Universität Paderborn
Warburger Straße 100
33098 Paderborn

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Beweise zur Vorlesung

Modellierung

WS 2016/2017

Prof. Dr. Johannes Blömer

Arbeitsgruppe Codes und Kryptographie

Graphen Teil 1 - ungerichtete Graphen

Satz 3
Für jeden ungerichteten Graphen $G = (V, E)$ gilt

$$\sum_{v \in V} \deg(v) = 2|E|.$$

Beweis. Sei $G = (V, E)$ ein beliebiger Graph. Für jeden Knoten $v \in V$ setzen wir $E(v) := \{e \in E | v \in e\}$. Damit ist $E(v)$ die Menge der Kanten, zu denen v inzident ist. Nach Definition des Grades $\deg(v)$ und der Nachbarschaft $\Gamma(v)$ von Knoten $v \in V$ gilt

$$\begin{aligned}\sum_{v \in V} \deg(v) &= \sum_{v \in V} |\Gamma(v)| \\ &= \sum_{v \in V} |\{u \in V | \{u, v\} \in E\}| \\ &= \sum_{v \in V} \sum_{e \in E(v)} 1\end{aligned}$$

Statt zunächst über alle Knoten und dann über die inzidenten Kanten können wir auch zunächst über alle Kanten und dann über die inzidenten Knoten summieren, also

$$\sum_{v \in V} \sum_{e \in E(v)} 1 = \sum_{e \in E} \sum_{v \in e} 1.$$

Jede Kante $e \in E$ enthält genau zwei Knoten. Damit gilt für alle Kanten $e \in E$, dass

$$\sum_{v \in e} 1 = 2.$$

Somit folgt, dass

$$\begin{aligned}\sum_{v \in V} \sum_{e \in E(v)} 1 &= \sum_{e \in E} 2 \\ &= 2|E|.\end{aligned}$$

Damit haben wir den Satz bewiesen. □

Satz 4
Für jeden ungerichteten Graphen $G = (V, E)$ gilt, dass die Anzahl der Knoten mit ungeradem Grad gerade ist.

Beweis. Sei $G = (V, E)$ ein Graph. Wir definieren

$$\begin{aligned}V_g &:= \{v \in V | \deg(v) \text{ ist gerade}\} \\ V_u &:= \{v \in V | \deg(v) \text{ ist ungerade}\}.\end{aligned}$$

Wir müssen zeigen, dass $|V_u|$ gerade ist. Zunächst beobachten wir, dass

$$V = V_g \cup V_u \quad \text{und} \quad V_g \cap V_u = \emptyset.$$

Damit folgt

$$\sum_{v \in V} \deg(v) = \sum_{v \in V_g} \deg(v) + \sum_{v \in V_u} \deg(v)$$

oder

$$\sum_{v \in V_u} \deg(v) = \sum_{v \in V} \deg(v) - \sum_{v \in V_g} \deg(v)$$

Nach Satz 3 gilt
$$\sum_{v \in V} \deg(v) = 2|E|,$$
insbesondere ist $\sum_{v\in V} \deg(v)$ gerade. Nach Definition von V_g ist jeder Summand in $\sum_{v\in V_g} \deg(v)$ gerade. Damit ist auch die gesamte Summe gerade. Es folgt, dass $\sum_{v\in V_u} \deg(v)$ als Differenz zweier gerader Zahlen ebenfalls gerade ist. Nach Definition von V_u ist jeder Summand in $\sum_{v\in V_u} \deg(v)$ ungerade. Damit muss die Anzahl der Summanden in dieser Summe gerade sein, da eine Summe ungerader vieler ungerade Zahlen ebenfalls ungerade ist. Die Anzahl der Summanden in $\sum_{v\in V_u} \deg(v)$ ist $|V_u|$. Damit ist der Satz bewiesen. □

Satz 10
Ein Graph $G = (V, E)$ besitzt mindestens $|V| - |E|$ viele Zusammenhangskomponenten.

