Preuves Formelles d'Inégalités et Programmation Semi-Définie

Directeur: Benjamin Werner (TypiCal)

Co-Directeur: Stéphane Gaubert (Maxplus)

Doctorant 1ère annee Victor MAGRON

LIX, École Polytechnique

Vendredi 14 Janvier 2011

Plan

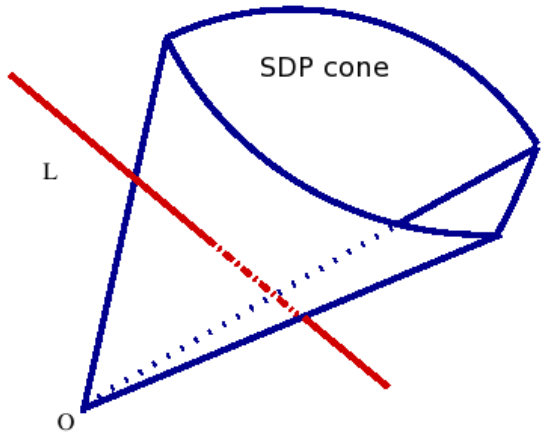
1. Contexte
2. Programmation semi-définie
3. Preuves formelles d'inégalités convexes

Contexte

- Preuves appelant des calculs informatiques:
  - Primalité
  - Théorème des 4 couleurs
  - Démonstration de Hales de la conjecture de Keppler
- Multiples intérêts:
  - Une partie du champ mathématique aborde ces techniques
  - L'interface entre la partie « conventionnelle » déductive et la partie calculatoire est particulièrement propice aux erreurs
  - Ouverture de nouveaux champs aux systèmes de preuves en permettant l'automatisation de certains résultats
- Améliorer les outils développés par Roland Zumkeller en utilisant des techniques de programmation semi-définie => intérêt pour les mathématiques appliquées

Programmation semi-définie

- Classe de problèmes d'optimisation sous contraintes portant sur des matrices symétriques définies-positives:



Trouver $X \in \mathbb{S}^n$, solution de:

$$(\mathrm{P}) \begin{cases} \inf \langle C, X \rangle \\ A(X) = b \\ X \succeq 0. \end{cases}$$

- De nombreux problèmes courants peuvent être formulés de cette manière: décomposition de polynômes en sommes de carrés, problèmes de graphes,...
- Résolution avec l'algorithme des points intérieurs

