

## 6.1400 Cheat Sheet (Computability & Complexity)

Gaten Culp (gculp@mit.edu) · 2025-05-21

### 1 Legend

Monospace = Turing Machines  
Sans-serif = Languages  
CAPS = Language Classes

## 2 Regular Languages

Closure under:

$$A \cup B, A \cap B, A^R, A^*, \neg A, A \cdot B, A - B = A \cap (\neg B)$$

Order of Operations:  $* \rightarrow \cdot \rightarrow +$

### 3 DFA

$$\text{DFA} = (Q, \Sigma, \delta, q_0, F)$$

#### 3.1 DFA → MinDFA

##### 3.1.1 Defining MinDFA and Ideas

Note: The minimum DFA is unique

A MinDFA requires (1) no indistinguishable states, (2) no unreachable states

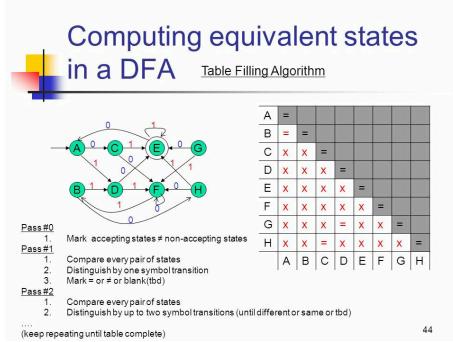
$M_p := M$  but starting on state  $P$

$w \in \Sigma^*$  distinguishes states  $p, q$   
 $\Rightarrow M_p$  and  $M_q$  have different outputs on  $w$

$p \sim q :=$  states  $p, q$  are distinguishable  
 $\Leftrightarrow \exists w$  distinguishing  $p, q$

Distinguishable states form a partition of equivalence on  $Q$ . These can be simplified after removing unreachable states.

##### 3.1.2 Table-Filling Algorithm (DFA → MinDFA)



## 4 NFA

$$\text{NFA} = (Q, \Sigma, \delta, Q_0, F)$$

#### 4.1 NFA → DFA

Create a table with  $n + 1$  columns – one for the DFA state and one for each of  $n$  transitions. List out the transitions in each column. Add rows for each new possible set of states reachable.

State	a	B
$q_0$	$\{q_0, q_1\}$	$q_0$
$\{q_0, q_1\}$	$\{q_0, q_1\}$	$\{q_0, q_2\}$
$\{q_0, q_2\}$	$\{q_0, q_1\}$	$q_0$

- Note: No bijection between  $\{1, \dots, n\}$  and  $\overbrace{\text{powerset}}^{2^{\{1, \dots, n\}}}$

#### 4.2 NFA → GNFA → RegExp

1 if |states| = 2:

2 || return  $R(q_{\text{start}}, q_{\text{acc}})$

3  $G' \leftarrow G.\text{copy}()$

4 pick  $q_{\text{rip}} \in (Q - \{q_{\text{start}}, q_{\text{acc}}\})$

5  $Q' \leftarrow Q \setminus q_{\text{rip}}$

6  $\forall q_i, q_j \in (Q' \setminus q_{\text{acc}}, Q' \setminus q_{\text{start}}):$

$$7 \quad R'(q_i, q_j) \leftarrow \begin{cases} R(q_i, q_{\text{rip}}) \cdot R(q_{\text{rip}}, q_{\text{rip}})^* \cdot R(q_{\text{rip}}, q_j) \\ \text{Self-loops} \\ + R(q_i, q_j) \end{cases}$$

8 Repeat from the top

## 5 Streaming Algorithms

- Initialize vars and their assignments on vars
- When next symbol =  $\sigma$ :
- || Run pseudocode for  $\sigma$
- Accept/reject based on vars

## 6 Myhill-Nerode Theorem

$$\forall L \in \text{Langs} : \text{either}$$

|| DFA recognizing  $L$

There are infinite strings to  
trick DFA attempting to recognize  $L$

i.e: equiv classes of  $\overline{\overline{L}}$  is finite  $\Leftrightarrow L$  is regular

### 6.1 Distinguishing Set

Strings  $w_1, \dots, w_n, \dots$  s.t.  $\forall i \neq j :$   
possibly infinite  
 $\exists z \text{ s.t. } (w_i z \in L) \text{ xor } (w_j z \in L)$

