Universität Karlsruhe (TH)
Lehrstuhl Informatik für Ingenieure und Naturwissenschaftler
Dr. Thomas Worsch
Matthias Schulz
3. März 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
Maximal-punktzahl	13	11	9	10	7
erreichte Punktzahl					

Punktsumme:	Note:

Diese Klausur besteht aus einem Deckblatt und weiteren **9** Blättern mit insgesamt **5** 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.

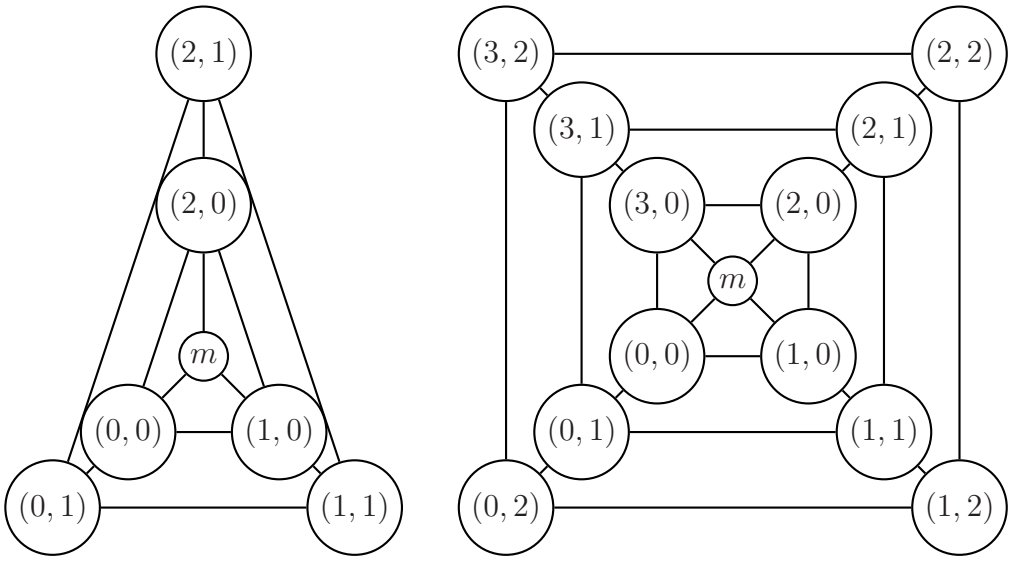
Wir wünschen Ihnen viel Erfolg!

Die Ergebnisse werden *voraussichtlich* in der 11. Kalenderwoche (9.3.2009 bis 13.3.2009) im WWW und per Aushang bekanntgegeben.

Aufgabe 1 (3+2+2+3+3 Punkte): Für $n \in \mathbb{N}^+$ sei $N_n = \{0, \ldots, n-1\}$.
Für $n \in \mathbb{N}, n \geq 3$ sei der (ungerichtete) n-te "Spinnengraph" $G_n = (V_n, E_n)$ gegeben durch:

$$\begin{aligned} V_n &= \{m\} \cup N_n \times N_{n-1}, \\ E_n &= \{\{m, (i,0)\} \mid i \in N_n\} \cup \{\{(i,j), (i, j+1)\} \mid i \in N_n, j \in N_{n-2}\} \\ &\quad \cup \{\{(i,j), ((i+1) \mod n, j)\} \mid i \in N_n, j \in N_{n-1}\} \end{aligned}$$

a) Stellen Sie die Graphen G_3 und G_4 graphisch dar.



b) Ist G_4 planar? Falls Ihre Antwort "ja" ist, geben Sie eine planare Darstellung von G_4 an. Falls Ihre Antwort "nein" ist, begründen Sie dies.

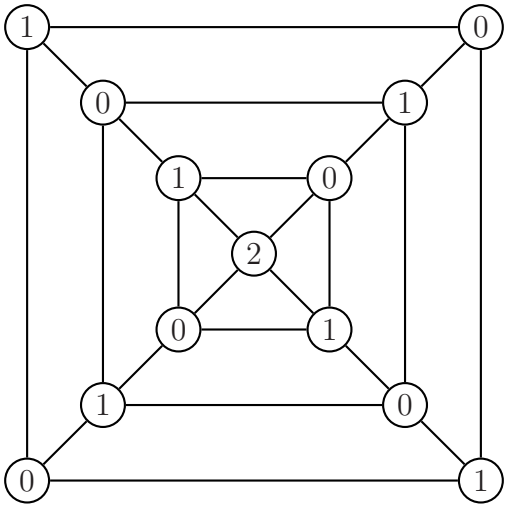
G_4 ist planar, siehe Abbildung.

c) Wie viele Knoten hat G_n in Abhängigkeit von n? Wie viele Kanten hat G_n in Abhängigkeit von n?

