# Task based parallelization of recursive linear algebra routines using Kaapi

### Clément PERNET

joint work with Jean-Guillaume DUMAS and Ziad SULTAN

Université Grenoble Alpes, LJK-CASYS

January 20, 2017









### High performance algebraic computing

### Domain of computation

- $\bullet$   $\mathbb{Z}, \mathbb{Q}$ : variable size, multi-precision
- $\mathbb{Z}_p$ ,  $\mathsf{GF}(p^k)$ : fixed size, specific arithmetic

#### Common belief: Slow

- terrible complexities,
- no need for all the precision

### Example (Linear System solving over Q)

Method	Complexity
Naive Gauss Elim over Q	$\mathcal{O}\left(2^{n}\right)$
Gauss mod det	$\mathcal{O}\left(n^{5}\right)$
Gauss mod $p$ + CRT	$\mathcal{O}\left(n^4\right), \mathcal{O}\left(n^{\omega+1}\right)$
p-adic Lifting	$\mathcal{O}(n^3)$ , $\mathcal{O}(n^\omega)$

And fast software: LU over  $(\mathbb{Z}/65521\mathbb{Z})^{5000\times5000}$  in 3.8s (21.8Gfops on 1 Haswell core)

### Gaussian elimination in computer algebra

### **Applications**

Algebraic cryptanalysis: RSA, DLP  $\Rightarrow$ LinSys, Krylov,  $\mathbb{F}_q$ 

Comp. number theory: modular forms databases: Echelon over  $\mathbb{F}_q$ 

Exact mixed-integer linear programming:  $\Rightarrow$ LinSys over  $\mathbb{Q}$ 

Formal proof: Sums of squares ⇒Cholesky over ℚ

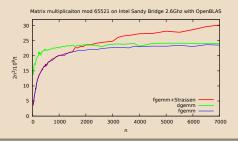
### HPC building block

- Dense linear algebra over  $\mathbb{Z}/p\mathbb{Z} \log_2 p \approx 20 30$  bits
- MatlMul (fgemm) and GaussElim (PLUQ)
  - triangular decomposition PLUQ (for LinSys, Det)
  - linear dependencies (Krylov, Grobner basis)

### FFLAS-FFPACK library

#### FFLAS-FFPACK features

- High performance implementation of basic linear algebra routines over word size prime fields
- Exact alternative to the numerical BLAS library
- Exact triangularization, Sys. solving, Det, Inv., CharPoly



### Exact vs numerical Gaussian elimination

#### Similarities

- Reduction to gemm kernel (Matrix Multiplication)
   Blocking: slab/tiled, iterative/recursive
- Parallel blocking is constrained by pivoting numeric: ensuring numerical stability exact: able to reveal rank profile

#### Similarities

- Reduction to gemm kernel (Matrix Multiplication)
   Blocking: slab/tiled, iterative/recursive
- Parallel blocking is constrained by pivoting numeric: ensuring numerical stability exact: able to reveal rank profile

### Specificities

Recursive tasks (vs block iterative in numeric)

#### Similarities

- Reduction to gemm kernel (Matrix Multiplication)
- ⇒Blocking: slab/tiled, iterative/recursive
- Parallel blocking is constrained by pivoting

```
numeric: ensuring numerical stability exact: able to reveal rank profile
```

### Specificities

- Recursive tasks (vs block iterative in numeric)
- Modular reductions
  Strassen's algorithm efficiency increases with the granularity
  - ⇒tradeoff between total work and fine granularity

#### Similarities

- Reduction to gemm kernel (Matrix Multiplication)
  - ⇒Blocking: slab/tiled, iterative/recursive
- Parallel blocking is constrained by pivoting

```
numeric: ensuring numerical stability exact: able to reveal rank profile
```

### Specificities

- Recursive tasks (vs block iterative in numeric)
- Modular reductions
  Strassen's algorithm

  efficiency increases with the granularity
  - ⇒tradeoff between total work and fine granularity
- Pivoting strategies: no stability constraints, but rank profiles

