Boolean Circuits

Definition 1. Syntax: *A Boolean circuit is a (directed acyclic) graph $C = (V, E)$ where the nodes (gates) in $V = \{1, \ldots, n\}$ can be either a boolean connective or a variable or $\{true, false\}$ and edges are of the form (i, j) where $i < j$. Gates with no incoming edges (variables or true/false) are input gates. Output gates have no outgoing edges (typically one — numbered n). The gates $\wedge$ and $\vee$ have indegree 2 and gate $\neg$ has indegree 1.*

Semantics: *Specifies a truth value to each appropriate truth assignment of the variable gates. The value of the circuit is value of the output gate computed inductively "bottom up".*

Computational Problems

CIRCUIT SAT: Given a circuit C, is there a truth assignment T appropriate to C such that $T(C) = true$.

Computationally equivalent to SAT, $\in NP$.

CIRCUIT VALUE: Given a circuit with no variable gates (i.e., only true/false inputs) is the value of the gate true.

$\in P$.

Size of Boolean Circuits

Theorem 1. [Shannon] *For any* $n \geq 2$ *there is a* n*-ary boolean function* f *such that no boolean circuit with* $\frac{2^n}{2n}$ *or fewer gates can compute it.*

Proof: We will give a counting argument.

Suppose not. Then for some $n \geq 2$ all n-ary boolean functions can be computed with $m = 2^n/2n$ or fewer gates.

The number of circuits with n variables and m or fewer gates is bounded by $((n+5).m^2)^m$.

The number of different n-ary boolean functions is 2^{2^n}.

$((n+5).m^2)^m < 2^{2^n}$ if $m = 2^n/2n$.

That is, two *different* boolean functions are computed by the same circuit. Contradiction. QED

Compactness Theorem

Theorem 2. *A set S of expressions is satisfiable iff every finite subset of S is satisfiable.*

Resolution

A method to determine whether a Boolean expression ϕ in CNF form is satisfiable.

0. $\phi^* = \phi$.

1. Repeat until possible:

Let $(x \vee C)$ and $(\neg x \vee D)$ be two clauses in ϕ^*.

Add the clause $(C \vee D)$ (*resolvent*) to ϕ^*.

2. If ϕ^* contains the empty clause then ϕ is not satisfiable else satisfiable.