Vérification formelle du théorème de Kantorovitch

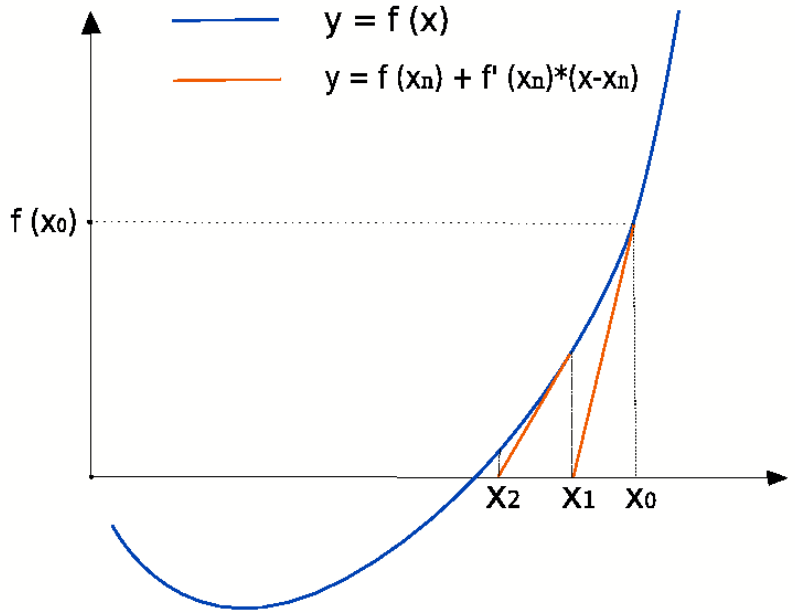
Ioana Paşca

INRIA Sophia, projet Marelle

28 Janvier 2008

Plan

Le processus de Newton



- trouver les racines d'une fonction f: $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$
- le théorème de Kantorovitch donne des contitions suffisantes pour la convergence de processus de Newton vers une racine de la fonction f

Théorème de Kantorovitch

Soit un système réel de p équations avec p inconnues $f(x) = 0$ avec $f(x) \in C^{(2)}(\omega)$ et $\overline{U_\varepsilon}(x^{(0)}) = \{\|x - x^{(0)}\| \leq \varepsilon\} \subset \omega$
Si:

- la matrice jacobienne $W(x) = [\frac{\partial f_i}{\partial x_j}]$ pour $x = x^{(0)}$ possède une inverse $\Gamma_0 = W^{-1}$ avec $\|\Gamma_0\| \leq A_0$;
- $\|\Gamma_0 f(x^{(0)})\| \leq B_0 \leq \frac{\varepsilon}{2}$;
- $\sum_{k=1}^{p} |\frac{\partial^2 f_i(x)}{\partial x_j \partial x_k}| \leq C$ pour $i, j = 1, 2, ..., p$ et $x \in \overline{U_\varepsilon}(x^{(0)})$;
- $2pA_0B_0C \leq 1$.

Alors, le processus de Newton $x^{(n+1)} = x^{(n)} - W^{-1}(x^{(n)})f(x^{(n)})$ converge et $x^* = \lim_{n\to\infty} x^{(n)}$ est la solution unique du système initial dans le domaine $\|x - x^{(0)}\| \leq 2B_0$.

Motivations

- formaliser des concepts mathématiques dans un assistant à la preuve
  - vérifier de grands théorèmes
- vérification d'algorithmes
  - garantir la correction d'algorithmes vis-à-vis de spécifications précises
  - vérification formelle pour les méthodes numériques

Preuve et outils

Idée de la preuve

- prouver des propriétés pour tout élément de la suite de Newton
- montrer que c'est une suite de Cauchy
- utiliser la complétude pour prouver la convergence
- prouver que la limite de la suite est une racine pour la fonction donnée
- montrer que dans un certain intervalle la racine est unique

Outils:

- assistant à la preuve
- formalisation des concepts d'analyse réelle

État de l'art

Les assistants à la preuve et l'analyse réelle

- PVS, Isabelle, HOL-Light, Coq, ACL2 contiennent des bibliothèques pour traiter les réels
- différentes approches:
  - définition axiomatique/constructive
  - formalisation issue de l'analyse réelle classique/non-standard

Organisation du travail

Assistant à la preuve: Coq

- bibliothèque standard: `Reals`
  - définition axiomatique
  - formalisation classique des concepts

Prouver le théorème:

- commencer par le cas $f : \mathbb{R} \longrightarrow \mathbb{R}$
- généraliser pour $f : \mathbb{R}^p \longrightarrow \mathbb{R}^p$
  - formaliser des concepts d'analyse multivariée
  - fournir la preuve formelle du théorème en plusieurs dimensions

La preuve dans le cas unidimensionnel

- adapter l'enonce et la preuve
- légère généralisation du théorème: $f \in C^{(2)} \rightarrow f \in C^{(1)}$ et une hypothèse sur la première derivée
- suivre essentiellement les mêmes pas de raisonnement de preuve "papier" en utilisant les concepts de la bibliothèque `Reals`

Resultats:

```
Theorem kantoro_exist_b:
exists xs:R, Un_cv Xn xs /\ c_disc X0 (2*B0) xs /\

Theorem kantoro_unic:
forall xs2:R, c_disc X0 (2*B0) xs2 -> f xs2 = 0 ->
```

Difficultés rencontrées: dérivabilité

sur "papier":

$$f : [a,b] \to \mathbb{R},\ f \in C^{(1)}([a,b]),\ x_0 \in [a,b],\quad x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

en Coq:

```
Variable f: R->R.
Hypothesis pr: forall x, a <= x <= b -> derivable_pt
Variable X0:R.
Hypothesis H: a <= X0 <= b.
Definition df_x0 := derive_pt f X0 (pr X0 H).
Fixpoint Xn (m:nat) : R :=
 match m with
   | 0 => X0
   | S n => Xn n - f (Xn n)/(derive_pt f (Xn n) (pr
 end.
```

Difficultés rencontrées: dérivabilité

```
Variable f':R->R.
Hypothesis: forall x, (H: a<=x<=b) ->f' x = derive_p
Fixpoint Xn (m:nat) : R :=
 match m with
   | 0 => X0
   | S n => Xn n - f (Xn n)/ f' (Xn n)
 end.
```

Travailler en plusieurs dimensions

- pas de travaux existants en Coq
- HOL-Light : bibliothèque `Multivariate`

Travail: trouver une bonne formalisation pour les éléments de $\mathbb{R}^p$

- critères
  - bonne représentation des concepts
  - preuves facilement manipulables
- les vecteurs de $\mathbb{R}^p$: $(x_0, x_1, \ldots, x_{p-1})$ sont de type $\{0, 1, .., p-1\} \to \mathbb{R}$
- formalisation avec `SSReflect`; projet Mathematical Components

Motivation du choix

I_(p): représente l'ensemble $\{0, 1, .., p-1\}$

- type fini avec cardinalité p
- les éléments du type sont coercibles aux nombres naturels
- le type contient une liste qui énumère tous ses éléments

Les vecteurs: I_(p)$\rightarrow \mathbb{R}$

- manipulation facile

```
Definition add_v (v1 v2:I_(p)->R):I_(p)->R:=
  (fun i:I_(p) => v1 i + v2 i).
```

- moyen de raisonner: induction sur la liste

```
Definition norm (v:I_(p)->R):R:=
  foldr (fun i:I_(p) => Rmax (Rabs (v i))) 0 (enum I

Lemma norm_pos: forall (v:I_(p)->R), 0 <= norm v.
```

Concepts et propriétés formalisés

- vecteur
- matrice (Sidi Ould Biha)
- norme de vecteurs et de matrices
- convergence d'une suite de vecteurs réels
- complétude de $\mathbb{R}^p$
- limite et continuité d'une fonction vectorielle
- concepts de différentiabilité
- ...

La preuve dans $\mathbb{R}^p$

Vérification de la structure du théorème

- la même structure que pour le cas réel
- généralisation des résultats
  - facile, ex. $0 \leq |a| \longrightarrow 0 \leq \|A\|$
  - difficile, ex. $|ax| = |a||x| \longrightarrow \|Ax\| \leq \|A\|\|x\|$

```
Theorem kantoroRp_exist:
exists xs, conv_Rp Xn xs /\
           norm (xs -^ X0) <= 2*B0 /\ f xs = vect0 p
```

Résultats admis

- propriétés des matrices liées à leur norme

```
Lemma matr_inv_norm:
forall A: MR_(p), norm_m (\1 -m A) < 1 -> \det A <>
Admitted.
```

Conclusions et perspectives

Le travail accompli

- fournir une preuve de la structure du théorème
- formaliser des concepts d'analyse multivariée

Perspectives

- vérifier les résultats manquants
- fournir des formalisations pour des cas particuliers du théorème

Liens utiles

- http://coqfinitgroup.gforge.inria.fr/
- http://www-sop.inria.fr/marelle/Ioana.Pasca/