Universität Karlsruhe (TH)
Lehrstuhl Informatik für Ingenieure und Naturwissenschaftler
Dr. Thomas Worsch
Matthias Schulz
1. Oktober 2009

Vordiplomklausur im Fach Informatik (für Elektrotechniker)

Tragen Sie bitte Ihren Namen, Ihren Vornamen und Ihre Matrikelnummer *sorgfältig* und *gut lesbar* in die dafür vorgesehenen Felder ein:

Name:	

Vorname:	

Matr.–Nr.:							

Die folgende Tabelle wird **nur von den Korrektoren** ausgefüllt:

Aufgabe	1	2	3	4	5	6
Maximal-punktzahl	6	10	9	8	8	9
erreichte Punktzahl						

Punktsumme:	Note:

Diese Klausur besteht aus einem Deckblatt und weiteren **7** Blättern mit insgesamt **6** Aufgaben. Bitte überprüfen Sie Ihr Exemplar auf Vollständigkeit!

Tragen Sie bitte Ihren Namen und Ihre Matrikelnummer in *jede* Kopfzeile ein!

Legen Sie bitte Ihren Studentenausweis bereit und denken Sie daran, dass elektronische Hilfsmittel (insbesondere Taschenrechner) nicht erlaubt sind.

Sollten Sie andere Quellen als das Vorlesungsskript verwenden, geben Sie diese bitte an der entsprechenden Stelle an. Geben Sie an, falls Sie Rechentabellen verwenden.

Ihre Lösungen tragen Sie bitte in die vorhandenen Leerräume ein. Wenn Sie mehr Platz benötigen, können Sie die Rückseiten der Aufgabenblätter benutzen. Machen Sie in diesem Fall eindeutig klar, zu welcher Aufgabe eine Bearbeitung gehört!

Zum **Bestehen der Klausur** benötigen Sie mindestens **25** Punkte.

Zur Bearbeitung haben Sie 120 Minuten Zeit.

Wir wünschen Ihnen viel Erfolg!

Die Ergebnisse werden *voraussichtlich* in der Woche vom 5.10.2009 bis 9.10.2009 im WWW und per Aushang bekanntgegeben.

Aufgabe 1 (2+2+2 Punkte):

a) Geben Sie einen regulären Ausdruck R und eine Sprache $M \subsetneqq \langle R \rangle$ an, so dass M durch keinen regulären Ausdruck beschrieben werden kann.

$$R = a^*b^*, M = \{a^n b^n \mid n \in \mathbb{N}_0\}$$

b) Geben Sie eine Sprache M an, die durch keinen regulären Ausdruck beschrieben werden kann, und einen regulären Ausdruck R, für den gilt: $\langle R \rangle \subsetneqq M$.

$$R = ab, M = \{a^n b^n \mid n \in \mathbb{N}_0\}$$

c) Geben Sie eine Funktion $f : \mathbb{N}_0 \to \mathbb{R}^+$ an, so dass für jeden regulären Ausdruck R gilt:

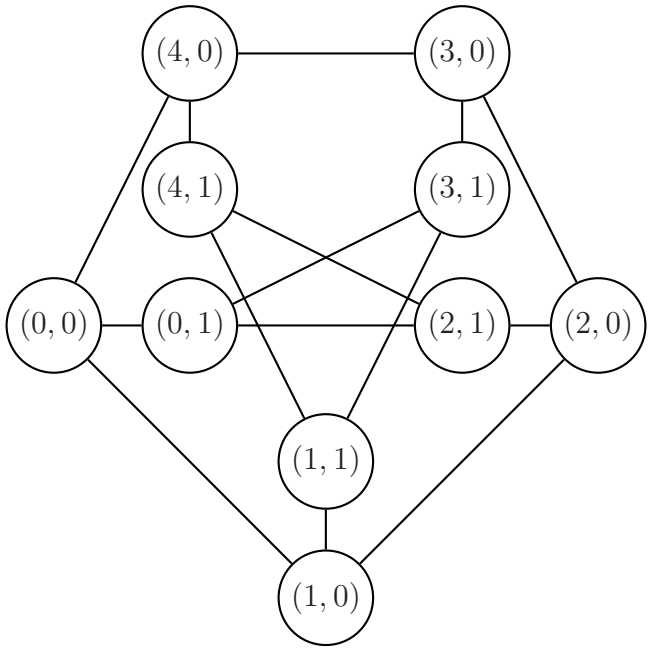
Die Zeit, die man braucht, um festzustellen, ob ein Wort w der Länge $n \in \mathbb{N}_0$ in $\langle R \rangle$ liegt, liegt in $O(f(n))$.

