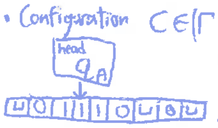
Definitions

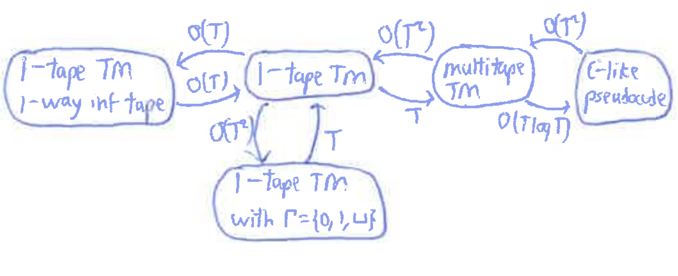
- alphabet Σ = finite nonempty set of symbols
- string over Σ = any finite sequence of symbols
- x: string, $|x|$ = length of string
- ε = empty string = string of length 0
- Σ^n = strings over Σ with exactly length n
- $\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \ldots = \bigcup_{i=0}^{\infty} \Sigma^i$
- $\langle X \rangle_\Sigma$ = encoding of math object X as a string in Σ^*, if Σ not specified then $\Sigma = \{0,1\}$.
  Reasonable encodings are
  ① injective, $X \neq Y \Rightarrow \langle X \rangle \neq \langle Y \rangle$
  ② data structure storing $X \xrightleftharpoons[\text{dec}]{\text{enc}} \langle X \rangle$ by "simple", "efficient" alg
  ③ $|\langle X \rangle|$ not much longer than it needs to be
- $[w]_T$ = decoding of w as type T
- Guido: garbage/unparseable input = default object
- Decision problem: $f: \Sigma^* \to \{no, yes\}$
- Function problem: $f: \Sigma^* \to \Sigma^*$, one unique answer
- Search problem: $f: \Sigma^* \to \Sigma^*$, $\begin{cases} \langle \text{answer(s)} \rangle \\ \langle \text{no answer} \rangle \end{cases}$
- Language is any subset of Σ^*
- Church Turing Thesis: any real world alg can be simulated by a Turing machine
- Extended Church Turing Thesis: any real world alg running in T steps can be simulated by a TM running in poly(T) steps
- Turing Machine $M = (\Sigma, \Gamma, Q, q_0, q_{acc}, q_{rej}, \delta)$
  $\sqcup \notin \Sigma$ $\quad \Gamma = \{\sqcup\} \cup \Sigma \cup \{\text{other symbols}\}$ $\quad q_{acc} \neq q_{rej}$
  $\delta: (Q \setminus \{q_{acc}, q_{rej}\}) \times \Gamma \to \Gamma \times \{L, R\} \times Q$
- Configuration $C \in (\Gamma \cup Q)$



has configuration
$0 1 q_A 1 1 0 \sqcup 0$
state is left of tape head

  initial configuration $q_0 x$
  halting configuration if contain either q_{acc} or q_{rej}
  NextConfig$_M$(C), where $C = uaqbv$
  $= \begin{cases} uq'adv & \text{if } \delta(q,b) = (d, L, q') \\ uadq'v & \text{if } \delta(q,b) = (d, R, q') \end{cases}$

- Computation Trace of TM M on $x \in \Sigma^*$
  $= C_0 C_1 C_2 \cdots$ where $C_{i+1} = \text{NextConfig}_M(C_i)$
  either until halting configuration C_t is reached or indefinitely
  Reaching C_t = halts, $q_{acc} \in C_t$ = accepts, $q_{rej} \in C_t$ = reject,
  M runs in time t on input x
- M decider = $\forall x \in \Sigma^*$, $M(x)$ halts
- M decides L iff M decider, $\forall x \in L$ $M(x)$ accepts, $\forall x \notin L$ $M(x)$ rejects
- $M(x)$ outputs y if final config $q_{acc} y$
- M solves function problem f if $\forall x \in \Sigma^*$, $M(x)$ outputs $f(x)$
- Running Time $T_M(n) = \max_{|x|=n} \{\text{time } M \text{ takes on input } x\}$



TM Tricks, where M' is usual model
- M can stay put, $T_{M'}(n) \leq 2T_M(n)$ } goLeftThen;
- M double moves, $T_{M'}(n) \leq 2T_M(n)$
- Symbol marking by doubling tape alphabet
- marking application: simulate 1-way inf by 2-way inf at cost of 1 extra time step
- stretching input $aba \to a\sqcup b \sqcup a$ in $O(|x|^2)$ time
- reduce any tape alphabet to $\{0,1,\sqcup\}$ (standard alphabet); if M runtime $T(n)$ then M' runtime $O(T(n)) + O(n^2)$
  achieved by reencoding (stretching, note $\sqcup \to \sqcup\sqcup$)
- any k-tape TM w/ runtime $T(n)$ can be simulated by M' with runtime $O(T(n)^2)$.

