Avatars du calcul

Yves Lafont

9 novembre 2001

Cailloux

En français, « calcul » a deux sens bien distincts : Action de calculer [...] ; Concrétion solide de sels minéraux ou de matières organiques [...] (*Petit Robert*). C'est le premier sens qui nous intéresse ici, mais l'origine est commune : *calculus* (caillou). Il s'agit donc de *compter*, de faire des *opérations arithmétiques*, mentalement ou en s'aidant d'un support matériel : cailloux, abaque, ou boulier.

Papier

Avec l'*algèbre*, le calcul devient *symbolique*, c'est-à-dire qu'il manie des nombres fractionnaires comme $1/3$, irrationnels comme $\sqrt{2}$, ou transcendants comme π, et aussi des *variables*, en utilisant des *identités* telles que $(x+y)z = xz + yz$. Les cailloux ne suffisent plus : il faut du papier et un crayon. On doit aussi définir le *résultat* du calcul : en général, c'est une *forme normale*. Par exemple, $1/3$ est la forme normale de $2/6$, et $x^2 + 2x + 1$ est la forme normale de $(x+1)^2$.

Horloges

Le mouvement des astres permet de mesurer le temps. Inversement, on a pu construire des *horloges astronomiques* qui calculent le mouvement des astres à partir de celui d'un balancier. Le Siècle des lumières compare ainsi l'univers à une horloge, et son créateur à un grand horloger ! Toujours est-il que le calcul devient *mécanique*, et de Pascal à Babbage, les *machines à calculer* resteront apparentées aux horloges.

Silicium

Ces machines mécaniques ne sont guère adaptées au calcul symbolique. On a donc continué à faire de longs calculs à la main jusqu'à l'avènement de l'*ordinateur*. Celui-ci ressemble peu à ses ancêtres : il ne contient ni engrenages, ni cames, mais de nombreux *composants électroniques*, aujourd'hui à base de silicium, qui oscillent entre deux états symbolisés par 0 et 1. Une horloge électronique découpe le temps en courtes périodes afin de *synchroniser* les transitions de tous ces composants.

Automates

Pour expliquer le fonctionnement d'un ordinateur, on le représente comme un *automate* qui exécute les instructions d'un *programme*, un peu comme une machine à laver. Les instructions sont simples : mettre un caillou dans une boîte, tester si une boîte est vide ou en extraire un caillou (*machine à registres*) ; se déplacer sur un ruban de papier, y lire ou y écrire un symbole (*machine de Turing*).

Cellules

Ainsi le calcul s'identifie avec l'exécution d'un programme. Existe-t-il d'autres modèles du calcul ? En voici un plus général : appelons calcul tout processus *discret* et *déterministe*. Cela signifie que l'espace est divisé en *cellules* qui prennent successivement des états bien différenciés, et que le calcul est déterminé par l'état initial. On garde l'idée du programme, mais son exécution n'est plus centralisée, et il n'est plus question de résultat.

Vie

En ce sens, la vie peut être considérée comme un calcul. Certes, le rôle du hasard est essentiel dans les mécanismes de la reproduction et de l'évolution, mais celui du déterminisme ne l'est pas moins dans le développement d'un organisme à partir de son *code génétique*. Une étape fondamentale de ce calcul est la *réplication* du code génétique, et c'est d'ailleurs ce qui caractérise la vie.

Diagrammes

Dans certaines applications du calcul, on remplace les expressions symboliques par des dessins. C'est le cas en physique quantique (*diagrammes de Feynman*) et relativiste (*diagrammes de Penrose*). On sait bien qu'en géométrie, un dessin ne vaut pas une preuve, mais ici, les *diagrammes* ont un véritable statut *syntaxique*, au même titre que les nombres et les expressions symboliques. On pourrait d'ailleurs étendre cette idée à tout le calcul symbolique : l'algèbre serait sans doute moins rébarbative !

Preuves

Les liens entre logique et calcul sont multiples : on cite souvent les *portes logiques*, mais il existe aussi une profonde analogie entre les *preuves mathématiques* et les programmes. Le *λ-calcul* est une sorte de calcul des preuves, qui est à l'origine de langages de programmation tels que LISP ou CAML. Ce calcul n'a qu'une règle, qui consiste à remplacer toutes les occurrences d'une variable dans une expression par une autre expression, mais il est *universel*, c'est-à-dire qu'on peut y traduire tous les autres calculs.

Interaction

La théorie des preuves a mis en évidence le rôle crucial de la *duplication* et de l'*effacement* dans le calcul. On peut ainsi définir un modèle très simple du calcul avec 3 types de cellules : *constructeur*, *duplicateur*, et *effaceur*. Connectées entre elles, ces cellules forment des diagrammes appelés *réseaux d'interaction*, et elles interagissent par *commutation* ou par *annihilation*. On montre que ce calcul est universel en utilisant un analogue du code génétique.

Temps

Le calcul prends du temps, mais faut-il un *temps global*, c'est-à-dire commun à tous les composants de l'ordinateur ? Dans un réseau d'interaction, le calcul est distribué et le temps est *local*, un peu comme en physique relativiste. Il semble que l'abolition de l'horloge simplifierait considérablement la conception des ordinateurs. Il reste à trouver un modèle d'*ordinateur asynchrone* qui remplacerait le bon vieux *modèle de Von Neumann* issu de la machine de Turing.

Fictions

D'autres pistes sont prometteuses : le *calcul réversible* et le *calcul quantique*. Le premier permettrait d'améliorer les performances des ordinateurs en réduisant leur échauffement. Le second rendrait possible certains calculs, comme la factorisation de grands nombres, qui sont hors de portée des ordinateurs classiques. Ceci reste spéculatif, car on ne sait pas s'il est possible de construire des ordinateurs quantiques.

Yves Lafont est professeur à l'*Université de la Méditerranée à Marseille*, et chercheur à l'*Institut de Mathématiques de Luminy* (UPR 9016 du CNRS).