Pour une axiomatisation minimale des réels en Coq[11]

Stage de fin de Licence sous la direction d'Yves Bertot
Équipe Marelle - INRIA Sophia-Antipolis

G. ALLAIS

Juin-Juillet 2009

Résumé

Ce stage a pour but d'étudier la démonstration assistée par ordinateur en se concentrant sur l'implémentation de résultats d'analyse fonctionnelle réelle. On portera tout particulièrement notre attention sur les théorèmes traitant la dérivabilité et la continuité des fonctions d'une variable réelle.

Une première partie tâchera d'établir la régularité de la fonction réciproque en fonction de celle de la fonction initiale. Une seconde partie permettra quant à elle de relier π aux fonctions trigonométriques. Ce travail devrait déboucher sur la suppression de l'axiome affirmant que « $\sin\left(\frac{\pi}{2}\right) = 1$ » de la bibliothèque standard de Coq.

1 Préliminaires

Contrairement aux preuves effectuées sur papier, les preuves établies dans un langage restreint et selon une grammaire simple (des « lois » simples) peuvent être vérifiées mécaniquement. La machine garantit alors que l'enchainement logique décrit par l'utilisateur est légal (dans le sens où il respecte les « lois » évoquées précédemment). Le fait que les systèmes de preuves se fondent sur la théorie des types et la logique formelle permet de garantir qu'une démonstration légale est également correcte grâce à un petit nombre de preuves simples effectuées sur papier et aisément vérifiables (pour Coq, par exemple, voir [1]).

La démonstration assistée par ordinateur permet donc de mettre en place des preuves robustes : une fois qu'un résultat est démontré, il est certain qu'on ne découvrira pas dans quelques années qu'il existe un cas particulier qui n'avait pas été envisagé.

La preuve assistée par ordinateur peut par conséquent être utilisée pour démontrer certaines propriétés de systèmes critiques afin de garantir qu'ils ne risquent pas de présenter des comportements anormaux. Une grande partie des systèmes critiques étant en interaction avec leur environnement (*via* des capteurs par exemple), il est important de pouvoir faire un lien entre un phénomène continu et sa modélisation et c'est là qu'intervient la formalisation des réels et plus particulièrement de l'analyse réelle.

Première partie

État de l'art : Analyse réelle et preuve assistée par ordinateurs

2 Automath

Automath[3] a été conçu par De Bruijn[5]. Contrairement aux langages plus modernes (Coq par exemple), Automath ne dispose ni d'un système de tactiques (toutes les preuves doivent donc être faites en exhibant un $\lambda-$terme du bon type), ni de types inductifs (ce qui force à l'utilisation d'axiomes supplémentaires)[20]. Cela rend les preuves très fastidieuses à développer (et à lire !) mais a l'avantage d'expliciter leur construction ainsi que le lien entre preuves et programmes établi *via* l'isomorphisme de Curry-Howard.

Dès les années 70, on trouve une vérification du « Grundlagen der Analysis » de E. Landau[13] dans le langage Automath. C'est une preuve de faisabilité de la formalisation de projets importants en un langage vérifiable par la machine ce qui laisse augurer de fructueux développements futurs.

3 ACL2

ACL2[15] est à la fois un langage de programmation, un langage permettant d'énoncer des spécifications et un langage permettant de construire des modèles et de les étudier formellement. Les preuves sont réalisées de manière semi-automatique.

Une bibliothèque d'analyse non standard[1][7] est présente dans la distribution standard d'ACL2. Elle permet la formalisation des notions de continuité, de dérivabilité des fonctions d'une variable réelle et implémente les théorèmes fondamentaux que sont le théorème de la valeur moyenne, le théorème des valeurs intermédiaires et le théorème de Rolle.

4 HOL light

HOL Light[10] est, comme tous les systèmes de preuve interactifs de la famille HOL[2], issu de LCF[3] et a donc hérité de son approche. Un type abstrait y définit les théorèmes et on ne peut appliquer aux théorèmes que des fonctions données par le système et traduisant des règles d'inférence. Si l'on peut garantir que ces fonctions sont correctement implémentées, alors tous les résultats prouvés par inférence sont corrects. Les preuves sont donc constructives.

La distribution standard de l'assistant de preuve HOL Light comprend, dans la section réservées aux exemples, une bibliothèque importante de théorèmes d'analyse réelle. Elle est issue du travail effectué par John Harrison au cours de sa thèse[9]. Il implémente en effet dès la première moitié des années 90 les séries, l'étude de la continuité et de la dérivabilité des fonctions d'une variable réelle (et de fait le théorème des valeurs intermédiaires, le théorème de Rolle, le théorème de la valeur moyenne, etc.) et l'étude des fonctions trigonométriques et de leurs réciproques respectives.

[1] L'analyse non standard fait intervenir le calcul infinitésimal *via* la définition rigoureuse d'infiniment petits.
[2] HOL : *Higher Order Logic* (Logique d'ordre supérieur)
[3] LFC : *Logic for Computable Functions* (Logique des fonctions calculables)

5 PVS

PVS[18][4] est un système basé sur la logique d'ordre supérieure et des mécanismes de typages complexes tels que les types dépendants. L'utilisation des types dépendants permet d'ajouter des contraintes supplémentaires sur les objets évoqués dans les théorèmes et donc d'énoncer ces derniers plus finement ce qui est fondamental dans la preuve de correction d'algorithmes par exemple[5].

