Introduction to Computational Complexity

Antonin Novak
antonin.novak@cvut.cz

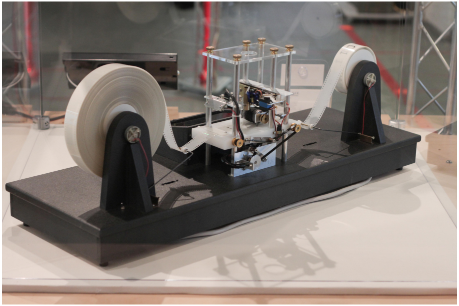
Czech Technical University in Prague

2024

Table of contents

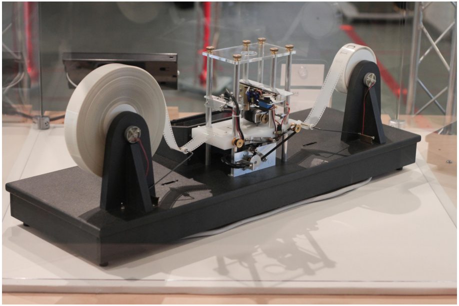
Computability

Central questions of theoretical computer science are connected to topics such as which problems are **computable** and **how efficiently**.



Computability

Central questions of theoretical computer science are connected to topics such as which problems are **computable** and **how efficiently**.



- A fascinating thing about computational complexity is that we basically all agree on what can be computed.
- How efficiently? Much less clear.

What does it mean to compute

By computing, we mean to evaluate a specific function $f : \{0,1\}^* \mapsto \{0,1\}^*$ ($S^* = \bigcup_{n \geq 0} S^n$ is the set of all finite strings over S). This can be done by a procedure called **an algorithm**:

Algorithm (informal)

An algorithm A computes a function f if:

1. It provides the output of f by following a **finite procedure** described by unambiguous elementary steps.
2. Runs in a **finite number of steps** with no particular bound on the storage space used (it can always ask for more if needed).

- An algorithm is essentially what we understand as a **computable function**.
- Notice that we do not speak about how efficient the computation of the function should be.

Power of different computational models

Power of a computational model:

- The sequence of steps that define the algorithm is executed by a **computational model** (e.g., mechanical machine, computer).
- But the computational model that manipulates with symbols should have a certain complexity (i.e., sufficiently powerful instruction set) to calculate (at least some) computable functions, right?
  - What operations are allowed? Random-access memory? Stack only? Conditional branching?
- What makes a computer a "universal" one?

Turing machine is the universal model of computation

- **Turing machine (TM)**: the universal model of computation.
  - Abstract machine described by Alan Turing that reads symbols, changes its state, **rewrites symbols** on the tape, **moves the tape**.
  - Our computers $\approx$ implementation of TM.

Church-Turing conjecture (1936)

All computable functions are exactly Turing-computable (although not necessarily very efficiently).

- Not so obvious: we have examples that are known to be strictly less powerful: finite state machines, push-down automata, ...
- On the other hand, different computational models (e.g., λ-calculus, TM with access to random bits) do not seem to be more powerful.
- We equate the intuitive concept of computable function with Turing-computable, which can be precisely defined.
- We can restrict our study of computational problems under the TM.

Computational problems

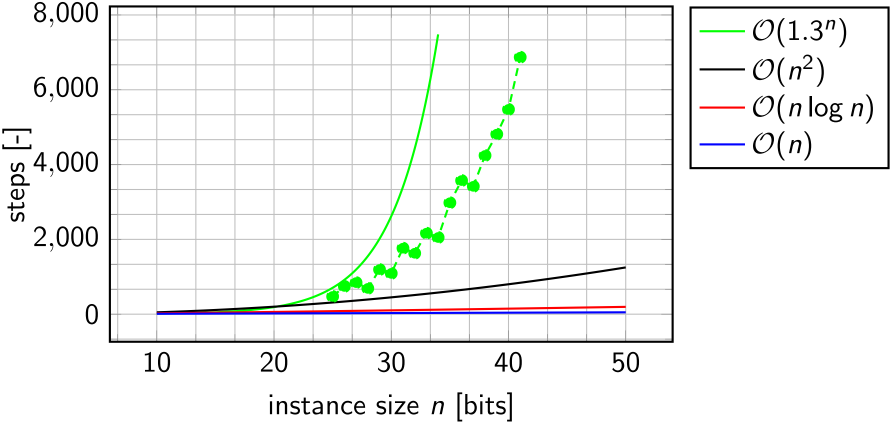
- Computational problems can be seen as relations between the inputs (instances) and outputs (solutions).
- x encoding of the instance, y encoding of the solution over some alphabet, $S = \{0, 1\}$, $S^* = \{\epsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$.
- Let $R(x, y) \subseteq S^* \times S^*$ be a relation. Each R defines a computational problem:

Types of computational problems

- **Decision problems**
  - Given x, determine if there is y satisfying $R(x, y)$?
- **Search problems**
  - Given x, find y such that $R(x, y)$ or state it does not exist.
- **Optimization problems**
  - Given x, find y such that $R(x, y)$ minimizing function $c(x, y)$ or say no such y exists.
- **Function problems**
  - Compute value of $f(x)$.

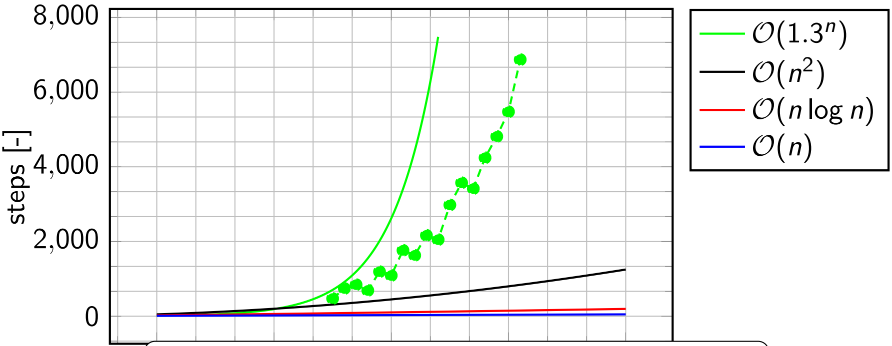
Complexity of problems

- Not all R (computational problems) are equally difficult.
- We can measure the difficulty of the problem by the number of steps $T(n)$ the best-known algorithm A on a TM needs to solve the problem R for a given input length $n = |x|$ in **the worst-case**.



Complexity of problems

- Not all R (computational problems) are equally difficult.
- We can measure the difficulty of the problem by the number of steps $T(n)$ the best-known algorithm A on a TM needs to solve the problem R for a given input length $n = |x|$ in **the worst-case**.



Computers are not to rescue: electron-sized transistor, clock time ≈ time of light between atoms, Earth-sized computer needs billions of years to brute force 300-bit solution.

