Langues et dictionnaires en informatique, en mathématiques, et au-delà

Pierre-Louis Curien
Directeur de recherche CNRS émérite
Picube, IRIF (INRIA, Université Paris Cité, CNRS)

25 avril 2022, Université de Haute Alsace

Résumé

L'informatique a ses langages de programmation, et ses dictionnaires entre le "haut niveau" (l'utilisateur) et le "bas niveau" (la machine).

Les mathématiques, quant à elles, sont écrites avec un mélange de symboles et de phrases "informellement" écrites dans la langue usuelle. Elles ont également leurs dictionnaires: entre domaines des mathématiques comme l'algèbre et la géométrie, ou, ce qui revient souvent au même, entre différentes manières de voir les mêmes objets.

Il y a aussi des (projets de) dictionnaires pour transformer la langue des mathématiciens en une langue entièrement formelle, vérifiable par l'ordinateur, par le truchement des assistants de preuve (qui servent aussi bien à vérifier des démonstrations de théorèmes complexes qu'à certifier des logiciels, et en particulier des logiciels critiques).

J'essaierai de montrer que l'attention portée à une belle écriture joue un rôle important dans ces deux sciences, au confluent desquelles se situe ma recherche; et donc, en quelque sorte, que la littérature s'y invite.

Dans tous les sens, dites-vous?

Vous me permettrez ici de prendre la partie “dans tous les sens” du titre de ce colloque dans un sens assez littéral. J’ai mis dans un bocal quelques idées, agrémentées de quelques particularités de ce qui a constitué ma propre personnalité au cours du temps, j’ai secoué le récipient, et ce qui suit en est le produit...

Dans ce qui suit, il sera beaucoup question de dictionnaires ou de traduction, que je considèrerai ici comme synonymes. Donc pour moi, le mot dictionnaire ne se résume pas à

$$\text{Wahlverswandshaften} \rightarrow \text{affinités électives}$$

mais s’étend aussi à

Goethe’s Wahlverswandshaften gehörten
zu den auffälligsten meiner Jugendlektüren

$$\downarrow$$

Les Affinités électives de Goethe ont été
parmi mes lectures de jeunesse les plus marquantes

Langage de haut niveau

Allons faire un tour à Syracuse, New York, où se répandit au milieu XXème siècle une

Conjecture. Le programme qui suit est correctement défini (appliqué à un nombre entier > 0):

$$\texttt{Syracuse}(n) = \begin{cases} \texttt{Syracuse}(n/2) & \text{si } n \text{ est pair} \\ \texttt{Syracuse}(3n+1) & \text{si } n \text{ est impair et différent de 1} \\ 1 & \text{si } n = 1 \end{cases}$$

et, de plus, on a $\texttt{Syracuse}(n) = 1$ pour tout n.

Essayons! $\texttt{Syracuse}(5) = \texttt{Syracuse}(16) = \texttt{Syracuse}(8) = \texttt{Syracuse}(4) = \texttt{Syracuse}(2) = \texttt{Syracuse}(1) = 1$

Peut-être était-ce un coup de chance? $\texttt{Syracuse}(11) = \texttt{Syracuse}(34) = \texttt{Syracuse}(17) = \texttt{Syracuse}(52) = \texttt{Syracuse}(26) = \texttt{Syracuse}(13) = \texttt{Syracuse}(40) = \texttt{Syracuse}(20) = \texttt{Syracuse}(10) = \texttt{Syracuse}(5)$, et on sait déjà que $\texttt{Syracuse}(5) = 1$.

Çà commence à devenir plausible! Eh bien, ceci est encore une conjecture aujourd'hui.

Langage impératif

Le style du programme, dit "fonctionnel" (car on y programme des fonctions), que nous avons écrit est proche des mathématiques. Un style plus traditionnel serait le suivant:

$$
\begin{array}{l}
\texttt{syracuse} := n; \\
\texttt{while n} \neq 1 \texttt{ do } \ (\texttt{if even(syracuse)} \\
\quad \texttt{then syracuse} := \texttt{syracuse}/2 \\
\quad \texttt{else syracuse} := (3 \times \texttt{syracuse}) + 1)
\end{array}
$$

Quand le programme s'arrête, on consulte la case mémoire `syracuse`, et l'on y trouve 1.
Ce style de programmation est plus proche de ce qui se passe réellement dans l'exécution sur une machine.
On a ainsi une chaîne de compilation (= traduction)

$$\text{langage fonctionel} \to \text{langage impératif} \to \cdots \to \text{langage machine}$$

A quoi ressemble le langage machine?

