Grundlagen der theoretischen Informatik

Kurt Sieber

Fakultät IV, Department ETI
Universität Siegen

SS 2013

Vorlesung vom 16.05.2013

Kontextfreie Sprachen

Die Beispiele zeigen, dass es kontextfreie Sprachen gibt, die *nicht* regulär sind.

Wir beweisen jetzt: Jede reguläre Sprache ist kontextfrei.

Um reguläre Sprachen zu erzeugen, reichen sehr spezielle Grammatiken aus.

Definition 2.50 *Eine Grammatik heißt* rechtslinear, *wenn jede Produktion von der Form $A \to aB$ oder $A \to \varepsilon$ (mit $A, B \in N$ und $a \in \Sigma$) ist. Sie heißt* linkslinear, *wenn jede Produktion von der Form $A \to Ba$ oder $A \to \varepsilon$ ist.*

In der Literatur sind oft noch Produktionen anderer Art in rechtslinearen Grammatiken zugelassen, etwa $A \to a$, $A \to B$ oder $A \to wB$ mit $w \in \Sigma^*$. Analog für linkslineare Grammatiken. Dadurch werden die Grammatiken nicht mächtiger.

Beispiel:

Sei $L = \{a^{2n} \mid n \geq 0\}$
und $G = (\{a\}, \{S_0, S_1\}, S_0, P)$ mit $P = \{S_0 \to aS_1, S_1 \to aS_0, S_0 \to \varepsilon\}$

Behauptung: $L(G) = L$.

Beweis:

'$\subseteq$': Jedes aus S_0 ableitbare Wort, das nicht in $\{a\}^*$ liegt, hat die Form $a^{2n}S_0$ oder $a^{2n+1}S_1$. (Induktion über die Länge der Ableitung).

Da jedes $w \in L(G)$ nur mit Produktion $S_0 \to \varepsilon$ aus einem solchen Wort entstehen kann, muss $w = a^{2n}$ sein für ein $n \geq 0$.

'$\supseteq$': Für jedes $n \geq 0$ gilt

$$S_0 \Rightarrow aS_1 \Rightarrow aaS_0 \Rightarrow \ldots \Rightarrow a^{2n}S_0 \Rightarrow a^{2n} \qquad \square$$

Am Beispiel sieht man, dass die Nichtterminalzeichen einer rechtslinearen Grammatik eine ähnliche Rolle spielen wie die Zustände eines endlichen Automaten.

In jedem Ableitungsschritt (außer dem letzten) wird ein Terminalzeichen erzeugt und das Nichtterminalzeichen am Ende des Wortes wird eventuell verändert.

So kann man sich im Nichtterminalzeichen eine Information über die bereits erzeugten Terminalzeichen merken.

Im Beispiel: S_0 bedeutet, dass bisher eine gerade Anzahl von as erzeugt wurde, S_1 bedeutet, dass eine ungerade Anzahl von as erzeugt wurde.

Satz 2.51

1. *Zu jedem NDEA A kann man eine rechtslineare Grammatik G mit $L(G) = L(A)$ konstruieren.*
2. *Zu jeder rechtslinearen Grammatik G kann man einen NDEA A mit $L(A) = L(G)$ konstruieren.*

Beweis:

1. Sei $A = (\Sigma, Q, s, F, \Delta)$ ein NDEA.

   Wir dürfen annehmen, dass $\Sigma \cap Q = \emptyset$.

