19.01.2015
MONTAG

LUDS BLATT 11

Aufgabe 7:

$M, |m| = 6$

z.zg. $\exists M' \subseteq M \quad |M'| = 3$, s.d. entweder $xRy \; \forall x \neq y$

oder $x \not R y \quad \forall x \neq y$.

Schubfachprinzip: Sei n Anzahl der Elemente, die verteilt werden sollen und m die Anzahl an Feldern und gilt $n > m \Rightarrow$ mindestes ein Fach muss mehr als ein Element enthalten

Sei $x \in M$ fixiert und S_0 und S_1 Schubfächer. Sei $y \in M: x \neq y$ und $x \in M$. Wenn $y \not R x$ dann lege y in S_0 und sonst in S_1. Da $|M \setminus \{x\}| = 5$ muss o.B.d.A. S_0 mindestens 3 Elemente enthalten. Seien $y_0, y_1, y_2 \in S_0$ unterschiedlich

Dann existiern zwei Fälle:

1. Fall $1 \leq i < j \leq 3$ so dass $y_i \not R y_j \Rightarrow M = \{x, y_i, y_j\}$ mit geforderten Eigenschaften

2. Fall ansonsten erfüllen $\{y_0, y_1, y_2\}$ die geforderten Eigenschafte

Aufgabe 5

$K = \{x \in \mathbb{R} \mid \forall q \in \mathbb{Q}\ x \cdot q \in \{\pi, \frac{1}{\pi}\}\}$

Ist $(K, +, \cdot)$ Körper?

Sei $a = \sqrt{2}$ und $b = \frac{\pi}{\sqrt{2}} \Rightarrow a \in K \wedge b \in K$

$a \cdot b = \sqrt{2} \cdot \frac{\pi}{\sqrt{2}} = \pi \notin K$

Aufgabe 1

$p = 5,\ q = 7 \qquad n = p \cdot q = 35$

$\varphi(n) = \varphi(p) \cdot \varphi(q) = 4 \cdot 6 = 24$

Sei $e \in \{5, 7, 11, 13, 17, 19, 23\}$, dann ist öff. Schlüsselpaar $(35, e)$

Der Text kann dann mittels $E(x) = \mathrm{mod}(x^e, n)$

verschlüsselt werden.

Suchen öffentlich (Schlüsselpaar) $SP(35, d)$, aber $d^{-1} = e$ in $\mathbb{Z}/n\mathbb{Z}$

Durch euklid. Algorithmus folgt $d = e \quad \forall e \in E$

Aufgabe 2:

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

x_1	x_2	x_3	φ
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

(2)

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

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

KANN FEHLERHAFT SEIN

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

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

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

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

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

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

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

Aufgabe 4

$(M, \circ)$ Halbgruppe $e \in M$ mit $e \circ x = x \; \forall x \in M$

und $\forall y \in M \; \exists x \in M$ so. dass $x \circ y = x$

Zu zeigen $(M, \circ)$ ist Gruppe

Wissen $\exists z \in M$ mit $z \circ x = e$

$y \circ x = e \circ (y \circ x) = (z \circ x) \circ (y \circ x)$

$= z \circ ((x \circ y) \circ x)$

$= z \circ (e \circ x)$

$= z \circ x$

$= e$

z.zg.

