A tourist guide through computational complexity

Why bother proving a problem to be hard ?

Stéphane Vialette

Stephane.Vialette@ens.fr

LGM

École Normale Supérieure

A tourist guide through computational complexity - p.1/42

Computational complexity

Computational Complexity studies:

- the efficiency of algorithms;
- the inherent "*difficulty*" of problems of practical and/or theoretical importance.

The time complexity of a problem is the number of steps that it takes to solve an instance (as a function of the size of the instance).

Review of order notation

- $f(n) = \mathcal{O}(g(n))$ iff $\exists c \exists n_0 \forall n \ge n_0, f(n) \le c g(n)$
- $f(n) = \Omega(g(n))$ iff $\exists c \exists n_0 \forall n \ge n_0, f(n) \ge c g(n)$
- $f(n) = \Theta(g(n)) \quad \text{ iff } \quad f(n) = \mathcal{O}(g(n)) \text{ and } f(n) = \Omega(g(n))$

Review of order notation

- $f(n) = \mathcal{O}(g(n))$ iff $\exists c \exists n_0 \forall n \ge n_0, f(n) \le c g(n)$
- $f(n) = \Omega(g(n))$ iff $\exists c \exists n_0 \forall n \ge n_0, f(n) \ge c g(n)$
- $f(n) = \Theta(g(n))$ iff $f(n) = \mathcal{O}(g(n))$ and $f(n) = \Omega(g(n))$

If f(n) = O(g(n)) then f has at most rate of growth g(n)
If f(n) = Ω(g(n)) then f has at least rate of growth g(n)
If f(n) = Θ(g(n)) then f has rate of growth g(n)

Review of order notation

Note that for sufficiently large n:

$$\log n < n < n \log n < n^2 < n^3 < 2^n$$

 $\log n$ is interpreted as base-2 logarithm (it does not really matter, since $\log_2 n = log_{10}n/log_{10}^2$ and constants are ignored as already mentioned).

This is sometimes stated as:

 $\mathcal{O}(\log n) < \mathcal{O}(n) < \mathcal{O}(n\log n) < \mathcal{O}(n^2) < \mathcal{O}(n^3) < \mathcal{O}(2^n)$

A *polynomial time algorithm* or a *good algorithm* is one that runs in O(p(n)) time for some polynomial p(n).

A *polynomial time algorithm* or a *good algorithm* is one that runs in O(p(n)) time for some polynomial p(n).

<u>Binary Search</u>: Search a sorted array by repeatedly dividing the search interval in half



Running time is $\mathcal{O}(\log n)$

A *polynomial time algorithm* or a *good algorithm* is one that runs in O(p(n)) time for some polynomial p(n).

<u>Quicksort</u>: An in-place sort algorithm that uses the divide and conquer paradigm



Quicksort has running time upper-case $\Theta(n^2)$ in the worst case, but it is typically $\mathcal{O}(n \log n)$.

A *polynomial time algorithm* or a *good algorithm* is one that runs in O(p(n)) time for some polynomial p(n).

<u>String matching (brute force algorithm)</u>: Check whether an occurrence of the pattern starts there or not



A *polynomial time algorithm* or a *good algorithm* is one that runs in O(p(n)) time for some polynomial p(n).

Optimal Alignment: Compute an optimal alignment of S and T.



Running time is $\mathcal{O}(m^n)$

The Fundamental Question

Do polynomial time algorithms exist for all problems ?

- The answer to this question is not known
- Is P = NP ?
- It is one of the great mysteries of modern computer science

I can't find an efficient algorithm ...







"I can't find an efficient algorithm, because no such algorithm is possible."



"I can't find an efficient algorithm, but neither can all these famous people."

Graph G = (V, E)



Is there exist a path between two vertices in G?



Finding a *shortest path* between two vertices in G



Finding a maximum *matching* in G



Finding a minimum weight *spanning tree* in *G*



Is the directed graph *G* acyclic?



Graph G = (V, E)



Finding a minimum *vertex cover* in G



Finding a maximum *independent set* in G



Finding a maximum *clique* in *G*



Finding a minimum *dominating set* in G



Finding an *hamiltonian circuit* in G



Finding an *hamiltonian path* between two vertices in G



Finding a minimum *coloring* of *G*



"polynomial" is a synonym to practical

	Size of Largest Problem Instance solvable in 1 Hour		
Time complexity	With present	With computer	With computer
	computer	100 times faster	1000 times faster
n	N_1	$100N_{1}$	$1000N_{1}$
n^2	N_2	$10N_{2}$	$3.6N_2$
n^3	N_3	$4.64N_{3}$	$10N_{3}$
2^n	N_4	$N_4 + 6.64$	$N_4 + 9.97$
3^n	N_5	$N_5 + 4.19$	$N_5 + 6.29$



The effect of improved technology is multiplicative in polynomialtime algorithms and only additive in exponential-time algorithms.



