第13卷第3期 数学研究与评论 Vol. 13 No. 3
1993年8月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION Aug. 1993

# 关于相对化的 $P=?NP$ 问题的注记*

宋恩民 金人超 黄文奇
(华中理工大学计算机系,武汉 430072)

## 摘 要

问题 $P=?NP$ 在相对化后随外部信息集的不同可能有相反的答案[1]. 本文得出如下进一步的结果:

1. 存在着无穷个集合 $S_1,S_2,\cdots$,这些集合的复杂度依次严格上升,并且在它们分别地作为外部信息集合,能交替地使命题 $P=NP$ 和 $P\neq NP$ 相对比;

2. 存在着在 $NP$ 类之外的递归集 $A$,使得 $P=NP$ 等价于 $P^A=NP^A$.

## 一 引 言

$P$ 是否等于 $NP$ 的问题是当今计算机科学界的具有实质性意义的难题. 但是对于相对化的 $P=?NP$ 的问题已有了明确的答案,即既存在着递归集 $A$,使 $P^A=NP^A$,也存在着另外的递归集 $B$ 使 $P^B\neq NP^B$. 之所以会出现这种答案相反的"两面"情况,当是外部信息集的计算复杂性的情况在这里起了作用. 经过探讨我们证明了存在着一个复杂度严格上升的集合的序列,其中的集合在作为外部信息集后能交替地使 $P=NP$ 和 $P\neq NP$ 相对化. 另外,我们具体地构造出了一个 $NP$ 类之外的递归集,在用它作为外部信息集后 $P=?NP$ 问题的相对化的答案与绝对的 $P=?NP$ 问题的答案一致.

我们希望这些探讨能有助于对"计算"的某些现象的进一步理解.

## 二 相对可比定理及推论

**定理 2.1** (相对等可比定理) 对任意 01 串集合 $A$,存在 01 串集合 $B$,使 $A\leqslant_1^p B$ 且 $P^B=NP^B$.

**证明** 我们用 $0^n$ 记恰由 $n$ 个"0"组成的字符串,用 $\langle x,y,z\rangle$ 记(其中 $x,y,z$ 均代表 01 串),将"$x,y,z$"中"0"用"00"代替、"1"用"01"代替、","用"11"代替所得的 01 串. 例如:

$$\langle 10,001,0^2\rangle = 0100110000001110000.$$

用 $xy$ 记将串 $x$ 后面接上串 $y$ 所得的一个 01 串.

定义 $B$ 为:$\{y0^{|y|+1}\mid y\in A\}\cup\{\langle i,x,0^n\rangle\mid NP_i^B$ 在不多于 $n$ 步内接受 $x\}$.

---

* 1991年3月11日收到. 国家自然科学基金资助项目.

显然对于所有的 01 串 $i$、$x$、$0^*$，$\langle i,x,0^*\rangle$ 都是一个长度为偶数的 01 串.

在上面对 $B$ 的定义中，第一个集合中的元素，其长度全部为奇数，当 $A$ 给定后，它就是确定的. 第二个集合中的元素其长度全部为偶数，但它的定义又涉及到了 $B$ 本身，不过 $B$ 的关于长度为 $2K$ 的串的定义只涉及了 $B$ 关于长度小于 $K$ 的串的定义，这是因为：按照我们的定义，判断一个具有 $\langle i,x,0^*\rangle$ 形式的串是不是 $B$ 的元素，只需让 $NP_i^B$ 对输入 $x$ 做至多 $n$ 步运算，运算中所能查询的串其长度不会超过 $n$，若 $\langle i,x,0^*\rangle$ 的长度为 $2K$，则 $n<K$. 故我们的定义是可行的递归定义.

因 $\forall x\in\{0,1\}^*$，$x\in A\Leftrightarrow x0^{|x|+1}\in B$，不难看出 $f(x)=x0^{|x|+1}$ 是多项式时间可计算的单一函数，故 $A\leqslant_1^p B$.

对 $\forall S\in NP^B$，设 $S$ 由 $NP_j^B$ 接受，$NP_j^B$ 的多项式时间界函数为 $q_j$，则对 $\forall x\in\{0,1\}^*$，$x\in S\Leftrightarrow NP_j^B$ 在不多于 $q_j(|x|)$ 步内接受 $x\Leftrightarrow\langle j,x,0^{q_j(|x|)}\rangle\in B$. 故 $S$ 可由这样一台确定型的查询机带上 $B$ 为天书来接受：对输入 $x$，先在查询带上写上 $\langle j,x,0^{q_j(|x|)}\rangle$，然后进入查询态，若查询结果使之进入是状态，则在接受停机状态停机；否则，若查询结果使之进入否状态，则在拒绝停机状态停机. 对给定了的 $s$，$j$ 是常数，可以看出上述确定型查询机是多项式时间界的查询机，故 $S\in P^B$（其实 $S\leqslant_1^p B$）.

由 $S$ 的任意性知，$NP^B\subseteq P^B$. 显然 $P^B\subseteq NP^B$，故 $P^B=NP^B$.

