Gliederung der Vorlesung

0. Einleitung und Grundbegriffe
1. Endliche Automaten
2. Formale Sprachen
3. Berechenbarkeitstheorie
4. Komplexitätstheorie

0.1. Hinführung zu Berechenbarkeit und Komplexität
0.2. Problemtransformation
0.3. Mathematische Grundlagen und Vorarbeiten
- **Sprachen**
- Mengen und Relationen
- Graphen und Wege

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

Alphabete / Zeichenketten / Sprachen

Alphabet

- Ein Alphabet Σ ist eine endliche Menge von Zeichen (Symbolen).

  $\Sigma = \{ a,b,c,\ldots,z \}$; $\Sigma_1 = \{ A,B,C,\ldots,Z \}$; $\Sigma_2 = \{ 0,1,\ldots,9 \}$

Zeichenketten und ihre Länge

- Eine Zeichenkette (ein Wort) ist eine endliche Folge von Zeichen.

  anton (über Σ), 123 (über Σ_2), ACHTUNG (über Σ_1)
  besondere Zeichenkette: ε (das leere Wort)

- Die Länge einer Zeichenkette u ist die Anzahl der Zeichen von u.

  $|\ \text{anton}\ | = 5$
  $|\ 123\ | = 3$
  $|\ \varepsilon\ | = 0$

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Verkettung zweier Zeichenketten

- Das Ergebnis der Verkettung $u \circ v$ von zwei Zeichenketten u und v ist die Zeichenkette, die entsteht, wenn v an u angehängt wird.

$u = abc$; $v = def$	→	$u \circ v = abc \circ def = abcdef$
$u_1 = aa$; $v_1 = bb$	→	$u_1 \circ v_1 = aa \circ bb = aabb$
$u_2 = aba$; $v_2 = \varepsilon$	→	$u_2 \circ v_2 = aba \circ \varepsilon = aba$
		$v_2 \circ u_2 = \varepsilon \circ aba = aba$

Gebräuchliche Abkürzungen

a^3	→ aaa
$a^3 \circ b^3$ bzw. a^3b^3	→ aaabbb
a^0	→ ε

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Menge aller Zeichenketten (informell)

- Σ^* ist die Menge aller Zeichenketten (aller Wörter) über dem Alphabet Σ.

  - Es sei Σ = { a, b }; dann ist ...

    Σ^* = { ε, a,b, aa,ab,ba,bb,
    aaa,...,bbb, aaaa,....,bbbb,
    ... }

Übrigens sind die Σ^*-Beispiele oben „längen-lexikographisch" geordnet, nicht wie im Lexikon (lexikalisch, lexikographisch).

Was ist der Unterschied?
... insbesondere beim Aufzählen unendlicher Sprachen?

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

Menge aller Zeichenketten (formal; induktive Definition 1)

- Es sei Σ ein Alphabet.
- Wir definieren die Menge Σ^* wie folgt induktiv:

<u>Induktionsanfang:</u> $\varepsilon \in \Sigma^*$

<u>Induktionsschritt:</u> $w \in \Sigma^*$ und $x \in \Sigma \;\Rightarrow\; w \circ x \in \Sigma^*$

:

Die Menge Σ^* bildet zusammen mit der Verkettungsoperation $\circ$ eine Halbgruppe,
wobei das leere Wort ε das neutrale Element ist.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

Menge aller Zeichenketten (formal; induktive Definition 2)

- Es sei Σ das zugrunde liegende Alphabet
- Wir definieren für alle $n \in N$ die Menge Σ^n wie folgt:

<u>Induktionsanfang:</u> $\Sigma^0 = \{ \varepsilon \}$
<u>Induktionsschritt:</u> $\Sigma^{n+1} = \{ w \circ x \mid w \in \Sigma^n \text{ und } x \in \Sigma \}$

- ... und verwenden Σ^* als Abkürzung für:

$$\Sigma^* = \bigcup_{i \in N} \Sigma^i \quad (= \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \ldots)$$

Sprachen

- Eine Menge $L \subseteq \Sigma^*$ ist eine (formale) Sprache.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Sprachen, Wortproblem

▶ formale Sprachen

- Eine (formale) Sprache (über Σ) ist eine Menge $L \subseteq \Sigma^*$.

▶ das Wortproblem

- Sei L eine formale Sprache über einem Alphabet Σ
- Beim Wortproblem für die Sprache L geht es um das folgende Entscheidungsproblem:

zulässige Eingaben:	eine Zeichenkette $w \in \Sigma^*$
zulässige Ausgaben:	Antwort auf die Frage, ob $w \in L$ gilt (ja/nein, W/F, 1/0)

Wir befassen uns mit
- unterschiedlichen Möglichkeiten, formale Sprachen zu beschreiben,
- und der Frage, ob und – wenn ja – wie effizient man jeweils das Wortproblem lösen kann

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

- Formale Sprachen sind für Informatiker wichtig.

