Intractable Problems

- Clique
- Independent Set
- Vertex Cover
- Set Cover
- Set Packing
- Satisfiability Problem
- Hamiltonian Cycle and Path
- Traveling Salesman Problem
- Graph Coloring
- Circuit Satisfiability
- Knapsack
- Subset Sum
- Prime and Factor
- Partition

Imdadullah Khan

The Satisfiability Problem : SAT

- Given n Boolean variables $x_1, \ldots, x_n$
- A literal is a variable appearing in some formula as x_i or $\overline{x_i}$
- A clause is an OR of one or more literals
- A CNF formula (conjunctive normal form) is a Boolean expression that is AND of one or more clauses
- A formula is satisfiable if there is an assignment of $0/1$ values to the variables such that the formula evaluates to 1 (or true)

1. $f_1 = (x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \bar{x_2}) \wedge (x_2 \vee \bar{x_3})$
   - f_1 is satisfiable (the assignment is $x_1 = 1, x_2 = 1, x_3 = 1$)
   - $x_1 = 1, x_2 = 0, x_3 = 0$ is also a satisfying assignment
2. $f_2 = (x_1 \vee \bar{x_2}) \wedge (x_1 \vee x_2) \wedge (\bar{x_1} \vee \bar{x_2}) \wedge (\bar{x_1} \vee x_2)$ is not satisfiable

The SAT(f) problem: Is there a satisfying assignment for the formula f?

The Satisfiability Problem : 3-SAT

- Given n Boolean variables $x_1, \ldots, x_n$
- Each can take a value of 0/1 (true/false)
- A literal is a variable appearing in some formula as x_i or $\bar{x}_i$
- A clause of size 3 is an OR of three literals
- A 3-CNF formula is AND of one or more clauses of size ≤ 3
- A formula is satisfiable if there is an assignment of 0/1 values to the variables such that the formula evaluates to 1 (or true)

The 3-SAT(f) problem: Is there a satisfying assignment for f?

The Satisfiability Problem :Applications

- Many applications in hardware/software verification
- Also in planning, partitioning, scheduling
- Model all kind of constrained satisfaction problem
- Many hard problems can be stated in terms of SAT
- Consider the following constraints:
  - John can only meet either on Monday, Wednesday or Thursday
  - Catherine cannot meet on Wednesday
  - Anne cannot meet on Friday
  - Peter cannot meet neither on Tuesday nor on Thursday
- Question: When can the meeting take place if at all?

Encode them into the following Boolean formula:

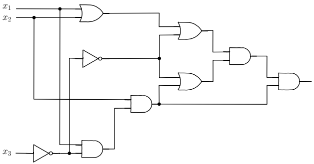
$$(Mon \vee Wed \vee Thu) \wedge (\neg Wed) \wedge (\neg Fri) \wedge (\neg Tue \vee \neg Thu)$$

The meeting must take place on Monday

Circuit Satisfiability Problem

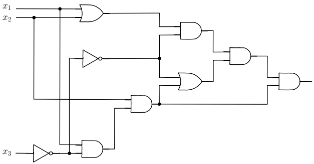
- A combinatorial circuit is a general purpose gate (general logic gate)
- It take n Boolean inputs and outputs one Boolean output
- Implemented with basic of AND, OR, and NOT logic gates

A combinatorial circuit C is satisfiable if there exits an input of 0's and 1's on which C outputs 1



This circuit is not satisfiable

Figures adapted from CLRS Figure 34.8



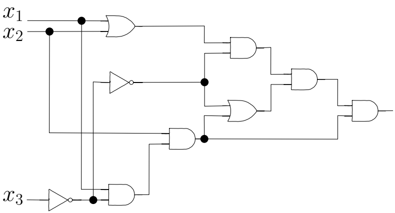
This circuit is satisfied with $(x_1, x_2, x_3) = (1, 1, 0)$

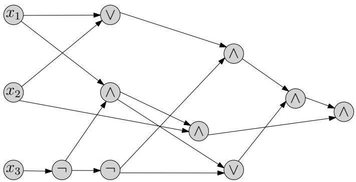
The CIRCUIT-SAT(C) problem: Is there an input satisfying C?

Computation of Combinatorial Circuit

Encoding of combinatorial circuits

- Encoded as a directed acyclic graph (DAG)
- nodes correspond to gates, input wires and output wire
- (nodes corresponding to) NOT gates have indegree 1
- AND gates and OR gates have indegree 2
- input wires with constant inputs have indegree 0 (labeled with input values)
- input wires with unknown inputs have indegree 0 (labeled with variable names)
- output wire has outdegree 0 (it is a sink)

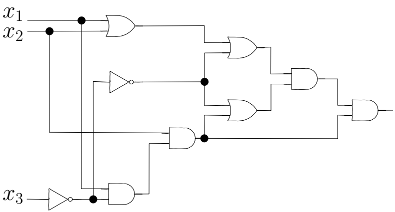


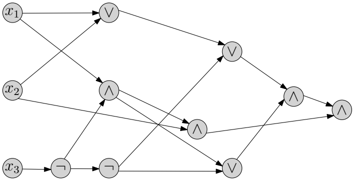


Computation of Combinatorial Circuit

Evaluation of a combinatorial circuit (DAG)

- Given an 0/1 values to the input variables
- Process vertices of DAG in topologically sorted order
- Compute value of a node using Boolean logic (e.g. $\mathbf{0}$ OR $\mathbf{1} = \mathbf{1}$)
- Value of the circuit is value at the sink node





Verify that on $(x_1, x_2, x_3) = (1, 1, 0)$ the output value is $\mathbf{1}$

CIRCUIT-SAT Applications

Computer-Aided Circuit (Hardware) Optimization:

- If a digital circuit or one of its sub-circuits is not satisfiable, then replace it with a constant output

Complexity Theory:

- A fundamental construct in complexity theory
- All problems listed above can be phrased in terms of CIRCUIT-SAT(C) for appropriately defined circuit C