$x \circ e = e$

Sei $x \in M$ beliebig

$\Rightarrow \exists y \in M$ s.dass $y \circ x = e$

$x \circ e = x \circ (y \circ x) = (x \circ y) \circ x = e \circ x = x$

$\Rightarrow e$ NE und mit Eigenschaft von oben

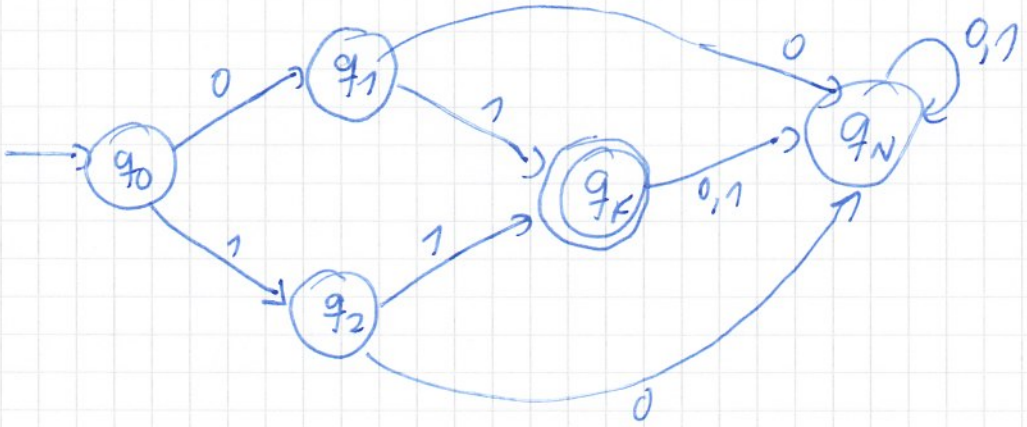
$\Rightarrow$ Alle $x \in M$ inv.

$\Rightarrow (M, \circ)$-Gruppe

Aufgabe 6:

$L \subseteq \{0,1\}^k$

a) $k=2$ $L=\{01,11\}$



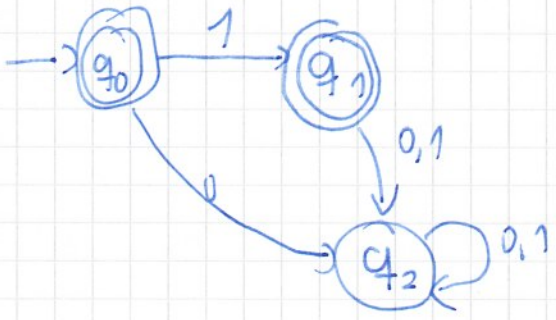
q_k = akzeptierender Zustand

q_N = nicht akzeptierbarer Zustand, in den $w \geq k$ gelangen

b) $k=1$

$L = L(R) = L((1+\varepsilon)) = \{\varepsilon, 1\}$

(regulär)



c)

y

Aufgabe 3)

$B: x \to \{0,1\}$ $\quad B': x' = \{0,1\}$

Zeige $\forall \varphi \in AL$ $Var(\varphi) \subseteq x \cap x'$ gilt

$B(x) = B'(x) \quad \forall x \in Var(\varphi) \Rightarrow [\![\varphi]\!]_B = [\![\varphi]\!]_B$

(IA) $\varphi = 0$, $\varphi = 1$ oder $\varphi = x \in x \cap x'$

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

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

$[\![x]\!]_B = x = [\![1]\!]_{B'}$

(IS) $\varphi = \neg \varphi_1 \qquad \varphi_1 \in AL$

$[\![\varphi]\!]_B = [\![\neg \varphi_1]\!]_B = 1 - [\![\varphi_1]\!]_B \overset{(IV)}{=} 1 - [\![\varphi_1]\!]_{B'} =$

$[\![\neg \varphi]\!]_{B'}$

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

$[\![\varphi]\!]_B = [\![\varphi_1 \wedge \varphi_2]\!]_B = \min\{[\![\varphi_1]\!]_B, [\![\varphi_2]\!]_B\} \overset{IV}{=} \min\{[\![\varphi_1]\!]_{B'}, [\![\varphi_2]\!]_{B'}\}$

$= [\![\varphi]\!]_{B'}$

ii) $\varphi = (\varphi_1 \vee \varphi_2)$

$[\![\varphi]\!]_B = [\![\varphi_1 \vee \varphi_2]\!]_B = \max\{[\![\varphi_1]\!]_B [\![\varphi_2]\!]_B\} \overset{(IV)}{=} \max\{[\![\varphi_1]\!]_{B'}, [\![\varphi_2]\!]_{B'}\}$

$= [\![\varphi]\!]_{B'}$

(iv) $\varphi = \varphi_1 \rightarrow \varphi_2 = \neg\varphi_1 \vee \varphi_2$ Folgt aus i) + iii) durch Hintereinanderschaltung

(v) $\varphi = \varphi_1 \leftrightarrow (\varphi_1 \rightarrow \varphi_2) \wedge (\varphi_2 \rightarrow \varphi_1)$ folgt aus (iv) + ii)