En 1996, il y a déjà des résultats concernant les convergences de suites, de fonctions et la formalisation de la continuité, de la dérivabilité et du théorème de la valeur moyenne[4].

6 Coq

La bibliothèque standard comprend une bibliothèque traitant de la formalisation des réels ainsi que des bases de l'analyse réelle grâce aux contributions d'Olivier Desmettre (fonctions trigonométriques, fonctions carré et racine carrée, sommes finies, propriété de Chasles, géométrie plane de base), de Micaela Mayero, etc[2].

Cette bibliothèque permet donc de traiter les suites, les séries, la continuité, la dérivabilité et implémente les théorèmes des valeurs intermédiaires, de la valeur moyenne, de Rolle, etc.

7 C-corn

Développé en Coq, C-CORN[17] est pourtant un projet à part entière. La théorie des types, à l'instar de la logique, permet de raisonner de deux manières distinctes : avec ou sans le tiers-exclu (ou tout énoncé équivalent). Sans le tiers exclus, toute preuve est dite « constructive » dans la mesure où une preuve d'existence d'un objet fournira nécessairement un procédé de construction de cet objet[6].

Si la bibliothèque standard de Coq a fait le choix du pragmatisme en autorisant l'usage d'axiomes faisant partie du bagage commun accepté par la majeure partie des mathématiciens, le projet C-CORN prend, quant à lui, une direction distincte en cherchant à pousser le cadre constructif le plus loin possible.

Les résultats démontrés en matière d'analyse réelle au sein du projet C-corn sont sensiblement les mêmes que ceux de la bibliothèque standard de Coq. L'approche est toutefois régulièrement différente et il peut être très intéressant de confronter les définitions choisies dans les deux projets.

Deuxième partie
Développements effectués lors du stage

8 Motivations

La bibliothèque standard de Coq utilise un ensemble d'axiomes indispensables à la formalisation des réels ainsi qu'un axiome statuant que « $\sin\left(\frac{\pi}{2}\right) = 1$ ». Cet axiome n'existe que pour

[4] PVS : *Prototype Verification System*

[5] Un exemple classique : correction de l'algorithme `quick sort : pour tout n, list[n] -> list[n]`.

[6] C'est d'ailleurs sur cette idée que se fondent les processus d'extraction d'algorithmes à partir de preuves destinés à la production de logiciels certifiés.

des raisons historiques : il peut en principe être éliminé et, ainsi, permettre aux réels de la bibliothèque standard d'être dôtés d'une axiomatisation minimale. Afin de supprimer cet axiome on semble devoir s'intéresser[7] à deux aspects de l'analyse réelle : le premier, fondamental, concerne la régularité des fonctions réciproques tandis que le second, pratique, vise à relier π aux fonctions trigonométriques.

Dans les bibliothèques d'analyse réel, la continuité et la dérivabilité des fonctions d'une variable réelle sont établies (sous les bonnes conditions) si ces fonctions sont la somme, la différence, le produit, la composition, l'inverse ou le quotient de deux fonctions dérivables. La régularité de la fonction réciproque n'est par contre jamais évoquée. Nous tâcherons donc de combler ce manque en étudiant la continuité et la dérivabilité de la fonction réciproque en fonction de celles de la fonction initiale.

Contrairemnt à d'autres bibliothèques standard (voir 9.2.3), la construction de π en Coq ne fait pas le lien avec les fonctions trigonométriques. On tâchera donc de remédier à ce problème en établissant un lien clair entre π, cos et sin.

9 Choix de la preuve à implémenter

La preuve imaginée pour supprimer l'axiome surnuméraire (et décrite en 10) met en avant deux sujets distincts : l'étude de la régularité de la fonction réciproque et l'explicitation du lien entre π et les fonctions trigonométriques.

Si la preuve de la régularité de la fonction réciproque est classique, il existe par contre de nombreuses façons de relier π aux fonctions trigonométriques et nous allons devoir définir celle qui sera la plus simple à mettre en oeuvre au sein de Coq et celle qui permettra le plus facilement de supprimer l'axiome.

9.1 Régularité de la fonction réciproque

Lors de l'implémentation de la preuve, j'ai pu constater que la régularité de la fonction réciproque en fonction de la fonction initiale nous est majoritairement donnée par le théorème d'inversion locale. Celui-ci nous permet en effet de garantir que la fonction réciproque est continue ce qui, une fois acquis, simplifie grandement la preuve de la dérivabilité.

On se placera dans le cas de fonctions strictement croissantes mais le résultat peut être étendu aux fonctions strictement monotones.

On supposera également que la fonction réciproque considérée est inverse à droite de la fonction initiale (on montre de toutes les manières que toute réciproque à gauche est réciproque à droite si la fonction initiale est strictement croissante et si la fonction réciproque a pour domaine d'arrivée le domaine de départ de la fonction initiale).

9.2 De nombreuses manières de relier π aux fonctions trigonométriques

On cherche une manière de relier la série définissant π en Coq aux fonctions trigonométriques de manière à pouvoir démontrer relativement simplement l'axiome que l'on veut supprimer.