  - Formalen Sprachen begegnen wir sehr häufig :

    Die Menge aller möglichen Eingaben, die ein Programm an einer bestimmten Stelle erwartet, bildet eine formale Sprache

  Beispiele:

    - die Menge aller „Quelltexte“ für Programme in einer bestimmten Programmiersprache, die sich mit einem Compiler für diese Programmsprache übersetzen lassen,
    - die Menge aller „Quelltexte“ für Dokumente, die von einem bestimmten Internet-Browser dargestellt werden können,
    - alle „Quelltexte“ für Dokumente, die ein Textverarbeitungssystem verarbeiten kann.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

Beschreibungen von Sprachen

- Es gibt u.a. die folgenden Ansätze eine Sprache L zu beschreiben
  - Man gibt direkt ein Programm an, das das **Wortproblem** für die Sprache L löst (Das geht nicht für alle Sprachen.). L ist die Menge aller Wörter, bei denen das Programm „ja“ ausgibt.
  - Man gibt Regeln an, die es erlauben, genau die zu L gehörenden Wörter zu **erzeugen**. Das geht auch dann, wenn es kein Programm gibt, das das Wortproblem für L löst.
  - Das Erzeugungsproblem lässt sich auf das Wortproblem **reduzieren**. Man erzeugt systematisch alle Wörter w aus Σ^*, entscheidet jeweils, ob $w \in L$, und gibt nur die w mit der Antwort „ja“ aus.

Beispiel (erster Ansatz)

- Es seien $\Sigma = \{ 0,1 \}$ und
- $L = \{ w \in \Sigma^* \mid w$ hat genauso viele Nullen wie Einsen $\}$.

Algorithmus für Wortproblem:

- Verarbeite das gegebene Wort w zeichenweise von links nach rechts.
- Initialisiere zwei Zähler C_0 und C_1 jeweils mit 0.
- Wenn das aktuell gelesene Zeichen …
  - eine Null ist, so setze $C_0 = C_0+1$;
  - eine Eins ist, so setze $C_1 = C_1+1$.
- Falls C_0 und C_1 nach vollständiger Verarbeitung von w denselben Wert haben, gib „ja“ aus; sonst gib „nein“ aus.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Beispiel (zweiter Ansatz)

- Es seien $\Sigma = \{ 0,1 \}$ und
- $L = \{ w \in \Sigma^* \mid w$ hat genauso viele Nullen wie Einsen $\}$.

Erzeugungsregeln (hier: simultane Induktion mit Hilfssprachen)**:**

- ε ist ein Wort von L (= L_0)
- Ist n eine ganze Zahl und w ein Wort in L_n, so ist $w \circ 0$ ein Wort in L_{n-1} und $w \circ 1$ ein Wort in L_{n+1}.

Wörter in L_3 z.B. haben 3 mehr Einsen als Nullen.

- Ist n eine ganze Zahl, v ein Wort in L_n und w ein Wort in L_{-n}, so ist $v \circ w$ ein Wort in L.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

▶ Präfix / Suffix (informell)

- Jedes Anfangsstück einer Zeichenkette u heißt Präfix von u.

  u = anton → ε, a, an, ant, anto, anton
  u_1 = 123 → ε, 1, 12, 123

- Jedes Endstück einer Zeichenkette u heißt Suffix von u.

  u = anton → ε, n, on, ton, nton, anton
  u_1 = 123 → ε, 3, 23, 123

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Präfix / Suffix (formal)

- es sei Σ das zugrunde liegende Alphabet
- es sei $u \in \Sigma^*$

Ein Wort $p \in \Sigma^*$ ist ein Präfix von u gdw. es gibt ein Wort $w \in \Sigma^*$ mit $p \circ w = u$.

Ein Wort $s \in \Sigma^*$ ist ein Suffix von u gdw. es gibt ein Wort $w \in \Sigma^*$ mit $w \circ s = u$.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Gliederung der Vorlesung

0. Einleitung und Grundbegriffe
1. Endliche Automaten
2. Formale Sprachen
3. Berechenbarkeitstheorie
4. Komplexitätstheorie

0.1. Hinführung zu Berechenbarkeit und Komplexität
0.2. Problemtransformation
0.3. Mathematische Grundlagen und Vorarbeiten
- Sprachen
- **Mengen und Relationen**
- Graphen und Wege

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

Mengen

- Eine Menge ist eine Zusammenfassung von Elementen.

  $M = \{ n \mid n \in N \text{ und } n \bmod 2 = 0 \}$
  $M_1 = \{ v \circ 111 \mid v \in \Sigma^* \}$, wobei $\Sigma = \{ 0,1 \}$ gelte
  besondere Menge: $\varnothing$

