# Laboratorul #1

## Tema:

Programarea paralelă şi distribuită cu ajutorul librăriilor OpenMP şi OpenMPI. Legea lui Amdahl

### Obiectiv:

Acest laborator are obiectivul de a face studenţii familiari cu tehnicile de programare paralelă şi distribuită cu ajutorul librăriilor OpenMP şi OpenMPI în limbajul C++.

### Descriere context:

Se dă o aplicaţie scrisă în limbajul C++ care încearcă să rezolve un crypto-puzzle similar celor pe care le rezolva minnerii de Bitcoin și Eutherium, și anume, găsește un un șir de caractere care adăugat șirului de caractere ”Hello World” și asupra căruiva va fi aplicat algoritmul de hash SHA-256 va genera un cod hash care va avea un număr predefinit de 0-uri la începutul hash-ului.

**Exemplu:**

SHA256(”Hello World”) →

”a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e”

Să presupune că vrem ca hash-ul nostru să înceapă cu un ”0”, pentru aceasta e nevoie să adăugăm la ”Hello World” caracterul ”2”

SHA256(”Hello World2”) →

”0de69f56365c10550d05e65ae8229dd0686f7894a807830daec8caa879731f4d”

Dacă numărul de căutat de 0-uri este 2 pentru această e nevoie să adaugăm la șirul de caractere inițial ”135”

SHA256(”Hello World135”) → ”005b70a99da108c694475b2f5a1db92e9b3a9414fe14b608f1647f77f2268969”

**Sarcina:**

1. Compilaţi codul propus în mapa ”default”. Rulați aplicația. Logați timpii de executare pentru diferite valori ai parametrului **n**. Ca exemplu puteți lua **n** egal cu 5, 6, 7.
2. Scrieți o aplicație care ar paraleliza codul propus cu ajutorul librăriei OpenMP. Algorimul de hash va rămîne neschimbat. Logați timpii de soluționare a crypto-puzzle-ului pentru valorile lui **n** din punctul 1). Schimbați numărul de fire de execuție pentru aplicația Dvs. Rulați codul și înregistrați rezultatele în tabela de mai jos.

**Tabel 1. Timpii de execuţie a aplicaţiei scrise cu ajutorul OpenMP**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Număr fire | 1 | 2 | 4 | 8 | 16 | 32 |
| Timp execuție |  |  |  |  |  |  |

1. Să se scrie o aplicaţie care va paraleliza codul propus cu ajutorul librăriei OpenMPI. Ca şi în cazul precedent algoritmul de soluționare a crypto-puzzle-ului trebuie să rămînă neschimbat. Completaţi tabela de mai jos:

**Tabel 2. Timpii de execuţie a aplicaţiei scrise cu ajutorul OpenMPI**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Număr procese | 1 | 2 | 4 | 8 | 16 | 32 |
| Timp execuție |  |  |  |  |  |  |

1. Scrieți un raport unde veți prezenta rezultatele din punctele 1-3.
2. Completați raportul cu următoarele date:

a) Comentaţi utilitatea acestor librării şi limitările din punct de vedere practic în contextul experienţei pe care o aveţi. În cazul lipsei experienței de dezvoltare a sistemelor, descrieți un sistem real unde sunt procese paralele și secvențiale. Faceți o analiza a gradului de paralelism.

b) Comendaţi datele din tabele în contextul legii lui Amdahl ([https://en.wikipedia.org/wiki/Amdahl%27s\_law](https://en.wikipedia.org/wiki/Amdahl's_law))

c) În trecut se practica păstrarea hash-ului la parola. Se alegea un oricare algoritm, de regula MD5. Acum această practică se consideră nesigură. Explicați care este atacul și care sunt practicile curente în acest caz.

**Suport:**

Se presupune că aveţi disponibil un calculator care are cel puţin două nuclee fizice (Multi core CPU).

Sistemul Dvs. poate rula Docker. În mapele **openmpi** şi **openmp** veţi găsi Dockerfile pentru a construi imaginea docker şi fişier pentru a rula containerul şi a face build la aplicaţia dezvoltată.

Urmaţi instrucţiunile din fişierele README în fişierul arhivă însoţitor.

Întrebările pot fi adresate pe email-ul: eugeniu.torica@isa.utm.md

**Barem Ciornă**

|  |  |
| --- | --- |
| **Criteriu de evaluare** | **Nota** |
| Înţelegere de bază a diferenţelor de principiu între soluţiile oferite de fiecare librărie. Abilitate de a da exemple practice unde principiile similare se regăsesc. Abilitate de a explica codul din lucrarea de laborator şi introduce modificari arbitrare cu anticiparea rezultatelor obţinute | 10 |
| Înţelegere de bază a diferenţelor de principiu între soluţiile oferite de fiecare librărie. Abilitate de a da exemple practice unde principiile similare se regăsesc. | 8 |
| Înţelegere de bază a diferenţelor de principiu între soluţiile oferite de fiecare librărie. | 6 |

**Cărţi recomandate:**

<https://pages.tacc.utexas.edu/~eijkhout/pcse/html/>

<http://perimeterinstitute.ca/personal/wcunningham/parallel.pdf>

<http://www.archer.ac.uk/training/course-material/2019/06/AdvOpenMP-manch/L01-OpenMPBasics.pdf>