A Portable Implementation of RANLUX++

Jonas Hahnfeld, Lorenzo Moneta

May 18, 2021

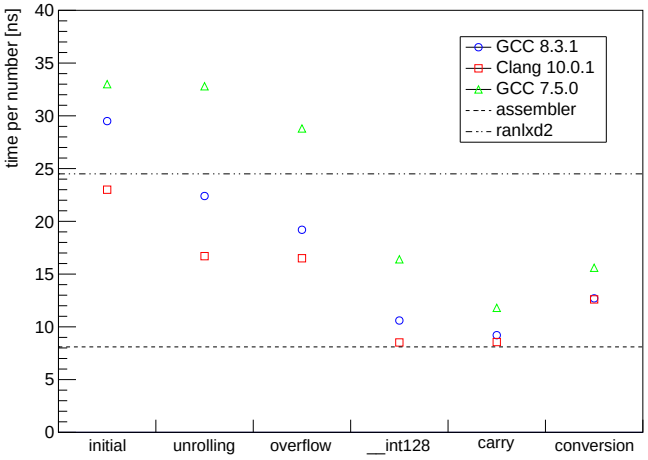
Portable RANLUX++ for ROOT

- RANLUX++: random number generator, extension of RANLUX
  - Use its equivalent Linear Congruential Generator (LCG)
  - Avoid computing unneeded intermediate results, fast skipping of numbers
  - But: requires large state and multipliers (576 bits)

- Shown to be profitable by A. Sibidanov in 2017
  - Arithmetic operations implemented in assembler for x86 architecture
  - For ROOT data analysis framework: portable implementation with standard C++

- Include a fix to avoid bias in generated numbers
  - Reported and solution proposed by M. Lüscher
  - $\Rightarrow$ Convert LCG state back to RANLUX numbers

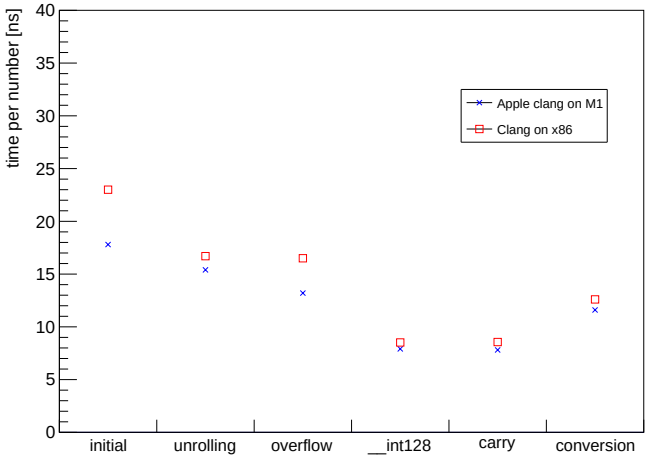
Optimization on x86



- AMD Ryzen 3900, produce `double` precision numbers
- Baselines:
  - assembler implementation by Sibidanov (bottom line)
  - `ranlxd2` by Lüscher
- Last column: conversion back to RANLUX numbers

Portability - Apple M1

- Implementation works on new architecture
- Optimizations give similar benefits



Portability - Nvidia GPUs

- Portable code can be reused with minor modifications:
  - Remove the dependency on ROOT's interface `TRandomEngine`
  - Hardcode the luxury level `p = 2048` (recommended value)
  - Add annotations `__host__ __device__`
  - Disable type `__int128` on the device
- Acceptable performance on the GPU
  - Condition: threads must advance state at the same time
  - Slower than default generator in cuRAND, but much better properties

Conclusion

- Portable implementation of RANLUX++
  - No assembler, only standard C++
  - Included in ROOT data analysis framework
- Portable optimizations on x86
  - Reached very competitive performance
- Tested on Apple M1 and Nvidia GPUs