Algèbre linéaire creuse ? Dense ?
Les deux, mon capitaine.

Antoine Joux [1,3] Cécile Pierrot [2,3]

[1]CryptoExperts et Chaire de la Fondation Partenariale de l'UPMC

[2]DGA et CNRS

[2]Equipe Almasty
Laboratoire d'Informatique de Paris 6
UPMC, Sorbonnes-Universités

Séminaire de la Butte aux Cailles,
25 Juin 2015, Telecom Paris

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Dis Papa...

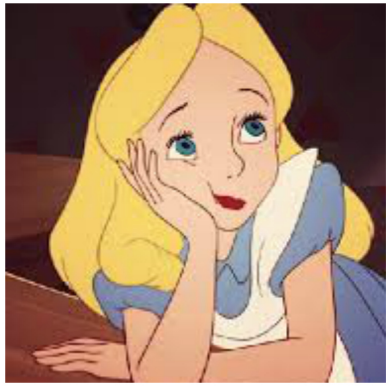
Oui ?

Tu me racontes une histoire ?

Stp

Stp

Laquelle ?



Pourquoi on dit "les deux mon capitaine ?"

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Algèbre linéaire et crypto

- Matrices sur des ensembles finis.
- Matrices creuses = la majorité des entrées sont nulles. Svt : le nombre de coeffs non nuls par ligne est bornée par une certaine constante, disons λ.
- Avantages ?
  - Moins de place en mémoire
  - Algo spécifiques

Exemples d'apparition

- Factorisation. Recherche d'un élt non nul du noyau d'une matrice $\mod 2$.
- Log discret. Derniers records en petite caractéristique.

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Algèbre linéaire creuse

Gestion de la mémoire : pr chaq. coeff. non nul sur une ligne, on retient le n° de la colonne et sa valeur.

Exemple

Sur $\mathbb{F}_7$, avec $\lambda = 3$.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 0 & 0 & 2 \\ 2 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 & 0 & 2 \\ 0 & 5 & 0 & 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 & 0 & 2 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} [1,1] & [5,3] & [8,2] \\ [1,2] & [3,1] & [6,2] \\ [4,4] & [7,1] & [0,0] \\ [4,3] & [8,1] & [0,0] \\ [1,1] & [2,1] & [0,0] \\ [3,5] & [8,2] & [0,0] \\ [2,5] & [6,6] & [0,0] \\ [5,2] & [6,1] & [0,0] \\ [2,3] & [4,1] & [7,1] \end{pmatrix}$$

Algèbre linéaire creuse, méthode naïve

Et si on veut résoudre $Mx = 0$?
Essayons un simple pivot de Gauss.

$$\left(\begin{array}{cccccccc|c}
1 & 0 & 0 & 0 & 3 & 0 & 0 & 2 & 0 \\
2 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 2 & 0 & 2 & 4 \\
0 & 0 & 0 & 4 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 3 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 5 & 0 & 0 & 0 & 0 & 2 & 0 \\
0 & 5 & 0 & 0 & 0 & 6 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 \\
0 & 3 & 0 & 1 & 0 & 0 & 2 & 0 & 0
\end{array}\right)
\begin{array}{c} \\ \\ l_2 - 2l_1 \\ \\ \\ \\ \\ \\ \\ \\ \end{array}
\rightarrow
\left(\begin{array}{ccc|c}
[1,1] & [5,3] & [8,2] & 0 \\
[1,2] & [3,1] & [6,2] & 0 \\
[5,1] & [3,1] & [6,2] & 4 \\
[4,4] & [7,1] & [0,0] & 0 \\
[4,3] & [8,1] & [0,0] & 0 \\
[1,1] & [2,1] & [0,0] & 0 \\
[3,5] & [8,2] & [0,0] & 0 \\
[2,5] & [6,6] & [0,0] & 0 \\
[5,2] & [6,1] & [0,0] & 0 \\
[2,3] & [4,1] & [7,1] & 0
\end{array}\right)$$

$[8,2]$??

Débordement de la mémoire allouée !
$\rightarrow$ Méthode stupide

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Algèbre linéaire creuse, les bonnes méthodes

- Ellimination Gaussienne adaptée
  = choix de pivots qui préservent le caractère creux

$$\left(\begin{array}{cccccccc|c}
1 & 0 & 0 & 0 & 3 & 0 & 0 & 2 & 0 \\
2 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 4 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 3 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 5 & 0 & 0 & 0 & 0 & 2 & 0 \\
0 & 5 & 0 & 0 & 0 & 6 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 \\
0 & 3 & 0 & 1 & 0 & 0 & 2 & 0 & 0
\end{array}\right) \rightarrow \left(\begin{array}{ccc|c}
[1,1] & [5,3] & [8,2] & 0 \\
[1,2] & [3,1] & [6,2] & 0 \\
[4,4] & [7,1] & [0,0] & 0 \\
[4,3] & [8,1] & [0,0] & 0 \\
[1,1] & [2,1] & [0,0] & 0 \\
[3,5] & [8,2] & [0,0] & 0 \\
[2,5] & [6,6] & [0,0] & 0 \\
[5,2] & [6,1] & [0,0] & 0 \\
[2,3] & [4,1] & [7,1] & 0
\end{array}\right)$$

- ou, sans modifier la matrice, en usant seulement de produits matrice-vecteurs :
  - méthode des sous-espaces de Krylov
  - méthode de Wiedemann

Wiedemann

1986

Problème

Résoudre:

$$Sx = 0 \quad ou \quad Sx = y$$

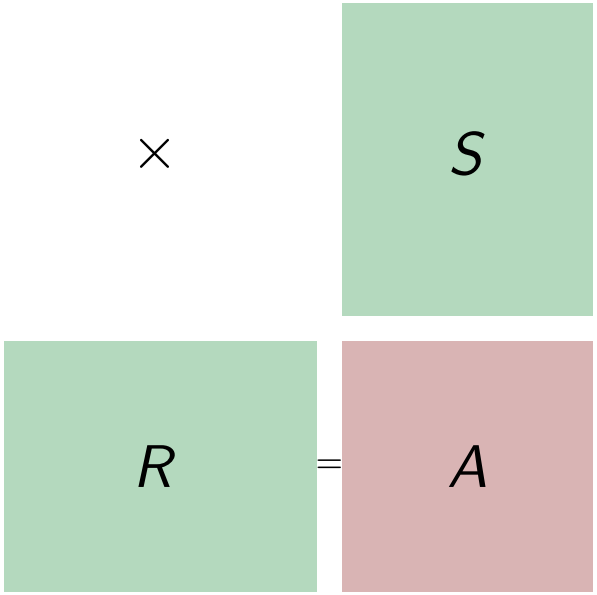
avec S matrice creuse à coefficients dans un anneau $\mathbb{K}$,
λ = nbr max de coeff non nuls par lignes,
N=taille max de la matrice.

