formula is an AND (conjunction) of clauses

For example,

$\varphi = (\neg x \vee y) \wedge (\neg y \vee z) \wedge (x \vee y \vee \neg z)$

Is φ satisfiable? Yes, y: true, z: true

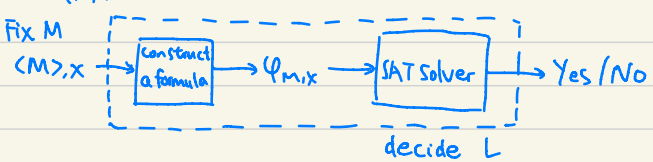
$SAT = \{\langle\varphi\rangle : \varphi \text{ is satisfiable}\}$

$SAT \in NP$

$(\forall L \in NP)(L \leq_p SAT)$

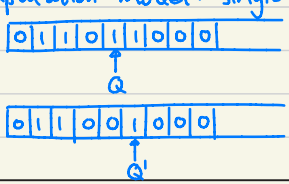
Thm 5.25 (Cook-Levin Theorem) SAT is NP-complete.

Proof. First, $SAT \in NP$. Because given an assignment, one can check if it is a satisfying assignment in polynomial time. To prove SAT is NP-complete, it suffices to prove for any NTM M and every input $x \in \{0,1\}^*$, one can construct a formula $\varphi_{M,x}$ efficiently such that M accepts x iff. $\varphi_{M,x}$ is satisfiable.



Snapshot (runtime configuration)

Computation model: single-tape one-way infinite NTM.



A = true A

A = false $\neg A$

We use the following variables

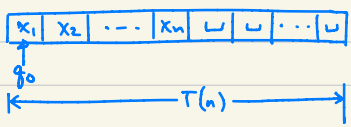
1) $T_{i,j,k}$, where $i,k \in \{1,\cdots,T(n)\}$, $j \in \Gamma$, indicates that at step k, cell i contains symbol j. $k \in \{0,\cdots,T(n)\}$

2) $H_{i,k}$, where $i,k \in \{1,\cdots,T(n)\}$, indicates that at step k the head points to cell i. $k \in \{0,\cdots,T(n)\}$

3) $Q_{q,k}$, where $q \in Q$ and $k \in \{0,\cdots,T(n)\}$ indicates that the machine is in state q at step k.

In total, we have introduced $O(T(n)^2 \times |\Gamma|) + O(T(n)) + O(|Q| \times T(n)) = O_M(T(n)^2)$.

Initialization



step 0

$H_{1,0}$ = true $H_{i,0}$ = false, $i = 2,\cdots,T(n)$

$T_{i,x_i,0}$ = true, $i = 1,\cdots,n$ $Q_{q_0,0}$ = true

$T_{i,\sqcup,0}$ = true, $i = n+1,\cdots,T(n)$ $Q_{q,0}$ = false, $\forall q \in Q \setminus \{q_0\}$.

Restrictions

1) At most one symbol per cell. $\forall i \in \{1,\cdots,T(n)\}$.
$\forall k \in \{0,\cdots,T(n)\}$, $\forall j \neq j' \in \Gamma$, we add the clause $\neg T_{i,j,k} \vee \neg T_{i,j',k}$

2) At least one symbol per cell. $\forall i \in \{1,\cdots,T(n)\}$
$\forall k \in \{0,\cdots,T(n)\}$, add $\bigvee_{j \in \Gamma} T_{i,j,k}$

3) M is in at most one state at any step.
$\forall k \in \{0,\cdots,T(n)\}$, for any $q \neq q' \in Q$, add $\neg Q_{q,k} \vee \neg Q_{q',k}$.

4) M is in at least one state at any step.
$\forall k \in \{0,\cdots,T(n)\}$, add $\bigvee_{q \in Q} Q_{q,k}$

5) The head points to at most one cell at any step.
$\forall k \in \{0, \cdots, T(n)\}$, $\forall i \neq i' \in \{1, \cdots, T(n)\}$, add $\neg H_{i,k} \vee \neg H_{i',k}$

6) The head points to at least one cell at any step.
$\forall k \in \{0, \cdots, T(n)\}$, add $\bigvee_{i=1,\cdots,T(n)} H_{i,k}$ $O(T(n))$

In total, we've added $O_M(T(n)^3)$ clauses.