Beweis. Wir beweisen den Satz durch Induktion über die Anzahl Kanten m.
Induktionsanfang $m = 0$.
Sei $G = (V, E)$ mit $E = \emptyset$. Dann ist jeder Knoten $v \in V$ eine eigene Zusammenhangskomponente. In diesem Fall besitzt G daher
$$|V| = |V| - 0 = |V| - |E|$$
Zusammenhangskomponenten. Damit gilt der Satz für $m = 0$.
Wir nehmen nun an
Induktionsvoraussetzung. Für ein beliebiges, aber festes $m \in \mathbb{N}$ gilt, dass jeder Graph $G = (V, E)$ mit m Kanten mindestens $|V| - |E|$ viele Zusammenhangskomponenten besitzt.
Wir zeigen im
Induktionsschritt von m auf $m+1$, dass die Behauptung für alle Graphen mit $m+1$ Kanten gilt.
Hierzu sei $G = (V, E)$ ein Graph mit $m+1$ Kanten. Sei $e \in E$ eine beliebige Kante. Wir setzen
$$G' := (V, E') \quad \text{mit} \quad E' = E \setminus \{e\},$$
d.h., G' hat dieselbe Knotenmenge wie G und besitzt alle Kanten aus G außer der gewählten Kante e. Der Graph G' hat somit m Kanten und nach Induktionsvoraussetzung mindestens $|V| - m$ Zusammenhangskomponenten. Für die Kante e gibt es nun zwei Möglichkeiten

1. e ist zu zwei Knoten inzident, die in derselben Zusammenhangskomponente von G' liegen.
2. e ist zu zwei Knoten inzident, die in unterschiedlichen Zusammenhangskomponenten von G' liegen.

Im ersten Fall ist die Anzahl der Zusammenhangskomponenten von G gleich der Anzahl der Zusammenhangskomponenten von G'. Somit ist in diesem Fall die Anzahl der Zusammenhangskomponenten von G mindestens
$$|V| - m \geq |V| - (m + 1) = |V| - |E|.$$
Im zweiten Fall (e ist zu Knoten aus unterschiedlichen Zusammenhangskomponenten von G') ist die Anzahl der Zusammenhangskomponenten von G um 1 kleiner als die Anzahl der Zusammenhangskomponenten von G'. Damit ist die Anzahl der Zusammenhangskomponenten von G mindestens
$$|V| - m - 1 = |V| - (m + 1) = |V| - |E|.$$
In beiden Fällen gilt der Induktionsschritt und der Satz ist bewiesen. □

Satz 11
Für jeden zusammenhängenden Graphen $G = (V, E)$ gilt:

$$|E| \geq |V| - 1.$$

Beweis. Nach Definition hat ein zusammenhängender Graph genau eine Zusammenhangskomponente. Nun gilt

$$|V| - |E| \leq 1,$$

da andernfalls G nach Satz 10 mindestens 2 Zusammenhangskomponenten besitzt, im Widerspruch zur Annahme, dass G zusammenhängend ist. $|V| - |E| \leq 1$ ist äquivalent zu $|E| \geq |V| - 1$, und der Satz ist bewiesen. □

Graphen Teil 2 - Bäume und Wälder

Lemma 2
Jeder Baum $T = (V, E)$ mit $|V| \geq 2$ Knoten enthält mindestens zwei Blätter.

Beweis. Sei $T = (V, E)$ ein beliebiger Baum mit $|V| \geq 2$. Wenn T keine Knoten mit Grad mindestens 2 enthält, gilt $|V| = 2$ und $|E| = 1$. Der Baum T besteht dann nur aus einer Kante und die beiden Knoten des Baums sind auch Blätter. In diesem Fall gilt das Lemma daher.

Sei jetzt $T = (V, E)$ ein Baum, der mindestens einen Knoten $u \in V$ mit Grad $\deg(u) \geq 2$ enthält. Seien $e_1 = \{u, v_1\}, e_2 = \{u, v_2\}$ unterschiedliche Kanten, zu denen u inzident ist. Nun betrachten wir in u beginnende Pfade P_1, P_2, wobei

1. der Pfad P_1 mit der Kante e_1 und der Pfad P_2 mit der Kante e_2 beginnt,
2. die Pfade in einem Blatt enden.

Solche Pfade existieren, da Pfade in Bäumen, die nicht in einem Blatt enden, durch weitere Kanten verlängern können. Die Pfade P_1, P_2 müssen unterschiedliche Knoten enthalten, da andernfalls T einen Kreis enthält und somit kein Baum wäre (Beweis siehe unten). Insbesondere enden die Pfade P_1, P_2 in unterschiedlichen Blättern, und T besitzt mindestens zwei Blätter.