Ex: For  $L = \{0^n \mid n \geq 0\}$

take  $S = \{0, 00, \dots, 0^n, \dots\}$  where  $z = 1^i$

Then  $\forall w_i, w_j \in S : [(0^i 1^i) \in L] \wedge [(0^j 0^j) \notin L]$

### 6.2 Streaming Distinguisher

Streaming Distinguisher  $D_n$ : Distinguishing set when limiting the concatenated strings to length  $n$ .

$$\begin{aligned} &(\forall \text{ distinct } x, y \in D_n)(\exists \text{ word } z) \\ &(xz \in L) \text{ xor } (yz \in L) \\ &\wedge (|xz|, |yz| \leq n) \end{aligned}$$

If  $\forall n, \exists D_n$  s.t.  $|D_n| \geq 2^{S(n)}$

then all streaming alg must also use  $\geq s(n)$

## 7 Communication Complexity

### 7.1 Protocol

$$A, B : \Sigma^* \times (\Sigma^* \cup \text{STOP})$$

Which collectively compute  $f$

If  $\exists$  streaming alg using  $\leq S(m)$  space on  $2m$  inputs then:

$$cc(f) \leq O(s(m))$$

### 7.2 Switcheroo Lemma

$(x, y)$  and  $(x', y')$  share comms pattern  $P$ ,  
then so do  $(x, y')$  and  $(x', y)$

#### 7.2.1 Example: ALICE-HAS-MORE Lower Bound

For ALICE-HAS-MORE( $A, B$ ), create set  $S = ((1^{i+1}0^{n-i-1}, 1^i0^{n-i}) : 0 \leq i \leq n - 1)$ .

All pairs in  $S$  have ALICE-HAS-MORE = 1.

If protocol uses  $< \log_2 n$  bits, by pigeonhole, two pairs share same pattern:  $(1^{i+1}0^{n-i-1}, 1^i0^{n-i})$  and  $(1^{j+1}0^{n-j-1}, 1^j0^{n-j})$ .

By switcheroo:  $(1^{i+1}0^{n-i-1}, 1^j0^{n-j})$  and  $(1^{j+1}0^{n-j-1}, 1^i0^{n-i})$  also share same pattern.

This implies  $i + 1 > j$  and  $j + 1 > i$ , contradiction when  $i \neq j$ .

## 8 Turing Machines

$$(M \in \text{TM}s) = (Q, \Sigma, \Gamma, \delta, q_o, q_{\text{acc}}, q_{\text{ref}})$$

(1) Read  $\sigma$  (2) Write  $\sigma$  (3) Move left/right (4) Change states

## 9 Equivalence Classes

$$\begin{aligned} (x \underset{L}{\equiv} y) &:= (\forall z \in \Sigma^*) (xz \in L \Leftrightarrow yz \in L) \\ &\Leftrightarrow x, y \text{ are } L \text{ equivalent} \\ &\Leftrightarrow x, y \text{ are distinguishable to } L \end{aligned}$$

This is similar to equivalence relation of DFA states. "Further transitions are identical."

Note: Equivalence classes require (1) Symmetric, (2) Transitive, (3) Reflexive

### 9.1 Under TMs

$$\Delta_x : \Sigma^x \rightarrow Q$$

:= State you end up in after reading a string

$$\begin{aligned} x \underset{M}{\approx} y &\Leftrightarrow \Delta(x) = \Delta(y) \\ &\Leftrightarrow x \underset{L}{\equiv} y \\ &\Leftrightarrow x \text{ and } y \text{ are distinguishable strings under } M \end{aligned}$$

Where I'm pretty sure  $M$  is the machine recognizing  $L$

## 10 Formal Systems & Their Limits

### Formal system $F$

• finite language, notion of proof, notion of truth

"Interesting" iff

- Expressive – each TM-input pair  $(M, w)$  maps (computably) to a sentence  $S_{M,w}$  with  $S_{M,w}$  true  $\Rightarrow M$  accepts  $w$ .
- Checkable – the set  $\{(S, P) \mid P \text{ is a proof of } S \text{ in } F\}$  is decidable.
- Halting-decide – if  $M$  halts on  $w$ , then  $F$  proves either  $S_{M,w}$  or  $\neg S_{M,w}$ .

