

## Ergänzung zum Abschnitt 13.5

Definition 13.5.1, Satz 13.5.2 und Lemma 13.5.3 wurden wie im Skript behandelt. Wir diskutieren zunächst die Folgerungen aus Lemma 13.5.3, die wir erhalten, wenn wir die Existenz von polynomiellen Schaltkreisen für SAT annehmen.

Im Folgenden sei eine Codierung von Eingaben für SAT festgelegt. Ein polynomieller Schaltkreis für SAT ist eine Folge  $C_0, C_1, \dots$  von Schaltkreisen, wobei wir davon ausgehen, dass der Schaltkreis  $C_i$  als Eingabe eine Codierung einer Formel (=Konjunktion von Klauseln) bekommt, wobei die Länge der Codierung höchstens  $i$  ist. Sei  $M$  die Orakelturingmaschine aus dem Beweis der Selbstreduzierbarkeit für SAT. Wir bezeichnen mit  $L(M, C_m)$  die Sprache, die von dieser Turingmaschine akzeptiert wird, wenn sie anstelle der Orakelaufrufe den Schaltkreis  $C_m$  auswertet. Wenn  $M$  polynomiell zeitbeschränkt ist und  $C_m$  polynomielle Größe hat, kann man (durch Simulation) für jede Eingabe  $x$  mit  $|x| \leq m$  in polynomieller Zeit testen, ob  $x \in L(M, C_m)$  ist.

Wie schon früher sei genau dann  $L(M, C_m)(w) = 1$ , wenn  $w \in L(M, C_m)$ , und ansonsten 0. Dann gilt:

$$\forall \text{ Codierungen } w \text{ mit Länge höchstens } m : L(M, C_m)(w) = C_m(w). \quad (1)$$

D.h., wir erhalten auf  $w$  dasselbe Ergebnis, wenn wir den Schaltkreis  $C_m$  auswerten oder wenn wir die Orakelturingmaschine  $M$  mit Orakel  $C_m$  laufen lassen. Diese Eigenschaft von Schaltkreisen für SAT (oder allgemeiner von Schaltkreisen für polynomiell selbstreduzierbare Sprachen) wird auch als Selbsttest-Eigenschaft bezeichnet. Lemma 13.5.3 besagt, dass bereits aus der Bedingung (1) folgt, dass  $C_m$  für Eingaben mit Länge höchstens  $m$  das Problem SAT berechnet. Im folgenden Beweis werden wir den Ausdruck

$$\exists \text{ Schaltkreis } S \text{ polynomieller Größe } \forall w, |w| \leq m : L(M, S)(w) = S(w) \quad (2)$$

benutzen. Wenn SAT polynomielle Schaltkreise  $C_0, C_1, \dots$  hat, erfüllt  $C_m$  für  $S$  eingesetzt die Bedingung in (2). Aus Lemma 13.5.3 folgt, wie eben gesagt, dass ein Schaltkreis  $S$  in (2) auf Eingaben mit Länge höchstens  $m$  das Problem SAT löst. Wir werden diesen Ausdruck in die  $\Sigma_3$ -Charakterisierung einer Sprache integrieren, die sich durch die Verwendung von  $S$  in eine  $\Sigma_2$ -Charakterisierung umformen lässt. Da  $S$  hinter einem Existenzquantor steht, braucht der verwendete polynomielle Schaltkreis für SAT nicht bekannt und auch nicht einmal berechenbar zu sein.

**Satz:**  $\text{SAT} \in P/Poly \Rightarrow \Sigma_2 = \Sigma_3$ .

**Beweis:** Sei  $C_0, C_1, \dots$  eine Folge von polynomiellen Schaltkreisen für SAT mit den o.g. Eingabekonventionen. Es genügt zu zeigen, dass  $\Sigma_3 \subseteq \Sigma_2$  folgt. Sei also  $L \in \Sigma_3$ . Nach Satz 7.3.11 gibt es ein Polynom  $p$  und eine Sprache  $B \in \mathbf{P}$ , so dass

$$L = \{x \mid \exists y, |y| \leq p(|x|), \forall z, |z| \leq p(|x|), \exists z', |z'| \leq p(|x|) : (x, y, z, z') \in B\}.$$