Es bleibt noch zu zeigen, dass die Pfade P_1, P_2 unterschiedliche Knoten enthalten. Wir führen einen Widerspruchsbeweis und nehmen an, dass es einen Knoten $x \in V$ gibt, der sowohl auf P_1 als auch auf P_2 liegt. Dann existieren zwei Pfade $\bar{P}_1$ und $\bar{P}_2$ von u zu x. Diese Pfade bilden dann einen Kreis in T im Widerspruch zur Annahme, dass T ein Baum ist. □

Lemma 3
Ist $T = (V, E)$ ein Baum mit $|V| \geq 2$ Knoten und $u \in V$ ein Blatt, so ist der durch $V' = V \setminus \{u\}$ induzierte Teilgraph T' ebenfalls ein Baum.

Beweis. Wir müssen zeigen, dass T' kreisfrei und zusammenhängend ist. Zunächst betrachten wir die Kreisfreiheit. Da u ein Blatt ist, ist u nur zu einer Kanten $e \in E$ inzident. Damit gilt $T' = (V', E')$ mit $V' = V \setminus \{u\}$ und $E' = E \setminus \{e\}$. Weiter können durch das Entfernen von Knoten und Kanten keine neuen Kreise in einem Graphen entstehen. Damit ist mit T auch T' kreisfrei.

Jetzt zeigen wir noch, dass T' zusammenhängend ist. Seien hierzu x, y zwei beliebige unterschiedliche Knoten in $V' = V \setminus \{u\}$. Wir zeigen, dass x, y in T' durch einen Pfad verbunden sind. Nun gibt es in T einen Pfad $P_{x,y}$ der x und y verbindet, da T zusammenhängend ist. Da die inneren Knoten eines Pfades mindestens Grad 2 besitzen, aber $\deg(u) = 1$, ist u nicht in $P_{x,y}$ enthalten. Damit ist $P_{x,y}$ auch ein Pfad in T'. Die Knoten $x, y \in V'$ waren beliebig. Damit gibt es für je zwei Knoten $x \neq y$ aus T' einen x-y-Pfad in T' und T' ist zusammenhängend. □

Satz 4
Ist $T = (V, E)$ ein Baum, so gilt

$$|E| = |V| - 1.$$

Beweis. Wir führen einen Widerspruchsbeweis. Sei hierzu $T_0 = (V_0, E_0)$ ein kleinstes Gegenbeispiel. Also

- T_0 ist ein Baum mit $|E_0| \neq |V_0| - 1$.
- Für jeden Baum $T = (V, E)$ mit $|V| < |V_0|$ gilt $|E| = |V| - 1$.

Nun gilt, $|V_0| \geq 2$, da der Satz für Graphen mit einem Knoten korrekt ist. Außerdem besitzt T_0 nach Lemma 2 mindestens zwei Blätter. Sei u eines dieser Blätter und sei $e = \{u, u'\}$ die einzige Kante in T_0, zu der u inzident ist. Wir betrachten nun $T' = (V', E'), V' = V_0 \setminus \{u\}, E' = E_0 \setminus \{\{u, u'\}\}$. Nach Lemma 3 ist T' ein Baum. Da $|V'| < |V_0|$ und T_0 kleinstes Gegenbeispiel für die Aussage des Satzes war, gilt $|E'| = |V'| - 1$. Außerdem haben wir $|V_0| - 1 = |V'|$ und $|E_0| - 1 = |E'|$. Insgesamt erhalten wir

$$|E_0| - 1 = |V_0| - 1 - 1$$

oder

$$|E_0| = |V_0| - 1.$$

Dies ist ein Widerspruch zur Annahme, dass T_0 ein Gegenbeispiel zur Aussage des Satzes ist. $\square$

Lemma 5
Sei $G = (V, E)$ ein zusammenhängender Graph und C ein Kreis in G. Dann gilt für alle im Kreis C enthaltenen Kanten e:

$$G_e := (V, E \setminus \{e\}) \text{ ist zusammenhängend.}$$

Beweis. Wir führen einen Widerspruchsbeweis. Sei hierzu $G = (V, E)$ ein zusammenhängender Graph, C ein Kreis in G und $e = \{u, v\} \in E$ eine Kante in E, so dass G_e nicht zusammenhängend ist. Dies bedeutet, dass G_e genau zwei Zusammenhangskomponenten G_1 und G_2 besitzt (da G zusammenhängend ist). Außerdem liegen die Knoten u und v in unterschiedlichen Zusammenhangskomponenten (den Beweis hierfür führen Sie in einer Übungsaufgabe). Da e in einem Kreis C liegt, existiert jedoch ein u-v-Pfad in G, der e nicht enthält, insbesondere ist der Kreis C ohne die Kante e ein solcher u-v-Pfad. Diesen Pfad gibt es auch im Graphen G_e. Damit liegen u, v in derselben Zusammenhangskomponente von G_e, im Widerspruch zur Annahme. $\square$

Satz 7
Jeder zusammenhängende Graph enthält einen Spannbaum.