   Sei $G = (\Sigma, Q, s, P)$ mit

   $P = \{p \to aq \mid (p, a, q) \in \Delta\} \cup \{p \to \varepsilon \mid p \in F\}$

   Dann folgt durch eine einfache Induktion über $|w|$:

$$p \overset{*}{\Rightarrow}_G wq \;\Leftrightarrow\; (p, w) \vdash (q, \varepsilon) \qquad (*)$$

Also gilt

$$
\begin{array}{rcl}
w \in L(G) & \Leftrightarrow & s \overset{*}{\Rightarrow}_G w \\
& \Leftrightarrow & \text{es existiert ein } p \in Q \text{ mit } s \overset{*}{\Rightarrow}_G wp \Rightarrow w \\
& & \text{und } (p \to \varepsilon) \in P \\
& & \text{(weil der letzte Ableitungsschritt nur mit einer} \\
& & \ \varepsilon\text{-Produktion erfolgen kann)} \\
& \Leftrightarrow & \text{es existiert ein } p \in Q \text{ mit } (s, w) \vdash_A^* (p, \varepsilon) \\
& & \text{und } p \in F \\
& & \text{(wegen (*) und der Definition von } P\text{)} \\
& \Leftrightarrow & w \in L(A)
\end{array}
$$

und damit ist $L(G) = L(A)$ bewiesen.

2. Sei $G = (\Sigma, N, S, P)$ eine rechtslineare Grammatik.

   Wir definieren $A = (\Sigma, N, S, F, \Delta)$ mit

   $F = \{B \in N \mid (B \to \varepsilon) \in P\}$ und

   $\Delta = \{(B, a, C) \in N \times \Sigma \times N \mid (B \to aC) \in P\}$

   Dann folgt durch eine einfache Induktion über $|w|$:

$$B \overset{*}{\Rightarrow}_G wC \iff (B, w) \vdash_A^* (C, \varepsilon)$$

   und ähnlich wie oben ergibt sich $L(A) = L(G)$ $\square$

Damit haben wir eine weitere Charakterisierung regulärer Sprachen.

Korollar 2.52 *Eine Sprache ist genau dann regulär, wenn sie sich von einer rechtslinearen Grammatik erzeugen lässt.*

Außerdem ist damit natürlich beweisen, dass jede reguläre Sprache kontextfrei ist, also gilt

Satz 2.53 $\mathcal{L}_{reg} \subseteq \mathcal{L}_{kf}$

wobei $\mathcal{L}_{kf}$ die Klasse der kontextfreien Sprachen bezeichnet.

Unsere Beispiele zeigen, dass diese Inklusion echt ist, wenn das Alphabet Σ mindestens zwei Elemente enthält. (Bei einelementigem Alphabet stimmen die beiden Sprachklassen überein.)

Definition 2.54 *Ein* Kellerautomat *(engl.* pushdown automaton *oder* PDA*) ist ein 6-Tupel* $M = (\Sigma, \Gamma, Q, s, F, \Delta)$ *mit:*

- Σ *ist ein Alphabet (das* Eingabealphabet*)*
- Γ *ist ein Alphabet (das* Kelleralphabet*)*
- Q *ist eine endliche Menge (von* Zuständen*)*
- $s \in Q$ *(der* Startzustand*)*
- $F \subseteq Q$ *(Menge der* Endzustände *oder* akzeptierenden Zustände*)*
- Δ *ist eine* endliche *Teilmenge von* $(Q \times \Sigma^* \times \Gamma^*) \times (Q \times \Gamma^*)$

Δ *heißt* Übergangsrelation *von* M*, die Elemente von* Δ *heißen* Übergänge *oder* Transitionen *von* M*.*

Man beachte: Ein Kellerautomat kann ‘extrem nichtdeterministisch’ sein, weil die Übergangsrelation Δ ähnlich wie die eines ε-NDEA ‘spontane Zustandsübergänge’ erlaubt, bei denen sowohl das Eingabewort als auch der Kellerinhalt ignoriert werden.

Intuition für die Übergänge:

$((p, u, \beta), (q, \gamma)) \in \Delta \subseteq (Q \times \Sigma^* \times \Gamma^*) \times (Q \times \Gamma^*)$ bedeutet:

Wenn der Kellerautomat M

- sich im Zustand p befindet,
- das aktuelle Eingabewort mit u beginnt
- und der aktuelle Kellerinhalt mit β,

dann darf er in einem Übergangsschritt

- u entfernen,
- in den Zustand q wechseln
- und β durch γ ersetzen.