$$f(n) = n$$

Aufgabe 2 (3+2+3+2 Punkte): Für $n \in \mathbb{N}$ sei $N_n = \{0, \ldots, n-1\}$.
Für $n, k \in \mathbb{N}, n \geq 3$ sei der (ungerichtete) Graph $G_{n,k} = (V_n, E_{n,k})$ gegeben durch:

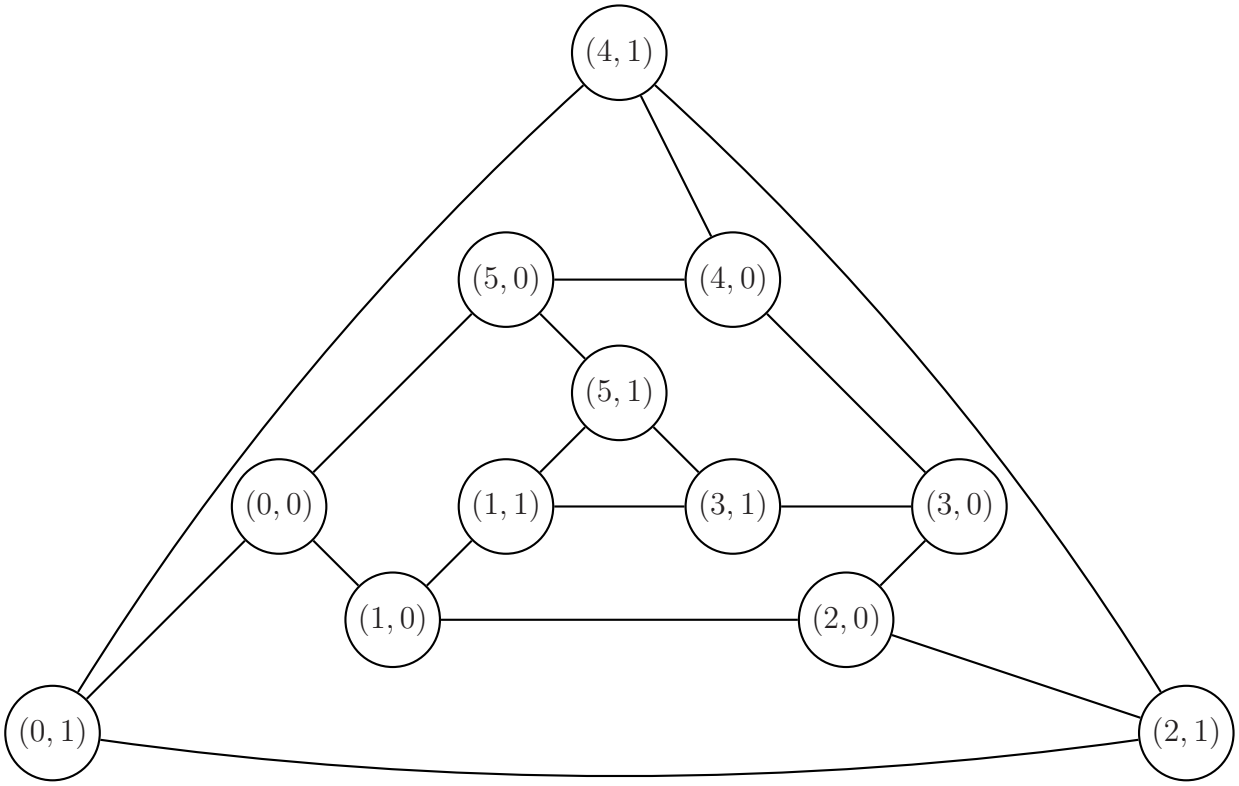
$$\begin{aligned} V_n &= \{(i,b) \mid i \in N_n, b \in N_2\}, \\ E_{n,k} &= \{\{(i,0),((i+1) \bmod n, 0)\} \mid i \in N_n\} \\ &\quad \cup \{\{(i,1),((i+k) \bmod n, 1)\} \mid i \in N_n\} \\ &\quad \cup \{\{(i,0),(i,1)\} \mid i \in N_n\} \end{aligned}$$

