

La Dernière Séance

Collège de France, 28 mars 2008

Séminaire : [Jacques Stern](#) (ENS et INGENICO)

Cours : [Gérard Berry](#)

Chaire d'innovation technologique Liliane Bettencourt
Gerard.Berry@college-de-france.fr

Rappel : les quatre piliers du numérique

1. L'idée de numérisation de l'information
2. Le prodigieux essor de la machine à information
3. La science et la technologie de son usage
4. Un espace d'innovation exceptionnel

Rappel : les quatre piliers du numérique

1. L'idée de numérisation de l'information
2. Le prodigieux essor de la machine à information
3. La science et la technologie de son usage
4. Un espace d'innovation exceptionnel

Principe du cours :

*leçon de choses sur les fondements
enabling sciences and technologies*

Rappel : les quatre piliers du numérique

1. L'idée de numérisation de l'information
2. Le prodigieux essor de la machine à information
3. La science et la technologie de son usage
4. Un espace d'innovation exceptionnel

Principe du cours :

*leçon de choses sur les fondements
enabling sciences and technologies*



y a-t-il un mot français aussi bon?

Sujets traités

1. Algorithmes
2. Circuits
3. Langages de programmation
4. Systèmes embarqués
5. Vérification de programmes
6. Réseaux
7. Images
8. Cryptologie

Pas traités : matériels du futur

- Disques tournants ou mémoire permanentes ?
combat au couteau !
- Spintronique => nouvelles mémoires (MRAM)
pourrait remplacer DRAM, SRAM, Flash ?
ou bien encore d'autres technologies?
- Optique ? Nanofibres ? Mémoires moléculaires ?
- Méga-calculateurs ou méga-réseaux de PC ?
qui consomme le plus d'énergie ?
utiliser les PC qui ne font presque rien pour la plupart ?
- Quantique (???)

Peu traitée : la science sous-jacente

- Théorie de l'information
- Algorithmique, complexité
- Modèles de calcul, calculabilité, logique
- Théorie de la programmation
- Modèles du parallélisme et de la communication
cf. S. Dehaene pour le cerveau, *Les neurones de la lecture*
- Calcul formel
- Géométrie algorithmique
- ...

Pas traités : infrastructure & applications

- Infrastructure

 - bases de données

 - systèmes d'exploitation

 - tolérance aux pannes

 - interface homme-machine

 - le Web et ses langages (XML, javascript, ...)

- Applications

 - bureautique, travail coopératif (local ou Web?)

 - jeux (autonomes, sur ordi ou en réseau)

 - aide au diagnostic et à la décision (systèmes experts)

- Logiciel libre ou logiciel commercial ?

Peu traité : informatique dans l'industrie

- Gestion, optimisation
- Conception assistée par ordinateur
transports, architecture, design
- Machines numériques, robotique
- Usines numériques
entièrement simulées virtuellement
- Traçabilité de la production et de l'utilisation
RFID

Peu traité : sécurité

- Confidentialité des données
la cryptologie est un élément, mais pas le seul
- Protection contre les virus
- Protection contre les intrusions
plusieurs milliers par an dans l'administration US
- Protection contre les attaques réseaux
éviter la saturation des serveurs
- Tolérance aux bugs résiduels

Cf. colloque du 23 mai

Peu traité : informatique et sciences

- Mécanique numérique
aérodynamique, combustion, crash-tests, ...
- Physique, chimie
géométrie des molécules
simulations, expériences virtuelles
- Biologie
séquençage de l'ADN
fonctionnement de la cellule, du cerveau, etc.
vers la simulation du vivant ?
- Médecine
imagerie, diagnostic, neurosciences
chirurgie, épidémiologie

Peu traité : informatique et sciences

- **Météorologie**
 - observation par satellites et capteurs variés
 - simulation de l'atmosphère et océans
 - simulation du climat
- **Géologie**
 - tomographie terrestre
- **Océanographie**
 - bouées numériques
 - sous-marins autonomes
- **Astronomie**
 - imagerie adaptative
 - modélisation du cosmos