Problems, instances and algorithms: summary

- A computational **problem** is a relation over **instances** and **solutions**.
- To solve problems, we develop **algorithms** with certain **time complexity**.
  - Measured in terms of the worst-case number of steps $T(n)$ over all instances of length n.
- The existence of an algorithm with given time complexity $\mathcal{O}(T(n))$ is a witness of the **problem** being in certain **complexity class**.
  - People started to categorize problems into a taxonomy.
- It turned out that there is a fundamental barrier between the polynomially solvable problems and the others.
  - In practice, we usually get low-degree polynomial algorithms or exponential ones (or even worse).

It motivates us to study which problems fall into the "good" category and which fall into "naughty".

Efficiently solvable: P

- We will use decision problems (yes/no) to demonstrate the most prominent complexity classes.
  - Similar can also be done for optimization problems, with a few definition adjustments.

Definition: Class P

The set of problems that are **solvable** in a polynomial time.

- For every $x \in \{0,1\}^*$ they state if $\exists y \in \{0,1\}^* : R(x,y)$ or no.
- Admit $\mathcal{O}(\text{poly}(n))$ algorithm, e.g. $\mathcal{O}(n^2)$, $\mathcal{O}(n \log n)$.

Examples

- Integer number problems: Addition, Multiplication, Primality test,...
- Graph problems: Topological Sorting, Minimum Spanning Tree, ...
- Miscellaneous problems: Discrete Fourier Transform, Linear Programming, ...

Efficiently checkable: NP

Definition: Class NP (non-deterministic polynomial)

The set of decision problems whose solutions are **checkable** in a polynomial time.

- What do we mean by checkable?

Efficiently checkable: NP

Definition: Class NP (non-deterministic polynomial)

The set of decision problems whose solutions are **checkable** in a polynomial time.

- What do we mean by checkable?
- **YES**-instances have so-called **polynomial certificates** (or witnesses, proofs): e.g., $|y| \leq poly(|x|)$.
- Given certificate y, one can in polynomial time verify that indeed $(x, y) \in R$.
- We do not know whether they admit a $\mathcal{O}(\text{poly}(n))$ algorithm, but we know that their solution is verifiable by $\mathcal{O}(\text{poly}(n))$ algorithm. $\approx$ there is an algorithm that solves the problem in polytime given the certificate y.

Examples

- Integer number problems: Sudoku, Knapsack, 2-Partition, ...
- Graph problems: Travelling Salesman, k-coloring, ...
- Miscellaneous problems: Linear equations with absolute values, Control theory: constrained state-space feedback

SubsetSum is in NP

Definition: SubsetSum problem

- **Instance:** A (multi)-set of n non-negative integers $A = \{a_1, \ldots, a_n\}$ and a non-negative integer W.
- **Decision:** Is there a subset $S \subseteq A$ such that $\sum_{a_i \in S} a_i = W$?

Example 1: YES-instance

$A = \{1, 1, 2, 3, 7, 9\}$, $W = 6$. The answer is **YES**: $S = \{1, 2, 3\}$.

- I claim (A, W) is YES-instance. This is a poly-sized proof: S.

SubsetSum is in NP

Definition: SubsetSum problem

- **Instance:** A (multi)-set of n non-negative integers $A = \{a_1, \dots, a_n\}$ and a non-negative integer W.
- **Decision:** Is there a subset $S \subseteq A$ such that $\sum_{a_i \in S} a_i = W$?

Example 1: YES-instance

$A = \{1, 1, 2, 3, 7, 9\}$, $W = 6$. The answer is **YES**: $S = \{1, 2, 3\}$.

- I claim (A, W) is YES-instance. This is a poly-sized proof: S.

Example 2: NO instance

$A = \{3, 5, 5, 6, 8, 10\}$, $W = 25$. The answer is **NO**.

- I claim (A, W) is NO-instance. I do not have a short proof.

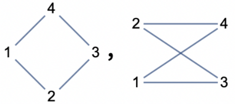
Generally, short certificates (proofs) of **NO**-instances may not exist.

Graph Isomorphism is in NP

Example: Graph Isomorphism problem

- Given two graphs G and H, decide if G is the same as H up to the vertex labelling.
- A $\mathcal{O}(\text{poly}(n))$ algorithm is not known.
- We have an algorithm by Babai (2015) that runs in $\mathcal{O}(\exp(\log(n)^c))$ for some constant $c > 1$, i.e., a quasipolynomial, grows smaller than an exponential.
- But its solution is checkable in a poly-time.

In[17]:= **FindGraphIsomorphism**[



]

Out[17]= { <| 1 → 1, 2 → 3, 3 → 2, 4 → 4 |> }

- **Remark:** in contrast to NP, problems in P have polynomial certificates even for **NO**-instances.

What is non-deterministic about NP?

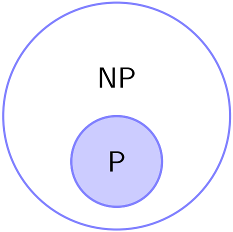
Why NP means "non-deterministic polynomial"?

- Connected with an alternative computational model, the so-called non-deterministic Turing Machine (TM).
- This abstract computational model explores all branches in your algorithm in parallel.
- This is an alternative description of class NP: the set of decision problems for which there is an algorithm that solves it in a polynomial time on a non-deterministic TM computational model.
- Useful for theoretical analysis, nobody knows how to build it physically (in contrast to the deterministic TM).
  - Quantum computers are not believed to be equivalent to non-deterministic TMs.

P vs NP question

How important is P vs NP question?

- At least \$1.000.000 important.
- Clay Math Institute's Millennium problems:
  - Solution smoothness of Navier–Stokes Equation
  - Poincaré Conjecture (solved)
  - Riemann Hypothesis
  - **P vs NP problem**
  - ...
- P vs NP question has wide implications to the world outside of CS: class P exactly corresponds to dynamical systems described by ODEs with polynomial RHS under a poly-length simulation (connection to control theory).



P vs NP question

Common belief is:

Conjecture

$$P \neq NP.$$

- Likely we are not in a position to resolve this question within the next 20 years.

[1] https://www.cs.umd.edu/users/gasarch/BLOGPAPERS/pollpaper3.pdf
[2] https://youtu.be/pQsdygaYcE4?si=N_22dOeZyHLeUngt

P vs NP question

Common belief is:

Conjecture

$$P \neq NP.$$

- Likely we are not in a position to resolve this question within the next 20 years.
- But, we can run a survey:

Year	2002	2012	2019
Thinks $P \neq NP$	61%	82%	88%

Table: William Gasarch's survey on P vs NP[1].

- See nice explanatory video on P vs NP[2].

