DPHPC Project Proposal

Neville Walo, Basil Fürer

October 26, 2020

Fast Hashing with GPU

Hashing finds many applications today and often we are interested in fast computation of a lot of hashes. This is mostly due to the rise of cryptocurrencies but it also has applications in generating rainbow tables.
Many cryptocurrencies are based on the notion of a *proof of work*, a process with a low probability of succeeding. For example, Bitcoin asks its miners to do a proof of work that includes all of the data in the current block. This process is based on the SHA-256 hashing function. [1]

The goal of this project is to accelerate hash computations by using a GPU. SHA-256 [2] used in the Bitcoin protocol has a lot sequential dependencies and a single hash computation is unlikely to be parallelizable, however the computation of many different hashes in parallel is possible. Our project consists of the following milestones:

- literature research, settling for a concrete hash function $H(\cdot)$ $(\star)$
- implement H with CUDA [3] $(\star\star\star)$
- evaluate and benchmark our implementation against existing implementations [4] $(\star\star)$

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.

[2] Quynh Dang. Changes in federal information processing standard (fips) 180-4, secure hash standard. *Cryptologia*, 37(1):69–73, 2013.

[3] NVIDIA Corporation. NVIDIA CUDA C programming guide, 2020. Version 11.1.0.

[4] Torsten Hoefler and Roberto Belli. Scientific benchmarking of parallel computing systems: Twelve ways to tell the masses when reporting performance results. In *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, SC '15, New York, NY, USA, 2015. Association for Computing Machinery.