Universität Karlsruhe (TH)
Lehrstuhl Informatik für Ingenieure und Naturwissenschaftler
Dr. Thomas Worsch
Matthias Schulz
2. September 2008

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	9	10	12	10	9
erreichte Punktzahl					

Punktsumme:	Note:

Diese Klausur besteht aus einem Deckblatt und weiteren **10** 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 bei Verwendung an. Sollten Sie Potenztabellen verwenden, verweisen Sie darauf und geben diese Sie diese mit der Klausur ab.

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.

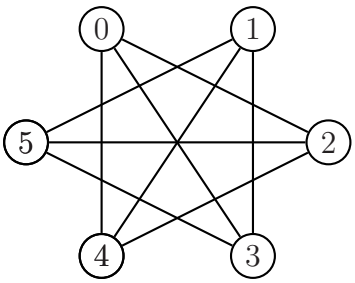
Wir wünschen Ihnen viel Erfolg!

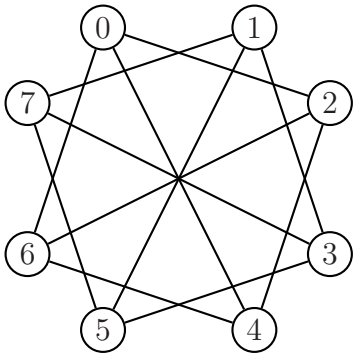
Die Ergebnisse werden *voraussichtlich* in der 43. Kalenderwoche (20.10.2008 bis 24.10.2008) im WWW und per Aushang bekanntgegeben.

Aufgabe 1 (2+3+2+2 Punkte): Für $p, q \in \mathbb{N}, p, q \geq 2$ sei der ungerichtete Graph $G_{p,q} = (V_{p,q}, E_{p,q})$ gegeben durch:

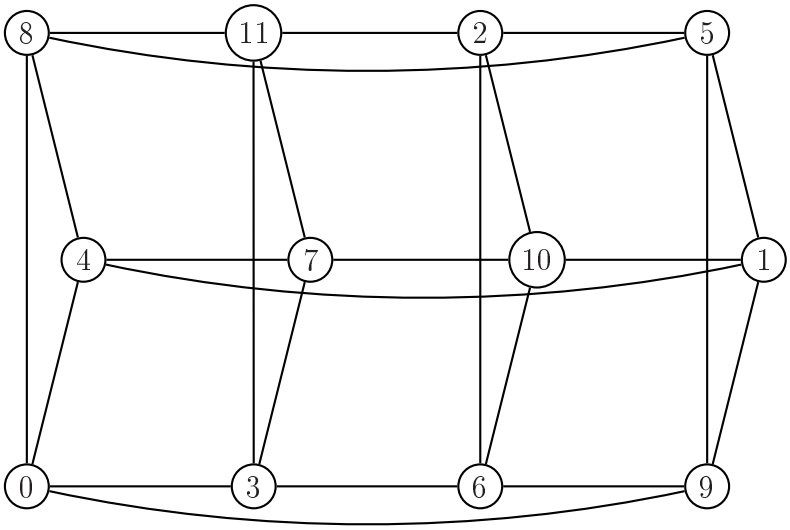
$$\begin{aligned} V_{p,q} &= \{0, 1, \ldots, p \cdot q - 1\}, \\ E_{p,q} &= \{\{u, v\} : u, v \in V_{p,q} \wedge |u - v| \in \{p, q, p \cdot q - p, p \cdot q - q\}\} \end{aligned}$$

a) Stellen Sie die Graphen $G_{2,3}$ und $G_{2,4}$ graphisch dar.