Toumaï - Michel Brunet 27 mars 2008



Moulage original

Toumaï - Michel Brunet 27 mars 2008



Moulage original

Toumaï - Michel Brunet 27 mars 2008



reconstitution numérique, impression 3D

Toumaï - Michel Brunet 27 mars 2008



reconstitution numérique, impression 3D

Toumaï - Michel Brunet 27 mars 2008



reconstitution numérique, impression 3D, sculpture

Pas traité : le langage

- Comprendre les textes écrits
la grammaire, le sens
lire l'écriture manuscrite (même des médecins)
- Savoir les traduire
l'esprit est fort, mais la chair est faible
=> la vodka est forte, mais la viande est pourrie
- Comprendre la parole réelle
avé l'assent, putaing cong, une fois, tabernacle !
- Savoir reconnaître une bonne blague d'une mauvaise

Pas traité : le langage

- Comprendre les textes écrits
 - la grammaire, le sens
 - lire l'écriture manuscrite (même des médecins)
- Savoir les traduire
 - l'esprit est fort, mais la chair est faible
 - => la vodka est forte, mais la viande est pourrie
- Comprendre la parole réelle
 - avé l'assent, putaing cong, une fois, tabernacle !
- Savoir reconnaître une bonne blague d'une mauvaise

Nécessaire pour les interfaces du futur !

Pas traité : la création artistique

- Facile: les 100 000 milliards de poèmes (Queneau)
- Difficile : les effets spéciaux du cinéma
- Mais est-ce un support pour **une nouvelle création** ?

Pas traité : la création artistique

- Facile: les 100 000 milliards de poèmes (Queneau)
- Difficile : les effets spéciaux du cinéma
- Mais est-ce un support pour **une nouvelle création** ?

Allez les internautes !

Pas traité : aspect sociaux

- Les **fractures** : sociales (âge, richesse, compétence), juridiques
- Qu'est ce que **l'identité numérique** ?
- Comment préserver la **vie privée numérique** ?
- Et se défendre contre une **surveillance généralisée** ?
- Vers où vont les **communautés virtuelles** ?
- Quelle confiance dans le **travail communautaire** (Wiki) ?
- Que deviennent **auteur / consommateur / autorité** ?
- Comment lutter **contre rumeurs et calomnies** ?
- Le "libre" a-t-il un vrai **modèle économique** ?
- Le traitement "**religieux**" de sujets techniques mérite-t-il l'intérêt ?
(Mac vs. Windows etc., libre contre commercial, etc.)

Bibliographie?

Bibliographie?

Il va bien falloir écrire un livre....

Questions : matériels

- Pourquoi 0 / 1 et pas 0 / 1 / 2 ou 0 / 1 / 2 / 3 ?
 - beaucoup plus simple en physique (charge + / -, spin up / down, etc)
 - seule base à **unifier les nombres et la logique** (cf. Vuillemin, les 2-adiques)
 - 0 / 1 = la dichotomie, centrale en algorithmique
 - base 2 = base 4 = base 8 ...
 - la base 3 se code en base 2 mieux que l'inverse !

Questions : matériels

- Pourquoi 0 / 1 et pas 0 / 1 / 2 ou 0 / 1 / 2 / 3 ?
 - beaucoup plus simple en physique (charge + / -, spin up / down, etc)
 - seule base à **unifier les nombres et la logique** (cf. Vuillemin, les 2-adiques)
 - 0 / 1 = la dichotomie, centrale en algorithmique
 - base 2 = base 4 = base 8 ...
 - la base 3 se code en base 2 mieux que l'inverse !
- Les circuits ne font-ils vraiment jamais d'erreurs?
 - erreur possible, mais **fiabilité vraiment exceptionnelle**
 - auto test et redondance arbitraire possible
 - calculs reproductibles => proba d'erreur décroissant exponentiellement
 - un exemple : preuve des 4 couleurs (Gonthier)

Questions : matériels

- Pourquoi 0 / 1 et pas 0 / 1 / 2 ou 0 / 1 / 2 / 3 ?
 - beaucoup plus simple en physique (charge + / -, spin up / down, etc)
 - seule base à **unifier les nombres et la logique** (cf. Vuillemin, les 2-adiques)
 - 0 / 1 = la dichotomie, centrale en algorithmique
 - base 2 = base 4 = base 8 ...
 - la base 3 se code en base 2 mieux que l'inverse !
- Les circuits ne font-ils vraiment jamais d'erreurs?
 - erreur possible, mais **fiabilité vraiment exceptionnelle**
 - auto test et redondance arbitraire possible
 - calculs reproductibles => proba d'erreur décroissant exponentiellement
 - un exemple : preuve des 4 couleurs (Gonthier)