The situation is much worse than that shown in the table if complexities involve factorials.

Decision problems

A decision problem is a problem where the answer is always "YES" or "NO".

- An arbitrary problem can always be reduced to a decision problem.
- Complexity theory often makes a distinction between "YES" answers or "NO" answers.

Classes P and NP

The class P consists of all those recognition problems for which a polynomial-time algorithm exists.

For the class NP, we simply require that any "yes" answer is "easily" verifiable. That is, both the encoding of the answer and the time it takes to check its validity must be "short", i.e. polynomially bounded. Formally we say that any "yes" instance of the problem has the "succinct certificate" property.



NP stands for "*Non deterministic Polynomial*", because of an alternative (and equivalent) definition based on the notion of nondeterministic algorithms.

" $\in \mathsf{P}$ ": *easy*" and " $\notin \mathsf{NP}$ ": "*hard*"

This is not always true in practice:

- It ignores constant factors. A problem that takes time $10^{100}n$ is in P (in fact, it's linear time), but is completely intractable in practice. A problem that takes time $10^{-1000}2^n$ is not in P (in fact, it's exponential time), but is very tractable for values of n up into the thousands.
- It ignores the size of the exponents. A problem with time n^{1000} is in P, yet intractable. A problem with time $2^{n/1000}$ is not in P, yet is tractable for n up into the thousands.
- It only considers worst-case times. There might be a problem that arises in the real world. Most of the time, it can be solved in time n, but on very rare occasions you'll see an instance of the problem that takes time 2ⁿ. This problem might have an average time that is polynomial, but the worst case is exponential, so the problem wouldn't be in P.

Polynomial time transformation

A decision problem Π_1 polynomially transforms to another decision problem Π_2 if, given any instance x_1 of Π_1 we can construct a corresponding instance x_2 of Π_2 within polynomial (in $|x_1|$) time such that x_1 is a "yes" instance of Π_1 if and only if x_2 is a "yes" instance of Π_2 .



NP-hard and NP-complete problem

A decision problem Π is NP-hard if all other problems in NP polynomially transform to Π .

A decision problem Π in NP is NP-complete if all other problems in NP polynomially transform to Π .

- This definition was given by Stephen Cook in 1971.
- At first it seems rather surprising that NP-complete problems should even exist, but in a celebrated theorem Cook proved that the Boolean satisfiability problem is NP-complete.
- If a problem Π is NP-complete, then it has a formidable property: If there is an efficient algorithm for Π, then there is an efficient algorithm for every problem is NP.

Proving NP-complete results

In order to prove that a problem is NP-complete, we must show two things:

- 1. That the problem is in NP.
- 2. That all other problems in NP polynomially transform to our problem.



In practice, Part 2 is usually carried out by showing that a known NP-complete problem is polynomially transformable to the problem at hand.

Dick Karp (1972)



LONGEST-COMMON-SUBSEQUENCE (LCS)

LCS

Instance: A set of n strings S_1, S_2, \ldots, S_n over an alphabet \mathcal{A} and a positive integer L. Question: Is there a string $x \in \mathcal{A}^*$ of length at least L that is a subsequence of S_i for $1 \le i \le n$?

LONGEST-COMMON-SUBSEQUENCE (LCS)

LCS

Instance: A set of *n* strings $S_1, S_2, ..., S_n$ over an alphabet \mathcal{A} and a positive integer *L*. Question: Is there a string $x \in \mathcal{A}^*$ of length at least *L* that is a subsequence of S_i for $1 \le i \le n$?

 $S_{1} = AAGGGATTCATAGT$ $S_{2} = ATATAGTGAAAACATCG$ $S_{3} = GAAGCTACAATGAGCC$ $S_{4} = AGGACCCAATGACGG$
LONGEST-COMMON-SUBSEQUENCE (LCS)

LCS

Instance: A set of n strings S_1, S_2, \ldots, S_n over an alphabet \mathcal{A} and a positive integer L. Question: Is there a string $x \in \mathcal{A}^*$ of length at least L that is a subsequence of S_i for $1 \le i \le n$?

$$S_{1} = AAGGGATTCATAGT$$
$$S_{2} = ATATAGTGAAACATCG$$
$$S_{3} = GAAGCTACAATGAGCC$$
$$S_{4} = AGGACCCAATGACGG$$





Consider a vertex $u_i \in V$ and suppose that u_i is adjacent to vertices

$$u_{i_1}, u_{i_2}, \ldots, u_{i_q}$$
 $(i_1 < i_2 < \ldots < i_q)$

Let p be the unique index such that $0 \le p \le q$ and $i_p < i < i_{p+1}$.





