Vers une certification du DDMF

Assia Mahboubi

INRIA Microsoft Research Joint Centre (France)
INRIA Saclay – Île-de-France
Lix, École Polytechnique, Palaiseau

12 Juillet 2012

Rectificatif

En fait on ne va pas beaucoup parler du DDMF ici.

Motivations

On s'intéresse à la preuve formelle d'identités validées par les propriétés des (et les algorithmes associées à) la classe des fonctions D-finies et à la classe des suites P-récursives.

Exemples:

$$arcsin(X)^2 = \sum_{k\geq 0} \frac{k!}{\frac{1}{2}\ldots(2k+\frac{1}{2})} \frac{X^{2k+2}}{(2k+2)}$$

$$F_{n+2}F_n - F_{n+1}^2 = (-1)^n$$

$$\sum_{k\in\mathbb{Z}} \binom{a+b}{a+k}\binom{a+c}{c+k}\binom{b+c}{b+k} = \frac{(a+b+c)!}{a!b!c!}$$

Série formelle D-finie

Soit $\mathbb{K}[[X]]$ l'anneau des séries formelles à coefficients dans $\mathbb{K}$.

$$A(X) \in \mathbb{K}[[X]] \Leftrightarrow A(X) = \sum_{k=0}^{+\infty} a_k X^k \quad avec \quad \forall k, a_k \in \mathbb{K}$$

La dérivée formelle est définie par:

$$A'(X) := \sum_{k=0}^{+\infty} (k+1) a_{k+1} X^k \in \mathbb{K}[[X]]$$

Une série formelle est D-finie si ses dérivées successives $A, A', \ldots, A^{(m)}, \ldots$ forment un espace vectoriel de dimension finie sur $\mathbb{K}(X)$.

$$\Leftrightarrow$$

A est solution d'une équation différentielle linéaire à coefficients des fractions rationnelles en $\mathbb{K}(X)$.

Suite P-récursive

Une suite $u := (u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ est dite P-récursive si elle est solution d'une récurrence linéaire à coefficients dans $\mathbb{K}[n]$.

Exemples: $F_{n+2} = F_{n+1} + F_n$, $\quad nu_{n+2} - (n^2 + 100)u_{n+1} - u_n = 0$

Dans le cas particulier où la récurrence est d'ordre 1 (et $u_0 \neq 0$) on dit que u est hypergéométrique.

Exemple: $(n+1)u_{n+1} = nu_n$

Remarque: une série est D-finie si et seulement si son terme général est une suite P-récursive.

Remarques élémentaires

Ces deux classes d'équations fonctionnelles imposent une structure d'espace vectoriel de dimention finie à l'espace de leur solutions.

Par exemple, pour prouver l'égalité de deux objets dans l'une de ces classes il "suffit" de:

- Trouver une équation annulatrice commune;
- Vérifier que les deux objets coïncident sur un ensemble de conditions initiales suffisantes.

Notations

Définissons:

- un operateur de décalage $S_n : (u_n) \mapsto (u_{n+1})$.
- un opérateur de multiplication $n\cdot\ (u_n) \mapsto (nu_n)$

Une récurrence linéaire avec des coefficients polynomiaux peut être vue comme un polynôme (non commutatif) annulateur en ces opérateurs:

$$(n+3)u_{n+2} + n^2 u_{n+1} + 3u_n = 0$$

devient :

$$P(u) = 0 \quad \text{with } P := (n+3)S_n^2 + n^2 S_n + 3$$

Si (u_{nk}) dépend de plusieurs indices, on pourra utiliser les analogues S_k et $k\cdot$ pour ces autres indices.

Exemples d'algorithmes

Preuves formelles et calcul formel

On voudrait pouvoir produire des preuves formelles (Coq) de correction des identités que ces algorithmes permettent d'établir. Et on a de la chance :

- Ces propriétés (et surtout les algorithmes associés (et bien d'autres)) sont implantés, en particulier dans la bibliothèque Algolib.
- On peut donc exploiter le résultat des calculs quand il est plus facile à certifier que l'algorithme qui l'a produit.

Exemple: clôture par produit

Trouver une équation différentielle qui annule $arcsin(X)^2$:

- Ma définition de *arcsin* :
  la solution de $(1-X^2)y'' - Xy' = 0$ telle que $y(0) = 0$ et $y'(0) = 1$.
- Posons $h := y^2$ et dérivons:
  - $h' = 2yy' \in Ev_{\mathbb{Q}(X)}(yy')$
  - $h'' = 2y'^2 + 2yy'' = 2y'^2 + \frac{2X}{1-X^2}yy' \in Ev_{\mathbb{Q}(X)}(yy', y'^2)$
  - $h''' = 4y'y'' + \frac{2X}{1-X^2}(y'^2 + \ldots yy'') + \cdots = \cdots \in Ev_{\mathbb{Q}(X)}(yy', y'^2)$

$\Rightarrow h', h'', h'''$ sont combinaisons linéaires à coefficients dans $\mathbb{Q}(X)$ de yy', y'^2

$\Rightarrow \exists A \in M_{3,2}(\mathbb{Q}(X))$ telle que $A\mathbf{y} = \mathbf{h}$ avec $\mathbf{h} := (h', h'', h''')^t$ et $\mathbf{y} := (yy', y'^2)^t$.

