Quelques exemples d'arithmétiques sur ordinateur

Nathalie Revol

Labo. ANO, Univ. Lille
et projet INRIA Arénaire, LIP, ENS Lyon
Nathalie.Revol@ens-lyon.fr

Forum des jeunes mathématiciennes et des jeunes informaticiennes, 8 mars 2002

Calculer à l'école primaire : les entiers

Addition

à la main :

$$\begin{array}{cccccc} & & & {\scriptstyle 1} & {\scriptstyle 1} & \\ & & 1 & 2 & 3 & 4 \\ + & & & 5 & 6 & 7 \\ \hline & & 1 & 8 & 0 & 1 \end{array}$$

Sur ordinateur : idem mais en base 2.

Complexité de l'addition de 2 nombres à n chiffres :

$$\mathcal{O}(n)$$

opérations sur des chiffres.

Calculer à l'école primaire : les entiers

Multiplication (en base 2)

				1	0	1	1
$\times$			1	1	0	1	
				1	0	1	1
			0	0	0	0	
		1	0	1	1		
	1	0	1	1			
1	0	0	0	1	1	1	1

Complexité de cette multiplication de 2 nombres à n chiffres :

$$\mathcal{O}(n^2)$$

Les entiers

Multiplication : on peut aller plus vite. . .

Si A et B s'écrivent chacun avec $2n$ chiffres en base β,

$$A = a_H\beta^n + a_L, \qquad B = b_H\beta^n + b_L$$

$$A \times B = a_H b_H \beta^{2n} + (a_H b_L + a_L b_H)\beta^n + a_L b_L$$

soit 4 multiplications de nombres 2 fois plus court. . .

Multiplication de Karatsuba

On peut aussi écrire le produit comme

$$A \times B = a_H b_H \beta^{2n} + [(a_H + a_L)(b_H + b_L) - a_H b_H - a_L b_L]\beta^n + a_L b_L$$

avec 3 multiplications de nombres 2 fois plus court. . .
on multiplie 2 nombres de n chiffres en $\mathcal{O}(n^{\log_2 3})$.

Calculer à l'école primaire : les entiers

Multiplication : on peut aller encore plus vite. . .

Multiplication rapide

Multiplication basée sur la transformée de Fourier rapide (FFT) (ou plutôt discrète : DFT) : la complexité asymptotique de la multiplication est

$$\mathcal{O}(n \log n \log \log n)$$

Calculer à l'école primaire : les entiers

division

$$\begin{array}{r|l} 990 & 252 \\ \hline -756 & 3 \\ \hline 234 & \end{array} \qquad \begin{array}{r|l} 252 & 234 \\ \hline -234 & 1 \\ \hline 18 & \end{array} \qquad \begin{array}{r|l} \overbrace{234} & 18 \\ \hline -18 & 13 \\ \hline 54 & \\ -54 & \\ \hline 0 & \end{array}$$

Complexité de la division de 2 nombres à n chiffres :

$$\mathcal{O}(M(n))$$

où $M(n)$ est la complexité de la multiplication.

Calculer à l'école primaire : les entiers

pgcd

Rappel : pgcd (a, b) = pgcd (b, r) avec $a = bq + r$ si $r \neq 0$.

Algorithme d'Euclide :

$$\text{pgcd}(990, 252) = \text{pgcd}(252, 234) = \text{pgcd}(234, 18) = 18.$$

Complexité du pgcd de 2 nombres à n chiffres : $\mathcal{O}(M(n) \log n)$.

factorisation

$990 = 2 \times 3 \times 3 \times 5 \times 11$ et $252 = 2 \times 2 \times 3 \times 3 \times 7$.

Complexité : difficile ! $\Rightarrow$ certains algorithmes de cryptographie à clé publique (RSA, cf. exposé Marion Videau).

Les rationnels

$+, -, \times, /$: on sait faire
(beaucoup de calculs de pgcd).

Exemples de logiciels : Maple, Mathematica, certaines calculatrices (TI).

Avantage : calcul exact.

Inconvénients :
Nombres grossissent.
Complexité : dépend de la taille des nombres.
$\sqrt{}, \exp, \sin$: on ne sait pas faire. . .

Les nombres en notation scientifique : les flottants

Représentation

$\pi \simeq 3.14 \times 10^0 = 0.314 \times 10^1 = 0.031 \times 10^2 = 314 \times 10^{-2} \ldots$

Nombre de chiffres utilisés dans la représentation : constant.

Calculs

$+, -, \times, /$: en temps constant

$\sqrt{}, \exp, \sin$: en temps constant.