9.2.1 Formule(s) de Machin

$$\frac{\pi}{4} = 4\arctan\left(\frac{1}{5}\right) - \arctan\left(\frac{1}{239}\right)$$

[7] À moins qu'il n'existe une démonstration efficace différente de celle que l'on souhaite mettre en place.

Il existe de nombreuses formules du type de celle de Machin (1706) : elles lient toutes π à une somme de termes de la forme $a_k \arctan b_k$.

En voici deux exemples remarquables :

Formule attribuée à Euler

$$\frac{\pi}{4} = \arctan\left(\frac{1}{2}\right) + \arctan\left(\frac{1}{3}\right)$$

Formule liant π et la suite de Fibonacci On peut également écrire une relation faisant intervenir les termes impaires de la suite de Fibonacci[8] comme le montre la formule suivante[14] :

$$\frac{\pi}{4} = \sum_{k=0}^{+\infty} \arctan\left(\frac{1}{F_{2k+1}}\right)$$

Ces formules présentent un inconvénient majeur : elles font intervenir arctan plus d'une fois au sein d'une somme et en présence d'un terme constant. Il semble extrêmemnt compliqué de faire disparaitre ces arctan au profit de sinus et cosinus, on ne les utilisera donc pas pour relier π aux fonctions trigonométriques.

Elles peuvent cependant s'avérer très utiles dans d'autres domaines (calcul efficace des décimales de π par exemple).

9.2.2 Formule de Gregory

$$\arctan x = \sum_{k=0}^{+\infty} \frac{(-1)^k}{2k+1} x^{2k+1}$$

Démontrée au cours des années 1670 par James Gregory, il semblerait qu'elle soit déjà connue d'un mathématicien indien du XV° siècle (Nilakantha)[19].

Elle a l'avantage de ne pas faire intervenir arctan dans la somme et donc de permettre d'appliquer tan afin de faire apparaitre sin et cos :

$$\forall x \in [-1;1], x = \tan\left(\sum_{k=0}^{+\infty} \frac{(-1)^k}{2k+1} x^{2k+1}\right)$$

9.2.3 Construction de $\frac{\pi}{2}$ en C-Corn

Étant donné que l'égalité « $\cos^2 + \sin^2 = 1$ » peut être démontrée en utilisant uniquement les axiomes habituels permettant la définition des réels, on en déduit qu'il est équivalent de démontrer l'axiome à supprimer ou le lemme « $\cos\left(\frac{\pi}{2}\right) = 0$ » (le signe de sin, série alternée, étant très aisé à déterminer).

La construction de $\frac{\pi}{2}$ en C-Corn permet d'envisager une démonstration possible. $\frac{\pi}{2}$ y est en effet défini de la manière suivante :

Soit

$$f_n = \begin{cases} 0 & \text{si } n = 0 \\ \cos(f_{n-1}) + f_{n-1} & \text{sinon} \end{cases}$$

[8] En pratique, on peut remplacer la suite de Fibonacci par n'importe quelle suite récurente de la forme $U_{n+2} = U_{n+1} + U_n$[8].

On pose alors :

$$\frac{\pi}{2} = \lim_{n \to +\infty} f_n$$

Étant donné que cos est continue, on a :

$$\lim_{n \to +\infty} f_n = \lim_{n \to +\infty} [\cos(f_{n-1}) + f_{n-1}] \Rightarrow \frac{\pi}{2} = \cos\left(\frac{\pi}{2}\right) + \frac{\pi}{2}$$

9.2.4 Limitations dues à Coq, choix de la preuve à implémenter

Dès lors que la définition de π est différente de celle de la bibliothèque standard de Coq, la preuve sera plus complexe puisqu'il faudra montrer que les deux définitions donnent bien le même réel. De plus, seule la définition de π en C-Corn établit un lien direct entre π et cos ou sin, elle permet d'ailleurs de montrer très aisément que $\cos\left(\frac{\pi}{2}\right) = 0$.

Mais relier les définitions de π de la bibliothèque standard et de C-Corn semble plutôt complexe du fait de leur éloignement certain :

- **En Coq**, π est défini comme étant quatre fois la somme de la série d'arctan prise en 1
- **En C-Corn**, π est défini comme le double de la limite de la fonction récursive vue précédemment.

On abandonnera donc cette option et on se dirigera plutôt vers une preuve tâchant d'utiliser le fait que π est défini avec la série d'arctan : la formule de Gregory permettra de faire le lien entre la définition de π et les fonctions trigonométriques.

10 Schéma de la preuve

On choisit donc de prouver que la série servant à définir π est celle d'arctan prise en 1. Cela permettra de déduire que $\tan\left(\frac{\pi}{4}\right) = 1$ puis que $\sin\left(\frac{\pi}{2}\right) = 1$ grâce aux relations trigonométriques.

Voici un squelette de la preuve, on trouvera cependant un schéma mettant mieux en valeur les dépendances entre les différentes parties au sein des annexes (16).

