Master degree internship

LU factorization of matrices over $\mathbb{F}_p$: *Efficient computation on GPUs*

INFORMATIONS

Place: Université Montpellier 2, laboratoire LIRMM (France)

Research team: ARITH - www.lirmm.fr/arith

Supervisor: Pascal Giorgi - pascal.giorgi@lirmm.fr

Duration: 6 month

CONTEXT

The last two decades have seen impressive progress in exact linear algebra, and in particular regarding algorithm's complexity. Algorithms are now practicable and they turns out to be very efficient with good care on their implementations. For instance, we can cite Coppersmith/Wiedemann's algorithms which enable to solve huge sparse linear systems over finite fields and which is quite successful with integer factorization problems or with discrete logarithm breaking problems [5, 6]. However, if one want to attack such intensive computing challenges (e.g. solving linear systems with more than 1 000 000 equations) one has to set up and use large clusters of CPU-based machines, which could become even more challenging by itself.

Generally, most of exact linear algebra algorithms have good intrinsic parallelism either on data and/or on instructions and are well suited to be implemented in a massively parallel computational environment. The use of HPC-oriented GPU is therefore quite natural to extend the limits of nowadays CPU-based solutions for exact linear algebra problems and this alternative sounds really promising.

OBJECTIVE

One of the major difficulty of implementing exact computation on any devices is the diversity of the computational domains (e.g. finite field, rational numbers, integers, polynomials, ...). Nevertheless, word-size finite field computation play a central role in exact exact linear algebra since it is used as a basic tool for computations over most of the others domains (e.g. rationals and integers through Chinese Remainder Algorithm). Therefore, doing efforts on this domain is a pretty good starting point. We have demonstrated in [3, 4] that a good way to achieve *high performance* for linear algebra over word-size finite field is to re-use well know BLAS library. Our idea is to control *a priori* numerical computation to achieve exact computation and then perform delayed modular reduction to get the result over the finite field. If the number of available bits in the mantissa of floating point numbers for a particular device is β then one can perform a $n \times n$ matrix multiplication over the prime field $\mathbb{F}_p$ by simply doing a numerical matrix multiplication followed by modular reduction in $\mathbb{F}_p$ assuming the following relation hold

$$n(p-1)^2 < 2^\beta.$$

This approach reveals quite valuable for matrix multiplication over finite fields since it allows similar performance as with BLAS library [4].

The first part of this work is then to re-use CUBLAS library to possibly provide an efficient matrix multiplication over fixed precision finite field over GPU. As in [4], the goal is to provide a CUDA implementation for the Strassen-Winograd matrix multiplication over finite field which should enable to outperform numerical computations. Following this work, the study of LU factorization of matrices over a finite field $\mathbb{F}_p$ will be done. In particular, the question will be weather we can efficiently re-use matrix multiplication to provide LU factorization or what do we need to fulfill expected efficiency. One of the main objective here is to provide a GPU equivalence to the FLAS and FFPACK package [4].

References

[1] Giorgi, P., Jeannerod, C.-P., and Villard, G. 2003. On the complexity of polynomial matrix computations. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, Philadelphia, Pennsylvania, USA*, R. Sendra, Ed. ACM Press, New York, 135–142.

[2] Eberly, W.; Giesbrecht, M.; Giorgi, P.; Storjohann, A.; Villard, G.. Solving sparse integer linear systems. Proc. ISSAC'06, Genova, Italy, ACM Press, 63-70, July 2006.

[3] Jean-Guillaume Dumas, Pascal Giorgi, and Clément Pernet. FFPACK: Finite field linear algebra package. In Jaime Gutierrez, editor, *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, Santander, Spain*, pages 119–126. ACM Press, New York, July 2004.

[4] Jean-Guillaume Dumas, Pascal Giorgi, and Clément Pernet. Dense linear algebra over prime fields. *ACM Transactions on Mathematical Software*, 35:(3), 2008.

[5] Milan, J. Factoring Small Integers: An Experimental Comparison, 2007. Tech. Report http://hal.inria.fr/inria-00188645/en.

[6] Montgomery, P.–L.; Kruppa, A. Improved Stage 2 to P$\pm$1 Factoring Algorithms, 2007. Tech. Report http://hal.inria.fr/inria-00188192/en.

[7] Volkov, V., and Demmel, J. W. Benchmarking GPUs to tune dense linear algebra, 2008. ACM/IEEE Conference on Supercomputing (SC08), 2008.