Consistency – no statement  $S$  with both  $S$  and  $\neg S$  provable.

Completeness – every statement  $S$  has either  $S$  or  $\neg S$  provable.

### Limit theorems

- Gödel (1931): any consistent, interesting  $F$  is incomplete (true but unprovable statements exist).
- Gödel (1931):  $F$  cannot prove its own consistency.
- Church-Turing (1936): deciding whether a sentence of  $F$  has a proof is undecidable.

## 11 Recursion Theorem

WLOG, a program can reference its own code

$$\forall t : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$$

(Write  $t$  as if it already has recursion)

$$\exists R : \Sigma^* \rightarrow \Sigma^* \text{ s.t. } \forall R(w) = t(\langle R \rangle, w)$$

## 12 Turing Machine Minimization

(UNDECIDABLE)

Where  $M$  ∈ TMs :

Minimal( $\langle M \rangle$ )  $\Leftrightarrow M$  is a minimal state TM

### 13 Fixed Point Theorem

If  $t : \Sigma^* \rightarrow \Sigma^*$  is computable:

$\exists F \in \text{TMs}$  s.t.

$t(\langle F \rangle)$  outputs  $\langle G \rangle$  where  $L(F) = L(G)$

ie: We can make a copy that is behaviorally identical to the input for any string-to-string function  $t$ .

## 14 Rice's Theorem

"Program analysis is hard"

let  $P :=$  Property

$$: \text{TMs} \rightarrow \{0, 1\}$$

$\wedge P$  is Non-Trivial (Not all acc/rej)

$\wedge P$  is Semantic ( $L(M) = L(M') \Rightarrow P(M) = P(M')$ )

then  $\{\langle M \rangle \mid P(M) = 1\} \in \text{UNDECIDABLE}$

### 15 Decidable Predicates

$$R \in \text{Predicates}, M \in \text{TMs}$$

$R(x, y)$  is True  $\Leftrightarrow M(x, y)$  accepts

Vaguely:

NM<sub>s</sub> = RECOGNIZABLE

TMs = DECIDABLE.

## 16 Computational Complexity

$T(n) :=$  Time complexity of  $M \in \text{TMs}$

on strings up to length  $n$

$\text{TIME}(t(n)) := \{L \mid L \text{ has time complexity } O(t(n))\}$

$\text{NTIME}(t(n)) := \{L \mid L \text{ is decided by } O(t(n)) \text{ time complexity NTM}\}$

$P :=$  Poly Time =  $\bigcup_{k \in \mathbb{N}} \text{TIME}(n^k)$

$NP :=$  Non-Deterministic Poly Time =  $\bigcup_{k \in \mathbb{N}} \text{NTIME}(n^k)$

## 17 Universal Turing Machines

$(U \in \text{UTMs}) =$  Universal TM

$U : \text{Code} \times \text{Input} \rightarrow \text{Output}$

$U$  on  $(\text{tm}, x)$ , accept if  $(M \text{ accepts } x)$  else reject

(A) Input tape, (B) State Tape, (C) Code Tape, (D) Simulation Tape

## 18 Time Hierarchy Theorem

"You can solve strictly more problems /w more time"

$$\text{if } g(n) > n^2 f(n)^2$$

then  $\text{TIME}(f(n)) \subset \text{TIME}(g(n))$

## 19 Extended Church Turing Thesis

All intuitions about efficient algs = Poly-time TMs

### 20 Mapping Reduction

$$A \leq_m B := (\exists f : \Sigma^* \rightarrow E^*)$$

s.t.  $w \in A \Leftrightarrow f(w) \in B$

### 20.1 Poly-Time Reduction $\leq_p$

Same as mapping reduce, but in poly-time (uses partial order)

## 21 NP-HARD and NP-COMPLETE

NP-HARD :=  $\{L \mid \forall A \in \text{NP}, A \leq_p L\}$

NP-COMPLETE :=  $\{L \mid L \in \text{NP} \wedge L \in \text{NP-HARD} \text{ ie: not EXPTIME or smthn}\}$

