CS256
Applied Theory of Computation

Circuit Complexity I

John E Savage
Overview

- The circuit model of computation
- Circuit complexity measures
  - Size, depth, formula size
  - Size with fan-out restriction
- Relationships between complexity measures
  - The effect of fan-out limitation and basis change
  - Formula size with different bases
Motivation

- Let $f_L^{(n)} : B^n \rightarrow B$ be characteristic function of an NP-complete language $L$ where $f_L^{(n)}(w)$ is 1 if $w$ is in $L$ and 0 otherwise.
- If $f_L^{(n)}$ has super-polynomial circuit size, then $P \neq NP$.
- It is very difficult to derive more than linear-sized lower bounds or more than logarithmic-depth lower bounds.
Circuit Complexity Measures

- Important terms
  - Basis (for a circuit), standard basis (AND, OR & NOT)
  - Complete basis
  - Fan-in, fan-out
  - Monotone basis (AND, OR)
  - Monotone increasing and decreasing functions
  - Disjunctive normal form
  - Conjunctive normal form
Circuit Complexity Measures

**Definition** Let $f : B^n \to B^m$. The circuit size $C_\Omega(f)$ of the function $f$ is the size of the smallest circuit for $f$ in which gates are drawn from the set $\Omega$ (the basis).

The circuit depth $D_\Omega(f)$ of $f$ is the depth of the smallest depth circuit in which gates are drawn from the basis $\Omega$. When obvious, the subscript $\Omega$ is dropped.
Circuit Complexity Measures

- The **circuit size with fan-out** $s$, denoted $C_{\Omega,s}(f)$, is the size of the smallest circuit for $f$ when each gate has fan-out of at most $s$.

- **Formula size** over the basis $\Omega$, denoted $L_{\Omega}(f)$, is the minimal number of *external inputs* to gates in circuit for $f$ in which each gate has fan-out at most 1.
Effect of Fan-Out on Circuit Size

Lemma A rooted tree of maximal fan-in \( r \) containing \( k \) internal vertices has at most \( k(r-1) + 1 \) leaves.

A rooted tree with edges directed toward the root with \( l \) leaves and fan-in 2 or more has at most \( l-1 \) internal vertices with fan-in 2 or more.

A rooted tree with \( l \) leaves and fan-in 2 or more has at most \( 2(l-1) \) edges.
Effect of Fan-Out on Circuit Size

**Lemma** Over the standard basis $\Omega$,
\[
\frac{(L(f) - 1)}{(r-1)} \leq C_{\Omega,1}(f) \leq 3L(f) - 2.
\]

**Proof** The second inequality counts the number of two-input gates ($\leq L(f) - 1$) and the number of NOTs ($\leq 2(L(f) - 1) + 1$, one per edge and the output).

- Let $l(\Omega)$ be the no. gates over a complete basis $\Omega$ to realize the identity function. To show that $l(\Omega)$ is 1 or 2, ask if a complete basis contains a non-monotone function. If so, can it realize the NOT gate?
Effect of Fan-Out on Circuit Size

Theorem Let $\Omega$ be a complete basis of fan-in $r$ and let $f : B^n \rightarrow B$. The following hold for $s \geq 2$:

$$C_\Omega(f) \leq C_{\Omega,s+1}(f) \leq C_{\Omega,s}(f) \leq C_{\Omega,1}(f)$$

$$C_{\Omega,s}(f) \leq C_\Omega(f) \left(1 + (l(\Omega)(r-1)/(s-1))\right)$$

Proof Consider second. For a gate in optimal circuit with fan-out $\Phi > s$, replace its $\Phi$ outputs by a tree with fan-out $s$ of identity functions. It has at most $k$ copies of the identify function where $k < (\Phi-1)/(s-1)$. Let $\Phi_i$ be fan-out of the $i$th gate in optimal fan-out circuit. Thus, at most $l(\Omega) \left(\sum_i C(f)(\Phi_i - 1)/(s-1)\right)$ extra gates are needed. But $\sum_i C(f) \Phi_i \leq rC_\Omega(f)$. (Why?)
Changing the Basis of a Circuit

**Lemma** The circuit size and depth of $f : \mathbb{B}^n \rightarrow \mathbb{B}^m$ over two different complete bases differ by multiplicative factors.