G_n besitzt $n(n-1)+1$ Knoten und $2n(n-1)$ Kanten.

d) Geben Sie eine 3-Färbung von G_4 an. (Sie können dazu die Darstellungen auf der vorherigen Seite benutzen.)

Gibt es eine Dreifärbung von G_3? Begründen Sie Ihre Antwort.



G_3 enthält eine Viererclique $\{m, (0,0), (1,0), (2,0)\}$, weswegen es keine Dreifärbung für G_3 geben kann.

e) Geben Sie jeweils für G_3 und G_4 einen Kreis an, der jeden Knoten aus G_3 beziehungsweise G_4 genau einmal enthält. Achten Sie auf eine **übersichtliche** Darstellung der Kreise.

Kreis für G_3 ist zum Beispiel $(m, (0,0), (0,1), (1,1), (2,1), (2,0), (1,0), m)$.

Kreis für G_4 ist zum Beispiel
$(m, (0,0), (0,1), (0,2), (1,2), (2,2), (3,2),$
$(3,1), (2,1), (1,1), (1,0), (2,0), (3,0), m)$.

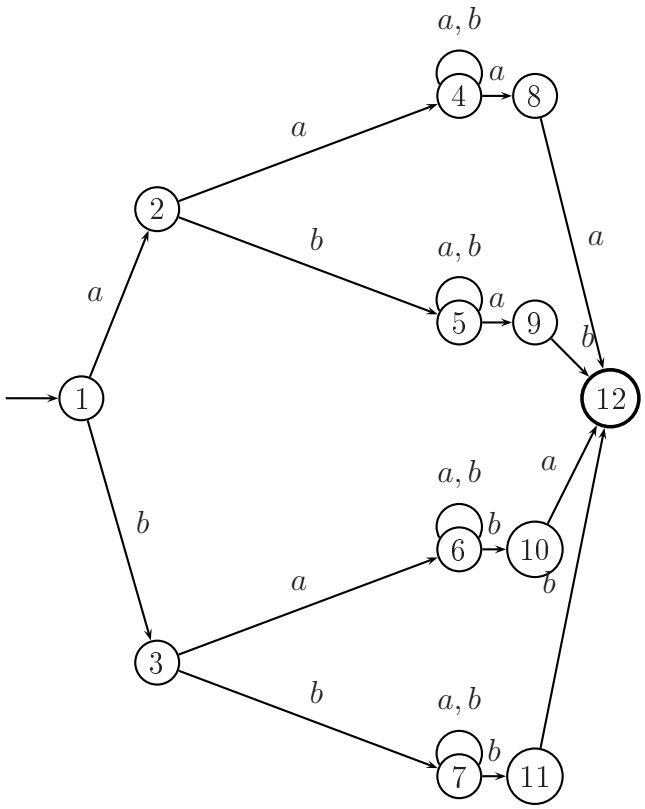
Aufgabe 2 (2+3+3+1+2 Punkte):

a) Die formale Sprache L sei als die Menge aller Wörter über dem Alphabet $\{a, b\}$ definiert, bei denen die ersten beiden Zeichen mit den letzten beiden Zeichen übereinstimmen und die mindestens die Länge 4 haben. Die Wörter *abab* und *abbab* sind also in L enthalten, die Wörter *abba* und *ab* jedoch **nicht**.

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

$R = aa(a \cup b)^*aa \cup ab(a \cup b)^*ab \cup ba(a \cup b)^*ba \cup bb(a \cup b)^*bb$

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



c) Sei L' die Sprache aller Wörter über $\{a, b\}$, die am Anfang genau so viele a stehen haben wie am Ende. (*aabbbaa* wäre so ein Wort, *aababba* nicht.)

