23.03.2015
MONTAG

LUDS ZUSATZVORLESUNG KLAUSURBESPRECHUNG

① Mathematische Grundlagen

a) Induktion

zeig $\sum_{k=1}^{n}(k+1)\,2^k = n \cdot 2^{n+1}$ für alle $n \in \mathbb{N}$ gilt

IA: $n=1$: $\sum_{k=1}^{1}(k+1)\,2^k = 2 \cdot 2^1 = 4 = 1 \cdot 2^2$

IV: Annahme die Aussage gilt für $n \in \mathbb{N}$

IS: $n \rightsquigarrow n+1$

$$\sum_{k=1}^{n+1}(k+1)2^k = \sum_{k=1}^{n}(k+1)\,2^k + (n+2)\,2^{n+1}$$

$$\overset{IV}{=} n \cdot 2^{n+1} + n \cdot 2^{n+1} + 2 \cdot 2^{n+1}$$

$$= 2n\,2^{n+1} + 2 \cdot 2^{n+1}$$

$$= n \cdot 2^{n+2} + 2^{n+2}$$

$$= (n+1) \cdot 2^{n+2}$$

$\square$

b) Funktionen, Injektivität, Surjektivität

Bijektivität

M, N nichtleere endl. Menge. $f: M \to N$ Abbildung

Zeige: $\forall n \in N \quad g(n) = m \iff f(m) = n$

defin. Abbildung $g: N \to M$ g.d.w. f bijektiv ist

1:1 Beziehung

(i) $g(n) = m$ und $g(n) = m'$ $\quad m, m' \in M$

$\Rightarrow m = m'$ (Eindeutigkeit des Bildes)

(ii) $\forall n \in N : \exists m \in M : g(n) = m$

(Existenz des Bildes)

(i) ist äquivalent zu (laut Def.)

$f(m) = n$ und $f(m') = n$

$\Rightarrow m = m'$

$\iff f$ injektiv

(ii) ist äquivalent zu $\forall n \in N \; \exists m \in M : f(m) = n$

$\iff f$ surjektiv

$\Rightarrow$ (i)+(ii) $\iff f$ bijektiv

$\boxed{\text{Umkehrbildung} \Rightarrow \text{Bijektiv}}$

c) Relationen, $\underbrace{\text{Reflexivität, Symmetrie, Transitivität}}_{\text{Äquivalenzrelation}}$

$$R = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid \exists a,b \in \mathbb{N} : y = a \cdot x^b\}$$

Gebe an, ob R reflexiv, symmetrisch oder transitiv ist

Reflexiv: Sei $x \in \mathbb{N}$ wollen $x = a \cdot x^b$ gilt für $a = b = 1 \in \mathbb{N}$

$\Rightarrow xRx \Rightarrow R$ reflexiv

Symmetrie: Sei $x = 1$ und $y = 2$ $\quad xRy$, da $2 = 2 \cdot 1^1$

Angenommen yRx: $x = a \cdot y^b \Rightarrow 1 = a \cdot 2^b$, da $b \geq 1 \Rightarrow 2^b \geq 2$

$a = 0{,}5$ nicht erlaubt

$\Rightarrow a < 1 \Rightarrow a \notin \mathbb{N}$ $\lightning$

$\Rightarrow R$ nicht symmetrisch

c)
Beh.

Transitiv: Seien $x, y, z \in \mathbb{N}$ mit $x R y$ und $y R z$

Dann ex. $a, b, c, d \in \mathbb{N}$ mit $y = a x^b$ und $z = c \cdot y^d$

x relativ

$$\Rightarrow z = c\left(a x^b\right)^d = \left(c \cdot a^d\right) x^{b \cdot d}$$

Da $c \cdot a^d \in \mathbb{N}$ und $b \cdot d \in \mathbb{N}$ folgt $x R z$

$\Rightarrow R$ transitiv

d) Relationen, Antisymmetrie

Wieviele symmetrische und gleichzeitig antisymmetr. Relationen $R \subseteq M \times M$ auf der Menge M gilt es?