Mais la complexité augmente tellement – **qui sait pour le futur ?**

Questions : matériels

- Quid des circuits asynchrones ?
 - idée : supprimer l'horloge globale,
la remplacer par des protocoles locaux
 - objectif : gagner en moyenne, consommer moins
mieux passer à l'échelle
 - mais la CAO et le debug sont trop compliqués....

Questions : matériels

- Quid des circuits asynchrones ?
 - idée : supprimer l'horloge globale,
la remplacer par des protocoles locaux
 - objectif : gagner en moyenne, consommer moins
mieux passer à l'échelle
 - mais la CAO et le debug sont trop compliqués....
- Des techniques asynchrones gagnent le monde synchrone !
circuits multi-horloges, horloges multi-phases
utilisation de latch transparents, vols de cycles
circuits élastiques (Cortadella - Kishinevsky)

Questions : matériels

- Quid des circuits asynchrones ?
 - idée : supprimer l'horloge globale,
la remplacer par des protocoles locaux
 - objectif : gagner en moyenne, consommer moins
mieux passer à l'échelle
 - mais la CAO et le debug sont trop compliqués....
- Des techniques asynchrones gagnent le monde synchrone !
circuits multi-horloges, horloges multi-phases
utilisation de latch transparents, vols de cycles
circuits élastiques (Cortadella - Kishinevsky)

Conserver la CAO synchrone, implémenter plus asynchrone !

Question : équipement

- Y aura-t-il un terme une différence entre un ordinateur, un téléviseur, un téléphone, etc?
 - pour les circuits, certainement
 - pour les logiciels, de plus en plus de commonalité
 - pour les interfaces, vive la simplicité, l'unification, sans oublier l'imagination bien placée !

Questions : loi de Moore

- La loi de Moore va-t-elle s'arrêter?
sans doute, mais si → 2020, on aura 256 G transistors !
saura-t-on quoi en faire ?

Questions : loi de Moore

- La loi de Moore va-t-elle s'arrêter?
sans doute, mais si → 2020, on aura 256 G transistors !
saura-t-on quoi en faire ?
- Toutes les fabs basculent-elles vers l'Asie ?
il en restera peut-être aux USA (pour cause d'indépendance?)

Questions : loi de Moore

- La loi de Moore va-t-elle s'arrêter?
sans doute, mais si → 2020, on aura 256 G transistors !
saura-t-on quoi en faire ?
- Toutes les fabs basculent-elles vers l'Asie ?
il en restera peut-être aux USA (pour cause d'indépendance?)
- Et quid du savoir faire ?
énormes investissements aux USA sur le post-CMOS
Ex: Albany : 2 G\$ Etat de New-York, bien plus du privé
grande université, 100 compagnies industrielles

Questions : loi de Moore

- La loi de Moore va-t-elle s'arrêter?
sans doute, mais si → 2020, on aura 256 G transistors !
saura-t-on quoi en faire ?
- Toutes les fabs basculent-elles vers l'Asie ?
il en restera peut-être aux USA (pour cause d'indépendance?)
- Et quid du savoir faire ?
énormes investissements aux USA sur le post-CMOS
Ex: Albany : 2 G\$ Etat de New-York, bien plus du privé
grande université, 100 compagnies industrielles

=> rapport de l'Académie des technologies à paraître

Questions : son et image

- Quid de l'analogique pour le son et l'image ?
condamné par l'accumulation intrinsèque du bruit
(pas de recopies ad libitum, dégradation par tout traitement)
et par l'absence de compression efficace
mais toujours excellente qualité pour les amateurs !