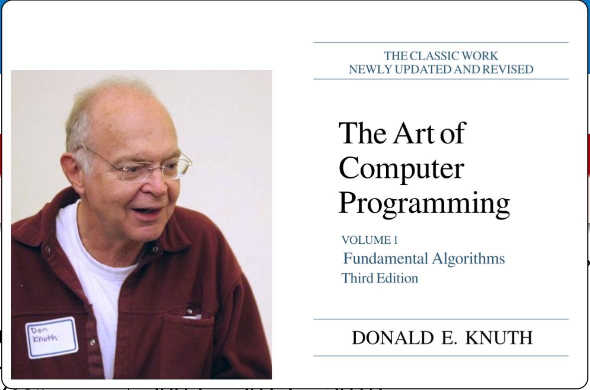
[1] https://www.cs.umd.edu/users/gasarch/BLOGPAPERS/pollpaper3.pdf
[2] https://youtu.be/pQsdygaYcE4?si=N_22dOeZyHLeUngt

P vs NP question

Common belief is:

Conjecture

- Likely we are not in ... xt 20 years.
- But, we can run a s...



Year	2002	2012	2019
Thinks P $\neq$ NP	61%	82%	88%

Table: William Gasarch's survey on P vs NP[1].

- See nice explanatory video on P vs NP[2].
- Donald Knuth is one of the great proponents of P $=$ NP.

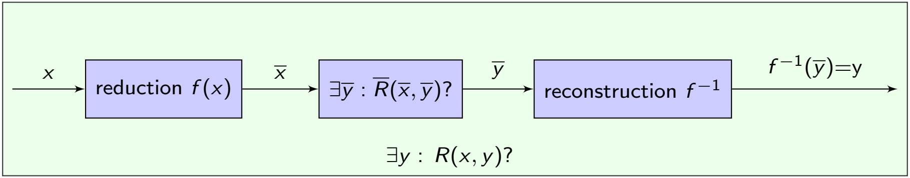
[1] https://www.cs.umd.edu/users/gasarch/BLOGPAPERS/pollpaper3.pdf
[2] https://youtu.be/pQsdygaYcE4?si=N_22d0eZyHLeUngt

Polynomial reductions

Problem reductions are one of the greatest inventions in computer science.

Motto: *My problems are your problems.*

- Solving a new problem $R(x, y)$ via existing problem $\overline{R}(\overline{x}, \overline{y})$:

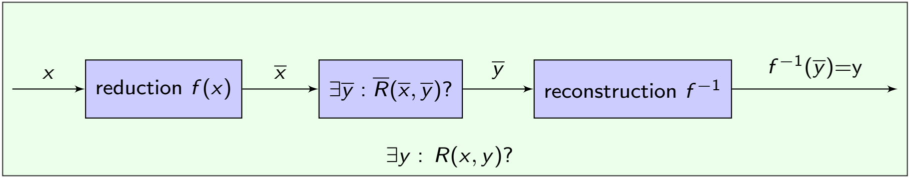


Polynomial reductions

Problem reductions are one of the greatest inventions in computer science.

Motto: *My problems are your problems.*

- Solving a new problem $R(x, y)$ via existing problem $\overline{R}(\overline{x}, \overline{y})$:

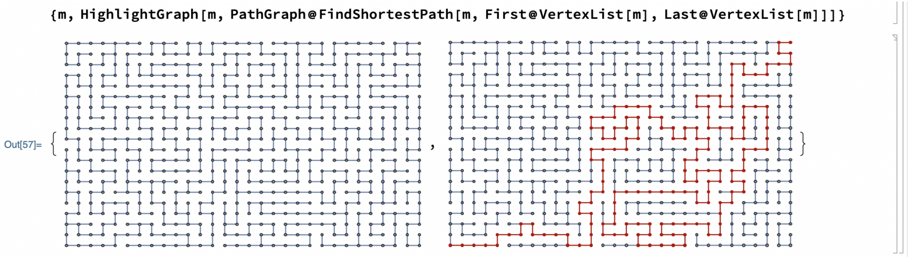


Namely, we will be interested in **polynomial-time reductions**.

- f and f^{-1} runs in a polynomial time
- Preserve membership in classes P and NP: $poly(poly(n)) \in \mathcal{O}(poly(n))$.
- Useful from the practical standpoint.

You have used polynomial reductions before

- Path with the minimum number of edges, but you only have Dijkstra.



- This is a polynomial reduction.

Some the reductions connect different worlds

- More examples: 3CNF-SAT $\triangleleft_P$ SubsetSum $(R(x,y) \triangleleft_P \overline{R}(\overline{x},\overline{y}))$

Definition: 3CNF-SAT Problem

- **Instance:** A propositional formula in conjunction normal form with clauses with 3 literals, e.g., $\phi = (x \vee \neg y \vee z) \wedge \ldots \wedge (\neg x \vee u \vee \neg v)$.
- **Decision:** Is the formula ϕ satisfiable?

Example

$$\phi = (x \vee y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge (x \vee \neg y \vee \neg z) \wedge$$
$$(\neg x \vee y \vee z) \wedge (\neg x \vee y \vee \neg z) \wedge (\neg x \vee \neg y \vee z) \wedge (\neg x \vee \neg y \vee \neg z)$$

The answer is **NO**.

3CNF-SAT to SubsetSum

- More examples: 3CNF-SAT $\triangleleft_P$ SubsetSum $(R(x,y) \triangleleft_P \overline{R}(\overline{x},\overline{y}))$

Definition: SubsetSum problem

- **Instance:** A (multi)-set of n non-negative integers $A = \{a_1, \dots, a_n\}$ and a non-negative integer W.
- **Decision:** Is there a subset $S \subseteq A$ such that $\sum_{a_i \in S} a_i = W$?

Example

$A = \{1, 1, 2, 3, 7, 9\}$, $W = 6$. Answer is **YES**: $S = \{1, 2, 3\}$.

- How can we use a number counting problem to solve a logic problem? These are different beasts.

Example: 3CNF-SAT to SubsetSum

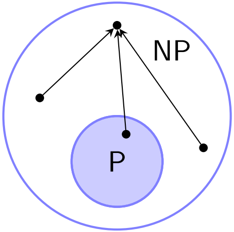
$$\phi = \underbrace{(\neg x \vee y \vee z)}_{C_1} \wedge \underbrace{(x \vee \neg y \vee z)}_{C_2} \wedge \underbrace{(\neg x \vee \neg y \vee \neg z)}_{C_3}$$

	x	y	z	C_1	C_2	C_3	
x	1	0	0	0	1	0	a_1
$\neg x$	1	0	0	1	0	1	a_2
y	0	1	0	1	0	0	a_3
$\neg y$	0	1	0	0	1	1	a_4
z	0	0	1	1	1	0	a_5
$\neg z$	0	0	1	0	0	1	a_6
	0	0	0	1	0	0	a_7
	0	0	0	2	0	0	a_8
	0	0	0	0	1	0	a_9
	0	0	0	0	2	0	a_{10}
	0	0	0	0	0	1	a_{11}
	0	0	0	0	0	2	a_{12}
	1	1	1	4	4	4	W

- Notice that no carry-overs are happening.
- **Homework:** does this work for kCNF-SAT (k literals in each clause)?

Complete problems: NP-complete

The idea of reductions can be used to identify so-called **complete problems** for the class.