Exemple: clôture par produit

Trouver une équation différentielle qui annule $arcsin(X)^2$:

- Ma définition de *arcsin* :
  la solution de $(1 - X^2)y'' - Xy' = 0$ telle que $y(0) = 0$ et $y'(0) = 1$.
- On a posé $h := y^2$
- On a trouvé $A \in M_{4,3}(\mathbb{Q}(X))$ telle que $A\mathbf{y} = \mathbf{h}$ avec $\mathbf{h} := (h', h'', h''')$.
- Si on trouve $u \in ker\ A^t$, alors :

$$u^t\mathbf{h} = u^tA\mathbf{y} = (A^tu)^t\mathbf{y} = 0$$

- $u^t\mathbf{h}$ est l'équation cherchée :

$$(1 - X^2)h''' - 3Xh'' - h' = 0$$

Exemple: clôture par produit

Prouver en Coq que l'équation différentielle $u^t\mathbf{h}$ annule $arcsin(X)^2$, avec $\mathbf{h} := (h', h'', h''')$:

- On doit prouver que $A\mathbf{y} = \mathbf{h}$ avec $\mathbf{y} := (y^2, yy', y'^2)$ et $h = y^2$:
  C'est de la normalisation d'expressions différentielles modulo l'équation connue pour y (+ formulaire).
- On laisse un oracle externe trouver un candidat u.
- On vérifie en Coq que $A^t u = 0$:
  C'est de la normalisation certifiée dans un anneau.

Exemple: création télescopique

On veut étudier $U_n := \sum_{k=0}^{n} u_{nk}$ avec (u) hypergéométrique (et même un peu plus).

Supposons qu' on obtient deux opérateurs linéaires sur les suites P et Q tels que:

$$P(u) - (S_k - 1)Q(u) = 0$$

avec S_k l'opérateur de décalage en k.
Par linéarité, on en déduit :

$$P(U)_n - \sum_{k=0}^{n} [(S_k - 1)Q(u)]_{nk} = 0$$

Exemple: création télescopique

On veut étudier $U_n := \sum_{k=0}^{n} u_{nk}$ avec (u) hypergéométrique (et même un peu plus).

On a obtenu : $P(U)_n - \sum_{k=0}^{n}[(S_k - 1)Q(u)]_{nk} = 0$

Alors il y a téléscopage:

$$\sum_{k=0}^{n}[(S_k - 1)Q(u)] = [Q(u)]_{n,n+1} - [Q(u)]_{n,0}$$

et $P(U)_n = [Q(u)]_{n,n+1} - [Q(u)]_{n,0}$

Si on peut montrer que le membre droit est nul, alors $P(U) = 0$ est une récurrence satisfaite par U et certifiée par Q.

Vérification d'un téléscope

- On part de (u_n) connu comme solution d'un ensemble $\mathcal{S}$ de récurrences:

  Exemple: $\binom{n+1}{k} = \frac{n+1}{n+1-k}\binom{n}{k}$ et $\binom{n}{k+1} = \frac{n-k}{k+1}\binom{n}{k}$
- Maple invente deux opérateurs P et Q.
- On vérifie que (u_n) satisfait:

$$\forall n, (P - (S_k - 1)Q)(u)_n = 0$$

  par normalisation modulo $\mathcal{S}$ et normalisation dans un anneau.
- On utilise un lemme général qui prouve le télescopage pour prouver l'identité $P(U)_n = [Q(u)]_{n,n+1} - [Q(u)]_{n,0}$.
- On peut prouver que ce qui reste de Q après le téléscopage est 0 par exemple par une propriété de clôture.

Ingrédients d'une formalisation en Coq

- Choisir des structures de données appropriées pour les objets (polynômes, récurrences, coefficients,...);
- Utiliser Maple pour générer les objets difficiles à calculer;
- Implémenter des stratégies de normalisation certifiées appropriées.

Ce qui reste flou, au moins pour moi

- Nombres réels, nombres complexes (ces derniers ne sont pas disponibles)
- Généralisation au cas multivarié (les normalisations sont moins évidentes à comprendre)
- Analogue différentiel (convergence des intégrales)
- Propriétés asymptotiques des solutions d'une équation différentielle (à formaliser...)

Projets reliés

- Tamadi
- CoqInterval
- Coqlicot
- Coqeal
- ?

Résultats attendus

- Outils de validation automatique et certifiée d'identités;
- Bibliothèque standardisée de fonctions mathématiques pour Coq;
- Connexion avec les efforts de certification des aspects numériques.