2200013213 计算理论
柯宇航 HW3.

1. 算法如下：

Input: $\phi = \bigwedge_{i=1}^{n} A_i$，其中 $A_i = \bigvee_{j=1}^{j_0} v_{ij}$；

v_{ij} 为 p 或 $\neg p$，p 是命题公式

Output: ϕ 是否可满足.

```
while (True) do:
    若 所有 A_i 中都含有 ¬p:
        将所有 A_i 中的 p 公式置为 False
        返 Return True
    Else if 有一个 A_i 不含任何 p 或 ¬p:
        Return False
    Else: [此时必有 A_i 仅包含 p]
        令 p = True，从其他 A_i 中删去 ¬p，并删掉 p 所在的 A_i
    End.
```

注：正确性显然. 多项式时间复杂度由每个循环至少清除一个变量，知是关于输入 ϕ 多项式时间的.

2. 设符号集为 Σ，则 $\exists$ 多项式时间函数 $p_1, p_2: \mathbb{N} \to \mathbb{N}$ 与对应的图灵机 M_1, M_2，有 $L_i = \{x \mid \exists u \in \Sigma^{p_i(|x|)}, M_i(x,u)=1\}$

则构造图灵机 M 接受 (x,u') $u' \in \Sigma^{p_1(|x|)+p_2(|x|)+1}$ 若

$u' = (u_1, u_2)$

M 分别运行 $M_1(x,u_1)$，$M_2(x,u_2)$

根据结果判断 x 是在 $L_1 \cap L_2$，$L_1 \cup L_2$ 中.

显然 $p_1(|x|)+p_2(|x|)+1$ 关于 $|x|$ 多项式

且 M 也是多项式时间的.

$\therefore L_1 \cap L_2, L_1 \cup L_2 \in NP$

3. 假设 n 是 w 的十进制表示

则 $|w| = \log_2 n$

(1) 我们先构造一个存疑的图灵机 M：

M 接受 $(w; Cw)$

其中 $Cw = (p_1, a_1, p_2, a_2 \cdots p_s, a_s)$

其中 p_i 是 n 所有素因数

$a_i \in \{2,3,\cdots n\}$ 且 $a_i^{n-1} \equiv 1 \pmod n$.

a_i 等于 $1 \pmod n$

由素数定理，p_i 个数 $\le \log_2 n$，$p_i, a_i \le w$

$|Cw| \le \sum_{i=1}^{|w|} 2\log_2 n = O(n \log n) = O(|w| 2^{|w|})$

而 M 依次验证 $a_i^{n-1} \equiv 1 \pmod n$，$a_i$ 等于 $1 \pmod n$ 是否成立.

① 注意乘法是 $|w|$ 位 $\times$ $|w|$ 位是 $O(|w|^2)$

② 带余除法可用二分法的乘法模拟.

至多 $|w|$ 共 $\log_2 n$ 次乘法 $\Rightarrow$ 除法 $O(|w|^3)$

③ $a_i^{n-1} \pmod n$ 可用快速幂，至多 $\log_2 n$ 次乘法和取模 $\Rightarrow$ 需 $O(|w|^4)$

④ 共 n 个 a_i 算 n 次 $\Rightarrow$ 需 $O(|w|^5)$

(2) 注意到，(1) 中 M 默认为提供的 p_i 都是素数，但这不一定

我们构造一个先否定的图灵机 M_1

M_1 接受 $(w, w_1, Cw_1, w_2, Cw_2 \cdots w_s, Cw_s)$

其中 $w_1 < w_2 < \cdots < w_s = w$ 是 $1 \sim w$ 间所有素数

(当然 Cw_i 是 (1) 中 w_i 对应的证明.)

~~也要保证验证~~

M_1 行为如下：

```
For i=1,2,...,s:
    若 w_i = 2,3,5, 直接 (避免小素数需要复杂判断)
        Goto Continue;
    Else:
        检查 Cw_i 中是否是在若干 w_1 ~ w_{i-1} 中
        并且有 M(w_i, Cw_i)
        若有一为不接受，则拒绝
    End.
```

显然 M_1 是一个聪正确的验证器

④ 下面给出构造 $(w_s, w_1, Cw_1, \cdots w_s, Cw_s)$ 的长度估计.

不妨设这个函数为 $p: \mathbb{N} \to \mathbb{N}$.

① 如何生成 $(w_1, Cw_1, \cdots w_s, Cw_s)$ 如何的
先调用(1)中生成 w, Cw，再对 Cw 中引入的
素数递归生成，最后排序大小排序后
去掉重复的

② 证书的长度是多项式的
~~事实上，设 w 生成的总证明长度为 $p(w)$~~
~~$\forall w_i$，设 w_i 引入素数 $w_{i,1}, w_{i,2}, \cdots w_{i,s}$~~
~~则 $w_{i,1} w_{i,2} \cdots w_{i,m} \mid \frac{w_i}{2}$~~ ∵偶素数可直接判定，所以只管奇素数了.
事实上，设 n 生成的总证明长度为 $p(n)$，并设 n 引入素数
$n_1, n_2, \cdots n_s$，则 $n_1 n_2 \cdots n_s \mid \frac{n-1}{2}$ ∵偶数直接判断所以只考虑奇数
由(1)，n, C_n 的长度是 $< \log_2^2 n$ 的 $O(\log_2^2 n)$ 的.