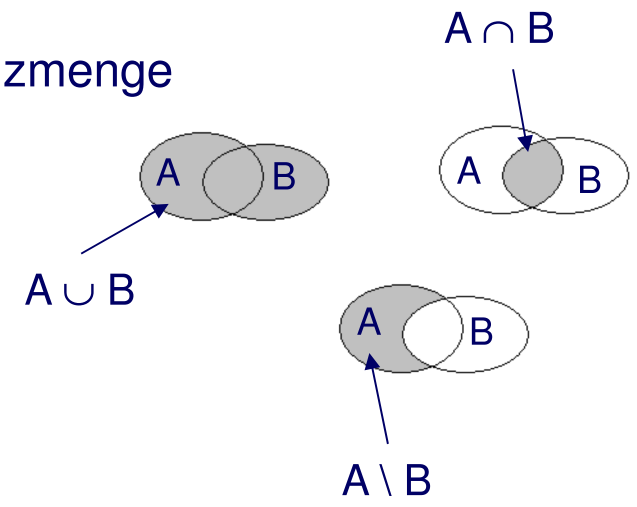
Teilmenge / Obermenge

- $A \subseteq B \leftrightarrow$ jedes Element von A ist auch ein Element von B
- $A \supseteq B \leftrightarrow$ jedes Element von B ist auch ein Element von A

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Durchschnitt / Vereinigung / Differenz / Potenzmenge

- $A \cup B = \{ x \mid x \in A \text{ oder } x \in B \}$
- $A \cap B = \{ x \mid x \in A \text{ und } x \in B \}$
- $A \setminus B = \{ x \mid x \in A \text{ und } x \notin B \}$
- $2^A = \{ M \mid M \subseteq A \}$



Einfache Zusammenhänge

- $A \subseteq (A \cup B)$, $B \subseteq (A \cup B)$
- $(A \cap B) \subseteq A$, $(A \cap B) \subseteq B$
- $(A \setminus B) \subseteq A$
- $\emptyset \in 2^A$, $A \in 2^A$

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

Mächtigkeit einer Menge

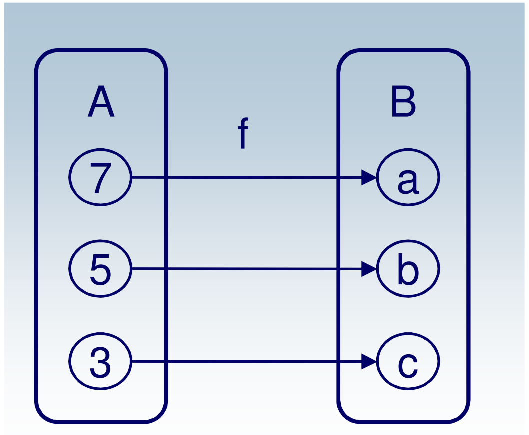
- $|A|$ ist die Anzahl der Elemente der Menge A.

  Bei unendlichen Mengen erfordert der Begriff eine eigene kleine Theorie ... → *Kardinalzahlen*

- 2^A hat $2^{|A|}$ Elemente: $|2^A| = 2^{|A|}$.

Mächtigkeitsvergleiche

- $|A| = |B|$ gilt gdw.:
  Es existiert eine bijektive Abbildung $f : A \to B$



- A heißt abzählbar, wenn $|A| = |\mathbb{N}|$.

$A = \{a_0, a_1, a_2, \dots\}$ (oder $\{a_1, a_2, a_3, \dots\}$)

Beispiele für abzählbare Mengen

- die Menge N der natürlichen Zahlen
- die Menge Q der rationalen Zahlen
- die Menge aller Zeichenketten über einem endlichen Alphabet
- jede unendliche formale Sprache über einem endlichen Alphabet

Beispiele für nicht abzählbare unendliche (überabzählbare) Mengen

- die Menge der reellen Zahlen (bereits zwischen 0 und 1)
- die Potenzmenge jeder abzählbaren Menge
- die Menge aller formalen Sprachen über einem endlichen Alphabet

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

Cantorsches Diagonalverfahren an einem Beispiel ...

> Die Menge der reellen Zahlen zwischen 0 und 1 ist nicht abzählbar.

Georg Cantors Beweis (1877)

- Annahme: Sie ist abzählbar.
- Dann kann man ihre Elemente abzählen: $r_1, r_2, r_3, \ldots$, und zwar jedes als unendlichen (!) Dezimalbruch

$$r_1 = 0,\; r_{11}\, r_{12}\, r_{13} \ldots$$
$$r_2 = 0,\; r_{21}\, r_{22}\, r_{23} \ldots$$
$$r_3 = 0,\; r_{31}\, r_{32}\, r_{33} \ldots$$

usw.

z.B. 0,1 = 0,0999...

- Sei nun die reele Zahl $s := 0, s_1\, s_2\, s_3 \ldots$ gegeben durch: $s_k := 5$ wenn $r_{kk} \neq 5$, ansonsten 4.
- Ist s eine der Zahlen $r_1, r_2, r_3, \ldots$?
- Also ist die Annahme falsch. (Widerspruchsbeweis)

$s_k \neq r_{kk}$, also $s \neq r_k$

Ja und Nein !!