#### Similarities

- Reduction to gemm kernel (Matrix Multiplication)
  - ⇒Blocking: slab/tiled, iterative/recursive
- Parallel blocking is constrained by pivoting

```
numeric: ensuring numerical stability exact: able to reveal rank profile
```

### Specificities

- Recursive tasks (vs block iterative in numeric)
- Modular reductions
  Strassen's algorithm 

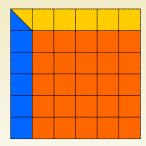
  → tradeoff between total work and fine granularity
- Pivoting strategies: no stability constraints, but rank profiles
- Rank deficienices:
  - blocks have unpredictable size ( ⇒and positions)
  - unbalanced task load

Tiled Iterative

Slab Recursive

Tiled Recursive

#### Tiled Iterative



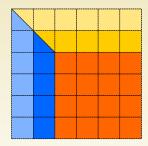
Slab Recursive

Tiled Recursive

Conclusion

trsm:  $B \leftarrow BU^{-1}$ ,  $B \leftarrow L^{-1}B$  gemm:  $C \leftarrow C - A \times B$ 

### Tiled Iterative



Slab Recursive

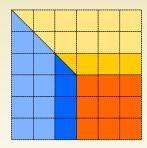
Tiled Recursive

getrf:  $A \rightarrow L$ , U

trsm:  $B \leftarrow BU^{-1}, B \leftarrow L^{-1}B$ 

gemm:  $C \leftarrow C - A \times B$ 

### Tiled Iterative



### Slab Recursive

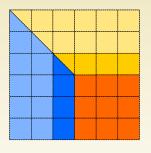
### Tiled Recursive

getrf:  $A \rightarrow L, U$ 

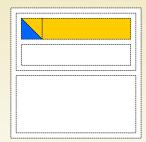
trsm:  $B \leftarrow BU^{-1}, B \leftarrow L^{-1}B$ 

gemm:  $C \leftarrow C - A \times B$ 

### Tiled Iterative

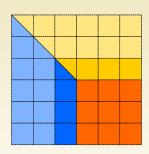


Slab Recursive

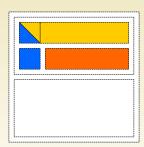


### Tiled Recursive

#### Tiled Iterative



Slab Recursive

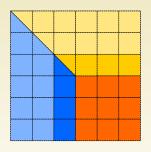


### Tiled Recursive

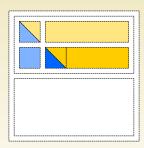
trsm:  $\mathbf{\textit{B}} \leftarrow \mathbf{\textit{B}}\mathbf{\textit{U}}^{-1}, \mathbf{\textit{B}} \leftarrow \mathbf{\textit{L}}^{-1}\mathbf{\textit{B}}$ 

gemm:  $C \leftarrow C - A \times B$ 

### Tiled Iterative

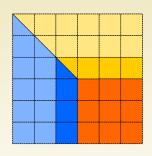


### Slab Recursive

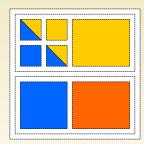


### **Tiled Recursive**

#### Tiled Iterative



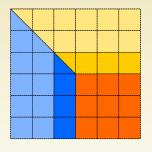
### Slab Recursive



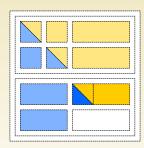
### Tiled Recursive

trsm:  $B \leftarrow BU^{-1}$ ,  $B \leftarrow L^{-1}B$ 

### Tiled Iterative

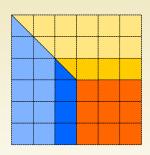


Slab Recursive

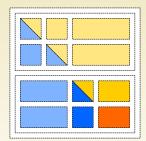


### Tiled Recursive

#### Tiled Iterative



Slab Recursive

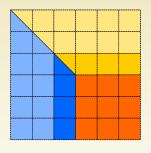


### Tiled Recursive

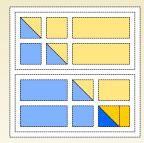
trsm:  $B \leftarrow BU^{-1}$ ,  $B \leftarrow L^{-1}B$ 