1. Propriétés générales
   - Continuité de la fonction réciproque sur un intervalle
   - Dérivabilité de la fonction réciproque sur un intervalle
2. $\arctan_1$ est la réciproque de tan
   - Dérivabilité et croissance de tan sur $[-1; 1]$
   - Bijectivité de tan : $\left[-\frac{7}{8}; \frac{7}{8}\right] \mapsto \left[\tan\left(-\frac{7}{8}\right); \tan\left(\frac{7}{8}\right)\right]$
   - Définition de $\arctan_1$ grâce au théorème des valeurs intermédiaires
3. $\arctan_2$ est la série $\sum_{k=0}^{+\infty} \frac{(-1)^k}{2k+1} x^{2k+1}$
   - Convergence de la série sur $[0; 1]$
   - Définition de $\arctan_2$ grâce à la réduction de l'argument
4. $\arctan_1 = \arctan_2$ sur $[0; 1]$
   - Égalité[9] des dérivées sur $]0; 1[$
   - Égalité des fonctions sur $[0; 1]$
5. $\sin\left(\frac{\pi}{2}\right) = 1$
   - $\tan\left(\frac{\pi}{4}\right) = 1$
   - Conclusion

[9] L'égalité des fonctions dérivées est plus aisée à démontrer que l'égalité des fonctions dans la mesure où la première est syntaxique alors que la seconde ne l'est pas.

Le squelette de cette preuve est assez simple mais nous allons voir que la démonstration formelle met en lumière certaines difficultés.

11 Un exemple de preuve : dérivabilité de la réciproque

Si l'on suppose la dérivabilité de la fonction réciproque, il est aisé de démontrer que la dérivée de la fonction réciproque vérifie la formule suivante :

$$(f^{-1})'(x) = \frac{1}{f'(f^{-1}(x))}$$

La difficulté réside donc dans la preuve de la dérivabilité de la réciproque de f en x qui s'exprime de la manière suivante :

$$\exists l, \forall \epsilon, \exists \delta, \forall h, |h| < \delta \wedge h \neq 0 \Rightarrow \left| \frac{f^{-1}(x+h) - f^{-1}(x)}{h} - l \right| < \epsilon$$

La majeure partie de la difficulté de la preuve de la dérivabilité de la fonction réciproque se situe dans la preuve de la continuité de la fonction réciproque. La preuve de la dérivabilité ne se réduit alors plus qu'à combiner des contraintes sur l'intervalle dans lequel doit se trouver h[10].

Examinons la façon dont on établit un lemme préliminaire contenant à peu près toute la preuve de la continuité de la fonction réciproque[11].

```
Lemma continuity_pt_recip_prelim1 :
 forall (f g:R->R)
 (lb ub:R) (Pr1:lb < ub),
 (forall x y, lb <= x -> x < y ->
  y <= ub -> f x < f y) ->
 (forall x, lb <= x <= ub ->
  (comp g f) x = id x) ->
 (forall a, lb <= a <= ub ->
  continuity_pt f a) ->
 forall b, f lb < b < f ub ->
 continuity_pt g b.
```

Lemma `continuity_pt_recip_prelim1` :
$\forall f, g : \mathbb{R} \to \mathbb{R}$,
$\forall lb, ub \in \mathbb{R}$,
si $\begin{cases} f \text{ strct. croissante sur } [lb, ub] \\ g \circ f = id \text{ sur } [lb; ub] \\ f \text{ continue sur } [lb; ub] \end{cases}$
alors g continue sur $]f(lb); f(ub)[$.

On veut montrer que la fonction réciproque de f (fonction strictement croissante et continue sur $[lb; ub]$) est continue sur l'intervalle $]f(lb); f(ub)[$. Cela revient à trouver un intervalle de $]f(lb); f(ub)[$ tel que toute image d'un point de cet intervalle par f^{-1} ne soit pas trop éloignée de l'image du centre de cet intervalle par f^{-1}.

Intégralité de la preuve[6] : voir annexes (17).

12 Résultats

J'ai choisi de diviser le travail effectué durant ce stage en trois parties ce qui se traduit par la réalisation de trois modules Coq. Le découpage est fait de manière thématique et vise à permettre aux lemmes d'être aisément réutilisés dans des projets futurs.

Liste des modules réalisés :

[10] On remplace en effet le h du dénominateur par $(f \circ f^{-1})(x+h) - (f \circ f^{-1})(x)$ et la continuité de f^{-1} nous permet alors de nous ramener à la dérivée de f en $f^{-1}(x)$.

[11] Le lemme final ne fait que transformer la condition "g est inverse à gauche" en "g est inverse à droite".

- `Ranalysis5` : dans le prolongement des Ranalysis$\{1-4\}$, Ranalysis5 établit le fait que la réciproque d'une fonction strictement croissante et continue sur un intervalle est croissante et continue sur l'intervalle image.
- `Rtrigo_bounds` : ce module démontre que cos est positif entre -1 et 1 sans utiliser l'axiome que l'on souhaite éliminer[12]. Il donne également une borne supérieure de $\frac{\pi}{4}$ plus fine[13] que les précédentes.
- `Ratan` : ce module démontre l'équivalence des définitions de la fonction arctan comme la réciproque de tan et comme la somme de la série d'arctan[14] et en déduit le résultat jusqu'alors posé en axiome : $\sin\left(\frac{\pi}{2}\right) = 1$.

L'ensemble de ces modules représente une centaine de lemmes pour environ 3250 lignes. Il reste encore deux lemmes à prouver (tous présents dans `Ratan`).

