Modèle de Blum, Shub et Smale

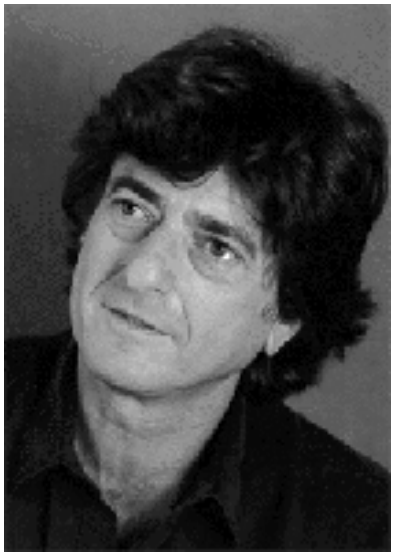
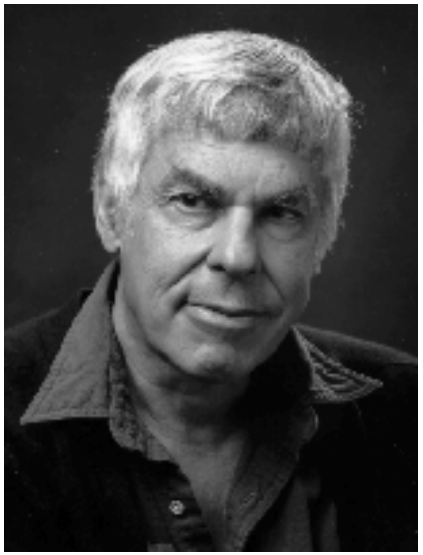
Stéphane Caron

7 janvier 2009

Modèle BSS

Motivations :

- modèle de calcul sur $\mathbb{R}$ affranchi des problèmes d'arrondi ;
- aborder la question « $\mathrm{P} = \mathrm{NP}$? » sur $\mathbb{R}$.

Au programme

1. Machines BSS et circuits algébriques
2. Comparaisons avec le modèle standard
3. La question « P = NP ? »

Machines BSS

&

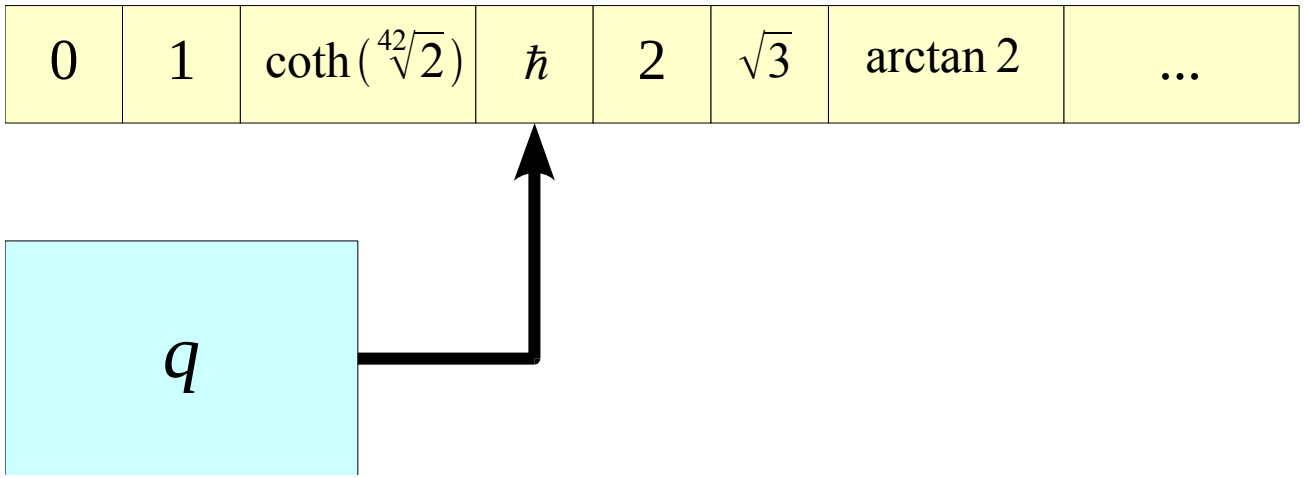
Circuits algébriques

Machines BSS

Définition (informelle)

Une machine BSS est une machine de Turing dont l'alphabet de bande est $\mathbb{R}$ et qui peut exécuter en temps unitaire des opérations sur les réels.

