

# Theoretische Grundlagen der Informatik

## Tutorium 4

Institut für Kryptographie und Sicherheit



Behauptung:  $L$  ist nicht regulär.

Beweis:

Sei  $p \in \mathbb{N}$  wie im Pumping-Lemma

Wähle  $w =$  \_\_\_\_\_,  $w \in L$ ,  $|w| > n$

Beh:  $\forall u, v, x : w = uvx, |uv| \leq p, v \neq \varepsilon$  gilt:  $\exists i \in \mathbb{N}_0 : uv^i x \notin L$

Bew: ( $\forall v$  gilt:)

Widerspruch zum Pumping Lemma  $\Rightarrow L$  ist nicht regulär.

1. Schritt: neues Startsymbol  
 $S' \rightarrow S | \varepsilon$
2. Schritt: Entfernen der  $\varepsilon$ -Produktionen
3. Schritt: Entfernen von Kettenregeln  
z.B.  $A \rightarrow B, B \rightarrow c \implies A \rightarrow c$   
x
4. Schritt: Überführen in Chomsky-Normalform
  - 4.1 Terminale ersetzen
  - 4.2 Regeln auf 2 Variablen 'kürzen'

Gegeben sei die Grammatik  $G = (\mathcal{T}, \mathcal{V}, S, \mathcal{P})$  mit den folgenden Produktionen aus  $\mathcal{P}$ :

$$S \rightarrow AX \mid AB$$

$$X \rightarrow SB \mid AB$$

$$A \rightarrow a$$

$$B \rightarrow b$$

1. Lässt sich der CYK-Algorithmus auf  $G$  anwenden?
2. Ist das Wort  $aaabbb$  in der Sprache  $\mathcal{L}(G)$ ?

Gegeben sei die folgende Grammatik:  $\mathcal{G} = (\mathcal{T}, \mathcal{V}, S, \mathcal{P})$  mit  
 $\mathcal{T} := \{a, b, c, d\}$ ,  $\mathcal{V} := \{S, A, D, M, X, Y, B, C\}$ ,  
 $\mathcal{P} := \{S \rightarrow AX \mid AD \mid BY \mid BY \mid \varepsilon, A \rightarrow AA \mid a, D \rightarrow DD \mid d, M \rightarrow BY \mid BC, X \rightarrow MD, Y \rightarrow MC, B \rightarrow b, C \rightarrow c\}$

1. Zeigen oder widerlegen Sie mit Hilfe des CYK-Algorithmus, ob die folgenden Wörter in der Sprache  $\mathcal{L}$  liegen, die durch die Grammatik  $\mathcal{G}$  erzeugt wird!

1.1 *aabbccdd*

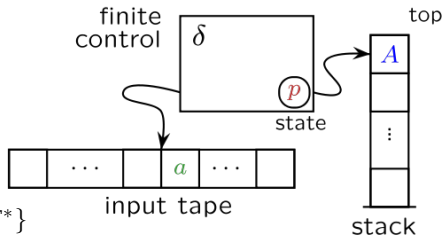
1.2 *abbcc*

1.3 *abcdd*

# Definition Kellerautomaten

Ein (nichtdeterministischer) **Kellerautomat** (NPDA bzw PDA, Pushdown Automaton) besteht aus  $(Q, \Sigma, \Gamma, q_0, Z_0, \delta, F)$ , wobei

- $Q$  endliche Zustandsmenge
- $\Sigma$  endliches Eingabealphabet
- $\Gamma$  endliches Stack-Alphabet
- $q_0 \in Q$  Anfangszustand
- $Z_0 \in \Gamma$  Initialisierung des Stacks
- $\delta : Q \times (\Sigma \cup \{\varepsilon\}) \times \Gamma \rightarrow 2^{Q \times \Gamma^*}$ 
  - $\delta(q, a, Z) \subseteq \{(q, \gamma) : q \in Q, \gamma \in \Gamma^*\}$
  - $\delta(q, \varepsilon, Z) \subseteq \{(q, \gamma) : q \in Q, \gamma \in \Gamma^*\}$
- $F \subseteq Q$  Menge der akzeptierenden Endzustände,  $F = \emptyset$  ist möglich.



- Akzeptieren nach Eingabeende, wenn
  - der Stack leer ist *oder*
  - der Automat in einen akzeptierenden Zustand kommt.
- Sind im Allgemeinen nichtdeterministisch
- Man kann Endzustände auch aus der Definition weglassen und alternativ verlangen, dass der Automat genau bei leerem Keller akzeptiert.
- Man kann sogar alle Zustände bis auf einen weglassen und alles in die Kellerbelegung kodieren

$$M = (Q, \Sigma, \Gamma, q_0, Z_0, \delta, F)$$

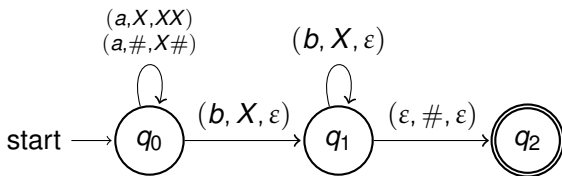
$$Q = \{q_0, q_1, q_2\}$$

$$\Sigma = \{a, b\}$$

$$\Gamma = \{\#, X\}$$

$$Z_0 = \#$$

$$F = \{q_2\}$$



- Welche Sprache akzeptiert dieser Automat?



