Soutenance de TER

Barnabé Chabaux

Implémentation en C/C++ de la résolution de systèmes linéaires à coefficients entiers

1. Introduction
2. Pivot de Gauss
3. Algorithme de Bareiss
4. Méthode modulaire
5. Mesures de temps de calcul, outils utilisés, et conclusion

INSTITUT FOURIER

Introduction

Notations :

- n : taille du système
- c : taille (nombre de bits) des coefficients initiaux
- L_i : i-ième ligne du système
- C_j : j-ième colonne du système
- $a_{i,j}$: coefficient de la i-ième ligne et de la j-ième colonne
- b_i : coefficient de la i-ième ligne du second membre

Un système :

$$\begin{cases} a_{1,1}x_1 & + & \cdots & + & a_{1,j}x_j & + & \cdots & + & a_{1,n}x_n & = & b_1 \\ \vdots & & & & \vdots & & & & \vdots & & \vdots \\ a_{i,1}x_1 & + & \cdots & + & a_{i,j}x_j & + & \cdots & + & a_{i,n}x_n & = & b_i \\ \vdots & & & & \vdots & & & & \vdots & & \vdots \\ a_{n,1}x_1 & + & \cdots & + & a_{n,j}x_j & + & \cdots & + & a_{n,n}x_n & = & b_n \end{cases}$$

INSTITUT FOURIER

Un système peut aussi être représenté sous cette forme matricielle :

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,j} & \cdots & a_{1,n} & b_1 \\ a_{2,1} & a_{2,2} & \cdots & a_{2,j} & \cdots & a_{2,n} & b_2 \\ \vdots & \vdots & & \vdots & & \vdots & \vdots \\ a_{i,1} & a_{i,2} & \cdots & a_{i,j} & \cdots & a_{i,n} & b_i \\ \vdots & \vdots & & \vdots & & \vdots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,j} & \cdots & a_{n,n} & b_n \end{pmatrix}$$

INSTITUT FOURIER

Pivot de Gauss

Pour k allant de 1 à $n-1$ et i allant de $k+1$ à n, on effectue l'opération suivante sur les lignes du système :

$$L_i \leftarrow L_i - \frac{a_{i,k}}{a_{k,k}} L_k$$

On obtient un système échelonné, c'est-à-dire un système dont la matrice est triangulaire supérieure.

$$\begin{pmatrix} 17 & 2 & -3 & 9 \\ 4 & 7 & -8 & -5 \\ 1 & 0 & 5 & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 17 & 2 & -3 & 9 \\ 0 & \frac{111}{17} & \frac{124}{17} & \frac{-121}{17} \\ 0 & 0 & \frac{560}{111} & \frac{371}{111} \end{pmatrix}$$

Algorithme de Bareiss

Variante du pivot de Gauss, avec l'opération suivante sur les lignes du système (En posant $a_{0,0} = 1$) :

$$L_i \leftarrow \frac{a_{k,k}L_i - a_{i,k}L_k}{a_{k-1,k-1}}$$

$$\begin{pmatrix} 17 & 2 & -3 & 9 \\ 4 & 7 & -8 & -5 \\ 1 & 0 & 5 & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 17 & 2 & -3 & 9 \\ 0 & 111 & -124 & -121 \\ 0 & 0 & 560 & 371 \end{pmatrix}$$

Bareiss : coefficients entiers

À chaque utilisation de "l'opération", le déterminant du système est multiplié par $\frac{a_{k,k}}{a_{k-1,k-1}}$.
On a donc :

$$\det_{fin} = \frac{a_{1,1}^{n-1}}{a_{0,0}^{n-1}} \times \frac{a_{2,2}^{n-2}}{a_{1,1}^{n-2}} \times \frac{a_{3,3}^{n-3}}{a_{2,2}^{n-3}} \times \ldots \times \frac{a_{n-2,n-2}^{2}}{a_{n-3,n-3}^{2}} \times \frac{a_{n-1,n-1}}{a_{n-2,n-2}} \times \det_{début}$$

$$\det_{fin} = a_{1,1} \times a_{2,2} \times \ldots \times a_{n-1,n-1} \times \det_{début}$$

D'autre part, comme la matrice en fin d'exécution est triangulaire supérieure :

$$\det_{fin} = a_{1,1} \times a_{2,2} \times \ldots \times a_{n-1,n-1} \times a_{n,n}$$

Donc finalement : $\det_{début} = a_{n,n}$

INSTITUT FOURIER

Bareiss : complexité

Borne de Hadamard :

$$|\det(A)| \leq \|C_1\|_2 \times \ldots \times \|C_n\|_2$$

- Taille de $\|C_j\|_2 = \sqrt{a_{1,j}^2 + \ldots + a_{n,j}^2}$: $O(c \ln(n))$
- Taille des coefficients : $O(cn \ln(n))$
- Coût des multiplications : $O(c^2 n^2 \ln(n)^2)$ (multiplication naïve) ou $O(cn \ln(n)^2)$ (FFT, à des $\ln(\ln(n))$ près)
- Coût total : $O(c^2 n^5 \ln(n)^2)$ (multiplications naïves) ou $O(cn^4 \ln(n)^2)$ (multiplications avec FFT)

INSTITUT FOURIER

Méthode modulaire

On va résoudre le système dans $\mathbb{Z}/p\mathbb{Z}$ pour diverses valeurs de p (nombre premier de taille "raisonnable") (à l'aide du pivot de Gauss), et en déduire la solution rationnelle du système.

Dans $\mathbb{Z}/p\mathbb{Z}$, les tailles des coefficients sont bornées, et le pivot de Gauss a donc un coût en $O(n^3)$.

