SCI6373 Programmation documentaire

Cours 15

Été 2025

Plan

- Retour sur les TP (fait au C14)
- Retour sur le cours et l'informatique en général
- C'est bien beau l'IA, mais…
- Modèles de calcul : permettent d'étudier…
  - Difficulté inhérente de certains problèmes
  - Limites du calcul

Modèles de calcul

- But: pouvoir faire des réflexions et des raisonnements "généraux", indépendants de modèles spécifiques d'ordinateur et de langages de programmation spécifiques
- Utilité: démontrer…
  - …l'optimalité de certains algorithmes
  - …les limites du calcul

Modèles de calcul

- Précurseur: Alan Turing (1912-1954)
  - Connu pour travaux sur "The enigma"
  - Définit une "machine" abstraite: "Machine de Turing"
  - Construit une machine "universelle"
  - Démontre que certaines fonctions ne sont pas calculables

Alan Turing (1912-1954)

- http://www.turing.org.uk/

- Précurseur dans plusieurs domaines
  - Intelligence artificielle
  - "Turing test" (CAPTCHA)

Modèles de calcul

- Turing démontre aussi l'équivalence entre sa machine et le formalisme des "fonctions récursives" d'Alonzo Church (1903-1995)
- Avec Church, il formule la fameuse "thèse de Church-Turing" sur la calculabilité (1936)

Modèles de calcul

- Autres formalismes:
  - Automates
  - Grammaires génératives
  - Résultat de Noam Chomsky
- Modèles de calcul parallèle
  - Automates cellulaires (von Neumann, 1903-1957)
  - Circuits booléens

Modèles de calcul

- Applications:
  - Bornes inférieures sur le temps de calcul
    - "Complexité" d'un problème
    - Cryptographie à clé publique (RSA)
  - Nouvelles approches pour le parallélisme
  - Exploitation de l'aléatoire (probabilisme)
  - Efficience énergétique
  - etc.

Modèles de calcul

- Question fondamentale (encore ouverte)

  P =? NP

- Derniers développements:
  - Informatique quantique
    - Basée sur les propriétés quantiques de la matière
    - Nature probabiliste du comportement de la matière
    - Parallélisme théoriquement illimité
    - Algorithmique quantique
    - Cryptographie quantique

Modèles de calcul

- RSA (Rivest, Shamir, Adelman, 1970)
  - Sécurité basée sur la difficulté de décomposer un grand entier en facteurs
  - ACM Turing Award 2002
  - Aucune démonstration mathématique de la sécurité
  - Compromis par les approches quantiques