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Binäre Relationen

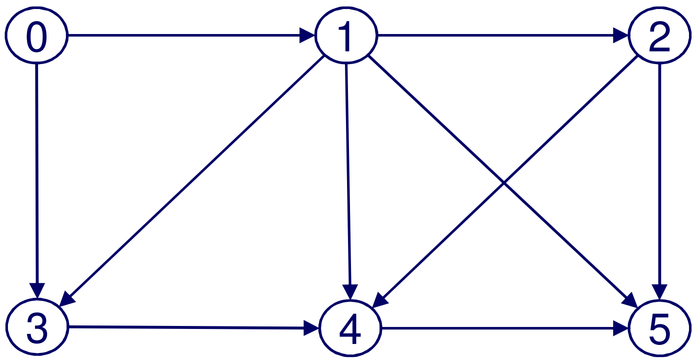
- Eine binäre Relation R zwischen A und B ist eine Menge von geordneten Paaren, d.h. $R \subseteq \{ (a,b) \mid a \in A \text{ und } b \in B \}$.
    - aRb ist eine andere Schreibweise für $(a,b) \in R$.
    - Falls $A = B$ gilt, so nennt man R Relation auf A.

Eine Relation auf A entspricht einem gerichteten Graphen mit Knotenmenge A.

Beispiel

$A = \{ 0,1,2,3,4,5 \}$

$R = \{ (0,1),(0,3),(1,2),(1,3),(1,4),(1,5),$
$(2,4),(2,5),(3,4),(4,5) \}$



 © 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

Reflexivität / Symmetrie / Transitivität

- Eine Relation R auf A ist reflexiv gdw. für alle $a \in A$ gilt: $(a,a) \in R$.

- Eine Relation R auf A ist symmetrisch gdw. für alle $a,b \in A$ gilt: Wenn $(a,b) \in R$, so $(b,a) \in R$.

- Eine Relation R auf A ist transitiv gdw. für alle $a,b,c \in A$ gilt: Wenn $(a,b) \in R$ und $(b,c) \in R$, so auch $(a,c) \in R$.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Transitive Hülle

- Die transitive Hülle Trans(R) einer Relation R auf A ist die kleinste Relation mit folgenden Eigenschaften:
    - wenn $(a,b) \in R$, so $(a,b) \in \text{Trans}(R)$
    - wenn $(a,b) \in \text{Trans}(R)$ und $(b,c) \in \text{Trans}(R)$, so $(a,c) \in \text{Trans}(R)$

... statt Trans(R) ist auch die Bezeichnung R^+ üblich

Reflexive Hülle

- Die reflexive Hülle Refl(R) einer Relation R über A ist die wie folgt definierte Relation: $\text{Refl}(R) = R \cup \{ (a,a) \mid a \in A \}$.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Ein einfacher Zusammenhang

- es sei R eine Relation R über A

Dann gilt: Refl(Trans(R)) = Trans(Refl(R)).

... es ist egal, ob man erst die transitive und dann die reflexive Hülle oder erst die reflexive und dann die transitive Hülle bildet

Reflexive und transitive Hülle

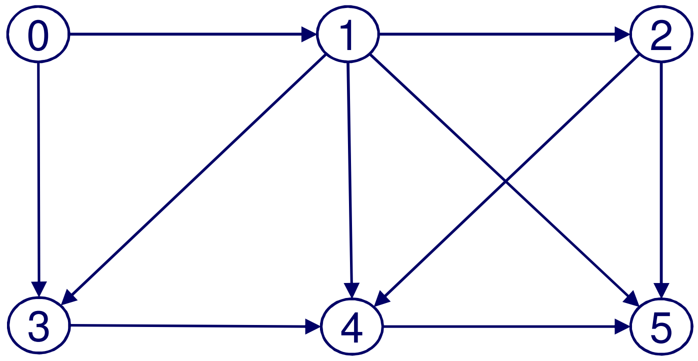
- Die reflexive und transitive Hülle R* einer Relation R über A ist die wie folgt definierte Relation: R* = Refl(Trans(R)).

... per Definition gilt: $R^* = R^+ \cup \{ (a,a) \mid a \in A \}$

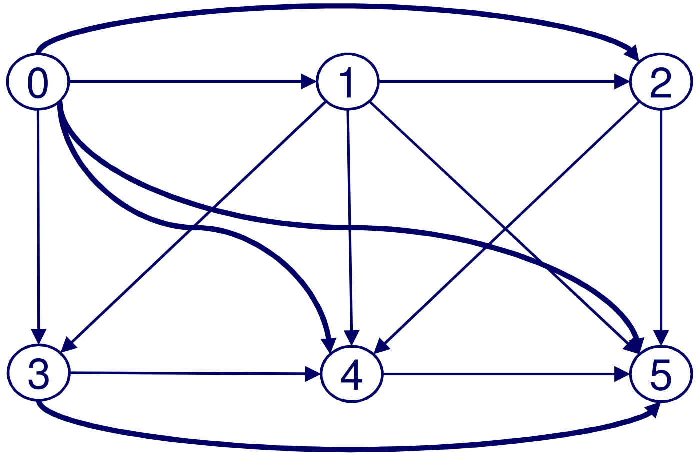
© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

- Beispiel

A = { 0,1,2,3,4,5 }
R = { (0,1),(0,3),(1,2),(1,3),(1,4),(1,5),
(2,4),(2,5),(3,4),(4,5) }



R⁺ = { (0,1),(0,3),**(0,2)**,**(0,4)**,**(0,5)**,
(1,2), (1,3),(1,4),(1,5),(2,4),
(2,5),(3,4),**(3,5)**,(4,5) }



© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

▶ Begriff: Äquivalenzrelation

- Sei M eine Menge und R eine zweistellige Relation über M.