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 0 & 0 & 2 \\ 2 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 & 0 & 2 \\ 0 & 5 & 0 & 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 & 0 & 2 & 0 \end{pmatrix} \quad \begin{matrix} \lambda = 3 \\ N = 9 \end{matrix}$$

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Wiedemann

1. Préconditionnement de la matrice S : On transforme S en une matrice carrée A.



Intérêt ?

- Puissances de A bien définies.
- A n'est pas creuse mais multiplier un vecteur par R S $=$ A se fait rapidement : $O(\lambda N)$
- $S.x = 0 \Rightarrow A.x = 0$ (ou $S.x = y \Rightarrow A.x = y' = R.y$). La réciproque est vraie pour presque tout R aléatoire.

On se ramène à la résolution de $A.x = 0$ (ou $A.x = y'$).

Wiedemann

2. Calcul d'une suite de scalaires : $({}^t wA^i v)_{i=0,\cdots,2n}$ avec v, w deux vecteurs quelc et $n = \#$ col. de A.
3. Reconstruction du polynôme minimal de A.

En quoi 2 aide-t-il 3 ?

- Th. Cayley-Hamilton : le polynôme caractéristique de A, de degré n, annule A.
- donc on cherche a_i tels que $\sum_{i=0}^{n} a_i A^i = 0$. $(\star_1)$
- $\Rightarrow \forall j \in \mathbb{N}, A^j(\sum_{i=0}^{n} a_i A^i) = 0$.
- $\Rightarrow \forall j \in \mathbb{N}, \sum_{i=0}^{n} a_i A^{i+j} = 0$.
- $\Rightarrow \forall j \in \mathbb{N}, \forall v$ vecteur, $\sum_{i=0}^{n} a_i A^{i+j} v = 0$.
- $\Rightarrow \forall j \in \mathbb{N}, \forall v, w$ vecteurs, $\sum_{i=0}^{n} a_i \, {}^t wA^{i+j} v = 0$. $(\star_2)$
- $\Rightarrow ({}^t wA^i v)_{i=0,\cdots,2n}$ satisfait une relation de récurrence linéaire !
- Berlekamp-Massey permet de retrouver le polynôme minimal d'une suite qui satisfait une rel. de réc. lin.
- $(\star_2)$ pour un v et un w quelc. $\Rightarrow_{\text{presq. tjr}} (\star_1)$.

On a trouvé a_i tels que $\sum_{i=0}^{n} a_i A^i = 0$.

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Wiedemann

4. Calcul de la solution.
   - Cmt résoudre $Ax = 0$ à partir de $\sum_{i=0}^{n} a_i A^i = 0$?
     S'il existe une solution alors $a_0 = 0$.
     Donc pour r vecteur qlcq :
     $$\sum_{i=1}^{n} a_i A^i r = 0 \Leftrightarrow A \underbrace{\left(\sum_{i=1}^{n} a_i A^{i-1} r\right)}_{\text{On a trouvé } x \text{ !}} = 0$$
   - Cmt résoudre $Ax = y$ à partir de $\sum_{i=0}^{n} a_i A^i = 0$?
     A inversible permet de supposer $a_0 \neq 0$.
     Donc $\displaystyle\sum_{i=0}^{n} a_i A^i x = 0 \Leftrightarrow -a_0 x = \sum_{i=1}^{n} a_i A^i x$
     $\Leftrightarrow x = -(1/a_0) \sum_{i=1}^{n} a_i A^{i-1} Ax$
     $\Leftrightarrow x = -(1/a_0) \sum_{i=1}^{n} a_i A^{i-1} y$, qu'il suffit de calculer !

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Wiedemann

1. Préconditionnement de la matrice S : Transformation de S en une matrice carrée A. Résolution de

$$A.x = 0 \quad \text{ou} \quad A.x = y'.$$

2. Calcul d'une suite de scalaires : $({}^t w A^i v)_{i=0,\cdots,2n}$ avec v, w deux vecteurs quelc et $n = \#$ col. de A.

   Complexité : Coût multiplication A-vecteur $\times$ nbr elmts de la suite $= O(\lambda N^2)$

3. Reconstruction du polynôme minimal de A via l'algorithme de Berlekamp-Massey.
   Complexité : quasi-linéaire en N
4. Calcul de la solution.

   Complexité : Coût multiplication A-vecteur $\times$ nbr elmts de la somme $= O(\lambda N^2)$

Complexité asymptotique finale :

$$O(\lambda N^2)$$

Et si on parallèlisait ?

- 1994. Coppersmith. Calculs distribués pour la résolution d'algèbre linéaire sur $\mathbb{F}_2$.
- 1995. Kaltofen. Généralise à $\mathbb{F}_{p^n}$.
- 2002. Thomé. Généralise Berlekamp-Massey.

Block Wiedemann

1. Préconditionnement de la matrice S : Transformation de S en une matrice carrée A. Résolution de

$$A.x = 0 \quad \text{ou} \quad A.x = y'.$$

2. Calcul d'une suite de scalaires matrices : $({}^t w W \; A^i V v)_{i=0,\cdots,2nn/c}$
avec v, w $V = (v_1, \cdots, v_c)$, W deux vecteurs matrices quelc. Parallélisation sur c machines :

$1 \quad ({}^t W A^i v_1)_{i=0,\cdots,2n/c}$

$\cdots \qquad \cdots$

$c \quad ({}^t W A^i v_c)_{i=0,\cdots,2n/c}$

Complexité : $O(\lambda N^2)$ mais distribués sur c machines.