gemm:  $C \leftarrow C - A \times B$ 

### Tiled Iterative

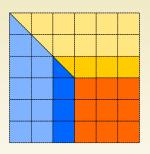


### Slab Recursive

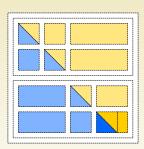


### Tiled Recursive

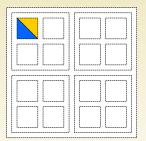
Tiled Iterative



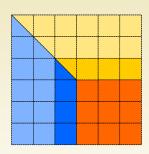
Slab Recursive



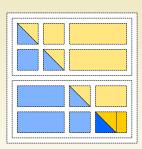
Tiled Recursive



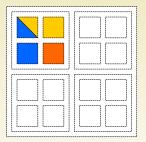
#### Tiled Iterative



Slab Recursive



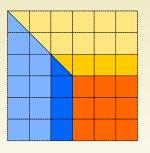
### Tiled Recursive



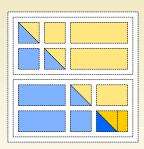
trsm:  $B \leftarrow BU^{-1}, B \leftarrow L^{-1}B$ 

gemm:  $C \leftarrow C - A \times B$ 

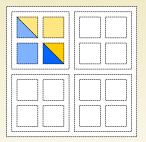
### Tiled Iterative



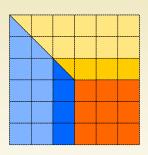
Slab Recursive



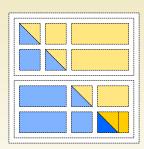
Tiled Recursive



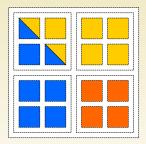
#### Tiled Iterative



Slab Recursive



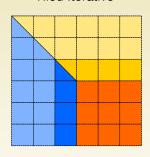
### Tiled Recursive



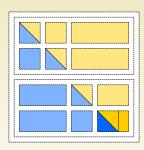
trsm:  $B \leftarrow BU^{-1}, B \leftarrow L^{-1}B$ 

gemm:  $C \leftarrow C - A \times B$ 

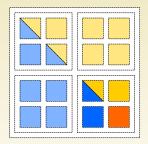
#### Tiled Iterative



Slab Recursive



Tiled Recursive

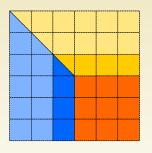


getrf:  $A \rightarrow L$ , U

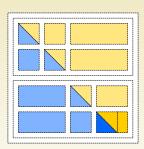
trsm:  $B \leftarrow BU^{-1}, B \leftarrow L^{-1}B$ 

gemm:  $C \leftarrow C - A \times B$ 

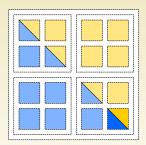
### Tiled Iterative



Slab Recursive



Tiled Recursive

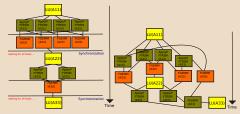


# Need for a high level parallel programming environment

### Features required

Portability, Performance and Scalability. But more precisely:

- Runtime system with good performance for recursive tasks.
- Dataflow task synchronization



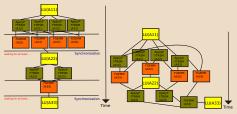
- Handle efficiently unbalanced workloads.
- Efficient range cutting for parallel for.