## 22 Non-Deterministic TMs (NTMs)

- May proceed according to several possible transitions
- Accepts if there is any accepting condition

## 23 Verifier Characterization of NP

$$L \in \text{NP}$$

$$\Leftrightarrow$$

$$\exists k \in \mathbb{R}, V(x, y) \in \{\text{Poly-time predicates}\} \text{ s.t.}$$

$$L = \{x \mid \exists y \in \Sigma^* [V(y) \leq k|x|^k \wedge V(x, y)]\}$$

ie: Guess and check with some poly-time verifier

something something

$V$  ran in poly( $n$ ) time  $\Leftrightarrow L \in \text{TIME}(2^{O(k^n)} \cdot \text{poly}(n))$

## 24 Oracles

$X^Y := \text{Problems solvable using any TM in } X \text{ with an oracle for the language } Y$   
(or selecting any oracle from  $Y$ )

## 25 BPP & Error-Reduction

$$\text{BPP} := \left\{ L \mid L \text{ is decided by a poly-time probabilistic TM with error } \leq \frac{1}{3} \right\}$$

Any constant  $< \frac{1}{2}$  works: once the error is bounded away from  $\frac{1}{2}$  by  $\frac{1}{\text{poly}(n)}$  we can amplify.

**Error-reduction lemma** Let  $\varepsilon \in (0, \frac{1}{2})$  and  $k \in \mathbb{N}$ . If machine  $M_1$  runs in  $t(n)$  and

$$\Pr(M_1(x) \neq L(x)) \leq \frac{1}{2} - \varepsilon,$$

there exists  $M_2$  with

$$\Pr(M_2(x) \neq L(x)) < \frac{1}{2^{n^k}},$$

$$\text{time}(M_2) = O\left(n^k \cdot \frac{t(n)}{\varepsilon^2}\right).$$

Construction: run  $M_1$  independently  $m := \Theta(\frac{n^k}{\varepsilon^2})$  times and output the majority vote.

**Chernoff bound** (additive form) For independent  $\frac{0}{1} X_i$ , let  $X = \sum_i X_i$ ,  $\mu = E[X]$ :

$$\Pr(X < (1 - \delta)\mu) \leq \exp\left(-\delta^2 \frac{\mu}{2}\right).$$

With  $X_i = 1$  iff  $M_1$  is correct  $\Rightarrow \mu \geq (\frac{1}{2} + \varepsilon)m$ . Choose  $\delta = 2\frac{\varepsilon}{1+2\varepsilon}$  to obtain

$$\Pr(\text{majority wrong}) \leq \exp(-2\varepsilon^2 m)$$

$$< 2^{-\varepsilon^2 \frac{m}{2}}.$$

Setting  $m = 10^{\frac{n^k}{\varepsilon^2}}$  yields error  $< 2^{-n^k}$ .

A *monotone clause* in a CNF formula is a clause consisting of all positive literals or all negative literals. For example,  $(x_1 \vee x_2 \vee x_3)$  and  $(\neg x_1 \vee \neg x_2 \vee \neg x_3)$  are monotone clauses, but  $(x_1 \vee \neg x_2 \vee \neg x_3)$  is not. The *clause-monotone SAT problem* is to decide the satisfiability of a CNF formula that consists only of monotone clauses.

Prove that the clause-monotone problem is NP-complete.

The clause-monotone SAT problem is clearly in NP, so it remains to prove that it is NP-hard. We reduce from 3SAT as follows:

Let  $\phi = C_1 \wedge \dots \wedge C_m$  be a 3CNF formula on variables  $x_1, \dots, x_n$ .

We introduce a new variable  $y_i$  for each  $x_i$ . For each  $C_i = (l_1 \vee l_2 \vee l_3)$ , we let the clause  $D_i$  be  $(m_1 \vee m_2 \vee m_3)$ , where  $m_i = x_j$  if  $l_i = x_j$ , and  $m_i = y_j$  if  $l_i = \neg x_j$ .

Take  $\phi' = D_1 \wedge \dots \wedge D_m \wedge (x_1 \vee y_1) \wedge (\neg x_1 \vee \neg y_1) \wedge \dots \wedge (x_n \vee y_n) \wedge (\neg x_n \vee \neg y_n)$ .