Beweis. Für Graphen $G = (V, E)$ mit $|V| = 1$ ist die Aussage des Satzes korrekt. Sei daher $G = (V, E)$ ein beliebiger zusammenhängender Graph mit $|V| \geq 2$. Wir betrachten folgendes Verfahren:

1. Setze $E_T := E$.
2. Solange $T := (V, E_T)$ Kreise enthält
3. Wähle beliebige Kante e in einem beliebigen Kreis von T.
4. Entferne e aus E_T, also setze $E_T := E_T \setminus \{e\}$.

Das Verfahren kann höchstens $|E|$ viele Kanten entfernen und wird daher nach endlich vielen Durchläufen der Schritte 3. und 4. anhalten. Wenn das Verfahren hält, besitzt der Graph T gemäß der Bedingung in 2. keine Kreise mehr. Da wir aber sukzessive Kanten aus Kreisen entfernen, ist nach Lemma 5 der Graph $T = (V, E_T)$ nach Beendigung des Verfahrens zusammenhängend. Seine Knotenmenge ist V. Insgesamt ist T ein Teilgraph von G mit Knotenmenge V, der kreisfrei und zusammenhängend ist. T ist damit ein Spannbaum von G. Wir haben also für jeden zusammenhängenden Graphen einen Spannbaum konstruiert. Insbesondere enthält damit jeder zusammenhängende Graph einen Spannbaum. □

Graphen Teil 4 - Wurzelbäume

Satz 4
Ein vollständiger Binärbaum der Höhe h hat 2^h Blätter und $2^{h+1} - 1$ Knoten.

Beweis. Wir beweisen den Satz durch Induktion über die Höhe h.
Induktionsanfang $h = 0$.
Ein Baum der Höhe h besteht aus einem Knoten w. Die Anzahl der Knoten und Blätter dieses Baums ist 1. Da $1 = 2^1 - 1 = 2^0$ gilt der Satz für $h = 0$.
Wir nehmen nun an
Induktionsvoraussetzung. Für ein beliebiges, aber festes $h \in \mathbb{N}$ gilt, dass der vollständige Binärbaum der Höhe h 2^h Blätter und $2^{h+1} - 1$ Knoten besitzt.
Wir zeigen im
Induktionsschritt von h auf $h + 1$, dass die Behauptung für den vollständigen Binärbaum mit Höhe $h + 1$ gilt. Hierzu sei T der vollständige Binärbaum der Höhe $h + 1$ und mit Wurzel w. Mit w_1, w_2 bezeichnen wir die direkten Nachfolger von w. Nach Definition eines vollständigen Binärbaums bildet für $i = 1, 2$ der Knoten w_i mit seinen Nachfolgern einen vollständigen Binärbaum T_i der Höhe h. Nach Induktionsvoraussetzung besitzen die Bäume T_1, T_2 jeweils 2^h Blätter und $2^{h+1} - 1$ Knoten.

- Die Menge der Blätter von T ist die Vereinigung der Blätter von T_1 und T_2. Der Baum T besitzt somit
$$2^h + 2^h = 2 \cdot 2^h = 2^{h+1}$$
viele Blätter.
- Die Menge der Knoten von T ist die Vereinigung von $\{w\}$ und der Knoten von T_1 und T_2. Der Baum T besitzt somit
$$2^{h+1} - 1 + 2^{h+1} - 1 + 1 = 2 \cdot 2^{h+1} - 1 = 2^{h+2} - 1$$
viele Knoten.

Damit gilt der Induktionsschritt und der Satz ist bewiesen. □

Grammatiken

Beispiel
Sei Grammatik $G_3 = (T, N, P, S)$ definiert durch
$$\begin{aligned} T &= \{a\} \\ N &= \{A\} \\ S &= \ \ A \\ P &= \{A ::= aA, A ::= a\}. \end{aligned}$$
Dann gilt $L(G_3) = \{a^n \mid n \geq 1\}$.

