Spooky reductions and hardness

10/31/24

Recall: Poly-time reductions

- What to compare the computational difficulty of problems
- Stick to decision problems: Answer is “yes” or “no”

- Poly-time reducibility:

  $A \leqslant_p B$ if x in A if and only if f(x) in B and

  f can be computed in polynomial time

- If B can be solved in polynomial time, then so can A
- If A cannot be solved in polynomial time, then neither can B

Recall: CIRCUIT-SAT

{<C> : C is a satisfiable boolean circuit }

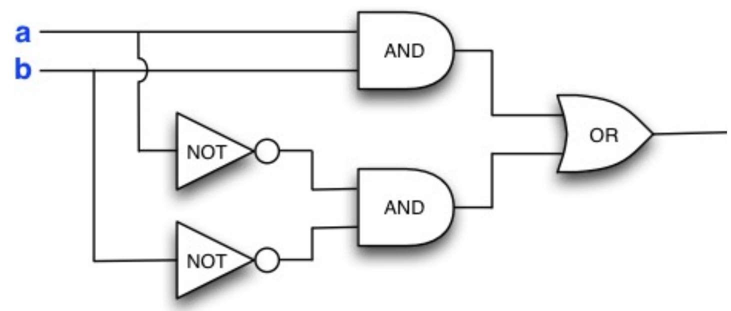

Image: https://algorithms.cs.aalto.fi/Teaching/CS-A1120/2018/notes/round-combinational-logic.html

Satisfiability (SAT)

- Boolean variables: $x_1, x_2, x_3, \ldots, x_n$
- Term: Variable or its negation $x_i, \overline{x_i}$
- Clause: Terms combined with or $x_i \vee \overline{x_j} \vee \overline{x_k} \vee x_l$
- Expression: Clauses joined with and $(x_i \vee \overline{x_j} \vee \overline{x_k} \vee x_l) \wedge (x_a \vee \overline{x_b})$

Satisfiability (SAT)

- Boolean variables: $x_1, x_2, x_3, \ldots, x_n$
- Term: Variable or its negation $x_i, \overline{x_i}$
- Clause: Terms combined with or $x_i \vee \overline{x_j} \vee \overline{x_k} \vee x_l$
- Expression: Clauses joined with and $(x_i \vee \overline{x_j} \vee \overline{x_k} \vee x_l) \wedge (x_a \vee \overline{x_b})$

Does an expression have a satisfying assignment? (i.e. can it be made true?)

Is the expression below satisfiable?

$$(x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (x_1 \vee x_2) \wedge (\overline{x_1} \vee x_2 \vee x_3) \wedge \overline{x_2}$$

A. Yes

B. No

Is the expression below satisfiable?

$$(x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (x_1 \vee x_2) \wedge (\overline{x_1} \vee x_2 \vee x_3) \wedge \overline{x_2}$$

A. Yes
B. No

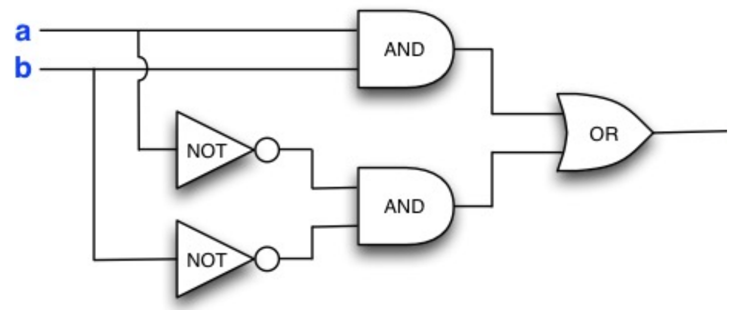

Image: https://algorithms.cs.aalto.fi/Teaching/CS-A1120/2018/notes/round-combinational-logic.html

3-Satisfiability (3SAT)

- Boolean variables: $x_1, x_2, x_3, \ldots, x_n$
- Term: Variable or its negation $x_i, \overline{x_i}$
- Clause: Exactly 3 terms combined with or $x_i \vee \overline{x_j} \vee \overline{x_k}$
- Expression: Clauses joined with and $(x_i \vee \overline{x_j} \vee \overline{x_k}) \wedge (x_a \vee \overline{x_b} \vee x_c)$

Does an expression have a satisfying assignment? (i.e. can it be made true?)

How many of the expressions below are in the correct form for 3SAT?

I. $(x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (x_1 \vee x_2) \wedge (\overline{x_1} \vee x_2 \vee x_3)$

II. $(x_1 \vee \overline{x_1} \vee \overline{x_3}) \wedge (\overline{x_1} \vee x_2 \vee x_3) \wedge (\overline{x_2} \vee x_3 \vee x_4)$

III. $(x_1 \wedge \overline{x_2} \wedge \overline{x_4}) \vee (\overline{x_1} \wedge x_3 \wedge x_4)$

IV. $(x_2 \vee \overline{x_3} \vee x_4) \wedge (x_1 \vee x_2 \vee \overline{x_3} \vee x_4)$

A. 0 B. 1 C. 2 D. 3 E. 4

How many of the expressions below are in the correct form for 3SAT?

I. $(x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (x_1 \vee x_2) \wedge (\overline{x_1} \vee x_2 \vee x_3)$

II. $(x_1 \vee \overline{x_1} \vee \overline{x_3}) \wedge (\overline{x_1} \vee x_2 \vee x_3) \wedge (\overline{x_2} \vee x_3 \vee x_4)$

III. $(x_1 \wedge \overline{x_2} \wedge \overline{x_4}) \vee (\overline{x_1} \wedge x_3 \wedge x_4)$

IV. $(x_2 \vee \overline{x_3} \vee x_4) \wedge (x_1 \vee x_2 \vee \overline{x_3} \vee x_4)$

A. 0

B. 1 (just II.)

C. 2

D. 3

E. 4

Transitivity

- We've now shown

  CIRCUIT-SAT $\leqslant_p$ SAT $\leqslant_p$ 3SAT

  Just as the notation suggests, this means CIRCUIT-SAT $\leqslant_p$ 3SAT.

  In other words, poly-time reductions are transitive

CLIQUE

- A clique of size k in a graph is k vertices that are all mutually adjacent
- Given a graph G and integer k, does G have a clique of size k?

INDEPENDENT SET

- An independent set of size k in a graph is k vertices, none of which are adjacent
- Given a graph G and integer k, does G have an independent set of size k?

Hardness so far

- Polynomial-time reductions:

  $A \leqslant_p B$ if x in A if and only if f(x) in B and

  f can be computed in polynomial time

CIRCUIT-SAT $\leqslant_p$ SAT $\leqslant_p$ 3SAT $\leqslant_p$ CLIQUE $\leqslant_p$ INDEPENDENT SET