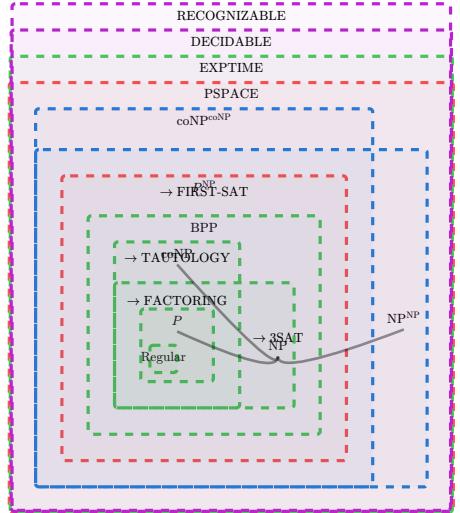
$\phi \mapsto \phi'$  is a computable in polynomial time.

Note that any satisfying assignment for  $\phi'$  is also a satisfying assignment for  $\phi$ , and that any satisfying assignment for  $\phi$  can be extended to a satisfying assignment for  $\phi'$  by setting  $y_i = \neg x_i$ . In particular,  $\phi$  is satisfiable iff  $\phi'$  is satisfiable.

## 26 Problems

PRIMES := $\{n \mid n \text{ is prime}\}$ in P	SAT := $\{\phi \mid \phi \text{ is a satisfiable boolean formula}\}$ in NP-COMPLETE
PATH := $\{(G, s, t) \mid \text{Graph } G \text{ has a path from } s \text{ to } t\}$ in P	3SAT := $\{\phi \mid \phi \text{ is a satisfiable 3-CNF formula}\}$ in NP-COMPLETE
HALT := $\{(Tm(M), w) \mid M \text{ halts on input } w\}$ in RECOGNIZABLE but UNDECIDABLE	CIRCUIT-SAT := $\{C \mid \text{Boolean circuit } C \text{ is satisfiable}\}$ in NP-HARD
NHALT := $\{(Tm(M), w) \mid M \text{ does not halt on input } w\}$ in UNRECOGNIZABLE	MAX-CLIQUE := $\{(G, k) \mid \text{Max clique size in graph } G \text{ is exactly } k\}$ in PNP
CLIQUE := $\{(G, k) \mid \text{Graph } G \text{ has a clique of size } \geq k\}$ in NP-COMPLETE	IS := $\{(G, k) \mid \text{Graph } G \text{ has an independent set of size } \geq k\}$ in NP-COMPLETE
VERTEX-COVER := $\{(G, k) \mid \text{Graph } G \text{ has a vertex cover of size } \leq k\}$ in NP-COMPLETE	SUBSET-SUM := $\{(S, t) \mid \exists S' \subset S \text{ s.t. } \sum_{x \in S'} x = t\}$ in NP-COMPLETE
	KNAPSACK := $\{(I, v, w, W, V) \mid \text{Item set } I \text{ with values } v \text{ and weights } w\}$ has subset with weight $\leq W$ and value $\geq V$ in NP-COMPLETE
	HOM := $\{(G, H) \mid \text{Exists homomorphism from graph } G \text{ to graph } H\}$ in NP-COMPLETE
	HOM-EDGE := $\{(G, H) \mid \text{Exists edge-preserving homomorphism from } G \text{ to } H\}$ in P
	PARTITION := $\{S \mid \exists S' \subset S \text{ s.t. } \sum_{x \in S'} x = \sum_{x \in S - S'} x\}$ in NP-COMPLETE
	BIN-PACKING := $\{(S, k, B) \mid \text{Items } S \text{ can fit in } k \text{ bins of capacity } B\}$ in NP-COMPLETE
	SHORTEST-PATH := $\{(G, s, t, k) \mid \text{Graph } G \text{ has path from } s \text{ to } t \text{ of length } \leq k\}$ in P
	LONGEST-PATH := $\{(G, s, t, k) \mid \text{Graph } G \text{ has path from } s \text{ to } t \text{ of length } \geq k\}$ in NP-COMPLETE
	HAM-PATH := $\{(G, s, t) \mid \text{Graph } G \text{ has Hamiltonian path from } s \text{ to } t\}$ in NP-COMPLETE
	NO-HAMPATH := $\{(G, s, t) \mid \text{Graph } G \text{ has no Hamiltonian path from } s \text{ to } t\}$ in coNP-COMPLETE
