Sparse Gaussian Elimination Modulo p: an Update

Claire Delaplace

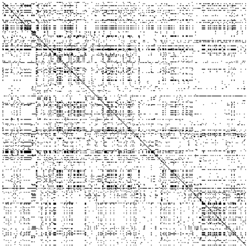
July 7, 2016

Background

Sparse Linear Algebra
Modulo p (coefficients : int)

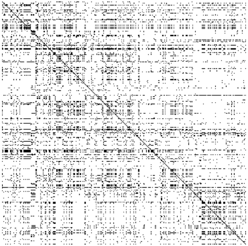
Operations

- Rank
- Linear systems
- Kernel
- etc...



Background

Sparse Linear Algebra
Modulo p (coefficients : int)



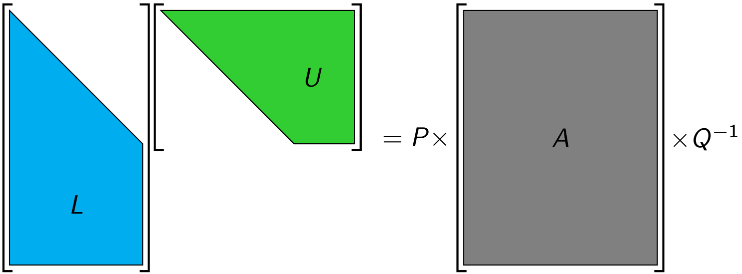
Operations

- Rank
- Linear systems
- Kernel
- etc...

Two families of Algorithms

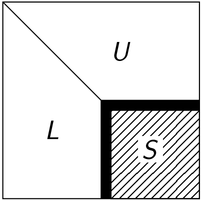
- **Direct methods** (Gaussian Elimination, LU, ...): Numerical World
- **Iterative methods** (Wiedmann, ...): Linear Algebra

PLUQ

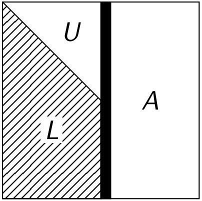


- A can be rectangular.
- A can be rank deficient
- L has unit diagonal.
- U has non zero diagonal

Usual right-looking Algorithm:



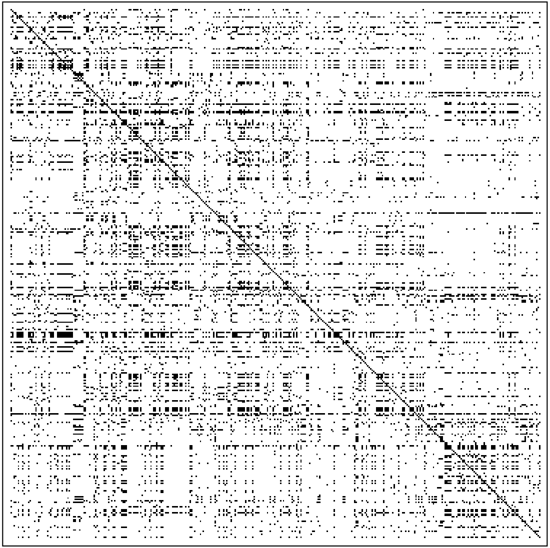
Left looking GPLU Algorithm:

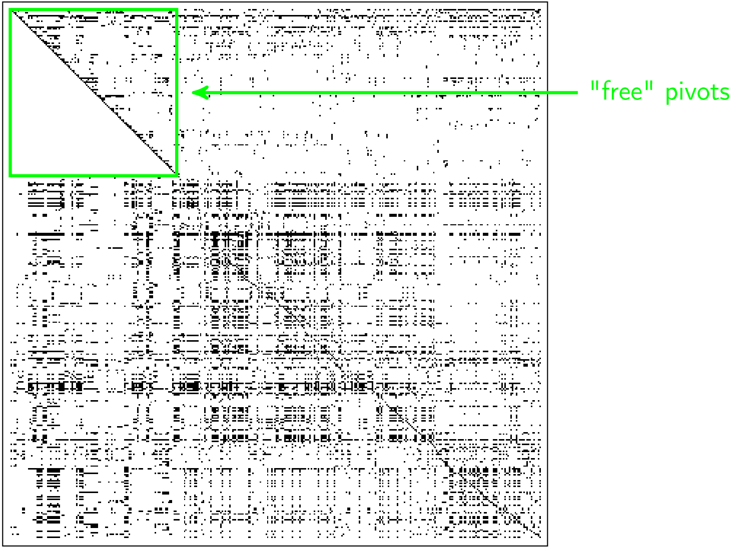


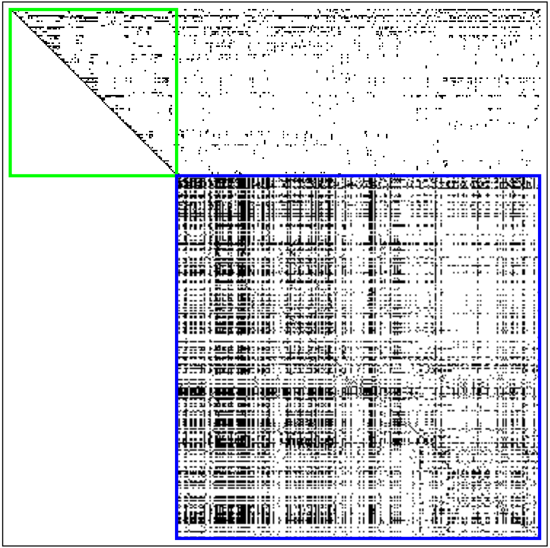
A new hybrid algorithm

Description

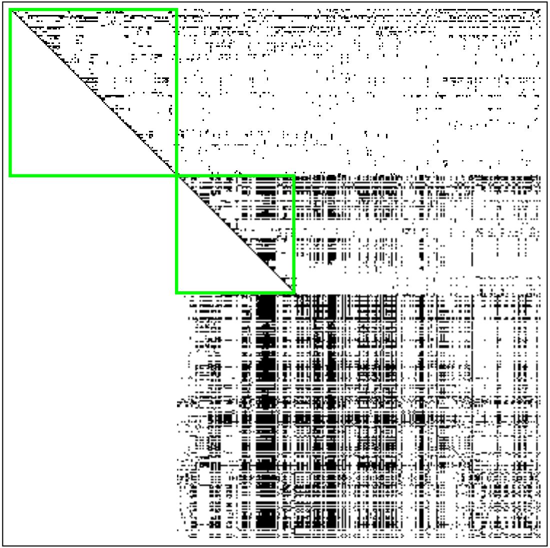
- Find pivots without performing any arithmetical operations ("free" pivots).
- Compute the Schur complement using a left-looking algorithm.
- Recurse.

