Theorem 5:

Es gibt A mit $P^A = NP^A$.

Beweis:

Sei $A := \{(T, x, 1^k) | T$ DTM die x akzeptiert und dabei höchstens k Bandzellen verbraucht$\}$

Natürlich ist $P^A \subseteq NP^A$, per Definition. Bleibt also zu zeigen, daß $NP^A \subseteq P^A$.

Sei nun L eine beliebige Sprache in NP^A. Also gibt es eine Orakel-NTM T mit $L = L(T^A)$, $TIME_T(x) \leq p(|\, x|)$ für ein Polynom p.

Wir bauen daraus jetzt eine DTM T', die $L(T^A)$ ohne Orakel erkennt und dabei höchstens $q(|x|)$ Bandzellen beschreibt. (q Polynom).

Damit ist $L = P^A$ mit Algorithmus:

input x
schreibe $(T', x, 1^{q(|x|)})$ aufs Anfrageband
akzeptiere falls in A, sonst verwirf

Was aber soll T' machen?

Wir lassen es den Berechnungsbaum von T durchsuchen (analog zu Theorem 5, Kapitel 1).

Jeder globale Zustand von T braucht höchstens $p(|x|)$ viel Platz auf dem Band. Die Simulation braucht also $O(p(|x|)) \leq q(|x|)$ Bandzellen (wähle q groß genug).

Und was ist mit den Orakel-Anfragen?

Wenn T die Anfrage $(T^*, x^*, 1^{k^*})$ stellt, dann ist insbesondere $k^* \leq p(|x|)$. Also lassen wir T' bei Eingabe x^* die Maschine T^* einfach simulieren. Da $k^* \leq q(|x|)$, ist dies möglich ohne mehr als $q(|\, x|)$ Bandzellen zu verbrauchen.

$\Rightarrow$ T' entscheidet ob $X \in L$.

Der Algorithmus von oben entscheidet L in polynomieller Zeit, also $NP^A \subseteq P^A$. $\square$

Theorem 6:

Es gibt ein Orakel $B \subseteq \{0,1\}^*$ mit $P^B \neq NP^B$.

Beweis:

Für $B \subseteq \{0,1\}^*$ definiere $L_B := \{0^n | \exists x \in B : |x| = n\}$.

Offensichtlich ist $L_B \in NP^B$, nämlich so:

input w
falls $w \neq 0^*$ verwerfe
sonst rate x mit $|x| = |w|$
akzeptiere, falls $x \in B$, sonst verwerfe

Bleibt B zu konstruieren mit $L_B \notin P^B$.

Sei dazu $T_0, T_1, T_2 ...$ eine Aufzählung von Orakel-DTM's derart, daß für jedes Orakel $X \subseteq \{0,1\}^*$gilt:

- $P^X = \{T_0^X, T_1^X \dots T_i^X \dots\}$
- für alle x und k hält T_k^X bei Eingabe x nach höchstens $|x|^k + k$ Schritten

B wird induktiv definiert:

$B := \bigcup_{i \in \mathbb{N}} B_i$, gemeinsam mit Schranken n_i mit $\forall x \in B_i : |x| \leq n_i$

$B_0 := \emptyset$, $n_0 := 0$.

$n_{i+1} := \min\{m | m > n_i^i + i, 2^m > m^{i+1} + (i+1)\}$

Um B_{i+1} zu definieren, betrachte die Berechnung von T_{i+1} bei Eingabe $0^{n_{i+1}}$.

Falls sie akzeptiert, so setze $B_{i+1} = B_i$.

Verwirft sie, dann wähle ein y_{i+1} mit $|y_{i+1}| = n_{i+1}$ für das die Berechnung nicht das Orakel befragt und setze $B_{i+1} := B_i \cup \{y_{i+1}\}$. So ein y_{i+1} existiert immer, da $T_{i+1}^{B_i}$ nur $n_{i+1}^{i+1} + i + 1 < 2^{n_{i+1}}$ Anfragen an das Orakel stellt.

Beobachtung:

Für alle i ist die Berechnung von $T_i^{B_i}$ bei Eingabe 0^{n_i} die gleiche wie von $T_i^{B_{i-1}}$ bei 0^{n_i}.

Denn $y_i \in B_i \backslash B_{i-1}$ wird von $T_i^{B_i}$ bei 0^{n_i} nicht befragt

Worte in $B \backslash B_i$ haben eine Länge $\geq n_{i+1} > n_i^i + i$, also hat T_i nicht genug Zeit, diese anzufragen.

Zu zeigen: $L_B \notin P^B$.

Sei also $L_B \in P^B$. Dann ist $L_B = L(T_j^B)$ für ein $j \in \mathbb{N}$.

Betrache $T_j^B(0^{n_j}) = T_j^{B_j}(0^{n_j})$.

Falls akzeptiert, dann gibt es in B kein Wort der Länge n_j, also $0^{n_j} \notin L_B$.

Falls verwirft, dann ist $y_j \in B$ mit $|y_j| = n_j$, also $0^{n_j} \in L_B$.

Also akzeptiert T_j^B nicht L_B!! Widerspruch

$\Rightarrow$ Somit ist $L_B \notin P^B$. $\square$

Ähnlich lassen sich alle möglichen Verhältnisse zwischen P, NP und co-NP relativ zu einem Orakel herstellen, z.B.:

$NP^C = co - NP^C$, aber $P^C \neq (co) - NP^C$	für ein C
$NP^D \neq co - NP^D, P^D = NP^D \cap co - NP^D$	für ein D
$NP^E \neq co - NP^E, P^E \neq NP^E \cap co - NP^E$	für ein E