INSTITUT FOURIER

Méthode modulaire : restes chinois

On cherche $x \in \mathbb{Z}/n_1n_2\mathbb{Z}$ tel que :

$$\begin{cases} x \equiv x_1 \pmod{n_1} \\ x \equiv x_2 \pmod{n_2} \end{cases}$$

Relation de Bézout minimale :

$$\begin{cases} n_1u + n_2v = 1 \\ |u| \leq \frac{|n_2|}{2} \\ |v| \leq \frac{|n_1|}{2} \end{cases}$$

Méthode naïve : $x = x_1vn_2 + x_2un_1$
Meilleure méthode : $x = x_1 + ((x_2 - x_1)u \pmod{n_2})n_1$

INSTITUT FOURIER

Méthode modulaire : reconstruction rationnelle

À partir d'un $b \in \mathbb{Z}/a\mathbb{Z}$, on cherche à obtenir un rationnel $\frac{num}{den}$, avec $num \in \mathbb{Z}$ et $den \in \mathbb{N}^*$ premiers entre eux, tel que :

$$\begin{cases} num\ den^{-1} \equiv b \pmod{a} \\ |num| < \frac{\sqrt{a}}{2} \\ 0 < den < \frac{\sqrt{a}}{2} \\ den \wedge a = 1 \end{cases}$$

Si une telle solution existe, on la trouve en utilisant une variante de l'algorithme d'Euclide étendu, où l'on s'arrête dès qu'on obtient un reste strictement inférieur à $\sqrt{a}$.

Méthode modulaire : premier algorithme

- Choisir un nombre premier p de taille "raisonnable"
- Résoudre le système dans $\mathbb{Z}/p\mathbb{Z}$ (pivot de Gauss)
- Par les restes chinois et avec l'étape précédente, en déduire la solution du système dans $\mathbb{Z}/prod\mathbb{Z}$ (où $prod$ est le produit des nombres premiers utilisés depuis le début de l'algorithme)
- Effectuer une reconstruction rationnelle. Tant qu'on n'obtient pas le même résultat qu'à l'itération précédente, on recommence ces quatre étapes

INSTITUT FOURIER

Méthode modulaire : deuxième algorithme

Borne de Hadamard (avec second membre b) :

$$hada = \|C_1\|_2 \times \ldots \times \|C_n\|_2 \times \|b\|_2$$

Les coefficients étant obtenus par reconstruction rationnelle dans $\mathbb{Z}/prod\mathbb{Z}$, on a besoin d'avoir $\frac{\sqrt{prod}}{2} \geq hada$. Dès que c'est le cas, il n'est plus nécessaire de faire des résolutions modulaires, et on peut effectuer une (seule) reconstruction rationnelle pour obtenir la solution du système.
Il est nécessaire d'effectuer $O(cn\ \ln(n))$ itérations.
La reconstruction rationnelle coûte $O(c^2n^3\ \ln(n)^2)$.

Méthode modulaire : règle de Cramer

Notons A_j la matrice du système (elle-même notée A) dont la j-ième colonne a été remplacée par le second membre b :

$$A_j = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,j-1} & b_1 & a_{1,j+1} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,j-1} & b_2 & a_{2,j+1} & \cdots & a_{2,n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{i,1} & a_{i,2} & \cdots & a_{i,j-1} & b_i & a_{i,j+1} & \cdots & a_{i,n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,j-1} & b_n & a_{n,j+1} & \cdots & a_{n,n} \end{pmatrix} \in M_n(\mathbb{Z})$$

On a alors : $\forall j \in [\![1, n]\!], x_j = \dfrac{\det(A_j)}{\det(A)}$

INSTITUT FOURIER

Méthode modulaire : troisième algorithme

Tant que $\frac{prod}{2} < hada$:

- Choisir un nombre premier p
- Échelonner/résoudre le système dans $\mathbb{Z}/p\mathbb{Z}$, et en déduire les déterminants de A et des A_j avec la formule de Cramer
- Par les restes chinois et avec l'étape précédente, en déduire les déterminants de A et des A_j dans $\mathbb{Z}/prod\mathbb{Z}$

Par la formule de Cramer, en déduire la solution du système

INSTITUT FOURIER

Mesures de temps de calcul, outils utilisés, et conclusion

↓ Taille ; Algorithme →	Gauss	Bareiss	Modulaire 1	Modulaire 2
$n = 5$, $c = 96$	0,000233	0,000093	0,00233 (35)	0,000362 (42)
$n = 5$, $c = 512$	0,00144	0,000382	0,0957 (180)	0,00293 (216)
$n = 5$, $c = 2048$	0,00736	0,00265	3,48 (719)	0,0261 (860)
$n = 50$, $c = 12$	0,0844	0,00934	0,0439 (45)	0,00896 (47)
$n = 50$, $c = 96$	1,03	0,124	4,50 (337)	0,103 (347)
$n = 50$, $c = 512$	12,4	1,72	493 (1796)	1,35 (1829)
$n = 50$, $c = 2048$	102	13,4	×	18,3 (7321)
$n = 200$, $c = 12$	26,1	1,36	5,28 (188)	1,47 (199)
$n = 200$, $c = 96$	444	30,9	900 (1361)	12,2 (1379)
$n = 200$, $c = 512$	×	388	×	117 (7729)
$n = 700$, $c = 12$	×	298	644 (698)	207 (734)

Outils utilisés :

- Nombres entiers de la bibliothèque GNU MP
- Implémentation maison des nombres rationnels
- Représentation et génération aléatoire des systèmes linéaires

INSTITUT FOURIER