$s_1 =$	u_1	$u_2 \ u_3 \ u_4$
$t_1=u_2\;u_3\;u_4$	u_1	$u_2 \ u_3 \ u_4$
$s_2 = u_1$	u_2	$u_1 \ u_3 \ u_4$
$t_2=u_1\;u_3\;u_4$	u_2	u_3
$s_3 = u_1 \ u_2$	u_3	$u_1 \ u_2 \ u_4$
$t_3=u_1\;u_2\;u_4$	u_3	u_4
$s_4 = u_1 \ u_3$	u_4	$u_1 \ u_2 \ u_3$
$t_4=u_1\;u_2\;u_3$	u_4	



$s_1 =$	u_1	$u_2 \ u_3 \ u_4$
$t_1=u_2\;u_3\;u_4$	u_1	$u_2 \ u_3 \ u_4$
$s_2 = u_1$	u_2	$u_1 \ u_3 \ u_4$
$t_2=u_1\;u_3\;u_4$	u_2	u_3
$s_3=u_1\;u_2$	u_3	$u_1 \ u_2 \ u_4$
$t_3=u_1\;u_2\;u_4$	u_3	u_4
$s_4=u_1\;u_3$	u_4	$u_1 \ u_2 \ u_3$
$t_4=u_1\;u_2\;u_3$	u_4	



$s_1 =$		<i>u</i> ₂ <i>u</i> ₃ <i>u</i> ₄
$t_1 = u_2 \ u_3 \ u_4$	u_1	$u_2 \ u_3 \ u_4$
$s_2 = u_1$	u_2	$u_1 \ u_3 \ u_4$
$t_2=u_1\;u_3\;u_4$	u_2	u_3
$s_3 = u_1 \ u_2$	u_3	$u_1 \; u_2 \; u_4$
$t_3 = u_1 \ u_2 \ u_4$	u_3	u_4
$s_4 = u_1 \ u_3$	u_4	$u_1 \ u_2 \ u_3$
$t_4=u_1\;u_2\;u_3$	u_4	

 u_4

 u_1





$s_1 =$	u_1	u_2 u_3 u_4
$t_1=u_2\;u_3\;u_4$		u_2 u_3 u_4
$s_2 = u_1$	u_2	u_1 u_3 u_4
$t_2=u_1\;u_3\;u_4$	u_2	u_3
$s_3 = u_1 \ u_2$	u_3	$u_1 \ u_2 \ u_4$
$t_3=u_1\ u_2\ u_4$	u_3	u_4
$s_4 = u_1 \; u_3$	u_4	$u_1 \ u_2 \ u_3$
$t_4=u_1\;u_2\;u_3$	u_4	











Complexity classes P and NP

The biggest open question in theoretical computer science concerns the relationship between those two classes:

 $\mathsf{P} = \mathsf{NP}$?

- most people think that the answer is probably "no";
- some people believe the question may be undecidable from the currently accepted axioms.

Consensus opnion: $P \neq NP$

In essence, the P = NP question asks: if positive solutions to a YES/NO

problem can be verified quickly, can the answers also be computed quickly?

NP map

The suggested map of the NP world:



Coping with NP-hardness

NP-hard optimization problems can not be efficiently solved in an exact way unless P = NP.

Classical methods to deal with intractable problems:

- Approximation algorithms
- Probabilistic algorithms
- Special cases
- Exponential algorithms
- Local search
- Heuristics

Approximation

If we want to solve an NP-hard optimization problem by means of an efficient (polynomial time) algorithm, we have to accept that the algorithm does not always return an optimal solution but rather an approximate one.

