112-1 DCLab NTUEE

Team09 proposal

B10901131 吳子傑
B09901118 曾善恆
B09901123 余智峰

Arbitrary-precision integer calculator

32-bit? Too short!

64-bit? Lame!!

I NEED MORE POWER!!!

How about... 131,072-bit?

Literatures to be reviewed

Knuth, D.E.: The Art of Computer Programming, Chapter 4, Section 3.3, 2nd edn., vol. 2, pp. 278–301. Addison-Wesley, Reading, MA

Schönhage, A., Strassen, V. Schnelle Multiplikation großer Zahlen. Computing 7, 281–292 (1971). https://doi.org/10.1007/BF02242355

FLYNN, Michael J. On division by functional iteration. IEEE Transactions on Computers, 1970, 100.8: 702-706.

Expected Algorithms and Reseources

Addition and Subtraction: Simply add/sub then carry out

Multiplication: Toom-Cook algorithm

Division: Newton-Raphson method

Hardware: FPGA, PC, USB cable

Goal

- Import n bits integers’ data from the pc for n is a large positive integer
- Save the data to DRAM and the pointer to SRAM
- Implement the arithmetic of the data in FPGA
- Export the result to the pc from DRAM

Difficulties and solutions

1. Data transmission time

RS232: baud 115200 -> 115200bit/s

1MiB integer -> 70s to transmit data!

USB2.0 low-speed: 1.5 Mbit/s

1MiB integer -> 6s to transmit data

2. Time complexity too long

Change algorithm(Schönhage-Strassen algorithm)