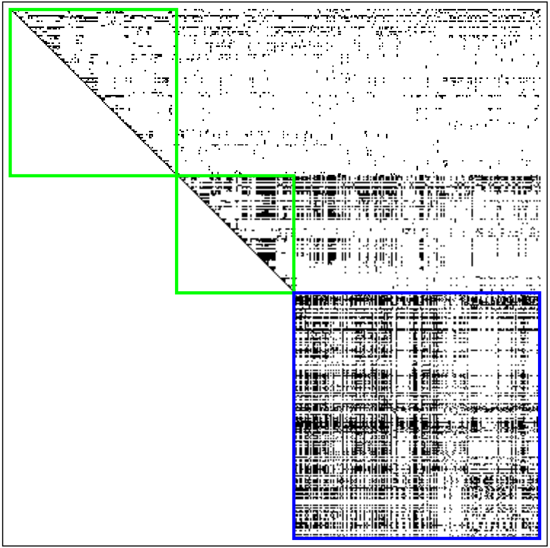


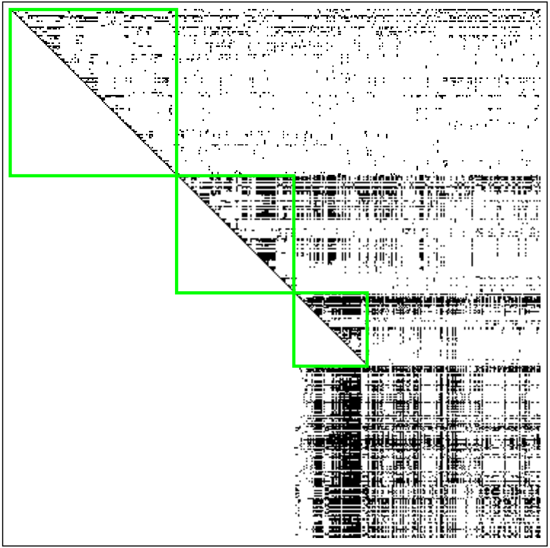

"free" pivots

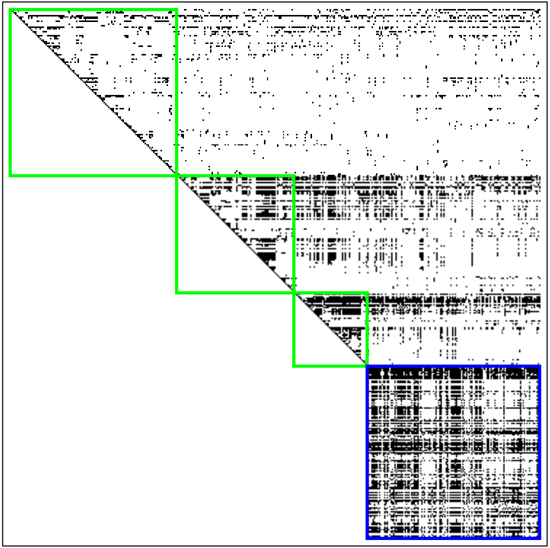


Schur Complement









← Parallelizable

Pivots Selection (Faugère and Lachartre (2010))

$$
\begin{array}{c}
0\\1\\2\\3\\4\\5\\6\\7
\end{array}
\begin{pmatrix}
\bullet & & & & \bullet & \bullet & \\
 & & \bullet & \bullet & & \bullet & \\
 & \bullet & \bullet & & & & \\
 & & & \bullet & & & \\
\bullet & & & & \bullet & \bullet & \\
 & & & & \bullet & \bullet & \\
 & \bullet & \bullet & & & & \bullet \\
 & \bullet & \bullet & \bullet & & & \bullet
\end{pmatrix}
\qquad
\begin{array}{c}
4\\2\\1\\3\\5\\0\\6\\7
\end{array}
\begin{pmatrix}
{\color{red}\bullet} & & & & \bullet & \bullet & \\
 & {\color{red}\bullet} & \bullet & & & & \\
 & & {\color{red}\bullet} & \bullet & & \bullet & \\
 & & & {\color{red}\bullet} & & & \\
 & & & & {\color{red}\bullet} & \bullet & \\
\bullet & & & & \bullet & \bullet & \\
 & \bullet & \bullet & & & & \bullet \\
 & \bullet & \bullet & \bullet & & & \bullet
\end{pmatrix}
$$

Description

- Each rows is mapped to the column of its leftmost coefficient.
- When several rows have the same leftmost coefficient, select the sparsest.
- Move the selected rows before the others and sort them by increasing position of the leftmost coefficient.

Schur Complement Computation

P denotes the permutation that pushes the "free" pivots in the top of A. Ignoring permutation over the columns of A:

$$PA = \begin{pmatrix} U_{00} & U_{01} \\ A_{10} & A_{11} \end{pmatrix} = \begin{pmatrix} Id & \\ L_{10} & L_{11} \end{pmatrix} \cdot \begin{pmatrix} U_{00} & U_{01} \\ & U_{11} \end{pmatrix}$$