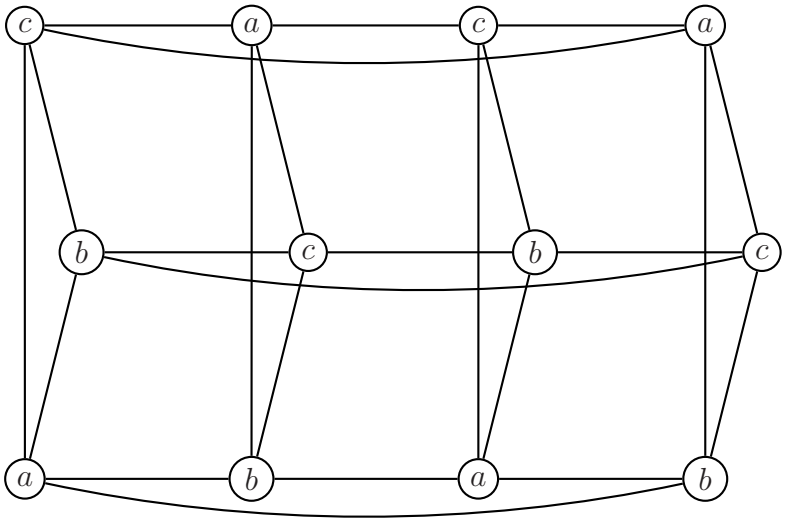
b) Die folgende Abbildung ist eine Darstellung des Graphen $G_{3,4}$, in der nur ein Knoten beschriftet ist. Beschriften Sie die übrigen Knoten des Graphen.



c) Sei $p \geq 3$. Zeigen Sie, dass es für jedes $q \geq 2$ einen u-Kreis der Länge p in $G_{p,q}$ gibt.

Wir betrachten die p Knoten $i \cdot q, 0 \leq i \leq p-1$. Für $0 \leq i \leq p-2$ ist jeder Knoten $i \cdot q$ über eine Kante mit dem Knoten $(i+1) \cdot q$ verbunden, da die Differenz gerade q beträgt.
Außerdem ist der Knoten $0 = 0 \cdot q$ mit dem Knoten $(p-1) \cdot q = pq - q$ über eine Kante verbunden.
Somit ergibt sich ein u-Kreis der Länge p mit den Knoten $0, q, \ldots, (p-1) \cdot q$.

d) Geben Sie eine 3-Färbung von $G_{3,4}$ an. (Sie können dazu die Abbildung auf der vorherigen Seite nutzen.)



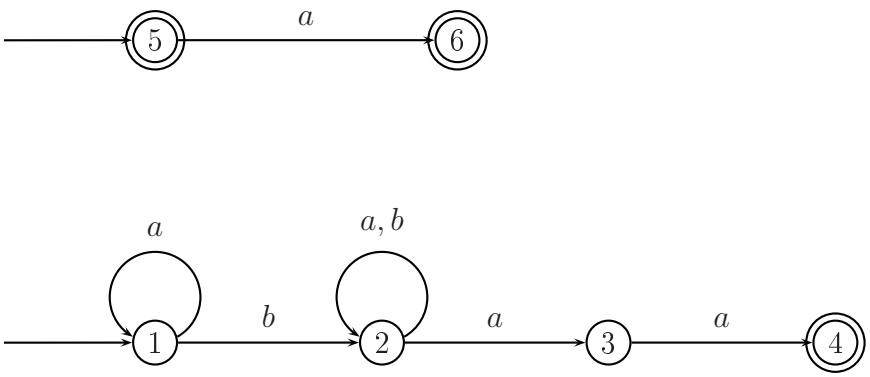
Aufgabe 2 (2+3+3+2 Punkte):

a) Die formale Sprache L_1 sei als die Menge aller Wörter über dem Alphabet $\{a, b\}$ definiert, die entweder das Zeichen b enthalten und mit aa enden, oder das Zeichen b nicht enthalten und nicht mit aa enden.

Geben Sie einen regulären Ausdruck R an, so dass $[R] = L_1$ gilt.

$L_1 = [a^*b(a \cup b)^*aa \cup a \cup \epsilon]$ oder
$L_1 = [(a \cup b)^*b(a \cup b)^*aa \cup a \cup$
$emptyset^*]$

b) Geben Sie einen endlichen Automaten A an, für den $L(A) = L_1$ gilt.

