Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

InIT Institut für angewandte
Informationstechnologie

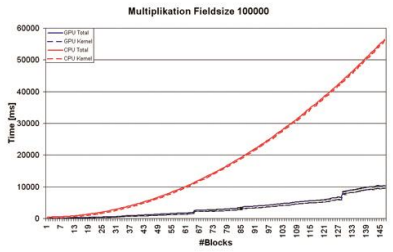
Arbitrary Precision Integer Arithmetik für Grafikprozessoren

Diplomierende
Lukas Funk
Felix Rohrer

Dozierende
Daniel Bachofen
Samuel Beer

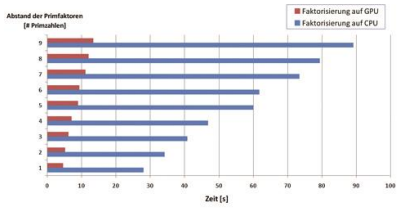
Das Thema dieser Bachelorarbeit war die Implementierung einer Software, die Grundrechenoperationen
für beliebig grosse Zahlen auf Grafikkarten ausführen kann. Die Hoffnung bestand, rechenintensive Operationen dadurch performanter zu machen.

Aufbauend auf einer bereits bestehenden Bibliothek, die mit sogenannten Bignums
(beliebig grosse Zahlen) auf der CPU rechen kann, wurden Addition, Subtraktion,
Multiplikation, Division, Modulo, Exponentiation und modulare Exponentiation für die
Verwendung von GPUs (Graphics Processing Unit) implementiert. Dazu wurde eine
Erweiterung der C-Programmiersprache verwendet, die von NVIDIA entwickelt wurde.
Diese wird unter dem Namen CUDA (Compute Unified Device Architecture) zur Verfügung
gestellt. Die Erweiterung ermöglicht es, die Leistung von NVIDIA-Grafikkarten
auch für nicht grafische Anwendungen zu verwenden.



Die durchgeführten Leistungstests zeigten eine deutliche Geschwindigkeitszunahme. Beim Beispiel der Multiplikation wurde ein Speedup von 5.5x erreicht. Getestet wurden Zahlen bis zu einer Länge von 4116 Bits. (rot: CPU, blau: GPU)

Im Leistungsvergleich wurde festgestellt, dass die GPU-Berechnungen im Vergleich
zu den CPU-Berechnungen je nach Operation 4-10 Mal schneller waren. Vor allem
bei zeitlich kostspieligen Operationen wie der Modulo-Operation konnten sehr grosse
Leistungsunterschiede ausgemacht werden. Auf einer Grafikkarte können, im Gegensatz
zu CPUs, Millionen von gleichzeitigen Prozessen, sogenannte Threads, abgearbeitet
werden, was sich auch in den erhaltenen Resultaten widerspiegelt.



Die Faktorisierung von zusammengesetzten Zahlen mit ähnlich grossen Primfaktoren kann durch die Verwendung einer Grafikkarte um ein Vielfaches schneller durchgeführt werden. (GPU: rot, CPU: blau)

Alle eigens implementierten Algorithmen wurden auf ihre Leistung und Richtigkeit
hin eingehend geprüft und bieten eine solide Grundlage für weiterführende Projekte.
Denkbar ist zum Beispiel die Implementierung kryptologischer Verfahren, basierend
auf der in dieser Bachelorarbeit erstellten Arithmetik-Bibliothek.