Quadratic-Time Certificates in Linear Algebra

Kévin Polisano

A partir d'un article de E.L Kaltofen, M. Nehring & B.D Saunders

17/12/2012

Contents

Introduction
Notion de certificats

Certification

Vérifier *a posteriori* le résultat d'un calcul sur des données, avec une complexité inférieure au coût du calcul seul.

Algorithme de calcul d'une décomposition LU

- Entrée : matrice A de taille $n \times n$
- Sortie : matrices L et U
- Complexité en $O(n^\omega)$ $(\omega > 2.37)$
- Certification : vérifier $A = LU$
- Produit matriciel coût en $O(n^\omega)$
- Entrée + Certificat : amélioration en $O(n^2)$

Introduction
Certification probabiliste

Méthodes de Monte Carlo

- Toute méthode visant à calculer une valeur numérique en utilisant des procédés aléatoires
- La certification probabilistique renvoie vraie si la solution est vérifiée (à l'aide de l'entrée et du certificat)
- La probabilité d'obtenir « vraie » alors que la solution est incorrect doit être inférieure à 50%

Lemme

Vérifier probabilistiquement qu'une expression matricielle est nulle dans $\mathbb{Z}_p^{n\times n}$ peut s'effectuer en $O(n^2)$ avec une probabilité d'erreur de $\frac{1}{p}$

Contents

Résultats préliminaires

Certification probabilistique de la décomposition LU

Certification décomposition LU

Expression matricielle $E = A - LU$ à vérifier la nullité modulo p. Le certificat est le couple (p, v) où $v \in \mathbb{Z}_p^n$ aléatoire.
$Ev = Av - L(Uv)$ coûte 3 multiplication + 1 soustraction.
$\Rightarrow$ Complexité en $O(n^2)$

Probabilité d'erreur

S'il y a erreur, i.e E non nul, son noyau est au plus de dimension $n-1$ dans $\mathbb{Z}_p^n$ contenant p^{n-1} vecteurs parmi p^n.
D'où une probabilité d'erreur de $\frac{1}{p}$

Résultats préliminaires

Théorème

Théorème

Soit $A \in \mathbb{Z}^{n \times n}$ et $b \in \mathbb{Z}$. Les problèmes suivant ont une complexité spatiale et une certification probabilistique en $n^{2+o(1)}(log\|[A,b]\|)^{o(1)}$:

1. Non singularité de A
2. Singularité de A
3. Consistance du système linéaire $Ax = b$
4. Inconsistance du système linéaire $Ax = b$

Résultats préliminaires
Démonstration

1 - Non singularité

Entrée : A
Certificat : (p, B) avec p nombre premier et $B = A^{-1}\ mod\ p$.
Vérification : $AB - I \equiv 0\ mod\ p$

Le choix du certificat détermine :

- Complexité temporelle ? en $O(n^2)$ via Freivalds.
- Complexité spatiale ? $|(p, B)| = |p| + n^2|p|$ où $|p| = log_2(p)$ taille en bits qu'il occupe en mémoire.
- Probabilité d'erreur ? Problème pour $p|det(A)$!

Résultats préliminaires
Démonstration

Nombre de diviseurs de $|det(A)| \leqslant n(log(n)/2 + log\|A\|)$

Si $p_1, \ldots, p_k$ sont les diviseurs premiers de q, alors $k \leqslant ln(q)$.
Inégalité d'Hadamard : $|det(A)| \leqslant (n^{1/2}\|A\|)^n = q$
$\Rightarrow$ Il y a au plus $M = ln(q) = n(log(n)/2 + log\|A\|)$ diviseurs premiers de $det(A)$.

Probabilité d'erreur et complexité spatiale

On choisit p parmi les $2M$ premiers nombres premiers, d'où une probabilité d'erreur de $1/2$. Comme le k-ième nombre premier est $\leqslant k(log_e(k) + loglog_e(k) - 1/2)$ pour $k \geqslant 20$ alors $|p|$ en $log(n)^{1+o(1)}$ donc $|(p, B)|$ en $n^{2+o(1)} log\|A\|^{o(1)}$ bits.

