EXTENDING THE GFN PRIME SEARCH BEYOND 1M DIGITS USING GPUS

PPAM 2013, Warsaw

Iain Bethune and Michael Goetz

Outline

- PrimeGrid

- Genefer: Background
- Genefer: New developments

- GFN prime search status

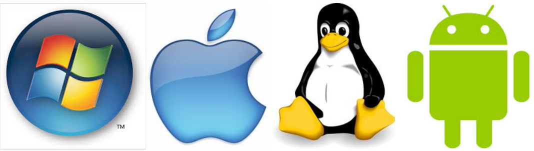
- Future plans

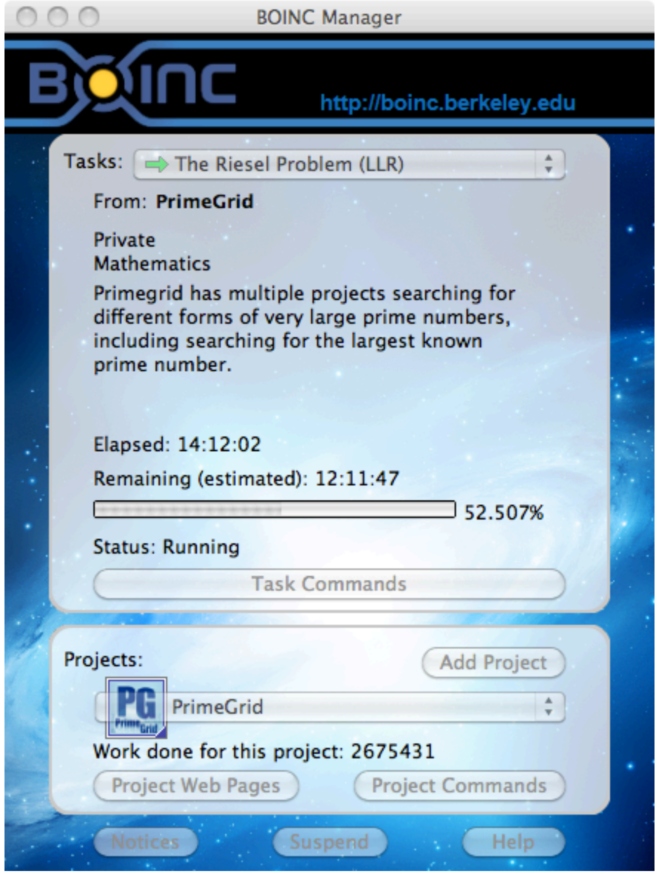
PrimeGrid

- What is PrimeGrid?
  - ‘Volunteer Computing’ project built on BOINC platform
  - Searching for large primes (GFNs, Cullen, Woodall, Proth, Riesel, Twin Primes, Sophie Germain Primes …)
  - Working on computational proofs of Sierpiński, Riesel Conjectures (also the Prime and Extended variants)
  - Set up in 2005 by Rytis Slatkevičius, now a team of volunteer admins and software developers
  - 50,000+ users, largest BOINC project by total credit

PrimeGrid

- Range of applications
  - LLR (CPU only)
  - PFGW (CPU only)
  - PPSieve (CPU, CUDA, OpenCL)

- Portable to many clients
  - OS: 
  - Hardware:
    - Intel, AMD, PPC, ARM CPUs
    - Nvidia & AMD GPUs, Cell BE



Tasks: The Riesel Problem (LLR)

From: **PrimeGrid**

Private
Mathematics

Primegrid has multiple projects searching for different forms of very large prime numbers, including searching for the largest known prime number.

Elapsed: 14:12:02

Remaining (estimated): 12:11:47

52.507%

Status: Running

Projects: PrimeGrid

Work done for this project: 2675431

Genefer: Background

- Program for (psuedo-)primality testing of Generalized Fermat Numbers

$$F_{b,n} = b^{2^n} + 1$$

- Implements a Fermat test
  - Essentially large-integer squaring (using DWT)
  - Modular reduction
  - Results in a 64-bit residue

$$a^{F_{b,n}-1} \equiv 1 \pmod{F_{b,n}}$$

- Original C-code written by Yves Gallot in 2002-2004
- Extended by Gallot and David Underbakke with hand-coded assembly (MASM) transforms using:
  - x87 FPU 80-bit precision for extended range of b
  - x86-64 / SSE2 vector arithmetic for ~80% speedup

Genefer: New Developments

- Converted MASM to GNU syntax
  - Allowed builds for Mac OS X and Linux clients

- Integrated BOINC API calls into Genefer
  - Task start/stop/pre-empt, checkpoint, progress reporting