Schur Complement Computation

P denotes the permutation that pushes the "free" pivots in the top of A.
Ignoring permutation over the columns of A:

$$PA = \begin{pmatrix} U_{00} & U_{01} \\ A_{10} & A_{11} \end{pmatrix} = \begin{pmatrix} Id & \\ L_{10} & L_{11} \end{pmatrix} \cdot \begin{pmatrix} U_{00} & U_{01} \\ & U_{11} \end{pmatrix}$$

Definition

The **Schur Complement** S of PA with respect to U_{00} is given by :

$$S = A_{11} - A_{10} U_{00}^{-1} U_{01}$$

Schur Complement Computation

P denotes the permutation that pushes the "free" pivots in the top of A.
Ignoring permutation over the columns of A:

$$PA = \begin{pmatrix} U_{00} & U_{01} \\ A_{10} & A_{11} \end{pmatrix} = \begin{pmatrix} Id & \\ L_{10} & L_{11} \end{pmatrix} \cdot \begin{pmatrix} U_{00} & U_{01} \\ & U_{11} \end{pmatrix}$$

Definition

The **Schur Complement** S of PA with respect to U_{00} is given by :

$$S = A_{11} - A_{10} U_{00}^{-1} U_{01}$$

Denote by $(\mathbf{a}_{i0}\ \mathbf{a}_{i1})$ the i-th row of $(A_{10}\ A_{11})$, and consider the following system :

$$(\mathbf{x}_0\ \mathbf{x}_1) \cdot \begin{pmatrix} U_{00} & U_{01} \\ & Id \end{pmatrix} = (\mathbf{a}_{i0}\ \mathbf{a}_{i1})$$

We obtain $\mathbf{x}_1 = \mathbf{a}_{i1} - \mathbf{a}_{i0} U_{00}^{-1} U_{01}$.

Schur Complement Computation

P denotes the permutation that pushes the "free" pivots in the top of A. Ignoring permutation over the columns of A:

$$PA = \begin{pmatrix} U_{00} & U_{01} \\ A_{10} & A_{11} \end{pmatrix} = \begin{pmatrix} Id & \\ L_{10} & L_{11} \end{pmatrix} \cdot \begin{pmatrix} U_{00} & U_{01} \\ & U_{11} \end{pmatrix}$$

Definition

The **Schur Complement** S of PA with respect to U_{00} is given by :

$$S = A_{11} - A_{10} U_{00}^{-1} U_{01}$$

Denote by $(\mathbf{a}_{i0}\ \mathbf{a}_{i1})$ the i-th row of $(A_{10}\ A_{11})$, and consider the following system :

$$(\mathbf{x}_0\ \mathbf{x}_1) \cdot \begin{pmatrix} U_{00} & U_{01} \\ & Id \end{pmatrix} = (\mathbf{a}_{i0}\ \mathbf{a}_{i1})$$

We obtain $\mathbf{x}_1 = \mathbf{a}_{i1} - \mathbf{a}_{i0} U_{00}^{-1} U_{01}$. $\mathbf{x}_1$ **is the i-th row of the** S

Results

We used J.-G. Dumas Sparse Integer Matrix Collection as benchmark matrices.

Hybrid versus Right-looking and GPLU

Matrix	Right-looking	GPLU	Hybrid
GL7d/GL7d24	34	276	11.6
Margulies/cat_ears_4_4	3	184	0.1
Homology/ch7-8.b4	173	0.2	0.2
Homology/ch7-8.b5	611	45	10.7

Hybrid versus Wiedmann

Matrix	Wiedmann	Hybrid
M0,6-D7	20397	0.8
relat8	244	2
relat9	176694	2024

Conclusion

- Will be presented at the CASC conference.
- Implemented in C in the SpaSM(SPArse System Modulo p) library and publicy available at:

`https://github.com/cbouilla/spasm`

Conclusion

- Will be presented at the CASC conference.
- Implemented in C in the SpaSM(SPArse System Modulo p) library and publicy available at:

`https://github.com/cbouilla/spasm`

What's next ?

- Improve the research of pivots in the Faugère-Lacharte Heuristic.
- Benchmark on specific matrices collections (GBLA, Cado-NFS).

Thank you for your time !