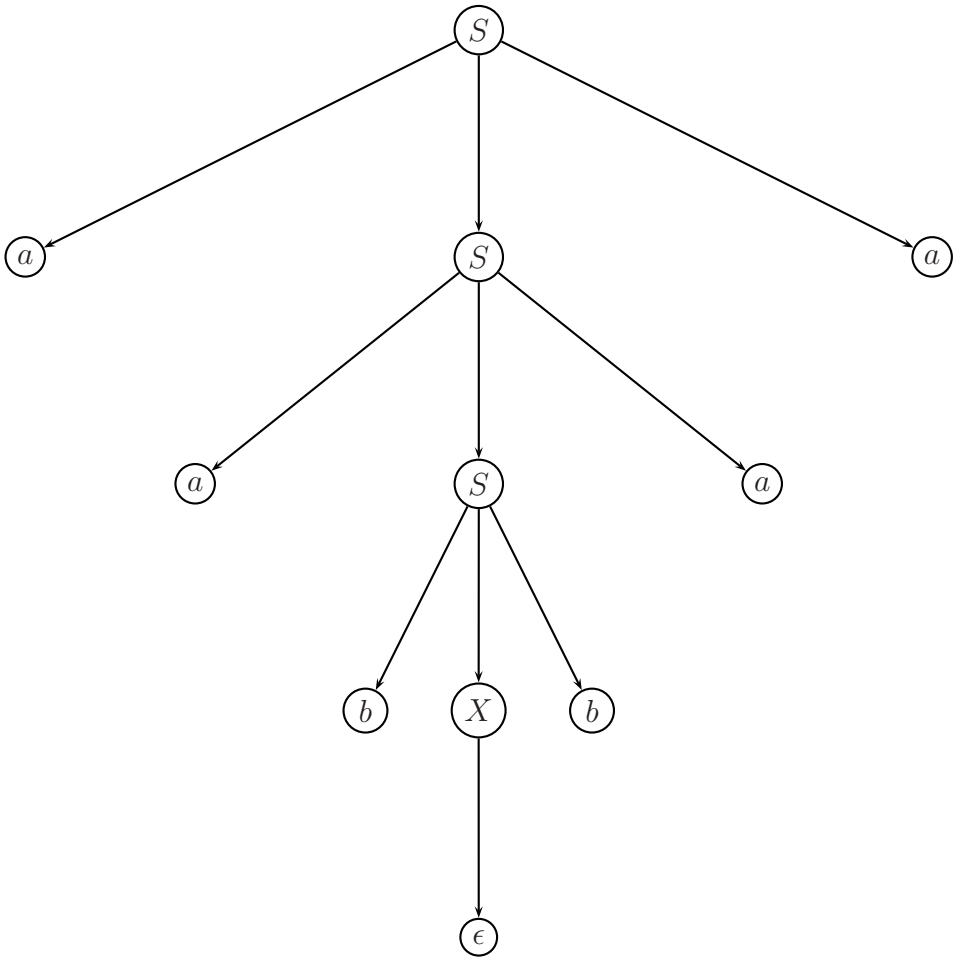


c) Sei L_2 die Sprache aller Palindrome über $\{a, b\}$ die nicht von der Form $a^nba^n, n \geq 0$ sind. (Das heißt, ein Wort w liegt genau dann in L_2, wenn w rückwärts gelesen wieder w ergibt und $w \notin [a^*ba^*]$ gilt.)

Geben Sie eine kontextfreie Grammatik $G = (N, T, S, P)$ an, die L_2 erzeugt.

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

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



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

$$(s_1 a_3 a_4)_1 (s_2 a_1 s_3)_2 (s_4 s_1 a_2)_4 (s_3 a_1 s_2)_3$$

Die Eingabe (x, y) erfolgt in den Registern 1 und 2, alle anderen Register enthalten anfangs den Wert 0.

a) Die Funktionen, die in den Registern R_1 und R_2 bei Eingabe von (x, y) berechnet werden, werden mit $f_1(x, y)$ und $f_2(x, y)$ bezeichnet.

Geben Sie für die Eingaben $(x, y) \in \{(3, 5), (5, 3), (4, 4)\}$ die Werte von $f_1(x, y)$ und $f_2(x, y)$ an.