Langage machine

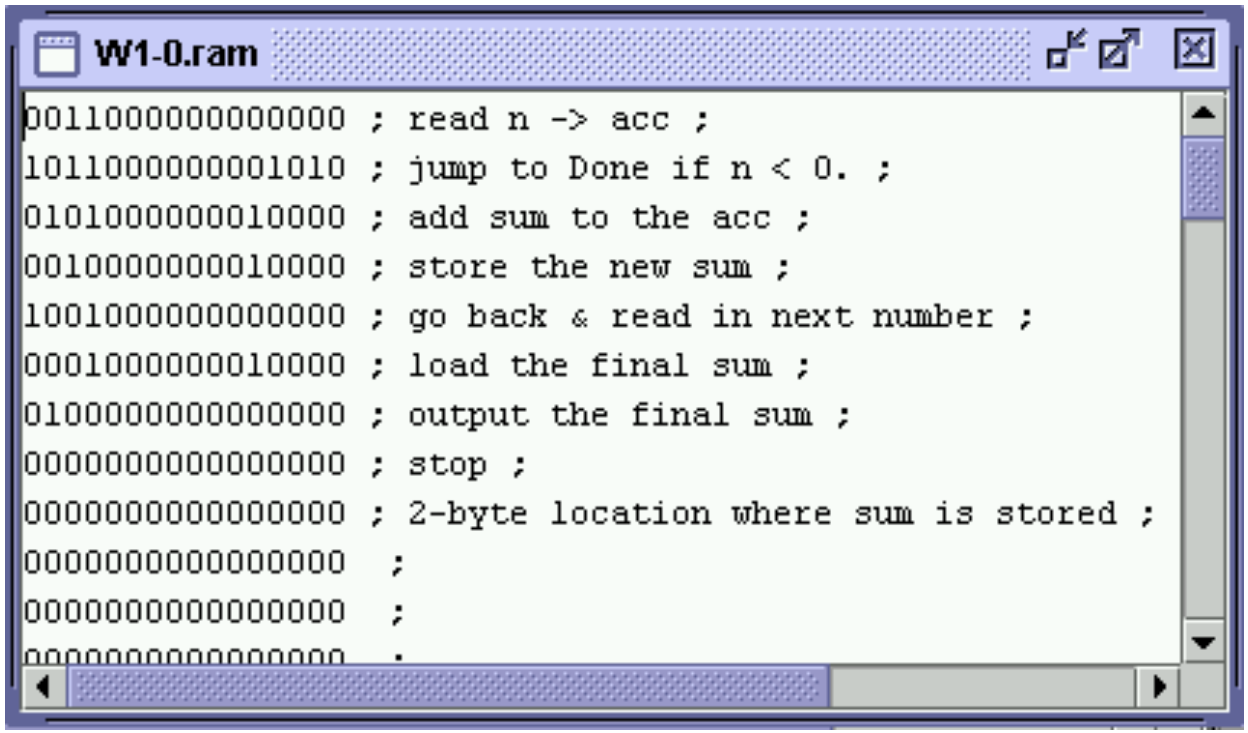


Figure 6. A simple machine language program.

Pas terrible pour les humains...

Les programmes et les preuves, les types et les formules

Autre dictionnaire fondamental pour l'informatique: les programmes "sont" des preuves mathématiques (entièrement explicites et formalisées), et les types "sont" des énoncés mathématiques, qui eux-mêmes peuvent s'écrire comme des formules logiques.

Mais qu'est-ce qu'un type?

- $4 : \texttt{nat}$
- $(4, 5) : \texttt{nat} \times \texttt{nat}$
- $\texttt{Syracuse} : (\texttt{nat} \setminus \{0\}) \to \texttt{nat}$

Voici la base de ce dictionnaire:

$$(A \times B) \leftrightarrow (A \text{ et } B) \qquad (A \to B) \leftrightarrow (A \text{ implique } B)$$

Plus difficile:

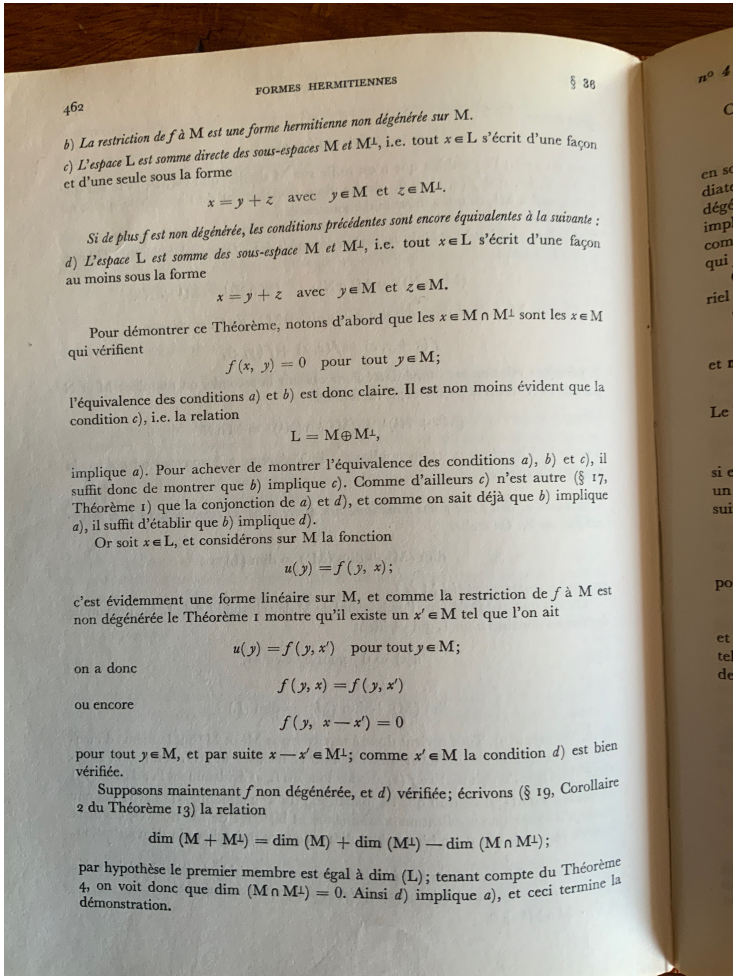
$$\texttt{nat} \leftrightarrow (\forall X\ X \to ((X \to X) \to X))$$

Quand on feuillette un livre de mathématiques, on trouve ...

- Du texte écrit en français, allemand, russe, ou, de nos jours (pour ce qui est des travaux de recherche) principalement (voire exclusivement) en anglais
- Des formules ou des équations
- Des figures

Cours d'algèbre de Godement

Une référence pour la rédaction mathématique!



462 FORMES HERMITIENNES § 36

b) La restriction de f à M est une forme hermitienne non dégénérée sur M.

c) L'espace L *est somme directe des sous-espaces* M *et* $M^\perp$, i.e. tout $x \in L$ s'écrit d'une façon et d'une seule sous la forme

$$x = y + z \quad \text{avec} \quad y \in M \quad \text{et} \quad z \in M^\perp.$$

Si de plus f est non dégénérée, les conditions précédentes sont encore équivalentes à la suivante :

d) L'espace L *est somme des sous-espace* M *et* $M^\perp$, i.e. tout $x \in L$ s'écrit d'une façon au moins sous la forme

$$x = y + z \quad \text{avec} \quad y \in M \quad \text{et} \quad z \in M.$$

Pour démontrer ce Théorème, notons d'abord que les $x \in M \cap M^\perp$ sont les $x \in M$ qui vérifient

$$f(x, y) = 0 \quad \text{pour tout } y \in M;$$

l'équivalence des conditions *a)* et *b)* est donc claire. Il est non moins évident que la condition *c)*, i.e. la relation

$$L = M \oplus M^\perp,$$

implique *a)*. Pour achever de montrer l'équivalence des conditions *a)*, *b)* et *c)*, il suffit donc de montrer que *b)* implique *c)*. Comme d'ailleurs *c)* n'est autre (§ 17, Théorème 1) que la conjonction de *a)* et *d)*, et comme on sait déjà que *b)* implique *a)*, il suffit d'établir que *b)* implique *d)*.