Beweis. Wie üblich beim Beweis der Gleichheit zweier Mengen zeigen wir:

1. $L(G_3) \subseteq \{a^n \mid n \geq 1\}$
2. $\{a^n \mid n \geq 1\} \subseteq L(G_3)$.

zu 1. Da $T = \{a\}$ gilt $L(G_3) \subseteq \{a^n \mid n \geq 0\}$. Die Produktionen in G_3 enthalten jedoch alle ein a auf ihren rechten Seiten. Damit gilt $a^0 \notin L(G_3)$ und somit $L(G_3) \subseteq \{a^n \mid n \geq 1\}$.

zu 2. Wir müssen zeigen, dass für $n \in \mathbb{N}$ beliebig, $a^n \in L(G_3)$. Sei daher $n \in \mathbb{N}$ beliebig. Wir betrachten die Folge von Produktionen

$$A \to aA \to aaA \to \cdots \to a^{n-1}A \to a^n,$$

wobei wir $(n-1)$-mal die Produktion $A \to aA$ und einmal die Produktion $A \to a$ angewandt haben. Diese Ableitung zeigt, dass a^n aus A ableitbar ist. Damit gilt $a^n \in L(G_3)$.

□

Beispiel
Sei Grammatik $G_4 = (T, N, P, S)$ definiert durch

$$\begin{aligned} T &= \{a, b\} \\ N &= \{S\} \\ S &= \ \ S \\ P &= \{S ::= aSb, S ::= \epsilon\} \end{aligned}$$

Dann gilt $L(G_4) = \{a^n b^n \mid n \geq 0\}$.

Beweis. Analog zum vorangegangenen Beispiel zeigen wir:

1. $L(G_4) \subseteq \{a^n b^n \mid n \geq 0\}$
2. $\{a^n b^n \mid n \geq 0\} \subseteq L(G_4)$.

zu 1. Jede Ableitung $S \to^* w$ besteht aus endlich vielen Anwendungen der Produktion $S \to aSb$ gefolgt von einer Anwendung der Produktion $S \to \epsilon$. Damit können nur Elemente der Form $a^n b^n, n \geq 0$, aus dem Startsymbol S abgeleitet werden. Daher gilt $L(G_4) \subseteq \{a^n b^n \mid n \geq 0\}$.

zu 2. Wir müssen zeigen, dass für $n \in \mathbb{N}$ beliebig, $a^{n-1}b^{n-1} \in L(G_n)$. Sei daher $n \in \mathbb{N}$ beliebig. Wir betrachten die Folge von Produktionen

$$S \to aSb \to aaSbb \to \cdots \to a^{n-1}Ab^{n-1} \to a^{n-1}b^{n-1},$$

wobei wir $(n-1)$-mal die Produktion $A \to aSb$ und einmal die Produktion $S \to a$ angewandt haben. Diese Ableitung zeigt, dass $a^{n-1}b^{n-1}$ aus S ableitbar ist. Damit gilt $a^{n-1}b^{n-1} \in L(G_4)$.

□

Satz 6
Die Grammatik G_2 ist nicht mehrdeutig.

Beweis. Wir zeigen, dass es für jedes Element in $w \in L(G_2)$ genau eine Rechtsableitung existiert. Nach Satz 7 der Vorlesung ist die Grammatik G_2 dann nicht mehrdeutig. Allgemeiner zeigen wir

Behauptung
Sei $w \in \{(,)\}$, so dass w aus Klammerung oder Liste abgeleitet werden kann, dass gibt es eine eindeutige Rechtsableitung von w aus Klammerung oder Liste.

Beweis. Wir zeigen die Behauptung durch Induktion der Ableitungsschritte t, die höchstens benötigt werden, um w aus *Klammerung* oder *Liste* abzuleiten.
Induktionsanfang $t = 1$.
Das einzige Wort w, dass aus *Klammerung* oder Liste in einem Schritt abgeleitet werden kann, ist das leere Wort ϵ. Die einzige Rechtsableitung von ϵ aus Liste $Liste \to \epsilon$.
Wir nehmen nun an
Induktionsvoraussetzung. Für ein beliebiges $w \in \{(,)\}$, das aus *Klammerung* oder *Liste* durch höchstens t Ableitungsschritte abgeleitet werden kann, gibt es eine eindeutige Rechtsableitung von w aus *Klammerung* bzw. *Liste*.
Wir zeigen im
Induktionsschritt von t auf $t + 1$, dass die Behauptung auch für Worte w gilt, die mit $t + 1$ Schritten aus *Klammerung* oder *Liste* abgeleitet werden können.
Hierzu sei w ein Wort, dass aus *Klammerung* oder L*Liste* mit $t + 1$ Ableitungsschritten abgeleitet werden kann. Wir betrachten zwei Fälle.