	HAM-CYCLE := $\{G \mid \text{Graph } G \text{ has a Hamiltonian cycle}\}$ in NP-COMPLETE
	LOW-WEIGHT-2SAT := $\{(\phi, k) \mid 2\text{-CNF formula } \phi \text{ has satisfying assignment with } \leq k \text{ true variables}\}$ in NP-COMPLETE
	MIN-WEIGHT-2SAT := $\{(\phi, k) \mid \text{Min weight of satisfying assignment for 2-CNF formula } \phi \text{ is } k\}$ in PNP
	+1-LI := $\{(A, b) \mid \text{System } Ax = b \text{ has a solution with entries in } \{-1, 0, 1\}\}$ in NP-COMPLETE
	TAUT = TAUTOLOGY := $\{\phi \mid \phi \text{ is a tautology}\}$ in coNP-COMPLETE
	UNSAT := $\{\phi \mid \phi \text{ is unsatisfiable}\}$ in coNP-COMPLETE
	FACTORING := $\{(n, k) \mid n \text{ has a non-trivial factor } \leq k\}$ in NP $\cap$ coNP
	FIRST-SAT := $\{\phi \mid \text{First assignment in lex order satisfies } \phi\}$ in P $\cap$ NP-COMPLETE
	MIN-FORMULA := $\{(\phi, k) \mid \phi \text{ has equivalent formula of size } \leq k\}$ in coNP $\cap$ NP-COMPLETE
	MIN-CNF := $\{(\phi, k) \mid \phi \text{ has equivalent CNF formula of size } \leq k\}$ in coNP $\cap$ NP-COMPLETE
	TQBF := $\{\phi \mid \text{Quantified boolean formula } \phi \text{ is true}\}$ in PSPACE-COMPLETE
	GG := $\{\text{Generalized Geography game}\}$ in PSPACE-COMPLETE
	FG := $\{\text{Formula Game}\}$ in PSPACE-COMPLETE
	NEQUIV := $\{(M_1, M_2) \mid M_1 \neq M_2\}$ in NP-COMPLETE
	EQUIV := $\{(M_1, M_2) \mid M_1 = M_2\}$ in coNP-COMPLETE
	A. $\{\text{DFA}\}$ := $\{(M) \mid M \text{ is a DFA that accepts some string}\}$ in DECIDABLE
	A. $\{\text{NFA}\}$ := $\{(M) \mid M \text{ is an NFA that accepts some string}\}$ in DECIDABLE
	EQ. $\{\text{DFA}\}$ := $\{(M_1, M_2) \mid M_1, M_2 \text{ are DFAs and } M_1 = M_2\}$ in DECIDABLE
	EQ. $\{\text{NFA}\}$ := $\{(M_1, M_2) \mid M_1, M_2 \text{ are NFAs and } M_1 = M_2\}$ in DECIDABLE
	A. $\{\text{TM}\}$ := $\{(M) \mid M \text{ is a TM that accepts some string}\}$ in RECOGNIZABLE but UNDECIDABLE
	HALT. $\{\text{TM}\}$ := $\{(M) \mid M \text{ is a TM that halts on some input}\}$ in RECOGNIZABLE
	EMPTY. $\{\text{TM}\}$ := $\{(M) \mid M \text{ is a TM and } M = \{\}\}$ in UNRECOGNIZABLE
	EQ. $\{\text{TM}\}$ := $\{(M_1, M_2) \mid M_1, M_2 \text{ are TMs and } M_1 = M_2\}$ in UNRECOGNIZABLE

## 27 Complexity Classes



Let  $\text{EMPTY}_{TM} = \{(M) \mid M \text{ is a Turing machine and } L(M) \text{ is empty}\}$ .

(a) Prove that  $\text{EMPTY}_{TM}$  is decidable with  $A_{TM}$ : that is, there is a Turing reduction from  $\text{EMPTY}_{TM}$  to  $A_{TM}$ .