Symmetr.: $x R y \Rightarrow y R x$

antisym. $x R y$ und $y R x \Rightarrow x = y$

$\Rightarrow$ Elemente dürfen nur zu sich selbst relatieren

$\Rightarrow R \subseteq \{(x, x) \mid x \in M\}$

Anzahl aller möglichen Teilmengen ist $|\mathcal{P}(M)| = 2^{|M|}$

② Endliche Automaten und formale Sprachen

Def. - Grammatik (Σ, V, S, P), reguläre Grammatik

- DFA $(Q, \Sigma, \delta : Q \times \Sigma \to Q, q_0, F)$

- Pumping Lemma

anders als Funktion

- NFA $(Q, \Sigma, \delta, q_0, F)$

$$\delta \subseteq (Q \times \Sigma) \times Q$$

δ ist Relation und keine Funktion

a) Wie sind die Ableitungsregeln einer regulären Grammatik definiert?

$A \to v$ mit $A \in V$ und $v = \varepsilon$ oder $v = aB$ mit $a \in \Sigma$ und $B \in V$

b) Seien L_1 und L_2 Sprachen über Σ

Zeige oder widerlege die Aussage

$$L_1^* = L_2^* \Rightarrow L_1 = L_2$$

Kleenescher Abschluss L_1^*

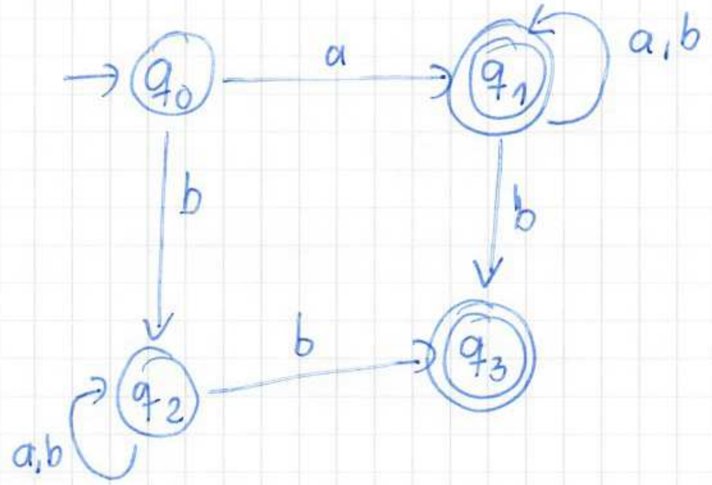
$L_1 = \{1\}$ und $L_2 = \{1, 11\} \Rightarrow L_1 \neq L_2$