a) Stellen Sie die Graphen $G_{5,2}$ und $G_{6,2}$ graphisch dar.



$G_{5,2}$:

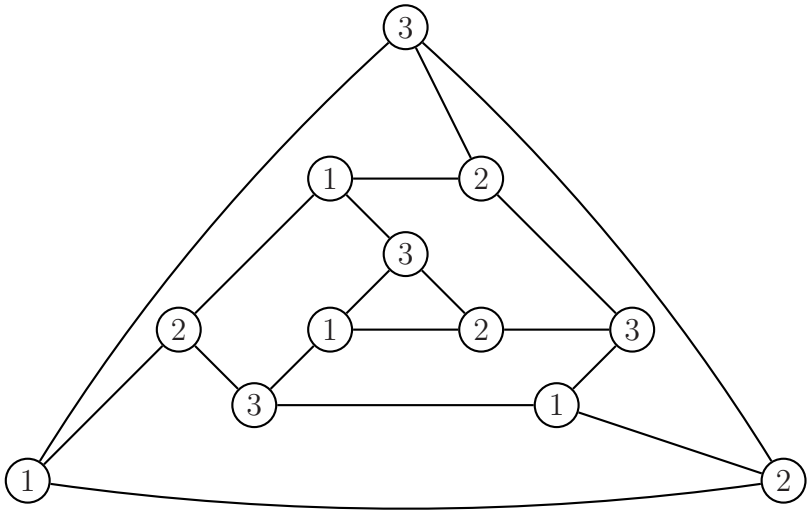
$G_{6,2}$:



b) Ist $G_{6,2}$ planar? Falls Ihre Antwort "ja" ist, geben Sie eine planare Darstellung von $G_{6,2}$ an. Falls Ihre Antwort "nein" ist, begründen Sie dies.

$G_{6,2}$ ist planar, siehe Abbildung.

c) Geben Sie eine 3-Färbung von $G_{6,2}$ an. (Sie können dazu die Darstellungen auf der vorherigen Seite verwenden.)



d) Sei $n \geq 10$ und gerade. Geben Sie die Bisektionsweite von $G_{n,1}$ an. (Ohne Beweis!)

Die Bisektionsweite ist 4.

Aufgabe 3 (2+2+2+3 Punkte): Die formale Sprache L sei als die Menge aller Wörter über dem Alphabet $\{a, b\}$ definiert, die **nicht** das Wort ab als Teilwort enthalten.
Die formale Sprache L_c sei als die Menge aller Wörter über dem Alphabet $\{a, b, c\}$ definiert, die **nicht** das Wort ab als Teilwort enthalten.

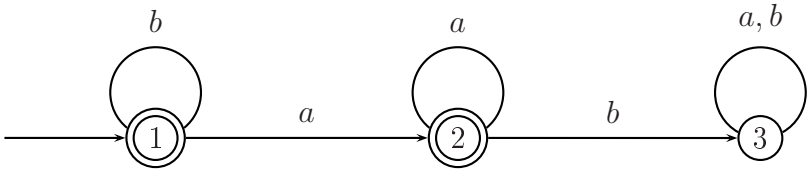
a) Geben Sie einen regulären Ausdruck R an, so dass $[R] = L$ gilt.