Or soit $x \in L$, et considérons sur M la fonction

$$u(y) = f(y, x);$$

c'est évidemment une forme linéaire sur M, et comme la restriction de f à M est non dégénérée le Théorème 1 montre qu'il existe un $x' \in M$ tel que l'on ait

$$u(y) = f(y, x') \quad \text{pour tout } y \in M;$$

on a donc

$$f(y, x) = f(y, x')$$

ou encore

$$f(y, x - x') = 0$$

pour tout $y \in M$, et par suite $x - x' \in M^\perp$; comme $x' \in M$ la condition *d)* est bien vérifiée.

Supposons maintenant f non dégénérée, et *d)* vérifiée; écrivons (§ 19, Corollaire 2 du Théorème 13) la relation

$$\dim(M + M^\perp) = \dim(M) + \dim(M^\perp) - \dim(M \cap M^\perp);$$

par hypothèse le premier membre est égal à dim (L); tenant compte du Théorème 4, on voit donc que dim $(M \cap M^\perp) = 0$. Ainsi *d)* implique *a)*, et ceci termine la démonstration.

Les formules

$\forall m, n \ \exists q, r \ \ (r < n) \wedge (m = qn + r)$
pour tout m, n, il existe q, r tels que $r < n$ et $m = qn + r$

Les formules n'ont fait qu'une apparition récente dans l'écriture mathématique: la logique mathématique est née seulement au début du XXème siècle. La logique a rendu de grands services en assurant des fondations solides aux mathématiques (crise des paradoxes dans les années 1920).

Elle a aussi montré les limites du pouvoir des mathématiques (théorèmes d'incomplétude de Gödel). Quelle que soit la puissance expressive d'un système logique, il y aura toujours des énoncés dont il est impossible de prouver dans ce système s'ils sont vrais ou faux.

(Une image pour comprendre l'incomplétude: pour réparer ses propres lunettes, il faut avoir une autre paire de lunettes...)

Le rôle des figures

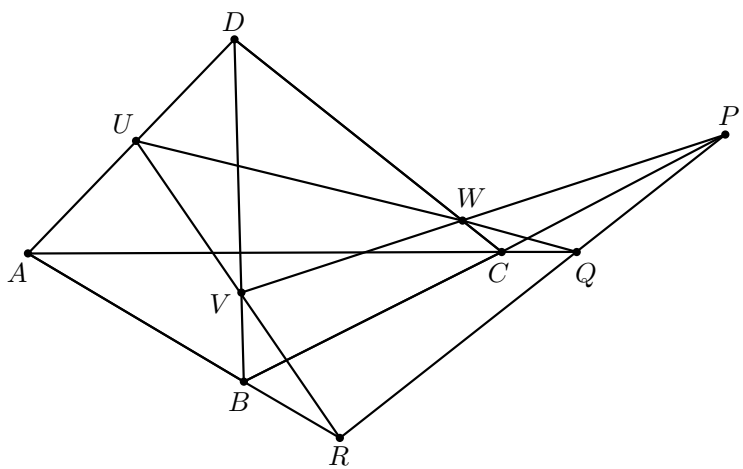
En dehors des formules et des phrases en langue naturelle, un texte mathématique (surtout s'il touche à la géométrie) peut aussi comprendre des figures. Mais il y a une longue histoire de méfiance (ou de distance) des mathématiciens à l'encontre des figures. Et pour de bonnes raisons.

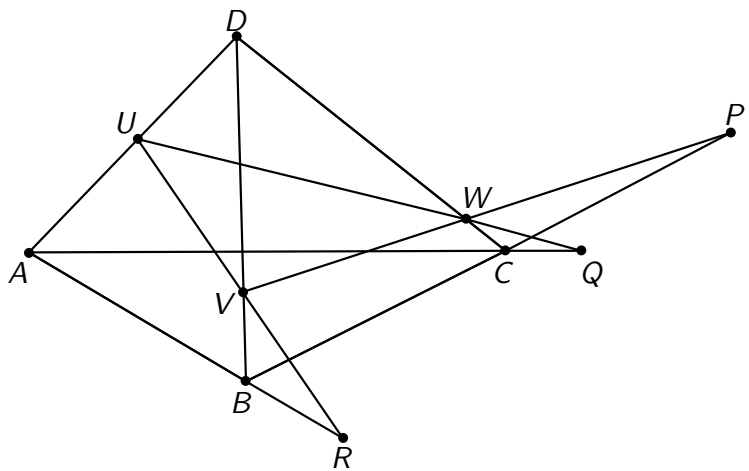
- Une figure est synthétique, et peut s'analyser/décomposer de différentes manières (ce qui pose souvent des problèmes mathématiques intéressants de cohérence).
- Certains ouvrages de géométrie du 19ème siècle (qui a vu fleurir la géométrie projective) n'incluent pas de figures, et laissent le soin au lecteur de les construire pas-à-pas.