**定理 2.2**（相对不等可比定理） 对任意 01 串集合 $C$，存在 01 串集合 $D$，使 $C\leqslant_1^p D$ 且 $P^D\neq NP^D$.

**证明** 对于任意集合 $W$，定义语言 $L(W)$ 为：$L(W)=\{0^*|$存在 $y\in W$ 使 $|y|=n\}$. $L(W)$ 可由这样一台多项式界的非确定型查询机带上 $W$ 为天书来接受：对于任意一输入符号行 $x$，先判断 $x$ 是否全由“0”组成，若不是，则 $x\notin L(W)$，查询机在拒绝停机状态停机；若 $x$ 是全由“0”组成，则查询机不确定地在查询带上写上一个与 $x$ 等长度的串，之后进入查询态，若查询结果使之进入是状态，就在接受停机状态停机；否则，若查询结果使之进入否状态，就转入死循环，永不停机. 显然，若 $x\in L(W)$，则该查询机带上天书 $W$ 有计算过程在 $|x|$ 的多项式时间界内接受停机；若 $x\notin L(W)$，则所有计算过程都不停机. 因此该查询机带上天书 $W$ 能接受 $L(W)$. 上述查询机是多项式时间界的，故 $L(W)\in NP^W$.

我们用如下过程来构造集合 $D$，使 $C\leqslant_1^p D$ 且 $L(D)\notin P^D$：

第 0 步： $D_0:=\{x0^{|x|+1}|x\in C\}$；$n_0:=0$

第 $i+1$ 步： 选最小的偶数 $n$，使 $n>n_i$ 且 $q_i(n)<2^n$，其中 $q_i$ 为第 $i$ 号多项式时间界的确定型查询机的多项式时间界函数. 显然，这样的偶数 $n$ 是存在的.

以下我们用 $P_i^x(x)$ 记 $P_i^x$ 以 $x$ 输入的计算过程.

若 $P_i^{D_i}(0^n)$ 在接受停机状态停机，则令 $D_{i+1}:=D_i$；若 $P_i^{D_i}(0^n)$ 在拒绝停机状态停机，则令 $D_{i+1}:=D_i\cup\{x_i\}$，其中 $x_i$ 是在 $P_i^{D_i}(0^n)$ 中未被查询的、长为 $n$ 的、按经典序最前的 01 串. 由于 $q_i(n)<2^n$，长为 $n$ 的 01 串共有 $2^n$ 个，$P_i^{D_i}(0^n)$ 计算时间不大于 $q_i(n)$，因此 $P_i^{D_i}(0^n)$ 查询的串不多于 $q_i(n)$ 个，故这样的 $x_i$ 一定可以被找到.

令 $n_{i+1}:=2^n$.

这样经过无穷步之后得到的集合就是 $D$，我们可以将 $D$ 看成是由 $D_0$ 经无穷步逐步增加元

素扩充而成的.

因为 $D_0$ 的全部元素长度均为奇数，而从第 1 步起，每步加进 $D$ 中的元素长度均为偶数，所以有：对$\forall\ x, x\in C\Leftrightarrow x0^{|x|+1}\in D_0\Leftrightarrow x0^{|x|+1}\in D$，容易看出，$C\leqslant_1^p D$.

下面我们用反证法证明 $L(D)\notin P^D$.

假设 $L(D)\in P^D$，不妨设 $P_j^D$ 接受 $L(D)$. 我们考虑构造 $D$ 的过程中第 $j+1$ 步的偶数 $n$. 不难发现：$n_0<n_1<n_2<\cdots<n_j<n<2^n=n_{j+1}<n_{j+2}<n_{j+3}<\cdots$.

设 $q_j$ 为第 $j$ 号多项式时间界确定型查询机的多项式时间界函数，则：$q_j(n)<2^n=n_{j+1}<n_{j+2}<\cdots$.

我们能得知以下结论：

1. 长度为 $n$ 的串只能在第 $j+1$ 步加入到 $D$ 中，如果第 $j+1$ 步没有将长度为 $n$ 的串加入 $D$ 中，则 $D$ 中就没有长度为 $n$ 的串.

2. $P_j^D(0^n)$所查询的串的长度不会超过 $q_j(n)$，而第 $j+1$ 步以后加入 $D$ 中的元素的长度均超过了 $q_j(n)$，故都不会影响 $P_j^D(0^n)$的计算，即 $P_j^{D_{j+1}}(0^n)$与 $P_j^D(0^n)$相同.

3. $D_{j+1}$ 与 $D_j$ 或者相同(若 $P_j^{D_j}(0^n)$在接受停机状态停机)，即 $D_{j+1}=D_j$，或者 $D_{j+1}=D_j\cup\{x_i\}$，且 $x_j$ 为 $P_j^{D_j}(0^n)$中没有被查询的串，因此有 $P_j^{D_j}(0^n)$与 $P_j^{D_{j+1}}(0^n)$相同，从而 $P_j^{D_j}(0^n)$与 $P_j^D(0^n)$相同.