# Need for a high level parallel programming environment

### Features required

Portability, Performance and Scalability. But more precisely:

- Runtime system with good performance for recursive tasks.
- Dataflow task synchronization



- Handle efficiently unbalanced workloads.
- Efficient range cutting for parallel for.
- → Wish to design a code independently from the runtime system
- → Using runtime systems as a plugin

### Outline

- Runtime systems

### Runtime systems to be supported

### OpenMP3.x and 4.0 supported directives: (using libgomp)

- Data sharing attributes:
  - OMP3 shared: data visible and accessible by all threads
  - OMP3 firstprivate: local copy of original value
  - OMP4 depend: set data dependencies
- Synchronization clauses: #pragma omp taskwait

### xKaapi: via the libkomp [BDG12] library:

- OpenMP directives → xKaapi tasks.
- Re-implem. of task handling and management.
- Better recursive tasks execution.

### TBB: designed for nested and recursive parallelism

- parallel\_for
- tbb::task\_group, wait(), run() using C++11 lambda functions



### **PALADIn**

### Parallel Algebraic Linear Algebra Dedicated Interface

### Mainly macro-based keywords

- No function call runtime overhead when using macros.
- No important modifications to be done to original program.
- Macros can be used also for C-based libraries.

### Complementary C++ template functions

- Implement the different cutting strategies.
- Store the iterators

### PALADIn description: task parallelism

### Task parallelization: fork-join and dataflow models

- PAR\_BLOCK: opens a parallel region.
- SYNCH\_GROUP: Group of tasks synchronized upon exit.
- TASK: creates a task.
  - REFERENCE (args...): specify variables captured by reference. By default all variables accessed by value.
  - READ (args...): set var. that are read only.
  - WRITE (args...): set var. that are written only.
  - READWRITE (args...): set var. that are read then written.

#### Example:



### Outline

- Runtime systems
- Matrix Multiplication
- 3 TRSM
- Parallel exact Gaussian elimination

### Parallel matrix multiplication

#### Iterative variants

- Fixed block size (FIXED, GRAIN)
  - Better control of data mapping in memory
  - Complexity:  $O(n^3)$
- Fixed number of tasks (THREADS)
  - Less control of data mapping in memory
  - Complexity:  $O(n^{\omega})$

#### Recursive variants

- Almost no control of data mapping in memory
- Complexity:  $O(n^{\omega})$  or  $O(n^3)$



### Performance of pfgemm

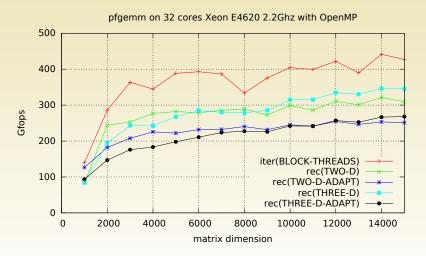


Figure: Speed of MatMul variants using OpenMP tasks

### Performance of pfgemm

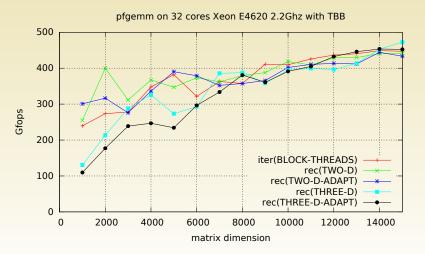


Figure: Speed of MatMul variants using IntelTBB tasks

### Performance of pfgemm

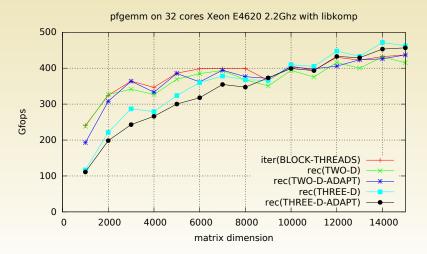


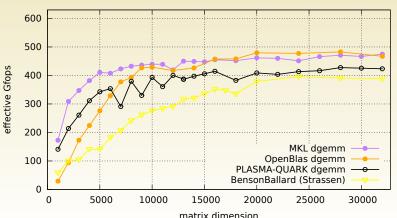
Figure: Speed of MatMul variants using XKaapi tasks