$f_1(5, 3) = f_1(3, 5) = 2, f_2(5, 3) = f_2(3, 5) = 3,$
$f_1(4, 4) = 0, f_2(4, 4) = 4$

b) Geben Sie allgemeine Formeln für die Funktionen $f_1(x, y)$ und $f_2(x, y)$ an.

$f_1(x, y) = |x - y|, f_2(x, y) = \min\{x, y\}$

c) Zeigen Sie: Falls $x \neq 0$ und $y \neq 0$ gilt, folgt $f_1(x, y) + f_2(x, y) < x + y$.

Es gilt: $|x - y| = \max\{x, y\} - \min\{x, y\} < \max\{x, y\}$ falls $\min\{x, y\} > 0$, wie in der Aufgabenstellung gefordert.
Somit folgt: $f_1(x, y) + f_2(x, y) = |x - y| + \min\{x, y\} < \max\{x, y\} + \min\{x, y\} = x + y$.

d) Das Registermaschinenprogramm P_2 sei gegeben durch

$$(P_1)_2 = ((s_1 a_3 a_4)_1 (s_2 a_1 s_3)_2 (s_4 s_1 a_2)_4 (s_3 a_1 s_2)_3)_2$$

Hält P_2 für jede Eingabe (x, y)? Begründen Sie Ihre Antwort. (Hinweis: Verwenden Sie das Ergebnis aus Teilaufgabe c.)

Jede der inneren Schleifen terminiert, da die jeweiligen Schleifenvariablen in jedem Durchlauf verringert werden.
Da die Summe der Inhalte der Register 1 und 2 in jedem Schleifendurchlauf der äußeren Schleife wegen Teilaufgabe c um mindestens 1 kleiner wird, solange keines der beiden Register eine 0 enthält, enthält nach spätestens $x + y$ Durchläufen eines der beiden Register eine 0.
Falls Register 2 eine 0 enthält, endet das Programm nach diesem Durchlauf.
Falls Register 1 eine 0 enthält, steht nach dem nächsten Schleifendurchlauf eine 0 in Register 2, da in Register 2 immer das Minimum der Registerinhalte von Register 1 und Register 2 berechnet wird. Auch in diesem Fall hält das Programm.
Somit hält das Programm für jede Eingabe (x, y).

e) Welche Funktion $f(x, y)$ berechnet P_2 in Register 1? (Hinweis: Die Werte von $f(x, y)$ für $(x, y) \in \{(3, 5), (8, 12), (9, 12)\}$ könnten Ihnen einen Hinweis geben.)

$f(x, y) = ggT(x, y)$.

Aufgabe 4 (3+7 Punkte): Für das RSA-Verfahren werde der öffentliche Schlüssel $(n, d) = (111, 17)$ 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, e).

Da $n = 3{\cdot}37$ gilt, folgt $\phi(n) = 2{\cdot}36 = 72$. Der Parameter e ist das multiplikative Inverse zu d modulo $\phi(n)$.
Mit dem erweiterten euklidschen Algorithmus ergibt sich:

n_1	n_2	s_1	s_2	t_1	t_2	q
72	17	1	0	0	1	4
17	4	0	1	1	-4	4
4	1	1	-4	-4	17	4
1	0	-4	17	17	-72	

Somit ergibt sich $(n, e) = (111, 17)$.

b) Verschlüsseln Sie das Wort SCHAL mit dem Schlüssel $(111, 17)$. Berechnen Sie alle weiteren verwendeten Werte, und geben Sie **alle** Zwischenergebnisse an.

Geben Sie eventuell verwendete Multiplikationstabellen mit ab.

(Hinweis: Für alle Zahlen c gilt $c^{17} = (((c^2)^2)^2)^2 \cdot c$.)