Aber $L_1^* = L_2^*$ $\lightning$

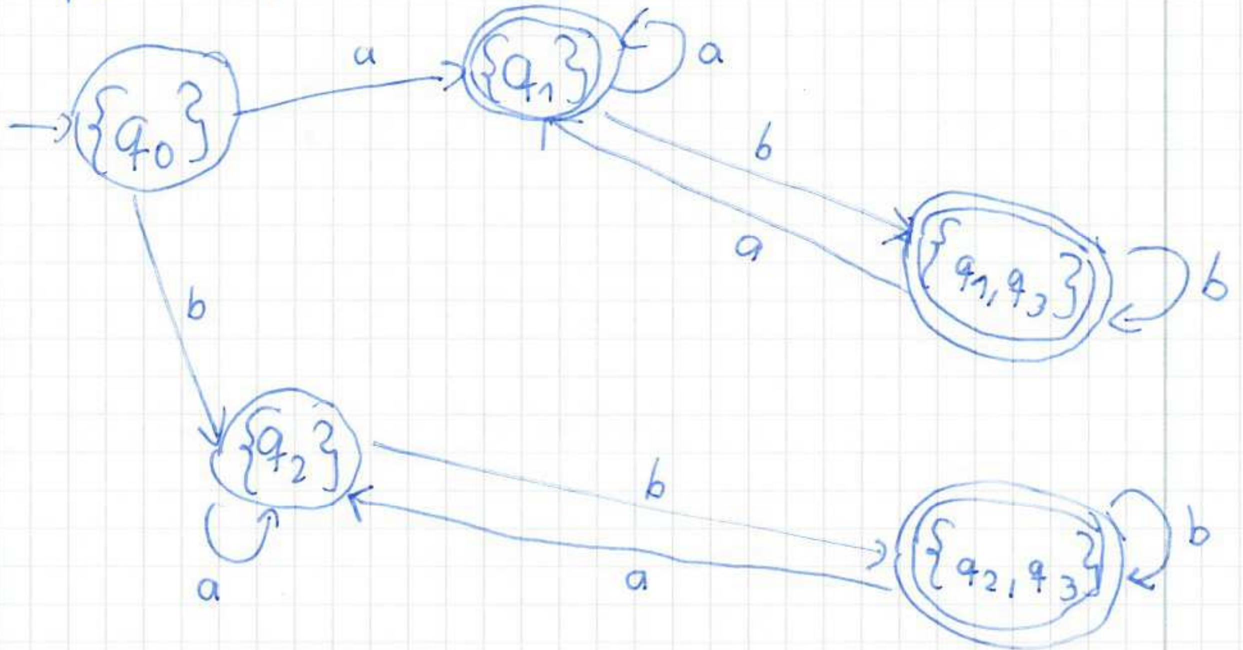
unendliche Folge nötig

1, 11

c) Gebe einen DFA an, der dieselbe Sprache entscheidet wie folgender NFA



POTENZMENGENKONSTRUKTION



d) Sei L reguläre Sprache über Σ

Ist $L' = \{ww \mid w \in L\}$ regulär?

Gegenbeispiel Sei $L = \{0^m 1 \mid m \in \mathbb{N}\}$

Sei $x = 0^n 1 \in L$: $n \in \mathbb{N}$

$z = x \cdot x = 0^n 1 0^n 1 \in L'$, $|z| \geq n$

Sei $z = uvw$ mit $|u \cdot v| \leq n$ $\Rightarrow$ uv besteht nur aus Nullen

$|v| \geq 1$ $\Rightarrow$ uv^iw für $i > 1$ hat die Form

$0^{|u| + |v|i} 1 0^n 1 \notin L'$, da existiert kein $x \in L$ mit

$x \cdot x = u \cdot v^i w$

$\Rightarrow$ L' nicht regulär

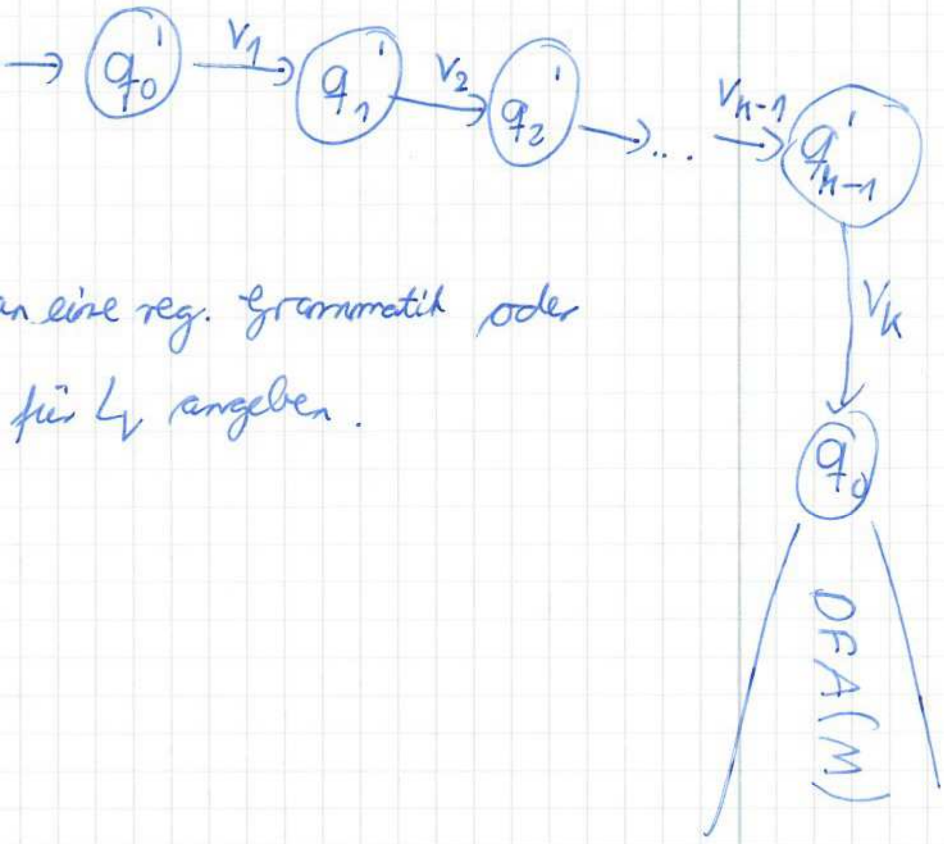
e) Sei L reguläre Sprache über Σ und $v \in L$

