P vs. NP and Reductions

CSE 421 Fall 22
Lecture 25

This week

What problems do we **not** know how to solve efficiently?

And how do we demonstrate it?

We need A LOT of definitions today. Some you've seen before (e.g., in 332)

We'll bold new words and use them in context.

If you don't recognize a word I say, please ask right away.

If you're watching asynchronously, pause and back up to find the word.

There are too many words to infer from context if you missed one.

How do we know a problem is hard?

At this point in the quarter, you've probably at least once been banging your head against a problem.

For so long that you began to thought "there's no way there's actually an efficient algorithm for this problem."

That wasn't true for any of the problems we gave you so far.

But it **is** true for some problems. At least we think it is.

The next few lectures are: what problems do we think there aren't efficient algorithms for, and how do we tell?

Some definitions

A problem is a set of inputs and the correct outputs.

"Find a Minimum Spanning Tree" is a problem.

Input is a graph, output is the MST.

"Tell whether a graph is bipartite" is a problem.

Input is a graph, output is "yes" or "no"

"Find the 'maximum subarray sum'" is a problem.

Input is an array, output is the number that represents the largest sum of a subarray.

Some definitions

An instance is a single input to a problem.

A single, particular graph is an instance of the MST problem

A single, particular graph is an instance of the bipartite-checking problem.

A single, particular array is an instance of the maximum subarray sum problem.

Decision Problems

Our goal is to divide problems into solvable/not solvable.
We're going to talk about decision problems.

Problems that have a "yes" or "no" answer. (a correct algorithm has a Boolean return type)

Why?

Theory reasons (ask me later).

But it's not too bad

most problems can be rephrased as very similar decision problems.

E.g. instead of "find the shortest path from s to t" ask
Is there a path from s to t of length at most k?

"Ranking" difficulty of problems

We'll use "reductions" to tell whether one problem is harder than another.

Reduction (informally)

Using an algorithm for Problem B to solve Problem A.

In that case, we'll say "A reduces to B"

In difficulty (for us, as algorithm designers), $A \leq B$

ANY algorithm for B solves A. A is no harder to solve than B.

A might be easier (maybe there's another way to solve A without B) or they might be about the same (maybe $B \leq A$ too!)

Reductions

Even less formally

Calling a library.

If you wrote a library to solve problem B

And your algorithm for A calls that library,

Then $A \leq B$ (A reduces to B).

Baseball Elimination (from last week)

g_{ij}	Angels	Rangers	Mariners	A's
Angels	-	5	3	4
Rangers	5	-	4	3
Mariners	3	4	-	5
A's	4	3	5	-

Team	w	g	P
Angels	81	12	93
Rangers	80	12	92
Mariners	70	12	82
A's	69	12	81

Transform Input

Max-Flow Algorithm

Transform Output

More Previous Examples

On Homework 1, you reduced “stable matchings with unacceptable pairs and unequal numbers of agents” to “[standard] stable matching”

On Homework 6, you (might have) reduced “finding a labeling with the minimum number of 0s on an unlabeled tree” to “2-coloring”

Last week, we reduced “telling whether the Mariners could win the division” to “finding a maximum flow”

A Formal Definition

We need a formal definition of a reduction.

We will say "A reduces to B in polynomial time" (or "A is polynomial time reducible to B" or "A reduces to B" or "$A \leq_P B$" or "$A \leq B$") if:

There is an algorithm to solve problem A, which, if given access to a library function for solving problem B,

- Calls the library at most polynomially-many times
- Takes at most polynomial-time otherwise excluding the calls to the library.

A Note on the wording

Make sure you have the direction right!

$A \leq B$ means "we can solve A using a library for B."

The name might make sense if you think of already having a library for B (we "reduced" our work to things we've already done; the "core difficulty" of the problem).

