

Polynomial-Time Verification of Boolean Circuit Evaluation Using DFS

Manav Mantry

Problem Statement

Given a Boolean circuit instance whose output evaluates to `true`, explain how the correctness of the result can be verified in polynomial time using Depth First Search (DFS).

Boolean Circuit Model

A Boolean circuit can be represented as a **directed acyclic graph (DAG)** where:

- Nodes represent logic gates (AND, OR, NOT)
- Leaves represent input variables or constants
- Edges represent signal flow from inputs to outputs
- There is a unique output node

Verification Goal

Given:

- A Boolean circuit C
- An assignment of truth values to input variables
- A claimed output value `true`

The goal is to verify that the circuit indeed evaluates to `true` under the given assignment.

Using Depth First Search (DFS)

Step 1: Represent the Circuit as a Graph

The circuit is treated as a directed graph, with edges directed from input nodes towards the output node.

Step 2: Perform DFS from the Output Node

A Depth First Search is initiated from the output gate and proceeds backwards toward the input nodes.

During DFS:

- Each gate is visited once
- The values of its input gates are recursively evaluated

Step 3: Gate Evaluation

For each visited node:

- If the node is an input variable, its value is read directly
- If the node is a NOT gate, the value of its child is negated
- If the node is an AND gate, all child values are checked to be **true**
- If the node is an OR gate, at least one child value must be **true**

The computed value is returned to the parent node in the DFS recursion.

Step 4: Verification of Output

If the DFS evaluation of the output node results in **true**, then the correctness of the circuit evaluation is verified.

Time Complexity Analysis

- Each gate and wire in the circuit is visited exactly once
- Each gate operation takes constant time

Let n be the size of the circuit (number of gates and wires). Then the total verification time is:

$$O(n)$$

Thus, the correctness of the Boolean circuit output can be verified in polynomial time.

Conclusion

Depth First Search enables polynomial-time verification of a Boolean circuit output by evaluating each g
--

This demonstrates that the Boolean Circuit Value problem belongs to the complexity class **NP**, since a proposed solution can be efficiently verified.