Ist $L_v = \{vw \mid w \in L\}$ regulär

Ja! Zeige ex. DFA der L_v entscheidet

Sei M DFA der L entscheidet, $v = v_1 \ldots\ldots v_k$

Betrachte M_v:



Alternativ kann man eine reg. Grammatik oder regulären Ausdruck für L_v angeben.

③ Ausgewählte Themen der Mathematik

Halbgruppen, Monoide, Gruppen, Ringe, Körper

a) Seien $(A,*)$ und $(B,\circ)$ Gruppen

Zeige, dass auch $(A\times B,\cdot)$ mit $(a_1,b_1)\cdot(a_2,b_2)=(a_1 * a_2, b_1\circ b_2)$

eine Gruppe ist.

i) Abgeschlossenheit von $\cdot$

Da $a_1 * a_2 \in A$ und $b_1\circ b_2\in B$, da $(A,\times)$ und $(B,\circ)$ Gruppen sind, folgt $(a_1,b_1)\cdot(a_2,b_2)\in A\times B$

ii) Assoziativität von $\cdot$ Seien $(a_1,b_1),(a_2,b_2),(a_3,b_3)\in A\times B$

$$((a_1,b_1)\cdot(a_2,b_2))\cdot(a_3,b_3)=(a_1 * a_2, b_1\circ b_2)\cdot(a_3,b_3)$$

$$=((a_1 * a_2) * a_3, (b_1\circ b_2)\circ b_3)$$

$$\overset{*,\circ \text{ assoziativ}}{=} (a_1 * (a_2 * a_3), b_1\circ(b_2\circ b_3))$$

$$= (a_1,b_1)\cdot(a_2 * a_3, b_2\circ b_3)$$

$$= (a_1,b_1)\cdot((a_2,b_2)\cdot(a_3,b_3))$$

iii) Neutrales Element

Seien 0_A und 0_B neutr. Elemente von A und B

Dann ist $(0_A,0_B)\in A\times B$ neutr. Element von $(A\times B,\cdot)$, da

$$(0_A,0_B)(a_1,b_1)=(0_A * a_1, 0_B\circ b_1)=(a_1,b_1)$$

$$=(a_1\times 0_A, b_1\circ 0_B)=(a_1,b_1)\cdot(0_A,0_B)$$

iv) Inverse Elemente

Seien $-a$ bzw $-b$ invers zu a bzw b in A bzw B

Dann ist $(-a,-b) \in A \times B$ invers zu $(a,b) \in A \times B$, da

$$(a,b) \cdot (-a,-b) = (a * (-a), b \circ (-b)) = (0_A, 0_B)$$

$$= ((-a) * a, (-b) \circ b) = (-a,-b) \cdot (a,b)$$

b) Euklidischer Algorithmus

Bestimme ggT von $a = 19$ und $b = 10$

$$19 = 1 \cdot 10 + 9$$

$$10 = 1 \cdot 9 + 1$$

$$9 = 9 \cdot \underline{\underline{1}} + 0 \quad \Longrightarrow ggT(10,19) = 1$$