- R ist eine Äquivalenzrelation über M, falls gilt:
  - R ist reflexiv, d.h. für alle $x \in M$ gilt: xRx,
  - R ist symmetrisch, d.h. für alle $x,y \in M$ gilt: $xRy \Rightarrow yRx$, und
  - R ist transitiv, d.h. für alle $x,y,z \in M$ gilt: xRy und $yRz \Rightarrow xRz$.

▶ Begriff: Klasseneinteilung / Partition

- Sei M eine Menge und $K = \{ M_i \mid i \in I \}$ eine Menge von nichtleeren Teilmengen von M.

- K ist eine Klasseneinteilung (bzw. Partition) der Menge M, falls gilt:
  - Je zwei verschiedene Mengen in K sind disjunkt: $i \neq k \Rightarrow M_i \cap M_k = \emptyset$
  - M wird von den M_i überdeckt: $M = \bigcup_{i \in I} M_i$

  … bzw.: Jedes $x \in M$ liegt in genau einem M_i.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Zusammenspiel der beiden Begriffe

- Sei M eine Menge und R eine Äquivalenzrelation über M,
- und für jedes $x \in M$ sei $[x]_R = \{ y \in R \mid xRy \}$, die Äquivalenzklasse von x.
- Dann gilt:

Die Menge $K = \{ [x]_R \mid x \in M \}$ ist eine , (die durch R induzierte) Klasseneinteilung auf der Menge M

- Sei M eine Menge und $K = \{ M_i \mid i \in I \}$ eine Klasseneinteilung auf der Menge M,
- und für alle $x,y \in M$ sei xRy die Relation „x und y liegen in derselben Menge M_i."
- Dann gilt:

Die Relation R ist eine (die durch K induzierte) Äquivalenzrelation auf der Menge M.

Genau dann induziert R K, wenn K R induziert.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Beispiel

- Sei M die Menge aller Schüler einer Schule mit festen Klassen.
- Sei R wie folgt definiert:
  - Für zwei Schüler s und s‘ gilt genau dann sRs‘, wenn s und s‘ in dieselbe Schulklasse gehen.
- Dann gilt:
  - R ist eine Äquivalenzrelation über M.
  - Die Äquivalenzklasse $[s]_R$ eines Schülers s ist die Schulklasse, in die dieser Schüler geht.
  - Die Äquivalenzklassen der durch R auf M induzierten Klassen-einteilung K sind genau die Schulklassen dieser Schule.

 © 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

Vergleich von Äquivalenzrelationen

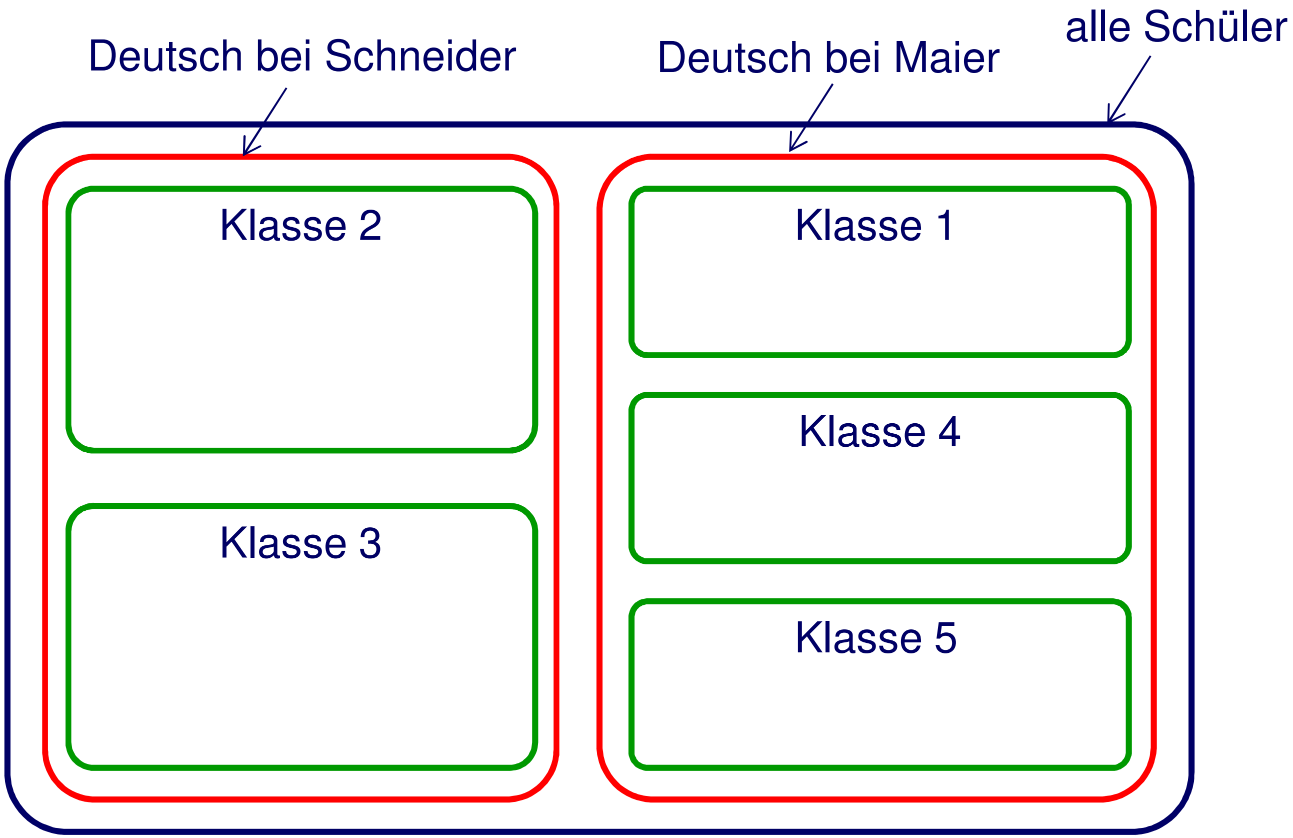
- Seien M eine Menge und R und Q Äquivalenzrelationen auf M.
- Dann nennt man R feiner als Q, falls gilt:
  - wenn (als Teilmengen von $M \times M$) $R \subseteq Q$,
  - bzw. - gleichbedeutend –
    für alle $x,y \in M$ gilt $xRy \Rightarrow xQy$.