Transition rule:

"computation is local"

$A \to B$ is equivalent to $\neg A \vee B$.

1) A cell is unchanged unless written. $\forall i \in \{1, \cdots, T(n)\}$, $\forall k \in \{0, \cdots, T(n)-1\}$, $\forall j \neq j' \in \Gamma$, add $T_{i,j,k} \wedge T_{i,j',k+1} \to H_{i,k}$

NTM
$\delta: Q \times \Gamma \to \mathcal{P}(Q \times \Gamma \times \{-1, 1\})$

2) Transition follows δ. $\forall i \in \{1, \cdots, T(n)\}$, $\forall k \in \{0, \cdots, T(n)-1\}$, $\forall q \in Q$, $\forall j \in \Gamma$, add

$$H_{i,k} \wedge Q_{q,k} \wedge T_{i,j,k} \to \bigvee_{(q',j',d) \in \delta(q,j)} H_{i+d,k+1} \wedge Q_{q',k+1} \wedge T_{i,j',k+1}$$

$A \to B$ $\neg A \vee B$

distributive law
$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

$$\neg H_{i,k} \vee \neg Q_{q,k} \vee \neg T_{i,j,k} \vee \left(\downarrow \ . \ . \right)$$

$O_M(T(n)^2)$

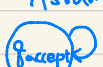
$((\square \wedge \square \wedge \square) \vee (\square \wedge \square \wedge \square) \vee \cdots)$ $\leq D$ times

We've added 3^D clauses, where $D \leq |Q| \times |\Gamma| \times 2$.

Thus, $3^D = O_M(1)$.

Halt in an accept state

Assume there is a self loop in q_{accept}. $O(1)$



Add $Q_{q_{accept}, T(n)}$

Finally, the formula $\varphi_{M,x}$ is the AND of all the above clauses.

clauses $\leq O_M(T(n)^2)$ □

每个都被满足：单个状态合法，转移合法，最后停在接收 ⇒ NTM ✓

5.5 NP complete problems

3SAT = $\{\langle\varphi\rangle : 3CNF\ \varphi \text{ is satisfiable}\}$.

3CNF is a formula where each clause has at most 3 literals.

For example, $\varphi = (x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee x_4) \wedge (x_2 \vee \neg x_3 \vee \neg x_4)$.

Thm 5.26 3SAT is NP-complete.

Proof. 3SAT is in NP.

$3SAT \leq_p SAT$ obvious

We need to prove $SAT \leq_p 3SAT$.

For example, $c = x_1 \vee x_2 \vee x_3 \vee x_4$.

$(x_1 \vee x_2 \vee z) \wedge (\bar{z} \vee x_3 \vee x_4)$

Let $c = l_1 \vee l_2 \vee \cdots \vee l_k$, $k \geq 4$, and $l_i \in \{x_1, \bar{x_1}, \cdots, x_n, \bar{x_n}\}$

Introduce new variables $z_1, z_2, \cdots, z_{k-3}$. Replace c by

$c' = (l_1 \vee l_2 \vee z_1) \wedge (\bar{z_1} \vee l_3 \vee z_2) \wedge (\bar{z_2} \vee l_4 \vee z_3) \cdots \wedge (\bar{z_{k-3}} \vee l_{k-1} \vee l_k)$

C is satisfiable iff. C' is satisfiable. □

Integer programming

Given a system of linear inequalities $Ax \leq b$, $x \in \mathbb{Z}^n$.

where A is an $m \times n$ matrix, b is an $m \times 1$ vector

The task is to find a vector x satisfying the inequalities.

INTERPROG = $\{(A, b) : Ax \leq b$ has an integer solution$\}$

Thm 5.27 INTERPROG is NP-complete.

Proof. INTERPROG $\in$ NP. Certificate is an satisfying assignment.

Now, we prove $3SAT \leq_p$ INTERPROG

$x_1 \vee \neg x_2 \vee \neg x_3$ $\quad x_1, x_2, x_3 \in \{0,1\}$ $\quad 0 \le x_i \le 1$.

$x_1 + (1-x_2) + (1-x_3) \ge 1$.

Let φ be a 3CNF in n variables $x_1, \cdots, x_n$ with m clauses $C_1, \cdots, C_m$.

For each variable, introduce a variable in integer programming.