如果 $0^n\in L(D)$，则由 $L(D)$的定义知道，$D$ 中存在长度为 $n$ 的元素；又因为 $P_j^D$ 接受 $L(D)$，故 $P_j^D(0^n)$应在接受停机状态停机，从而 $P_j^{D_j}(0^n)$应在接受停机状态停机，由 $D$ 的构造知，$D$ 中因此不会有长度为 $n$ 的元素. 矛盾.

如果 $0^n\notin L(D)$，则由 $L(D)$的定义知，$D$ 中不存在长度为 $n$ 的元素；又因 $P_j^D$ 接受 $L(D)$，故 $P_j^D(0^n)$应在拒绝停机状态停机，从而 $P_j^{D_j}(0^n)$应在拒绝停机状态停机. 由 $D$ 的构造知，$D$ 中有长度为 $n$ 的元素 $x_j$. 矛盾.

因此，无论 $0^n\in L(D)$还是 $0^n\notin L(D)$都存在矛盾. 至此我们用反证法证明了 $L(D)\notin P^D$.

由于 $L(D)\in NP^D, L(D)\notin P^D$，故 $P^D\neq NP^D$

**定理 2.3**（相对一致定理） 对于任意两个 01 串集合 $A$ 和 $B$，有$(A\equiv_T^p B)\Leftrightarrow(P^A=P^B\ \&.\ NP^A=NP^B)$. 这里 $A\equiv_T^p B$ 表示 $A\leqslant_T^p B\ \&.\ B\leqslant_T^p A$.

**证明** ($\Rightarrow$)因 $A\equiv_T^p B$，有 $A\leqslant_T^p B, B\leqslant_T^p A$. 又 $A\leqslant_T^p B$，即 $A\in P^B$，不妨设 $P_i^B$ 接受 $A$.

对$\forall\ S\in P^A$，不妨设 $P_j^A$ 接受 $S$. 我们可如下构造一台多项式时间界的确定型查询机 $P_k^B$ 接受 $S$：$P_k^B$ 平时模拟 $P_j^A$ 工作，当 $P_j^A$ 进入查询状态时，$P_k^B$ 又对需查询的字模拟 $P_i^B$ 工作，当 $P_i^B$ 停机时 $P_k^B$ 根据 $P_i^B$ 是在接受停机状态还是在拒绝停机状态分别进入是状态或否状态，转回来模拟 $P_j^A$ 继续工作. 由于 $P_j^A$ 和 $P_i^B$ 都是多项式时间界的，故 $P_k^B$ 也是多项式时间界的.

由构造知，$P_k^B$ 接受 $S$，即 $S\in P^B$. 由 $S$ 的任意性知，$P^A\leqslant P^B$. 同理可证 $P^B\leqslant P^A$. 从而 $P^A=P^B$.

将上面的 $P_k^B$ 和 $P_j^A$ 都换成不确定的查询机进行模拟，可以证得 $NP^A\subseteq NP^B$. 同理可证 $NP^B\subseteq NP^A$ 故有 $NP^A=NP^B$.

($\Leftarrow$)由 $P^A=P^B$ 和 $A\in P^A$ 知 $A\in P^B$ 故 $A\leqslant_T^p B$；由 $P^A=P^B$ 和 $B\in P^B$ 知 $B\in P^A$ 故 $B\leqslant_T^p A$.

因此有 $A\equiv_T^p B$.

**定理 2.4**（天书等价定理） 对任意两个 01 串集合 $A$ 和 $B$，若 $A\equiv_T^p B$ 且 $P^A=NP^A$，则 $P^B=$

$NP^B$.

**证明** 此定理是相对一致定理的直接推论.

因 $A\equiv_T^p B$,故 $P^A=P^B$,$NP^A=NP^B$. 又 $P^A=NP^A$,故 $P^B=P^A=NP^A=NP^B$,即 $P^B=NP^B$.

天书等价定理表明,对任何一个多项式时间界的图灵等价类,或者其中所有集合都使 $P=NP$ 相对化,或者其中所有集合都使 $P\neq NP$ 相对化.

**推论** 2.5 存在一个集合序列 $A_0,B_0,A_1,B_1,A_2,B_2,\cdots$ 满足:$A_0<_T^p B_0<_T^p A_1<_T^p B_1<_T^p A_2<_T^p B_2<\cdots$,使得对所有非负整数 $i$ 有 $P^{A_i}=NP^{A_i}$ 且 $P^{B_i}\neq NP^{B_i}$. 这里 $A<_T^p B$ 表示 $A\leqslant_T^p B$ & $B\not\leqslant_T^p A$.

