The Next Ten Years

Rich Schroeppel

Sandia National Laboratories

rcs @ cs.arizona.edu

Experimental Mathematics Workshop

Oakland, California

March 30, 2004

Prediction is very difficult – especially of the future.

-- Niels Bohr

Moore's Law: 10 Years = 100x

Doubling every 18 months: $2^{10/1.5} = 101.6$

For the same cost, we expect 100x improvements in computing speed, memory, disk storage, and bandwidth. Each decade. (!)

Compared with 10 years ago, this is roughly right. Our machines were 100x slower, our memories 20x smaller, our disks 100x smaller, our bandwidth 25x slower.

Three impediments: Physics, Demand, Infrastructure

Physics: Creeping up on the limits of silicon &c. Still some room.

Demand: Driven by games – players can use the 100x for better pix.

Infrastructure: Lots of fibre to lay and ditches to dig. It's happening.

Drivers

Gamers want ever better rendering. This can use 100x computing speedup. Not clear that folks want 25GB memory. They can use the 20TB disks for storing home movies & video calls. We can use bandwidth up to 1GB or so for high quality video.

Market today wants ubiquity rather than power.

Architecture: A Wildcard

The Pentium has 50M gates, laboring mightily to do a few 32-bit additions every clock cycle. Can we do better?

Landscape is littered with failed architectures.

We are still using descendants of the 4004 chip.

Some successes: DSP, MMX, caches, clusters.

MMX ideas work for rendering.

Caches: tapped out.

Branch prediction & speculative execution: dead end.

Dataflow, FPGA, LispMachines, RISC(?), Connection Machine, bit-parallel SIMD, database machines, …, haven't caught on.

Networked Parallelism

Thousands of machines, loosely coupled, same task.

GIMPS & SETI

I think Multiplication can be distributed.

Combinatorial counts and searches can be split up.

Wanted: an army of PCs supporting Experimental Math.

Needs serious coordination work.

It's worth doing.

Parallel Multiplication

Multi-piece Karatsuba multiplication can be parallelized.

The heavy lifting is multiplication of the short pieces, which can be farmed out. Individual machines do FFT multiplies.

Bandwidth a potential problem in practice.

Center machine needed to generate sub-problems, and combine the results. Bandwidth hog, storage hog.

Can storage requirements be subdivided?

Petabit & Exabit multiplications!

Great Expectations!

Checkers solved.

Chess, doubtful.

$10^{15\text{-}20}$ digits of Pi.

Working with 100M term math expressions.

Magic Squares of order 6 counted.

Omino-related counts to 10^{15}, more if theory improved.

Combinatorics counts & searches: 100x – 100,000x

A couple of automated reasoning successes.

Factoring to 175-200 digits.

More mathematics online: Databases of integrals, theorems, etc.

Parallel LLL?   Sloane Superseeker?   Plouffe ISC?