Dem entspricht in den induzierten Klasseneinteilungen K_R und K_Q,
dass K_R feiner als K_Q ist, d.h. dass

- jede R-Äquivalenzklasse $[x]_R$ eines Elements x ganz in dessen Q-Äquivalenzklasse $[x]_Q$ enthalten ist,
- bzw. - gleichbedeutend –
  dass für alle $M_R \in K_R$ ein $M_Q \in K_Q$ mit $M_R \subseteq M_Q$ existiert.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

- Im Schulbeispiel … : R feiner als Q
  - R = gehen in dieselbe Schulklasse
  - Q = haben denselben Deutschlehrer



 © 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

Äquivalenzrelationen und Abbildungen

- Sei R eine Relation auf einer Menge M.
  Dann gilt genau dann

  - R ist eine Äquivalenzrelation

  wenn gilt

  - Es existiert eine Menge M' und eine Abbildung $f\colon M \to M'$ so, dass für alle $x,y \in M$ gilt: $x \mathrel{R} y$ gdw. $f(x) = f(y)$.

Äquivalenz bedeutet Wertegleichheit unter einer Abbildung.

Beweisidee $\Rightarrow$: f ordne jedem Element seine Äquivalenzklasse zu.

Beweisidee $\Leftarrow$: Verwenden: = ist Äquivalenzrelation

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Mehrstellige Relationen

- Eine n-stellige Relation R zwischen Mengen $M_1, \ldots, M_n$ ist eine Menge von n-Tupeln (≈ records, ohne Namen für die Positionen) mit den entsprechenden Komponenten,
  d.h. $R \subseteq \{ (x_1, \ldots, x_n) \mid \text{für } i=1, \ldots, n: x_i \in M_i \}$.

Beispiele

- M_1 = Personen, M_2 = Warengruppen, M_3 = Ladentypen
- R = Einkaufsgewohnheiten
- Frau Müller kauft Kleidung bei Kik.
- Frau Maier kauft Kleidung bei Desigual.
- Herr Blaumann kauft Schnaps an der Tankstelle.

R = { (Mü,Kl,Ki),
(Ma,Kl,De),
(Bl,Sc,Ta) }

- $M_1 = M_3$ = Personen, M_2 = soziale Beziehungsweisen
- Q = soziale Beziehungen
- Frau Müller beneidet Frau Maier.
- Frau Maier geht Herrn Blaumann aus dem Weg.
- Herr Bl. und Frau Müller sind im gleichen Kegelverein (und nicht identisch).

Q = { (Mü,Be,Ma),
(Ma,Gw,Bl),
(Bl,Kv,Mü),
(Mü,Kv,Bl) }

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

Relationen: Beschreibungsvarianten

- Beschreibung der beteiligten Mengen, im letzten Beispiel …

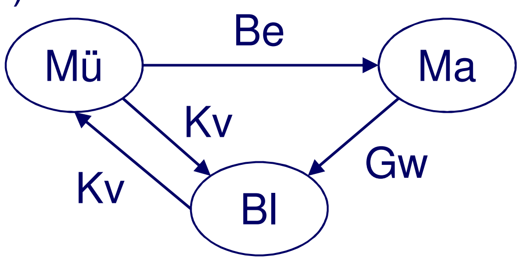
  M_1 = M_3 = Personen = { Mü, Ma, Bl }, M_2 = soziale Beziehungsweisen = …

- Beschreibung der Tupelmenge

  Da gibt es zahlreiche Alternativen!