- Les réels sont manipulés comme des entités atomiques.
- Peu d'opérations en général : $(\mathbb{R}, +, -, =)$, $(\mathbb{R}, +, -, \times, <)$, etc.



Circuits

Définition

Un *circuit* est un DAG dont les portes (sommets) représentent des entrées ou des opérations. Une seule porte est de degré sortant nul.

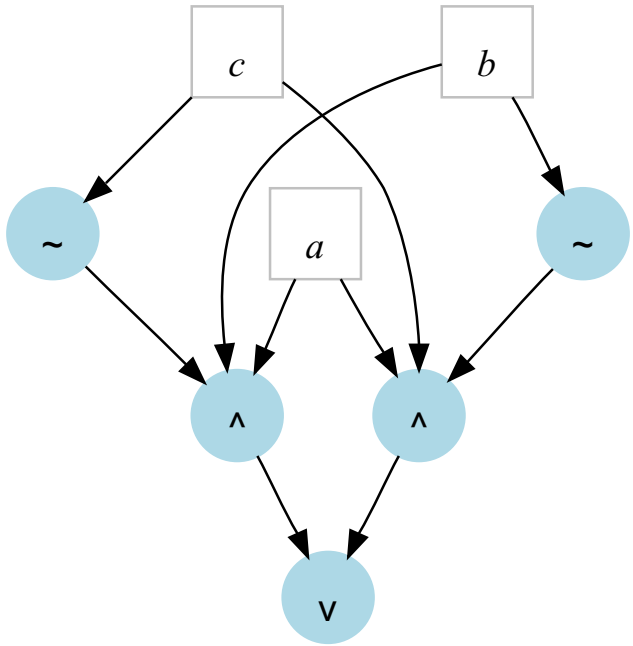


FIGURE: circuit booléen reconnaissant $1.\{10, 01\}$.

Circuits algébriques

Définition

Un *circuit algébrique* est un circuit dont les portes sont des variables ou des opérations réelles et dont la porte de sortie est un test.

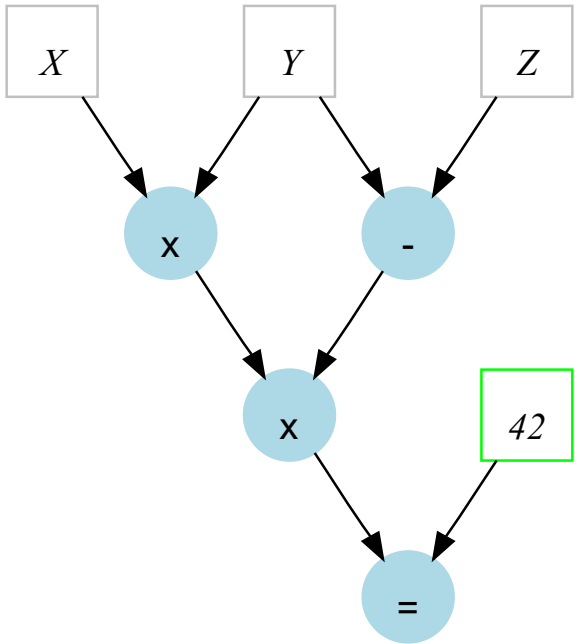


FIGURE: circuit décidant si $X.Y.(Y - Z) = 42$.

Dernières définitions

Définition (reconnaissance par une famille de circuits)

Un problème X est reconnu par une famille $(C_n(x,y))_{n\in\mathbb{N}}$ de circuits algébriques s'il existe un uplet a de paramètres tel que :

$$\forall n \in \mathbb{N},\ \forall x \in \mathbb{R}^n,\ x \in X \iff C_n(x,a) = 1$$

Définition (famille uniforme)

Une famille de circuits (C_n) est dite *uniforme* s'il existe une machine de Turing *booléenne* qui, étant donné un entier n, construit en *temps polynomial* le circuit C_n.