- Historically: MULTIPROCESSOR-SCHEDULING and BIN-PACKING
- Poor quality of approximation:
 - Lack in ability to design good approximation algorithm, or
 - Structural properties of the problem

Performance ratio

Given an optimization problem Π , for any instance x of Π and for any feasable solution y of x, the *performance ratio* of y with respect to x defined as

$$R(x,y) = \max\left(\frac{\mathsf{Algo}(x,y)}{\mathsf{opt}(x)}, \frac{\mathsf{opt}(x)}{\mathsf{Algo}(x,y)}\right)$$

Both in the case of minimization problems and of maximization problems, the value of the performance ratio R(x, y) is

- equal to 1 in the case of an optimal solution;
- arbitrary large in case of poor approximate solution.

r-Approximate algorithm

Given an optimization problem Π and an approximation algorithm Algo for Π , we say that Algo is an *r*-approximate algorithm for Π if, given any input instance *x* of Π , the performance ratio of the approximate solution Algo(*x*) is bounded by *r*, that is:

 $R(x, \mathsf{Algo}(x)) \le r$

- A 1-approximate algorithm is an exact algorithm
- Any desired performance ratio can be obtained ?

NPO

NPO: Optimization

The class NPO is the set of all NP optimization problems

- The goal of an NPO problem is to find an optimum solution
- *minimization* or *maximization*
- feasible solutions are short and easy to recognize

APX

APX: Approximable

The subclass of NPO problems that admit constantfactor approximation algorithms. (I.e., there is a polynomial-time algorithm that is guaranteed to find a solution within a constant factor of the optimum cost.)



Equals the closure of MaxSNP and of MaxNP under PTAS reduction.

- SHORTEST-COMMON-SUPERSTRING
- Max-Cut for $\Delta \geq 3$

PTAS

PTAS: Polynomial-Time Approximation Scheme

The subclass of NPO problems that admit an approximation scheme in the following sense. For any $\varepsilon > 0$, there is a polynomial-time algorithm that is guaranteed to find a solution whose cost is within a $1 + \varepsilon$ factor of the optimum cost. (However, the exponent of the polynomial might depend strongly on ε .)

- NEAREST-STRING
- TRAVELING-SALESMAN in the Euclidean plane.
- MAX-INDEPENDENT-SET for planar graphs

FPTAS

FPTAS: Fully Polynomial-Time Approximation Scheme

The subclass of NPO problems that admit an approximation scheme in the following sense. For any $\varepsilon > 0$, there is an algorithm that is guaranteed to find a solution whose cost is within a $1 + \varepsilon$ factor of the optimum cost. Furthermore, the running time of the algorithm is polynomial in n (the size of the problem) and in $1/\varepsilon$.

- Maximum-Integer-K-Choice-Knapsack
- MINIMUM-MULTIPROCESSOR-SCHEDULING for constant number of processor

Inclusions

$\mathsf{FPTAS} \subseteq \mathsf{PTAS} \subseteq \mathsf{APX} \subseteq \mathsf{NPO}$



These inclusions are strict if and only if $\mathsf{P} \neq \mathsf{NP}.$

Between APX and NPO

$\mathsf{PTAS} \subseteq \mathsf{APX} \subseteq \mathsf{log} - \mathsf{APX} \subseteq \mathsf{poly} - \mathsf{APX} \subseteq \mathsf{exp} - \mathsf{APX} \subseteq \mathsf{NPO}$

If $P \neq NP$ then exp-APX is strictly contained in NPO.

- SHORTEST-COMMON-SUPERSEQUENCE
- LONGEST-PATH

Using the compendium

http://www.nada.kth.se/~viggo/problemlist/compendium.html

LONGEST COMMON SUBSEQUENCE

- INSTANCE: Finite alphabet Σ , finite set R of strings from Σ^* .
- SOLUTION: A string $w \in \Sigma^*$ such that w is a subsequence of each $x \in R$, i.e. one can get w by taking away letters from each x.
- \blacksquare MEASURE: Length of the subsequence, i.e., |w|.
- **GOOD NEWS:** Approximable within $O(m \log m)$, where *m* is the length of the shortest string in *R* [223].
- BAD NEWS: Not approximable within $n^{1/4-\varepsilon}$ for any $\varepsilon > 0$, where n is the maximum of |R| and $|\Sigma|$ [77], [275] and [68].
- COMMENT: Transformation from MAX-INDEPENDENT-SET. APX-complete if the size of the alphabet Σ is fixed [275] and [89]. Variation in which the objective is to find the shortest maximal common subsequence (a subsequence that cannot be extended to a longer common subsequence) is not approximable within $|R|^{1-\varepsilon}$ for any $\varepsilon > 0$ [170].
 - Garey and Johnson: SR10

Approximate the mult alignment problem

1. Find $S_1 \in T$ that minimizes

$$\sum_{S \in T-S_1} D(S_1, S)$$

- 2. Add the remaining strings S_2, \ldots, S_k one at a time to a multiple alignment that initially contains only S_1
 - Suppose $S_1, S_2, \ldots S_{i-1}$ has already aligned as $S'_1, S'_2, \ldots S'_{i-1}$
 - Align S'_i and S_i to produce S''_1 and S'_1 .
 - Adjust S'_2, \ldots, S'_{i-1} by adding spaces to these columns where spaces were added to get S''_1 from S'_1
 - Replace S'1 by S''_1

Analysis of the center star algorithm

TIME ANALYSIS

The preceding algorithm runs in $O(k^2m^2)$ time where k is the number of sequences and m is the maximum length.