3. Reconstruction du polynôme minimal de A
Reconstruction des coeffs. a_{ij} tels que $\sum_{j=1}^{c} \sum_{i=0}^{n/c} a_{ij} A^i v_j = 0$ via l'algorithme de Berlekamp-Massey Thomé. Complexité : $\tilde{O}(c^2 N)$

Quel est le problème ?

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Problème d'identité

A votre avis, elle est quoi, elle ?

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 0 & 0 & 2 & 5 & 3 \\ 2 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 6 & 2 \\ 0 & 0 & 0 & 4 & 0 & 0 & 1 & 0 & 6 & 4 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 & 1 & 5 & 2 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 5 & 0 & 0 & 0 & 0 & 2 & 1 & 1 \\ 0 & 5 & 0 & 0 & 0 & 6 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 1 & 6 \\ 0 & 3 & 0 & 1 & 0 & 0 & 2 & 0 & 5 & 6 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 3 & 4 & 2 \\ 0 & 2 & 0 & 3 & 0 & 0 & 2 & 0 & 5 & 1 \end{pmatrix}$$

Creuse ? Dense ?

$\lambda = 5$
$N = 11$

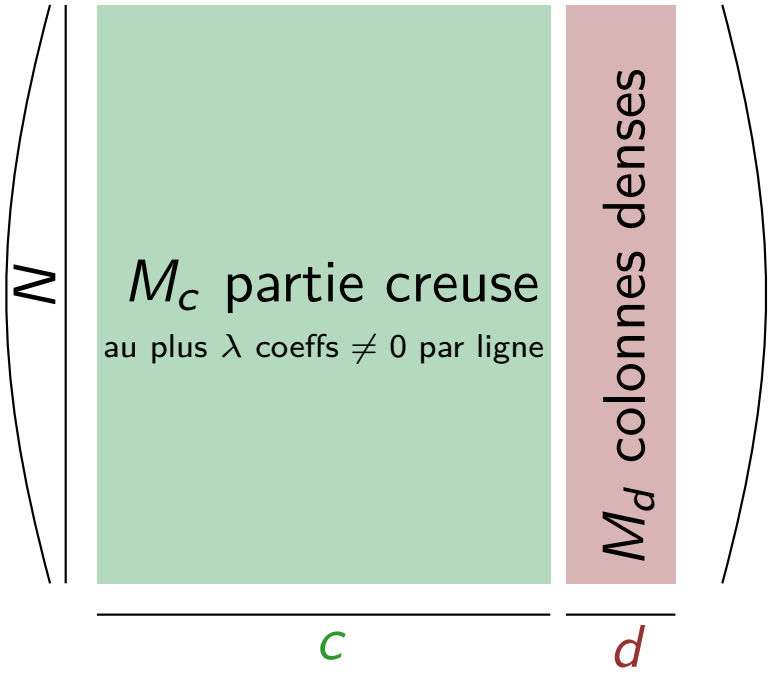
- Si on applique un algo classique, on ne tire pas partie des coeffs $= 0$.
- Si on applique Block-Wiedemann, on ne tire pas partie de la répartition particulière des coeffs $\neq 0$.

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Algèbre linéaire presque creuse

Définition

M est dite (d-)presque creuse si elle est de la forme :



Problème

Résoudre :

$$M \cdot x = 0 \quad ou \quad M \cdot x = y$$

avec M une matrice presque creuse à coeff. dans un anneau $\mathbb{K}$.

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Algèbre linéaire presque creuse

Remarque

- Il n'y a pas de restriction sur le nbr. de col. denses.
- Savoir retrouver un élt (non trivial) du noyau d'une matrice presque creuse suffit !

Supposons que l'on veuille résoudre $M \cdot x = y$ avec M une matrice d-presque creuse.

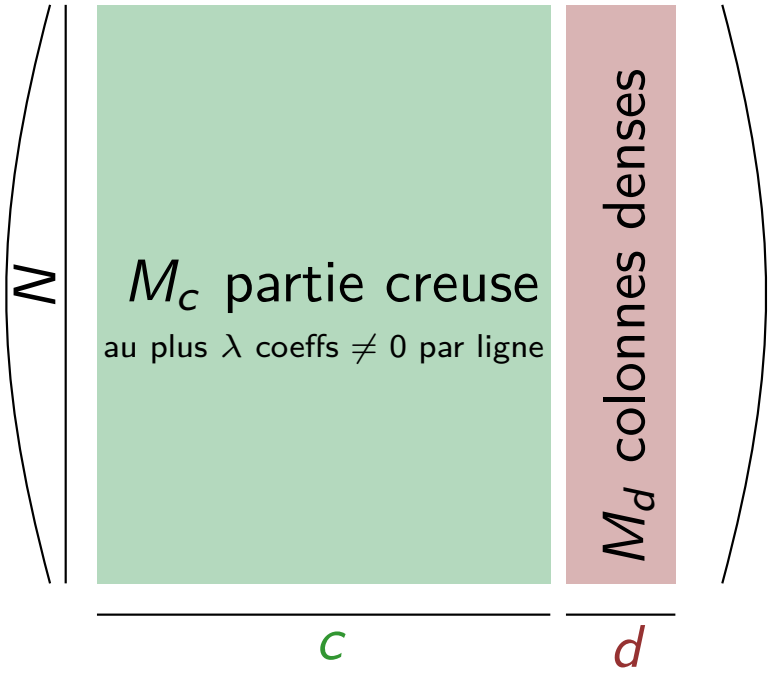
On a $\begin{pmatrix} M & \\ & \end{pmatrix} \cdot \begin{pmatrix} x \\ \\ \end{pmatrix} = \begin{pmatrix} y \\ \\ \end{pmatrix} \Leftrightarrow \begin{pmatrix} M & y \\ & \end{pmatrix} \cdot \begin{pmatrix} x \\ \\ -1 \end{pmatrix} = 0.$

Comme $\begin{pmatrix} M & y \\ & \end{pmatrix}$ est $d+1$-presque creuse, c'est gagné.