Definition: NP-complete class

Problem R is NP-complete if $R \in \mathrm{NP}$ (i.e., efficiently checkable) and for every problem A :

$$\forall A \in \mathrm{NP} : A \lhd_P R \text{ (i.e., acts as a solver).}$$

- The meaning of an NP-complete problem is that it represents a "universal" problem for NP class (can be used to solve all problems in NP).
- The first NP-complete problem was discovered by Cook (1971):
  - Proof: non-deterministic TM $\lhd_P$ CNF-SAT.
  - Hence, CNF-SAT acts as a solver for class NP.
- Nowadays, we know thousands of NP-complete problems.

Example: CNF-SAT

Problem reductions are not particularly useful if they do not run in a polynomial time.

kCNF-SAT Problem

- **Instance:** A propositional formula in conjunction normal form, e.g., $\phi = (x \vee \neg y \vee z) \wedge ... \wedge (\neg x \vee u \vee \neg v)$.
- **Decision:** Is the formula ϕ satisfiable?

kDNF-SAT Problem

- **Instance:** A propositional formula in **disjunctive normal form**, e.g., $\phi = (x \wedge \neg y \wedge z) \vee ... \vee (\neg x \wedge u \wedge \neg v)$.
- **Decision:** Is the formula ϕ satisfiable?

Theorem

kCNF-SAT is in NP-complete (NTM reduces to poly-sized CNF formula).
kDNF-SAT is in P (easy algorithm).

Reduction idea: We have learned in TGR and LPS courses how to convert CNFs to DNFs (disjunctive normal form), and we know that DNF-SAT is solvable in a polynomial time (how?). So lets try

$$\text{kCNF-SAT} \lhd_P \text{kDNF-SAT}.$$

Example: CNF-SAT

```
In[12]:= cnf = (x1 ∨ y1) ∧ (x2 ∨ y2) ∧ (x3 ∨ y3) ∧ (x4 ∨ y4) ∧ (x5 ∨ y5) ∧ (x6 ∨ y6) ∧ (x7 ∨ y7);
         BooleanConvert[cnf] // TraditionalForm
```

Example: CNF-SAT

In[12]:=
```
cnf = (x₁ ∨ y₁) ∧ (x₂ ∨ y₂) ∧ (x₃ ∨ y₃) ∧ (x₄ ∨ y₄) ∧ (x₅ ∨ y₅) ∧ (x₆ ∨ y₆) ∧ (x₇ ∨ y₇);
BooleanConvert[cnf] // TraditionalForm
```