- Merged the (slightly diverged) versions into a single code
  - Uniform front-end: main algorithm, UI, checkpointing, benchmarks
  - Simple API implemented by each back-end
  - Build a particular version via pre-processor defines

Genefer: New Developments

- Support for Nvidia GPUs via CUDA back-end
  - FFTs using CuFFT library
  - Rounding and normalisation via four custom kernels
  - Initial port by Shoichiro Yamada, then optimised and auto-tuned
  - Entire calculation loop on GPU
  - Minimal data transfer
    - Initialisation
    - Infrequent check of max round-off error
    - Periodic checkpoints
  - CUDA is all encapsulated below the back-end API

- Code and binaries released: https://www.assembla.com/spaces/genefer

Genefer: New Developments

	Genefer80		Genefer		Genefx64		GeneferCUDA	
2^n	b limit	t (ms)	b limit	t (ms)	b limit	t (ms)	b limit	t (ms)
32768	67,210,000	2.34	1,630,000	1.67	1,575,000	0.912	1,840,000	0.212
131072	45,450,000	11.2	1,095,000	7.54	1,060,000	4.05	1,270,000	0.601
524288	30,020,000	57.4	695,000	35.3	735,000	19.3	815,000	1.98
2097152	20,250,000	277	490,000	175	515,000	102	580,000	8.23
4194304	-	-	-	-	-	-	480,000	16.5

b limits and performance (ms per multiplication) for selected *n* on a Core 2 Quad 2.4 GHz with Nvidia GTX480.

GFN Prime Search Status

- Since 2009, we have extended the GFN search to higher *b* and started work on larger *n*
  - In the process discovered 12 new GFN mega-primes
    - 7 of these found using GeneferCUDA
  - No primes yet in *n=20*, *n=22* searches although current search limits are at 10th and 2nd place on the top 5000 prime list.

n	b limit (Sep 2013)	Largest Prime	Date	Decimal digits
15	6,961,316	$15547296^{32768}+1$	Jul 2011	235,657
16	3,196,780	$19502212^{65536}+1$	Jan 2005	477,763
17	1,166,000	$1372930^{131072}+1$	Sep 2003	804,474
18	1,024,466	$773620^{262144}+1$	Feb 2012	1,528,413
19	750,244	$475856^{524288}+1$	Aug 2012	2,976,663
20	201,460	-	-	-
22	10,428	-	-	-

GFN Prime Search Status

- Used our results to extend Gallot and Dubner’s tables (Math. Comp. 71, 2002)
  - Good agreement with predicted distribution of primes except at *n=18,19*

	$b \leq 10^5$			$b \leq 10^6$			Search Limit			
2^n	Est.	Act.	Err.	Est.	Act.	Err.	b	Est.	Act.	Err.
8192	10	3	-2.2	81	74	-0.8	13,000,000	764	730	-1.2
16384	5	1	-1.7	38	33	-0.9	4,560,000	156	137	-1.5
32768	2	1	-0.5	14	16	0.6	6,961,000	84	91	0.8
65536	2	1	-0.5	13	14	0.2	3,196,000	35	38	0.5
131072	1	1	0.2	7	5	-0.6	1,166,000	8	7	-0.4
262144	0	2	2.2	4	7	1.5	1,024,000	4	7	1.5
524288	0	1	1.6	2	-	-	750,000	2	4	2.0
1048576	0	-	-	1	-	-	201,460	0	0	0.0
⋮	⋮			⋮			⋮			⋮
4194304	0	-	-	0	-	-	10,428	0	0	0.0

Future Plans

- Already developed several new CPU transforms
    - SSE3, AVX, 128-bit software ‘double-double’ precision

- OpenCL implementation currently in beta
    - Targetted at AMD GPUs
    - Can be faster than CUDA for some *n* on some hardware

- Merge CPU back-ends into single executable
    - Auto-select transform based on hardware support and performance
    - Expose parameters for auto-tuning

- (Hopefully) find a new World Record Prime!

Summary

- PrimeGrid is a popular BOINC project with many primality testing sub-projects, including searching for large GFN primes
- We have ported the Genefer program to many architectures and OS, including Nvidia GPU using CUDA
  - 10x speedup over single CPU core for large *n*
- Large steps forward in search breadth and depth over previous GFN search effort
- Closing in on a new world record prime

Acknowledgements

Rytis Slatkevičius

Lennart Vogel

John Blazek

Jim Breslin

Yves Gallot

David Underbakke

Mark Rodenkirch

rackspace®
the open cloud company

NAIS
Centre for
Numerical Algorithms
& Intelligent Software

epcc

PrimeGrid

Thanks for listening

Any questions?

www.primegrid.com

www.epcc.ed.ac.uk/~ibethune