### Parallel Matrix Multiplication: State of the art

HPAC server: 32 cores Xeon E4620 2.2Ghz (4 NUMA sockets)

Comparison of our best implementations with the state of the art numerical librarie:



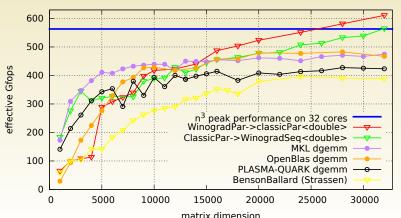


### Parallel Matrix Multiplication: State of the art

HPAC server: 32 cores Xeon E4620 2.2Ghz (4 NUMA sockets)

Effective Gfops = # of field ops using classic matrix product time.

Comparison of our best implementations with the state of the art numerical libraries



#### Outline

- Runtime systems
- 2 Matrix Multiplication
- **3** TRSM
- Parallel exact Gaussian elimination

### Parallel Triangular Solving Matrix

#### Iterative variant:

$$\left[\begin{array}{c|c}X_1 & \ldots & X_k\end{array}\right] \leftarrow L^{-1} \left[\begin{array}{c|c}B_1 & \ldots & B_k\end{array}\right].$$

- The computation of each  $X_i \leftarrow L^{-1}B_i$  is independent
- k sequential tasks set as the number of available threads

#### Recursive variant:

1: Split 
$$\begin{bmatrix} X_1 \\ X_2 \end{bmatrix} = \begin{bmatrix} L_1 \\ L_2 & L_3 \end{bmatrix}^{-1} \begin{bmatrix} B_1 \\ B_2 \end{bmatrix}$$

- 2:  $X_1 \leftarrow L_1^{-1}B_1$
- 3:  $X_2 \leftarrow B_2 L_2 X_1$  // Parallel MatMul
- 4:  $X_2 \leftarrow L_2^{-1}BX_2$

### Parallel Triangular Solving Matrix

#### Iterative variant:

$$\left[\begin{array}{c|c}X_1 & \dots & X_k\end{array}\right] \leftarrow L^{-1} \left[\begin{array}{c|c}B_1 & \dots & B_k\end{array}\right].$$

- The computation of each  $X_i \leftarrow L^{-1}B_i$  is independent
- k sequential tasks set as the number of available threads

#### **Recursive variant:**

1: Split 
$$\begin{bmatrix} X_1 \\ X_2 \end{bmatrix} = \begin{bmatrix} L_1 \\ L_2 & L_3 \end{bmatrix}^{-1} \begin{bmatrix} B_1 \\ B_2 \end{bmatrix}$$

- 2:  $X_1 \leftarrow L_1^{-1}B_1$
- 3:  $X_2 \leftarrow B_2 L_2 X_1$  // Parallel MatMul
- 4:  $X_2 \leftarrow L_3^{-1}BX_2$

#### Hybrid PFTRSM: column dimension of B small

- use iterative splitting in priority
- when #cols(X) < #proc: save some threads for recursive calls

Runtime systems Matrix Multiplication TRSM Parallel Exact Gaussian elimination Conclusion

### Parallel Triangular Solving Matrix Experiments

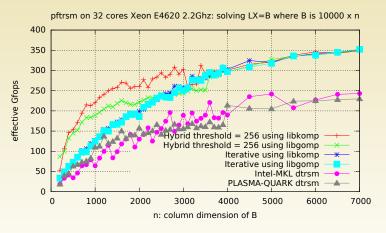


Figure: Comparing the Iterative and the Hybrid variants for parallel FTRSM using libkomp and libgomp. Only the outer dimension varies: B and X are  $10000 \times n$ .