Aufgrund der Charakterisierung von NP in Satz 3.2.10 gibt es eine Sprache  $R \in \text{NP}$ , so dass

$$L = \{x \mid \exists y, |y| \leq p(|x|), \forall z, |z| \leq p(|x|) : (x, y, z) \in R\}.$$

Da SAT NP-vollständig ist, gilt  $R \leq_p \text{SAT}$ , d.h., es gibt eine polynomiell berechenbare Funktion  $f$ , so dass  $f(x, y, z)$  eine Konjunktion von Klauseln ist, die genau dann erfüllbar ist, wenn  $(x, y, z) \in R$ . Dabei ist die Größe von  $f(x, y, z)$  polynomiell in der Länge von  $(x, y, z)$  beschränkt. Wir gehen o.B.d.A. davon aus, dass die Länge der Codierung von  $f(x, y, z)$  durch  $p(|x|)$  beschränkt ist. Im Folgenden unterscheiden wir nicht mehr explizit zwischen  $f(x, y, z)$  und seiner Codierung. Wir erhalten:

$$L = \{x \mid \exists y, |y| \leq p(|x|), \forall z, |z| \leq p(|x|) : f(x, y, z) \text{ erfüllbar}\}. \quad (3)$$

Um zu zeigen, dass  $L \in \Sigma_2$ , beweisen wir die folgende Charakterisierung von  $L$ . Sei  $M$  wieder die Orakelturingmaschine aus dem Beweis der Selbstreduzierbarkeit von SAT.

$$\begin{aligned} L = \{x \mid \exists \text{ Schaltkreis } S \text{ polynomieller Größe } \exists y, |y| \leq p(|x|), \\ \forall w, |w| \leq p(|x|), \forall z, |z| \leq p(|x|) : \\ \text{(a) } L(M, S)(w) = S(w) \text{ und} \\ \text{(b) } S(f(x, y, z)) = 1\}. \end{aligned} \quad (4)$$

Zunächst beachten wir, dass die Bedingungen (a) und (b) in polynomieller Zeit getestet werden können, da es sich um die Simulation einer polynomiell zeitbeschränkten Orakelturingmaschine mit einem durch einen polynomiellen Schaltkreis ersetzten Orakel und um die Simulation von polynomiellen Schaltkreisen handelt. Also handelt es sich um eine Charakterisierung nach Satz 7.3.11, d.h., es folgt  $L \in \Sigma_2$ .

Es bleibt die Korrektheit der Charakterisierung zu zeigen. Wir beginnen mit der Inklusion „ $\subseteq$ “. Sei  $x \in L$  gegeben. Als Schaltkreis  $S$  wählen wir den polynomiellen Schaltkreis  $C_{p(|x|)}$  für SAT; dieser erfüllt nach der Vorbetrachtung die Bedingung (a) für alle  $w$  mit  $|w| \leq p(|x|)$ . Da  $x \in L$ , gibt es wegen (3) ein  $y, |y| \leq p(|x|)$ , so dass für alle  $z, |z| \leq p(|x|)$ , die Formel  $f(x, y, z)$  erfüllbar ist. Da die Länge von  $f(x, y, z)$  durch  $p(|x|)$  beschränkt ist, berechnet der Schaltkreis  $S$  für SAT auf dieser Formel eine 1.

Wir zeigen nun die Inklusion „ $\supseteq$ “. Das Wort  $x$  erfülle also die Charakterisierung (4). Da nach dieser Charakterisierung

$$\forall w, |w| \leq p(|x|) : L(M, S)(w) = S(w),$$

berechnet der Schaltkreis  $S$  nach Lemma 13.5.3 für Eingaben mit Länge höchstens  $p(|x|)$  das Problem SAT. Wegen Bedingung (b) gibt es ein  $y, |y| \leq p(|x|)$ , so dass für alle  $z, |z| \leq p(|x|)$  die Formel  $f(x, y, z)$  erfüllbar ist. Wegen (3) folgt  $x \in L$ .