Et pourtant une discussion entre mathématiciens se déroule généralement devant un tableau (voir plus loin!), sur lequel on dessine des figures. Anectode que je tiens de quelqu'un qui le tient de quelqu'un qui assistait à un exposé d'un membre du groupe Bourbaki: l'orateur, ayant perdu le fil de son exposé, griffonne une figure en la cachant à l'auditoire puis, ayant recouvré ses esprits grâce au dessin, reprend son exposé (sans figure).

Le théorème de Desargues (1591-1661)

Le piège d'une figure. Que veut dire la figure de gauche? Celle de droite l'explique, par ce qui lui manque! Si l'on a A, B, C, D, et U, V, W, P, Q, R chacun situé sur l'une des 6 droites supportant les côtés du tétraèdre $ABCD$ et tels que V, W, P (resp. U, W, Q, resp. U, V, R) sont alignés, alors P, Q, R sont alignés.





Mais la figure de gauche dit plus que celle de droite. Il y a quatre triplets de points. Il suffit que trois triplets témoignent chacun d'un alignement pour qu'il en soit de même du dernier.

Ménélaüs d'Alexandrie (70–140)

Pour prouver cet énoncé, on fait appel à un dictionnaire, fourni par le théorème de Ménélaüs.
Simplifions encore la figure de droite, en ne considérant plus que le triangle ABC, P sur BC, Q sur AC, R sur AB (ici tous en dehors des segments respectifs). Chacun détermine une quantité (rapport des distances):

$$BP/CP \quad \text{resp. } CQ/AQ, AR/BR$$

affectée d'un coefficient (-1 pour "en dehors", $+1$ pour "situé sur").

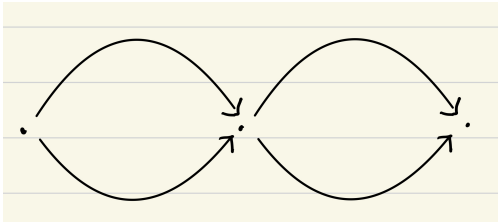
Théorème (Ménélaüs). P, Q, R sont alignés si et seulement si le produit de ces trois quantités est égal à -1.

Ce théorème permet de traduire le problème géométrique (Desargues) en un problème de manipulation d'expressions (des produits), que l'on résout aisément, et en appliquant Ménélaüs en sens inverse, on achève la démonstration du théorème de Desargues.

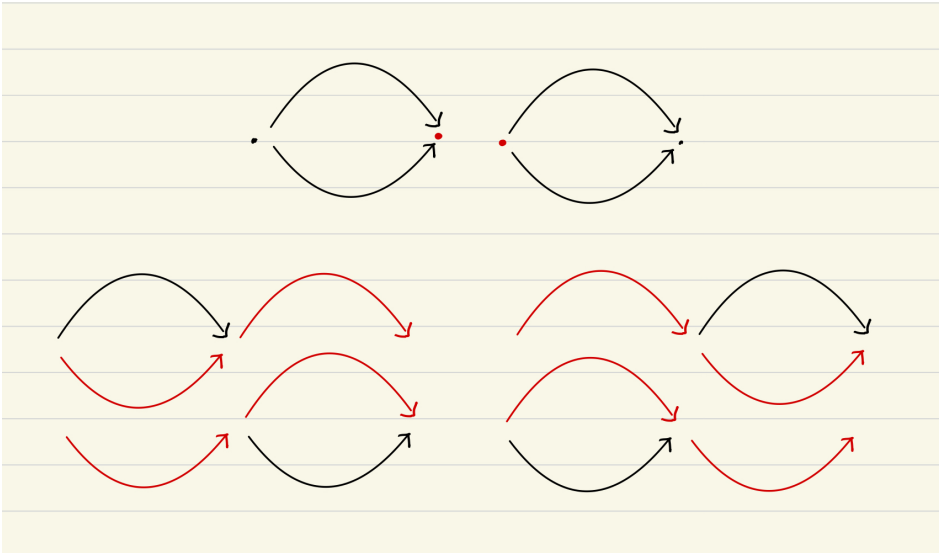
Ce dictionnaire particulier continue et s'étend en direction des surfaces triangulées et de leur homologie...