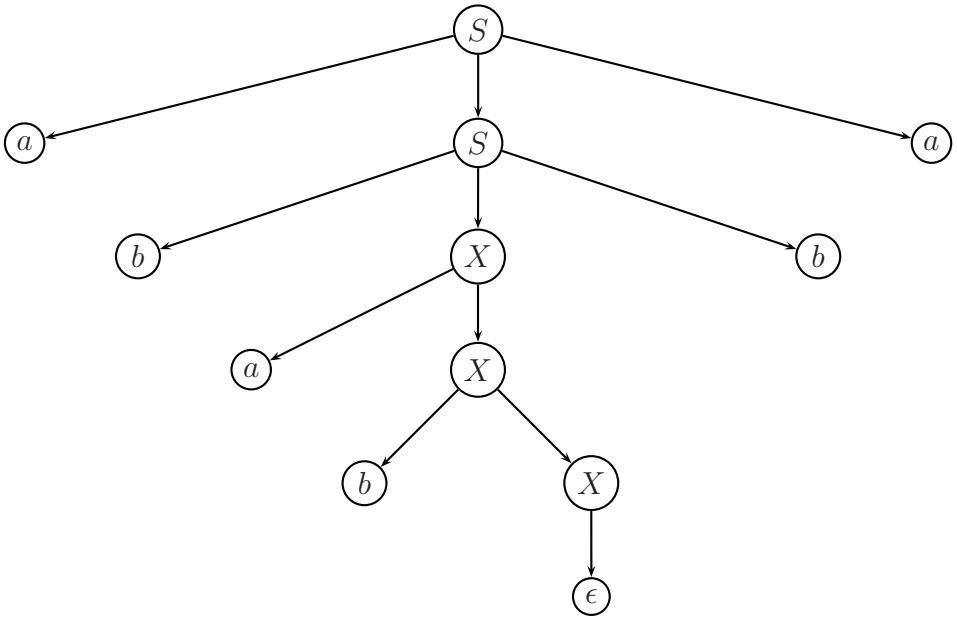
Geben Sie eine kontextfreie Grammatik $G = (N, T, S, P)$ an, die L' erzeugt.

$N = \{S, X\}, T = \{a, b\}, P = \{S \to aSa|bXb|a|b|\epsilon, X \Rightarrow aX|bX|\epsilon\}$

d) Finden Sie ein möglichst kurzes Wort $w \in L'$, das mit a beginnt und **kein** Palindrom ist.

$w = ababba$ *oder* $w = abbaba$.

e) Geben Sie für Ihre kontextfreie Grammatik aus Teil c) einen Ableitungsbaum für das Wort w aus d) an.



Aufgabe 3 (4+2+3 Punkte): Gegeben ist das Registermaschinenprogramm P_1:

$$(s_1 a_3 (s_3 a_4 s_2)_2 (s_3 a_2)_3)_1$$

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

a) Die Funktionen, die in den Registern R_2 und R_4 bei Eingabe von n berechnet werden, werden mit $f_2(n)$ und $f_4(n)$ bezeichnet.

Geben Sie für die Eingaben $n \in \{3, 5, 6, 7\}$ die Werte von $f_2(n)$ und $f_4(n)$ an.

n	$f_2(n)$	$f_4(n)$
3	1	1
5	1	2
6	0	3
7	1	3

b) Geben Sie allgemeine Formeln für die Funktionen $f_2(n)$ und $f_4(n)$ an.

$$f_2(n) = \begin{cases} 0 & \text{falls } n \text{ gerade} \\ 1 & \text{falls } n \text{ ungerade} \end{cases}$$

$$f_4(n) = \lfloor \tfrac{n}{2} \rfloor$$

c) Das Registermaschinenprogramm P_2 sei gegeben durch

$$\begin{aligned} P_2 &= ((s_2)_2 P_1 (s_4 a_1)_4)_1 \\ &= ((s_2)_2 (s_1 a_3 (s_3 a_4 s_2)_2 (s_3 a_2)_3)_1 (s_4 a_1)_4)_1 \end{aligned}$$

Geben Sie die Belegungen aller Register bei Eingabe von $n \in \mathbb{N}_0$ nach Ablauf des Programmes P_2 für beliebige Werte von n an.

Register 1, 3 und 4 enthalten jeweils eine 0. Register 2 enthält eine 1, falls $n > 0$ gilt, und ansonsten 0.

Aufgabe 4 (3+7 Punkte): Für das RSA-Verfahren werde der öffentliche Schlüssel $(n, e) = (407, 7)$ verwendet; jeder Buchstabe werde durch die Anzahl der Buchstaben, die im Alphabet vor ihm stehen, codiert. (Also A durch 0, B durch 1, ...)

a) **Berechnen** Sie den zugehörigen privaten Schlüssel (n, d).

(Hinweis: 407 ist durch 11 teilbar.)

Es gilt $407 = 11 \cdot 37 \Rightarrow \Phi(407) = 10 \cdot 36 = 360$.

Mit dem Erweiterten Euklidschen Algorithmus wird nun das multiplikative Inverse von 7 *modulo 360 berechnet:*

n	m	s	t	u	v	q	r
360	7	1	0	0	1	51	3
7	3	0	1	1	-51	2	1
3	1	1	-51	-2	103	3	0
1	0	-2	103	7	-360		

Damit ist der private Schlüssel $(407, 103)$.

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

Das Wort LACKE wird codiert durch 1100021004.