Troisième partie
Conclusions

13 Difficultés rencontrées

La démonstration assistée par ordinateur présente quelques inconvénients qui peuvent rendre le travail fastidieux. Le principal problème vient du fait que, contrairement aux démonstrations papier, il est impossible d'être elliptique.

13.1 Formulation des théorèmes à réinventer

Un même théorème formulé de deux manières différentes peut être soit dur, soit relativement facile à prouver et ce même lorsque seules des notions très simples sont utilisées. Formuler le théorème revient donc à faire une partie de la démonstration (il n'est d'ailleurs pas rare de retoucher l'énoncé au cours de la preuve d'un lemme intermédiaire afin de faciliter celle-ci).

On pourra par exemple essayer de démontrer que tout nombre pair appartient à $2 * \mathbb{N}$ en démontrant l'un des deux théorèmes suivants.

```
Lemma even_is_dble :
  forall n:nat,
  even n = true ->
  exist p:nat, n = 2*p.
```

Lemma `even_is_dble` : $\forall n \in \mathbb{N}$,
Si n est pair, alors :
$\exists p \in \mathbb{N}, n = 2p$.

```
Lemma nat_decomp :
 forall n:nat,
 (even n = true ->
  exist p:nat, n = 2*p)
 /\ (even n = false ->
  exist p:nat, n = 2*p+1).
```

Lemma `nat_decomp` : $\forall n \in \mathbb{N}$,
Si n est pair (resp. impair), alors :
$\exists p \in \mathbb{N}, n = 2p$ (resp. $2p+1$).

[12] Contrairement au lemme semblable déjà présent dans la bibliothèque standard.
[13] $\frac{\pi}{4} <= \frac{139}{160}$
[14] Les preuves de convergence et la définition de arctan sur $\mathbb{R}$ sont issues du travail de Guillaume Melquiond[16].

La seconde formulation facilite grandement la preuve : il n'y a plus qu'à faire une induction sur n pour obtenir le résultat. Le lemme `even_is_dble` prouvé afin de faciliter le raisonnement sur les sommes partielles de séries est d'ailleurs démontré en utilisant la première projection du lemme `nat_decomp`.

13.2 Lourdeurs du formalisme

Contrairement aux démonstrations mathématiques, la preuve assistée par ordinateur ne peut pas se permettre d'utiliser des énoncés elliptiques : tout doit être explicité. Cela peut allourdir considérablement les notations et rendre la manipulation de certains concepts fastidieuse.

Ainsi, en analyse réelle, on ne pourra jamais évoquer la dérivée d'une fonction sans fournir la preuve qu'elle est dérivable. Celle-ci pourra ne pas être explicité (idéal pour un travail général) mais introduite à l'aide d'un `forall`, elle n'en devra pas moins être présente (voir l'énoncé ci-dessous). C'est d'ailleurs dans la preuve de la dérivabilité d'une fonction que l'on va trouver la valeur de sa dérivée : la preuve de la dérivabilité construit la valeur.

```
Lemma derive_pt_recip_interv :
 forall (f g:R->R) (lb ub x;R)
 (Prf:derivable_pt f (g x))
 (Prg:derivable_pt g x),
 lb < ub -> lb < x < ub ->
 (forall x, lb < x < ub ->
   (comp f g) x = id x) ->
 derive_pt f (g x) Prf <> 0 ->
 derive_pt g x Prg
 =
 1 / (derive_pt f (g x) Prf).
```

Lemma `derive_pt_recip_interv` :
$\forall f, g : \mathbb{R} \to \mathbb{R}$,
$\forall lb, ub \in \mathbb{R}$,
$\forall x \in]lb; ub[$,
si $\begin{cases} f \circ g = id \text{ sur }]lb; ub[\\ f \text{ dérivable en } g(x), \\ g \text{ dérivable en } x, \\ \text{et } f'(g(x)) \neq 0 \end{cases}$
alors $g'(x) = \frac{1}{f'(g(x))}$

La lourdeur de ce formalisme est encore plus présente lorsqu'on ne quantifie pas universellement sur les preuves de dérivabilité.

La dérivabilité de la fonction réciproque est, par exemple, donnée par les mêmes hypothèses que celles utilisées pour donner la valeur de la dérivée. Lorsqu'on veut exprimer cette valeur on peut donc, au lieu de quantifier universellement sur les preuves de dérivabilité, fournir un témoin de cette dérivabilité en invoquant un lemme précédent et en lui appliquant les hypothèses appropriées. Le $\lambda-$terme peut alors être énorme si le découpage en lemmes préliminaires n'est assez astucieux.

13.3 Découpage d'un théorème en lemmes préliminaires

Étant donné que le formalisme de Coq impose de tout expliciter, la preuve d'un théorème non trivial devra être découpée en plusieurs lemmes préliminaires afin d'éviter une preuve gargantuesque. Il ne faut cependant pas tomber dans l'excés et découper systématiquement chaque preuve en une quinzaine de preuves triviales.

Exemple de découpage : voir le graphe de dépendance de la bibliothèque `Ranalysis5` en annexe (15).

14 Prolongements

14.1 Deux lemmes encore à démontrer

La preuve de $sin\left(\frac{\pi}{2}\right) = 1$ comporte encore deux lemmes admis. Leur démonstration n'a pas été implémentée par manque de temps lors du stage[15].