Résultats préliminaires
Démonstration

2 - Singularité

Certificat : $m = 2n(log(n)/2 + log\|A\|)$ nombres premiers (p_i) et vecteurs non nuls (v_i) tels que $Av_i \equiv 0 \ mod \ p_i$.
Vérification : on tire (p_i, v_i) et on teste $Av \equiv 0 \ mod \ p_i$

Pourquoi m ?

Combien de nombres premiers renverront un test vrai alors que l'hypothèse est fausse (A est inversible) ?
$p_i \in D = \{p \text{ premier}, p|det(A) \neq 0\}$ alors $det(A) = 0 \ mod \ p_i$ donc A n'est pas inversible modulo p_i et il existe $v_i \in (\mathbb{Z}\backslash p_i\mathbb{Z})^n$ non nul tel que $Av_i = 0 \ mod \ p_i$ (test vrai), alors que $Av_i \neq 0$ dans $\mathbb{Z}$ puisque A inversible. Et $\sharp D \leqslant n(log(n)/2 + log\|A\|)$.

Résultats préliminaires
Démonstration

3 - Consistence de système linéaire rationnels $Ax = b$

Certificat : un vecteur d'entiers x et un entier δ tels que $Ax = \delta b$, avec x_i et δ bornés par $n^{n/2}\|(A, b)\|$
Vérification : zéro équivalence de $Ax - \delta b$ modulo un p_i aléatoire.

Cas où A est carrée et non singulière

Règle de Cramer : composantes de x sont des mineurs de (A, b) et $\delta = det(A)$

Résultats préliminaires
Démonstration

Cas où A est rectangulaire

$r = rang(A)$, en écrivant $A = PJ_rQ$, $A = \begin{pmatrix} B & C \\ D & DB^{-1}C \end{pmatrix}$,

$b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ avec B $r \times r$ non singulière, b taille r. $Ax = b$ étant consistant, il existe $x = (x_1, x_2)$ tel que

$$\begin{cases} Bx_1 + Cx_2 = \delta b_1 \\ Dx_1 + DB^{-1}Cx_2 = \delta b_2 \end{cases} \Rightarrow DB^{-1}b_1 = b_2$$

x_1 solution de $Bx_1 = \delta b_1$ avec $\delta = det(B)$, on construit $x = (x_1, 0, ..., 0)$ $(x_2 = 0)$ qui est alors solution du système.

Résultats préliminaires

Démonstration

Vérification

Combien de nombres premiers p_i peuvent certifier que $Ax = \delta b$ alors que (x, δ) n'est pas une solution correcte ?

Soit $(\hat{x}, \hat{\delta})$ la vraie solution, il y a falsification si $x - \hat{x} \equiv 0 \ mod \ p_i$ (n composantes) et $\delta - \hat{\delta} \equiv 0 \ mod \ p_i$. p_i divise les $n + 1$ différences. Il y en a au plus $k = 1 + n(log(n)/2 + log\|(A, b)\|)$. Choix de p_i parmi $3k + 3$ premiers. Enfin 2 tests de zéro équivalence de $Ax - \delta b$ donne une probabilité $1/3 + 2/3 \times 1/4 = 1/2$

Résultats préliminaires
Démonstration

4 - Inconsistence de système linéaire rationnels $Ax = b$

Certificat : $2n(log(n)/2 + log\|(A, b)\|)$ premiers p_i et vecteurs v_i tels que $v_i^T A = 0 \ mod \ p_i$ et $v_i^T b \neq 0 \ mod \ p_i$ contredisant $v_i^T Ax = v_i^T b$ sur les entiers.
Vérification : tirer (p_i, v_i) et tester les 2 conditions.