Out[13]//TraditionalForm=

$(x_1 \land x_2 \land x_3 \land x_4 \land x_5 \land x_6 \land x_7) \lor (x_1 \land x_2 \land x_3 \land x_4 \land x_5 \land x_6 \land y_7) \lor (x_1 \land x_2 \land x_3 \land x_4 \land x_5 \land y_6 \land x_7) \lor (x_1 \land x_2 \land x_3 \land x_4 \land x_5 \land y_6 \land y_7) \lor$
$(x_1 \land x_2 \land x_3 \land x_4 \land y_5 \land x_6 \land x_7) \lor (x_1 \land x_2 \land x_3 \land x_4 \land y_5 \land x_6 \land y_7) \lor (x_1 \land x_2 \land x_3 \land x_4 \land y_5 \land y_6 \land x_7) \lor (x_1 \land x_2 \land x_3 \land x_4 \land y_5 \land y_6 \land y_7) \lor$
$(x_1 \land x_2 \land x_3 \land y_4 \land x_5 \land x_6 \land x_7) \lor (x_1 \land x_2 \land x_3 \land y_4 \land x_5 \land x_6 \land y_7) \lor (x_1 \land x_2 \land x_3 \land y_4 \land x_5 \land y_6 \land x_7) \lor (x_1 \land x_2 \land x_3 \land y_4 \land x_5 \land y_6 \land y_7) \lor$
$(x_1 \land x_2 \land x_3 \land y_4 \land y_5 \land x_6 \land x_7) \lor (x_1 \land x_2 \land x_3 \land y_4 \land y_5 \land x_6 \land y_7) \lor (x_1 \land x_2 \land x_3 \land y_4 \land y_5 \land y_6 \land x_7) \lor (x_1 \land x_2 \land x_3 \land y_4 \land y_5 \land y_6 \land y_7) \lor$
$(x_1 \land x_2 \land y_3 \land x_4 \land x_5 \land x_6 \land x_7) \lor (x_1 \land x_2 \land y_3 \land x_4 \land x_5 \land x_6 \land y_7) \lor (x_1 \land x_2 \land y_3 \land x_4 \land x_5 \land y_6 \land x_7) \lor (x_1 \land x_2 \land y_3 \land x_4 \land x_5 \land y_6 \land y_7) \lor$
$(x_1 \land x_2 \land y_3 \land x_4 \land y_5 \land x_6 \land x_7) \lor (x_1 \land x_2 \land y_3 \land x_4 \land y_5 \land x_6 \land y_7) \lor (x_1 \land x_2 \land y_3 \land x_4 \land y_5 \land y_6 \land x_7) \lor (x_1 \land x_2 \land y_3 \land x_4 \land y_5 \land y_6 \land y_7) \lor$
$(x_1 \land x_2 \land y_3 \land y_4 \land x_5 \land x_6 \land x_7) \lor (x_1 \land x_2 \land y_3 \land y_4 \land x_5 \land x_6 \land y_7) \lor (x_1 \land x_2 \land y_3 \land y_4 \land x_5 \land y_6 \land x_7) \lor (x_1 \land x_2 \land y_3 \land y_4 \land x_5 \land y_6 \land y_7) \lor$
$(x_1 \land x_2 \land y_3 \land y_4 \land y_5 \land x_6 \land x_7) \lor (x_1 \land x_2 \land y_3 \land y_4 \land y_5 \land x_6 \land y_7) \lor (x_1 \land x_2 \land y_3 \land y_4 \land y_5 \land y_6 \land x_7) \lor (x_1 \land x_2 \land y_3 \land y_4 \land y_5 \land y_6 \land y_7) \lor$
$(x_1 \land y_2 \land x_3 \land x_4 \land x_5 \land x_6 \land x_7) \lor (x_1 \land y_2 \land x_3 \land x_4 \land x_5 \land x_6 \land y_7) \lor (x_1 \land y_2 \land x_3 \land x_4 \land x_5 \land y_6 \land x_7) \lor (x_1 \land y_2 \land x_3 \land x_4 \land x_5 \land y_6 \land y_7) \lor$
$(x_1 \land y_2 \land x_3 \land x_4 \land y_5 \land x_6 \land x_7) \lor (x_1 \land y_2 \land x_3 \land x_4 \land y_5 \land x_6 \land y_7) \lor (x_1 \land y_2 \land x_3 \land x_4 \land y_5 \land y_6 \land x_7) \lor (x_1 \land y_2 \land x_3 \land x_4 \land y_5 \land y_6 \land y_7) \lor$
$(x_1 \land y_2 \land x_3 \land y_4 \land x_5 \land x_6 \land x_7) \lor (x_1 \land y_2 \land x_3 \land y_4 \land x_5 \land x_6 \land y_7) \lor (x_1 \land y_2 \land x_3 \land y_4 \land x_5 \land y_6 \land x_7) \lor (x_1 \land y_2 \land x_3 \land y_4 \land x_5 \land y_6 \land y_7) \lor$
$(x_1 \land y_2 \land x_3 \land y_4 \land y_5 \land x_6 \land x_7) \lor (x_1 \land y_2 \land x_3 \land y_4 \land y_5 \land x_6 \land y_7) \lor (x_1 \land y_2 \land x_3 \land y_4 \land y_5 \land y_6 \land x_7) \lor (x_1 \land y_2 \land x_3 \land y_4 \land y_5 \land y_6 \land y_7) \lor$
$(x_1 \land y_2 \land y_3 \land x_4 \land x_5 \land x_6 \land x_7) \lor (x_1 \land y_2 \land y_3 \land x_4 \land x_5 \land x_6 \land y_7) \lor (x_1 \land y_2 \land y_3 \land x_4 \land x_5 \land y_6 \land x_7) \lor (x_1 \land y_2 \land y_3 \land x_4 \land x_5 \land y_6 \land y_7) \lor$
$(x_1 \land y_2 \land y_3 \land x_4 \land y_5 \land x_6 \land x_7) \lor (x_1 \land y_2 \land y_3 \land x_4 \land y_5 \land x_6 \land y_7) \lor (x_1 \land y_2 \land y_3 \land x_4 \land y_5 \land y_6 \land x_7) \lor (x_1 \land y_2 \land y_3 \land x_4 \land y_5 \land y_6 \land y_7) \lor$
$(x_1 \land y_2 \land y_3 \land y_4 \land x_5 \land x_6 \land x_7) \lor (x_1 \land y_2 \land y_3 \land y_4 \land x_5 \land x_6 \land y_7) \lor (x_1 \land y_2 \land y_3 \land y_4 \land x_5 \land y_6 \land x_7) \lor (x_1 \land y_2 \land y_3 \land y_4 \land x_5 \land y_6 \land y_7) \lor$
$(x_1 \land y_2 \land y_3 \land y_4 \land y_5 \land x_6 \land x_7) \lor (x_1 \land y_2 \land y_3 \land y_4 \land y_5 \land x_6 \land y_7) \lor (x_1 \land y_2 \land y_3 \land y_4 \land y_5 \land y_6 \land x_7) \lor (x_1 \land y_2 \land y_3 \land y_4 \land y_5 \land y_6 \land y_7) \lor$
$(y_1 \land x_2 \land x_3 \land x_4 \land x_5 \land x_6 \land x_7) \lor (y_1 \land x_2 \land x_3 \land x_4 \land x_5 \land x_6 \land y_7) \lor (y_1 \land x_2 \land x_3 \land x_4 \land x_5 \land y_6 \land x_7) \lor (y_1 \land x_2 \land x_3 \land x_4 \land x_5 \land y_6 \land y_7) \lor$
$(y_1 \land x_2 \land x_3 \land x_4 \land y_5 \land x_6 \land x_7) \lor (y_1 \land x_2 \land x_3 \land x_4 \land y_5 \land x_6 \land y_7) \lor (y_1 \land x_2 \land x_3 \land x_4 \land y_5 \land y_6 \land x_7) \lor (y_1 \land x_2 \land x_3 \land x_4 \land y_5 \land y_6 \land y_7) \lor$
$(y_1 \land x_2 \land x_3 \land y_4 \land x_5 \land x_6 \land x_7) \lor (y_1 \land x_2 \land x_3 \land y_4 \land x_5 \land x_6 \land y_7) \lor (y_1 \land x_2 \land x_3 \land y_4 \land x_5 \land y_6 \land x_7) \lor (y_1 \land x_2 \land x_3 \land y_4 \land x_5 \land y_6 \land y_7) \lor$
$(y_1 \land x_2 \land x_3 \land y_4 \land y_5 \land x_6 \land x_7) \lor (y_1 \land x_2 \land x_3 \land y_4 \land y_5 \land x_6 \land y_7) \lor (y_1 \land x_2 \land x_3 \land y_4 \land y_5 \land y_6 \land x_7) \lor (y_1 \land x_2 \land x_3 \land y_4 \land y_5 \land y_6 \land y_7) \lor$
$(y_1 \land x_2 \land y_3 \land x_4 \land x_5 \land x_6 \land x_7) \lor (y_1 \land x_2 \land y_3 \land x_4 \land x_5 \land x_6 \land y_7) \lor (y_1 \land x_2 \land y_3 \land x_4 \land x_5 \land y_6 \land x_7) \lor (y_1 \land x_2 \land y_3 \land x_4 \land x_5 \land y_6 \land y_7) \lor$
$(y_1 \land x_2 \land y_3 \land x_4 \land y_5 \land x_6 \land x_7) \lor (y_1 \land x_2 \land y_3 \land x_4 \land y_5 \land x_6 \land y_7) \lor (y_1 \land x_2 \land y_3 \land x_4 \land y_5 \land y_6 \land x_7) \lor (y_1 \land x_2 \land y_3 \land x_4 \land y_5 \land y_6 \land y_7) \lor$
$(y_1 \land x_2 \land y_3 \land y_4 \land x_5 \land x_6 \land x_7) \lor (y_1 \land x_2 \land y_3 \land y_4 \land x_5 \land x_6 \land y_7) \lor (y_1 \land x_2 \land y_3 \land y_4 \land x_5 \land y_6 \land x_7) \lor (y_1 \land x_2 \land y_3 \land y_4 \land x_5 \land y_6 \land y_7) \lor$
$(y_1 \land x_2 \land y_3 \land y_4 \land y_5 \land x_6 \land x_7) \lor (y_1 \land x_2 \land y_3 \land y_4 \land y_5 \land x_6 \land y_7) \lor (y_1 \land x_2 \land y_3 \land y_4 \land y_5 \land y_6 \land x_7) \lor (y_1 \land x_2 \land y_3 \land y_4 \land y_5 \land y_6 \land y_7) \lor$
$(y_1 \land y_2 \land x_3 \land x_4 \land x_5 \land x_6 \land x_7) \lor (y_1 \land y_2 \land x_3 \land x_4 \land x_5 \land x_6 \land y_7) \lor (y_1 \land y_2 \land x_3 \land x_4 \land x_5 \land y_6 \land x_7) \lor (y_1 \land y_2 \land x_3 \land x_4 \land x_5 \land y_6 \land y_7) \lor$
$(y_1 \land y_2 \land x_3 \land x_4 \land y_5 \land x_6 \land x_7) \lor (y_1 \land y_2 \land x_3 \land x_4 \land y_5 \land x_6 \land y_7) \lor (y_1 \land y_2 \land x_3 \land x_4 \land y_5 \land y_6 \land x_7) \lor (y_1 \land y_2 \land x_3 \land x_4 \land y_5 \land y_6 \land y_7) \lor$
$(y_1 \land y_2 \land x_3 \land y_4 \land x_5 \land x_6 \land x_7) \lor (y_1 \land y_2 \land x_3 \land y_4 \land x_5 \land x_6 \land y_7) \lor (y_1 \land y_2 \land x_3 \land y_4 \land x_5 \land y_6 \land x_7) \lor (y_1 \land y_2 \land x_3 \land y_4 \land x_5 \land y_6 \land y_7) \lor$
$(y_1 \land y_2 \land x_3 \land y_4 \land y_5 \land x_6 \land x_7) \lor (y_1 \land y_2 \land x_3 \land y_4 \land y_5 \land x_6 \land y_7) \lor (y_1 \land y_2 \land x_3 \land y_4 \land y_5 \land y_6 \land x_7) \lor (y_1 \land y_2 \land x_3 \land y_4 \land y_5 \land y_6 \land y_7) \lor$
$(y_1 \land y_2 \land y_3 \land x_4 \land x_5 \land x_6 \land x_7) \lor (y_1 \land y_2 \land y_3 \land x_4 \land x_5 \land x_6 \land y_7) \lor (y_1 \land y_2 \land y_3 \land x_4 \land x_5 \land y_6 \land x_7) \lor (y_1 \land y_2 \land y_3 \land x_4 \land x_5 \land y_6 \land y_7) \lor$
$(y_1 \land y_2 \land y_3 \land x_4 \land y_5 \land x_6 \land x_7) \lor (y_1 \land y_2 \land y_3 \land x_4 \land y_5 \land x_6 \land y_7) \lor (y_1 \land y_2 \land y_3 \land x_4 \land y_5 \land y_6 \land x_7) \lor (y_1 \land y_2 \land y_3 \land x_4 \land y_5 \land y_6 \land y_7) \lor$
$(y_1 \land y_2 \land y_3 \land y_4 \land x_5 \land x_6 \land x_7) \lor (y_1 \land y_2 \land y_3 \land y_4 \land x_5 \land x_6 \land y_7) \lor (y_1 \land y_2 \land y_3 \land y_4 \land x_5 \land y_6 \land x_7) \lor (y_1 \land y_2 \land y_3 \land y_4 \land x_5 \land y_6 \land y_7) \lor$