Le premier lemme devrait pouvoir être démontré en utilisant des outils de calcul réel non intégrés à la bibliothèque standard tandis que le second nécessitera plus de travail puisqu'il serait opportun d'utiliser un théorème plus général (non encore implémenté) permettant d'établir un lien entre dérivée de la limite d'une suite de fonction et limite de la suite dérivée.

14.1.1 $\sin\left(\frac{7}{8}\right) > \cos\left(\frac{7}{8}\right)$

```
Lemma sin_gt_cos_7_8 :
 sin (7 / 8) > cos (7 / 8).
```

Ce lemme doit pouvoir être démontré en utilisant l'outil `Gappa` ou le travail de Nicolas Julien[12] sur le calcul réel exact.

14.1.2 La série d'arctangente est dérivable entre 0 et 1

```
Lemma derivable_pt_lim_atanSeq_interv :
 forall x,
 0 <= x < 1 ->
 derivable_pt_lim atan x (/(1+x^2)).
```

La démonstration de ce résultat nécessite d'établir des relations entre la dérivée de la somme d'une série et la somme de la série des dérivées.

14.2 Généraliser les résultats

Les résultats concernant la dérivée de la réciproque n'ont été établis que pour des fonctions strictement croissantes. Il serait opportun de généraliser le résultat aux fonctions strictement monotones.

De la même manière, l'ensemble des théorèmes ont été établis pour des fonctions réciproques l'une de l'autre sur un intervalle. Le cas des fonctions réciproques l'une de l'autre sur $\mathbb{R}$ tout entier mériterait également d'être traité (les démonstrations établies peuvent être adaptées simplement).

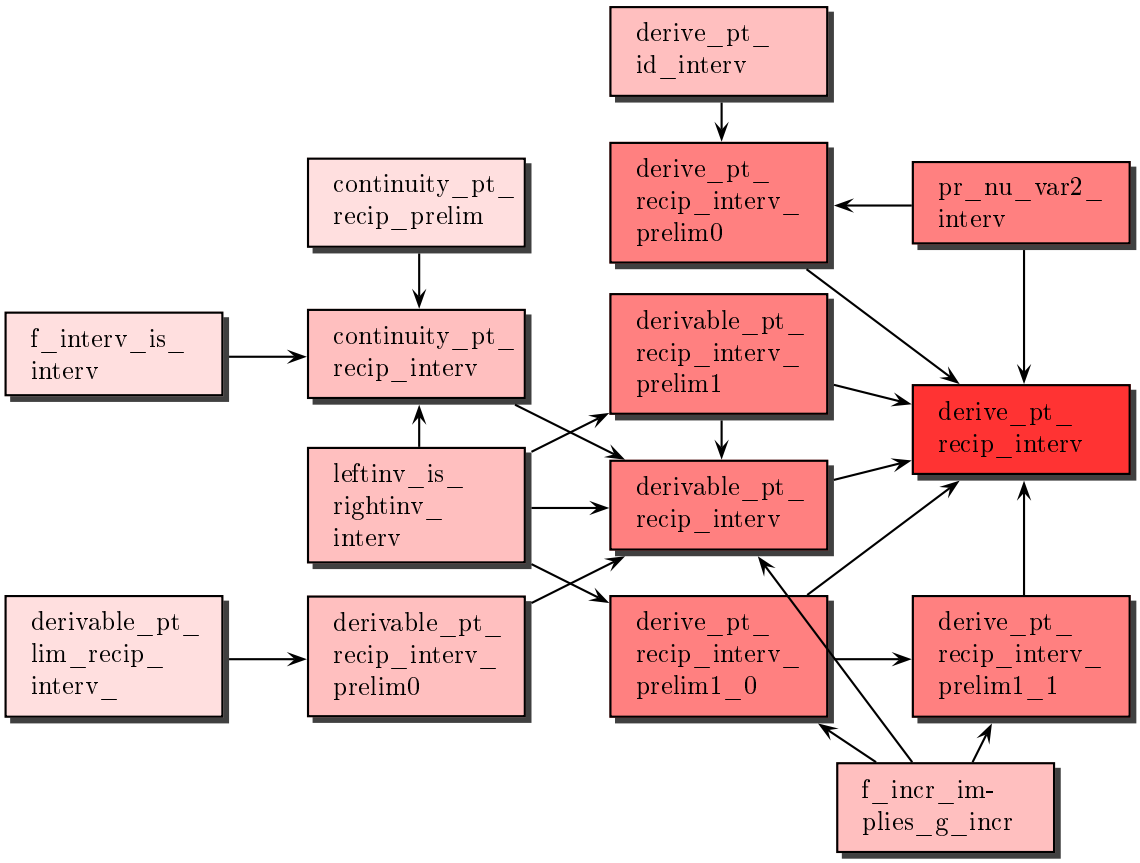
[15] Un troisième lemme manquait également à la fin du stage mais il a été démontré depuis : il s'agissait de prouver la continuité de la définition d'arctan utilisant les séries en 1. L'utilisation de la convergence uniforme des sommes partielles vers la fonction arctan sur $[0;1]$ permet une démonstration relativement rapide.

