From an experimental paper (Bailey, Lee and Simon):

"For many years it was though that [the level at which Strassen' s algorithm is more efficient] was well over 1000x1000. In fact, for some new workstations, such as the Sun-4 and SGI IRIS 4D, Strassen is faster for matrices as small as 16x16."

Most modern matrix libraries now use Strassen, typically as a choice:

- Cray libraries
- IBM ESSL library
- LAPACK

On Strassen

From Numerical Recipes (Press et al. 1986):

"We close this chapter with a little entertainment, a bit of algorithmic prestidigitation ....."

and later in the same section

"This is fun, but let' s look at practicabilities: If you estimate how large N has to be before the difference between exponent 3 and exponent 2.807 is substantial enough to outweigh the bookkeeping overhead, arising from the complicated nature of the recursive Strassen algorithm, you will find that LU decomposition is in no immediate danger of becoming obsolete."

Standard complaints about algorithm analysis

- Irrelevant problem
- Impractical constants hidden in big-O
- Bad machine models
- Too complicated

Why care about algorithms?

Just about every field uses sophisticated algorithms.

- engineering
- physical sciences
- social sciences
- business

The level of sophistication used in practice has greatly increased in recent years

Asymptotics becoming more important.

- Linear programming (interior point methods)
- Factoring (number field sieve)
- ....

Clustering

Problems

- Fixed cardinality vs. not
- Predefined groupings vs. not

Algorithms

- Hierarchical (top down or bottom up)
- Optimization, density search, clumping, SVD

Applications

- Compression, search-engines
- Classification (e.g. V isa)
- Machine learning

Search Engines

Problems

- Exact vs. Partial matching
- Image and sound retrieval
- Grouping

Algorithms

- Inverted indices
- Clustering, Filtering

Applications

- Hotbot, L ycos, Altavista, ...
- Searching in multimedia digital libraries

Pattern matching

Problems

- Exact matching
- Approximate matching

Algorithms

- (Exact) Knuth-Morris-Pratt, Boyer -More, Rabin-Karp
- (Approximate) Smith-W aterman

Applications

- DNA sequence analysis
- Text analysis

N-body problem

Problems

- Coulomb forces
- Other forces

Algorithms

- particle-mesh, nested-grid particle-mesh
- (tree based) Barnes-Hut, Greengard, Callahan

Applications

- Astronomy -- formation of galaxies
- Biology/chemistry -- molecular dynamics
- Other: plasma physics, PDEs, Fluid-dynamics

VLSI Layout

Problems

- Placement
- Global and detailed routing

Algorithms

- (Placement) partition-based, cluster -growth, simulated-annealing
- (Routing) Maze, Shortest path, Steiner tree, integer prog.

Applications

- Intel, Sun, SGI, HP , ...
- FPGAs

Triangulation

Problems

- Delaunay and constrained-Delaunay
- Boundary meshing (conforming Delaunay)

Algorithms

- Guibas-Stolfi, Dwyer , Bucketing, Edge-flipping, Edelsbruner
- Bern-Epstein-Gilbert, Rupert (boundary meshing)

Applications

- Meshing for finite-element simulations (airflow , stress, ...)
- Terrain modeling
- Interpolation and compression

Integer programming

Problems

- General
- 0-1 programming

Algorithms

- Approximating with linear programming
- Branch-and-bound, Cutting plane

Applications

- Airline scheduling (Delta, American, United)
- Delivery and inventory management (W allmart, Shell)
- VLSI placement

Linear Programming

Problems (and related problems)

- Straight linear programs
- Network flows
- Multiobjective optimization

Algorithms

- Simplex (many variants)
- Ellipsoid and interior point algorithms

Applications

- Finance, job-shop scheduling, inventory control
- A step in integer programming

Cryptography

Problems

- Symmetric encryption (secret keys)
- Asymmetric encryption (public keys)
- Other: Digital signatures, hash functions

Algorithms

- (Symmetric) DES, NewDES, Skipjack, IDEA
- (Asymmetric) Knapsack, RSA, Diffie-Hellman, ElGamal
- (Hash functions) MD5, SHA, T iger

Applications

- Kerberos, Netscape, PGP , ISDN, Digital cash, ...

Compression

Problems

- Lossless
- Lossy

Algorithms

- (Lossless) Huffman coding, LZW , LZ77, PPM, DMC
- (Lossy) T ransform coding, fractal coding, vector quant..

Applications

- communication (reducing bandwidth) --
- archiving
- encryption and machine learning