Example: CNF-SAT

Perhaps, if the DNF reduction would be done in a more sophisticated way:

```
In[16]:= BooleanMinimize[BooleanConvert[cnf]] // TraditionalForm
```

Example: CNF-SAT

Perhaps, if the DNF reduction would be done in a more sophisticated way:

In[16]:= `BooleanMinimize[BooleanConvert[cnf]] // TraditionalForm`

Out[16]//TraditionalForm=

$(x_1 \land x_2 \land x_3 \land x_4 \land x_5 \land x_6 \land x_7) \lor (x_1 \land x_2 \land x_3 \land x_4 \land x_5 \land x_6 \land y_7) \lor (x_1 \land x_2 \land x_3 \land x_4 \land x_5 \land x_7 \land y_6) \lor (x_1 \land x_2 \land x_3 \land x_4 \land x_5 \land y_6 \land y_7) \lor$

$(x_1 \land x_2 \land x_3 \land x_4 \land x_6 \land x_7 \land y_5) \lor (x_1 \land x_2 \land x_3 \land x_4 \land x_6 \land y_5 \land y_7) \lor (x_1 \land x_2 \land x_3 \land x_4 \land x_7 \land y_5 \land y_6) \lor (x_1 \land x_2 \land x_3 \land x_4 \land y_5 \land y_6 \land y_7) \lor$

$(x_1 \land x_2 \land x_3 \land x_5 \land x_6 \land x_7 \land y_4) \lor (x_1 \land x_2 \land x_3 \land x_5 \land x_6 \land y_4 \land y_7) \lor (x_1 \land x_2 \land x_3 \land x_5 \land x_7 \land y_4 \land y_6) \lor (x_1 \land x_2 \land x_3 \land x_5 \land y_4 \land y_6 \land y_7) \lor$

$(x_1 \land x_2 \land x_3 \land x_6 \land x_7 \land y_4 \land y_5) \lor (x_1 \land x_2 \land x_3 \land x_6 \land y_4 \land y_5 \land y_7) \lor (x_1 \land x_2 \land x_3 \land x_7 \land y_4 \land y_5 \land y_6) \lor (x_1 \land x_2 \land x_3 \land y_4 \land y_5 \land y_6 \land y_7) \lor$

$(x_1 \land x_2 \land x_4 \land x_5 \land x_6 \land x_7 \land y_3) \lor (x_1 \land x_2 \land x_4 \land x_5 \land x_6 \land y_3 \land y_7) \lor (x_1 \land x_2 \land x_4 \land x_5 \land x_7 \land y_3 \land y_6) \lor (x_1 \land x_2 \land x_4 \land x_5 \land y_3 \land y_6 \land y_7) \lor$

$(x_1 \land x_2 \land x_4 \land x_6 \land x_7 \land y_3 \land y_5) \lor (x_1 \land x_2 \land x_4 \land x_6 \land y_3 \land y_5 \land y_7) \lor (x_1 \land x_2 \land x_4 \land x_7 \land y_3 \land y_5 \land y_6) \lor (x_1 \land x_2 \land x_4 \land y_3 \land y_5 \land y_6 \land y_7) \lor$

$(x_1 \land x_2 \land x_5 \land x_6 \land x_7 \land y_3 \land y_4) \lor (x_1 \land x_2 \land x_5 \land x_6 \land y_3 \land y_4 \land y_7) \lor (x_1 \land x_2 \land x_5 \land x_7 \land y_3 \land y_4 \land y_6) \lor (x_1 \land x_2 \land x_5 \land y_3 \land y_4 \land y_6 \land y_7) \lor$

$(x_1 \land x_2 \land x_6 \land x_7 \land y_3 \land y_4 \land y_5) \lor (x_1 \land x_2 \land x_6 \land y_3 \land y_4 \land y_5 \land y_7) \lor (x_1 \land x_2 \land x_7 \land y_3 \land y_4 \land y_5 \land y_6) \lor (x_1 \land x_2 \land y_3 \land y_4 \land y_5 \land y_6 \land y_7) \lor$

$(x_1 \land x_3 \land x_4 \land x_5 \land x_6 \land x_7 \land y_2) \lor (x_1 \land x_3 \land x_4 \land x_5 \land x_6 \land y_2 \land y_7) \lor (x_1 \land x_3 \land x_4 \land x_5 \land x_7 \land y_2 \land y_6) \lor (x_1 \land x_3 \land x_4 \land x_5 \land y_2 \land y_6 \land y_7) \lor$

$(x_1 \land x_3 \land x_4 \land x_6 \land x_7 \land y_2 \land y_5) \lor (x_1 \land x_3 \land x_4 \land x_6 \land y_2 \land y_5 \land y_7) \lor (x_1 \land x_3 \land x_4 \land x_7 \land y_2 \land y_5 \land y_6) \lor (x_1 \land x_3 \land x_4 \land y_2 \land y_5 \land y_6 \land y_7) \lor$