**证明** 我们考虑 01 串集合. 由定理 2.1 知,存在 $A_0$ 使 $P^{A_0}=NP^{A_0}$;由定理 2.2 知,存在 $B_0$ 使 $A_0\leqslant_1^p B_0$ 且 $P^{B_0}\neq NP^{B_0}$;由定理 2.4 知,$A_0\not\equiv_T^p B_0$;因 $A_0\leqslant_1^p B_0\Rightarrow A_0\leqslant_T^p B_0$,而 $A_0\not\equiv_T^p B_0$,故有 $A_0<_T^p B_0$;再由定理 2.1 知,存在 $A_1$ 使 $B_0\leqslant_1^p A_1$ 且 $P^{A_1}=NP^{A_1}$;再由定理 2.4 知,$A_1\not\equiv_T^p B_0$,从而 $B_0<_T^p A_1$.

以此类推,还存在满足推论 2.5 的 $B_1$、$A_2$、$B_2$、….

推论 2.5 说明,存在一个复杂度严格上升的集合序列,其中的集合交替地使 $P=NP$ 和 $P\neq NP$ 相对化.

## 三 相对天书定理

**定义** 3.1 对任意给定的集合 $A$,如果 $A$ 满足:(1) 在 $P=NP$ 的假设下,可推出 $P^A=NP^A$ 的结论;(2) 在 $P\neq NP$ 的假设下,可推出 $P^A\neq NP^A$ 的结论,则称 $A$ 为相对天书.

容易看出,空集就是相对天书.

**定理** 3.2 $NP-NPT$ 中的所有集合都是相对天书. 其中 $NPT$ 表示所有 $NP$ 图灵完全集组成的类.

**证明** 考虑$\forall$ $A\in NP-NPT$.

(1) 假设 $P=NP$,则 $A\in P$,就有 $A\equiv_T^p\varnothing$. 由定理 2.3(相对一致定理)知 $P^A=P^\varnothing$ & $NP^A=NP^\varnothing$ 而 $P^\varnothing=P$,$NP^\varnothing=NP$. 故有 $P^A=P^\varnothing=P=NP=NP^\varnothing=NP^A$ 即 $P^A=NP^A$.

(2) 假设 $P\neq NP$. 我们用反证法证明 $P^A\neq NP^A$.

对于$\forall$ $B\in NPT$,应有 $A<_T^p B$. 若 $P^A=NP^A$,则有 $B\in NP\subseteq NP^A=P^A$ 即 $B\in P^A$,亦即 $B\leqslant_T^p A$ 矛盾. 故应有 $P^A\neq NP^A$.

综合以上两点知,$A$ 为相对天书.

由 $A$ 的任意性知,$NP-NPT$ 中的所有集合都是相对天书.

**定义** 3.3 对任意给定的集合 $B$,如果 $B$ 满足:无论假设 $P=NP$ 还是 $P\neq NP$,都有 $P^B=NP^B$ 或有 $P^B\neq NP^B$ 的结论,即相对化的结论不随 $P=?\ NP$ 的假设不同而变化,则称 $B$ 为绝对天书.

我们用 $CO-NP$ 记所有补集属于 $NP$ 的集合组成的集合类.

**定理** 3.4 若 $NP=CO-NP$,则 $NPT$ 中所有集合都是绝对天书,它们使 $P=NP$ 相对化.

**证明** 对$\forall$ $A\in NPT$,记 $A$ 的补集为 $\overline{A}$. 由 $NP=CO-NP$ 知,$\overline{A}\in NP$. 不妨设 $NP_i$ 和 $NP_k$ 分别接受 $A$ 和 $\overline{A}$,设 $NP_j$ 和 $NP_k$ 的多项式时间界函数分别为 $q_j$ 和 $q_k$.

对$\forall$ $S\in NP^A$,不妨设 $NP_i^A$ 接受 $S$,其多项式时间界函数为 $q_i$.

我们可如下构造一台多项式时间界的非确定型图灵机 $NP_i$ 来接受 $S$：对任意输入 $x$，$NP_i$ 模拟 $NP_i^A$ 的计算. 当 $NP_i^A$ 进入查询状态时，设此时要查询的字符串为 $z$，$NP_i$ 不确定地模拟 $NP_j$ 和 $NP_k$ 对 $z$ 的计算. 因为 $NP_j$ 和 $NP_k$ 分别接受 $A$ 和 $\overline{A}$，故 $NP_i$ 存在不多于 $q_j(|z|)+q_k(|z|)$ 步的计算过程判断出 $z$ 是否属于 $A$. 之后，$NP_i$ 根据 $z$ 是否属于 $A$ 模拟 $NP_i^A$ 进入是状态(即 $z\in A$)或进入否状态(即 $z\in\overline{A}$)后的计算. 此过程直至 $NP_i^A$ 停机止.

由构造知，$NP_i^A$ 接受 $x$ 当且仅当 $NP_i$ 接受 $x$. 又 $NP_i^A$ 接受 $x$ 当且仅当 $NP_i^A$ 的某个计算过程接受 $x$，且该计算过程不多于 $q_i(|x|)$ 步，在这个计算过程中，$NP_i^A$ 至多进入查询状态 $q_i(|x|)$ 次，且查询的字长度不会超过 $q_i(|x|)$，故 $NP_i$ 有多项式时间界：

$$q_i(|x|)\cdot[q_j(q_i(|x|))+q_k(q_i(|x|))]+q_i(|x|).$$

因此 $S\in NP$.

