Accelerating Shor’s Factorization Algorithm on GPUs

I. Savran,1,∗ M. Demirci,2,† and A. H. Yılmaz2,‡

1Department of Computer Engineering and
2Department of Physics, Karadeniz Technical University, 61080 Trabzon, Turkey
(Dated: November 8, 2018)

Shor’s quantum algorithm is very important for cryptography, since it can factor large numbers much faster than classical algorithms. In this study, we implement a simulator for Shor’s quantum algorithm on graphic processor units (GPU) and compare our results with Liquid—which is Microsoft quantum simulation platform—and two classical CPU-implementations. We evaluate 10 benchmarks for comparing our GPU implementation with Liquid and single-core implementation. The analysis shows that GPU vector operations is more suitable for Shor’s quantum algorithm. Our GPU kernel function is compute-bound, due to all threads in a block reach to the same element of the state vector. Our implementation has 52.5× speedup over single-core algorithm and 20.5× speedup over Liquid.

I. INTRODUCTION

In the past thirty years, quantum computing has received considerable attention regarding performance speedup in the IT Society. It focuses on developing computer technology based on the principles of quantum theory such as superposition, entanglement and interference. Especially, it can accept input states that represent a coherent superposition of many different possible inputs and then turn them into a corresponding superposition of outputs. Quantum computation have an effect simultaneously on each element of the superposition and it generates a massive parallel data processing, even within one piece of quantum hardware. It enables large improvements in computational efficiency such as Shor’s quantum algorithm for factoring large integers [1, 2], Grover’s algorithm for accelerating combinatorial searches [3] and quantum cryptography for secure communication [4, 5]. As a result, some problems that are difficult to solve in a classical computer can be effectively solved by a quantum computer. One problem of this type is factorization.

A well-known quantum algorithm for factorization is Shor’s algorithm. The computational resources increase exponentially with system size, and the simulation results are easily confirmed, making it an ideal test candidate. Many cryptographic protocols are based on the computational difficulty of obtaining the prime factors of a large number: a small increase in the size of the number causes an exponential increase in computational resources. However, such limitation does not appear in Shor’s quantum algorithm for prime number factorisation, and its realization represents a major challenge in quantum computation. This algorithm is a set of protocols that convert the factorization problem into a period detection problem.

Since the announcement of the NVIDIA Compute Unified Device Architecture (CUDA) [6] in 2008, graphic processor units (GPUs) computing has become widely adopted by the computing society. The GPU executes one or more kernels launched by the CPU. As compared to CPUs, a larger portion of their resources are devoted to functional units in GPUs. GPUs use smaller, nonexpandable DRAMs but have substantially higher memory bandwidth than CPUs. Most of the large-scale supercomputer installations equipped with computing accelerators, Intel Xeon Phi, NVIDIA and AMD Radeon are well known computing accelerators.

In this work we implement a simulator for Shor’s quantum algorithm on GPUs in order to compute the prime factors of a few integers. The inherit parallelism involved in simulating a quantum system makes it suitable for on GPUs implementations. We compare our results with those obtained from Liquid-Microsoft quantum simulation platform. In ref [7], they have reported results applying matrix product state to Shor’s algorithm.

The remainder of this work is organized as follows. Section II provides a review of Shor’s algorithm. Section III describes our implementation in detail. Section IV provides the numerical results related to finding the prime factors of several number and discusses for different implementations. Section V summarizes the highlights of the study.
II. A BRIEF INTRODUCTION TO SHOR’S ALGORITHM

We describe Shor’s algorithm from a functional point of view which means that it doesn’t deal with the implementation for a specific hardware architecture. A detailed information and implementation about the Shor’s algorithm can be found in references [8–10], for a more rigid mathematical description, please refer to [11, 12].

Shor’s algorithm tries to find even integer $p$, the period of $x^a \mod n$, where $n$ is the number to be factored and $x$ is an integer coprime to $n$. To do this, a quantum memory register with two parts is created by Shor’s algorithm as follows: $|r_1, r_2\rangle$. In the first part a superposition of the integers which are to be $a$’s in the $x^a \mod n$ function is placed by the algorithm. Here, $a$’s can be chosen to be the integers 0 through $q-1$, where $q$ is the power of 2 such that $n^2 \leq q < 2n^2$. In this step, the state of the quantum memory register is

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle. \tag{2.1}$$

Then $x^a \mod n$ is calculated, and the result is placed in the second part of the quantum memory register.