#### Outline

- Runtime systems
- 2 Matrix Multiplication
- 3 TRSM
- Parallel exact Gaussian elimination

time systems Matrix Multiplication TRSM Parallel Exact Gaussian elimination Conclusion

### Gaussian elimination design

#### Reducing to MatMul: block versions

- ightarrow Asymptotically faster  $(O(n^{\omega}))$
- → Better cache efficiency

#### Variants of block versions

#### Split on one dimension:

→ Row or Column slab cutting

#### Split on 2 dimensions:

 $\rightarrow$  Tile cutting



Slab iterative Slab recursive



Tile iterative Tile recursive

Runtime systems Matrix Multiplication TRSM Parallel Exact Gaussian elimination Conclusion

### Gaussian elimination design

#### Reducing to MatMul: block versions

- ightarrow Asymptotically faster  $(O(n^{\omega}))$
- → Better cache efficiency

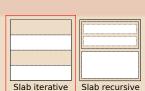
#### Variants of block versions

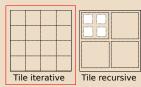
#### Iterative:

- Static → better data mapping control
- Dataflow parallel model → less sync

#### Recursive:

- Adaptive
- sub-cubic complexity
- No Dataflow → more sync





ntime systems Matrix Multiplication TRSM Parallel Exact Gaussian elimination Conclusion

### Gaussian elimination design

#### Reducing to MatMul: block versions

- ightarrow Asymptotically faster  $(O(n^{\omega}))$
- → Better cache efficiency

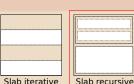
#### Variants of block versions

#### Iterative:

- Static → better data mapping control
- Dataflow parallel model → less sync

#### Recursive:

- Adaptive
- sub-cubic complexity
- No Dataflow → more sync





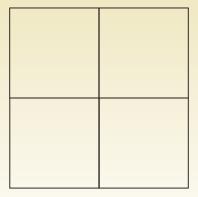








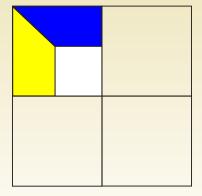




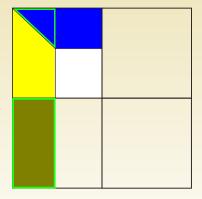
 $2 \times 2$  block splitting

ntime systems Matrix Multiplication TRSM Parallel Exact Gaussian elimination Conclusion

### Parallel tile recursive PLUQ algorithm

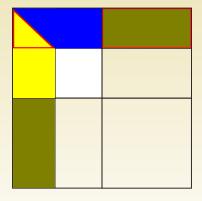


Recursive call



```
ptrsm: B \leftarrow BU^{-1}

TASK(MODE(READ(A) READWRITE(B)), pftrsm(..., A, Ida, B, Idb));
```

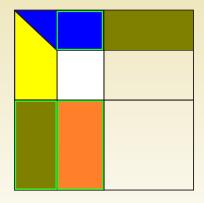


ptrsm: 
$$B \leftarrow L^{-1}B$$

 $\begin{array}{ll} \mathsf{TASK}(\mathsf{MODE}(\mathsf{READ}(\mathsf{A})\ \mathsf{READWRITE}(\mathsf{B}))\,,\\ \mathsf{pftrsm}\,(\ldots,\ \mathsf{A},\ \mathsf{Ida}\,,\ \mathsf{B},\ \mathsf{Idb}\,))\,; \end{array}$ 



Conclusion

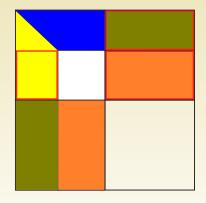


```
\texttt{pfgemm:} \ C \leftarrow C - A \times B
```

 $\begin{array}{ll} \mathsf{TASK}(\mathsf{MODE}(\mathsf{READ}(\mathsf{A},\mathsf{B})\ \mathsf{READWRITE}(\mathsf{C}))\,,\\ \mathsf{pfgemm}\,(\ldots\,,\ \mathsf{A},\ \mathsf{Ida}\,,\ \mathsf{B},\ \mathsf{Idb}\,))\,; \end{array}$ 



