





What the course is about

Design of Algorithms

design methods common or important types of problems analysis of algorithms - efficiency correctness proofs

What the course is about

Complexity, NP-completeness and intractability solving problems in principle is not enough

algorithms must be efficient

some problems have no efficient solution

NP-complete problems

important & useful class of problems whose solutions (seemingly) cannot be found efficiently, but *can* be checked easily

5

Very Rough Division of Time

Algorithms (7 weeks) Analysis of Algorithms Basic Algorithmic Design Techniques Graph Algorithms Complexity & NP-completeness (2 weeks)

Check online calendar page for (evolving) details

Complexity Example

Cryptography (e.g. RSA, SSL in browsers) Secret: p,q prime, say 512 bits each

Public: n which equals $p \times q$, 1024 bits

In principle

there is an algorithm that given n will find p and q: try all $2^{512} > 1.3 \times 10^{154}$ possible p's: kinda slow...

In practice

no fast algorithm known for this problem (on non-quantum computers) security of RSA depends on this fact ("quantum computing": strongly driven by possibility of changing this)

Algorithms versus Machines

6

8

We all know about Moore's Law and the exponential improvements in hardware...

Ex: sparse linear equations over 25 years

10 orders of magnitude improvement!











Printed circuit-board company has a robot arm that solders components to the board

Time: proportional to total distance the arm must move from initial rest position around the board and back to the initial position

For each board design, find best order to do the soldering









Then walk back to p_0

























Does it seem wacky?

Maybe, but it's *always* within a factor of 2 of the best tour!

deleting one edge from best tour gives *a* spanning tree, so *Min* spanning tree < best tour best tour \leq wacky tour \leq 2 * MST < 2 * best

29

The Morals of the Story

Algorithms are important Many performance gains outstrip Moore's law Simple problems can be hard Factoring, TSP Simple ideas don't always work Nearest neighbor, closest pair heuristics Simple algorithms can be very slow Brute-force factoring, TSP Changing your objective can be good Guaranteed approximation for TSP And: for some problems, even the *best* algorithms are slow