Next the state of the second register is measured by the algorithm, the one that includes the superposition of all possible outcomes for $x^a \mod n$. In this step, the state of the quantum memory register is given by

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \mod n\rangle. \tag{2.2}$$

Measuring this register has the effect of collapsing the state into some observed value, say $k$. This means that after this measurement the second part of the register contains the value $k$, and the first part of the register contains a superposition of the base states which when plugged into $x^a \mod n$ produce $k$. Because $x^a \mod n$ is a periodic function, the first part of the register will contain the values $c, c + p, c + 2p, \ldots$ and so on, where $c$ is the lowest integer such that $x^c \mod n = k$.

The next step is to perform a discrete Fourier transform (DFT) on the contents of first part of the register and to put the result back into register one. DFT when applied to a state $|a\rangle$ changes it in the following manner:

$$|a\rangle = \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi ac/q}|c\rangle \tag{2.3}$$

which is computed by the quantum computer. The application of the DFT has the effect of peaking the probability amplitudes of the first part of the register at integer multiples of the quantity $q/p$. Now measuring the first part of the quantum register will give an integer multiple of the inverse period. Once this number is retrieved from the quantum memory register, a classical computer can do some analysis of this number, make an estimation as to the actual value of $p$, and from that compute the possible factors of $n$.

III. IMPLEMENTATION

We now describe the details of our simulations and present our benchmarks. In conventional implementation, approximately 97% of the runtime is devoted to Quantum Fourier Transform (QFT) calculations. Therefore, we designed a GPU kernel function which computes QFT from scratch. The computations related to the evolution of the quantum system are carried out by thousands of threads inside a GPU. Each thread is assigned to compute each element of the result vector. This approach allows threads to access memory coalescingly.

The Quantum Fourier Transform

In quantum computing, QFT is a linear transformation on qubits and an essential part of many quantum algorithms, such as Shor’s factoring algorithm. The quantum computers can perform QFT efficiently, with a particular decomposition into a product of simpler unitary matrices. Using a simple decomposition, DFT can be implemented as a quantum circuit consisting of only $O(n^2)$ Hadamard and controlled phase shift gates, where $n$ is the number of qubits.

A typical four-qubit quantum circuit for the QFT is shown in Figure 1.

![FIG. 1. Standard quantum circuit for QFT on four qubits. $H$ is the Hadamard gate and other operators are controlled-phase gates.](image-url)
FIG. 2. (color online). (a) Block configuration and threads running order in GPU. Each color indicates a different block of threads. (b) By using more blocks, the workload of the threads can be reduced.

| Architecture    | Intel I7-2760QM | NVIDIA GTX285 | NVIDIA 970m |
|-----------------|-----------------|---------------|-------------|
| Processor Core  | Sandy Bridge    | Tesla 2.0     | Maxwell     |
| Threads/Core    | 4               | 30 (8 shaders) | 10 (128 shaders) |
| Clock Frequency | 2.2 GHz         | 648 Mhz       | 924 MHz     |
| Memory Bandwidth| 21.3 GB/s       | 159 GB/s      | 120 GB/s    |
| Power           | 45 W            | 204 W         | 81 W        |

Hadamard gate is represented by a 2 by 2 matrix and controlled phase operators are 4 by 4 matrices. A system of $n$-qubit is expressed by $2^n$ values with a tensor product. The QFT operator is also specified by a matrix of $2^n \times 2^n$. Unfortunately, after measurements, collapsed states cannot easily be converted to qubits. Therefore, it is easier to multiply $2^n \times 2^n$-QFT matrix by $2^n$ state vector.

In Figure 2(a) we give a block configuration and running order in GPU. Here, the number of blocks is equal to $2^n$/(block size). Each thread computes each line which requires $2^n$ complex multiplications as follows:

$$V_k = \sum_{j=0}^{q} e^{i2\pi jk/q} V_j. \quad (3.1)$$

When we create more blocks to decrease computation load on the blocks, we need to allocate more space to handle semi-results, as shown in Figure 2(b).

Another idea is to compute complex QFT matrix before the transform operation. In this case only two complex matrix and two complex state vector will be transferred between CPU and GPU. Considering the memory bandwidth of GTX 285 and GTX 970m GPUs in Table I, we can conclude that whether our kernel has memory bottleneck. According to Table II, GPU transferring time is reasonable. But for factoring large integers the memory capacity is not efficient. For a 8-qubit system about 32 GB space required which is unfeasible with current devices.