Dabei wird der Kellerinhalt von oben nach unten gelesen, d.h. β besteht aus den ersten Zeichen, die *oben* im Keller stehen.

Spezialfälle:

- $u = \varepsilon$:

  Das aktuelle Eingabewort wird ignoriert und bleibt unverändert.

- $\beta = \varepsilon$:

  Der aktuelle Kellerinhalt wird ignoriert und mit γ aufgefüllt.

- $\gamma = \varepsilon$:

  β wird durch ε ersetzt, d.h. vom Keller entfernt.

- $\beta = \gamma$:

  Der aktuelle Kellerinhalt bleibt unverändert.

- $\beta = \alpha\gamma$:

  $\alpha\gamma$ wird durch γ ersetzt, d.h. α wird vom Keller entfernt.

- $\gamma = \alpha\beta$:

  β wird durch $\alpha\beta$ ersetzt, d.h. der aktuelle Kellerinhalt wird mit α aufgefüllt.

Definition 2.55 *Sei $M = (\Sigma, \Gamma, Q, s, F, \Delta)$ ein Kellerautomat.*

1. *Eine* Konfiguration *von M ist ein Element $(q, w, \alpha) \in Q \times \Sigma^* \times \Gamma^*$.*

   Intuition: q ist der aktuelle Zustand, w das aktuelle Eingabewort und α der aktuelle Kellerinhalt.

2. *Die Relation $\vdash_M$ (oder kurz: $\vdash$) auf der Menge der Konfigurationen ist wie folgt definiert:*

   Wenn $((p, u, \beta), (q, \gamma)) \in \Delta$, dann gilt für alle $v \in \Sigma^*$ und $\alpha \in \Gamma^*$:

$$(p, uv, \beta\alpha) \ \vdash_M \ (q, v, \gamma\alpha)$$

   und das sind die einzigen Konfigurationen, die in Relation $\vdash_M$ stehen.

Ein Paar $(p, uv, \beta\alpha) \vdash_M (q, v, \gamma\alpha)$ heißt Übergangsschritt *von M.*
$\vdash_M^n$ $(n \geq 0,)$ $\vdash_M^+$ und $\vdash_M^*$ sind wie üblich definiert.

Beispiel:

Sei $M = (\Sigma, \Gamma, Q, s, F, \Delta)$ mit

- $\Sigma = \Gamma = \{a, b\}$
- $Q = \{s, f\}$
- $F = \{f\}$
- $\Delta = \{$

$((s, a, \varepsilon), (s, a)),$	(1)	a in den Keller verschieben
$((s, \varepsilon, \varepsilon), (f, \varepsilon)),$	(2)	spontaner Zustandswechsel
$((f, b, a), (f, \varepsilon))\ \}$	(3)	b gegen a aufheben

Dann gilt z.B.

$$
\begin{array}{rlll}
(s, aabb, \varepsilon) & \vdash_M & (s, abb, a) & \text{mit (1)} \\
& \vdash_M & (s, bb, aa) & \text{mit (1)} \\
& \vdash_M & (f, bb, aa) & \text{mit (2)} \\
& \vdash_M & (f, b, a) & \text{mit (3)} \\
& \vdash_M & (f, \varepsilon, \varepsilon) & \text{mit (3)}
\end{array}
$$

Definition 2.56 *Sei $M = (\Sigma, \Gamma, Q, s, F, \Delta)$ ein Kellerautomat.*

1. *M akzeptiert das Wort $w \in \Sigma^*$, wenn ein $q \in F$ existiert mit $(s, w, \varepsilon) \vdash^* (q, \varepsilon, \varepsilon)$.*
2. *$L(M) = \{w \in \Sigma^* \mid M \text{ akzeptiert } w\}$ heißt die von M akzeptierte oder erkannte Sprache.*

In Worten: M startet im Startzustand s mit dem Wort w auf dem Eingabeband und mit leerem Keller. w wird akzeptiert, wenn M einen Endzustand q erreichen kann, so dass sowohl das Eingabeband als auch der Keller leer sind.