Quatrième partie

Annexes

15 Ranalysis5

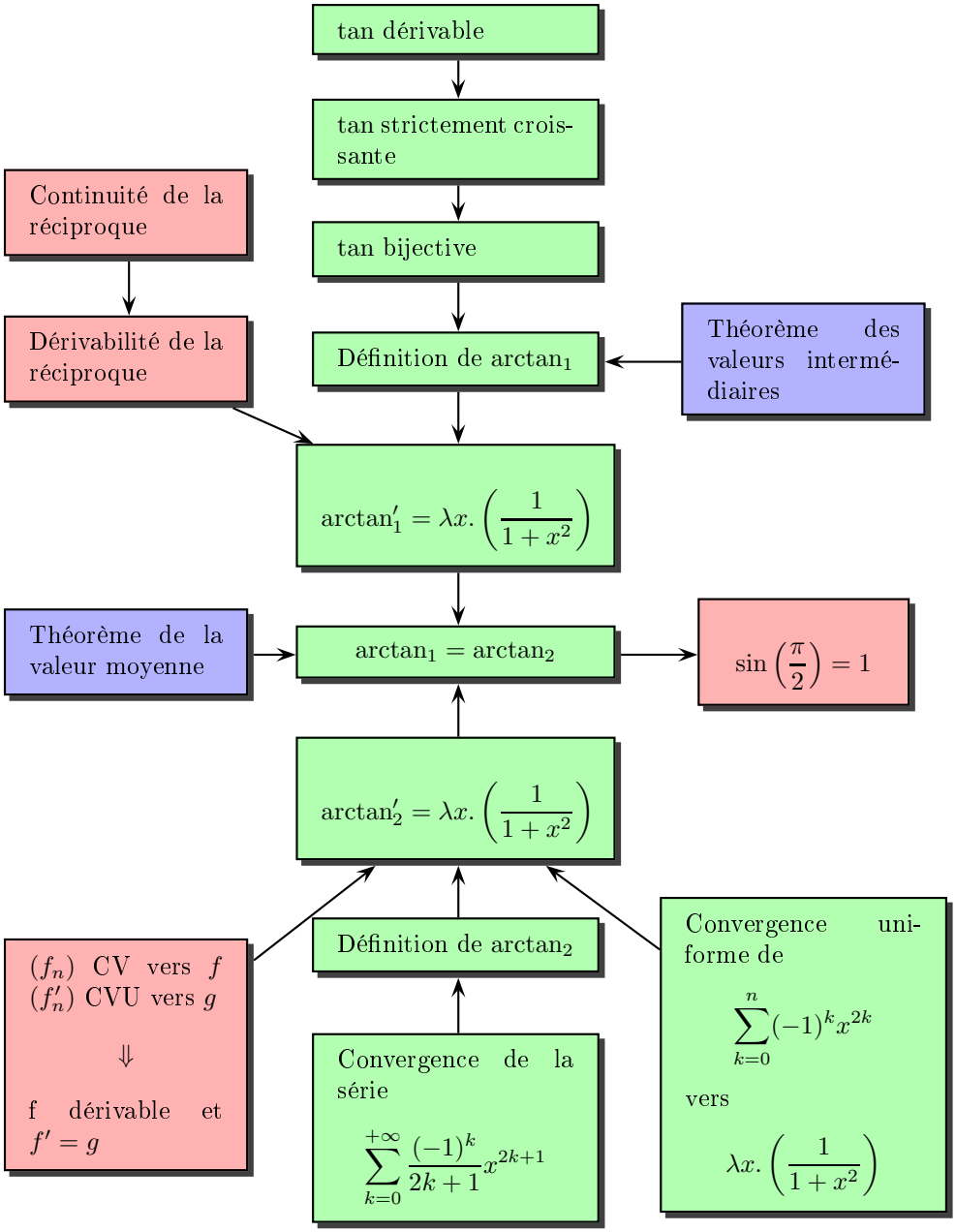
Le théorème qui a été à l'origine de la création de cette librairie est figuré en rouge vif. Les lemmes permettant sa démonstration sont d'une teinte plus ou moins foncée en fonction de leur proximité avec ce théorème.



16 Schéma de la preuve

Les résultats les plus généraux sont figurés en rouge, ceux existant déjà sont en bleu[16] et les lemmes traitant de cas particuliers sont figurés en vert.

[16] Des résultats de la bibliothèque standard sont utilisés pour démontrer des lemmes mais n'apparaissent pas sur ce diagramme car ils n'ont pas un statut particulier.

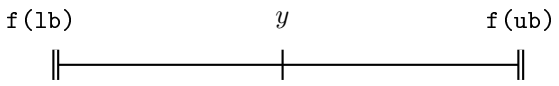


17 Continuité de la fonction réciproque

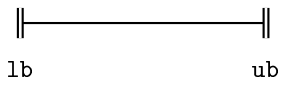
Soit y un réel quelconque de l'intervalle $]f(lb); f(ub)[$.

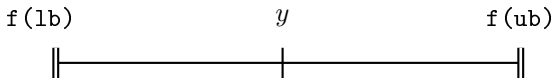
On introduit donc ϵ un réel positif et on cherche δ un réel positif tel que :

$$\forall h, |h| < \delta \Rightarrow \left|f^{-1}(y+h) - f^{-1}(y)\right| < \epsilon$$

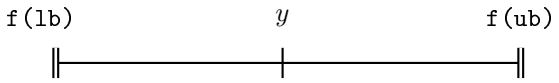


y est un point quelconque de l'intervalle $]f(lb); f(ub)[$.