- w kann aus *Klammerung* mit $t + 1$ Schritten abgeleitet werden.
- w kann aus *Liste* mit $t + 1$ Schritten abgeleitet werden.

zu 1. Jede Ableitung $Klammerung \to^* w$von w aus *Klammerung* beginnt mit der Ableitung $Klammerung \to (Liste)$. Damit ist w von der Form $w = (w')$, wobei w' aus *Liste* mit t Schritten abgeleitet werden kann. Damit gibt es nach Induktionsvoraussetzung nur eine Rechtsableitung von w' aus *Liste*. Hieraus folgt, dass es auch nur eine Rechtsableitung von w aus *Klammerung* geben kann, die Ableitung, die mit $Klammerung \to (w')$ beginnt, gefolgt von der Rechtsableitung von w' aus *Liste*.

zu 2. Jede Ableitung $Liste \to^* w$ von w aus *Liste* beginnt mit $Liste \to KlammerungListe$. Damit ist w von der Form $w = w_1 w_2$, wobei w_1 aus *Klammerung* und w_2 aus *Liste* mit jeweils höchstens t Schritten abgeleitet werden können. Nach Induktionsvoraussetzung gibt es nur eine Rechtsableitung von w_1 aus *Klammerung* und eine Rechtsableitung von w_2 aus *Liste*. Somit gibt es eine eindeutige Rechtsableitung von w aus *Liste*, die Ableitung, die mit $Liste \to KlammerungListe$ beginnt, gefolgt von der Rechtsableitung von w_2 aus *Liste*, gefolgt von der Rechtsableitung von w_1 aus *Klammerung*.

Damit gilt der Induktionsschritt und die Behauptung ist bewiesen. □

Der Satz folgt unmittelbar aus der (allgemeineren) Behauptung. □

Reguläre Ausdrücke

Lemma 14
Die Sprache $L_1 = \{0,1\}^* \setminus \{11\}$ ist regulär.

Beweis. Wir zeigen $L_1 = L(R_1)$, wobei

$$R_1 = 0\{0,1\}^*|10\{0,1\}^*|111\{0,1\}^*|110\{0,1\}^*|1|\epsilon.$$

Um dieses zu sehen partitionieren wir zunächst die Sprache L in die folgenden Teilmengen.

$$\begin{aligned} L_1 &= \{0,1\}^* \setminus \{11\} \\ &= \{w \in \{0,1\}^* | w \text{ beginnt mit } 0\} \cup \\ &\quad \{w \in \{0,1\}^* | w \text{ beginnt mit } 10\} \cup \\ &\quad \{w \in \{0,1\}^* | w \text{ beginnt mit } 111\} \cup \\ &\quad \{w \in \{0,1\}^* | w \text{ beginnt mit } 110\} \cup \\ &\quad \{1\} \cup \\ &\quad \{\epsilon\}. \end{aligned}$$

Weiter gilt

$$\begin{aligned} \{0,1\}^* \setminus \{11\} &= L(0\{0,1\}^*) \\ \{w \in \{0,1\}^* | w \text{ beginnt mit } 0\} &= L(10\{0,1\}^*) \\ \{w \in \{0,1\}^* | w \text{ beginnt mit } 10\} &= L(111\{0,1\}^*) \\ \{w \in \{0,1\}^* | w \text{ beginnt mit } 10\} &= L(110\{0,1\}^*) \\ \{1\} &= L(1) \\ \{\epsilon\} &= L(\epsilon). \end{aligned}$$

□

Lemma 15
Die Sprache

$$L_2 = \{w \in \{0,1\}^* | w \textit{ enthält nicht die Teilfolge } 101\}$$

ist regulär.

Beweis. Sei

$$R_2 = ((0^*1^*)100)^*\, 0^*1^*(10|\epsilon).$$

Wir schreiben R_2 als S_1S_2 mit $S_1 = ((0^*1^*)100)^*$ und $S_2 = 0^*1^*(10|\epsilon)$. Wir zeigen $L_2 = L(R_2)$, indem wir die beiden folgenden Inklusionen zeigen.