$(x_1 \land x_3 \land x_5 \land x_6 \land x_7 \land y_2 \land y_4) \lor (x_1 \land x_3 \land x_5 \land x_6 \land y_2 \land y_4 \land y_7) \lor (x_1 \land x_3 \land x_5 \land x_7 \land y_2 \land y_4 \land y_6) \lor (x_1 \land x_3 \land x_5 \land y_2 \land y_4 \land y_6 \land y_7) \lor$

$(x_1 \land x_3 \land x_6 \land x_7 \land y_2 \land y_4 \land y_5) \lor (x_1 \land x_3 \land x_6 \land y_2 \land y_4 \land y_5 \land y_7) \lor (x_1 \land x_3 \land x_7 \land y_2 \land y_4 \land y_5 \land y_6) \lor (x_1 \land x_3 \land y_2 \land y_4 \land y_5 \land y_6 \land y_7) \lor$

$(x_1 \land x_4 \land x_5 \land x_6 \land x_7 \land y_2 \land y_3) \lor (x_1 \land x_4 \land x_5 \land x_6 \land y_2 \land y_3 \land y_7) \lor (x_1 \land x_4 \land x_5 \land x_7 \land y_2 \land y_3 \land y_6) \lor (x_1 \land x_4 \land x_5 \land y_2 \land y_3 \land y_6 \land y_7) \lor$

$(x_1 \land x_4 \land x_6 \land x_7 \land y_2 \land y_3 \land y_5) \lor (x_1 \land x_4 \land x_6 \land y_2 \land y_3 \land y_5 \land y_7) \lor (x_1 \land x_4 \land x_7 \land y_2 \land y_3 \land y_5 \land y_6) \lor (x_1 \land x_4 \land y_2 \land y_3 \land y_5 \land y_6 \land y_7) \lor$

$(x_1 \land x_5 \land x_6 \land x_7 \land y_2 \land y_3 \land y_4) \lor (x_1 \land x_5 \land x_6 \land y_2 \land y_3 \land y_4 \land y_7) \lor (x_1 \land x_5 \land x_7 \land y_2 \land y_3 \land y_4 \land y_6) \lor (x_1 \land x_5 \land y_2 \land y_3 \land y_4 \land y_6 \land y_7) \lor$

$(x_1 \land x_6 \land x_7 \land y_2 \land y_3 \land y_4 \land y_5) \lor (x_1 \land x_6 \land y_2 \land y_3 \land y_4 \land y_5 \land y_7) \lor (x_1 \land x_7 \land y_2 \land y_3 \land y_4 \land y_5 \land y_6) \lor (x_1 \land y_2 \land y_3 \land y_4 \land y_5 \land y_6 \land y_7) \lor$

$(x_2 \land x_3 \land x_4 \land x_5 \land x_6 \land x_7 \land y_1) \lor (x_2 \land x_3 \land x_4 \land x_5 \land x_6 \land y_1 \land y_7) \lor (x_2 \land x_3 \land x_4 \land x_5 \land x_7 \land y_1 \land y_6) \lor (x_2 \land x_3 \land x_4 \land x_5 \land y_1 \land y_6 \land y_7) \lor$

$(x_2 \land x_3 \land x_4 \land x_6 \land x_7 \land y_1 \land y_5) \lor (x_2 \land x_3 \land x_4 \land x_6 \land y_1 \land y_5 \land y_7) \lor (x_2 \land x_3 \land x_4 \land x_7 \land y_1 \land y_5 \land y_6) \lor (x_2 \land x_3 \land x_4 \land y_1 \land y_5 \land y_6 \land y_7) \lor$

$(x_2 \land x_3 \land x_5 \land x_6 \land x_7 \land y_1 \land y_4) \lor (x_2 \land x_3 \land x_5 \land x_6 \land y_1 \land y_4 \land y_7) \lor (x_2 \land x_3 \land x_5 \land x_7 \land y_1 \land y_4 \land y_6) \lor (x_2 \land x_3 \land x_5 \land y_1 \land y_4 \land y_6 \land y_7) \lor$

$(x_2 \land x_3 \land x_6 \land x_7 \land y_1 \land y_4 \land y_5) \lor (x_2 \land x_3 \land x_6 \land y_1 \land y_4 \land y_5 \land y_7) \lor (x_2 \land x_3 \land x_7 \land y_1 \land y_4 \land y_5 \land y_6) \lor (x_2 \land x_3 \land y_1 \land y_4 \land y_5 \land y_6 \land y_7) \lor$

$(x_2 \land x_4 \land x_5 \land x_6 \land x_7 \land y_1 \land y_3) \lor (x_2 \land x_4 \land x_5 \land x_6 \land y_1 \land y_3 \land y_7) \lor (x_2 \land x_4 \land x_5 \land x_7 \land y_1 \land y_3 \land y_6) \lor (x_2 \land x_4 \land x_5 \land y_1 \land y_3 \land y_6 \land y_7) \lor$

$(x_2 \land x_4 \land x_6 \land x_7 \land y_1 \land y_3 \land y_5) \lor (x_2 \land x_4 \land x_6 \land y_1 \land y_3 \land y_5 \land y_7) \lor (x_2 \land x_4 \land x_7 \land y_1 \land y_3 \land y_5 \land y_6) \lor (x_2 \land x_4 \land y_1 \land y_3 \land y_5 \land y_6 \land y_7) \lor$

$(x_2 \land x_5 \land x_6 \land x_7 \land y_1 \land y_3 \land y_4) \lor (x_2 \land x_5 \land x_6 \land y_1 \land y_3 \land y_4 \land y_7) \lor (x_2 \land x_5 \land x_7 \land y_1 \land y_3 \land y_4 \land y_6) \lor (x_2 \land x_5 \land y_1 \land y_3 \land y_4 \land y_6 \land y_7) \lor$

$(x_2 \land x_6 \land x_7 \land y_1 \land y_3 \land y_4 \land y_5) \lor (x_2 \land x_6 \land y_1 \land y_3 \land y_4 \land y_5 \land y_7) \lor (x_2 \land x_7 \land y_1 \land y_3 \land y_4 \land y_5 \land y_6) \lor (x_2 \land y_1 \land y_3 \land y_4 \land y_5 \land y_6 \land y_7) \lor$

$(x_3 \land x_4 \land x_5 \land x_6 \land x_7 \land y_1 \land y_2) \lor (x_3 \land x_4 \land x_5 \land x_6 \land y_1 \land y_2 \land y_7) \lor (x_3 \land x_4 \land x_5 \land x_7 \land y_1 \land y_2 \land y_6) \lor (x_3 \land x_4 \land x_5 \land y_1 \land y_2 \land y_6 \land y_7) \lor$

$(x_3 \land x_4 \land x_6 \land x_7 \land y_1 \land y_2 \land y_5) \lor (x_3 \land x_4 \land x_6 \land y_1 \land y_2 \land y_5 \land y_7) \lor (x_3 \land x_4 \land x_7 \land y_1 \land y_2 \land y_5 \land y_6) \lor (x_3 \land x_4 \land y_1 \land y_2 \land y_5 \land y_6 \land y_7) \lor$

