# НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ УНИВЕРСИТЕТ «МИФИ» ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

### КАФЕДРА №42 «КРИПТОЛОГИЯ И КИБЕРБЕЗОПАСНОСТЬ»

# ЛАБОРАТОРНАЯ РАБОТА №3 ПО ДИСЦИПЛИНЕ «Параллельное программирование» НА ТЕМУ «Реализация алгоритма с использованием технологии ОрепМр»

Работу выполнил студент группы Б20-505 Остриков Денис

#### Рабочая среда:

```
3:24PM: neofetch
                                         piggy@warmachine
                 `000/
                                         os: Arch Linux x86_64
               `+0000:
                                         Host: 82FG IdeaPad 5 15ITL05
              `+000000:
                                         Kernel: 5.15.82-1-lts
                                         Uptime: 12 hours, 41 mins
              -+000000+:
            `/:-:++0000+:
                                         Packages: 1372 (pacman)
                                         Shell: zsh 5.9
                                         Resolution: 1920x1080
         `/+++0000000000000/`
                                         WM: i3
                                         Theme: Emacs [GTK2/3]
        ./ooosssso++osssssso+`
       .oossssso-```\ossssss+`
                                         Icons: ePapirus [GTK2/3]
      -osssssso.
                      :ssssssso.
                                         Terminal: alacritty
                                         Terminal Font: black: "
                       osssso+++.
     :osssssss/
    /osssssss/
                        +ssssooo/-
                                          CPU: 11th Gen Intel i5-1135G7 (8) @ 4.200GHz
  `/ossssso+/:-
                                         GPU: Intel TigerLake-LP GT2 [Iris Xe Graphics]
                       -:/tossssot-
 `+sso+:-`
                            `.-/+oso:
                                         Memory: 6723MiB / 15800MiB
                                 `-/+/
3:29PM: lscpu
               x86_64
```

```
32-bit, 64-bit
  CPU op-mode(s):
 Byte Order:
                          Little Endian
CPU(s):
 On-line CPU(s) list:
Vendor ID:
                          GenuineIntel
  Model name:
                          140
    Model:
    Thread(s) per core:
    Stepping:
    CPU(s) scaling MHz: 27%
    CPU max MHz:
                          4200.0000
    CPU min MHz:
    BogoMIPS:
                          4838.40
                          fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss
ht tm pbe syscall nx pdpe1gb rdtscp lm constant_tsc art arch_perfmon pebs bts rep_good nopl xtopology nonstop_
    Flags:
                          tsc cpuid aperfmperf tsc_known_freq pni pclmulqdq dtes64 monitor ds_cpl vmx est tm2 ssse3 sdbg fma cx16 xtpr p
                          dcm pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand lahf_lm abm 3dnowprefe
                          tch cpuid_fault epb cat_12 invpcid_single cdp_12 ssbd ibrs ibpb stibp ibrs_enhanced tpr_shadow vnmi flexpriori
                          ty ept vpid ept_ad fsgsbase tsc_adjust bmi1 avx2 smep bmi2 erms invpcid rdt_a avx512f avx512dq rdseed adx smap
                           avx512ifma clflushopt clwb intel_pt avx512cd sha_ni avx512bw avx512vl xsaveopt xsavec xgetbv1 xsaves split_lo
                          ck_detect dtherm ida arat pln pts hwp hwp_notify hwp_act_window hwp_epp hwp_pkg_req avx512vbmi umip pku ospke
                          avx512_vbmi2 gfni vaes vpclmulqdq avx512_vnni avx512_bitalg avx512_vpopcntdq rdpid movdiri movdir64b fsrm avx5
                          12_vp2intersect md_clear flush_l1d arch_capabilities
Virtualization features:
 Virtualization:
                          5 MiB (4 instances)
                          8 MiB (1 instance)
  NUMA node(s):
 NUMA node0 CPU(s):
                          0-7
Vulnerabilities:
                          Not affected
 Itlb multihit:
                          Not affected
                          Not affected
  Meltdown:
                          Not affected
  Mmio stale data:
                          Not affected
                          Not affected
  Retbleed:
  Spec store bypass:
                          Mitigation; Speculative Store Bypass disabled via prctl and seccomp
                          Mitigation; usercopy/swapgs barriers and __user pointer sanitization
  Spectre v2:
                          Mitigation; Enhanced IBRS, IBPB conditional, RSB filling, PBRSB-eIBRS SW sequence
  Srbds:
                          Not affected
 3:30PM:
```

```
3:31PM: gcc --version
gcc (GCC) 12.2.0
Copyright (C) 2022 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
```

#### OpenMP 4.5

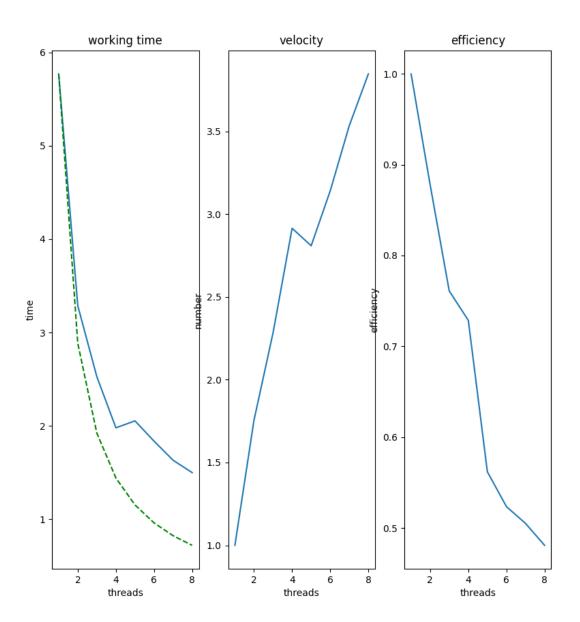
#### Алгоритм.

В переменной п — число элементов в одном массиве (10 000 000). Изначально идет выделение памяти для массивов и их заполнение. Далее запускается сортировка Шелла, которая заключается в разбиении массива на группы с шагом h. Каждая группа сортируется вставками. Сортировку групп мы выполняем параллельно.

## #pragma omp parallel for num\_threads(k) shared(A, n, h)

#### Директива

задает параллельно исполняемый цикл, выполняемый в k потоках. В нем используются A, n, h - общие переменные, то есть они не копируются для каждого отдельного потока.



1	2	3	4	5	6	7	8
5.76855 7	3.28651 6	2.52696 7	1.97934 3	2.05363	1.83672 1	1.63191	1.499652

Заключение: Мы реализовали параллельную сортировку Шелла. Также при сравнении теоретических и практических результатов работы алгоритма обнаружили, что наши ожидания относительно ускорения, эффективности и времени работы подтвердились.

Приложение