Algèbre linéaire presque creuse

Définition

M est dite (d-)presque creuse si elle est de la forme :



Problème

Résoudre :

$$M \cdot x = 0$$

avec M une matrice presque creuse à coeff. dans un anneau $\mathbb{K}$.

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Complexités asymptotiques

M est aussi une matrice creuse de paramètres $\lambda+d$, N.
On peut appliquer Block-Wiedemann !
Complexité asymptotique :

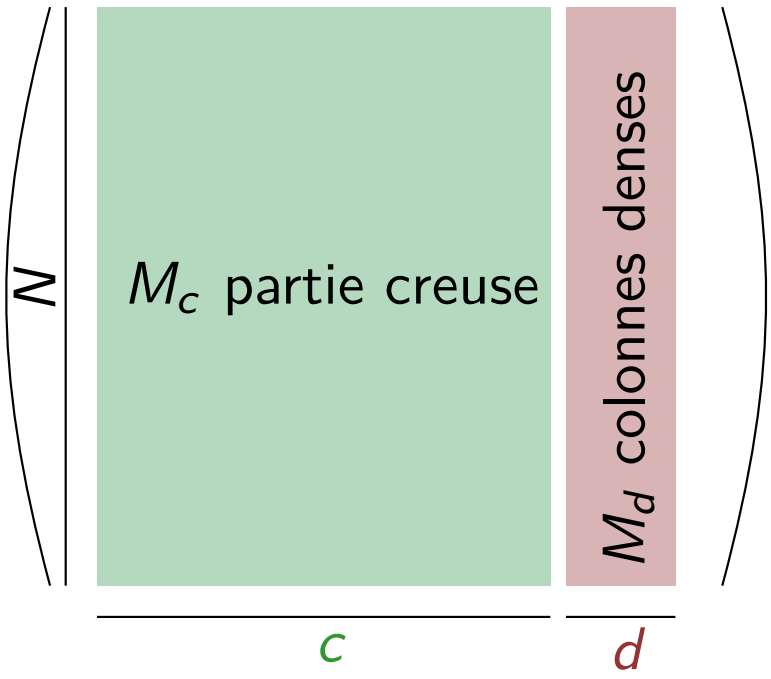
$$O((\lambda + d)N^2) + \tilde{O}(c^2 N)$$

Résultat principal

On peut construire un algo de complexité asymptotique :

$$O(\lambda N^2) + \tilde{O}(\max(c^2, d^2)N)$$

Idées directrices

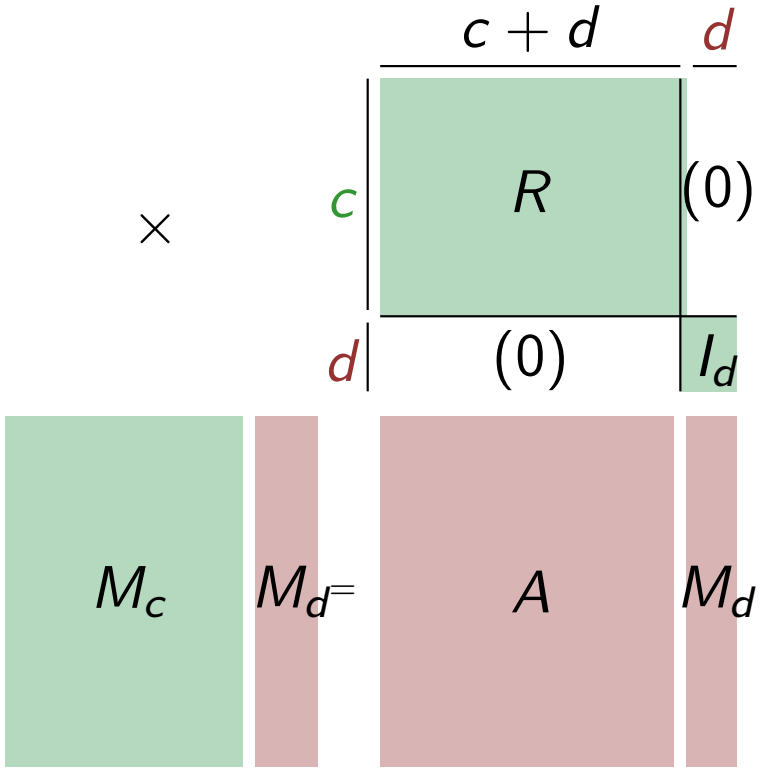


1. Appliquer Block-Wiedemann uniq^{mt} sur la partie creuse.
2. Faire intervenir les colonnes denses dans la construction du bloc V = prendre chacune des colonnes comme pt de départ des suites de scalaires à construire.

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Algorithme pour l'algèbre linéaire presque creuse

1. Préconditionnement A DROITE de la matrice M :



Intérêt ?

- Puissances de A bien définies.
- Multiplier un vecteur par $M_c\ R = A$ se fait rapidmt.
- Si R surj. : $(A|M_d).x = 0 \Rightarrow M.x = 0$

On se ramène à la résolution de $(A|M_d).x = 0$.

Algorithme pour l'algèbre linéaire presque creuse

Pour simplifier le problème : # machines = # col. denses.