$$R = b^*a^*$$

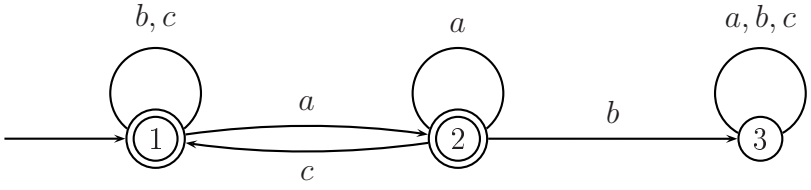
b) Geben Sie einen regulären Ausdruck R_c an, so dass $[R_c] = L_c$ gilt.

$$R_c = (b \cup c \cup a^*c)^*a^*$$

c) Geben Sie einen endlichen Automaten A an, für den $L(A) = L$ gilt.



d) Geben Sie einen endlichen Automaten A_c an, für den $L(A_c) = L_c$ gilt.



Aufgabe 4 (2+3+1+2 Punkte): Die formalen Sprachen L und L' seien definiert durch $L = \{a^n b a^m \mid n \leq m \leq 2n\}$ und $L' = \{a^n b a^m \mid n < m < 2n\}$.

a) Geben Sie eine kontextfreie Grammatik $G = (N, T, S, P)$ an, die L erzeugt.

$$G = (\{S\}, \{a, b\}, S, \{S \to aSa \mid aSaa \mid b\})$$

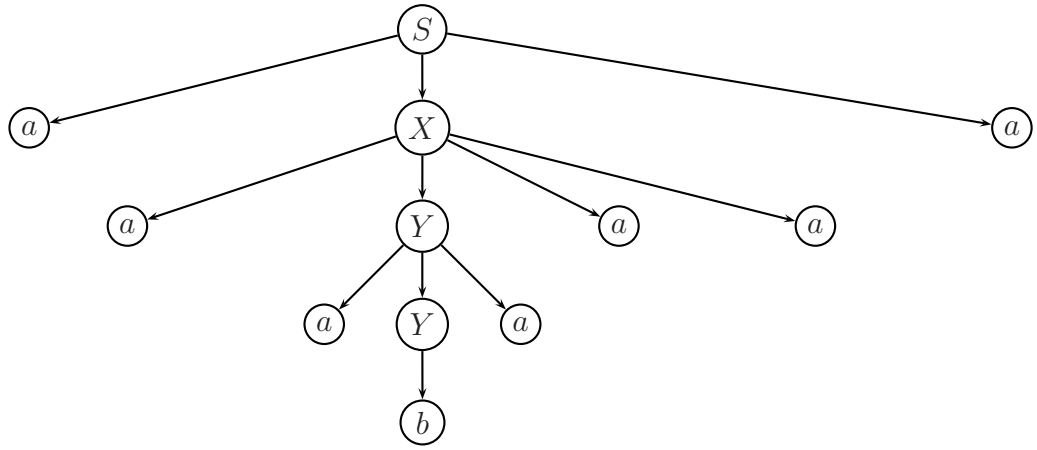
b) Geben Sie eine kontextfreie Grammatik $G' = (N', T, S', P')$ an, die L' erzeugt.

$$G = (\{S, X, Y\}, \{a, b\}, S, \{S \to aXa, X \to aYaa, Y \to aYa \mid aYaa \mid b\})$$

c) Geben Sie für Ihre Grammatik G eine Ableitung für das Wort *aaabaaaa* an.

$$S \Rightarrow aSa \Rightarrow aaSaaa \Rightarrow aaaSaaaa \Rightarrow aaabaaaa$$

d) Geben Sie für Ihre Grammatik G' einen Ableitungs**baum** für das Wort *aaabaaaa* an.



Aufgabe 5 (3+1+2+2 Punkte): Gegeben ist das Registermaschinenprogramm P:

$$a_3(s_3(s_1a_2a_3)_1a_3(s_2s_2s_3s_3a_1)_2a_4)_3$$
$$s_4(s_1a_3a_3)_1s_3$$

Die Eingabe n erfolgt in Register 1, alle anderen Register enthalten anfangs den Wert 0.

a) Die Funktionen, die in den Registern R_3 und R_4 bei Eingabe von n berechnet werden, werden mit $f_3(n)$ und $f_4(n)$ bezeichnet.

