Tutorium Theorie I, 3.11.2009

Notiztitel 11/3/2009

Bisherige Themen:

- mathematische Beweisfuehrung, Induktion

- Endliche Automaten, Konstruktion / Analyse

FRAGEN:

- Simultane / strukturelle Induktion
- Automaten analysieren mit Induktion

→ "Gleichzeitige Induktion" für ein y

gerade $\equiv x = 2y$

x gerade $\Leftrightarrow$ nicht (x ungerade) = ungerade $\equiv x = 2y+1$

Basis $x = 0$ $\quad$ 0 gerade "$= 2 \cdot 0$", 0 ~~nicht~~ ungerade, nicht $2y+1 = 0$ ↯

Behauptung gelte für $x = n$

Sei $x = n+1$

Falls x gerade, dann n ungerade

also n nicht gerade

also $n+1 = \cancel{x}$ nicht ungerade

2.4.3: $L_3 = \{ w \in \{0,1\}^* \mid$ w ist Binärdarstellung einer Zahl x mit $3 \mid x \}$

Bits kommen wie immer in 'absteigender' Reihenfolge d.h. größte Stelle ist links

Gesucht Automat, der L_3 akzeptiert

Idee: Bits kommen herein - wie ändert sich die Zahl x die bis jetzt beschrieben wurde?

$w_0 = \varepsilon \qquad x_0 = 0$

$w_1 = 1 \qquad$ '$x_0 x_1$' $= 1 = x_0 \cdot 2 + 1$

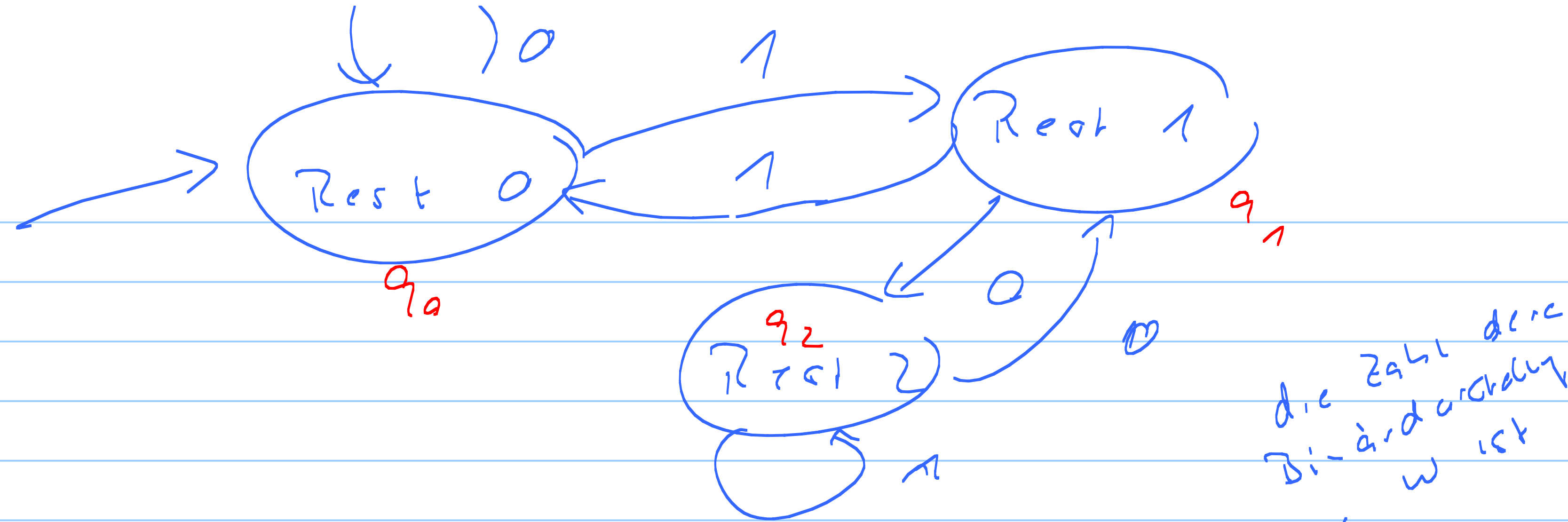
$w_2 = 0 \qquad$ '$x_0 x_1 x_2$' $= 2 \qquad x_0 x_1 \cdot 2 + 0$

$\varepsilon \quad 1 \quad 0$

alte Zahl wird verdoppelt, letztes Bit aufaddiert

Wie wirkt sich das auf Teilbarkeit aus?

wie schnell werde ich das von Teilbarkeit durch 3



zeige $B_0 :\equiv \hat\delta(q_0, w) = q_0 \iff bin(w) \bmod 3 = 0$

$B_1 :\equiv \hat\delta(q_0, w) = q_1 \iff$ " " $= 1$

$B_2 :\equiv \hat\delta(q_0, w) = q_2 \iff$ " " $= 2$

$$\boxed{\hat\delta(q_0, w) = q_i \iff bin(w) \bmod 3 = i}$$

Beweise $B_1 \wedge B_2 \wedge B_3$ durch simultane Induktion über die Struktur von w