### IV. EXPERIMENTAL RESULTS

In this section, we describe the experimental environment and discuss the performance of our implementations. We have utilized GPUs and CPU for benchmark tests. The differences in micro-architectural philosophy between NVIDIA GPUs and CPU used for all test results are shown in Table I. The experimental computer system contains 8 GB of memory whereas the GPU device has only 3 GB. This difference between the memory sizes of host and the GPU requires frequent data transfers. Theoretical performance of a computing device could be estimated by multiplying the number of cores, core clock speed,
TABLE III. The performance results for factorization. Here, all the execution times are in seconds. $T_{H,F,L,liquid}$ represent the timing result of Hayward, Fast-Hayward and Liquid, respectively. $T_{G285,G970m}$ refer to the timing result of GPU GTX285 and GTX970m, respectively.

| n  | Cofactors | $T_H$ | $T_{FH}$ | $T_{Liquid}$ | $T_{G285}$ | $T_{G970m}$ |
|----|-----------|-------|---------|--------------|------------|-------------|
| 77 | 7×11      | 111.462 | 3.205 | 47.125 | 0.725 | 1.167 |
| 143| 11×13     | 114.015 | 34.841 | 189.523 | 3.236 | 1.791 |
| 323| 17×19     | 1915.227 | 462.850 | 1171.650 | 45.424 | 21.375 |
| 551| 19×29     |         |         |         |         | 710.100 |
| 589| 19×31     |         |         |         |         | 952.166 |
| 231| 3×7×11    | 459.258 | 60.218 | 214.320 | 11.857 | 5.725 |
| 255| 3×5×17    | 1812.330 | 115.955 | 195.579 | 11.568 | 5.833 |
| 399| 3×7×19    | 4846.131 | 1126.599 | 180.153 | 83.675 |
| 423| 3×3×47    | 5130.147 | 1179.300 | 180.485 | 85.140 |
| 539| 7×7×11    | 11645.820 | 6705.252 | 714.752 |

| Cofactors | Speed-up |
|-----------|----------|
| 2         | 52.5     |
| 3         | 20.5     |
|           | 2.1      |
|           | 1.0      |

FMA and SIMD. The theoretical values of our CPU and GTX970m are 27.66 Gflop (Giga Floating-Point Operation) and 2657 Gflop per second, respectively.

We have tested our GPU implementation to find the prime factors of 10 integers. We compare the timing results with Hayward, optimized-Hayward [12] and Liquid [13]. Hayward and optimized-Hayward implementations run on single CPU-core. Liquid is the Microsoft quantum simulation platform and it is fairly optimized for CPUs. Table III shows the performance results from factorization, using Intel I7-2760QM, NVIDIA GTX285 and NVIDIA 970m. In this table, gray cells indicate that no results are obtained due to a memory fault occurred or the computation lasted over 3 hours. Furthermore, speedup-values are calculated according to run-time values in blue cells and timing values of GTX970m are determined as reference. As seen in Table III, GTX970m has 52.5× speedup over Fast-Hayward, 20.5× speedup over Liquid and 2.1× speedup over GTX285. These results show a significant performance improvement when using a GPU. Consequently, it is clear that the algorithm is achieving its goal of accelerating of the factorization computation on the GPU.

V. CONCLUSION

We have proposed a GPU implementation of Quantum Fourier Transform. For this we have presented a simulator for Shor’s quantum algorithm on GPUs and compare our results with Liquid and two CPU-implementations. Due to transferring data is not a bottleneck (see Table II), our QFT kernel is limited by compute-bound of the GPUs. We achieved 52.5x, 20.5x speedup against the classical transform function and Liquid respectively.

[1] P.W. Shor, Proc. 35th Annu. Symp. Found. of Comput. Sci., pp. 124134 (1994).
[2] P.W. Shor, SIAM J.Sci. Statist.Comput. 26, 14841509 (1997).
[3] L. K. Grover, Phys. Rev. Lett. 79, 325-328 (1997).
[4] S. Wiesner, Sigact News 15, 78-88 (1983).
[5] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol. 5, 3-28 (1992).
[6] NVIDIA, “CUDA Toolkit”, https://developer.nvidia.com/cuda-toolkit, 2017.
[7] D. S. Wang, Charles D. Hill and L. C. L. Hollenberg, Quantum Inf. Processing 16,176 (2017).
[8] D. Beckman, A. N. Chari, S. Devabhaktuni and J. Preskill, Phys. Rev. A 54, 1034 (1996).
[9] J. A. Jones, Progr. NMR Spectr. 38, 325360 (2001).
[10] L.M.K., Vandersypen et al. Phys. Rev. Lett. 85, 54525455 (2000).
[11] A. Ekert and R. Jozsa, Rev. Mod. Phys. 68, pp.733-753 (1996).
[12] M. Hayward, Illinois Mathematics and Science Academy 1, 1-61 (2005).
[13] D. Wecker, and K. M. Svore, LIQUID: A Software Design Architecture and Domain-Specific Language for Quantum Computing, 2014.