Arrondis

$3.14 \times 10^0 + 5.36 \times 10^{-1} = 3.676 \times 10^0$

sa représentation ne doit prendre que 3 chiffres

$\Rightarrow 3.14 \times 10^0 + 5.36 \times 10^{-1} \simeq 3.68 \times 10^0$.

Les flottants : encore de la recherche à faire !

Opérateurs

division : algorithmes différents selon les processeurs

opérations : basse consommation

Fonctions élémentaires

fonctions élémentaires : les calculer vite et bien

système	$sin(10^{22})$ (Ng)
valeur exacte	-0.852200849767. . .
HP 48 GX	-0.852200849767
HP 700	0.0
IBM 3090/600S-VF AIX 370	0.0
Matlab 4.2c.1 Sparc	-0.8522
Matlab 4.2c.1 MacIntosh	0.8740
SG Indy	0.87402806
Sharp EL5806	-0.090748172
DEC Station 3100	NaN

Les flottants : problème avec les arrondis

Les faits :

"On February 25, 1991, a Patriot missile defense system [. . .] failed to track and intercept an incoming Scud. This Scud subsequently hit an Army barracks killing 28 Americans."

L'explication :

"The Patriot battery at Dhahran failed [. . .] because of a software problem [. . .] This problem led to an inaccurate tracking calculation that became worse the longer the system operated. At the time of the incident, the battery had been operating continuously for over 100 hours."

(*cf.* `http ://www.fas.org/spp/starwars/gao/im92026.htm`)

Les flottants : problème avec les arrondis

Les faits :

- 1982 : the Vancouver stock exchange introduced an index with nominal value 1000.000
- after each transaction, it was recomputed and truncated to the third place to the right of the decimal point
- after 22 months the index was 524.881
- the correct value was 1098.811

L'explication :

toutes les erreurs d'arrondis sont dans le même sens ("truncation").

(d'après la page Web de Pete Stewart)

Les flottants : sans compter d'autres bugs. . .

Processeur : bug du Pentium

4195835.0 / 3145727.0 $\Rightarrow$ 1.333739068 au lieu de 1.33382044. . .

Logiciel :

Excel v3.0 à 7.0 : entrez 1.40737488355328 et vous aurez 0.64

Maple v6 : Entrez 5×2^{31} et vous aurez son opposé,
multipliez-le par 2 et ça fera 0.

Programme : Ariane 5

oubliez de gérer les cas particuliers et vous ferez exploser votre fusée.

Algorithme : la suite de Muller converge vers 100, jamais vers 6.

Problème : résolvez $\begin{pmatrix} 10^{-\alpha} & 1 \\ 1 & 1 \end{pmatrix} x = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ par Gauss

(cf. exposé Sylvie Boldo).

Flottants en précision multiple : plus de chiffres

Principe :

utiliser des représentations de longueur fixée
($\Rightarrow$ le produit de 2 nombres a la même longueur que les multiplicandes)
mais plus longues que celles des flottants machine.

Complexité :

$\leq$ celle du calcul sur des entiers de même longueur.

Avantage :

plus de précision.

Inconvénient :

toujours aucune garantie sur les résultats.

Calcul garanti avec les flottants : arithmétique par intervalles

(Moore 1966, Kulisch 1983, Neumaier 1990, Rump 1994, Alefeld and Mayer 2000. . .)

(cf. exposé Martine Ceberio)

Principe

Nombres remplacés par des intervalles.

π remplacé par $[3.14159, 3.14160]$

Vecteurs remplacés par des vecteurs d'intervalles.

Matrices remplacées par des matrices d'intervalles.

Intérêt : incertitudes sur les données (de mesure. . .) prises en compte.

Calcul garanti avec les flottants : arithmétique par intervalles

Calculs

$$[-2,3] + [5,7] = [3,10]$$

$[-3,2] * [-3,2] = [-6,9]$ est différent de $[-3,2]^2 = [0,9]$

$$[-3,2]/[0.5,1] = [-6,4]$$

$$X \diamond Y = \{x \diamond y \,/\, x \in X,\ y \in Y\}$$

$$\exp[-2,3] = [\exp(-2), \exp(3)]$$

car $\exp$ est une fonction croissante.

$$\sin[\pi/3, \pi] = [0,1]$$

attention, $\sin$ n'est pas monotone.

Arithmétique par intervalles : avantages

Calcul garanti
le résultat cherché appartient à l'intervalle calculé.

Information globale
on sait encadrer l'image d'une fonction sur tout un intervalle.