For each $i = 1, \cdots, n$, add constraint $0 \le x_i \le 1$.

For each clause $C_j = \ell_i \vee \ell_j \vee \ell_k$, where $\ell_i \in \{x_i, \bar{x}_i\}$, $\ell_j \in \{x_j, \bar{x}_j\}$, $\ell_k \in \{x_k, \bar{x}_k\}$

introduce a constraint $y_i + y_j + y_k \ge 1$,

where $y_i = \begin{cases} x_i, & \text{if } \ell_i = x_i \\ 1 - x_i, & \text{if } \ell_i = \bar{x}_i \end{cases}$ and similar for y_j, y_k.

It is clear that φ is satisfiable iff. the integer programming is satisfiable.

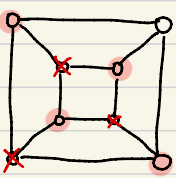
□

Independent Set

$G = (V, E)$. $I \subseteq V$ is <u>independent set</u> if there is no edge between any two vertices in I.

● : the independent set.

G:



INDSET $= \{(G, k)$: undirected graph G has an independent set of size $k\}$.

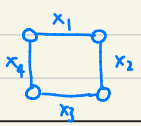
$\langle G, 4 \rangle \in$ INDSET $\quad \langle G, 5 \rangle \notin$ INDSET

Thm 5.28 INDSET is NP-complete.

Proof. INDSET is in NP.

We prove 3SAT $\le_p$ INDSET.

Given a 3CNF φ with m clauses,

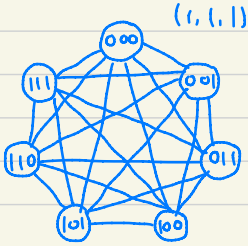


we construct a graph G with 7m vertices such that

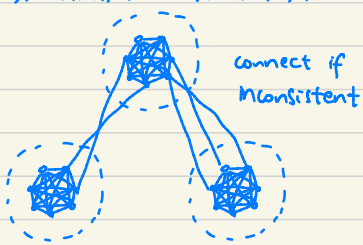
$\langle \varphi \rangle \in SAT$ iff.

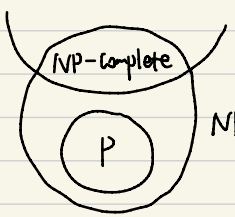
$C = x_1 \vee \bar{x}_2 \vee x_3$

$(x_1, x_2, x_3) \in \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)\}$



cluster.

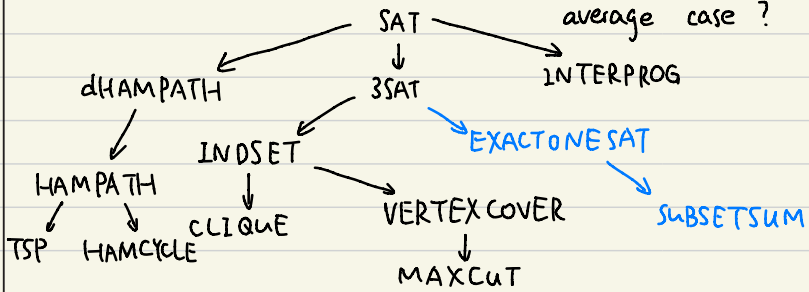




$P \neq NP$

L is NP-complete if
1) $L \in NP$, and
2) $(\forall k \in NP)(k \leq_p L)$

Worst case
average case ?



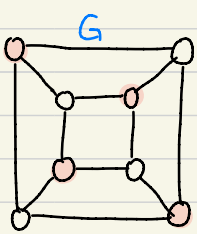
INDSET = $\{\langle G,k\rangle : G$ has an ind. set of size $k\}$

Represent G by its adj. matrix

$|V(G)| = v \quad |\langle G\rangle| = O(v^2)$

$\langle G,4\rangle \in$

$\langle G,5\rangle \notin$



Thm 5.28 INDSET is NP-complete.