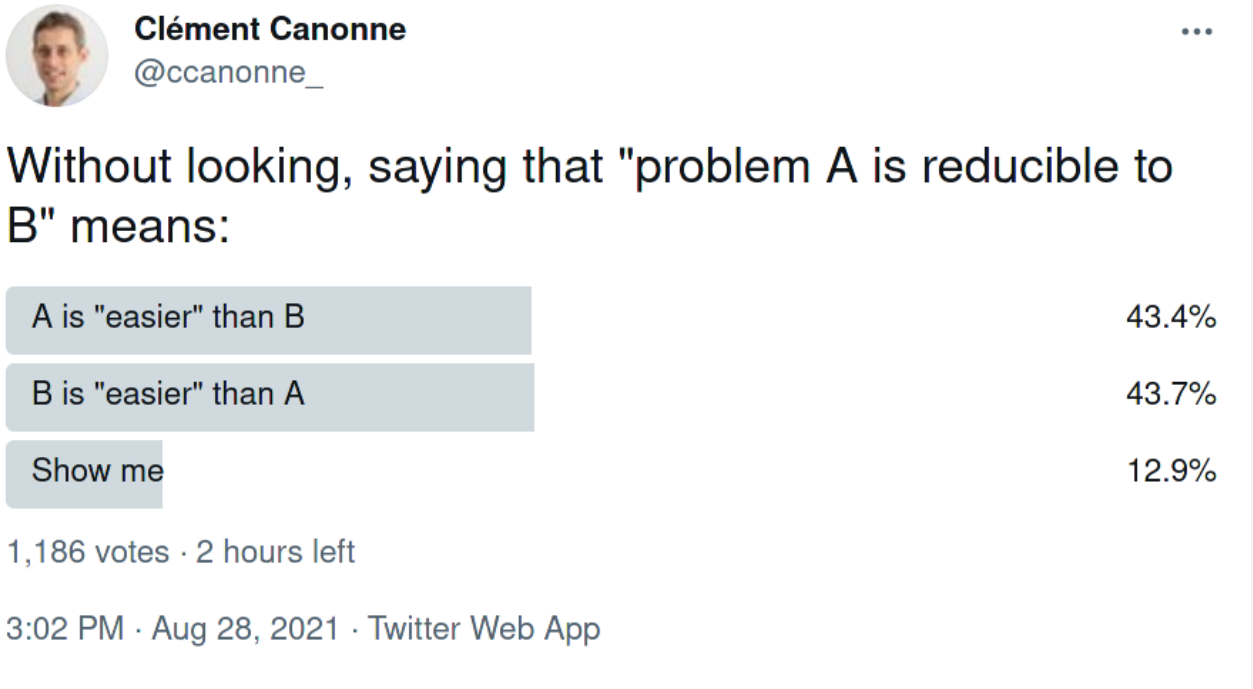
Buuuut, it also might not make sense. In the stable matching example you reduced the (harder looking) "general" SM to the basic problem.

So $general \leq basic$

A Note on the wording

Make sure you have the direction right!

$A \leq B$ means "we can solve A using a library for B."



Tl;dr check the direction you're going every time. It's going to take a while to be intuitive.

Let's Do A Reduction

4 steps for reducing (decision problem) A to problem B.

1. Describe the reduction itself (i.e. the algorithm, with call(s) to a library for problem B)

2. Make sure the running time would be polynomial (in lecture, we'll sometimes skip writing out this step).

3. Argue that if the correct answer (to the instance for A) is YES, then our algorithm answers YES.

4. Argue that if the correct answer (to the instance for A) is NO, then our algorithm answers NO.

Reduce 2-coloring to 3-coloring

What's 3-coloring?

3-coloring

Input: Undirected Graph G
Output: `True` if the vertices of G can be labeled with red,green, and blue so that no edge has both of its endpoints colored the same color. `False` if it cannot.

Reduce 2-coloring to 3-coloring

Given a graph G, figure out whether it can be 2-colored, by using an algorithm that figures out whether it can be 3-colored.