(Aufbau von w: Entweder $w = \varepsilon$

oder $w = u0$ $\quad u \in \{0,1\}^*$

$w = u1$

Zahlen: $0 \to 1 \to 2 \to \dots\ n \to n+1$

Wörtern: $\varepsilon \to 0, 1$; $0 \to 00, 01$; $1 \to 10, 11$ … $u \to u0, u1$

allgemein: ε, $u \to ua$, $a \in \Sigma$, $u \in \Sigma^*$

Basisfall $w = \varepsilon$

$$\hat\delta(q_0, w) = \hat\delta(q, \varepsilon) = q_0$$

und $bin(w) = 0$ per Konvention

und $0 \bmod 3 = 0$

also folgt B_0 weil $\hat\delta(q_0, w) = q_0$ und $bin(w) \bmod 3 = 0$ ✓

(wahr $\Leftrightarrow$ wahr) = wahr = (falsch $\Leftrightarrow$ falsch))

B_1 weil $\hat\delta(q_0, w) \neq q_1$ und $bin(w) \bmod 3 \neq 1$

B_2 analog

Schrittfall: es gelte B_1, B_2, B_3 für ein $u \in \{0,1\}^*$

Sei $w = u0$ (später $w = u1$)

B_0: $\Rightarrow$ es gelte $\hat\delta(q_0, w) = q_0$

$\Leftarrow$ dann $\hat{\delta}(q_0, w) = \delta(\hat{\delta}(q_0, u), 0)$

$\Leftarrow$ dann muß $\hat{\delta}(q_0, u) = q_0$ sein (diagramm!)

$\Leftarrow$ also $bin(u) \bmod 3 = 0$ nach Ind. annahme B_0

$\Leftarrow$ dann $bin(w) = 2 \cdot bin(u) + 0$

und $bin(w) \bmod 3 =$

$= (2 \cdot bin(u) + 0) \bmod 3$

$(2 \cdot (bin(u) \bmod 3) + 0) \bmod 3$

$0 \bmod 3 = 0$

$\Leftarrow$ Es gelte $bin(w) \bmod 3 = 0$

dann $(2 \cdot bin(u) \bmod 3 \cancel{+0} \bmod 3) = 0$

dann $bin(u) \bmod 3 = 0$

also $\hat{\delta}(q_0, u) = q_0$ nach Annahme

also $\hat{\delta}(q_0, w) = \delta(q_0, 0) = q_0$ ✓

$\underline{B_1}$ $\underline{\text{Kurzfassung}}$: $\hat{\delta}(q_0, w) = q_1$

$\Leftrightarrow \hat{\delta}(q_0, u) = q_2$

$\Leftrightarrow bin(u) \bmod 3 = 2$ (Annahme B_2)

$\Leftrightarrow bin(w) \bmod 3 = (2 \cdot 2 + 0) \bmod 3 = 1$

$\underline{B_2}$ $\hat{\delta}(q_0, w) = q_2$

$\Leftrightarrow \hat{\delta}(q_0, u) = q_1$

Analog mit $\underline{B_1}$

$\Leftrightarrow$ bin(u) mod 3 = 1

$\Leftrightarrow$ bin(w) mod 3 = (2·1 + 0) mod 3 = 2

Falls w = u1 dann

B_0 analog mit B_1 statt B_0

B_1 analog mit B_0 statt B_2

B_2 analog mit B_2 statt B_1

1.4 Palindrome besser mit "vollständige Induktion"

- Pal(w) $\equiv$ $w = w^R$ (w und w rückwärts gleich)
- Pal'(ε), Pal'(a) für $a \in \Sigma$ abba a

Pal'(x) $\Leftrightarrow$ Pal'(axa) (kein andere Art Pal' zu erzeugen) b

zeige Pal(w) $\Leftarrow$ Pal'(w)

strukturelle Induktion ist nicht gut!

Induktion über Länge von w (|w|)

Start

$|w| = 0 \Rightarrow w = \varepsilon \quad Pal(w) \wedge Pal'(w)$

$|w| = 1 \Rightarrow w = a \in \Sigma \quad Pal(w) \wedge Pal'(w)$

Es gelte $Pal(u) \Leftrightarrow Pal'(u)$ für u mit $|u| < n$

und $n \geq 2$

Sei $|w| = n$ und es gelte $Pal(w)$

dann $w = a\,u\,a$ für ein $a \in \Sigma$

und $Pal(u)$

per Annahme (weil $|u| < n$)

wissen wir

$Pal'(u)$ und damit $Pal'(a u a)$

$\equiv Pal'(w)$

$\boxed{\text{Prinzip gilt } P(n) \text{ falls } P(i) \text{ für alle } i < n \text{ dann gilt } P(k) \text{ für alle } k\,!}$

Es gelte $Pal'(w)$ für w mit $|w| = n \geq 2$

dann per definition muß w die Form $w = a\,u\,a$

haben und $Pal'(u)$ gelten

per Annahme gilt $Pal(u)$ da $|u| < n$

und damit $Pal(ava)$ also $Pal(w)$