2. Calcul d'une suite de matrices : $({}^tWA^iV)_{i=0,\cdots,2N}$
   avec $V = (v_1, \cdots, v_d)$, W deux matrices quelc.
   Parallélisation sur c machines :

$1 \quad ({}^tWA^iv_1)_{i=0,\cdots,2N/d}$

$\cdots \qquad \cdots$

$d \quad ({}^tWA^iv_d)_{i=0,\cdots,2N/d}$

Calcul d'une suite de matrices : $({}^tWA^iV)_{i=0,\cdots,2N}$
avec $V = (d_1, \cdots, d_d)$, W matrice quelc. et $d_1, \cdots, d_d$ les d col. denses.
Parallélisation sur d machines :

$1 \quad ({}^tWA^id_1)_{i=0,\cdots,2N/d}$

$\cdots \qquad \cdots$

$d \quad ({}^tWA^id_d)_{i=0,\cdots,2N/d}$

Algorithme pour l'algèbre linéaire presque creuse

4. Calcul d'un élt du noyau de $\begin{pmatrix} A & M \end{pmatrix}_d$

$$\sum_{j=1}^{d}\sum_{i=0}^{N/d} a_{ij}A^i d_j = 0 \quad \Leftrightarrow \quad \sum_{j=1}^{d}\sum_{i=1}^{N/d} a_{ij}A^i d_j + \sum_{j=1}^{d} a_{0j} d_j = 0$$

$$\Leftrightarrow \quad A \cdot \underbrace{\sum_{j=1}^{d}\sum_{i=1}^{N/d} a_{ij}A^{i-1} d_j}_{\text{notons le } x'} + \sum_{j=1}^{d} a_{0j} d_j = 0$$

$$\Leftrightarrow \quad A \cdot x' + a_{01} d_1 + a_{02} d_2 + \cdots + a_{0d} d_d = 0$$

Donc ${}^t(x' | a_{01} | a_{02} | \cdots | a_{0d}) \in \ker \begin{pmatrix} A & M \end{pmatrix}_d$.

Complexités asymptotiques

Résultat principal

On a une complexité asymptotique en :

$$O(\lambda N^2) + \tilde{O}(\max(c^2, d^2)N) \text{ opérations.}$$

Lorsque $d \leq c$, on a une complexité asymptotique en :

$$O(\lambda N^2) + \tilde{O}(c^2 N) \text{ opérations.}$$

Remarque

Lorsque le nbr de colonnes est inférieur au nbr de machines, les colonnes denses ne coûtent rien !

Complexités asymptotiques

Et si $c < d$, combien de colonnes denses s'autorise-t-on ?

- Tant que $d < N^{1-\epsilon}$ ($\epsilon > 0$ quelc.), notre algo est plus performant que Block-Wiedemann.
- Tant que $d < N^{\omega-2-\epsilon}$ ($\epsilon > 0$ quelc.), il est plus performant aussi que les algos d'algèbre linéaire dense de complexité $O(N^{\omega})$.

$\omega \approx 2,37$ donc pour $N^{1/3}$ colonnes denses par exemple, notre algo est à privilégier.

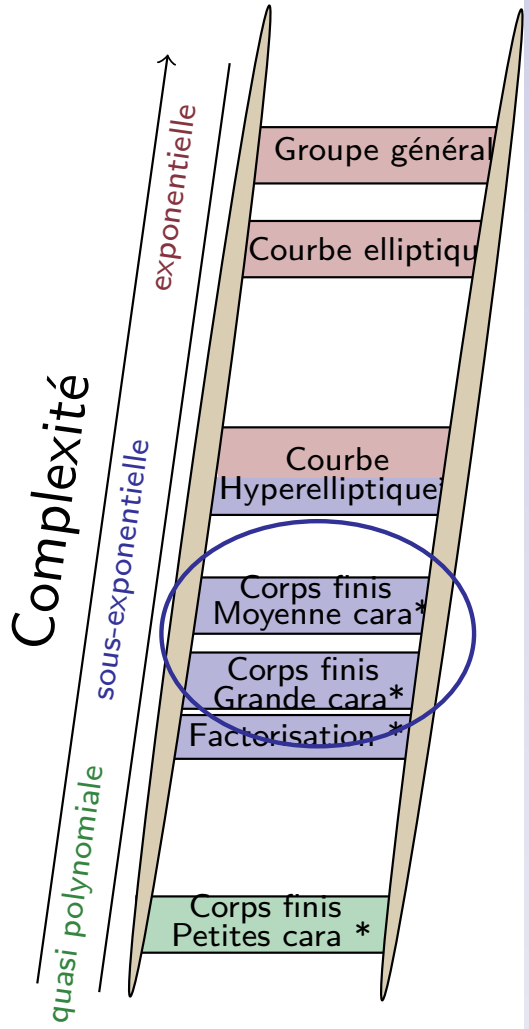
Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Applications

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

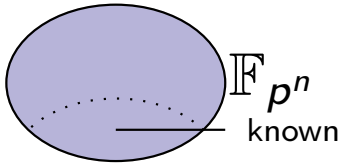
Le problème du logarithme discret

- Groupe multiplicatif G engendré par g: résoudre le pb du log discret dans G, c'est inverser l'application $x \mapsto g^x$
- Un pb difficile en général, utilisé comme tel en crypto.
- Divers groupes en pratique:
- Deux familles d'algo:
  - Algo génériques (Pollard's Rho, Pohlig-Hellman...)
  - Algo spécifiques (Calcul d'Indice *)



Calcul d'Indice

Si l'on souhaite résoudre le pb du log discret dans $\mathbb{F}_{p^n}$:



1. Collecte des relations
   $\rightarrow$ Crée un gd nbr de relations mult. creuses entre certains (petits) élts particuliers = les élts de la base de facteurs :

$$\prod g_i^{e_i} = \prod g_i^{e_i'} \quad \Rightarrow \quad \sum (e_i - e_i') \log(g_i) = 0$$

   $\rightarrow$ Donc un gd nbr d'équations linéaires creuses.
2. Algèbre linéaire creuse
   $\rightarrow$ Retrouve le log discret des élts de la base de facteurs.
3. Phase de logarithme discret individuel
   $\rightarrow$ Retrouve le log discret d'un élt quelc.

Algèbre linéaire creuse pour le log discret

- Effectuée modulo le plus gros facteur de $|\mathbb{F}_{p^n}^*|$.
- Domine en pratique le calcul de log pr toutes les caractéristiques.
- Domine asymptotiquement le calcul de log pr les corps de moyenne et grande cara.