1. $L(R_2) \subseteq L_2$
2. $L_2 \subseteq L(R_2)$.

zu 1. Wir schreiben R_2 als S_1S_2 mit $S_1 = ((0^*1^*)100)^*$ und $S_2 = 0^*1^*(10|\epsilon)$. Sei weiter $w \in L(R_2)$ beliebig. Damit können wir w schreiben als w_1w_2, wobei $w_1 \in L(S_1)$ und $w_2 \in L(S_2)$.

Die Teilfolge w_1 enthält nicht die Teilfolge 101, da in jeder Folge aus $L(S_1)$ auf eine 1 eine weitere 1 oder 00 folgt. Die Teilfolge w_2 kann ebenfalls nicht die Teilfolge 101 enthalten, da in jeder Folge aus $L(S_2$ auf eine 1 eine weitere 1 folgt oder eine 0 und dann das Ende der Teilfolge erreicht ist. Schließlich müssen wir uns noch überzeugen, dass die Teilfolge 101 nicht durch die letzten Symbole von w_1 und die ersten Symbol von w_2 gebildet werden kann. Nach Definition von S_1 ist jedoch entweder $w_1 = \epsilon$ oder w_1 endet mit einer 0. Damit kann die Teilfolge 101 nicht aus den letzteren Symbolen von w_1 und den ersten Symbolen von w_2 gebildet werden.

zu 2. Sei $w \in L_2$ beliebig. Wir zeigen $w \in L(R_2)$. Wir betrachten zwei Fälle

a) w enthält die Teilfolge 10 nicht,

b) w enthält die Teilfolge 10.

zu a) In diesem Fall gilt $w \in L(0^*1^*)$, da auf keine 1 eine weitere 0 folgen kann. Da $L(0^*1^*) \subset L(S_2)$ und $\epsilon \in L(S_1)$, gilt in diesem Fall $w \in L(R_2)$.

zu b) Wir unterteilen die Folge w in Teilfolgen $w_1 w_2 \dots w_t$, wobei

- Für $i = 1, \dots, t$ enthält w_i die Teilfolge 100 höchstens einmal.
- Für $i = 1, \dots, t-1$ endet w_i mit 100.
- w_t enthält nicht die Teilfolge 100.

Dann gilt

- $w_i \in L((0^*1^*)100), i = 1, \dots, t-1$ und $w_1 \dots w_{t-1} \in L(S_1)$
- $w_t \in L(S_2)$

Insgesamt gilt $w \in L(R_2)$.

□

Reguläre Sprachen

Satz 5 (Pumpimg Lemma für reguläre Sprachen)
Sei $L \subseteq \Sigma^*$ regulär. Dann gibt es ein $p \in \mathbb{N}$, so dass für alle $x \in L$ mit $|x| \geq p$ eine Aufteilung von x in 3 Teile $u, v, w \in \Sigma^*, x = uvw$ existiert mit:

1. $|uv| \leq p$
2. $|v| \geq 1$
3. *für alle $i \geq 0$ liegt das Wort uv^iw in L.*

Beweis. Da L regulär ist, gibt es einen DFA $A = (Q, \Sigma, \delta, q_0, F)$ mit $L(A) = L$. Wie setzen nun $p := |Q|$. Weiter sei $x = x_1 \cdots x_m \in L$ beliebig mit $|x| = m \geq p$. Seien schließlich $q_0 = r_0, r_1, \dots, r_m$ die Zustände, die A bei Eingabe x durchläuft. Da $x \in L$ gilt $r_m \in F$. Aus $m \geq p$, können wir schliessen, dass $i, j, 0 \leq i, j \leq p, i < j$, gibt mit $r_i = r_j$. Wir setzen

$$\begin{aligned} u &:= x_1 \cdots x_i, v := x_{i+1} \cdots x_j, \\ w &:= x_{j+1} \cdots x_m \end{aligned}$$

Nach Definition von u, v und w erfüllt die Aufteilung von x in uvw die Eigenschaften 1. und 2. des Satzes. Es muss noch gezeigt werden, dass die Aufteilung auch Eigenschaft 3. erfüllt.

Wir betrachten zunächst den Fall $i = 0$. Hier erhalten wir

$$\begin{aligned} \delta(q_0, uv^0w) &= \delta(q_0, uw) \\ &= \delta(\delta(q_0, u), w) \\ &= \delta(r_j, w) \\ &= r_m. \end{aligned}$$

Da $r_m \in F$ gilt $uv^0w \in L$.