Inconsistence sur un corps K $(A \in K^{n\times n}, b \in K^{n\times 1})$

Il n'existe pas de $x \in K^{n\times 1}$ tel que $Ax = b$ si et seulement si il existe $u \in K^{1\times n}$ tel que $uA = (0, ..., 0) \in K^{1\times n}$ et $ub \neq 0$.
Preuve : $\boxed{\Rightarrow}$ $\nexists x, Ax = b \Rightarrow rang(A|b) = rang(A) + 1 \Rightarrow dim(Ker(A|b)) = dim(KerA) - 1 \Rightarrow \exists u \in K^{1\times n} \in Ker(A) \backslash Ker(A|b) \Rightarrow uA = 0, ub \neq 0$

Contents

Certificats basés sur la LU decomposition

Quelques définitions

Définition 1

A $(m \times n)$ possède une decomposition LU de rang r si $A = LU$ avec L $(m \times r)$ matrice triangulaire inférieure unitaire et U $(r \times n)$ matrice triangulaire supérieure sans 0 sur la diagonale.

Définition 2

Soit A de taille $m \times n$, un système de LU résidus de rang r et de longueur k est une suite de k triplets distincts $(p_1, L_1, U_1), ..., (p_k, L_k, U_k)$ où les nombres premiers p_i sont strictement croissants, les entrées de L_i, U_i sont normalisés modulo p_i et $A = L_i U_i \ mod \ p_i$ decomposition de rang r..

Certificats basés sur la LU decomposition

Lemme

Lemme

Soit A de rang r et un système de LU résidus de rang s et de taille k, posons $M = n(log(n)/2 + log\|A\|)$ bornant la taille en bits de tout mineur de A. Alors $s \leqslant r$, et si $s < r$ on a $k \leqslant M$.

Preuve

$s \leqslant r$ toujours vérifié, le rang dans $\mathbb{Z}$ est plus grand ou égal au rang réduit. A possède un rang s modulo p_i strictement inférieur à son rang r dans $\mathbb{Z}$ que si un mineur $r \times r$ est divisible par p. Le nombre maximal de tels p est M, donc la longueur maximale du système de LU résidus est M.

Certificats basés sur la LU decomposition

Certificat pour le rang

Théorème

Soit $A \in \mathbb{Z}^{n \times n}$, $M = n(log(n)/2 + log\|A\|)$. Il existe un système de LU résidus général de longueur $3M$ et dont les p_i ont une taille en bits $(logM)^{1+o(1)}$ qui certifie $rang(A)$. Le certificat occupe $n^{3+o(1)}(log\|A\|)^{1+o(1)}$ en espace et $n^{2+o(1)}(log\|A\|)^{1+o(1)}$ en temps.

Validation

Tirer (p, L, U) et valider zéro équivalence $PAQ = LU \ mod \ p$ (probabilité $1/p$ de se tromper). Le nombre de p à l'origine d'une falsification est au plus M, on choisit p parmi $3M$ donc probabilité $1/3$ soit au total une probabilité d'un mauvais certificat $1/3 + 2/3 \times 1/p \leqslant 1/2$ pour $p > 5$.

Certificats basés sur la LU decomposition

Certificat pour le déterminant

Théorème

Soit $A \in \mathbb{Z}^{n \times n}$, $M = n(log(n)/2 + log\|A\|)$. Il existe un système de LU résidus général de longueur $3M + 3$ et dont les p_i ont une taille en bits $(logM)^{1+o(1)}$ qui certifie $det(A)$.

Validation

Si le rang du système LU est inférieur à n, cf. précédent. Tirer (p, L, U) et valider zéro équivalence $PAQ = LU \ mod \ p$ (probabilité $1/p$ de se tromper) et $d = \prod_{i=1}^{n} U_{i,i}$. Le nombre de p à l'origine d'une falsification est au plus $M + 1$ (diviseurs de $d - det(A)$), on choisit p parmi $3M + 3$ donc probabilité $1/3$ soit au total $1/3 + 2/3 \times 1/p \leqslant 1/2$ pour $p > 5$.