Crible par corps de nombres (NFS)

- Meilleur algo en moyenne et grande cara ?
  NFS et ses variantes
- Bien. Mais. Corps de nombres complexifient l'algèbre linéaire : prise en compte des contributions des unités des corps de nombres.
- $\Rightarrow$ application de Schirokauer
- $+1$ appli. de Schirokauer $= +1$ col. dense

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

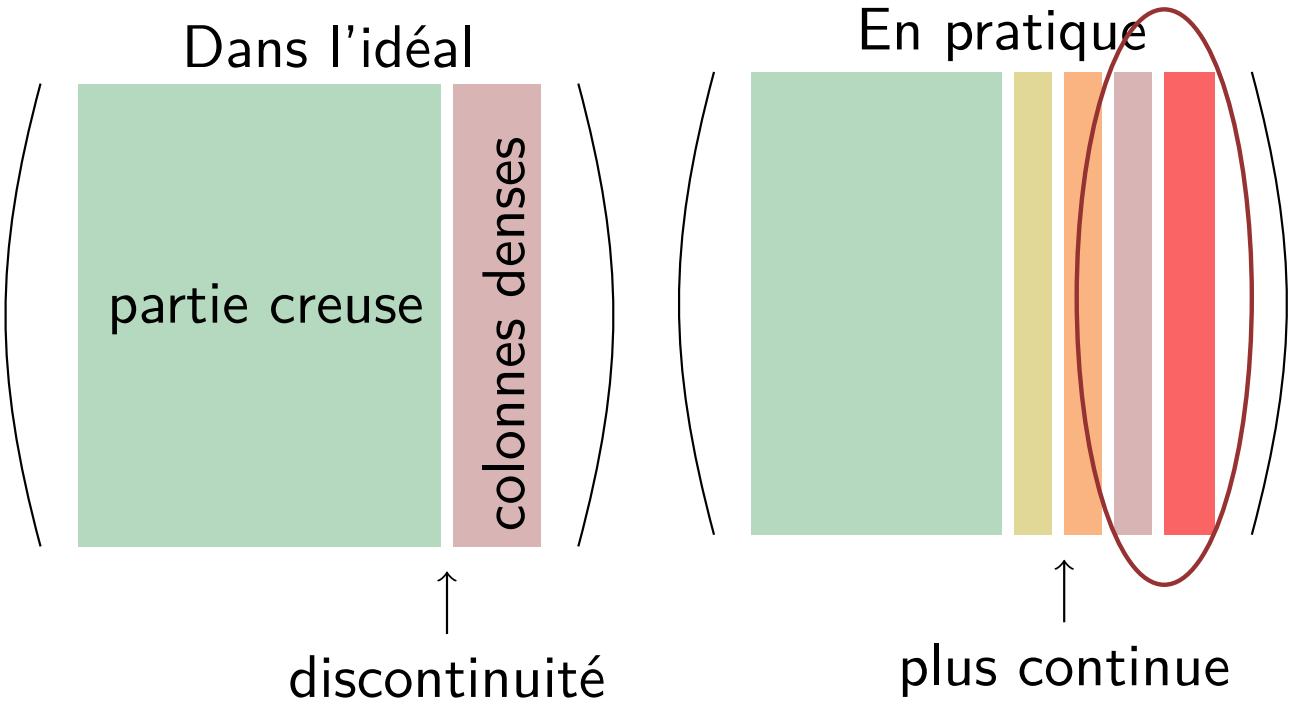
Exemple

- Dernier record sur $\mathbb{F}_p$, p premier ($p \approx 180$ chiffres)
- Juin 2014 par Bouvier, Gaudry, Imbert, Jeljeli, Thomé.
- Paramètres de la matrice : $N \approx 7,28$ millions lignes, $\lambda = 150$ coeff. non nuls par ligne, 4 colonnes denses.

Allons plus loin ?

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Trouve-t-on ailleurs de telles matrices ?

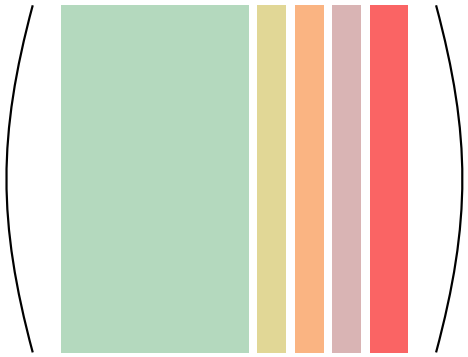


Discontinuité totale non indispensable en pratique.

Exemple

- Dernier record en caractéristique 3, sur $\mathbb{F}_{3^{5*479}}$
- Septembre 2014, Joux, P.
- Même idée déjà implantée sur une matrice creuse.