Als nächstes betrachten wir den Fall $i \geq 1$. Nutzen wir aus, dass für alle $k \geq 1$ gilt

$$\delta(r_j, v^kw) = \delta(\delta(r_j, v), v^{k-1}w) = \delta(r_j, v^{k-1}w),$$

erhalten wir

$$
\begin{aligned}
\delta(q_0, uv^i w) &= \delta(\delta(q_0, u), v^i w) \\
&= \delta(r_j, v^i w) \\
&= \delta(\delta(r_j, v), v^{i-1} w) \\
&= \delta(r_j, v^{i-1} w) \\
&\vdots \\
&= \delta(r_j, vw) \\
&= \delta(\delta(r_j, v), w) \\
&= \delta(r_j, w) = r_m.
\end{aligned}
$$

Wiederum folgt aus $r_m \in F$, dass $uv^i w \in L$. Damit ist der Satz bewiesen. □

Satz 6
Die Sprache $\{0^n 1^n \mid n \geq 0\}$ *ist nicht regulär.*

Beweis. Um diesen wie auch die beiden folgenden Sätzen zu beweisen, nutzen wir die Kontraposition des Pumping Lemmas für reguläre Sprachen:

Wenn für alle $p \in \mathbb{N}$ *ein* $x \in L$ *existiert mit* $|x| \geq p$ *so dass für alle Aufteilungen* $x = uvw$ *mit* $|uv| \leq p, |v| \geq 1$, *ein* $i \geq 0$ *existiert, so dass* $uv^i w \notin L$, *dann ist* L *nicht regulär.*

Nun zum eigentlichen Beweis. Sei $p \in \mathbb{N}$ beliebig und sei $x = 0^p 1^p$. Damit gilt $x \in L_1$ und $|x| \geq p$. Sei $x = uvw$ eine beliebige Aufteilung von x, die $|uv| \leq p$ und $|v| \geq$ erfüllt. Dann gilt $v = 0^k$ mit $1 \leq k \leq p$. Wir wählen nun $i = 2$. Damit gilt $uv^i w = 0^{p+k} 1^p$ und $uv^i w = uv^2 w \notin L_1$. Aus dem Pumping Lemma (Anwendung der Kontraposition) folgt, dass L_1 nicht regulär ist. □

Satz 7
Die Sprache $L_2 := \{1^{n^2} | n \geq 1\}$ *ist nicht regulär.*

Beweis. Sei $p \in \mathbb{N}$ beliebig. Wir wählen $x = 1^{p^2}$, also $x \in L_2$ und $|x| \geq p$. Sei $x = uvw$ eine beliebige Aufteilung von x mit $|uv| \leq p$ und $1 \leq |v| \leq p$. Wir wählen $i = 2$. Dann gilt $uv^i w = 1^{|x|+|v|} = 1^{p^2+|v|}$. Aus $p^2 + |v| > p^2$ und $p^2 + |v| \leq p^2 + p < (p+1)^2$ folgt, dass $p^2 + |v|$ kein Quadrat ist. Damit gilt $uv^i w \notin L_2$. Aus dem Pumping Lemma (Anwendung der Kontraposition) folgt, dass L_2 nicht regulär ist. □

Satz 8
Die Sprache $L_3 := \{1^q | q$ *Primzahl*$\}$ *ist nicht regulär.*

Beweis.

$p \in \mathbb{N}$ beliebig. Aus der Zahlentheorie ist bekannt, dass es unendlich viele Primzahlen gibt. Also gibt es zu jeder natürlichen Zahl n eine Primzahl, die größer ist als n. Wir können daher eine Primzah $q \geq p + 2$ wählen. Sei $x = 1^q$, also $x \in L_3$ und nach Wahl von q gilt $|x| \geq p$. Sei weiter $x = uvw$ eine beliebige Aufteilung von x mit $|uv| \leq p$ und $|v| \geq 1$. us $|uv| \leq p$ und $q \geq p + 2$ folgt $|uw| \geq 2$. Wir wählen $i = |uw|$. Somit gilt

$$uv^i w = 1^{|uw|+i|v|} = 1^{|uw|+|uw||v|} = 1^{(|v|+1)|uw|}.$$

Weiter wissen wir, dass $|uw|, |v| + 1 \geq 2$. Damit kann $(|v| + 1)|uw|$ keine Primzahl sein. Also gilt $uv^i w = 1^{(|v|+1)|uw|} \notin L_3$. Aus dem Pumping Lemma (Anwendung der Kontraposition) folgt, dass L_3 nicht regulär ist. □