c) Inverse in Restklassen

Bestimme das Inverse von $[\![10]\!]$ in $(\mathbb{Z}/19\mathbb{Z}, \odot_{19})$

mit b) $\quad 1 = 10 - 1 \cdot 9$

$$= 10 - 1(19 - 1 \cdot 10)$$

$$= -1 \cdot 19 + \underline{\underline{2}} \cdot 10$$

Das Inverse ist $[\![2]\!]_{19}$

d) Chinesischer Restsatz

Bestimme eine Zahl $x \in \{0, \dots\dots, 99\}$ mit

$x \equiv 9 \mod 10$ mit c) $x = 9 \cdot (-1) \cdot 19 + 13 \cdot 2 \cdot 10$

$x \equiv 13 \mod 19$ $\qquad = -171 + 260$

$= \underline{\underline{89}}$

e) Sei $G = (M, \cdot)$ ein Monoid.

Zeige jedes $a \in M$ besitzt höchstens ein inverses Element $b \in M$

Sei c neutr. Element von M (existiert da M Monoid)

Seien $a \cdot b = c = b \cdot a$ Angenommen ex $b' \neq b$ $b' \in M$ mit $a \cdot b' = e = b' \cdot a$

$$b = b \cdot e = b \cdot a \cdot b' = e \cdot b' = b'$$

$\Rightarrow b = b'$ ↯

④ Mathematische Logik

a) Wahlen im Zweiparteiensystem, Drei Wähler A, B und C

- A sagt: „Wenn ich P.1 gewählt habe, dann auch B und C
- B sagt: „ — „ — „ — „ dann weder A noch C
- C sagt: „ — „ — „ — „ dann auch A oder B

Gebe Formel f an, die die Aussagen modelliert. Gebe an, wer wen gewählt hat.

$x \in \{a, b, c\}$ $\quad X \mathrel{\hat{=}} x$ wählt P. 1

$\neg X \mathrel{\hat{=}}$ ~~x~~ wählt P. 2.

$$f = (a \rightarrow b \wedge c) \wedge (b \rightarrow \neg a \wedge \neg c) \wedge (c \rightarrow a \vee b)$$

a	b	c	f	
0	0	0	1	$\rightarrow \neg a \wedge \neg b \wedge \neg c$
0	0	1	0	
0	1	0	1	$\rightarrow \neg a \wedge b \wedge \neg c$
0	1	1	0	
1	0	0	0	
1	0	1	0	
1	1	0	0	
1	1	1	0	

$\Rightarrow$ A und C wählen P.2
von B weiß man es nicht

$\boxed{\text{KNF}}$

$(\neg a \wedge \neg b \wedge \neg c) \vee (\neg a \wedge b \wedge \neg c)$

$(\neg a \vee \neg c) \wedge (b \wedge \neg b)$

0

b) Strukturelle Induktion

Sei AL_1 kleinste Teilsprache von AL mit folgenden Eigenschaften.

- Für jede Aussagevariable $x \in AV$ gilt $x \in AL_1$
- Ist $f_1 \in AL_1 \Rightarrow \neg f_1 \in AL_1$
- Sind $f_1, f_2 \in AL_2$ mit $Var(f_1) \cap Var(f_2) = \emptyset$

  $\Rightarrow (f_1 \wedge f_2) \in AL_1$ und $(f_1 \vee f_2) \in AL_1$

Zeige jede Formel $f \in AL_1$ ist erfüllbar, aber nicht gültig

rekursiv induktiv definiert

f erfüllbar $\Leftrightarrow$ $\exists$ passende Bewertung B mit $[\![f]\!]_B = 1$

f gültig $\Leftrightarrow$ $\forall$ passenden Bewertungen — „ — gilt $[\![f]\!]_B = 1$

z.z. $\forall f \in AL_1$ ex. Bew. B, B' s.d. $[\![f]\!]_B = 1$ und $[\![f]\!]_{B'} = 0$

I.A. Betrachte $f = x \in AV$

Für $B(x) = 1$ gilt $[\![f]\!]_B = 1$ und für $B'(x) = 0 \Rightarrow [\![f]\!]_{B'} = 0$