$\therefore p(n) = p(n_1) + \cdots + p(n_s) + \log_2^2 n$.
当 $n \le 20$ 时，存在 $C_0 > 100$，$p(n) < C_0 \log_2^3 n$
~~则由归纳~~ 而~~我们用归纳~~
而 $\sum_{i=1}^{s} C_0 \log_2^3 n_i + \log_2^2 n \le C_0 \log_2^3 \frac{n-1}{2} + \log_2^2 n$
$< C_0 [\log_2^3 n - 3\log_2^2 n + 3\log_2 n - 1] + \log_2^2 n$
$= C_0 \log_2^3 n - [0.5 C_0 - 1] \log_2^2 n - C_0 [2.5 \log_2^2 n - 3\log_2 n + 1]$
$< C_0 \log_2^3 n$
∴由归纳法，$p(n) < C_0 \log_2^3 n$
最终 $p(w) < C_0 \log^3 |w|$
∴证书长度多项式

③ 图灵机验证所用多项式
设验证所用为 $T(n)$
则由(1)，有
$T(n) = \sum_{i=1}^{s} T(n_i) + C_0 \log_2^5 n$

我们归纳证明 $T(n) \le C_1 \log_2^b n$.
显然显然，归纳部分，由
$T(n) \le C_1 \sum_{i=1}^{s} \log_2^b n_i + C_0 \log_2^5 n$
$\le C_1 [\log_2 \frac{n-1}{2}]^b + C_0 \log_2^5 n$
$\le C_1 [\log_2 n - 1]^b + C_0 \log_2^5 n$.
$= C_1 \log_2^b n + (C_0 - bC_1) \log_2^5 n - C_1 \log_2^4 n [\log_2 n - 3]$
$- 20 bC_1 [\log_2^3 n - \frac{3}{4} \log_2^2 n] - bC_1 [b \log_2 n + 1]$
在 n 较大，$C_1 > C_0$ 时恒 $< C_1 \log_2^b n$
∴ $T(n) \le C_1 \log_2^b n$ 对较大的 C_1 成立
综上：∴在 NP 内

4.(1)我们将3-SAT归约到停机问题.

$\forall A \in 3SAT$

设A有n个变量 x_i $(1 \le i \le n)$

构造图灵机 M_A

M_A: n个for循环为x_i赋值

验证是否满足

不满足就死循环.

则生成$\langle M_A \rangle$是多项式时间的.

扫描全能王 创建

~~则将 (<M>, A) 输入到~~

~~1. ∀A∈3SAT，构造M~~

定义 $f(A) = (\langle M_A \rangle, A)$

则 $A \in 3SAT \Leftrightarrow f(A) \in HALT$

∴ 3SAT 多项式归约到 HALT

而 3SAT 是 NP-Hard

∴ HALT 是 NP-hard

但 HALT 不是 NP 问题

⇒ HALT 不是 NPC 问题

5. 证明：

∵ $A \neq \phi$, $A \neq \Sigma^*$

∴ $\exists a, b \in \Sigma^*$, $a \in A$, $b \notin A$

$\forall w \in$ 3-SAT

$f(w) = \begin{cases} a & 若w可满足 \\ b & 若w不可满足 \end{cases}$

由 P=NP ⇒ 3-SAT 有多项式判定法

⇒ f(w) 多项式时间

而 $w \in$ 3-SAT $\Leftrightarrow f(w) \in A$

∴ 3-SAT 多项式归约到 A

而 3-SAT 是 NP-hard

∴ A 是 NP-hard

又 $A \in P \subseteq NP$ ⇒ A 是 NPC.

6(1) 设 $\phi = \wedge C_i$ $i = 1, 2, \cdots n$

其中 $C_i = y_{i,1} \vee y_{i,2} \vee y_{i,3}$

$y_{i,k}$ 是原子公式或原子公式的否定

任取 ϕ 一个 ≠ 赋值

则 $y_{i,1}, y_{i,2}, y_{i,3}$ 中有 1~2 个真

⇒ $\neg y_{i,1}, \neg y_{i,2}, \neg y_{i,3}$ 有 1~2 个真

∴ 反转也是 ≠ 赋值

(2) 由于 C_i 循环共有 n 个

∴ 归约是 $O(n) = O(|\phi|)$ 的

也即多项式时间.

记 ϕ' 是归约后的 ϕ，则

$\phi' = \wedge d_i \wedge e_i$ $1 \le i \le n$

$d_i = y_{i,1} \vee y_{i,2} \vee z_i$

$e_i = \overline{z_i} \vee y_{i,3} \vee b$.

① 先证 $\phi \in 3SAT \Rightarrow \phi' \in \neq SAT$.

~~任取 ϕ 一个赋值 $(y_{i,1}, y_{i,2}, y_{i,3})$~~

~~令 ϕ' 令 $(y_{i,1}, y_{i,2}, z_i, y_{i,3}, b)$~~

~~‖~~

~~$(y_{i,1}, y_{i,2}, y_{i,3})$~~

接下来确定 z_i 赋值，而 b 恒为 0

$y_{i,1}$	$y_{i,2}$	$y_{i,3}$	z_i
1	1	1	0
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	1

不难验证出样赋值 $\phi \in \neq SAT$

② 再证 $\phi' \in \neq SAT \Rightarrow \phi \in SAT$

任取 ϕ' 赋值，只把令 ~~把~~ z_i 换成 $y_{i,3}$

去掉所有 e_i 即可.

综上，$\phi \in \neq SAT \Leftrightarrow \phi \in SAT$

∴ 3SAT 多项式归约到 ≠SAT

(3) 由 (2)，且 3SAT∈NPC ⇒ ≠SAT∈NP-hard

又 ≠SAT 显然 ∈NP

⇒ ≠SAT∈NPC.