第九章作业

袁晨圃

7.1

习题 1 (9.9)：证明若 $\mathrm{NP} = \mathrm{P}^{\mathrm{SAT}}$，那么 $\mathrm{NP} = \mathrm{coNP}$

证明：

a. $\mathrm{coNP} \subseteq \mathrm{NP}$

引理：$\mathrm{coNP} \subseteq \mathrm{P}^{\mathrm{SAT}}$

证明：对于任意语言 $L \in \mathrm{coNP}$，它的补 $\overline{L} \in \mathrm{NP}$。通过将 $\overline{L}$ p 规约到 SAT，可以在一次查询之后得到输入 w 是否属于 $\overline{L}$，对结果取反即可得到 w 是否属于 L。因此，L 可以在多项式时间内被判定，从而 $L \in \mathrm{P}^{\mathrm{SAT}}$。

$\mathrm{coNP} \subseteq \mathrm{P}^{\mathrm{SAT}} \wedge \mathrm{NP} = \mathrm{P}^{\mathrm{SAT}} \longrightarrow \mathrm{coNP} \subseteq \mathrm{NP}$

b. $\mathrm{NP} \subseteq \mathrm{coNP}$

$\forall L \in \mathrm{NP}, \overline{L} \in \mathrm{coNP}$

又 $\mathrm{NP} = \mathrm{P}^{\mathrm{SAT}} \longrightarrow \mathrm{coNP} \subseteq \mathrm{NP}$，所以 $\overline{L} \in \mathrm{NP}$，所以 $L \in \mathrm{coNP}$

$\forall L \in \mathrm{NP}, L \in \mathrm{coNP} \longrightarrow \mathrm{NP} \subseteq \mathrm{coNP}$

综上，$\mathrm{NP} = \mathrm{P}^{\mathrm{SAT}} \longrightarrow \mathrm{NP} = \mathrm{coNP}$

习题 2 (9.11)：证明 $\text{MAX-CLIQUE} \in \mathrm{P}^{\mathrm{SAT}}$

> $\text{MAX-CLIQUE} = \{\langle G, k\rangle \mid G \text{ 中最大团大小恰好为 } k\}$

证明：定义 φ_s 表示 至少有大小为 s 的团，那么最大团大小恰好为 k 可以表示为 $\varphi_k \wedge \overline{\varphi_{k+1}}$，通过查询两次 SAT oracle 得到结果

下面证明可以在多项式时间内构造 φ_s 的 CNF 表达式

设 $G = (V, E)$

每一个节点 v 对应一个变量 x_v

$\forall (u, v) \notin E$, 加入 $\neg x_u \vee \neg x_v$，表示 u, v 不能同时选（因为没边）

构造 $O(n \log n)$ 个字句来表示数量 $\geq s$：

将节点编号 $1 \ldots n$，对于任意一个节点 i 构造 $\log n$ 个布尔变量表示前 i 个点里选了的点数量的二进制每一位

这样在最终式中引入了 $O(n \log n)$ 个约束

最终在 CNF 中加入一个约束，包含 $n-s+1$ 个字句，每个字句包含 $\log n$ 个变量，表示计数结果 $\geq s$。

这样构造出来的 CNF 属于 $O(n\log n) \subseteq O(n^2)$

所以 MAX-CLIQUE $\underset{p}{\leq}$ SAT

所以 MAX-CLIQUE $\in \mathrm{P}^{\mathrm{SAT}}$

不用构造一个 CLIQUE 规约，直接说因为 CLIQUE 可以 p-规约到 SAT 所以存在多项式时间机器 M^{SAT} 判定 CLIQUE.