由 $S$ 的任意性知，$NP^A\subseteq NP$. 又由于 $A\in NPT$，故 $NP\subseteq P^A\subseteq NP^A$ 从而有 $NP=P^A=NP^A$，即 $A$ 为绝对天书. 由 $A$ 的任意性知定理 3.4 成立.

**定理 3.5**（相对天书定理） 集合 $\{0^{2^i}|i=0,1,2,\cdots\}$ 的所有子集都是相对天书.

**证明** 对 $\forall\ A\subseteq\{0^{2^i}|i=0,1,2,\cdots\}$，我们在以下证明 $A$ 是相对天书.

(1) 假设 $P=NP$. 对 $\forall\ S\in NP^A$，不妨设 $S$ 被 $NP_j^A$ 接受，$NP_j^A$ 的多项式时间界函数为 $q_j$. 考虑集合 $H=\{\langle x,a_1,a_2,\cdots,a_y\rangle|NP_j^{\{a_1,a_2,\cdots,a_y\}}$ 接受 $x\}$，其中 $x,a_1,a_2,\cdots,a_y$ 都是 01 串.

我们如下构造一台多项式时间界非确定型图灵机 $NP_k$ 来接受 $H$：对任意输入 $z$，$NP_k$ 将 $z$ 解码成 $\langle x,a_1,a_2,\cdots,a_y\rangle$ 的形式(此过程需时间不多于 $z$ 的常数倍，设为 $c|z|$). 如解码不出这种形式，则 $z\notin H$，$NP_k$ 在拒绝停机状态停机；如解码出了，则令 $NP_k$ 模拟 $NP_j^{\{a_1,a_2,\cdots,a_y\}}(x)$ 的计算，当需查询时，$NP_k$ 将要查询的字符串与 $a_1,a_2,\cdots,a_y$ 逐一比较，然后 $NP_k$ 的下一步计算将模拟 $NP_j^{\{a_1,a_2,\cdots,a_y\}}(x)$ 进入是状态(若比较有相同的)或进入否状态(比较没有相同的)后的计算. 此过程直至 $NP_j^{\{a_1,a_2,\cdots,a_y\}}(x)$ 停机止.

$NP_j^{\{a_1,a_2,\cdots,a_y\}}(x)$ 的计算时间不会超过 $q_j(|x|)$，故查询天书不多于 $q_j(|x|)$ 次，每次查询的字符串不长于 $q_j(|x|)$，因此 $NP_k$ 每次模拟查询的时间不多于 $q_j(|x|)+|z|$ 的常数倍(设为 $c_1[q_j(|x|)+|z|]$). 故 $NP_k(z)$ 计算时间不多于

$$\begin{aligned}&c|z|+q_j(|x|)+q_j(|x|)\cdot c_1\cdot[q_j(|x|)+|z|]\\&<c|z|+q_j(|z|)+q_j(|z|)\cdot c_1\cdot[q_j(|z|)+|z|]\end{aligned}$$

故 $NP_k$ 为多项式时间界的.

由构造知，$NP_k$ 接受 $z$ 当且仅当 $NP_j^{\{a_1,a_2,\cdots,a_y\}}$ 接受 $x$，即当且仅当 $\langle x,a_1,a_2,\cdots,a_y\rangle\in H$. 而 $z=\langle x,a_1,a_2,\cdots,a_y\rangle$. 故 $NP_k$ 接受 $H$，从而 $H\in NP$.

因为已设 $P=NP$，所以又有 $H\in P$. 不妨设 $P_n$ 接受 $H$. $P_n$ 的多项式时间界函数为 $q_n$.

我们再如下构造一台多项式时间界的确定型查询机 $P_i^A$ 带上天书 $A$ 接受 $S$：

对于任意输入字符串 $x$，$NP_j^A(x)$ 的计算时间不多于 $q_j(|x|)$，故计算中可能查询的字符串长度不大于 $q_j(|x|)$，设 $a_1,a_2,\cdots,a_y$ 为 $A$ 中长度不大于 $q_j(|x|)$ 的全部元素，则有 $NP_j^A(x)=NP_j^{\{a_1,a_2,\cdots,a_y\}}(x)$，即 $x\in S\Leftrightarrow\langle x,a_1,a_2,\cdots,a_y\rangle\in H$.

又 $A$ 中元素形如 $0^{2^i}$，故 $a_1,a_2,\cdots,a_y$ 一共不多于 $q_j(|x|)$ 个，故

$$|\langle x,a_1,a_2,\cdots,a_y\rangle|\leqslant 2[|x|+q_j(|x|)(q_j(|x|)+1)]$$

$P_i^A$ 先依次查询所有长度不大于 $q_j(|x|)$ 的. 形如 $0^{2^i}$ 的串(不多于 $q_j(|x|)$ 个)是否属于 $A$, 从而找到全部 $a_1,a_2,\cdots,a_\varphi$ 是长度不大于 $q_j(|x|)$、属于 $A$ 的串. 此过程需时间不多于 $q_j^2(|x|)$ 的常数倍,不妨设为 $c_1q_j^2(|x|)$.