Beispiel:
Der oben definierte Kellerautomat M akzeptiert das Wort $aabb$, weil $(s, aabb, \varepsilon) \vdash_M^* (f, \varepsilon, \varepsilon)$ und $f \in F$. Er 'errät' dabei den Zeitpunkt, in dem er vom Zustand s in den Zustand f wechselt.

Behauptung: $L(M) = \{a^n b^n \mid n \geq 0\}$.

Beweis:

'$\supseteq$': Sei $n \geq 0$. Dann gilt (auch für $n = 0$):

$$\begin{array}{llll} (s, a^n b^n) & \vdash_M^n & (s, b^n, a^n) & \text{mit (1)} \\ & \vdash_M & (f, b^n, a^n) & \text{mit (2)} \\ & \vdash_M^n & (f, \varepsilon, \varepsilon) & \text{mit (3)} \end{array}$$

'$\subseteq$': Sei $w \in L(M)$, d.h. $(s, w, \varepsilon) \vdash_M^* (f, \varepsilon, \varepsilon)$, da f einziger Endzustand ist. In $\vdash_M^*$ muss genau ein Schritt mit Transition (2) vorkommen, davor können nur (1)-Schritte stehen, dahinter nur (3)-Schritte. Also existieren $n \geq 0$, $v \in \Sigma^*$ mit $w = a^n v$ und

$$(s, w, \varepsilon) \ \vdash_{(1)}^* \ (s, v, a^n) \ \vdash_{(2)} \ (f, v, a^n) \ \vdash_{(3)}^* \ (f, \varepsilon, \varepsilon)$$

Das kann aber nur gelten, wenn $v = b^n$, also $w = a^n b^n$. □

Anmerkungen zur Literatur:

Sowohl die Definition des Kellerautomaten als auch die Definition des Akzeptierens variieren stark in der Literatur.

- Unsere Kellerautomaten sind sehr flexibel:

  Sowohl vom Eingabeband als auch vom Keller darf in jedem Schritt ein ganzes Wort (auch ε) gelesen werden. Oft wird stattdessen

  $$\Delta \subseteq (Q \times (\Sigma \cup \{\varepsilon\}) \times \Gamma) \times (Q \times \Gamma^*)$$

  gefordert. Das setzt natürlich voraus, dass im Keller stets mindestens ein Zeichen steht, d.h. man benötigt ein spezielles Startzeichen, das zu Beginn schon im Keller steht.

- Unsere Definition des Akzeptierens ist sehr streng:

  Der Kellerautomat muss im Endzustand sein *und* der Keller muss leer sein. Oft wird nur eins von beiden gefordert.

Man kann sich davon überzeugen, dass solche unterschiedlichen Definitionen zur gleichen Sprachklasse führen.

Weiteres Beispiel:

Sei $L = \{w \in \{a,b\}^* \mid \#_a(w) = \#_b(w)\}$.

Sei $M = (\Sigma, \Gamma, Q, s, F, \Delta)$ mit

- $\Sigma = \Gamma = \{a,b\}$
- $Q = F = \{s\}$
- $\Delta = \{$ $((s,a,\varepsilon),(s,a))$, (1) a in den Keller verschieben

  $((s,b,\varepsilon),(s,b))$, (2) b in den Keller verschieben

  $((s,a,b),(s,\varepsilon))$, (3) a gegen b aufheben

  $((s,b,a),(s,\varepsilon))$ $\}$ (4) b gegen a aufheben

Behauptung: $L = L(M)$.