Questions : son et image

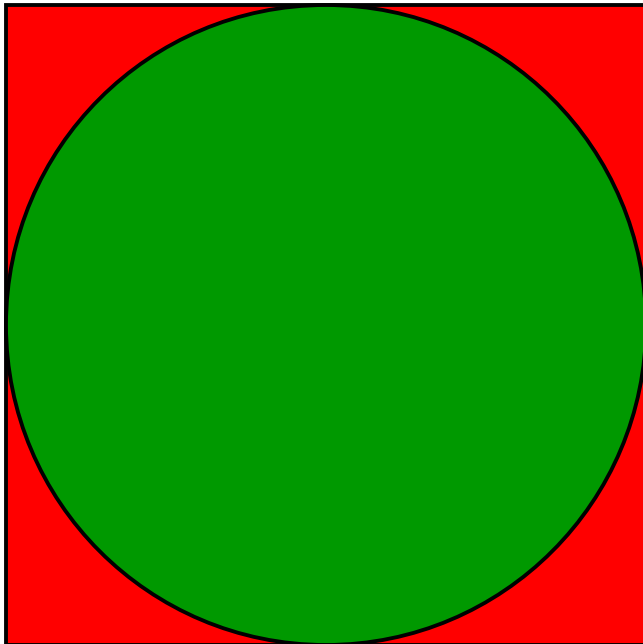
- Quid de l'analogique pour le son et l'image ?
 - condamné par l'accumulation intrinsèque du bruit
 - (pas de recopies ad libitum, dégradation par tout traitement)
 - et par l'absence de compression efficace
 - mais toujours excellente qualité pour les amateurs !
- Une photo corrigée numériquement vaut elle une photo réelle ?
 - le réel n'a jamais existé en photographie !
 - car on ne regarde pas la photo dans son contexte de prise
 - (ex. gamut de couleurs, balance des blancs)
 - le jeu est de donner l'impression que l'on souhaite au spectateur, qui varie beaucoup suivant les photographes...
 - le numérique peut simuler les imperfections de l'argentique
 - ex: DxO Film Pack → Velvia, Ekta, Kodakchrome, etc

Pourquoi l'aléatoire fonctionne-t-il ?

- Il explore efficacement des espaces compliqués
- Il se sort tout seul des minimums locaux
- Shannon: le codage aléatoire est théoriquement optimal
(sauf qu'on ne sait pas le décoder vite)

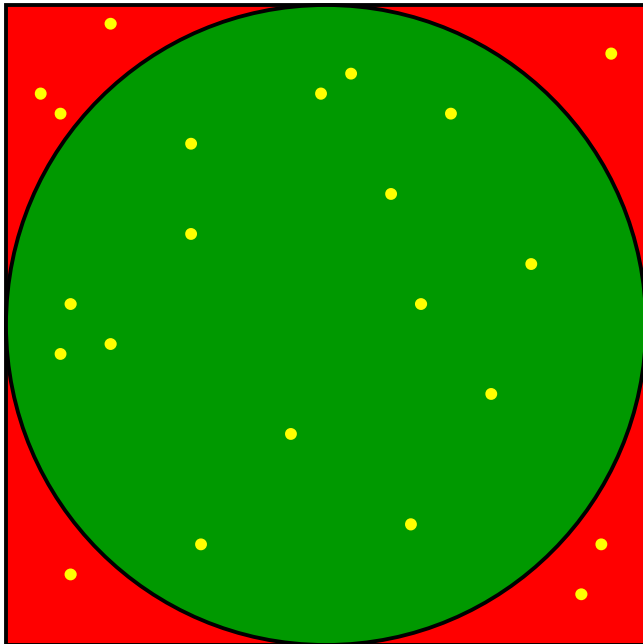
Pourquoi l'aléatoire fonctionne-t-il ?

- Il explore efficacement des espaces compliqués
- Il se sort tout seul des minimums locaux
- Shannon: le codage aléatoire est théoriquement optimal
(sauf qu'on ne sait pas le décoder vite)