**Proof** Let $\Omega_1$ and $\Omega_2$ be the two complete bases in question. Since every element of one basis can be simulated by a few elements of the other, this results in at most a constant factor difference in the minimal circuit sizes and depths over the two bases.
Separator Theorem for Trees

- To establish a relationship between formula size and circuit depth, we develop a separator theorem for trees.

- A separator theorem says that a graph can be separated into two parts by removing a small number of elements (the separator) and bounds the size of each part and the size of the separator.
Separator Theorem for Trees

- **Theorem** Let $T$ be a tree with $n$ leaves of fan-in $r$. Then for any $r \leq k \leq n$, $T$ has a vertex $v$ (the separator) such that subtree $T_v$ rooted at $v$ has $\geq k$ leaves but each of its children has $< k$ leaves.

- **Proof** If the condition is not true at the root of $T$, $T$ has a child with more than $k$ leaves. Apply the procedure to this child. This procedure terminates before reaching a leaf vertex or it terminates on a leaf vertex because leaves have no children.
Separator Theorem for Trees

- **Corollary** Let $T$ be a tree of fan-in $r$ with $n$ leaves. Then it has a subtree $T_v$ rooted at $v$ that has at least $n/(r+1)$ and at most $rn/(r+1)$ leaves.

- **Proof** Use previous theorem with $k = \lceil n/(r+1) \rceil$. Since $T_v$ has at most $r$ subtrees and each has at most $k-1 = n/(r+1)$ elements, the result follows.
Formula Size Versus Depth

- If a formula for a function is represented by a balanced tree, the depth of the tree is logarithmic in its size. For such functions their depth is at most logarithmic in formula size.

- When a formula for a function is not represented by a balanced tree (the normal case), we use the separator theorem on trees to devise an algorithm that rebalances an unbalanced tree without increasing its size very much.
Formula Size Versus Depth

We use the following multiplexer function

\[ f_{\text{mux}}(a, y_0, y_1) = (a \land y_0 \lor a \land y_1) \]

and define

\[ d(\Omega) = \frac{D(f_{\text{mux}}) + 1}{\log_r (r+1)/r}. \]

Note that the value of \( D(f_{\text{mux}}) \) depends on the basis \( \Omega \).
Formula Size Versus Depth

**Theorem** Let $\Omega$ be a complete basis of fan-in $r$. Any $f : B^n \rightarrow B$ with formula size $L(f) \geq 2$ has depth $\log_r L(f) \leq D(f) \leq d(\Omega) \log_r L(f)$

**Proof** The lower bound is obvious. The upper bound follows from induction on formula size. For the base case $L(f) = 2$, consider all 16 functions with $n = 2$. 
Formula Size Versus Depth

Assume result holds for $L(f) \leq L_0 - 1$. Show it holds for $L(f) = L_0$. Let $T$ be such a tree. Find subtree $T_v$ with $L_0/(r+1) \leq |T_v| \leq rL_0/(r+1)$ leaves. Note that $rL_0/(r+1)) \leq L_0 - 1$. Let $T_0$ and $T_1$ be $T$ when $T_v$ is replaced by the constants 0 and 1, respectively. Use value of $T_v$ to select between values of these two trees using $f_{\text{mux}}$. Since $\left\lceil L/(r+1) \right\rceil + \left\lceil rL/(r+1) \right\rceil = L$, $T_0$ & $T_1$ have at most $L_0 - \left\lceil L_0/(r+1) \right\rceil \leq rL_0/(r+1) \leq L_0 - 1$ leaves. Thus, $T_0$, $T_1$, and $T_v$ each has at most $L_0 - 1$ leaves, which implies

$$D(f) \leq D(f_{\text{mux}}) + d(\Omega) \log_r (rL(f)/(r+1)) \leq d(\Omega) \log_r L(f)$$
Theorem Let $\Omega_a$ and $\Omega_b$ be two complete bases. Let $D_a(f)$ and $D_a(f)$ the circuit depth of $f$ over these two bases. Then there is a constant $e$ such that

$$L_a(f) \leq [L_b(f)]^e$$

where $L_a(f)$ and $L_b(f)$ are formula size of $f$ over these two bases.

Proof Invoke the above theorem and the fact that there is a constant $E$ such that $D_a(f) \leq E \times D_a(f)$. 