  - **Liste**/Aufzählung der Tupel
    im Beispiel: Q = { (Mü,Be,Ma), (Ma,Gw,Bl), (Bl,Kv,Mü), (Mü,Kv,Bl), }

  - **Graphen** (beschriftet, manchmal möglich)
    im Beispiel:



  - **Funktionen/Abbildungen**

  - z.B. so: Q_1(Mü) = { (Be,Ma), (Kv,Bl) }, Q_1(Ma) = … usw.
  - oder so: Q_2(Mü,Be) = { Ma }, Q_2(Mü,Kv) = { Bl }, … usw.
  - oder geschachtelt: Q_3(Mü,P_1) , P_1(Be) = { Ma }, … usw.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Beschreibungsvarianten von Relationen, Konsequenzen

- Die Umgruppierungen im Punkt „Funktionen/Abbildungen“ erzeugen mit *Funktionen* natürlich auch spezielle (linkstotal, rechtseindeutige) *Relationen*, die letztlich definiert oder aufgezählt werden müssen.
- Eigentlich ein und dieselbe Relation *kann* nicht nur auf solche unterschiedlichste Weisen definiert bzw. beschrieben werden – das *passiert* auch tatsächlich!
- … und führt dann oft dazu, dass die im Prinzip gleichen Begriffe in unterschiedlichen Büchern oder Webseiten scheinbar ganz unterschiedlich definiert werden. ☹
- Da Haskell Curry (1900-1982) als (fast) erster diese Darstellungsweisen systematisch verwendet und untersucht hat, nennt man den Übergang zwischen solchen Varianten auch Currying.

 © 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

Gliederung der Vorlesung

0. Einleitung und Grundbegriffe
1. Endliche Automaten
2. Formale Sprachen
3. Berechenbarkeitstheorie
4. Komplexitätstheorie

0.1. Hinführung zu Berechenbarkeit und Komplexität
0.2. Problemtransformation
0.3. Mathematische Grundlagen und Vorarbeiten
- Sprachen
- Mengen und Relationen
- **Graphen und Wege**

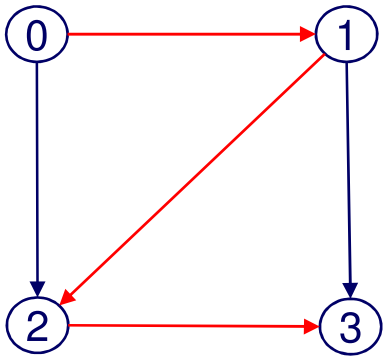
© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten

▶ Wege … von a nach b, und ihre Länge (induktive Definition)

- Es sei (R,A) ein gerichteter Graph über einer Menge A.
- Wir definieren Wege in (R,A) [von $a \in A$ nach $b \in A$ & ihre Länge] wie folgt:

<u>Induktionsanfang:</u> ε ist ein Weg der Länge 0 von a nach a.
<u>Induktionsschritt:</u> Ist w ein Weg von a nach b der Länge n und $(b,c) \in R$, dann ist w(b,c) ein Weg von a nach c der Länge n+1.

- $W_{a,b}$ sei die Menge aller Wege von a nach b.



Anfangsknoten Endknoten

w = (0,1) (1,2) (2,3) $\in W_{0,3}$, Weg: Wort über R.

Gleichwertige Sichtweise eines Wegs als Knotenfolge:

w = 0 1 2 3 Weg: Wort über A.

... passende induktive Definition(en)?

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Graphen und Wege

Geschlossene Wege (Schleifen)

- Es sei (R,A) ein gerichteter Graph über einer Menge A.
- Ein Weg $u = (u_0,u_1) \ldots (u_{m-1}, u_m)$
heißt geschlossen oder Schleife genau dann, wenn $u_0=u_m$.

  Spezialfall: der leere Weg ε der Länge 0 von a nach a.

Wie sehen bei Knotenfolgen-Sichtweise Schleifen aus?
... und leere Schleifen?

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Etwas mehr über Wege …

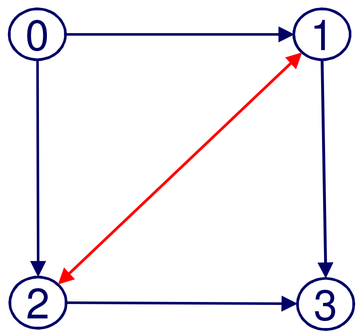
- Lange Wege in „kleinen“ Graphen (d.h. mit wenigen Knoten)

<u>Schleifen-Lemma</u> für Wege:

- Es sei (R,A) ein gerichteter Graph über einer Menge A mit n Knoten.
- Es sei w ein Weg (w_0,w_1) … (w_{m-1}, w_m)
  (also aus m Kanten bzw. über m+1 Knoten) mit $m \geq n$.

- Dann enthält w eine nicht leere Schleife (w_i,w_{i+1}) … (w_{k-1}, w_k)
  (also mit $w_i = w_k$) mit $0 \leq i < k \leq n$.

