IITM-CS6840: Advanced Complexity Theory Mar 05, 2012

Lecture 34 : Boolean Circuit Model of Computation

Lecturer: Jayalal Sarma *Scribe: Rahul CS*

THEME: Modelling computation using Circuits, Gates and Basis functions & Emil Post's characterization (1941) of a complete basis for boolean circuits.

In this lecture, we discuss a new model for decision making problems. Consider the task of deciding whether a binary string is in the language or not. We can view this as feeding the string as input to a boolean circuit and viewing its output. Any decision problem has an equivalent family of boolean circuits, or could also be viewed as family of boolean functions.

$$\{f_n\}_{n\geq 0},\ s.t.\ f(x)_{|x|=n} = \chi_L(x)$$

Where $\chi_L(x)$ is the characteristic function for the language L. To decide a string x of length n, we select the boolean function f_n(representing boolean circuit that has n inputs and single output) and evaluate $f(x)_{|x|=n}$. Such a function always exists which exactly equals the truth table of all n length strings.

Definition 1. A boolean circuit is a Directed Acyclic graph. There exists a unique outdegree 0 vertex called root. This represents output of the circuit. It possibly contains indegree 0 vertices which represents input variables. If the circuit does not contain such vertices, then the graph represents constant boolean functions. Vertices with positive values for both indegree and outdegree represents logical gate labels. The direction of edge represents direction of flow of data.

Consider a set of boolean functions Ω. We say, this set forms the basis for the set of all boolean functions that can be obtained by composing functions from Ω. The set is minimal if none of the elements in the set could be obtained by composing the remaining elements in the set.

If all boolean functions can be computed by functions over Ω, then we say Ω forms a complete basis. For example, $\{\neg, \wedge, \vee\}$ forms a complete basis, since circuit for any boolean function can be implemented using these gates.

We can form several complete bases. Clearly, each function in one basis could be formed out of functions from any other basis.

Given a set of boolean functions, there should be a way to check whether the set is a complete basis or not. Of course if we have a standard complete basis in hand and if the set

under consideration contains elements that could be composed to form each of the elements in the complete basis, then it good enough to confirm that the set forms a complete basis. But this technique is not good enough to confirm that a set lacks in being a complete basis. In 1941 Emil Post came up with a way to characterize complete bases.

1 Characterizing Complete Bases

Post's theorem provides a way to characterize complete bases.

Before discussing the theorem, let us go through some relevant aspects.

1. Constant functions:Irrespective of input, output remains constant.

$$f(x_1, x_2, ..., x_n) = 0/1$$

2. Monotone Functions: We can define a partial order of the following kind among binary strings. Let $x, y \in \{0,1\}^n$. $x \leq y \leftrightarrow \forall_i\ x_i \leq y_i$, where subscript i represents i^{th} bit in the string. There are pairs of strings among which this relation is not defined. For example $\{001, 100\}$. A boolean function is monotone if $x \leq y \Rightarrow f(x) \leq f(y)$. In other words, if a bit in a string x changes from 0 to 1, and if $f(x)$ before the flip was 1, then $f(x)$ after the flip should also be 1.

   Consider a Directed acyclic graph G containing 2^n vertices representing all possible n length strings. There is an edge between two vertices if they differ by exactly one bit. And the direction of edge will be representing the $0 \rightarrow 1$ flip. We can assign values to vertices from the set $\{0,1\}$ such that value at vertex v is $f(v)$ where f is some boolean function. Clearly vertex 1^n has indegree n and outdegree 0 and 0^n has indegree 0 and outdegree n. The function f is monotone if, there does not exists a vertex u such that the sequence of values seen on the path from u to 1^n does not contain a $1 \rightarrow 0$ flip.

   $\wedge$ and $\vee$ are trivial monotone functions.

3. Self Dual Functions: A function f is self dual if $f(\overline{x_1}, \overline{x_2}, ..., \overline{x_n}) = \overline{f(x_1, x_2, ..., x_n)}$. For example negation($\neg$) is a self dual function. Another example is $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$.

4. Affine functions: A function $f(x_1, x_2, ..., x_n)$ is affine if for each x_i, either it always affects the truth value of f, or never affects.

$$f(x_1, x_2, ..., x_n) = \bigoplus_{\substack{i \in S \\ S \subseteq [n]}} x_i$$

   For example, parity over a subset of bits.

Theorem 1. *Consider,* $\Omega \subseteq \{f | f : \{0,1\}^n \rightarrow \{0,1\}\}$. Ω *forms a complete bases if,*

1. $\exists f \in \Omega$ *such that*, $f(0,0,...,0) = 1$
2. $\exists f \in \Omega$ *such that*, $f(1,1,...,1) = 0$
3. $\exists f \in \Omega$ *such that*, f *is not monotone.*
4. $\exists f \in \Omega$ *such that*, f *is not self dual.*
5. $\exists f \in \Omega$ *such that*, f *is not affine.*

The set $\{\wedge\}$ does not form a complete basis, as property 2 is violated. Whenever property 2 is violated, $f(1,1,...,1) = 1$ for all $f \in \Omega$. Ω fails to generate a function $f'(1,1,...,1) = 1$. $\{\neg, \wedge\}$ forms a complete basis as both constant functions could be generated and $\neg$ is not monotone, $\wedge$ is not self dual and $\wedge$ is not affine. Similarly, $\{\oplus, \neg\}$ is not a complete basis as property 5 violated.