Usual outline:

Transform G into an input for the 3-coloring algorithm

Run the 3-coloring algorithm

Transform the answer from the 3-coloring algorithm into the answer for G for 2-coloring

Reduction

If we just ask the 3-coloring algorithm about G, it might use 3 colors…we can't get it to use just 2…

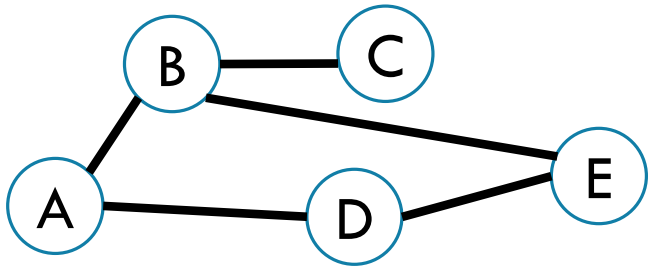
…unless…

Unless we force it not to, by adding extra vertices that **force** the 3-coloring algorithm to "use up" one color on the extra vertices, leaving only two colors for the "real" vertices.

Add an extra vertex v, and attach it to **everything** in G.

Reduction

```
2ColorCheck(Graph G)
    Let H be a copy of G
    Add a vertex to H, attach it to all other
      vertices.
    Bool answer = 3ColorCheck(H)
    return answer //don't need any modification!
```



Transform Input

3ColorCheck algorithm

Transform Output

Correctness?

```
2ColorCheck(Graph G)
     Let H be a copy of G
     Add a vertex to H, attach it to all
       other vertices.
     Bool answer = 3ColorCheck(H)
     return answer
```

TWO statements to prove: (“two directions”)

If the correct answer for G is YES, then we say YES

If the correct answer for G is NO, then we say NO

Correctness?

```
2ColorCheck(Graph G)
     Let H be a copy of G
     Add a vertex to H, attach it to all
       other vertices.
     Bool answer = 3ColorCheck(H)
     return answer
```

TWO statements to prove: (“two directions”)

If the correct answer for G is YES, then we say YES

If G is 2-colorable, then H will be 3-colorable – you can extend a 2-color labeling of G to 3 colors on H by making the new vertex the new color. All the edges in G have different colors (because we started with a 2-coloring) and any added edge has different endpoints (because v is a new color) so 3ColorCheck returns True and we return True!

If the correct answer for G is NO, then we say NO

Correctness?

```
2ColorCheck(Graph G)
     Let H be a copy of G
     Add a vertex to H, attach it to all
       other vertices.
     Bool answer = 3ColorCheck(H)
     return answer
```

TWO statements to prove: (“two directions”)

If the correct answer for G is YES, then we say YES

The new vertex can be a new color!

If the correct answer for G is NO, then we say NO

So we **can’t 2-color G**. That’s going to be hard to work with.
Take the contrapositive!!

Correctness?

```
2ColorCheck(Graph G)
     Let H be a copy of G
     Add a vertex to H, attach it to all
       other vertices.
     Bool answer = 3ColorCheck(H)
     return answer
```

TWO statements to prove: (“two directions”)

If the correct answer for G is YES, then we say YES

The new vertex can be a new color!

If the correct answer for G is NO, then we say NO

We want to show instead: If we say YES, then the correct answer is YES.
If we say YES, then 3ColorCheck(H) must have returned YES, what does a 3-coloring of H look like? The added vertex must be a different color than all the other vertices (otherwise it’s not a valid coloring – there’s an edge between the added vertex and all others). So deleting the added vertex we get a 2-coloring of G. So the right answer is YES!!

Correctness

Two DIFFERENT statements

Correct Answer YES → Our algorithm says YES

If G is 2-colorable, then H will be 3-colorable – you can extend a 2-color labeling of G to 3 colors on H by making the new vertex the new color. All the edges in G have different colors (because we started with a 2-coloring) and any added edge has different endpoints (because v is a new color) so 3ColorCheck returns True and we return True!

Our algorithm says YES → Correct Answer YES

We want to show instead: If we say YES, then the correct answer is YES.