Geben Sie für die Eingaben $n \in \{7, 14, 8\}$ die Werte von $f_3(n)$ und $f_4(n)$ an.

$$f_3(7) = 7, f_3(14) = 7, f_3(8) = 1$$
$$f_4(7) = 0, f_4(14) = 1, f_4(8) = 3$$

b) Für welche Eingaben $n \in \mathbb{N}_+$ ist $f_3(n)$ gerade?

Für keine $n \in \mathbb{N}_+$ ist dies der Fall; $f_3(n)$ ist immer ungerade.

c) Für ein $n \in \mathbb{N}_+$ sei $f_3(n) = k$ und $f_4(n) = l$. Geben Sie eine Formel für n in Abhängigkeit von k und l an.

$$n = k \cdot 2^l$$

d) Geben Sie die Menge aller Zahlen an, für welche die Schleife $(s_3(s_1a_2a_3)_1a_3(s_2s_2s_3s_3a_1)_2a_4)_3$ im Programm P genau einmal durchlaufen wird.

Die gesuchte Menge ist die Menge aller ungeraden Zahlen, oder $\{2n + 1 \mid n \in \mathbb{N}_0\}$

Aufgabe 6 (3+6 Punkte): Für das RSA-Verfahren werde der öffentliche Schlüssel $(n, e) = (185, 7)$ verwendet; jeder Buchstabe werde durch seine Position im Alphabet codiert. (Also A durch 1, B durch 2, ...)

a) **Berechnen** Sie den zugehörigen privaten Schlüssel (n, d) **mit dem Erweiterten Euklidschen Algorithmus**.

Es gilt $185 = 5 \cdot 37 \Rightarrow \Phi(185) = 4 \cdot 36 = 144$.

Mit dem Erweiterten Euklidschen Algorithmus wird nun das multiplikative Inverse von 7 modulo 144 berechnet:

n	m	s	t	u	v	q	r
144	7	1	0	0	1	51	3
7	4	0	1	1	-20	1	3
4	3	1	-20	-1	21	1	1
3	1	-1	21	2	-41	3	0
1	0	2	-41	-7	144		

Wir suchen nun die kleinste positive Zahl d, die modulo 144 kongruent zu -41 ist, und erhalten den privaten Schlüssel $(185, 103)$.

b) Verschlüsseln Sie das Wort ECKE mit dem Schlüssel (n, e). Berechnen Sie alle weiteren verwendeten Werte, und geben Sie **alle** Zwischenergebnisse an.

Das Wort ECKE wird codiert durch 05031105.

Da $10^2 < n < 10^3$ gilt, wird das Wort 1100021001 in Zweierblöcke unterteilt.

Es gilt:

$$5^7 \mod 185 = 5^4 \cdot 5^3 \mod 185 = 625 \cdot 5^3 \mod 185 = 70 \cdot 5 \cdot 5^2 \mod 185$$
$$= 350 \cdot 5^2 \mod 185 = 165 \cdot 5 \cdot 5 \mod 185 = 825 \cdot 5 \mod 185$$
$$= 85 \cdot 5 \mod 185 = 425 \mod 185 = 55$$

$$3^7 \mod 185 = 3^5 \cdot 3^2 \mod 185 = 243 \cdot 3^2 \mod 185 = 58 \cdot 9 \mod 185$$
$$= 522 \mod 185 = 152$$

$$11^7 \mod 185 = 1331 \cdot 1331 \cdot 11 \mod 185 = 36 \cdot 36 \cdot 11 \mod 185$$
$$= 1296 \cdot 11 \mod 185 = 1 \cdot 11 \mod 185 = 11$$

Wir bringen alle Ergebnisse auf die Länge 3 und erhalten das Wort

055152011055.