Équivalence entre les deux modèles

Théorème (équivalence entre les deux modèles)

Un problème X est dans la classe $\mathrm{P}_{\mathrm{BSS}}$ si et seulement s'il est reconnu par une famille uniforme de circuits.

Idée de la preuve.

($\Leftarrow$) L'algorithme qui construit le circuit adéquat puis l'exécute est en temps polynomial.

($\Rightarrow$) On construit des circuits qui simulent une étape de calcul de la machine pour une certaine largeur de la bande de travail, puis on empile $t(n)$ tels circuits pour simuler le calcul entier. □

Comparaisons avec

le modèle standard

Classes polynomiales non-uniformes

Définition (classe non-uniforme)

$\mathbb{P}$ est la classe des problèmes reconnus par une famille *non-uniforme* de circuits de taille polynomiale.

Du point de vue des machines BSS, cela revient à fournir un « conseil » c_n de taille polynomiale à la machine pour toute entrée de taille n.

Proposition (un intérêt des classes non-uniformes)

Si NP *n'est pas un sous-ensemble de* $\mathbb{P}$, *alors* $\mathrm{P} \neq \mathrm{NP}$.

Apport des classes non-uniformes ?

On peut *a priori* décider plus de problèmes dans $\mathbb{P}$ que dans P, mais...

Théorème

Sur $(\mathbb{R}, +, -, <)$ *on a* $\mathrm{P}_{\mathrm{BSS}} = \mathbb{P}_{\mathrm{BSS}}$.

Idée de la preuve. On peut coder une famille non-uniforme (C_n) de circuits de taille polynomiale dans le développement dyadique d'un paramètre supplémentaire $\alpha \in [0, 1[$. L'algorithme qui décode le circuit adéquat avant de l'exécuter est en temps polynomial, donc $\mathbb{P}_{\mathrm{BSS}} \subset \mathrm{P}_{\mathrm{BSS}}$. □

Problèmes booléens

Définition

Un *problème booléen* est un sous-ensemble de $\{0,1\}^*$.

- Intérêt : voir si les machines BSS peuvent calculer plus de choses que les machines de Turing à entrées équivalentes.
- Dépend bien sûr de la structure qu'on étudie...

Théorème

Dans la structure $(\mathbb{R}, +, -, =)$ *la classe* $\mathrm{P}_{\mathrm{BSS}} \cap \{0,1\}^*$ *des problèmes booléens de* $\mathrm{P}_{\mathrm{BSS}}$ *est la classe* P *standard, et de même la classe* $\mathbb{P}_{\mathrm{BSS}} \cap \{0,1\}^*$ *est la classe* $\mathbb{P}$ *standard.*

Problèmes booléens

Théorème

Dans la structure $(\mathbb{R}, +, -, =)$ *la classe* $\mathrm{P}_{\mathrm{BSS}} \cap \{0,1\}^*$ *des problèmes booléens de* $\mathrm{P}_{\mathrm{BSS}}$ *est la classe* P *standard, et de même la classe* $\mathbb{P}_{\mathrm{BSS}} \cap \{0,1\}^*$ *est la classe* $\mathbb{P}$ *standard.*

Idée de la preuve. Les entrées de notre algorithme initial étant des booléens, tous les réels manipulés sont des combinaisons linéaires des paramètres $(a_1, \ldots, a_m)$. On voit $\mathbb{R}$ comme un $\mathbb{Q}$-e.v. et on choisit une base $(a_1, \ldots, a_p)$ de $\mathrm{Vect}(a_1, \ldots, a_m)$. On effectue une première transformation pour que les coefficients deviennent entiers, puis on représente les combinaisons linéaires par des uplets d'entiers : $\sum_{i=1}^{p} \alpha_i a_i \mapsto (\alpha_1, \ldots, \alpha_p)$ pour obtenir un algorithme booléen équivalent qui est en temps polynomial. □

Théorèmes de Koiran

On peut citer d'autres liens remarquables.

Théorème (premier théorème de Koiran)

Sur $(\mathbb{R}, +, -, =, <)$, *les problèmes booléens de* $\mathrm{P}_{\mathrm{BSS}}$ *sont les problèmes* $\mathbb{P}$ *au sens standard, soit* $\mathrm{P}_{\mathrm{BSS}} \cap \{0,1\}^* = \mathbb{P}$.

