscité de nouvelles questions que j'aborderai dans cet exposé avec des pistes de solutions. Je ferai aussi un état des lieux sur un problème ancien et difficile.

10h45. Judicaël Courant : *Application de la complexité en cryptographie.*

Je présenterai rapidement la notion de cryptographie à clé publique, puis je montrerai comment les questions de sécurité de ces outils cryptographiques peuvent être modélisées par des notions de complexité de programmes. Nous verrons pourquoi il est nécessaire de faire intervenir des probabilités. Enfin, j'expliquerai comment on peut concrètement montrer une propriété de sécurité (la sécurité sémantique) d'un système de chiffrement (ElGamal).

* Si vous n'avez jamais entendu parler de cryptographie, venez : l'exposé devrait être accessible à tous ceux qui savent ce qu'est la complexité d'un programme !

* Si vous avez entendu parler de cryptographie et que vous pensez que RSA est sûr parce qu'on ne sait pas factoriser efficacement de grands entiers, vous devriez venir : j'ai mis de nombreuses années avant de réaliser que c'était aussi absurde que dire «Socrate est mortel parce qu'il est humain». J'espère remettre en cause vos certitudes et vous aider à gagner du temps !