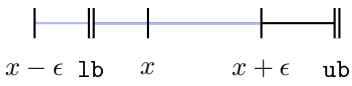


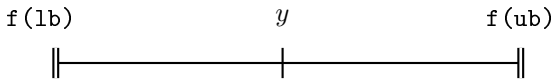


Il existe $x \in]lb; ub[$ tel que $y = f(x)$.

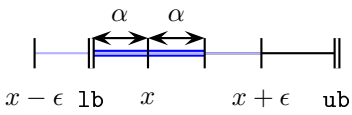


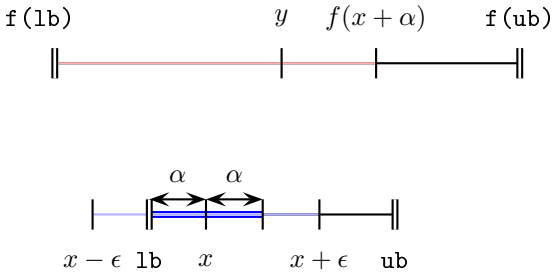
On cherche l'ensemble des points à distance ϵ de x.



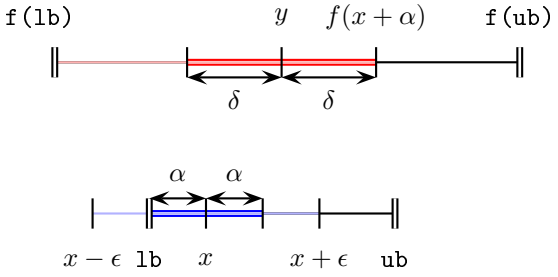


On définit α le rayon de l'intervalle de taille maximale centré sur x et inclus dans $]lb; ub[\cap]x - \epsilon; x + \epsilon[$.





On cherche l'intervalle image de $]x-\alpha; x+\alpha[$ par f.



On peut alors définir δ comme le rayon de l'intervalle de taille maximale centré sur y et inclus dans $]f(x-\alpha); f(x+\alpha)[$. On peut alors garantir qu'il permet de prouver que :

$$\forall h \in \mathbb{R}, |h| < \delta \Rightarrow$$

$$\left|f^{-1}(y+h) - f^{-1}(y)\right| < \epsilon$$

Cinquième partie

Références

Références

[1] Yves Bertot and Pierre Castéran. *Interactive Theorem Proving and Program Development, Coq'Art :the Calculus of Inductive Constructions*. Texts in Theoretical Computer Science. Springer-Verlag, 2004.

[2] The Coq Development Team. *The Coq Proof Assistant Reference Manual Version 8.2*. INRIA-Rocquencourt, December 2001.

[3] F. Dechesne. Archives automath. `http://www.win.tue.nl/automath/`.

[4] Bruno Dutertre. Elements of mathematical analysis in pvs. In *TPHOLs*, pages 141–156, 1996.

[5] Wikipédia (en). Automath. `http://en.wikipedia.org/wiki/Automath`, août 2009.

[6] Wikipédia (fr). Théorème d'inversion locale. `http://fr.wikipedia.org/wiki/Th%C3%A9or%C3%A8me_d%27inversion_locale`, juillet 2009.

[7] Ruben A. Gamboa and Matt Kaufmann. Nonstandard analysis in acl2. *J. Autom. Reason.*, 27(4) :323–351, 2001.

[8] Boris Gourévitch. Lien entre pi et suites récurrentes (démonstration). `http://www.pi314.net/fibonacci.php`, 2009.

[9] John Harrison. *Theorem Proving with the Real Numbers*. Springer-Verlag, 1998.

[10] John Harrison. Site officiel hol light. `http://www.cl.cam.ac.uk/~jrh13/hol-light/`, Mai 2008.

[11] INRIA. Site officiel coq. `http://coq.inria.fr/`, Mai 2009.

[12] Nicolas Julien. Certified exact real arithmetic using co-induction in arbitrary integer base. In *Functional and Logic Programming Symposium (FLOPS)*, LNCS. Springer, 2008.

[13] L. S. Van Benthem Jutting. Checking landau's grundlagen in the automath system. In *Selected papers on Automath*. 1994.

[14] Ron Knott. Lien entre pi et fibonacci. `http://www.mcs.surrey.ac.uk/Personal/R.Knott/Fibonacci/fibpi.html#gen`, 2007.

[15] J. Strother Moore Matt Kaufmann. Site officiel acl2. `http://www.cs.utexas.edu/users/moore/acl2/index.html`, Avril 2009.

[16] Guillaume Melquiond. `http://www.lri.fr/~melquion/`.

[17] Russel O'Connor. Site officiel c-corn. `http://c-corn.cs.ru.nl/`, 2009.

[18] Sam Owre. Site officiel pvs. `http://pvs.csl.sri.com/`, Avril 2009.

[19] Roy Ranjan. The discovery of the series formula for π by leibniz, gregory and nilakantha. *Mathematics Magazine*, 5 :291–306, 1990.

[20] Freek Wiedijk. Automath. `http://www.cs.ru.nl/~freek/aut/`, septembre 1999.