IV Aussage gilt für $f' \in AL_1$

ii) $f = \neg f'$ für $f' \in AL_1$

$[\![f]\!]_B = [\![\neg f']\!]_B = 1 - [\![f']\!]_B$

Laut I.V existiert B, B' mit $[\![f]\!]_B = 1$ und $[\![f']\!]_{B'} = 0$

$\Rightarrow [\![f]\!]_{B'} = 1$ und $[\![f]\!]_B = 0$

(ii) $\varphi = (\varphi_1 \vee \varphi_2)$ mit $\varphi_1, \varphi_2 \in AL_1$, $Var(\varphi_1) \cap Var(\varphi_2) = \emptyset$

I.V. ist erfüllt für φ_1 und φ_2

$$[\![\varphi]\!]_B = [\![\varphi_1 \vee \varphi_2]\!]_B = max\{[\![\varphi_1]\!]_B, [\![\varphi_2]\!]_B\}$$

Da $Var(\varphi_1) \cap Var(\varphi_2) = \emptyset$ ex. B und B' mit $[\![\varphi_1]\!]_B = [\![\varphi_2]\!]_B = 1$

und $[\![\varphi_1]\!]_{B'} = [\![\varphi_2]\!]_{B'} = 0$

$\Rightarrow [\![\varphi]\!]_B = 1$ und $[\![\varphi]\!]_{B'} = 0$

iii) $\varphi = (\varphi_1 \wedge \varphi_2)$

$$[\![\varphi]\!]_B = [\![\varphi_1 \wedge \varphi_2]\!]_B = min\{[\![\varphi_1]\!]_B, [\![\varphi_2]\!]_B\}$$

Seien B, B' wie in ii)

$[\![\varphi]\!]_B = 1$ und $[\![\varphi]\!]_{B'} = 0$

$\square$

Entscheide ob folgende Formel erfüllbar, gültig oder unerfüllbar sind.

$$f_1 = (x_1 \rightarrow x_2) \leftrightarrow ((x_1 \wedge \neg x_2) \rightarrow x_2)$$

$$= \neg(x_1 \wedge \neg x_2) \vee x_2$$

$$= \neg x_1 \vee x_2 \cancel{\vee x_2}$$

$$= x_1 \rightarrow x_2$$

$\Rightarrow f_1$ gültig

weil Äquivalente

$$f_2 = (x_1 \rightarrow x_2) \leftrightarrow ((x_1 \wedge \neg x_2) \rightarrow x_2) \wedge x_3$$

$$\Leftrightarrow (x_1 \rightarrow x_2) \leftrightarrow (x_1 \rightarrow x_2) \wedge x_3$$

f_2 erfüllt für $x_3 = 1$
nicht erfüllt für $x_3 = 0$
$\Rightarrow f_2$ erfüllbar aber nicht gültig

$$f_3 = (x_1 \rightarrow x_2) \wedge (x_1 \vee x_3) \wedge \neg(x_2 \vee x_3)$$

KNF Bed.

$$\Leftrightarrow (\neg x_1 \vee x_2) \wedge (x_1 \vee x_3) \wedge \neg x_2 \wedge \neg x_3$$

Resolutions-Kalkül

$$x_2 \wedge x_3$$

$$x_3$$

$$\Box$$

$\Rightarrow f_3$ unerfüllbar

DNF in KNF

d) Resolutionskalkül

$$(x_1 \vee \neg x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_2) \wedge x_3 \wedge (\neg x_2 \vee \neg x_3)$$

$$x_2 \wedge \neg x_3$$

$$\neg x_3$$

$$\square$$

unerfüllbar

(5) Sei L reguläre Sprache. Ist jede Sprache $L' \subseteq L$ stets regulär?

$L' = \{0^n 1^n \mid n \in \mathbb{N}\}$ nicht regulär

$L = \{0^n 1^m \mid n, m \in N\}$ ist regulär und $L' \subseteq L$

NEIN

Gebe einen regulären Ausdruck an, der die Sprache L entscheidet, wobei

$L = \{w \in \{0,1\}^* \mid$ entweder w beginnt mit 0 oder w endet mit $1\}$

$$0 + 0\,[0+1]^*\,0 + 1\,[0+1]^*\,1 + 1$$