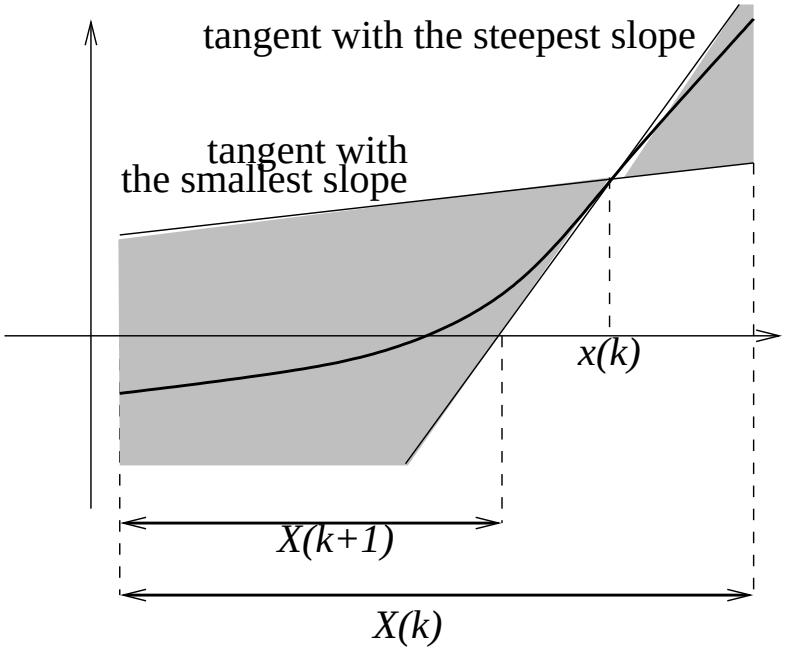
Théorème de Brouwer : si $f(I) \subset I$ alors f admet un point fixe dans I.
Application à Newton.

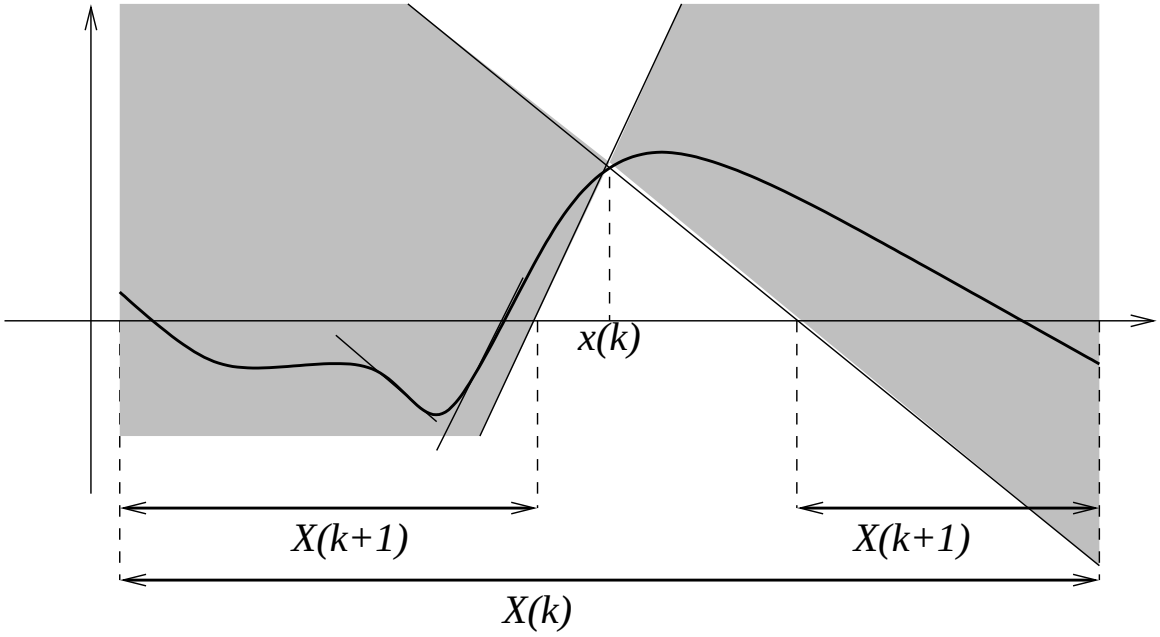
Algorithme de Hansen pour l'optimisation globale.

Arithmétique par intervalles : exemple d'algorithme

Algorithme de Newton par intervalles

(Hansen & Greenberg 1983, Mayer 1995, van Hentenryck et al. 1997. . .)