$P_i^A$ 再将 $x$ 与 $a_1,a_2,\cdots,a_\varphi$ 一起编码成 $\langle x,a_1,a_2,\cdots,a_\varphi\rangle$. 此过程需时间不多于 $|\langle x,a_1,a_2,\cdots,a_\varphi\rangle|$ 的常数倍,设为 $c_2|\langle x,a_1,a_2,\cdots,a_\varphi\rangle|$.

注意到 $P_e$ 接受 $II$,再 $P_i^A$ 模拟 $P_e(\langle x,a_1,a_2,\cdots,a_\varphi\rangle)$ 的计算直至停机止. 此过程需时间不多于 $q_e(|\langle x,a_1,a_2,\cdots,a_\varphi\rangle|)$.

如此构造的 $P_i^A$ 对输入串 $x$ 需时间不多于

$$\begin{aligned}&c_1q_j^2(|x|)+c_2|\langle x,a_1,a_2,\cdots,a_\varphi\rangle|+q_e(|\langle x,a_1,a_2,\cdots,a_\varphi\rangle|)\\&\leqslant c_1q_j^2(|x|)+c_2\cdot 2\cdot[|x|+q_j(|x|)\cdot|q_j(|x|)+1)]\\&\quad+q_e(2[|x|+q_j(|x|)\cdot(q_j(|x|)+1)]).\end{aligned}$$

故 $P_i^A$ 是多项式时间界的.

由构造知:$P_i^A$ 接受 $x\Leftrightarrow\langle x,a_1,a_2,\cdots,a_\varphi\rangle\in II\Leftrightarrow NP_j^{\{a_1,a_2,\cdots,a_\varphi\}}$ 接受 $x\Leftrightarrow NP_j^A$ 接受 $x\Leftrightarrow x\in S$. 所以 $P_i^A$ 接受 $S$. 从而 $S\in P^A$. 由 $S$ 的任意性知:$NP^A\subseteq P^A$. 从而 $P^A=NP^A$.

(2) 假设 $P\neq NP$

众所周知,$SAT$ 集(可满足的合取范式集合)是 $NP$ 完全集,故 $SAT\in NP$ &. $[(SAT\in P)\Leftrightarrow(P=NP)]$.

因此 $SAT\in NP^A$. 我们如能证明 $SAT\notin P^A$,就证明了 $P^A\neq NP^A$.

下面我们证明:若 $SAT\in P^A$,则 $SAT\in P$,从而 $P=NP$,产生矛盾. 这样就用反证法证明了 $SAT\notin P^A$,即 $P^A\neq NP^A$.

设 $SAT\in P^A$,不妨设 $P_j^A$ 接受 $SAT$,$P_j^A$ 的多项式时间界函数为 $q_j$.

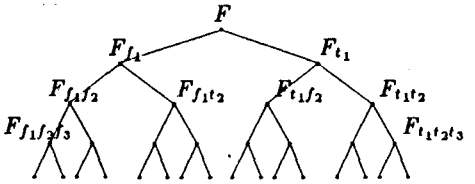
我们如下构造多项式时间界的确定型图灵机 $P_k$ 来接受 $SAT$:

对任意输入 $F$,$P_j^A(F)$ 的计算时间不多于 $q_j(|F|)$,因此计算中要查询的字的长度不大于 $q_j(|F|)$,设 $b_1,b_2,\cdots,b_l$ 是全部长度不大于 $q_j(|F|)$ 的形如 $0^{2^i}$ 的串,显然 $b_1,b_2,\cdots,b_l$ 一共不多于 $[\log_2q_j(|F|)]+1$ 个,且 $P_j^A(F)=P_j^{A\cap\{b_1,b_2,\cdots,b_l\}}(F)$.

设 $B_1,B_2,\cdots,B_{2^l}$ 为 $\{b_1,b_2,\cdots,b_l\}$ 的所有子集,则 $B_1,B_2,\cdots,B_{2^l}$ 一共不多于 $4q_j(|F|)$ 个集合,且其中之一为 $A\cap\{b_1,b_2,\cdots,b_l\}$.

$P_k$ 首先判断 $F$ 是否为一个合取范式的编码,若不是,则 $F\notin SAT$,这时 $P_k$ 进入拒绝停机状态;若是,$P_k$ 再进行下面的工作. 此过程需 $|F|$ 的多项式时间,设为 $q(|F|)$.