存在大小为 k 的团 $\Longleftrightarrow$ 最大团大小不小于 k

模拟两次 M^{SAT}，分别输入 $\langle G,k\rangle$ 和 $\langle G,k+1\rangle$，第一次接受且第二次拒绝即 接受，反之 拒绝

习题 3 (°9.21)：定义函数 $\mathrm{pad}:\Sigma^*\times\mathbb{N}\to\Sigma^*\#^*:(s,t)\mapsto s\#^j, \text{where } j=\max(0,l-\mathrm{len}(s))$

对于语言 A 和函数 $f:\mathbb{N}\to\mathbb{N}$ 定义语言 $\mathrm{pad}(A,f)=\{\mathrm{pad}(s,f(m))\mid s\in A, m=\mathrm{len}(s)\}$

证明：若 $A\in\mathrm{TIME}(n^6)$ 则 $\mathrm{pad}(A,n^2)\in\mathrm{TIME}(n^3)$

解：$O\Big(\big(n^{1/2}\big)^6\Big)=O(n^3)$

构造判定 $\mathrm{pad}(A,n^2)$ 的图灵机 $M=$对于输入 w: 去掉后缀 # 得到 w' 在其上模拟运行判定 A 的 $O(n^6)$ 机器 M_A

由于对于每个 A 中的串 s，$\mathrm{pad}(s,|s|^2)$ 会导致长度变为原来的平方倍，所以 $|w'|=O\big(|w|^{1/2}\big)$

先计算 $\lfloor\sqrt{n}\rfloor$，然后判断 $\lfloor\sqrt{n}\rfloor..n$ 的子串是否全是 #，不是则拒绝

所以整体复杂度为 $O(n^3)$，所以 $\mathrm{pad}(A,n^2)\in\mathrm{TIME}(n^3)$

习题 4 (°9.22)：证明 NEXPTIME $\neq$ EXPTIME $\longrightarrow$ P $\neq$ NP

提示：pad

解：证明逆否命题 P = NP $\longrightarrow$ NEXPTIME = EXPTIME

显然有 EXPTIME $\subseteq$ NEXPTIME

下面证明 P = NP $\longrightarrow$ NEXPTIME $\subseteq$ EXPTIME

对于语言 $L\in\mathrm{NTIME}(2^{kn}), k>0$，定义函数 $f:n\mapsto 2^{kn}$

构造语言 $L_{\mathrm{pad}}=\mathrm{pad}(L,f)$ (ref: 习题 3)

此时 L_{pad} 中串 w' 长度为 原始串 w 长度的指数级 $|w'|=O\big(2^{k|w|}\big)$，因此在去掉 padding 后缀之后有效部分长度 $l=(1/k)\log_2(|w'|)$

因为 $L\in\mathrm{NTIME}\big(2^{kn}\big)$

所以判定 L_{pad} 的非确定性机器时间复杂度为 $O\big(2^{kl}\big)=O\big(2^{k\cdot(1/k)\log_2(n)}\big)=O(n)$，得 $L_{\mathrm{pad}}\in\mathrm{NP}$

由于 P = NP，所以 $L_{\mathrm{pad}}\in\mathrm{P}$

判定串 w 是否属于 L 时，确定性的将其 pad 成 $w', |w'|=O\big(2^{k|w|}\big)$，然后调用 L_{pad} 的确定性多项式时间算法，得 $L\in\mathrm{EXPTIME}$

所以 $\mathrm{NEXPTIME} \subseteq \mathrm{EXPTIME}$

所以 $\mathrm{P} = \mathrm{NP} \longrightarrow \mathrm{NEXPTIME} = \mathrm{EXPTIME}$

习题 5 (°9.24)：证明 $\mathrm{TQBF} \notin \mathrm{SPACE}\left(n^{1/3}\right)$

解：

若 $\mathrm{TQBF} \in \mathrm{SPACE}\left(n^{1/3}\right)$，则由空间层次定理 $\exists L \in \mathrm{SPACE}(n), L \notin \mathrm{SPACE}\left(n^{1/3}\right)$

但 L 可对数空间规约到 TQBF，所以 $L \in \mathrm{SPACE}\left(n^{1/3}\right)$ 矛盾