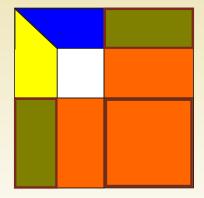
#### Parallel Exact Gaussian elimination Conclusion



$$pfgemm: C \leftarrow C - A \times B$$

TASK(MODE(READ(A,B) READWRITE(C)), pfgemm (..., A, Ida, B, Idb));





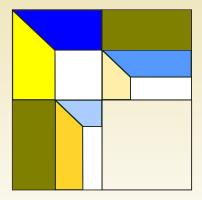
pfgemm: 
$$C \leftarrow C - A \times B$$

TASK(MODE(READ(A,B) READWRITE(C)), pfgemm (..., A, Ida, B, Idb));



titime systems Matrix Multiplication TRSM Parallel Exact Gaussian elimination Conclusion

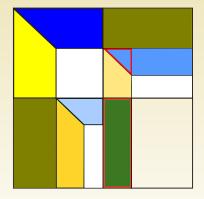
# Parallel tile recursive PLUQ algorithm



2 independent recursive calls (concurrent  $\rightarrow$  tasks)

```
TASK(MODE(READWRITE(A)),
     ppluq(..., A, Ida));
```

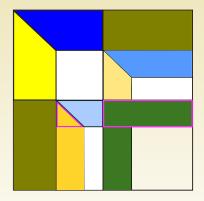




```
ptrsm: B \leftarrow BU^{-1}

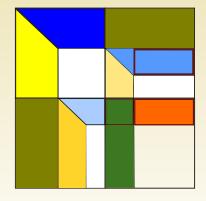
TASK(MODE(READ(A) READWRITE(B)), pftrsm(..., A, Ida, B, Idb));
```





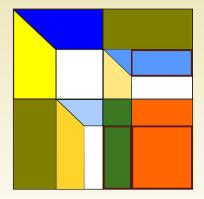
ptrsm: 
$$B \leftarrow L^{-1}B$$

 $\begin{array}{ll} \mathsf{TASK}(\mathsf{MODE}(\mathsf{READ}(\mathsf{A})\ \mathsf{READWRITE}(\mathsf{B}))\,,\\ \mathsf{pftrsm}\,(\ldots,\ \mathsf{A},\ \mathsf{Ida}\,,\ \mathsf{B},\ \mathsf{Idb}\,))\,; \end{array}$ 



$$pfgemm: C \leftarrow C - A \times B$$

TASK(MODE(READ(A,B) READWRITE(C)), pfgemm (..., A, Ida, B, Idb));

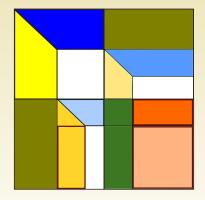


pfgemm: 
$$C \leftarrow C - A \times B$$
  
TASK(MODE(READ(A,B) READWRITE(C)),





Conclusion



pfgemm: 
$$C \leftarrow C - A \times B$$

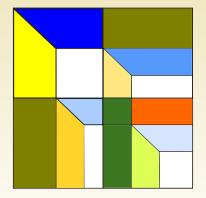
TASK(MODE(READ(A,B) READWRITE(C)), pfgemm(..., A, Ida, B, Idb));



Conclusion

intime systems Matrix Multiplication TRSM Parallel Exact Gaussian elimination Conclusion

### Parallel tile recursive PLUQ algorithm

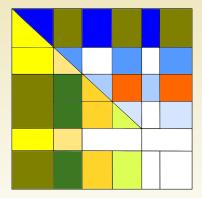


Recursive call



ntime systems Matrix Multiplication TRSM Parallel Exact Gaussian elimination Conclusion

### Parallel tile recursive PLUQ algorithm



#### Puzzle game (block permutations)

Tile rec: better data locality and more square blocks for M.M.