ERROR ANALYSIS

The preceding algorithm produces an alignment whose SP value alignment is less than twice that of the optimal SP value alignment.

$$\frac{\mathsf{ALGO}(x)}{\mathsf{opt}(x)} \le \frac{2(k-1)}{k} < 2$$



For small value of k the approximation is significantly better than a factor of 2.

	2	4	6	8	10	12	14	16	18	20	30	40
J	1	1.5	1.66	1.75	1.8	1.83	1.85	1.87	1.88	1.9	1.93	1.95

Parameterized complexity

- To deal with problems that are NP-hard or worse.
- Solutions produced by approximation algorithms or heuristics are in many cases not satisfying in practice.
- Exact algorithms often yield more expressive results.

Restrict the *combinatorial explosion* of NP-hard problems to a part of the input, the *parameter*.



A central area is computational biology where we encounter many examples of fixed-parameter algorithms.

Fixed-parameter tractability (FPT)

A problem is *fixed-parameter tractable* (in FPT) w.r.t parameter k when it has an algorithm with running time

f(k) p(n)

where f is an arbitrary function in k and p is a polynomial in the input size n.

- f is exponential or worse.
- \checkmark p may be even linear.
- design of efficient algorithms.

Example

The NP-complete VERTEX-COVER problem is to determine whether there is a subset of vertices $V' \in V$ with k or fewer vertices (the parameter) such that each edge in E has at least one of its endpoints in V'.

The VERTEX-COVER problem is fixed-parameter tractable (in FPT).

- Solvable in time $\mathcal{O}(kn + 1.3248^k k^2)$.
- Efficiently solvable for small values of k.

Fixed-parameter intractability

Some problems appear to be fixed-parameter in-

- It is not known whether the CLIQUE problem can be solved in time f(k) p(n) where f might be an arbitrary fast growing function only depending on k.
- Unless P = NP the well-founded conjecture is that no such algorithm exist.
- The best known algorithm soling the CLIQUE problem runs in time $\mathcal{O}(n^{ck/3})$ where c is the exponent on the time bound for multiplying two integer $n \times n$ matrices.

W hierarchy

Hierarchy of W classes

$\mathsf{FPT} \subseteq \mathsf{W}[1] \subseteq \mathsf{W}[2] \subseteq \ldots \mathsf{W}[\mathsf{P}]$

- Many parameterized problems have been proved to be complete for W[1] and W[2]
 - VERTEX-COVER is in FPT
 - INDEPENDENT-SET is complete for W[1]
 - DOMINATING-SET is complete for W[2]
- The class W[P] contains the parameterized problems that reduce to the family of decision circuit of any weft and depth
- While no W[t] class with $t \ge 3$ seems to be well populated, there are several W[P]-complete problems.

LONGEST-COMMON-SUBSEQUENCE

n: number of sequences

L: size of the longest common subsequence

parameter	unbounded alph.	parameterized alph.	fixed alph.
n	W[t]-hard for $t \ge 1$	$W[t]$ -hard for $t \ge 1$	W[1]-complete
L	W[2]-hard	FPT	FPT
n et L	W[1]-complete	FPT	FPT

Questions ...

Why bother proving a problem to be NP-hard?

Questions ...

- Why bother proving a problem to be NP-hard?
- When to attempt such a proof ?
- Why bother proving a problem to be NP-hard?
- When to attempt such a proof ?
- What are the steps in proving a problem to be NP-complete?

- Why bother proving a problem to be NP-hard?
- When to attempt such a proof ?
- What are the steps in proving a problem to be NP-complete?
- Does there exist any short-cut for proving NP-hardness?

- Why bother proving a problem to be NP-hard?
- When to attempt such a proof ?
- What are the steps in proving a problem to be NP-complete?
- Does there exist any short-cut for proving NP-hardness?
- How to deal with a problem once it is proved to be NP-hard?

- Why bother proving a problem to be NP-hard?
- When to attempt such a proof ?
- What are the steps in proving a problem to be NP-complete?
- Does there exist any short-cut for proving NP-hardness?
- How to deal with a problem once it is proved to be NP-hard?
- Do I need parameterized complexity ?