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

Es gilt:

$0^7 \mod 407 = 0$
$2^7 \mod 407 = 128$
$4^7 \mod 407 = 4^5 \cdot 4^2 \mod 407 = 1024 \cdot 16 \mod 407 = 210 \cdot 16 \mod 407 = 420 \cdot 8 \mod 407 = 13 \cdot 8 \mod 407 = 104$
$10^7 \mod 407 = 10000000 \mod 7;$
$10000000 : 407 = 24570$ Rest $10 \Rightarrow 10^7 \mod 407 = 10$
$11^7 \mod 407 = 1331 \cdot 1331 \cdot 11 \mod 407 = 110 \cdot 110 \cdot 11 \mod 407 = 133100 \mod 407 = 11000 \mod 407 = 2860 \mod 407 = 11$

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

011000128010104.

Aufgabe 5 (5+2 Punkte):

a) Zeigen Sie, dass folgendes Programm partiell korrekt ist, indem Sie Vor- und Nachbedingungen ergänzen.

Geben Sie bei Folgerungen alle Zwischenschritte an, eventuell auf Rückseite.

$\langle \underline{\mathtt{n}} = a \wedge a \geq 1 \rangle$
$\Downarrow$
$\langle \underline{\mathtt{n}} \leq a \wedge a < \underline{\mathtt{n}} + 1 \rangle$
$\Downarrow$
$\langle 2^0 \cdot \underline{\mathtt{n}} \leq a \wedge a < 2^0 \cdot (\underline{\mathtt{n}} + 1) \rangle$
$\mathtt{p} \leftarrow 0;$
$\langle 2^{\underline{\mathtt{p}}} \cdot \underline{\mathtt{n}} \leq a \wedge a < 2^{\underline{\mathtt{p}}} \cdot (\underline{\mathtt{n}} + 1) \rangle$
while $\mathtt{n} \neq 1$ **do**
$\quad \langle 2^{\underline{\mathtt{p}}} \cdot \underline{\mathtt{n}} \leq a \wedge a < 2^{\underline{\mathtt{p}}} \cdot (n + 1) \wedge n \neq 1 \rangle$
II $\Downarrow$
$\quad \langle 2^{\underline{\mathtt{p}}} \cdot \underline{\mathtt{n}} \leq a \wedge a < 2^{\underline{\mathtt{p}}} \cdot 2(\lfloor \frac{\mathtt{n}}{2} \rfloor + 1) \rangle$
I $\Downarrow$
$\quad \langle 2^{\underline{\mathtt{p}}} \cdot 2\lfloor \frac{\mathtt{n}}{2} \rfloor \leq a \wedge a < 2^{\underline{\mathtt{p}}} \cdot 2(\lfloor \frac{\mathtt{n}}{2} \rfloor + 1) \rangle$
$\Downarrow$
$\quad \langle 2^{\underline{\mathtt{p}}+1} \cdot \lfloor \frac{\mathtt{n}}{2} \rfloor \leq a \wedge a < 2^{\underline{\mathtt{p}}+1} \cdot (\lfloor \frac{\mathtt{n}}{2} \rfloor + 1) \rangle$
$\quad \mathtt{n} \leftarrow \lfloor \frac{n}{2} \rfloor;$
$\quad \langle 2^{\underline{\mathtt{p}}+1} \cdot \underline{\mathtt{n}} \leq a \wedge a < 2^{\underline{\mathtt{p}}+1} \cdot (\underline{\mathtt{n}} + 1) \rangle$
$\quad \mathtt{p} \leftarrow \mathtt{p} + 1;$
$\quad \langle 2^{\underline{\mathtt{p}}} \cdot \underline{\mathtt{n}} \leq a \wedge a < 2^{\underline{\mathtt{p}}} \cdot (\underline{\mathtt{n}} + 1) \rangle$
od
$\langle 2^{\underline{\mathtt{p}}} \cdot \underline{\mathtt{n}} \leq a \wedge a < 2^{\underline{\mathtt{p}}} \cdot (\underline{\mathtt{n}} + 1) \wedge n = 1 \rangle$
$\Downarrow$
$\langle 2^{\underline{\mathtt{p}}} \cdot 1 \leq a \wedge a < 2^{\underline{\mathtt{p}}} \cdot 2 \rangle$
$\Downarrow$
$\langle 2^{\underline{\mathtt{p}}} \leq a \wedge a < 2^{\underline{\mathtt{p}}+1} \rangle$

Verwenden Sie die Ungleichungen

I $\forall n \in \mathbb{N}_0 : 2\lfloor \frac{n}{2} \rfloor \leq n$

II $\forall n \in \mathbb{N}_0 : 2\lfloor \frac{n}{2} \rfloor + 2 \geq n + 1$

Markieren Sie Folgerungen, bei denen Sie eine dieser Ungleichungen verwenden, entsprechend.

b) Welche Zahl berechnet obiges Programm bei Eingabe von n in der Variablen p?

Das Programm berechnet $\lfloor log_2 n \rfloor$