CSE596 — Lecture Wed Oct 24 — Fall 2018

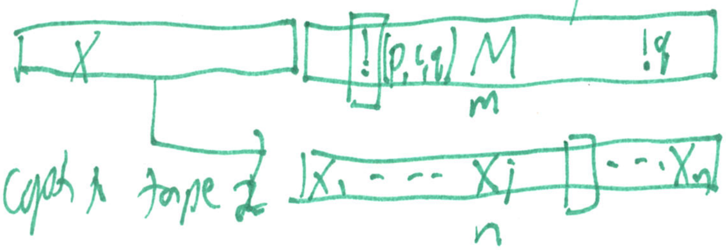
1) $A_{DFA} = \{\langle M, x\rangle : M$ is a DFA and M accepts $x\}$

Decidable — in P: just run $M(x)$. $n = |x|$, $m = |\langle M\rangle| \approx \|Q\|$

Time: $O(n \cdot m)$ if the code of M has to be accessed linearly. Ignore difference between m and $\tilde{O}(m) = O(m \text{ polylog } m)$.

$x = x_1 \cdots x_n$

Can argue time $O(n \log m)$ on a random-access model.



Even on a TM, both $m, n \le N = |\langle M, x\rangle|$ so $m \cdot n = O(N^2)$: quadratic time.

2) $A_{NFA} = \{\langle N, x\rangle : N$ is an NFA and N accepts $x\}$. Decidable:

- Debray (p58) says: Convert N to DFA M and run as for $\langle M, x\rangle \overset{?}{\in} A_{DFA}$.
  Flaw: this approach can use $\exp(N)$ time. Time $\approx n \cdot \exp(m)$
- Maintain for $i = 0, \dots, n = |x|$ the sets S_i of up to m states that N can possibly process $x_1 \cdots x_i$ to. Then $x \in L(N) \iff S_n \cap F \neq \emptyset$

Time: $\approx (n$ bits of $x) \times ($update up to m entries of S_{i-1} to $S_i) \approx \tilde{O}(mn)$ time given random access. Direct TM time: $\tilde{O}(N^3)$ — ? $\boxed{\text{In P.}}$

3) $E_{DFA} = \{M : M$ is a DFA and $L(M) = \emptyset\}$

$NE_{DFA} = \{M : M$ is a DFA and $L(M) \neq \emptyset\}$ $NE_{NFA} = \{N : N$ is an NFA and $L(N) \neq \emptyset\}$.

$\iff$ there is a path from s to some state $f \in F$. Whatever string x is processed by the path belongs to the language.

In P by breadth-first search (BFS) in the graph of M or N.

$E_{DFA} = \sim NE_{DFA}$ so is in P too.

4) $ALL_{DFA} = \{\langle M\rangle : M$ is a DFA and $L(M) = \Sigma^*\}$ $\neq \sim E_{DFA}$! 13

Algorithm: Complement M to M' s.t. $L(M') = \sim L(M)$. $O(n)$ time: change F to $Q \setminus F$.

Then $L(M) = \Sigma^* \iff L(M') = \emptyset \iff \langle M'\rangle \in E_{DFA} \iff \langle M'\rangle \notin NE_{DFA}$.

This gives a $\leq_m^p$ reduction from ALL_{DFA} to $E_{DFA} \in P$, so $ALL_{DFA} \in P$.

5) $ALL_{NFA} = \{\langle N\rangle : N$ is an NFA and $L(N) = \Sigma^*\}$. E_{NFA} is in P. Is ALL_{NFA}?

Shock: Not even known to belong to NP or to co-NP!

Complement $\widetilde{ALL}_{NFA} = \{\langle N\rangle : L(N) \neq \Sigma^*\}$ is NP-hard.

6) "$ALLSHORT_{NFA}$" $= \{\langle N, K\rangle : K \leq m \equiv \|Q_N\|$ and $\{0,1\}^K \subseteq L(N)\}$.

i.e. N accepts all strings of "short" length K.

If the answer is no, then we can guess a bad $x \in \{0,1\}^K$ and verify that $\langle N, x\rangle \notin A_{NFA}$ using our poly-time routine for A_{NFA}.

[But if yes, we might have to try 2^K different x-es.]

///

$\widetilde{ALLSHORT}_{NFA} \in NP$

$ALLSHORT_{NFA} \in$ co-NP.

The second shock with ALL_{NFA} is that the shortest $x \notin L(N)$ can have length exponential in the number on of states of N! Too long for x to be an "NP witness" for the complementary language.

(7) SAT = { Boolean formulas ϕ using $\wedge, \vee, \neg$ and variables $x_1, \dots, x_n$, such that *some* truth assignment $a_1 \cdots a_n \in \{0,1\}^n$ makes $\phi(a) = \text{true}$ }.

$$= \{ \langle \phi \rangle : (\exists a : |a| = n \leq |\phi|) \underbrace{[\phi(a) = \text{true}]}_{\text{in } O(n^2)^* \text{ time, actually } \tilde{O}(n) \text{ with random access.}} \}.$$

$(\exists^{\text{linear}} a)$

$\therefore$ SAT $\in$ NP.

$$\text{TAUT} = \{ \phi(x_1 \cdots x_n) : \phi \text{ is a tautology, i.e. } (\forall a \in \{0,1\}^n)\ \phi(a) = \text{true} \}.$$

$$\text{TAUT} = \{ \langle \phi \rangle : \neg\phi \notin \text{SAT} \} \approx \widetilde{\text{SAT}}, \text{ in } \underline{\text{co-NP}}.$$

We will in particular be concerned with formulas ϕ that are conjunctions

$$\phi = C_1 \wedge C_2 \wedge \dots \wedge C_m$$

of *clauses*, each of which is a disjunction of up to k *literals*. A literal means a variable x_i or its negation $\bar{x}_i$. A typical clause:

$$C = (x_1 \vee \bar{x}_3 \vee x_6),$$

with $k=3$ literals. This is called *k-conjunctive normal form* (*k-CNF*).

$N = |\langle \phi \rangle|$

In 3CNF, when each variable appears at most a fixed number of times, N is linear in the # of variables.

*Footnote: Debray's notes for Theorem 13.11 on page 43 give $O(n^2)$ time for 3SAT but for the wrong reason. The 3CNF form is easily checkable in one pass in $O(N)$ time. The evaluation is trickier only because one needs to make sure the assignment consistently gives the same value to the same variable. But the formula can *wlog.* be laid out to make that easy, so we can say both SAT and 3SAT belong to $\underline{\text{NLIN}} =_{\text{def}} \text{NTIME}[O(N)]$.