$(x_3 \land x_5 \land x_6 \land x_7 \land y_1 \land y_2 \land y_4) \lor (x_3 \land x_5 \land x_6 \land y_1 \land y_2 \land y_4 \land y_7) \lor (x_3 \land x_5 \land x_7 \land y_1 \land y_2 \land y_4 \land y_6) \lor (x_3 \land x_5 \land y_1 \land y_2 \land y_4 \land y_6 \land y_7) \lor$

$(x_3 \land x_6 \land x_7 \land y_1 \land y_2 \land y_4 \land y_5) \lor (x_3 \land x_6 \land y_1 \land y_2 \land y_4 \land y_5 \land y_7) \lor (x_3 \land x_7 \land y_1 \land y_2 \land y_4 \land y_5 \land y_6) \lor (x_3 \land y_1 \land y_2 \land y_4 \land y_5 \land y_6 \land y_7) \lor$

$(x_4 \land x_5 \land x_6 \land x_7 \land y_1 \land y_2 \land y_3) \lor (x_4 \land x_5 \land x_6 \land y_1 \land y_2 \land y_3 \land y_7) \lor (x_4 \land x_5 \land x_7 \land y_1 \land y_2 \land y_3 \land y_6) \lor (x_4 \land x_5 \land y_1 \land y_2 \land y_3 \land y_6 \land y_7) \lor$

$(x_4 \land x_6 \land x_7 \land y_1 \land y_2 \land y_3 \land y_5) \lor (x_4 \land x_6 \land y_1 \land y_2 \land y_3 \land y_5 \land y_7) \lor (x_4 \land x_7 \land y_1 \land y_2 \land y_3 \land y_5 \land y_6) \lor (x_4 \land y_1 \land y_2 \land y_3 \land y_5 \land y_6 \land y_7) \lor$

$(x_5 \land x_6 \land x_7 \land y_1 \land y_2 \land y_3 \land y_4) \lor (x_5 \land x_6 \land y_1 \land y_2 \land y_3 \land y_4 \land y_7) \lor (x_5 \land x_7 \land y_1 \land y_2 \land y_3 \land y_4 \land y_6) \lor (x_5 \land y_1 \land y_2 \land y_3 \land y_4 \land y_6 \land y_7) \lor$

$(x_6 \land x_7 \land y_1 \land y_2 \land y_3 \land y_4 \land y_5) \lor (x_6 \land y_1 \land y_2 \land y_3 \land y_4 \land y_5 \land y_7) \lor (x_7 \land y_1 \land y_2 \land y_3 \land y_4 \land y_5 \land y_6) \lor (y_1 \land y_2 \land y_3 \land y_4 \land y_5 \land y_6 \land y_7)$

Example: CNF-SAT

Takeaways:

- The above example shows an exponential explosion of the resulting DNF formula.
- Unfortunately, we do not know how to convert, in general, every CNF formula to DNF in a polynomial time.
- But reductions in the opposite direction, i.e., something $\triangleleft_P$ CNF-SAT, are in fact very useful:
  - formal verification: some states are not reachable within any k steps
  - proof checking: Keller's conjecture[3]
  - graph coloring, ...
- CNF-SAT is both theoretically (a universal NP problem) and practically (existence of solvers) appealing.

[3] `https://www.quantamagazine.org/computer-search-settles-90-year-old-math-problem-20200819/`

NP-complete: summary

NP-complete class summary:

- The set of universal (most difficult) problems for class NP.
- All algorithms we know for NP-complete problems have complexity above $\mathcal{O}(poly(n))$.
  - e.g., CNF-SAT algorithm is $\mathcal{O}(1.308^n) \approx \mathcal{O}(2^{0.387n})$
- Solving efficiently one of the thousands known NP-complete problems would mean P = NP.
  - Hence, if your problem is NP-complete do not hope for a poly-time algorithm.

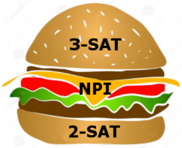
NP problems suspected not being NP-complete and not in P

- Graph Isomorphism (GI)
  - We know a subexponential algorithm, but still above a polynomial complexity.
- Integer Factoring
- Computing VC (Vapnik-Chervonenkis) dimension

NP-complete: summary

NP-complete class summary:

- The set of universal (mos
- All algorithms we know f ... xity above $\mathcal{O}(poly(n))$.
  - e.g., CNF-SAT algorithm i
- Solving efficiently one of ... blems would mean P = NP.
  - Hence, if your problem is l ... n.



Complexity sandwich: But can it be filled with natural ingredients?

NP problems suspected **not being** NP-complete and not in P

- Graph Isomorphism (GI)
  - We know a subexponential algorithm, but still above a polynomial complexity.
- Integer Factoring
- Computing VC (Vapnik-Chervonenkis) dimension

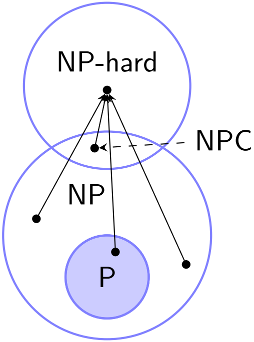
Beyond NP-complete: NP-hard class

Definition: NP-hard class

Problem R is NP-hard if for every problem A

$$\forall A \in \mathrm{NP} : A \triangleleft_P R.$$

- sets a **lower bound** on the complexity of the problem (acts as a solver for class NP)
- the difference from NP-complete is that R can be much harder (does not have to be in NP)



if P $\neq$ NP

Examples

- every NP-complete decision problem
- optimization variants of NP-complete decision problems
- Quantified Boolean formula satisfiability: $\forall x_1 \exists x_2 \forall x_3, \ldots : f(x_1, x_2, x_3, \ldots)$

Conclusion

The main takeaways:

- Turing machine is the universal model of computation
  - Gives us a formal way studying and categorizing problems according to their complexity.
- Easy problems (P) vs. hard problems (NP-complete, NP-hard):
  - Easily solvable vs. easily checkable vs. just hard problems
  - More complexity classes live in Complexity ZOO: `https://complexityzoo.net/`.
- Polynomial reductions:
  - Using somebody else's problem to solve your problems.

References

- A. Borodin, Torronto Uni, CSC373[4]
- W. Gasarch: P vs NP survey[5]
- S. Aaronson: P vs NP status [6]
- L. Babai: Quasipoly algorithm for GI[7]
- Bournez et al.: Polynomial Time Corresponds to Solutions of Polynomial Ordinary Differential Equations of Polynomial Length[8]

[4] https://www.cs.toronto.edu/~bor/373s13/
[5] https://www.cs.umd.edu/users/gasarch/BLOGPAPERS/pollpaper3.pdf
[6] https://www.scottaaronson.com/papers/pnp.pdf
[7] https://arxiv.org/abs/1512.03547
[8] https://arxiv.org/abs/1601.05360