If we say YES, then 3ColorCheck(H) must have returned YES, what does a 3-coloring of H look like? The added vertex must be a different color than all the other vertices (otherwise it's not a valid coloring – there's an edge between the added vertex and all others). So deleting the added vertex we get a 2-coloring of G. So the right answer is YES!!

Write two separate arguments

You need to show **both** "we won't get any false positives" and "we won't get any false negatives."

To make sure you handle both directions, I **strongly** recommend:

1. Always do two separate proofs (don't try to prove both directions at once, don't refer back to the prior proof and say "for the same reason").

2. Don't use contradiction (it's easy to start from the wrong spot and accidentally prove the same direction twice without realizing it).

3. Follow one of the four pairs on the next slide (don't accidentally take a contrapositive wrong)

Argument Outlines

Most common

If the correct answer is YES, then our algorithm says YES.
And If our algorithm says YES, then the correct answer is YES

Less common but sometimes:

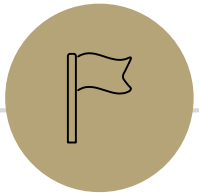
If our algorithm says NO, then the correct answer is NO.
And If our algorithm says YES, then the correct answer is YES

OR

If the correct answer is YES, then our algorithm says YES.
And If the correct answer is NO, then our algorithm says NO

Works, but rarely the best:

If our algorithm says NO, then the correct answer is NO.
And If the correct answer is NO, then our algorithm says NO



Back to Problem Ranking

P (can be solved efficiently)

P (stands for "Polynomial")

The set of all decision problems for which there exists an algorithm that runs in time $O(n^k)$ for some constant k, where n is the size of the input.

The decision version of all problems we've solved in this class are in P.

P is an example of a "complexity class"
A set of problems that can be solved under some limitations (e.g. with some amount of memory or in some amount of time).

Problems go in complexity classes. Not algorithms.
We're comparing problem difficulty, not algorithm quality.

Solve vs. Verify

To solve a problem, you get the instance, an algorithm decides whether the correct answer is "YES" or "NO"

"Is there a spanning tree of weight at most k?" can be solved with Kruskal's algorithm

To **verify,** you get an instance AND a claimed "certificate", an algorithm decides whether the certificate PROVES the instance is a YES instance.

"Is there a spanning tree of weight at most k?" is **verified** by getting (1) the graph (2) the proposed spanning tree and returning "is the spanning tree *you gave me* weight at most k**?"**

NP

Our second set of problems have the property that "I'll know it when I see it"
We're looking for **something**, and if someone shows it to me, we can recognize it quickly (it just might be hard to find)

NP (stands for "nondeterministic polynomial")

The set of all decision problems such that for every YES-instance (of size n), there is a certificate (of size $O(n^k)$) for that instance which can be verified in polynomial time.

A "verifier" takes in: an instance of the NP problem, and a "proof"
And returns "true" if it received a valid proof that the instance is a YES instance, and "false" if it did not receive a valid proof

NP problems have "verifiers" that run in polynomial time.
Do they have **solvers** that run in polynomial time? The definition doesn't say.

NP

Our second set of problems have the property that "I'll know it when I see it"
We're looking for **something,** and if someone shows it to me, we can recognize it quickly (it just might be hard to find)

NP (stands for "nondeterministic polynomial")

The set of all decision problems such that for every YES-instance (of size n), there is a certificate (of size $O(n^k)$) for that instance which can be verified in polynomial time.

If you have a "YES" instance, a little birdy can magically find you this certificate-thing, and you'll say "Oh yeah, that's totally a yes instance!"

What if it's a NO instance? No guarantee.

NP

NP

The set of all decision problems such that for every YES-instance (of size n), there is a certificate (of size $O(n^k)$) for that instance which can be verified in polynomial time.

Decision Problems such that:
If the answer is YES, you can prove the answer is yes by
- Being given a "proof" or a "certificate"
- Verifying that certificate in polynomial time.

What certificate would be convenient for short paths?
- The path itself. Easy to check the path is really in the graph and really short.

Light Spanning Tree:
Is there a spanning tree of graph G of weight at most k?

The spanning tree itself.
Verify by checking it really connects every vertex and its weight.