Pasting diagrams

La figure suivante



peut se lire/décomposer de trois manières:



La transcription algébrique précise de l'indifférence entre ces trois manières de voir conduit à la définition d'une structure algébrique, appelée 2-catégorie.

Tempête sous un crâne

• 1991: deux mathématiciens russes, Mikhail Kapranov et Vladimir Voevodsky, publient un article (∞-groupoids and homotopy types).

• 1998: un mathématicien américain, Carlos Simpson, publie un contre-exemple au résultat prouvé dans cet article.

• Souvenirs de Voevodsky: "I was busy with the work on the motivic program [pour lequel il obtient la médaille Fields en 2002[1]] and very sure that our proof is correct and ignored the preprint[2]."

• Dans les années 2000, Voevodsky (prémonition?) s'intéresse à la preuve assistée par ordinateur, et commence à travailler sur la théorie homotopique des types. "The correspondence between the infinity groupoids and homotopy types reemerged as the cornerstone [de ce nouveau programme]. And then in the Fall of 2013, some sort of a block in my mind collapsed and I suddenly understood that Carlos Simpson was correct."

[1] Pour des travaux sans lien avec cet article: ouf!

[2] https://www.math.ias.edu/vladimir/sites/math.ias.edu.vladimir/files/2014_08_ASC_lecture.pdf.

Les assistants de preuve

Un assistant de preuve est un outil logiciel interactif de développement de preuve formelle. L'utilisateur entre un énoncé à prouver, puis, progressivement, les étapes de son raisonnement, en spécifiant les règles logiques utilisées, les résultats intermédiaires utilisés (eux-même vérifiés interactivement ...). L'ordinateur approuve (ou non), et le tient à jour de ce qui est déjà prouvé et de ce qui reste à prouver.

La preuve est terminée par un magique QED (quid erat demonstrandum) renvoyé par la machine lorsqu'il n'y a plus rien à vérifier et toutes les étapes ont été validées.

Logiciels: Coq ("made in France", depuis 1989), Lean (inspiré de Coq)...

- Certification des logiciels: projet CompCert ("Comp" pour compilation), projet DeepSpec (encore plus loin vers le hardware)
- Certification mathématique: du théorème des 4 couleurs, de la classification des groupes finis, des perfectoïdes de Scholze (médaille Fields 2018)

Types, formules, structures mathématiques, espaces

Au cours des 40 dernières années, la correspondance "formulas as types" de tout à l'heure (Curry-Howard) s'est complétée:

• d'abord par les lumières de la théorie des catégories (branche de l'algèbre qui promeut les morphismes entre structures (fonctions les préservent) avant les structures elles-mêmes) (Curry-Howard-Lambek): "types as objects, programs as morphisms".

• ensuite, depuis une quinzaine d'années, par la théorie de l'homotopie (étude des espaces topologiques à déformation près) (Curry-Howard-Lambek-Voevodsky): "types as spaces".

Le dictionnaire s'est agrandi!

