



AAD - Assignment 1

107474-Joseane Pereira
109050-Gabriel Costa
Universidade de Aveiro, DETI

December 2, 2024

Contents

1	Introduction	3
2	Method	3
2.1	AVX and AVX2	3
2.2	OpenMP	4
2.3	CUDA	4
3	Results	4
4	Conclusions	5

1 Introduction

In this assignment we were tasked with implementing search functions for a cryptocurrency, "**deti coin**", using many different search algorithms and type of instructions.

This coin is a file with exactly 52 bytes whose MD5 message-digest1, when printed in hexadecimal, ends with at least 8 hexadecimal zeros (i.e., its last 32 bits are all 0). The file contents must begin with "DETI coin " (note the space at the end) and must end with a newline ('\n' in C). The other bytes may have arbitrary values, but it is strongly recommended that these other bytes encode utf-8 text.

Having this in mind, we implemented the following suggested search methods:

- **AVX** - We used the AVX intrinsics to implement the search function.
- **AVX2** - We used the AVX2 intrinsics to implement the search function.
- **OpenMP** - We used OpenMP to parallelize the AVX2 search function as is the fastest one.
- **CUDA** - We used CUDA instructions to implement the search function.

2 Method

2.1 AVX and AVX2

For the AVX implementation, part of the code was already provided to us, so our task was to only implement the search function. To achieve this, we initialized all lanes with the standard DETI coin format. To introduce variety, we modified a given integer of the coin (stored as **v1** in each lane) by adding the lane number.

To maintain continuous variety across iterations, we increment the **v1** value in each lane by the total number of lanes (4). To ensure these values remain within the ASCII range, we utilized the "next_value_to_try_ascii" function. If **v1** overflows, we increment the next integer (**v2**) and reset **v1** to its initial value.

The AVX2 implementation required only minor adjustments to the AVX code, as it processes 8 lanes instead of 4.

2.2 OpenMP

For OpenMP we used the AVX2 search function and parallelized it using OpenMP. We used the pragma **#pragma omp parallel for** to parallelize the search function. Similiar to the AVX2 implementation, we initialized all lanes with the standard DETI coin format. To introduce variety, we modified a given integer of the coin (stored as **v1** in each lane) by adding the thread number, and at the end all the numbers of the attempts as well as the coins found are summed giving the result complete result. This way we ensure that each thread will explore different possibilities of coins.

2.3 CUDA

For CUDA, we initialized the **hash_size** with 0 since the hashes are not being stored. Instead, each thread calculates a hash, and if it meets the condition of ending with 8 hexadecimal zeros, the corresponding **coin** is saved in a shared list accessible by all threads. This shared list is defined in "deti_coins_cuda_search.h" and has its first index set to 1, indicating the next available position. When a thread finds a valid coin, it uses **atomicAdd** to increment this index by 13 (which represents the size of the coin), updating the next available position in the list.

To generate a coin, each thread initializes its own unique candidate coin using the "v1" and "v2" values passed to them in the parameters. The thread modifies a specific part of the coin by adding its thread number (n) to an integer in the coin, while ensuring the values remain within the ASCII range. Each thread generates and evaluates 95 potential coins before completing its execution.

To ensure that the threads explore different coin possibilities in successive runs, 95 (or 0x5E in hexadecimal) is added to the "v1" value for each iteration. If it overflows, we add 1 to the v2 value. The "next_value_to_try_ascii" variable ensures that the values remain within the valid ASCII range.

3 Results

After implementing the search functions, we conducted experiments to evaluate the performance of each method. We measured the time taken to find a valid DETI coin, the number of attempts made, and the number of coins found. The experiments were conducted on two different systems: one with a AMD Ryzen 5 4600H and NVIDIA GeForce RTX 2060 and another with a intel core i7-11370H and a NVIDIA GeForce RTX 3060.

Method	Time (h)	N of attempts	coins found
AVX	1	$9.07 * 10^{10}$	1
AVX2	1	$1.51 * 10^{11}$	1
OpenMP(avx2)	1	$1.17 * 10^{12}$	1
CUDA	1	$4.06 * 10^{13}$	1

Table 1: Results of the experiments on a AMD Ryzen 5 4600H and NVIDIA GeForce RTX 2060

Method	Time (h)	N of attempts	coins found
AVX	1	$9.57 * 10^{10}$	2
AVX2	1	$1.50 * 10^{11}$	3
OpenMP(avx2)	1	$7.93 * 10^{11}$	9
CUDA	1	1	1

Table 2: Results of the experiments on a intel core i7-11370H and a NVIDIA GeForce RTX 3060

4 Conclusions

In this assignment, we explored various parallel computing methods to implement a search function for generating valid DETI coins. Each method leveraged different technologies, ranging from vectorization with AVX/AVX2 to multithreading with OpenMP and GPU programming with CUDA. The performance of these methods varied significantly, reflecting the strengths and limitations of the underlying architectures.

From our results, CUDA demonstrated the highest efficiency, significantly outperforming the other approaches in terms of the number of attempts per unit time. This is attributed to the massive parallelism provided by GPU threads, which is ideal for the highly parallel nature of this search problem. OpenMP, when combined with AVX2, also delivered notable performance improvements over standalone AVX2 by utilizing multithreading on the CPU. Lastly, AVX and AVX2 provided a solid baseline, with AVX2 benefiting from the increased lane count for processing data.

The key takeaway is that leveraging hardware-specific optimizations can yield dramatic improvements in computational efficiency. CUDA, with its specialized GPU capabilities, is the best choice for this problem, especially when scalability and performance are the primary objectives. OpenMP provides a strong alternative for systems where GPU resources are unavailable.

Overall, this assignment reinforced the importance of understanding and effectively utilizing the strengths of different parallel computing frameworks.

Each method showcased unique advantages that can be leveraged based on specific hardware and performance requirements.