Palindrome decided by 2-tape TM in $O(n)$ time
Hennie65 proved 1-tape TM for palindrome $\Omega(n^2)$ time
} quadratic slowdown cannot be improved

For $t: \mathbb{N} \to \mathbb{R}$, $\text{TIME}(t(n)) = \{\text{languages } L : \exists \text{ TM deciding } L \text{ in } O(t(n)) \text{ time}\}$ — note choice of model matters!
$P = \bigcup_{c \in \mathbb{N}} \text{TIME}(n^c)$

standard-alphabet TM has $\Sigma = \{0,1\}$ and $\Gamma = \{0,1,\sqcup\}$
ACCEPTS = $\{\langle M, w \rangle : M \text{ std alphabet}, w \in \{0,1\}^*, M(w) \text{ accepts}\}$
BOUNDEDACCEPTS$_{2^n}$ = $\{\langle M, w \rangle : M(w) \text{ accepts within } 2^{|w|} \text{ steps}\}$
Universal Turing Machine U simulates $\langle M, w \rangle$ (std alphabet, $\in \{0,1\}^*$), ie $U(\langle M, w \rangle)$ $\begin{cases} \text{loops if } M(w) \text{ loops} \\ \text{same output as } M(w) \text{ otherwise} \end{cases}$
Turing36 proved $\exists$ UTM U.
Thm. $\exists U$, if $M(w)$ halts in t steps then U's simulation has time $O(|\langle M \rangle|^2 \cdot t)$
Alarm-clocked UTM U has time bound $t \in \mathbb{N}$, $U(\langle t, M, w \rangle)$ runs until first of $\begin{cases} M(w) \text{ halts} \\ M(w) \text{ runs for } t \text{ steps} \end{cases}$
and $U(\langle t, M, w \rangle)$ at most $O(|\langle M \rangle|^2 + \log t) \cdot t$ steps
$f: \mathbb{N} \to \mathbb{R}$ clockable if $\exists$ 1-tape TM computing $m \to \lceil f(m) \rceil$ in $O(f(m))$ steps
Thm. If f clockable, $\exists U_f$ st if $|\langle M, w \rangle| = n$ then $U_f(\langle M, w \rangle)$ simulates $M(w)$ correctly for up to $f(|w|)$ steps in time $O(n \log n) + O(|\langle M \rangle|^2 + \log f(n)) \cdot f(n) \leq O(n^2 + \log f(n)) \cdot f(n)$
Cor. BoundedAccepts$_{f(n)} \in \text{TIME}(n^2 \cdot f(n))$

Time Hierarchy Theorem

A-tier: $f(n)$ clockable, $n \log n \leq O(f(n)) \Rightarrow \exists L$, $L \in \text{TIME}(f(n) \cdot \log f(n))$, $L \notin \text{TIME}\left(\frac{f(n)}{\log f(n)}\right)$
B-tier: $f(n)$ clockable, $n^2 \log n \leq O(f(n)) \Rightarrow \exists L$, $L \in \text{TIME}(n^2 \cdot f(n) \log f(n))$, $L \notin \text{TIME}\left(\frac{f(n)}{\log f(n)}\right)$
C-tier: $\exists L \in \text{TIME}(3^n)$, $\nexists$ std alphabet TM deciding L with $T(n) \leq O(1.1^n)$
D-tier: $\exists L \in \text{TIME}(3^n)$, $\nexists$ std alphabet TM deciding L with $T(n) \leq 2^n$

Turing36 ACCEPTS undecidable
AFSOC M_A decides ACCEPTS, let $D(\langle M \rangle) = !M_A(\langle M, \langle M \rangle \rangle)$, what is $D(\langle D \rangle)$? ⊥

Boolean Circuits
  input gates x_i, $\wedge$, $\vee$, $\neg$, 1, 0. size = # gates, depth = max dist between input/output
  boolean formula = all gates fan-out 1
  tree method to simulate fan-in > 2
  n inputs, m gates: $m \leq |\langle C \rangle| \leq O(m \log m)$

Efficient Chip Fabrication Thm
  For M TM deciding $L \subseteq \{0,1\}^*$, $T_M(n) \geq n$, then for any n exists n-input C_n of size $O(T_M(n)^2)$ deciding L on length-n inputs
  If $T_M(n) \leq n^k$, then $\exists F_M$ st $F_M(n)$ outputs $\langle C_n \rangle$ in poly(n) time.