3-Coloring:
Can you color vertices of a graph red, blue, and green so every edge has differently colored endpoints?

The coloring.
Verify by checking each edge.

Large flow:
Is there a flow from s to t in G of value at least k?

The flow itself.
Verify the capacity constraints, conservation, and that flow value at least k.

NP

Our second set of problems have the property that "I'll know it when I see it"
We're looking for **something,** and if someone shows it to me, we can recognize it quickly (it just might be hard to find)

NP (stands for "nondeterministic polynomial")

The set of all decision problems such that for every YES-instance (of size n), there is a certificate (of size $O(n^k)$) for that instance which can be verified in polynomial time.

It's a common misconception that NP stands for "not polynomial"

Never, ever, ever, ever say "NP" stands for "not polynomial"
Please
Every time someone says that, a theoretical computer scientist sheds a single tear
(That theoretical computer scientist is me)

Solve vs. Verify

Verification is equivalent to the “magic” of nondeterminism

Remember NFAs? That could “magically” decide which state to jump to?

It’s that kind of nondeterminism. But instead of just jumping state-to-state, you can also “magically” write bits to memory too.

More on this week’s homework.

P vs. NP

P vs. NP

Are P and NP the same complexity class?
That is, can every problem that can be verified **in polynomial time also be** solved **in polynomial time.**

If you'll know it when you see it, can you also search to find it efficiently?

No one knows the answer to this question.

In fact, it's the biggest unsolved question in Computer Science.

Some New Problems

Here are some new problems. Are they in NP?

If they're in NP, what is the "certificate" when the answer is yes?

COMPOSITE – given an integer n is it composite (i.e. not prime)?

MAX-FLOW – find a maximum flow in a graph.

VERTEX-COVER – given a graph G and an integer k, does G have a vertex cover of size at most k?

NON-3-Color – given a graph G, is it not 3-colorable?

Some New Problems

COMPOSITE – given an integer n is it composite (i.e. not prime)?

In NP (certificate is factors).

MAX-FLOW – find a maximum flow in a graph.

Not in NP (not a decision problem)

VERTEX-COVER – given a graph G and an integer k, does G have a vertex cover of size at most k?

In NP (certificate is cover)

NON-3-Color – given a graph G, is it not 3-colorable?

Not known to be in NP.

Hard Problems

Let's say we want to figure out if every problem in NP can actually be solved efficiently.

We might want to start with a really hard problem in NP.

What is the hardest problem in NP?

What does it mean to be a hard problem?

Reductions are a good definition:

If A reduces to B then "$A \leq B$" (in terms of difficulty)

- Once you have an algorithm for B, you have one for A automatically from the reduction!

NP-hardness

NP-hard

The problem B is NP-hard if
for all problems A in NP, A reduces to B.

An NP-hard problem is "hard enough" to design algorithms for that if you write an efficient algorithm for it, you've (by accident) designed an algorithm that works for every problem in NP.

What does it look like? Let A be in NP, and let B be the NP-hard problem you solved, on an input to A, "run the reduction" and plug in your actual algorithm for B!

NP-Completeness

NP-Complete

The problem B is NP-complete if B is in NP
and B is NP-hard

An NP-complete problem is a "hardest" problem in NP.

If you have an algorithm to solve an NP-complete problem, you have an algorithm for **every** problem in NP.

An NP-complete problem is a **universal language** for encoding "I'll know it when I see it" problems.

Why is being NP-hard/-complete interesting?

Let B be an NP-hard problem. Suppose you found a polynomial time algorithm for B. Why is that interesting?

You now have for free a polynomial time algorithm for **every** problem in NP. (if A is in NP, then $A \leq B$. So plug in your algorithm for B!)

So $P = NP$. (if you find a polynomial time algorithm for an NP-hard problem).

On the other hand, if any problem in NP is not in P (any doesn't have a polynomial time algorithm), then no NP-complete problem is in P.

NP-Completeness

An NP-complete problem does exist!