Obviously, INDSET $\in$ NP

3SAT $\leq_p$ INDSET

Given any 3CNF φ with m clauses, we

$\forall k \in NP$

$k \leq_p 3SAT \leq_p INDSET \Rightarrow k \leq_p INDSET$

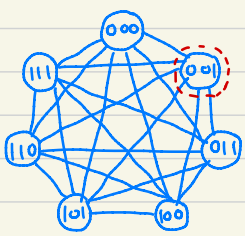
Construct a graph G with 7m vertices such that

1. $\varphi \in SAT \Rightarrow \langle G, m \rangle \in INDSET$
2. $\varphi \notin SAT \Rightarrow \langle G, m \rangle \notin INDSET$

For each clause, make a cluster, consisting of 7 satisfying assignments. Connect all of them within the cluster.

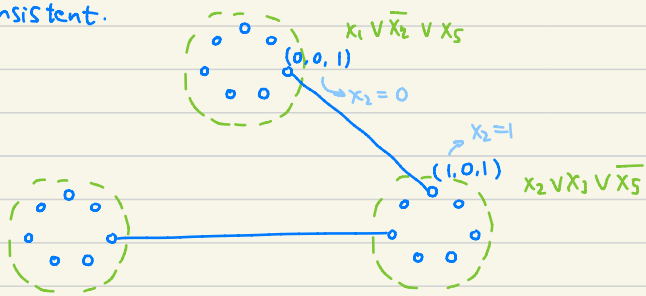
$C = x_1 \vee \bar{x}_2 \vee x_3$

0	0	0
0	0	1
~~0~~	~~1~~	~~0~~
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1



$\#IS \leq m$

For different clauses, connect the vertices if the assignments are inconsistent.



φ is satisfiable iff. G has ind. set of size m.

$\Rightarrow$ ✓

↳ 对每个 variable 有一个赋值，每团一个，且两两(团)间无矛盾). ind. set

$\Leftarrow$ ✓

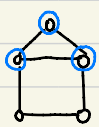
G有ind. set，必每团至多一个，又共m个，故每团一个，且团间无连线，故无矛盾，

↓

取此赋值. φ sat. □

CLIQUE = $\{\langle G, k\rangle : G \text{ has a } K_k \text{ subgraph}\}$

Thm 5.29 CLIQUE is NP-complete.



$\langle G, 3\rangle \in$ CLIQUE

$\langle G, 4\rangle \notin$ CLIQUE

CLIQUE $\in$ NP:

The certificate is a set of k vertices.

The verifier checks if they form a K_k.

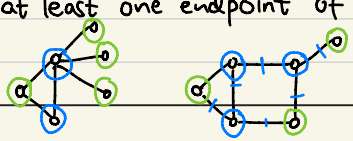
We show INDSET $\leq_p$ CLIQUE.

Given graph G and integer K.

$\langle G, k\rangle \in$ INDSET iff. $\langle \bar{G}, k\rangle \in$ CLIQUE. □

VERTEX-COVER = $\{\langle G, k\rangle : G \text{ has a vertex cover of size } k\}$

a vertex cover of a graph is a set of vertices that includes at least one endpoint of every edge of the graph.



O vertex cover

O ind. set

O—O 一定没边. 因为若有，必使被O cover. 但未被cover

Thm 5.30 VERTEX-COVER is NP-Complete

Proof. VERTEX-COVER $\in$ NP.

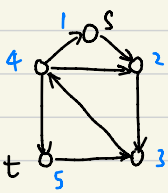
INDSET $\leq_p$ VERTEX-COVER

Let $G=(V,E)$ be a graph. $W \subseteq V$ is a vertex cover of G iff. $V \setminus W$ is an ind. set.

Thus, $\langle G, k\rangle \in$ INDSET iff. $\langle G, \#V(G)-k\rangle \in$ VERTEX-COVER. □

访问每个点一次仅一次.

dHAMPATH = {$\langle G,s,t\rangle$: directed graph, G has a Hamiltonian path from s to t}.



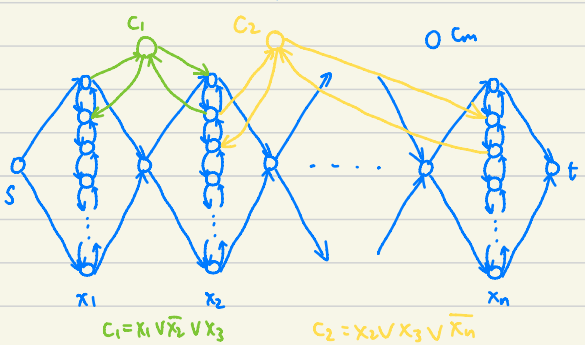
Thm 5.31 dHAMPATH $\in$ NP-Complete.