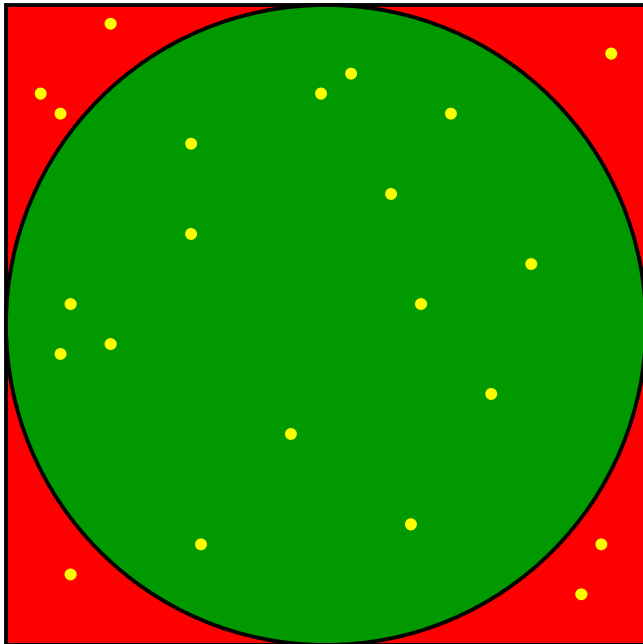
Pourquoi l'aléatoire fonctionne-t-il ?

- Il explore efficacement des espaces compliqués
- Il se sort tout seul des minimums locaux
- Shannon: le codage aléatoire est théoriquement optimal
(sauf qu'on ne sait pas le décoder vite)



Pourquoi l'aléatoire fonctionne-t-il ?

- Il explore efficacement des espaces compliqués
- Il se sort tout seul des minimums locaux
- Shannon: le codage aléatoire est théoriquement optimal
(sauf qu'on ne sait pas le décoder vite)



$$V / (V+R) \sim \pi / 4$$

Question : Préservation des données

- Comment conserver les données de façon fiable ?
 1. ne pas faire confiance aux supports uniques
 2. ni aux supports peu pérennes (CD, DVD gravés)
 3. répliquer et disperser
 4. avenir : fermes d'archivage réparties ?

Question : Préservation des données

- Comment conserver les données de façon fiable ?
 1. ne pas faire confiance aux supports uniques
 2. ni aux supports peu pérennes (CD, DVD gravés)
 3. répliquer et disperser
 4. avenir : fermes d'archivage réparties ?
- Comment numériser les archives ?
 - Numérisation des livres par Google
 - Et par la Bibliothèque de France (Gallica)
 - d'abord en scan image basse résolution.....
 - Numérisation et stockage à long terme des images médicales



élégants, où, tout en prenant les anti-anémiques à la mode, on passe en revue tous les petits potins du jour, on s'imprègne de toutes les médisances et calomnies qui sont dans l'air. Ou bien M^{me} Lacombe s'en allait un peu bourricoter, tâcher de mettre à flot son budget trop souvent chargé d'excédents de dépenses, par quelques bénéfices réalisés à la Bourse. L'agente de change qui la guidait se trompait souvent et le budget de ménage s'équilibrait à grand'peine. M. Lacombe n'avait pour tout revenu que ses appointements, 35,000 francs et le logement, juste de quoi vivoter à la campagne, en se contraignant à une sévère économie. Dure nécessité, d'autant plus que M^{me} Lacombe aimait aussi à magasiner, et qu'au lieu de se faire montrer par Télé, sans se déranger, les étoffes ou les confections dont elle et sa fille pouvaient avoir besoin, elle préférait courir les grands magasins de Paris et vite filer on tube ou en vélocé aérien pour la moindre occasion, pour une idée de ruban qui lui passait par la tête. Cette modeste situa-

LAUTERBRUNNER-STATION.

2555*1443 = 3.5 Mpixels

moins qu'un APN
bas de gamme...

Les forces du marché ne suffisent pas !

- Les procédés de stockage deviennent obsolètes
disquettes, DAT, magéto-optiques, etc.
- Les supports courants ne sont pas pérennes
- Le problème n'est pas pris assez au sérieux
achetez d'abord, vous verrez bien après!

Les forces du marché ne suffisent pas !

- Les procédés de stockage deviennent obsolètes
disquettes, DAT, magéto-optiques, etc.
- Les supports courants ne sont pas pérennes
- Le problème n'est pas pris assez au sérieux
achetez d'abord, vous verrez bien après!

Le problème est soluble si on s'en occupe !

Questions: défis / enseignement

Q1 : quels sont pour vous les principaux défis pour les STIC à l'horizon d'une génération ?

Q2 : la génération actuelle dispose-t-elle des moyens (ressources, compétences) pour aborder ces défis ?