Contents

Certificats basés sur la similarité

Définition

Une matrice carrée A est sous forme normale de Frobenius si elle est la somme directe de matrices de companions de polynômes unitaires $f_1(x), ..., f_k(x)$ tels que $\forall i, f_i | f_{i+1}$

Exemple : $A_1 = \begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}$ matrice compagnon de $x^2 + 2$

$$M = A_1 \oplus A_2 \oplus A_3 = \begin{pmatrix} 0 & -2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Certificats basés sur la similarité

Propriété

Toute matrice carrée sur un corps est semblable à une unique forme normale de Frobenius

Définition

Un système résiduel de similarité pour $A, B \in \mathbb{Z}^{n \times n}$ de taille k est une suite de quadruplet $(p, S, T, \bar{B})$ avec p premiers distincts, $S, T, \bar{B} \in \mathbb{Z}_p^{n \times n}$ et tels que S inversible avec $T \equiv S^{-1}$, $B \equiv \bar{B}$ et $A = S\bar{B}T$ modulo p. ($\bar{B}$ forme normale de Frobenius semblable)

Certificats basés sur la similarité

Certificat pour le polynôme caractéristique

Théorème

Soit $A \in \mathbb{Z}^{n \times n}$, $M_A = n(1 + log(n)/2 + log\|A\|)$. Il existe un système résiduel de similarité de longueur $6M_A + 6$ qui certifie le polynôme caractéristique $f(x)$, $n^{3+o(1)}(log\|A\|)^{1+o(1)}$ en espace et $n^{2+o(1)}(log\|A\|)^{1+o(1)}$ en temps.

Preuve

$c^A(x)$ vrai polynôme caractéristique de A. Le i-ème coefficient est la somme des $\binom{n}{i}$ $(\leqslant 2^n)$ mineurs principaux $i \times i$ $(\leqslant 2^M)$ donc $\leqslant 2^{n+M}$ soit de longueur en bits $n + M = M_A$.
$g(x) = f(x) - c^A(x)$ a des coefficients de taille $k = M_A + 1$, donc nul pour au plus k premiers. $k/(6M_a + 6) = 1/6$.

Certificats basés sur la similarité

Certificat pour le polynôme caractéristique

Vérification $f(x) = c^A(x)$

- Tirer $(p, S, T, \bar{B})$, vérifier zéro équivalence de $ST - I$ et $A - S\bar{B}T$ modulo p en $O(n^2)$ et proba erreur $2/p$.
- Vérifier dans $\bar{B}$ que $f_i | f_{i+1}$ (en $d^\circ(f_{i+1})^{1+o(1)}$), former $f_p(x) = \prod f_i(x)$ modulo p en $O(n^2)$. Par unicité de la forme de Frobenius on doit avoir $c^A(x) \equiv f_p(x)\ mod\ p$.
- Enfin vérifier que $f(x) \equiv f_p(x)\ mod\ p$

Conclusion
Ce qu'il faut retenir

Ce qu'il faut retenir

- Nécessité de vérifier des résultats, de manière fiable
  $\Rightarrow$ estimer la probabilité d'erreur
- Rapidement (essentiellement quadratique $n^{2+o(1)} log \|A\|$)
  $\Rightarrow$ effectuée dans des corps finis + Certificats
- Limiter la place en mémoire ($O(n^{3+o(1)} log \|A\|)$ bits)

Conclusion
Ouverture

Réduction de la complexité spatiale

- Autre type d'algorithme de vérification : Las Vegas
  $\Rightarrow$ toujours correct mais rapidité aléatoire.
- (Storjohann) Vérification du rang et du déterminant
  $\Rightarrow$ en $n^{\omega+o(1)} log \|A\|^{1+o(1)}$ bits
- Dépend du coût de la brique de base de l'algèbre linéaire
  $\Rightarrow$ le produit matriciel en $O(n^{\omega})$ avec $\omega \in [2, 3]$.

Questions ?