Beispiel



w = 0 1 2 1 3
w = (0,1)(1,2)(2,1)(1,3)

Begründung:

Da w über mindestens n+1 Knoten führt, und es nur n<n+1 verschiedene gibt, muss er bei mindestens einem Knoten zweimal vorbeiführen.

pigeonhole principle – Taubenschlagprinzip

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Etwas mehr über Wege …

- „Pumping“ bei Schleifen

Eine nicht leere Schleife in einem Weg von a nach b
Garantiert die Existenz *eines kürzeren*
und *unendlich vieler längerer*
Wege von a nach b:

w = 0 1 2 1 3
w = (0,1)(1,2)(2,1)(1,3)

0 1 3
(0,1) (1,3)

0 1 2 1 2 1 3
(0,1)(1,2)(2,1)(1,2)(2,1)(1,3)

0 1 2 1 2 1 2 1 3
(0,1)(1,2)(2,1)(1,2)(2,1) (1,2)(2,1)(1,3)

usw.

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Etwas mehr über Wege

Verkettung von Wegen

Es seien

- (R,A) ein gerichteter Graph über einer Menge A,
- $a,b,c \in A$,
- $u = (u_0,u_1) \ldots (u_{m-1}, u_m) \in W_{a,b}$ $(u_0=a,\ u_m=b)$ und
  $v = (v_0,v_1) \ldots (v_{n-1}, v_n) \in W_{b,c}$ $(v_0=b,\ v_n=c)$.

Die Verkettung $u \circ v := (u_0,u_1) \ldots (u_{m-1}, u_m)\ (v_0,v_1) \ldots (v_{n-1}, v_n)$
ist ein Weg von $u_0=a$ nach $v_n=c$.

Achtung bei Knotenfolgen-Sichtweise:
Endknoten u_m = *Anfangsknoten* v_0 –
erscheint in $u \bullet v := u_0 \ldots u_m\, v_1 \ldots v_n$ *an der „Klebestelle" nur einmal!*

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Etwas mehr über Wege …

Verkettung von Schleifen

- Die Verkettung $u \circ v$ zweier Schleifen $u,v \in W_{a,a}$ ist wiederum eine Schleife $\in W_{a,a}$.

- Für jede Teilmenge $Q \subseteq W_{a,a}$ ist Q^*, die Menge aller endlichen Verkettungen von Schleifen aus Q, induktiv definiert durch

Induktionsanfang:	$\varnothing \in Q^*$
Induktionsschritt:	Ist $u \in Q^*$ und $v \in Q$ dann ist $u \circ v \in Q^*$.

induktiv beweisbar: $Q^* \subseteq W_{a,a}$

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Etwas mehr über Wege …

- Wege über ausgewählte Zwischenknoten

Es seien
- (R,A) ein gerichteter Graph über einer Menge A und
- A = {0, 1, 2, …, n}

<u>Zwischenknoten-Lemma für Wege</u>:

Sei $W_{i,j,k}$ die Menge der Wege von i nach j,
bei denen nach dem Anfangsknoten i
und vor dem Endknoten j
nur Knoten l mit $l \leq k$ vorkommen.

Dann ist

$$W_{i,j,k+1} = W_{i,j,k} \cup W_{i,k+1,k} (W_{k+1,k+1,k})^* W_{k+1,j,k}$$

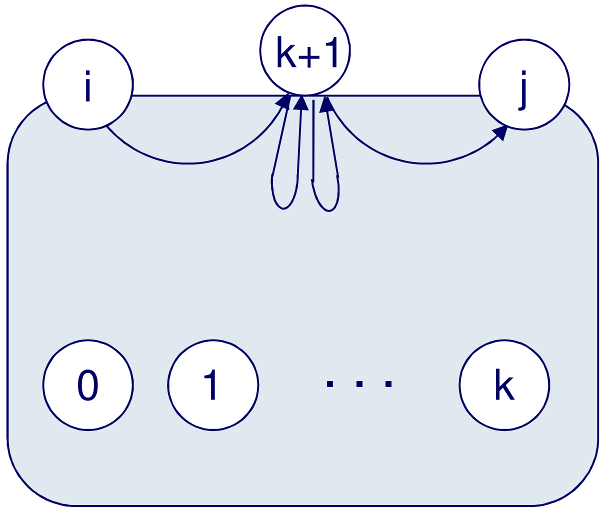
© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik

Etwas mehr über Wege ...

- Klingt kompliziert?

Zwischenknoten-Lemma

$$W_{i,j,k+1} = W_{i,j,k} \cup W_{i,k+1,k}\ (W_{k+1,k+1,k})^*\ W_{k+1,j,k}$$



... egal ob i bzw. j ≤ k oder nicht.

Begründung:

Sei $w \in W_{i,j,k+1}$.

Entweder ist (k+1) gar nicht unter den Zwischenknoten, also $u \in W_{i,j,k}$.

Oder es geht von i
zum ersten Mal nach (k+1),

dann evtl. noch mehrmals
von (k+1) zu sich selbst

und nach dem letzten Mal von (k+1) nach j

(jeweils über Zwischenknoten ≤ k).

© 2017 Prof. Steffen Lange, Dr. Bernd Baumgarten - h_da/FbI - Theoretische Informatik