Proof. Obviously, dHAMPATH $\in$ NP.

We prove 3SAT $\leq_p$ dHAMPATH.

Given a 3CNF φ, construct a directed graph $G=(V,E)$ and $s,t \in V(G)$ such that φ is satisfiable iff. $\langle G,s,t\rangle \in$ dHAMPATH.

↓ true ↑ false



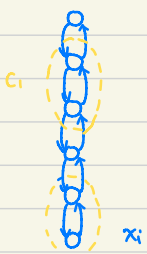
"Think geometrically, prove algebraically."
John Tate

For any 3CNF φ, construct a directed graph G with two designated vertices s and t, such that G has a Ham path from s to t if φ is satisfiable.

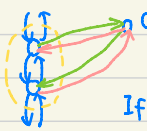
Suppose φ has n variables $x_1 \cdots x_n$ and m clauses $c_1 \cdots c_m$.

For each x_i, create a diamond-shaped structure, that can be traversed in either of the two ways, corresponding to true or false.

Each diamond structure contains $3m+1$ vertices.

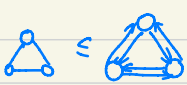


If a variable x_i appears in c_j, add the green edge



If $\bar{x_i}$ appears in c_j, add the pink edge

Verify φ is satisfiable iff. G has a Ham path from s to t. □



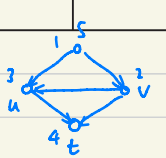
HAM

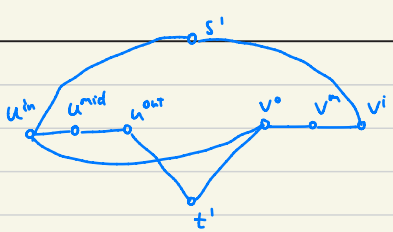
Thm 5.32 HAMPATH $\in$ NP-Complete

Proof. HAMPATH $\in$ NP.

We prove dHAMPATH $\leq_p$ HAMPATH.

Given any directed graph $G(V,E)$ and $s,t \in V(G)$, construct an undirected graph $G'(V,E)$ and $s',t' \in V(G')$ such that G has a Ham path from s to t iff. G' has a Ham. path from s' to t'.





Replace $s \in V(G)$ by s', and replace $t \in V(G)$ by t'. For each $u \in V(G) \setminus \{s,t\}$. replace u by u^{in}, u^{mid}, u^{out}, and

If $(u,v) \in E(G)$, add $(u^{out}, u^{in}) \in E(G')$. Verify G has a Ham. path from s to t iff. G' has a Ham. path from s to t.

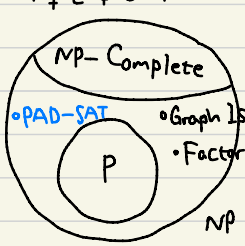
$\Rightarrow$) Say $s, u_1, u_2, \cdots, u_L, t$ is a Ham. path in G,
$s', u_1^{in}, u_1^{mid}, u_1^{out}, \cdots, u_L^{in}, u_1^{mid}, u_L^{out}, t'$ is a Ham path

$\Leftarrow$) If G' has a Hamilton path from s' to t'. then it has to be in the following form.
$s', u_1^{in}, u_1^{mid}, u_1^{out}, u_2^{in}, u_2^{mid}, u_2^{out}, \cdots, u_L^{in}, u_L^{mid}, u_L^{out}, t'$.
We claim $s, u_1, \cdots, u_L, t$ is a Ham. path in G. □

5.6 Hierarchy Theorem

$DTIME(n) \subsetneq DTIME(n^2) \subsetneq DTIME(n^3)$?

$P \subsetneq E \subsetneq EXP$? $\quad E = DTIME(2^{O(n)})$. $EXP = DTIME(2^{n^{O(1)}})$



Thm 5.33 (Ladner's theorem)
If $P \neq NP$. then there exists a language $L \in NP$ and $L \notin P$.

"padding"
input: x $|x| = n$.
$|x \# 1^{2^n}| = n + 2 + 2^n$

ToC main problems
P≠NP?
P≠NC? 为了拍表.
P= BPP?
P≠SPACE?
L≠P?