Réseaux et matrices presque creuses

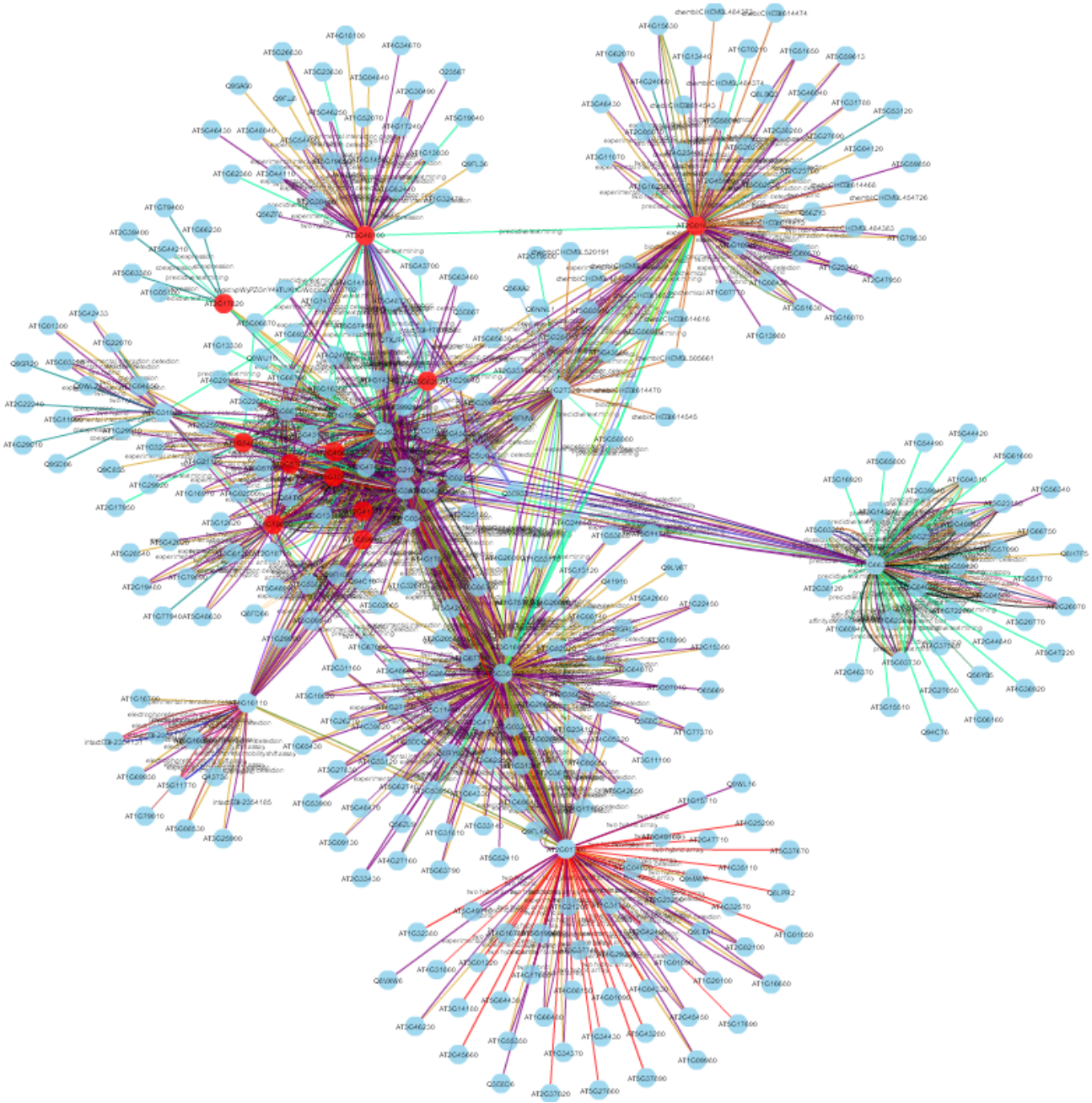


- presque creuses
- coeff. dans un ens. fini

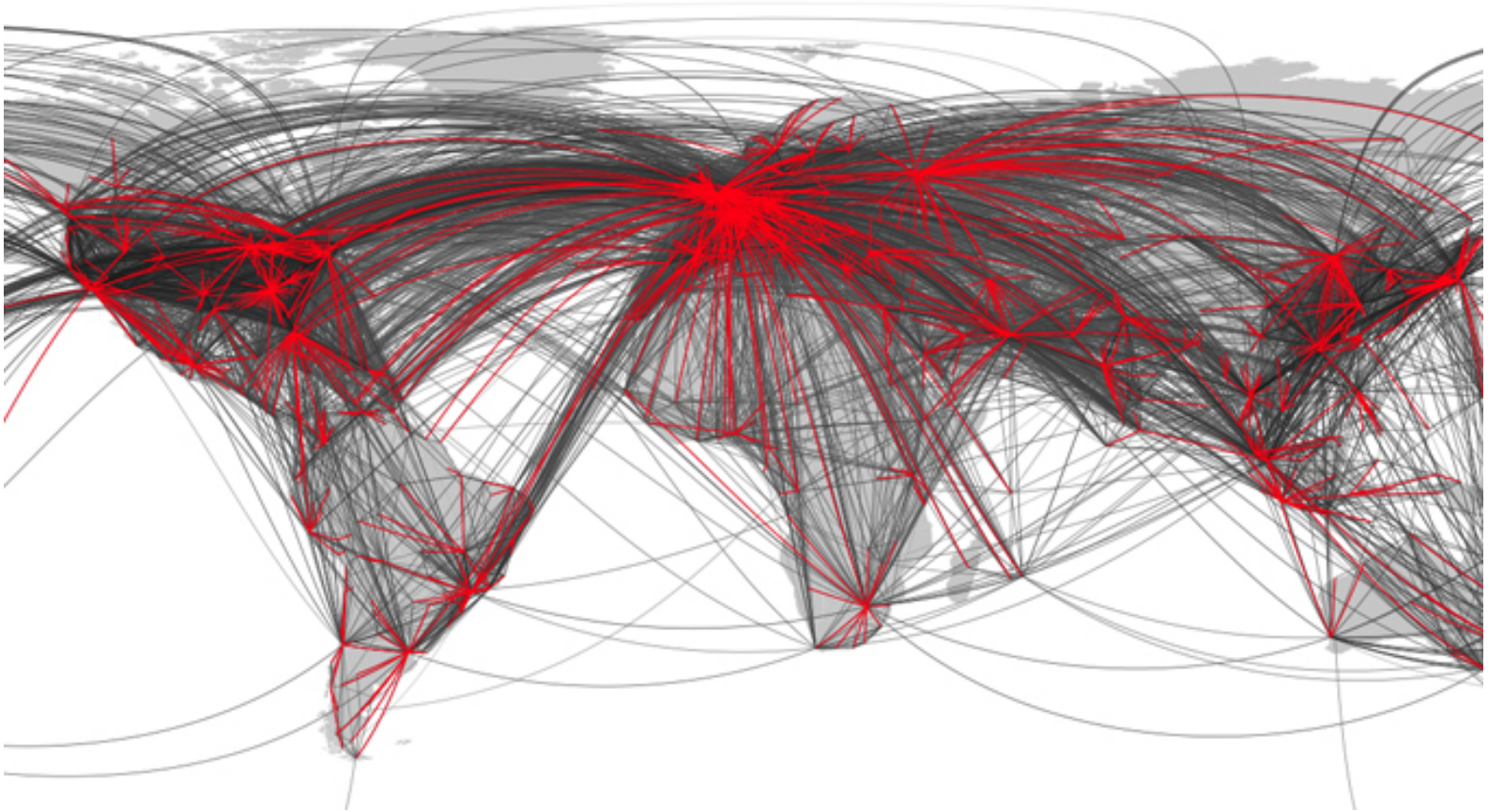
Ces matrices sont omniprésentes dans la vie rélle !