考虑 $F$ 的计算二叉树(如图所示),其根结点为 $F$. 设 $F$ 有 $n$ 个变元 $x_1,x_2,\cdots,x_n$. $F$ 的左儿子为 $F_{f_1}$,表示将 $F$ 中的变元 $x_1$ 赋值假设时得到的子公式. $F$ 的右儿子为 $F_{t_1}$,表示将 $F$ 中的 $x_1$ 赋值真时得到的子公式. $F_{f_1}$ 的左儿子为 $F_{f_1f_2}$,表示将 $F$ 中 $x_1,x_2$ 赋值假时得到的子公式. $F_{f_1}$ 的右儿子为 $F_{f_1t_2}$ 表示将 $F$ 中 $x_1$ 赋值假、$x_2$ 赋值真时得到的子公式. …



$F$ 的计算树的叶子为将 $F$ 的 $n$ 个变元赋值后的结果，为真值或假值. 如叶子中有真值的，则 $F\in SAT$，否则 $F\notin SAT$. 由 $SAT$ 的性质，可知：

若 $F\in SAT$，则 $F_{f_1}\in SAT$ 或 $F_{t_1}\in SAT$；

若 $F_{f_1}\in SAT$，则 $F_{f_1f_2}\in SAT$ 或 $F_{f_1t_2}\in SAT$；

… … …

$P_k$ 将依次模拟 $P_j^{B_1},P_j^{B_2},\cdots,P_j^{B_{2^l}}$. 若 $P_j^{B_1},P_j^{B_2},\cdots,P_j^{B_{2^l}}$ 都拒绝 $F$，则 $P_j^{A\cap\{b_1,b_2,\cdots,b_l\}}$ 也一定拒绝 $F$，从而 $P_j^A$ 拒绝 $F$，因而说明 $F\notin SAT$，$P_k$ 在拒绝停机状态停机.

若 $P_j^{B_1},P_j^{B_2},\cdots,P_j^{B_{2^l}}$ 不都拒绝 $F$，不妨设 $P_j^{B_2}$ 接受 $F$，则我们可在多项式时间内判断出 $F\in SAT$ 或 $B_2\neq A\cap\{b_1,b_2,\cdots,b_l\}$.

令 $P_k$ 模拟 $P_j^{B_2}(F_{f_1})$ 和 $P_j^{B_2}(F_{t_1})$ 的计算，若 $P_j^{B_2}$ 拒绝 $F_{f_1}$ 和 $F_{t_1}$，则说明 $B_2\neq A\cap\{b_1,b_2,\cdots,b_l\}$（因为若 $B_2=A\cap\{b_1,b_2,\cdots,b_l\}$，则 $F\in SAT$，这时 $F_{f_1}\in SAT$ 或 $F_{t_1}\in SAT$，$P_j^{B_2}$ 应接受 $F_{f_1}$ 或 $F_{t_1}$）；否则，不妨设 $P_j^{B_2}$ 接受 $F_{t_1}$，$P_k$ 再模拟 $P_j^{B_2}(F_{t_1f_2})$ 和 $P_j^{B_2}(F_{t_1t_2})$ 的计算，若 $P_j^{B_2}$ 拒绝 $F_{t_1f_1}$ 和 $F_{t_1t_2}$，则说明 $B_2\neq A\cap\{b_1,b_2,\cdots,b_l\}$；否则 $P_k$ 再模拟 $P_j^{B_2}$ 对 $F_{t_1f_2}$ 和 $F_{t_1t_2}$ 之中被 $P_j^{B_2}$ 接受的那一个的两儿子的计算 …. 如此下去，$P_k$ 至多经 $(2n+1)q_j(|F|)$ 步模拟和 $2n|F|$ 常数倍（不妨设为 $c\cdot 2n|F|$）的时间将 $F$ 转化为 $F_f$ 和 $F_{t_1}$，将 $F_{t_1}$ 转化为 $F_{t_1f_2}$ 和 $F_{t_1t_2}$… 的转化过程，就能找到 $F$ 的计算树上的真值叶子或证明 $B_2\neq A\cap\{b_1,b_2\cdots,b_l\}$. $P_k$ 若找到了真值叶子，就说明 $F$ 是可满足的，$P_k$ 就在接受停机状态停机. $P_k$ 若发现 $B_2\neq A\cap\{b_1,b_2\cdots,b_l\}$，则找另一个使 $P_j^{B_m}$ 接受 $F$ 的 $B_m$ 重复以上过程. 这样，$P_k$ 至多需时 $4q_j(|F|)[(2n+1)q_j(|F|)+c\cdot 2n\cdot|F|]$ 就能找到 $F$ 的计算树上的真值叶子或判断出所有使 $P_j^{B_m}$ 接受 $F$ 的 $\{b_1,b_2\cdots,b_l\}$ 的子集 $B_m$ 不是 $A\cap\{b_1,b_2\cdots,b_l\}$，前一种情况说明 $F\in SAT$，$P_k$ 在接受停机状态停机，后一种情况说明 $F\notin SAT$，$P_k$ 在拒绝停机状态停机.

