ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Computer Science Department
Advanced Computing Laboratory

Extreme scale integer multiplication in GPU

Master's Thesis

Advisors: Joao Rivera, Prof. Markus Püschel

1. Project Description

Multiplication of very large integers is the core computation of many algorithms and has applications in many fields, e.g., in cryptography, symbolic computations, number theory, etc. One of fastest algorithms to multiply two big integers is the one proposed by Schönhage–Strassen [1] which is based on the fast Fourier transform (FFT). Implementations of this algorithm using floating-point can unfortunately lead to numerical error that may lead to incorrect result [2,3]. These numerical errors however are likely to lead to incorrect results only for very big integers and can be overcame using a higher floating-point precision, e.g. double-double [4]. In this project we would like to take advantage of the efficient support of floating-point arithmetic in current GPUs to implement big integer multiplication. We would like to push the input sizes as large as possible till we are restricted either by the limitation of the hardware or by the limitation of the numerical errors during the computation. Interval arithmetic [5,6] will be used for the computations to bound the numerical error guarantee that it stays small enough to be useful.

2. Specific Goals

- Review the related work.
- Implement an interval arithmetic library for GPUs possibly supporting double-double arithmetic.
- Use the library to implement extreme scale integer multiplication.
- Evaluate thoroughly the performance of the approach.
- Maintainability and extendibility of the code should receive high priority.

3. Deliverables

- The source code of the implementation.
- A digital and two printed exemplars of the bachelor thesis containing a detailed description of the problem, an overview of related work and existing approaches, a description of the tool that was built, and evaluation of results.

4. Organization

- The student will have weekly or biweekly meetings with her advisors in which progress and occasional problems will be discussed.

Contact

If you are interested in pursuing this master thesis, please contact hector.rivera@inf.ethz.ch or pueschel@inf.ethz.ch.

References

[1] A. Schönhage and V. Strassen. *Schnelle Multiplikation großer Zahlen*. Computing, 7:281–292, 1971.

[2] http://www.cs.rug.nl/~ando/pdfs/Ando_Emerencia_multiplying_huge_integers_using_fourier_transforms_paper.pdf

[3] http://numbers.computation.free.fr/Constants/Algorithms/fft.html

[4] T. J. Dekker, "*A floating-point technique for extending the available precision*," Numerische Mathematik, vol. 18, no. 3, pp. 224–242, 1971.

[5] R. E. Moore, "*Interval analys*is," Prentice-Hall, 1966.

[6] J. Rivera, F. Franchetti, M. Püschel. "An interval compiler for sound floating-point computations", *in International Symposium on Code Generation and Optimization (CGO)*. 2021.