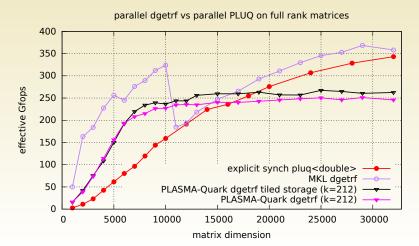


Runtime systems Matrix Multiplication TRSM Parallel Exact Gaussian elimination Conclusion

### State of the art: exact vs numerical linear algebra

#### State of the art comparison:

- Exact PLUQ using PALADIn language: best performance with xKaapi
- Numerical LU (dgetrf) of PLASMA-Quark and MKL dgetrf

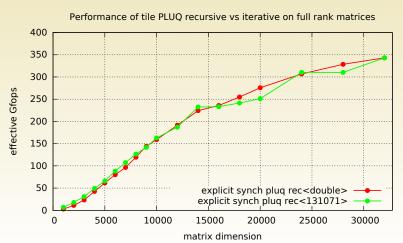


Runtime systems Matrix Multiplication TRSM Parallel Exact Gaussian elimination Conclusion

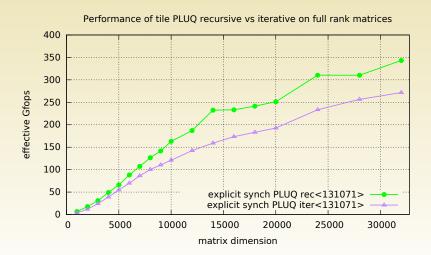
# Performance of parallel PLUQ decomposition

#### Low impact of modular reductions in parallel

→ Efficient SIMD implementation

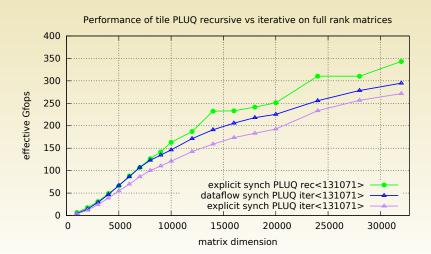


#### Performance of task parallelism: dataflow model





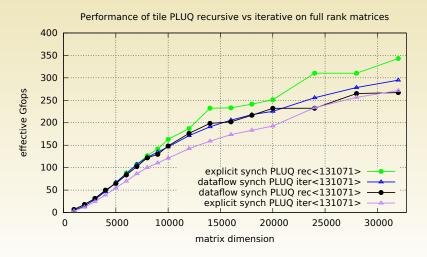
#### Performance of task parallelism: dataflow model





Runtime systems Matrix Multiplication TRSM Parallel Exact Gaussian elimination Conclusion

### Performance of task parallelism: dataflow model



Possible improvement: implementation of the delegation of recursive tasks dependencies (Postpone access mode in the parallel programming environments)



#### Outline

- Runtime systems
- Matrix Multiplication
- **3** TRSM
- Parallel exact Gaussian elimination

#### Conclusion

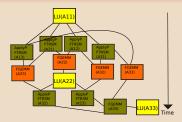
#### Lessons learnt for the parallelization of LU over $\mathbb{Z}/p\mathbb{Z}$

- Blocking impacts arithmetic cost ⇒fine granularity hurts
- Rank deficiency can offer more parallelism (cf. separators)
- sub-cubic perfs in parallel
- requires a runtime efficient for recursive tasks (XKaapi)

ntime systems Matrix Multiplication TRSM Parallel Exact Gaussian elimination Conclusion

### Perspectives

#### Data flow task dependencies



- already at use in tiled iterative algorithms (XKaapi)
- new challenges for recursive tasks:
  - Recursive inclusion of sub-matrices
  - Postponed modes (removing fake dependencies)
- Distributed on small sized clusters

Thank you