Beweis:

'$\subseteq$': Man *kann* die Übergangsschritte stets so wählen, dass im Keller der Überschuss an as bzw. bs des bisher gelesenen Wortes steht, d.h. wenn $w \in \Sigma^*$ mit $\#_a(w) = m$ und $\#_b(w) = n$, dann gilt:

$(s, w, \varepsilon) \ \vdash_M^* \ (s, \varepsilon, a^{m-n})$ falls $m \geq n$

$(s, w, \varepsilon) \ \vdash_M^* \ (s, \varepsilon, b^{n-m})$ falls $m \leq n$

Das zeigt man durch Induktion über $|w|$:

$w = \varepsilon$:

$(s, w, \varepsilon) \vdash_M^0 (s, \varepsilon, a^{0-0}) = (s, \varepsilon, b^{0-0})$

$w = va$:

Wenn $m > n$, dann ist $m - 1 \geq n$, also nach Induktionsannahme $(s, v, \varepsilon) \vdash_M^* (s, \varepsilon, a^{m-1-n})$ und damit $(s, w, \varepsilon) \vdash_M^* (s, a, a^{m-1-n}) \vdash_M (s, \varepsilon, a^{m-n})$. Wenn $m \leq n$, dann ist $m - 1 < n$, also nach Induktionsannahme $(s, v, \varepsilon) \vdash_M^* (s, \varepsilon, b^{n-(m-1)})$ und damit $(s, w, \varepsilon) \vdash_M^* (s, a, b^{n-(m-1)}) \vdash_M (s, \varepsilon, b^{n-m})$. Damit ist auch im Falle $m = n$ alles bewiesen, weil dann $b^{n-m} = \varepsilon = a^{m-n}$.

$w = vb$:

Analog zu $w = va$ (wegen der Symmetrie).

Damit ist '$\subseteq$' bewiesen, denn für $w \in L$ gilt $m = n$, also $(s, w, \varepsilon) \vdash_M^* (s, \varepsilon, a^0) = (s, \varepsilon, \varepsilon)$ und das bedeutet $w \in L(M)$.

'$\supseteq$': Sei $w \in L(M)$, d.h. $(s, w, \varepsilon) \vdash_M^* (s, \varepsilon, \varepsilon)$.

Für jeden Übergangsschritt von M gilt: Entweder es wird nur ein Zeichen verschoben (vom Eingabeband in den Keller), oder es wird gleichzeitig ein a und ein b entfernt (eines vom Eingabeband, das andere vom Keller).

Da in der letzten Konfiguration $(s, \varepsilon, \varepsilon)$ gleich viele as und bs vorhanden sind (Eingabewort und Kellerwort zusammengerechnet), muss dies auch für jede vorhergehende Konfiguration gelten, also insbesondere für die Anfangskonfiguration (s, w, ε).

Das bedeutet aber $\#_a(w) = \#_b(w)$, d.h. $w \in L$. $\square$

Im Beweis wurde die Tatsache benutzt, dass eine Verlängerung des Eingabewortes vom Kellerautomaten ignoriert werden kann. Gleiches gilt für das Kellerwort.

Lemma 2.57 *Wenn*

$$(p, u, \alpha) \ \vdash_M^* \ (q, v, \beta)$$

dann gilt auch

$$(p, uw, \alpha\gamma) \ \vdash_M^* \ (q, vw, \beta\gamma)$$

für alle $v \in \Sigma^*$ *und* $\gamma \in \Gamma^*$.

Beweisidee:

Mit $(p, uv, \alpha\gamma)$ kann man die gleiche Folge von Übergangsschritten durchführen wie mit (p, u, α), indem man v und γ ignoriert.

(Die Tatsache, dass man mit $(p, uv, \alpha\gamma)$ vielleicht auch neue Übergangsschritte durchführen kann, indem man γ benutzt, interessiert hier nicht.) $\square$

Satz 2.58 *Zu jeder kontextfreien Grammatik G lässt sich ein Kellerautomat M mit $L(M) = L(G)$ konstruieren.*

Beweisidee:

Man konstruiert den Kellerautomaten so, dass er eine Ableitung für das Eingabewort w in der Grammatik G 'erraten' kann.