**PROOF:** First, we give a decider for  $\text{EMPTY}_{TM}$  using an oracle for  $A_{TM}$ :

Let  $M$  be a given TM. Let  $M'$  be the following TM:  
“On input  $x$ , for all pairs  $(y, z)$  in  $\text{lex order}$ , do:  
If  $M$  reaches an accept state on  $y$  in at most  $|z|$  steps, then accept.”

Why does this work? Observe that  $L(M) \neq \emptyset$  if and only if there is some input  $y$  and some  $t$  such that, if  $M$  is run on  $y$  for  $t$  steps, then  $M$  accepts. This condition is true if and only if  $M'$  accepts  $\varepsilon$  (by definition of  $M'$ ). And that is true if and only if  $(M', \varepsilon) \in A_{TM}$ . So the above decides correctly if  $L(M) \neq \emptyset$  or not.  $\square$

(b) Prove that there is no mapping reduction from  $\text{EMPTY}_{TM}$  to  $A_{TM}$ .

**PROOF:** If there were such a reduction, then  $\text{EMPTY}_{TM}$  would be recognizable because  $A_{TM}$  is recognizable. However, the complement of  $\text{EMPTY}_{TM}$  is also recognizable, because it can be written in the form:

$$(M \mid \exists y(\exists t)[M \text{ reaches an accept state on input } y \text{ in at most } t \text{ steps}]),$$

where the [...] is a decidable predicate. That would mean  $\text{EMPTY}_{TM}$  is decidable, which we have shown is not true in lecture. (You could also prove it's undecidable by Rice's theorem.)  $\square$

(a) Let  $M$  be a deterministic Turing machine that, on inputs of length  $n$ , uses space  $O(n^2)$ . Then for every input  $x$ , and every configuration  $C$  of the computation of  $M$  on input  $x$ ,  $K(C) \leq O(|x|)$  where  $K$  is Kolmogorov complexity and  $|x|$  is the length of  $x$ .

The claim is false.

**PROOF:** Let  $M$  be the following TM:

On input  $x$ :

Count to  $2^{|x|^2}$  (in binary).

Reject.

First note that for any word  $w$  and any prefix  $v$  of  $w$ ,  $K(v) \in O(K(w) + \log |v|)$ . Now let  $w$  be a string of length  $|x|^2 - 1$ . Since  $w$  is a prefix of some configuration  $C$  of  $M$  on input  $|x|$ ,  $K(w) \in O(K(C) + \log |x|)$ . There exist incompressible strings of every length, so there is some configuration  $C$  such that  $K(C) \in \Omega(|x|^2)$ .  $\square$

(b) Let  $M$  be a deterministic Turing machine that, on inputs of length  $n$ , uses space  $O(n^2)$  and time  $O(n^3)$ . Then for every input  $x$ , and every configuration  $C$  of the computation of  $M$  on input  $x$ ,  $K(C) \leq O(|x|)$ , where  $K$  is Kolmogorov complexity and  $|x|$  is the length of  $x$ .

The claim is true.

**PROOF:** Let  $M'$  be the following TM:

On input  $M, x, i$ :

Simulate  $M$  on input  $x$  for  $i$  steps.

Output the simulated configuration of  $M$ .

Let  $C$  be a configuration of  $M$  on input  $x$ . Then since  $M$  takes time  $O(n^3)$ ,  $C$  is the  $i$ th configuration for some  $i$  represented by a binary string of length  $O(\log |x|)$ . Then since  $|M|$  and  $|M'|$  are fixed,  $(M', (M, x, i))$  is a representation of  $C$  of length  $O(|x|)$ .  $\square$

## 28 Complexity/Computability Relationships

Given five languages with these properties:

$A$	: in P
$B$	: in NP
$C$	: is NP-complete
$D$	: is decidable
$E$	: is recognizable but not decidable

Determining whether the following reductions are ALWAYS, MAYBE, or NEVER true:

$$E \leq D : \text{NEVER true}$$

$$B \leq C : \text{ALWAYS true}$$

$$A \leq B : \text{MAY BE true}$$

$$B \leq_p C : \text{MAY BE true}$$

$$D \leq_m C : \text{ALWAYS true}$$