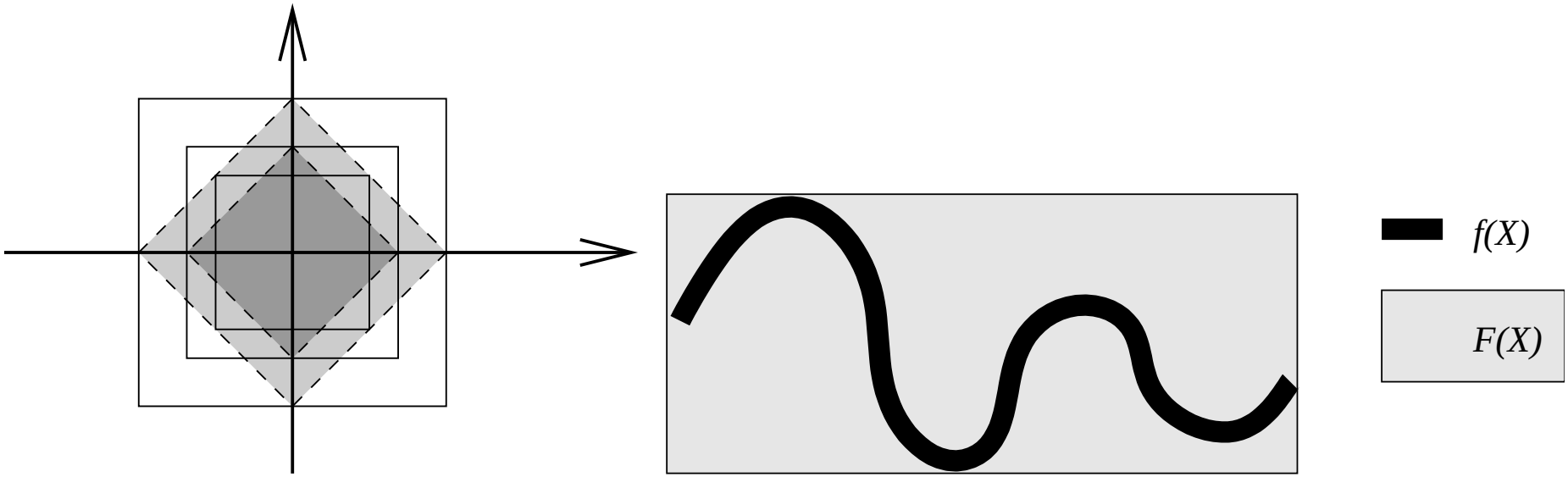
The result will be a list of intervals.

Arithmétique par intervalles : problèmes

Décorrélation des variables ou *variable dependency*

$$I * I = \{x * y \,;\, x \in I,\, y \in I\} \neq I^2 = \{x^2 \,;\, x \in I\}$$

Effet enveloppant ou *wrapping effect*



Arithmétique par intervalles
solution : bissection

Couper les intervalles en deux :

si $X = X_1 \bigcup X_2$, $F(X_1) \bigcup F(X_2) \subset F(X)$:

avec $F : x \mapsto x^2 - 2x + 1$, $X = [-1, 3]$ et $X_1 = [-1, 1]$, $X_2 = [1, 3]$

on a

$$F(X) = [-1,3]^2 - 2[-1,3] + 1 = [0,9] + [-6,2] + 1 = [-5,12]$$

$$F(X_1) = [-1,1]^2 - 2[-1,1] + 1 = [0,1] + [-2,2] + 1 = [-1,4]$$

$$F(X_2) = [1,3]^2 - 2[1,3] + 1 = [1,9] + [-6,-2] + 1 = [-4,8]$$

Arithmétique par intervalles
plus de précision

Motivation

- théorique : limite de validité de certains algorithmes : $n^3 u < 1 \Rightarrow n < 2 \times 10^5$
- expérimentale : optimiser les fonctions “boîtes à œufs”
- couper les intervalles en 2

Arithmétique par intervalles
plus de précision

Aspirateur autonome

- par intervalles : ne casse rien mais passe loin du vase en porcelaine de Chine
- en précision arbitraire : passe près du vase en porcelaine de Chine et le casse peut-être
- par intervalles en précision arbitraire : passe près du vase en porcelaine de Chine et ne le casse pas !

Arithmétique par intervalles MP
qu'y a-t-il à faire ?

Newton par intervalles en précision arbitraire

test d'arrêt : quand précisions voulues (arbitraires) sur la racine **et** le résidu atteintes ;

adaptation automatique de la précision : déterminer quand l'augmenter et comment ;

preuve d'arrêt ;

ne pas recommencer tous les calculs quand la précision est augmentée.

Conclusion

Choix d'arithmétiques

- exacte : entière et rationnelle
- flottante en précision fixe
- flottante en précision arbitraire
- intervalles en précision fixe
- intervalles en précision arbitraire
- mais aussi : en ligne, stochastique, paresseuse. . .

Comment choisir ? selon ses besoins

- rapidité
- précision
- garantie
- . . .