Problems in P

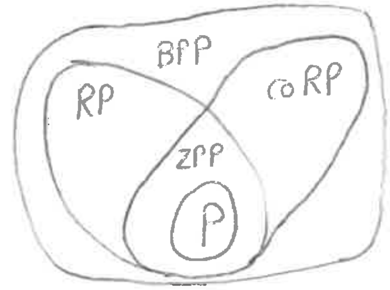
- $s \leadsto t$ path, $\langle G,s,t \rangle \to \{0,1\}$
  - $O(mn)$ - iterate over edges until no new marked vertices
  - $O(m)$ – BFS
- 2-COLORING, $\langle G \rangle \to \{0,1\}$
  - $O(m2^n)$ – brute force
  - $O(m+n)$ – BFS coloring on every connected component, conflict ⇒ odd cycle ⇒ not 2-colorable
- 3-COLORING, $\langle G \rangle \to \{0,1\}$
  - $O(m3^n)$ – brute force
  - $O(m2^n)$ – ??
  - $O(1.33^n \text{poly}(n))$ – Beigel-Epstein 01
- Longest Common Subsequence, $x,y \in \Sigma^n \to$ length of $lcs(x,y)$
  - $O(n2^n)$ – brute force
  - $O(n^2)$ – $LCS_{i,j} = \begin{cases} 1+LCS'_{i+1,j+1} & \text{if } x[i]=y[j] \\ \max\{LCS'_{i,j+1}, LCS'_{i+1,j}\} & \text{else} \end{cases}$
    where $LCS'_{i,j} = LCS(x[i:], y[j:])$
- 3-CLIQUE/TRIANGLE-FINDING, $\langle G \rangle \to \{0,1\}$
  - $O(n^3)$ – brute force
  - $O(n^{2.373})$ – matrix magic
- K-CLIQUE, $\langle G \rangle \to \{0,1\}$
  - $O(n^k)$ – brute force

Randomized Algorithms

Problem	Randomized	Deterministic
Primality Testing	$O(\langle n \rangle^2)$	$O(\langle n \rangle^6)$
Median Finding	$O(n)$	$O(n)$
Verify Matrix Multiply	$O(n^2)$	$O(n^{2.372})$
Minimum Spanning Tree	$O(m)$	$O(m\,\alpha(m,n))$ (inverse Ackermann)
3SAT	$O(1.31^n)$	$O(1.34^n)$
Polynomial Identity Testing	unstated but simple	open

- Probabilistic Turing Machine PTM has two δ_1, δ_2 where it applies either at each step with probability ½.
  Running time $f(n)$ if $\forall x$ input, random choices, at most $f(|x|)$ steps.
- PTM M decides L with one-sided error ε if M always halts and
  $\forall x \in L$, $\mathbb{P}\{M(x) \text{ accepts}\} \geq 1-\varepsilon$
  $\forall x \notin L$, $\mathbb{P}\{M(x) \text{ accepts}\} = 0$
  } no false positives, ε chance of false negative
- $RTIME(f(n)) = \{L : \exists \text{PTM } M \text{ w/ runtime } O(f(n)) \text{ deciding } L \text{ w/ } \varepsilon \leq 1/3\}$
- $RP = \bigcup_{c \in \mathbb{N}} RTIME(n^c)$
- Error Reduction: run k independent copies ⇒ one-sided error at most ε^k
- $\text{COMPOSITES} = \{\langle n \rangle \mid n \in \mathbb{N}, n = ab \text{ for } 1 < a,b \in \mathbb{N}\} \in RP$
  Number Theory fact: x prime ⇒ no composite witness
  x composite ⇒ at least ¾ of $0 \leq b \leq x$ witness compositeness,
  i.e. $b^d \not\equiv 1 \bmod x$ and $b^{2^i d} \not\equiv -1 \bmod x$ $\forall i \in \{0,1,s-1\}$
  we can verify witnesses in deterministic polytime
- $L^c = \Sigma^* \setminus L$
- $coRP = \{L : L^c \in RP\}$, i.e. $\exists$ PTM M such that
  $\forall x \in L$ $\mathbb{P}\{M(x) \text{ accepts}\} = 1$
  $\forall x \notin L$ $\mathbb{P}\{M(x) \text{ accepts}\} \leq \frac{1}{3}$
- PRIMES $\in$ coRP, without proof also PRIMES $\in$ P, i.e. PRIMES $\in$ ZPP
- $ZPP = RP \cap coRP$
  ← Zero-Error Probabilistic Polynomial Time

- BPP = Bounded-Error Probabilistic Polynomial Time
  $L \in BPP \Rightarrow \exists \text{PTM } M$, $\forall x \in L$ $\mathbb{P}\{M(x) \text{ accepts}\} \geq 2/3$
  $\forall x \notin L$ $\mathbb{P}\{M(x) \text{ accepts}\} \leq 1/3$
- We can similarly reduce error with k independent copies so that
  $x \in L \Rightarrow \mathbb{P}\{M(x) \text{ accepts}\} \geq 1 - \frac{1}{3^k}$
  $x \notin L \Rightarrow \mathbb{P}\{M(x) \text{ accepts}\} \leq \frac{1}{3^k}$



END DIDEROT CHAPTERS 1-8