Q3 : que faudrait-il faire au niveau de l'enseignement des STIC pour mieux préparer les chercheurs et ingénieurs de demain ?

Questions: défis / enseignement

Q1 : quels sont pour vous les principaux défis pour les STIC
à l'horizon d'une génération ?

être du côté des créateurs de technologie et de contenu,
et pas seulement du côté des consommateurs

Questions: défis / enseignement

Q1 : quels sont pour vous les principaux défis pour les STIC à l'horizon d'une génération ?

être du côté des créateurs de technologie et de contenu, et pas seulement du côté des consommateurs

Q2 : la génération actuelle dispose-t-elle des moyens (ressources, compétences) pour aborder ces défis ?

pas clair; l'impulsion en Europe existe, mais pas au niveau des USA, de l'Inde ou de la Chine. Le sujet n'est encore que partiellement reconnu socialement, y compris chez les enseignants et les scientifiques.

Questions: défis / enseignement

Q1 : quels sont pour vous les principaux défis pour les STIC à l'horizon d'une génération ?

être du côté des créateurs de technologie et de contenu, et pas seulement du côté des consommateurs

Q2 : la génération actuelle dispose-t-elle des moyens (ressources, compétences) pour aborder ces défis ?

pas clair; l'impulsion en Europe existe, mais pas au niveau des USA, de l'Inde ou de la Chine. Le sujet n'est encore que partiellement reconnu socialement, y compris chez les enseignants et les scientifiques.

Q3 : que faudrait-il faire au niveau de l'enseignement des STIC pour mieux préparer les chercheurs et ingénieurs de demain ?

augmenter d'un ordre de grandeur la considération du sujet, en faire une vraie matière très tôt, en compagnie des autres sciences

Questions: défis / enseignement

Q1 : quels sont pour vous les principaux défis pour les STIC à l'horizon d'une génération ?

être du côté des créateurs de technologie et de contenu, et pas seulement du côté des consommateurs

Q2 : la génération actuelle dispose-t-elle des moyens (ressources, compétences) pour aborder ces défis ?

pas clair; l'impulsion en Europe existe, mais pas au niveau des USA, de l'Inde ou de la Chine. Le sujet n'est encore que partiellement reconnu socialement, y compris parmi les scientifiques.

Q3 : que faudrait-il faire au niveau de l'enseignement des STIC pour mieux préparer les chercheurs et ingénieurs de demain ?

augmenter d'un ordre de grandeur la considération du sujet, en faire une vraie matière très tôt, en compagnie des autres sciences

Données sur l'emploi (Syntec-informatique)

- Industrie du logiciel seule (SSII, éditeurs, consulting)
55 000 recrutements en 2007, dont 15 000 créations d'emploi
croissance 7%, chômage 2,1%, avec 50% de BAC+5
ne compte ni l'électronique ni l'informatique immergée ailleurs !
- Chiffres d'affaires
pharmacie : 38 G Euros
logiciel : 33 G Euros
Aérospace / Défense : 28 G Euros
beaucoup d'électronique / informatique!

Données sur l'emploi (Syntec-informatique)

- Industrie du logiciel seule (SSII, éditeurs, consulting)
55 000 recrutements en 2007, dont 15 000 créations d'emploi
croissance 7%, chômage 2,1%, avec 50% de BAC+5
ne compte ni l'électronique ni l'informatique immergée ailleurs !
- Chiffres d'affaires
pharmacie : 38 G Euros
logiciel : 33 G Euros
Aérospace / Défense : 28 G Euros
beaucoup d'électronique / informatique!

Et pourtant en manque de jeunes !

Conclusion de la Dernière Séance

Conclusion de la Dernière Séance

L'informatique du futur
ne ressemblera pas à l'actuelle

Conclusion de la Dernière Séance

L'informatique du futur
ne ressemblera pas à l'actuelle

Sauf pour ses principes !