Diese Ableitung führt er im Keller durch, d.h. er schreibt zu Beginn das Startzeichen in den Keller und führt dann die Ableitungsschritte der Grammatik im Keller aus.

Problem:

In einem Ableitungsschritt der Grammatik wird ein Nichtterminalzeichen A an einer *beliebigen* Stelle des bisher abgeleiteten Wortes durch die rechte Seite γ einer Produktion $A \to \gamma$ ersetzt.

Das kann der Kellerautomat nicht leisten, da er immer nur auf die Zeichen zugreifen kann, die *oben* im Keller stehen.

Lösung(?):

Wir betrachten nur *Linksableitungen*, bei denen ja immer das linkeste Nichtterminalzeichen ersetzt wird.

Aber auch das muss nicht ganz oben im Keller stehen, es können noch Terminalzeichen im Wege sein.

Die müssen aber, wenn die bisherige Ableitung richtig erraten wurde, mit den ersten Zeichen des Eingabewortes w übereinstimmen.

Also kann man sie in diesem Fall entfernen (und der andere Fall interessiert nicht, weil dann die bisherige Ableitung schon falsch erraten wurde).

Damit ist klar, dass der Kellerautomat drei Arten von Transitionen besitzen sollte, nämlich:

Kontextfreie Sprachen

1. eine Transition, um das Startzeichen in den Keller zu legen,
2. für jede Produktion der Grammatik eine Transition, die den entsprechenden Ableitungsschritt durchführt,
3. Transitionen, um Terminalzeichen auf dem Eingabeband und im Keller miteinander zu vergleichen und zu entfernen.

Formal:

Sei $G = (\Sigma, N, S, P)$. Wir definieren $M = (\Sigma, \Gamma, Q, s, F, \Delta)$ mit

- $\Gamma = N \cup \Sigma$
- $Q = \{s, f\}$
- $F = \{f\}$
- $$\begin{array}{rcll} \Delta & = & \{((s,\varepsilon,\varepsilon),(f,S))\} & (1) \\ & \cup & \{((f,\varepsilon,A),(f,\gamma)) \mid (A \to \gamma) \in P\} & (2) \\ & \cup & \{((f,a,a),(f,\varepsilon)) \mid a \in \Sigma\} & (3) \end{array}$$

Bevor wir $L(M) = L(G)$ beweisen, wollen wir uns die Arbeitsweise dieses Kellerautomaten M an einem kleinen **Beispiel** verdeutlichen:

Sei $G = (\{a,b\},\{S\},S,P\}$ mit $P = \{S \to aSb, S \to \varepsilon\}$.

Dann ist $M = (\{a,b\},\{a,b,S\},\{s,f\},s,\Delta)$

mit

$$
\begin{aligned}
\Delta \ = \{ \ & ((s,\varepsilon,\varepsilon),(f,S)),\\
& (((f,\varepsilon,S),(f,aSb)),\\
& (((f,\varepsilon,S),(f,\varepsilon),\\
& ((f,a,a),(f,\varepsilon)),\\
& ((f,b,b),(f,\varepsilon))\}
\end{aligned}
$$

also gilt z.B. bei Eingabe $aabb$:

$$
\begin{aligned}
(s,aabb,\varepsilon) & \vdash_M (f,aabb,S)\\
& \vdash_M (f,aabb,aSb)\\
& \vdash_M (f,abb,Sb)\\
& \vdash_M (f,abb,aSbb)\\
& \vdash_M (f,bb,Sbb)\\
& \vdash_M (f,bb,bb)\\
& \vdash_M (f,b,b)\\
& \vdash_M (f,\varepsilon,\varepsilon)
\end{aligned}
$$