Complexity Reading Group 10/1/2015

1 Circuit

- C_n n-input circuit
- DAG n sources and 1 sink
- All non sources labelled with $\wedge, \vee \neg$
- $|C|$ = number of vertices

2 Circuit Families

Different circuit depending on what n is in. Specifcally, have a function $T(n)$ that determines the size of the circuit. $\forall_n : |C_n| \leq T(n)$.

Definition 1: A language $\mathcal{L}$ is in $\textsc{Size}(T(n))$ if $\exists$: $T(n)$-sized circuit family s.t. $\forall_x \in \{0,1\}^n x \in \mathcal{L} \equiv C_n(x) = 1$.

Definition 2: P_{poly} is the class of languages decidable by polynomially sized circuit families:

$$P_{\text{poly}} = \cup_c \textsc{Size}(n^c)$$

Claim: $p \subseteq P_{\text{poly}} : \mathcal{L} \in P \to P_{\text{poly}}$, where $\mathcal{L}$ is a language, P is the complexity class.

wts: $\forall : T(n)$-time Turing Machines M¡ $\exists : \mathcal{O}(T(n))$ sized circuit fam:

$$\{C_n\}_{m \in \mathbb{N}} : C_n(x) = M(x), \forall_x : x \in \{0,1\}^n$$

Definition 3: Oblivious Turing Machine is a machine where head movements depend on $|x|$ but not on contents of x.

2.1 Proof about circuit family relation to TM

Intuition: the class of languages decidable by polynomial sized circuit families is a superset of P (polynomial time TMs).

Lemma 1: Given a TM M that decides L in $t(n)$ time $\exists$ oblivious TM M' that decides L in $\mathcal{O}(t(n)^2)$ time, (and uses 2 tapes).

Proof: For any input $x \in \{0,1\}^n$, define transcript of M's execution to be: $z_1, \ldots, z_{T(n)}$, where z_i denotes what's happening at step i:

- input read by each head
- current state of the TM (constant number of states)

Note: z_i depends on $z_{i-1}, z_{i_1}, z_{i_2}$, where z_{i_n} is the last time step where head h was at the same position it's at in step i.

$\therefore \exists$: a constant sized circuit C_i representing z_i's dependance on $z_{i-1}, z_{i_1}, z_{i_2}$.

Now, chain together the C_i's for $i = 1, \ldots, T(n)$.

This creates a circuit of size $\mathcal{O}(T(n))$.

Add a constant number of additional gates to determine if we're in an accept state. $\square$

3 Uniform vs. Non-Uniform Circuits

$\textsc{Halt} = \{1^n \mid n$ encodes TM, input pairs $\langle M, x\rangle : M$ halts on x$\}$

Non-uniform circuit families contain the language $\textsc{Halt}$.

Definition 4: A uniform circuit is one where the circuits can be constructed by a poly-time TM. This defines the class P-uniform.

Some other results:

1. L can be decided by a P-uniform circuit family $\equiv L \subseteq P$
2. $P_{\text{poly}} = P+$ "advice"

Definition 5: Class of language decidable by $T(n)$ TM's equiv with $a(n)$ advice $\textsc{Dtime}(T(n))/a(n)$

Claim: $P_{\text{poly}} = \cup_{c,d} \frac{\textsc{Dtime}(n^c)}{n^d}$

Proof:

First direction ($\rightarrow$): $L \in P_{\text{poly}}$: let α_n be description of C_n

Second direction ($\leftarrow$): $\exists : M(x, \alpha_n)$, hard code α_n, use same transformation as $P \subseteq P_{\text{poly}}$ proof.

3.1 Karp, Lipton Theorem '80

Theorem 2: $NP \subseteq P_{\text{poly}} \rightarrow PH = \Sigma_2^P$

4 Polynomial Hierarchy

Definition 6: For $i \geq 1$, $L \in \Sigma_i^P$ if $\exists$ poly-time TM, M, and a polynomial q, s.t.:

$$x \in L \equiv \exists_{u_1} : u_1 \in \{0,1\}^{q(|x|)} \forall_{u_2} : u_2 \in \{0,1\}^{q(|x|)} \dots Q_i u_i \in \{0,1\}^{q(|x|)}$$

Where $Q_i = \begin{cases} \forall & i = 0 \mod 2 \\ \exists & i = 1 \mod 2 \end{cases}$

$$\text{Polynomial Hierarchy}(PH) = \cup_i \Sigma_i^P$$
$$\Pi_i^P = co\Sigma_i^P = \{\bar{L} : L \in \Sigma_i^P\}$$

$$coNP = \Pi_i^P$$
$$NP = \Sigma_i^P$$

So:

$$\Sigma_i^P \subseteq \Pi_{i+1}^P \subseteq \Sigma_{i+2}^P \rightarrow PH = \cup_i \Pi_i^P$$

5 In Summary:

Circuits: Covered 6.1, 6.2, 6.3 of the book.

Polynomial Hierarchy: 5.2.