Un objet mathématique non identifié

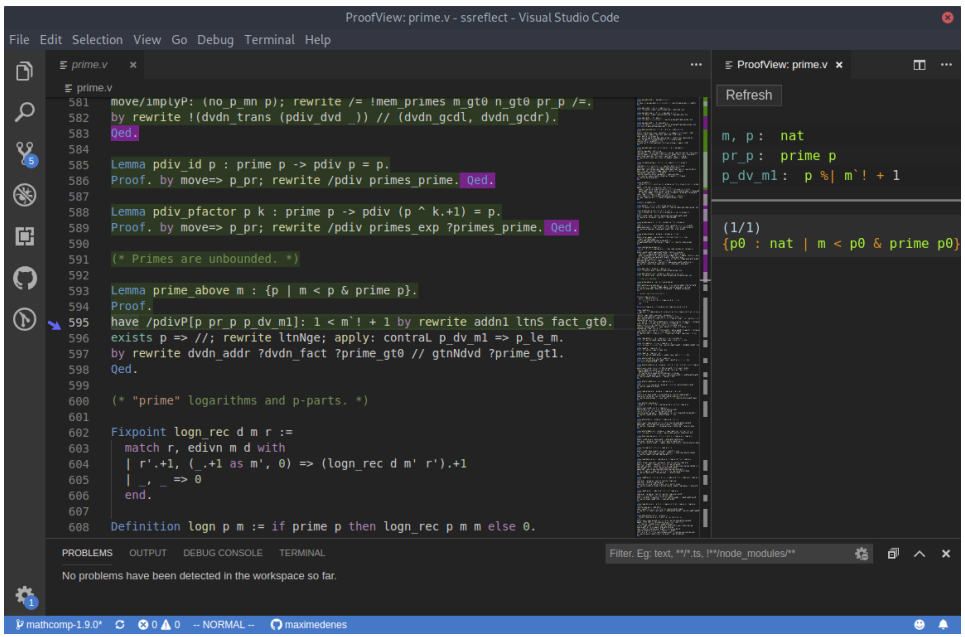
"Quitte à prendre le risque d'une généralisation forc(en)ée, les mathématiciens sont souvent des êtres solitaires qui, du fond de leur bureau, écrivent seuls des textes d'ampleur variable. [...] En juin dernier [2013], débarquait sur la planète maths un omni (objet mathématique non identifié) : 600 pages écrites de façon collective en 6 mois par 40 scientifiques de tous âges, originaires de toute la planète, sur un sujet de recherche essentiellement neuf [...], qui ont saisi l'occasion [de l'année spéciale "Univalent foundations of mathematics", Institute for Advanced Study, 2012/2013] [...] pour nous livrer un gros et fascinant livre[3] qui synthétise leurs progrès. [...] Ils se sont appuyés sur les nouvelles technologies collaboratives d'usage courant en logiciel libre [site web, blog, logiciel de contrôle de versions distribué git][4]."

[3] The HoTT book, `https://homotopytypetheory.org/book`

[4] Antoine Chambert-Loir, À la croisée des fondements des mathématiques, de l'informatique et de la topologie, Images des Mathématiques, CNRS, 2013.

Assistants, dites-vous?

Une session en Coq ne ressemble pas à la langue utilisée dans la littérature mathématique (et encore moins à celle, épurée et “littéraire”, de Godement).



Il y a un défi majeur à relever pour répandre massivement ces outils dans la communauté mathématique: “parler” à l’ordinateur directement dans la langue des mathématiciens (haut niveau). Les outils de l’intelligence artificielle (deep learning) seront utiles!

La notion d'élégance

Qu'est-ce qu'une preuve élégante?

- Clarté, structuration (placer les hypothèses au bon endroit, niveau de généralité adapté à la chose prouvée)
- Rapprochements inattendus
- Pas ennuyeuse
- Rapproche l'idée intuitive du traitement formel

$\vdots$

La notion de style

• Le choix des notations: $\forall$ (All) et $\exists$ (Exists), $\int$, ∇..

• Le choix d'un nom pour une notion. Jeune doctorant (1978), j'étais en quête d'un nom pour les objets que j'avais mis à jour: des fonctions munies d'une stratégie d'ordonnancement pour leur calcul. Mon directeur de thèse, installé dans sa position favorite (étendu à plat ventre sur le sol ... et donc moi aussi) réfléchit et me dit: "tu devrais les appeler algorithmes séquentiels": ma thèse venait de gagner son titre!

• Les images utilisées pour expliquer les idées...

Un menu logique

Voici ce qu'un de mes collègues, Yves Lafont, avait trouvé pour expliquer certaines idées à l'œuvre dans un système logique appelé logique linéaire (Jean-Yves Girard):

Menu (price 17 Euros)

Quiche or Salad
Chicken or Fish
Banana or "Surprise du Chef"*

$$17E \vdash \left\{ \begin{array}{c} (Q \& S) \\ \otimes \\ (C \& F) \\ \otimes \\ (B \& (P \oplus T)) \end{array} \right.$$

(*) either "*Profiteroles*" or "*Tarte Tatin*"

Par exemple, il y a deux sortes de choix (conduisant à des règles logiques différentes):

- celui du client (le programme): quiche ou salade
- celui du chef (son environnement): profiteroles ou Tatin

La notion de conviction

Il est rare que les démonstrations soient entièrement vérifiées par beaucoup de personnes (parfois même par les auteurs eux-mêmes...) “Il est facile de voir que ...”.

C’est souvent un processus complexe de discussions entre mathématiciens qui emporte la conviction: “ah oui, c’était bien le chemin qu’il fallait prendre, il évite l’écueil sur lequel j’étais moi-même tombé”.