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Matrice d'adjacence des liens entre les protéines

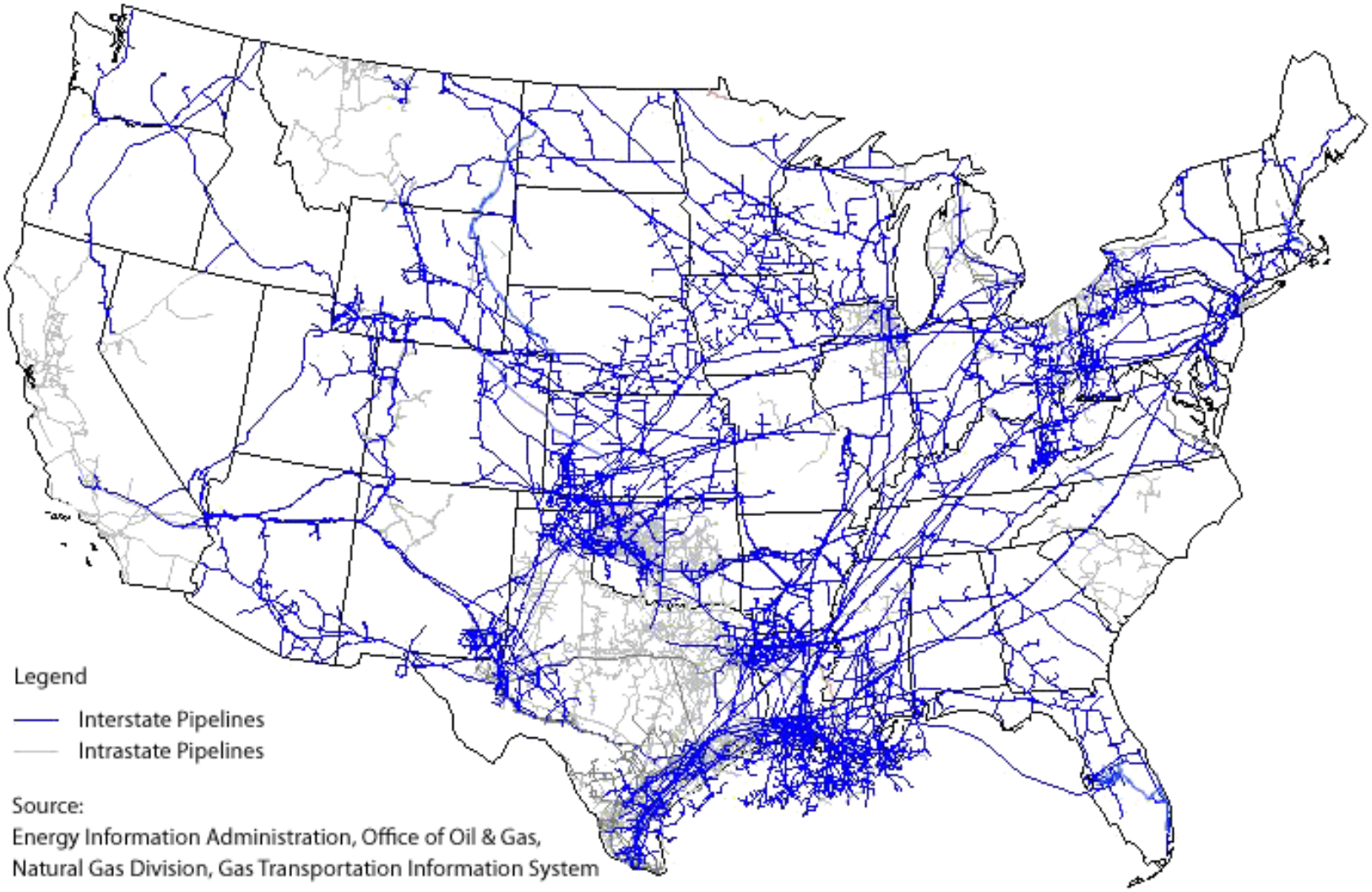


Matrice d'adjacence des aéroports mondiaux



Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Réseau de distribution du pétrole aux Etats-Unis



Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

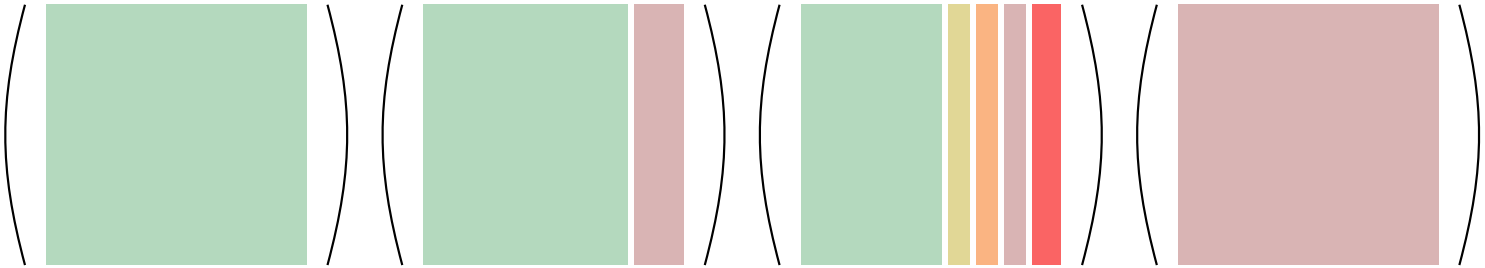
Réseaux et matrices presque creuses

La question en suspens :

Sur ces matrices, à quelle fin la résolution de problème d'algèbre linéaire pourrait-elle être utile ?

Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?

Merci de votre attention !



Algèbre linéaire creuse
Wiedemann
Block Wiedemann
Algèbre linéaire presque creuse
Définition
Un algorithme dédié
Gain théorique
Applications
Calcul de logarithmes discrets
Vers d'autres perspectives ?