Cook-Levin Theorem (1971)

3-SAT is NP-complete

Theorem 1: If a set S of strings is accepted by some nondeterministic Turing machine within polynomial time, then S is P-reducible to {DNF tautologies}.

This sentence (and the proof of it) won Cook the Turing Award.

What's 3-SAT?

Input: A list of Boolean variables $x_1, \ldots, x_n$

A list of constraints, all of which must be met.

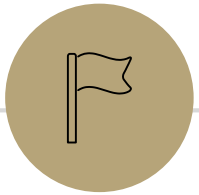
Each constraint is of the form:

$$(z_i \vee z_j \vee z_k)$$

Where z_i is a "literal" a variable or the negation of a variable.

Output: true if there is a setting of the variables where all constraints are met, false otherwise.

Why is it called 3-SAT? 3 because you have 3 variables per constraint
SAT is short for "satisfiability" can you satisfy all of the constraints?



More Reduction Facts

I have a problem

My problem C is too difficult to solve (at least for me).

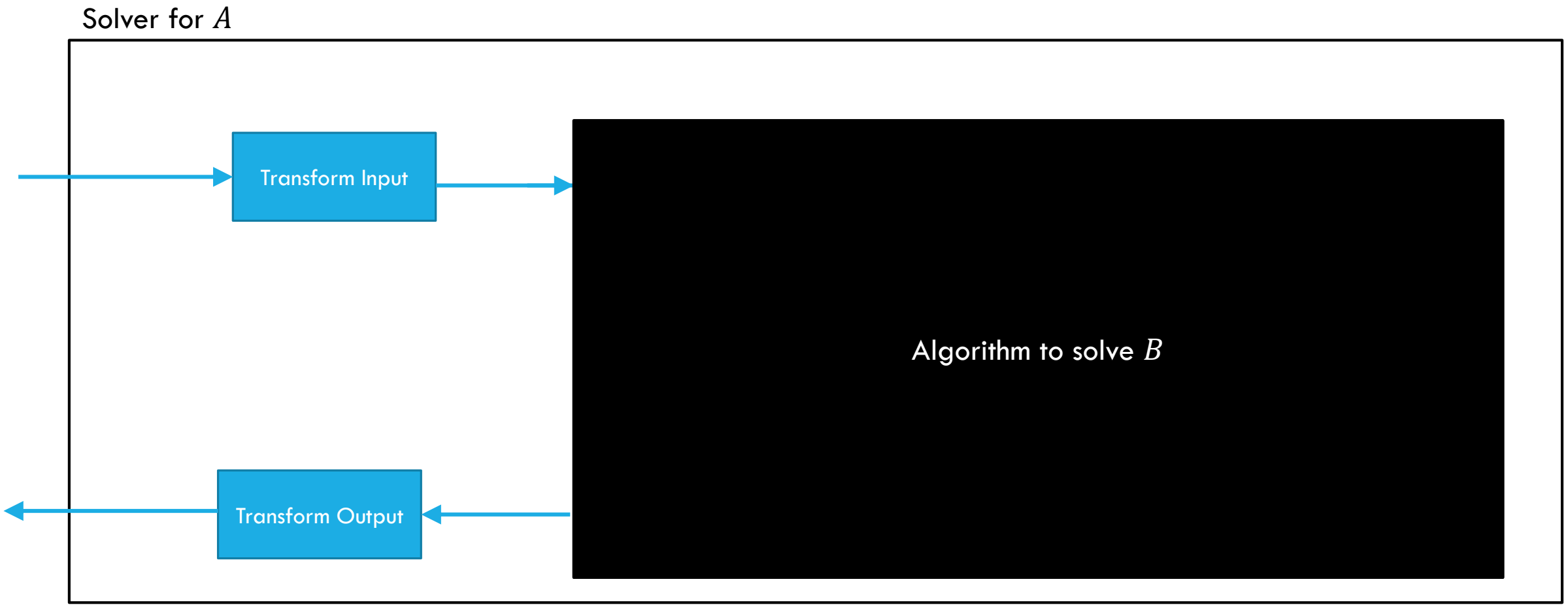
So difficult, it's probably NP-hard. How do I show it?