$P_k$ 的多项式时间界函数为：

$$q_j(|F|)+4q_j(|F|)\cdot[(2n+1)q_j(|F|)+c\cdot 2n\cdot|F|].$$

下表为 $P_k$ 的计算过程的一个示例：

| | $b_1$ | $b_2$ | … | $b_l$ | $F$ | $F_{f_1}$ | $F_{t_1}$ | $F_{t_1f_1}$ | $F_{t_1t_2}$ | … | $F_{t_1t_2f_3}$ | … | $f_n$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $B_1$ | 0 | 0 | … | 0 | $f$ | | | | | | | | |
| $B_2$ | 0 | 0 | … | 1 | $t$ | $f$ | $f$ | | | | | | |
| | 0 | 1 | … | 0 | $t$ | $f$ | $t$ | $f$ | $t$ | … | $T$ | | |
| | 0 | 1 | … | 1 | $f$ | | | | | | | | |
| … | … | … | … | … | | | | | | | | | |
| $B_{2^l}$ | 1 | 1 | … | 1 | $f$ | | | | | | | | |

表中 $b_1b_2\cdots b_l$ 不多于 $\log_2 q_j(|F|)+1$ 个，$B_1,B_2,\cdots,B_{2^l}$ 不多于 $4q_j(|F|)$ 个；$P_k$ 模拟 $P_j^B$ 分别将 $B_1,B_2,\cdots,B_{2^l}$ 作为天书时，对 $F,F_{f_1},F_{t_1},\cdots$，的计算示例. 表中 $f$ 表示 $P_j^B$ 拒绝 $F_{f_1}$ 等，$t$ 表示接受，$T$ 表真值叶子.

由 $P_k$ 的构造知：$P_k$ 接受 $F\Leftrightarrow F\in SAT$，即 $P_k$ 接受 $SAT$. 故 $SAT\in P$，从而 $P=NP$，这与假设矛盾.

至此我们用反证法证明了 $SAT\notin P^A$，故 $P^A\neq NP^A$.

综上(1)、(2)二点知，$A$ 为相对天书. 由 $A$ 的任意性知，定理成立.

**定理 3.6** 存在 $NP$ 之外的递归集为相对天书.

**证明** 定义集合 $A$ 为：$A=\{0^{2^i}\mid NP_i(0^{2^i})$的所有计算过程在 $i+(2^i)^i$步内不会接受停机$\}$显然，这样定义的 $A$ 是递归的.

因 $A\subseteq\{0^{2^i}\mid i=0,1,2,3,\cdots\}$，由定理 3.5 知，$A$ 为相对天书.

以下用反证法证明 $A\notin NP$，即 $A$ 在 $NP$ 之外.

设 $A\in NP$，不妨设 $NP_j$ 接受 $A$，$NP_j$ 的多项式时间界函数为 $q_j$. 一定存在一个常数 $t$，对任意数 $n\geqslant t$ 和任意自然数 $m$，有 $q_j(m)\leqslant n+m^n$ 成立. 众所周知，存在无穷多的 $NP_i$，其对任何输入，计算过程与 $NP_j$ 的一样(Pading 引理). 设 $i\geqslant t$，且 $NP_i$ 与 $NP_j$ 对任何输入，其计算过程都相同，则 $NP_i$ 也接受 $A$ 且 $NP_i$ 的时间界函数也为 $q_j$. 注意到对任何自然数 $m$ 有 $q_j(m)\leqslant i+m^i$.

考虑字符串 $0^{2^i}$，若 $0^{2^i}\in A$，则 $NP_i$ 接受 $0^{2^i}$，即 $NP_i(0^{2^i})$的某个计算过程在 $q_j(2^i)$步内会接受停机，亦即 $NP_i(0^{2^i})$的某个计算过程会在 $i+(2^i)^i$步内接受停机，这与 $A$ 的定义相矛盾. 若 $0^{2^i}\notin A$，则 $NP_i$ 拒绝 $0^{2^i}$，即 $NP_i(0^{2^i})$的所有计算过程都不会接受停机，根据 $A$ 的定义又应有 $0^{2^i}\in A$，亦矛盾.

至此，我们用反证法证明了 $A$ 是 $NP$ 之外的集合.

综上知 $A$ 是 $NP$ 之外的递归集，又是相对天书.

## 参 考 文 献


[1] Theodore Baker, John Gill and Robert Solovay, *Relativizations of the P=? NP question*, SIAM J. Comput., 4; 4(1975), 431—442.

[2] Richard E. Ladner, *On the structure of polynomial time reducibility*, J. ACM 22; 1(1975), 155—171.

[3] 李赓，关于空间有界图灵机的细分非确定性，兰州大学学报，22; 2(1986)，10—14.

[4] Li Xiang, *Some properties on the class of NP turing complete sets*, Recurive Function Theory, Newsletter (1986), 13—14.


# Note on the $P=?NP$ Problem Relativized


*Song Enmin* *Jin Renchao* *Huang Wenqi*

(Dept. of Computer, Huazhong Univ. of Scie. and Tech., Wuhan)



## Abstract

The $P=?NP$ problem relativized can have two opposite results with the difference of oracle sets. In this paper, we get the results as follows:

1. There exists an infinite series of sets $S_1, S_2, \cdots$, whose complexity is strictly increasing, and if they become oracles, they can make the $P=?NP$ and $P\neq NP$ relativized alternately.

2. There exists recursive oracle $A$ out of $NP$ such that $P=NP$ equals $P^A=NP^A$.