Gegeben sei folgende Sprache für das Alphabet  $\Sigma = \{a, b, c\}$ :

$$\mathcal{L} = \{w_1 w_2 \in \Sigma^* \mid w_1 \in \{a, b\}^*, w_2 \in \{b, c\}^*, \\ \#_a w_1 + \#_b w_1 = \#_b w_2 + \#_c w_2\}$$

Hier gibt  $\#_x w$  die Häufigkeit des Vorkommens eines Zeichens  $x \in \Sigma$  in einem Wort  $w \in \Sigma^*$  an.

1. Zeigen Sie, dass  $\mathcal{L}$  nicht regulär ist!
2. Geben Sie eine Chomsky-2-Grammatik an, die genau die Sprache  $\mathcal{L}$  erzeugt!
3. Geben Sie einen Kellerautomaten  $\mathcal{M}$  an, der genau die Sprache  $\mathcal{L}$  erkennt! Zeichnen Sie den Zustandsübergangsgraphen für  $\mathcal{M}$ !

## Lemma

Für jede kontextfreie Sprache  $L$  gibt es eine Konstante  $n \in \mathbb{N}$ , so dass sich jedes Wort  $z \in L$  mit  $|z| \geq n$  so als

$$z = uvwxy$$

schreiben lässt, dass

- $|vx| \geq 1$ ,
- $|vwx| \leq n$  und
- für alle  $i \geq 0$  das Wort  $uv^iwx^iy \in L$  ist.

# Pumping Lemma Formalia (kontextfrei)

Behauptung:  $L$  ist nicht kontextfrei.

Beweis:

Nehme an  $L$  sei kontextfrei.

Sei  $n$  beliebig aber fest.

Wähle  $z = \text{_____} \in L$  mit  $|z| \geq n$

Beh.:  $\forall u, v, w, x, y : uvwxy = z$  mit  $|vx| \geq 1$  und  $|vwx| \leq n$ ,  $\exists i \in \mathbb{N}$ ,  
so dass  $uv^iwx^iy \notin L$ .

Bew.: \_\_\_\_\_

Widerspruch zum Pumping Lemma  $\Rightarrow L$  ist nicht kontextfrei.

Zeige, dass die Sprache

$$L = \{\omega\omega \mid \omega \in \{0, 1\}^*\}$$

nicht kontextfrei ist.

# Aufgabe 3

1. Geben Sie für die Sprache  $\mathcal{L} = \{a^n b^n c^n \mid n \in \mathbb{N}\}$  eine Grammatik des höchstmöglichen Chomsky-Typs an!
2. Zeigen Sie, dass die Sprache  $\mathcal{L}' = \{a^{2^n} \mid n \in \mathbb{N}\}$  nicht kontextfrei ist!



Seien  $L_1, L_2$  kontextfrei so sind auch diese  $L$  kontextfrei:

■  $L = L_1 \cup L_2$

■  $L = L_1 \cdot L_2$

■  $L = L_1^*$

# Bis zum nächsten Mal!

<p>□□□□□□□□□□□□□□</p> <p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Trøub4dor &amp;3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERICAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO FREQUENCY FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS)</p>	<p>~28 BITS OF ENTROPY</p> <p>□□□□□□□□ □ □□□□□□□□ □ □□□ □□□ □□□□ □</p> <p><math>2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>(PLAUSIBLE ATTACK ON A WORK REMOTE WEB SERVICE YES, CRACKING A STORED HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: <b>EASY</b></p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O's WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p>  <p>DIFFICULTY TO REMEMBER: <b>HARD</b></p>
<p>correct horse battery staple</p> <p>□□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>□□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□</p> <p><math>2^{44} = 530 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>DIFFICULTY TO GUESS: <b>HARD</b></p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p>  <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



Dieses Werk ist unter einem "Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 3.0 Deutschland"-Lizenzvertrag lizenziert. Um eine Kopie der Lizenz zu erhalten, gehen Sie bitte zu <http://creativecommons.org/licenses/by-sa/3.0/de/> oder schreiben Sie an Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.

Davon ausgenommen sind das Titelbild, welches aus der März-April 2002 Ausgabe von American Scientist erschienen ist und ohne Erlaubnis verwendet wird, sowie das KIT Beamer Theme. Hierfür gelten die Bestimmungen der jeweiligen Urheber.