What does it mean to be NP-hard?

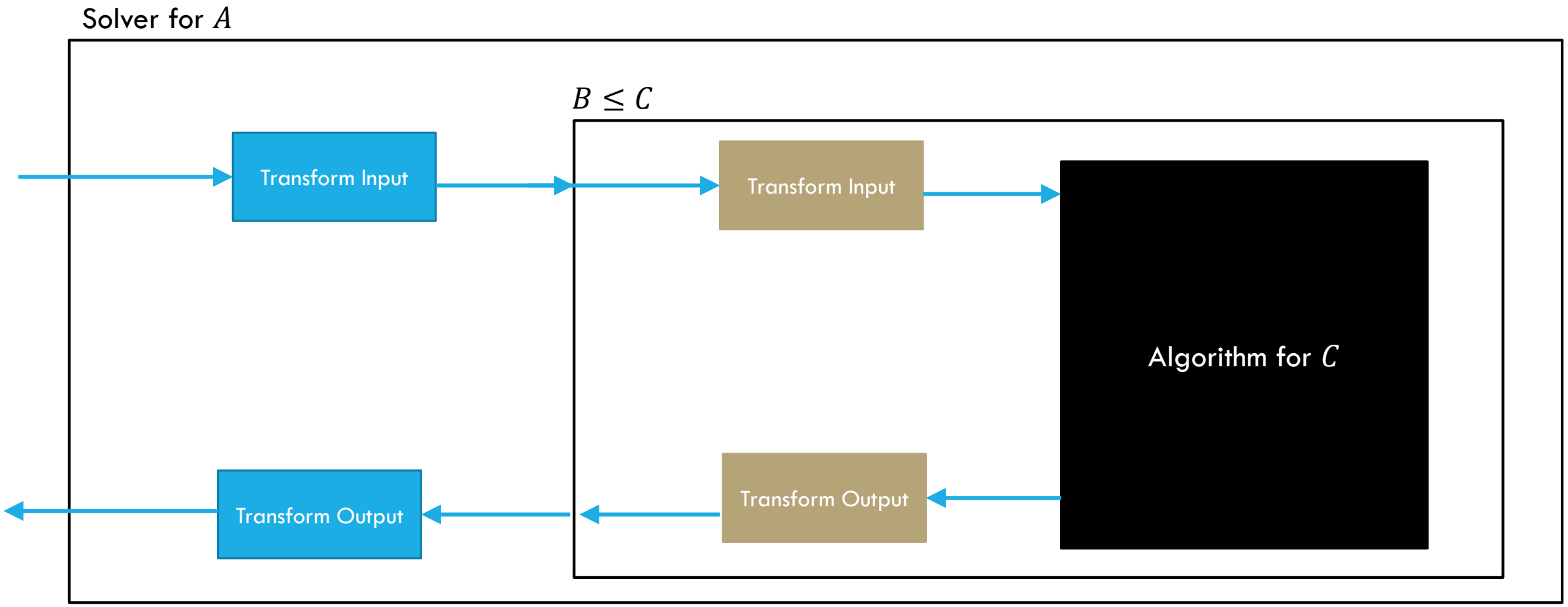
We need to be able to reduce any problem A in $\mathbf{NP}$ to C.

Let's choose B to be a **known** NP-hard problem. Since B **is known** to be NP-hard, $A \leq B$ for every possible A. So if **we show** $B \leq C$ too then $A \leq B \leq C \rightarrow A \leq C$ so every NP problem reduces to C!