Un exemple d'inégalité polynomiale

$$\forall x \in \left([4;(2t_0)^2],[4;(2t_0)^2],[4;(2t_0)^2],[4;(2t_0)^2],[4;(2t_0)^2],[4;8]\right).$$
$$x_1^5x_4 - 2x_1^4x_2x_4 + x_1^3x_2^2x_4 - 2x_1^4x_3x_4 + 4x_1^3x_2x_3x_4$$
$$- 2x_1^2x_2^2x_3x_4 + x_1^3x_3^2x_4 - 2x_1^2x_2x_3^2x_4 + x_1x_2^2x_3^2x_4 - x_1^4x_2x_5$$
$$+ 2x_1^3x_2^2x_5 - x_1^2x_2^3x_5 + x_1^4x_3x_5 - x_1^3x_2x_3x_5 - x_1^2x_2^2x_3x_5$$
$$+ x_1x_2^3x_3x_5 - x_1^3x_3^2x_5 + 2x_1^2x_2x_3^2x_5 - x_1x_2^2x_3^2x_5 - 2x_1^4x_4x_5$$
$$+ 4x_1^3x_2x_4x_5 - 2x_1^2x_2^2x_4x_5 + 2x_1^3x_2x_5^2 - 4x_1^2x_2^2x_5^2 + 2x_1x_2^3x_5^2$$
$$- x_1^3x_3x_5^2 + 3x_1^2x_2x_3x_5^2 - 3x_1x_2^2x_3x_5^2 + x_2^3x_3x_5^2 + x_1^3x_4x_5^2$$
$$- 2x_1^2x_2x_4x_5^2 + x_1x_2^2x_4x_5^2 - x_1^2x_2x_5^3 + 2x_1x_2^2x_5^3 - x_2^3x_5^3$$
$$+ x_1^4x_2x_6 - x_1^3x_2^2x_6 - x_1^4x_3x_6 - x_1^3x_2x_3x_6 + 2x_1^2x_2^2x_3x_6$$
$$+ 2x_1^3x_3^2x_6 - x_1^2x_2x_3^2x_6 - x_1x_2^2x_3^2x_6 - x_1^2x_3^3x_6 + x_1x_2x_3^3x_6$$
$$- 2x_1^4x_4x_6 + 4x_1^3x_3x_4x_6 - 2x_1^2x_3^2x_4x_6 - x_1^3x_2x_5x_6 + 3x_1^2x_2^2x_5x_6$$
$$- x_1^3x_3x_5x_6 - 4x_1^2x_2x_3x_5x_6 + x_1x_2^2x_3x_5x_6 + 3x_1^2x_3^2x_5x_6 + x_1x_2x_3^2x_5x_6$$
$$- 2x_2^2x_3^2x_5x_6 + 4x_1^3x_4x_5x_6 - 4x_1x_2x_3x_4x_5x_6 - x_1^2x_2x_5^2x_6 - 3x_1x_2^2x_5^2x_6$$
$$+ 2x_1^2x_3x_5^2x_6 + x_1x_2x_3x_5^2x_6 + x_2^2x_3x_5^2x_6 - 2x_1^2x_4x_5^2x_6 + x_1x_2x_5^3x_6$$
$$+ x_2^2x_5^3x_6 - x_1^3x_2x_6^2 + 2x_1^3x_3x_6^2 + 3x_1^2x_2x_3x_6^2 - 4x_1^2x_3^2x_6^2$$
$$- 3x_1x_2x_3^2x_6^2 + 2x_1x_3^3x_6^2 + x_2x_3^3x_6^2 + x_1^3x_4x_6^2 - 2x_1^2x_3x_4x_6^2$$
$$+ x_1x_3^2x_4x_6^2 + 2x_1^2x_2x_5x_6^2 - x_1^2x_3x_5x_6^2 + x_1x_2x_3x_5x_6^2 - 3x_1x_3^2x_5x_6^2$$
$$+ x_2x_3^2x_5x_6^2 - 2x_1^2x_4x_5x_6^2 - x_1x_2x_5^2x_6^2 - x_1x_3x_5^2x_6^2 - 2x_2x_3x_5^2x_6^2$$
$$+ x_1x_4x_5^2x_6^2 - x_1^2x_3x_6^3 + 2x_1x_3^2x_6^3 - x_3^3x_6^3 + x_1x_3x_5x_6^3 + x_3^2x_5x_6^3 < 0$$

Un exemple d'inégalité polynomiale

- L'inégalité d'avant peut se ramener à un problème de somme de carrés (SOS) en multipliant le polynôme par un autre de degré suffisamment grand
- On utilise la méthode de Gram, $F(x)$ SOS ssi $F(x) = \omega(x)\ {}^t Q \omega(x)$ avec $\omega(x)$ un vecteur de monômes, et $Q \succeq 0$
- On se ramène au problème de réalisibilité SDP: $f_\alpha = \sum_{\beta+\gamma=\alpha} Q_{\beta,\gamma}$ (en posant $F(x) = \sum_\alpha f_\alpha$)
- On factorise $Q = L\ {}^t L$ (Cholesky), le SDP est donné par $f = Lz$

Preuves formelles d'inégalités convexes

- Comment exploiter de tels algorithmes en Coq de manière à pouvoir en accepter les résultats comme des preuves formelles?
- Les algorithmes sont très gourmands en calcul donc:
  - On délègue à un outil extérieur et rapide (C, Caml,...) le calcul, le résultat étant le certificat
  - Le système de preuves doit alors seulement vérifier ce certificat: calcul formel
- Par exemple, on peut obtenir un certificat sur la décomposition en SOS.

Difficultés et points techniques

- Limiter la taille du certificat en choisissant un format hybride pour représenter les nombres, mêlant représentations numériques classiques et symboliques
- Les conditions de réalisabilité qui sont nécessaires pour avoir la convergence des méthodes de points intérieurs ne sont pas tout le temps satisfaites => points passés sous silence dans la littérature (Parillo, Lasserre, Peyrl, ...)
- Des erreurs d'arrondi peuvent faire augmenter la taille du certificat
- Difficulté d'interfacer les outils extérieurs (languages de l'algorithme de résolution des SDP) avec COQ => mise en relation avec des travaux récents de David Monniaux sur les SOS
- Intérêt de traiter le problème SDP avec d'autres outils mathématiques récents comme les amibes

Fin

Merci pour votre attention!