5.6 Hierarchy Theorem

$DTIME(n) \subsetneq DTIME(n^2) \subsetneq DTIME(n^3) \subsetneq SPACE(n) \subsetneq SPACE(n^2) \subsetneq SPACE(n^3) \cdots$

Def 5.28 Function $T: \mathbb{N} \to \mathbb{N}$ is time-constructible if there is a TM M that, on input 1^n, outputs the binary representation of $T(n)$ within time $O(T(n))$. ($|x| = n$.)

For example, n: 111 n=3 // double一个n, 直到起过, 成掉.

$n^2, n^3, n\lfloor \log_2 n \rfloor, 2^n, 2^{n^2}$ $(\log n)^2$

不是时间可构造的: eg. 不可计算 (一些奇怪的函数)

Thm 5.29 (Time Hierarchy Theorem) If f, g are time-constructible functions satisfying $f(n) \log f(n) = o(g(n))$, then $DTIME(f(n)) \subsetneq DTIME(g(n))$. ($L \in$ / $L \notin$)

Proof. "diagonalization"

claim. $\frac{g(n)}{\log g(n)} = \omega(f(n))$ Condition $f(n)\log f(n) = o(g(n))$.

$\Rightarrow f(n) = o\left(\frac{g(n)}{\log f(n)}\right)$ $\omega(f(n)) = \frac{g(n)}{\log f(n)}$.

Proof of claim.

Case 1. $g(n) \geq f(n)^2$.

$\frac{g(n)}{\log g(n)} \geq \frac{g(n)}{g(n)^{1/3}} = g(n)^{2/3} \geq f(n)^{4/3} = \omega(f(n))$.

Case 2. $g(n) < f(n)^2$.

$\frac{g(n)}{\log g(n)} \geq \frac{g(n)}{\log f(n)^2} = \frac{g(n)}{2\log f(n)} = \omega(f(n))$. □

Since $f(n), g(n)$ are time-constructible, we can construct $t(n) \overset{\text{def}}{=} \left\lfloor \frac{g(n)}{\lfloor \log_2 g(n) \rfloor} \right\rfloor$ in time $O(g(n))$.

N: 在 $t(n)$ 步仍停下來

Since $f(n), g(n)$ are time-constructible, we can construct $t(n) \overset{\text{def}}{=} \left\lfloor \frac{g(n)}{\lfloor \log_2 g(n) \rfloor} \right\rfloor$ in time $O(g(n))$.

	M_0	M_1	M_2	M_3	M_4	M_5	M_6	
ε	$A^{\to R}$							$\le t(n)$ steps
0		$R^{\to A}$						$L \in \text{DTIME}(g(n))$.
1			$N^{\to A}$					$L \notin \text{DTIME}(f(n))$.
00				$R^{\to A}$				
01								

Construct the following TM: On input $x \in \{0,1\}^*$, simulate M_x on input x for $t(n)$ steps and flip the output, i.e.,

1) If M_x accepts x, reject
2) If M_x rejects x, accept
3) If M_x does not stop in $t(n)$ steps, accept.

The simulation takes $O\left(\left\lfloor \frac{g(n)}{\lfloor \log_2 g(n) \rfloor} \right\rfloor \cdot \log \left\lfloor \frac{g(n)}{\lfloor \log_2 g(n) \rfloor} \right\rfloor\right)$

$= O\left(\frac{g(n)}{\log_2 g(n)} \cdot \log \frac{g(n)}{\log_2 g(n)}\right)$ // $\lfloor a \rfloor \le a$, $\lfloor a \rfloor \ge \frac{a}{2}$. ($a \ge 1$ 時)

$= O\left(\frac{g(n)}{\log_2 g(n)} \cdot \log_2 g(n)\right) = O(g(n))$.

Claim. $L(M) \notin \text{DTIME}(f(n))$

Proof (of the claim). Suppose for contradiction that L is decided by M_α in time $O(f(n))$.

Case 1. M_α accepts $\alpha \Rightarrow \alpha \notin L$.

Contradiction!

Case 2. M_α rejects $\alpha \Rightarrow \alpha \in L$. Contradiction!

□

Corollary 5.30

1) $DTIME(n) \subsetneq DTIME(n^2) \subsetneq DTIME(n^3) \subsetneq$

2) $P \subsetneq EXP$