Is the implication true? $A \leq B \leq C \rightarrow A \leq C$



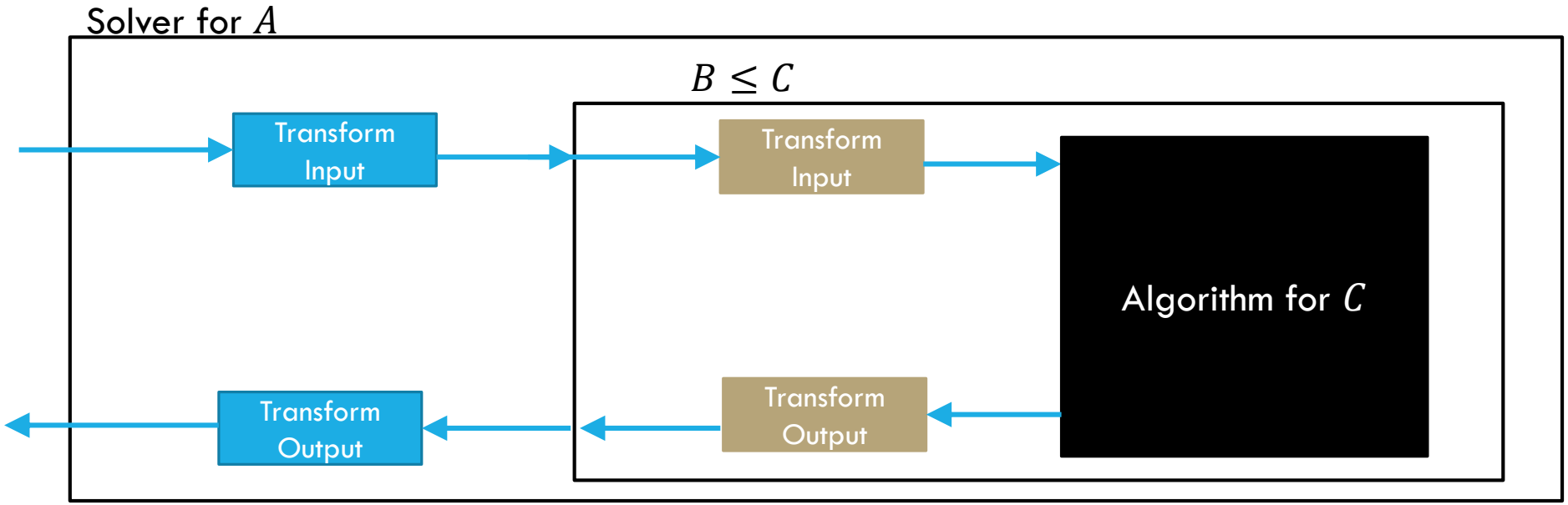
Is the implication true? $A \leq B \leq C \rightarrow A \leq C$



Is the implication true? $A \leq B \leq C \rightarrow A \leq C$

Why does it work? Because our reductions work!

How long does it take? We need polynomially many calls to B, each requires polynomially many calls to C. That's still polynomial. Similarly running time is polynomial times a polynomial, so a polynomial.



Said Differently

$A \leq B$

If I know B is not hard [I have an algorithm for it] then A is also not hard.

This is how we usually use reductions

$A \leq B$

If I know A is hard, then B also must be hard.

(contrapositive of the last statement)

Want to prove your problem is hard?

To show B is hard,

Reduce **FROM** the known hard problem **TO** the problem you care about

A reduction **From** an NP-hard problem A to B, shows B is also NP-hard.

Which Direction?

How do you remember which direction?

The core idea of an NP-completeness reduction is a proof by contradiction:

Suppose, for the sake of contradiction, there were a polynomial time algorithm for B. But then if there were I could use that to design a polynomial time algorithm for problem A.

But we really, really, really don't think there's a polynomial time algorithm for problem A. So we should really, really, really think there isn't one for B either!

P (stands for "Polynomial")

The set of all decision problems that have an algorithm that runs in time $O(n^k)$ for some constant k (on input of size n).

NP (stands for "nondeterministic polynomial")

The set of all decision problems such that for every YES-instance (of size n), there is a certificate (of size $O(n^k)$) for that instance which can be verified in polynomial time.

NP-hard

The problem B is NP-hard if
for all problems A in NP, A reduces to B.

NP-Complete

The problem B is NP-complete if B is in NP
and B is NP-hard