Remerciements

- A la Fondation Bettencourt et au Collège de France
- Aux 12 orateurs des séminaires
- A l'assistance publique et internette
- A mes collègues François Baccelli, Gérard Huet et Jean Vuillemin
- A l'équipe de Marion Susini au Collège et à Bernard Iseni pour la réalisation et la diffusion des vidéos

Remerciements

- A la Fondation Bettencourt et au Collège de France
- Aux 12 orateurs des séminaires
- A l'assistance publique et internette
- A mes collègues François Baccelli, Gérard Huet et Jean Vuillemin
- A l'équipe de Marion Susini au Collège et à Bernard Iseni pour la réalisation et la diffusion des vidéos

Et tout particulièrement à [Marie Chéron](#) et [Cécile Barnier](#)

Le quantique : algorithmique, physique, ordinateur
robotique et informatique
développements logiciels, logiciel libre, gratuité,
téléchargements, modèles économiques
linguistique, traitement du langage et du texte
Probabilités et algorithmes : pourquoi ça marche ?
(à la Flajolet, ou comme l'autostabilisation)

Questions

Codages itératifs probabilistes

importance de l'aléatoire algos auto-stabilisants, tirer au d

proba pourquoi ça marche Shannon ets

optimalité réseau, type de preuve?

energie grosses vs petites machines

quantique?

logiciel libre, modele economique

metriques en info (bugs, preuves)

est toujours aussi génial les vendredi matin au collège de France ! Quelques questions bêtes en vrac :

- à propos des turbocodes, tu as parlé de codages itératifs probabilistes. Pourrais-tu développer le "probabiliste".
 - c'est je crois Laurent Massoulié qui a dit "quand on ne sait pas quoi faire on prend la décision au hasard", que tu as repris. J'aimerais bien voir développer une réflexion autour de ces idées des probabilités et de leur utilisation en algorithmique (garantie de ne pas laisser le système boucler sur une trajectoire rare, de probabilité nulle. Il "faut" tirer aux dés pour casser).
 - j'aimerais bien des choses sur la résistance aux pannes. En particulier dans ce que tu as raconté pour les routages, je n'ai pas bien vu où le traitement de la panne se différencie de la problématique habituelle du routage, reroutage.
 - à propos des délais et débits, il a été question ce matin de garantie d'optimalité. Avec quel type de preuve ?
 - Sur les systèmes pair à pair : il n'y a pas que [Seti@home](#), les extra terrestres et les téléchargements. Il y a aussi l'exploitation des grosses masses de données intrinsèquement réparties, le vol de cycles, et bien d'autres choses.
- à propos du vol de cycles : est-ce que qq'un a regardé les questions de consommation d'énergie comparativement aux grosses machines ?

- Peut-on entrevoir un monde numérique déterministe ?
- A-t-on une idée assez précise des limites physiques de la loi de Moore ? L'auteur, à ma connaissance, donnait une date de validité jusqu'en 2017. Quelle en était la signification ?

Qu'en est-il actuellement ?

Loi de Metcalfe

"L'utilité d'un réseau est proportionnelle au carré du nombre de ses utilisateurs "

Circuits asynchrones ?

que c'est le débit qui est asymétrique.

2-Etat des connaissances et des savoir-faire. Laurent Thi sont réalisés principalement à Taïwan, pas ou pas seule sont là. Quelle est la géographie des savoir-faire en mat numériques? Y a t-il risque d'évolution vers un unique : Même question sur les détenteurs du savoir en la matiè précision comment ils se répartissent dans le monde?

1- Laurent (et je suis d'accord) predisait que les reseaux P2P (pour simplifier) sont probablement l'avenir MAIS j'imagine que les societes comme Thales sont tres reluctantes a laisser leurs « machines » utilisees par d'autres particuliers ou societes
vas t on arriver a un point ou les particuliers disposeront de plus de puissance de calcul que les societes ?
ne doit on pas modifier l'architecture des ordinateurs afin de constituer des couches materielles a l'instar des logicielles (des ceintures de fortifications) ?
et ainsi liberer cette barriere

2- Un televiseur reste connecte sur le reseau internet (pour ceux qui disposent du cable ou le connecte derriere une set up box) , il sera equipe d'un processeur massivement parallele , il pourra etre facile de lui « greffer » un pentium lui permettant d'executer le protocole TCP IP et pourquoi pas un OS type windows
ne pensez vous pas que notre TV va etre prochainement un PC utilisable en reseau P2P

Le seul probleme reside dans la capacite du reseau a assumer les transferts de donnees et Images