Théorème (deuxième théorème de Koiran)

Sur $(\mathbb{R}, +, -, \times, =)$, *les problèmes booléens de* $\mathbb{P}_{\mathrm{BSS}}$ *sont les problèmes* $\mathbb{P}$ *au sens standard, soit* $\mathbb{P}_{\mathrm{BSS}} \cap \{0,1\}^* = \mathbb{P}$.

Démonstrations : élaborées.

La question « P = NP ? »

NP : la classe existentielle

Cadre standard : NP est la classe des problèmes vérifiables en temps polynomial. Ce point de vue permet de généraliser.

Définition

Un problème X est dans la classe $\mathrm{NP}_{\mathrm{BSS}}$ *ssi* il existe $Y \in \mathrm{P}_{\mathrm{BSS}}$ tel que :

$$x \in X \iff \exists y \in \mathbb{R}_\infty \text{ de taille polynomiale en } |x| \text{ t.q. } (x, y) \in Y$$

Question « P = NP ? »

Sur certaines structures, on sait y répondre.

Théorème

Dans la structure $(\mathbb{R}, +, -, =)$, *on a* $\mathrm{P}_{\mathrm{BSS}} \neq \mathrm{NP}_{\mathrm{BSS}}$.

Un lien aux implications plus sonnantes et trébuchantes...

Théorème (Fournier, Koiran, 1999)

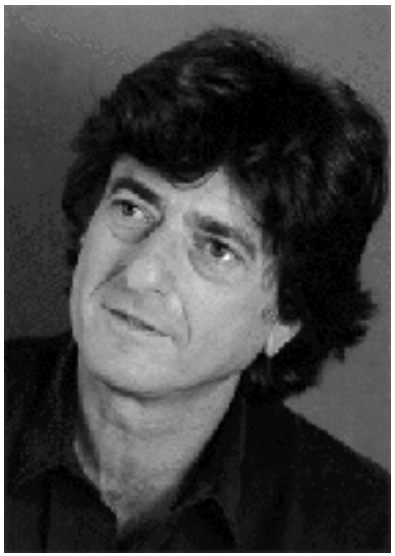
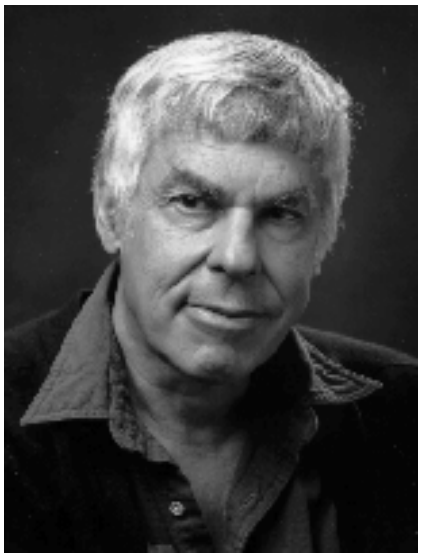
Sur $(\mathbb{R}, +, -, <)$ *on a :* $\mathrm{P}_{\mathrm{BSS}} = \mathrm{NP}_{\mathrm{BSS}} \iff \mathrm{P} = \mathrm{NP}$.

Démonstrations : difficiles.

Conclusion

Avec Blum, Shub et Smale, nous avons ébauché un modèle :

- où on peut calculer confortablement sur $\mathbb{R}$;
- lié au modèle standard : nouvelles perspectives d'étude ;
- qui permet une autre approche de la question « P = NP ? ».

Conclusion

Avec Blum, Shub et Smale, nous avons ébauché un modèle :

- où on peut calculer confortablement sur $\mathbb{R}$;
- lié au modèle standard : nouvelles perspectives d'étude ;
- qui permet une autre approche de la question « P = NP ? ».

Conclusion

Avec Blum, Shub et Smale, nous avons ébauché un modèle :

- où on peut calculer confortablement sur $\mathbb{R}$;
- lié au modèle standard : nouvelles perspectives d'étude ;
- qui permet une autre approche de la question « P = NP ? ».

□