Ce qui parfois nous ramène à la case “tempête sous un crâne”!

Différentes formes d'esprit

- Le laboureur obsessionnel
- Le rapide et le lent
- Le "problem-solver"
- Le génie bouillonnant touche à tout
- Le créateur (et sa part de folie)
- Un petit grain d'espièglerie

Sérendipité

Mon itinéraire m'a amené, de proche en proche, sans que j'aie rien prévu du parcours:

- des modèles mathématiques des langages de programmation à la théorie des catégories. Les algorithmes séquentiels fraîchement nés et nommés ne rentraient pas dans les cadres qui avaient cours à l'époque, qui ne parlaient que de fonctions: l'abstraction catégorique était donc nécessaire.
- de ce cadre "ultra-abstrait" à ... un compilateur pour le λ-calcul (langage catégorique comme "langage machine")
- toujours de ce cadre 'ultra-abstrait" à l'étude de diverses questions de cohérence... (étude de la bonne définition des programmes ou des notions mathématiques, indépendamment du représentant choisi pour décrire un objet, comme sur les figures plus haut), qui se posent en informatique comme en mathématiques. Pour une formulation informatique: étudier les relations entre toutes les preuves qui assurent qu'un programme est bien typé.

Au-delà

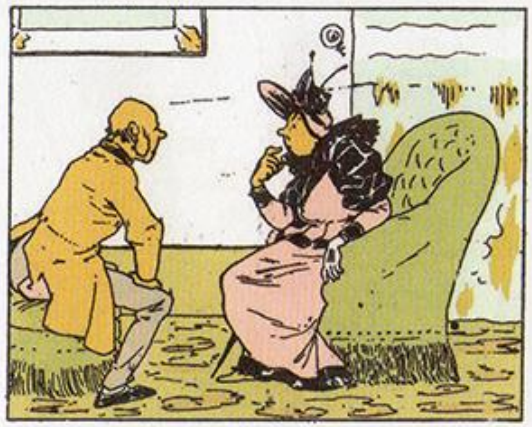
J'ai eu la chance d'avoir eu Georges Dumézil pour grand-père.

Il parlait une trentaine de langues (mortes, la plupart)... Pendant plus de 50 ans, il a établi des correspondances structurelles entre religions, mythes et épopées indo-européens: Jupiter-Mars-Quirinus, Odin-Thor-Freyr, Yudhishthira, Bhima/Arjuna, Nakula/Sahadeva,...

Langages et dictionnaires... L'érudition jointe à l'audace.

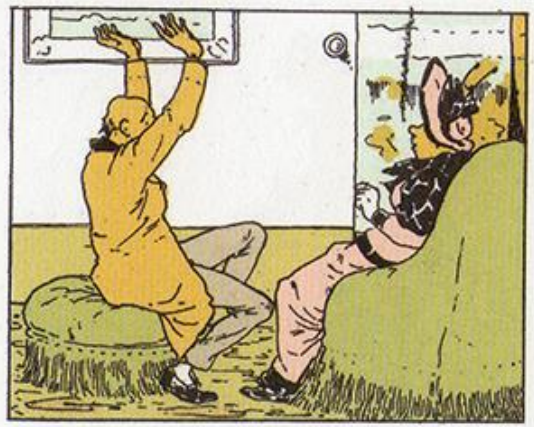
Le savant Cosinus

Christophe (1856–1945)



— Prenez donc ce fauteuil, madame, je vous en prie, dit aimablement Cosinus... Et maintenant en quoi puis-je vous être utile ?

— Monsieur, on m'a beaucoup parlé de vous, dit Mme Belazor qui prend Cosinus pour le dentiste : j'ai recours à votre habileté. J'ai là une vieille racine que je voudrais faire extraire...



— Une extraction de racine, s'exclame Zéphyrin ! Mais c'est ma spécialité, ça ! Dès ma plus tendre enfance, j'extrayais, par plaisir, toutes les racines de mes camarades ! et j'ose dire que j'ai acquis dans ce genre d'opérations une habileté extraordinaire. Je ne me vante pas, madame, je constate !.... Par quel procédé désirez-vous que j'opère ?

— Mais, monsieur, par celui qui me fera le moins de mal.

— Oh ! madame, riposte plaisamment Zéphyrin, j'opère toujours sans douleur ! Mais, puisque vous me laissez le choix, nous allons, si vous le voulez bien, employer des tables de logarithmes.