Die Codierung des Wortes SCHAL ergibt 1802070011.
Da $10^2 < n < 10^3$, muss die Ziffernfolge in Blöcke der Länge $3-1 = 2$ unterteilt werden.
$18^2 = 324 = 102 \mod 111; 102^2 = 10404 = 414 \mod 111 = 81 \mod 111;$
$81^2 = 6400 + 160 + 1 = 6561 = 1011 \mod 111 = 12 \mod 111; 12^2 = 144 = 33 \mod 111;$
$33 \cdot 18 = 660 - 66 = 594 = \mathbf{39} \mod 111.$
$2^2 = 4; 4^2 = 16; 16^2 = 256 = 34 \mod 111;$
$34^2 = 900 + 240 + 16 = 1156 = 46 \mod 111; 46 \cdot 2 = \mathbf{92}.$
$7^2 = 49; 49^2 = 2500 - 100 + 1 = 2401 = 181 \mod 111 = 70 \mod 111;$
$70^2 = 4900 = 460 \mod 111 = 16 \mod 111; 16^2 = 256 = 34 \mod 111;$
$34 \cdot 7 = 210 + 28 = 238 = \mathbf{16} \mod 111.$
$0^17 = \mathbf{0}.$
$11^2 = 121 = 10 \mod 111; 10^2 = 100; 100^2 = 10000 = 10 \mod 111; 10^2 = 100; 100 \cdot 11 = 1100 = \mathbf{101} \mod 111.$
Auffüllen mit Nullen, um gleiche Blocklänge zu erhalten, liefert als Chiffre:
039092016000101

Aufgabe 5 (7+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.

Hinweis: Für jede Aussage A ist die Aussage $\forall z \in \mathbb{N} : 0 < z < 1 \Rightarrow A$ wahr.

$\langle \underline{\mathtt{m}} = n \wedge n > 1 \rangle$
$\Downarrow$
$\langle \underline{\mathtt{m}} \geq n \rangle$
$\Downarrow$
$\langle \underline{\mathtt{m}} \geq n \wedge \forall z \in \mathbb{N} : (0 < z < 1 \Rightarrow ggT(z, \underline{\mathtt{m}}) = 1) \rangle$
$\mathtt{a} \leftarrow 1$
$\langle \underline{\mathtt{m}} \geq n \wedge \forall z \in \mathbb{N} : (0 < z < \underline{\mathtt{a}} \Rightarrow ggT(z, \underline{\mathtt{m}}) = 1) \rangle$
while $\mathtt{a} \neq \mathtt{m}$ **do**
$\langle \underline{\mathtt{m}} \geq n \wedge \forall z \in \mathbb{N} : (0 < z < \underline{\mathtt{a}} \Rightarrow ggT(z, \underline{\mathtt{m}}) = 1) \wedge \underline{\mathtt{a}} \neq \underline{\mathtt{m}} \rangle$
if $ggT(\mathtt{a}, \mathtt{m}) \neq 1$ **then**
$\langle \underline{\mathtt{m}} \geq n \wedge \forall z \in \mathbb{N} : (0 < z < \underline{\mathtt{a}} \Rightarrow ggT(z, \underline{\mathtt{m}}) = 1) \wedge \underline{\mathtt{a}} \neq \underline{\mathtt{m}} \wedge ggt(\underline{\mathtt{a}}, \underline{\mathtt{m}}) \neq 1 \rangle$
$\Downarrow$
$\langle \underline{\mathtt{m}} + 1 \geq n \rangle$
$\Downarrow$
$\langle \underline{\mathtt{m}} + 1 \geq n \wedge \forall z \in \mathbb{N} : (0 < z < 1 \Rightarrow ggT(z, \underline{\mathtt{m}} + 1) = 1) \rangle$
$\mathtt{a} \leftarrow 1;$
$\langle \underline{\mathtt{m}} + 1 \geq n \wedge \forall z \in \mathbb{N} : (0 < z < \underline{\mathtt{a}} \Rightarrow ggT(z, \underline{\mathtt{m}} + 1) = 1) \rangle$
$\mathtt{m} \leftarrow \mathtt{m} + 1;$
$\langle \underline{\mathtt{m}} \geq n \wedge \forall z \in \mathbb{N} : (0 < z < \underline{\mathtt{a}} \Rightarrow ggT(z, \underline{\mathtt{m}}) = 1) \rangle$
else
$\langle \underline{\mathtt{m}} \geq n \wedge \forall z \in \mathbb{N} : (0 < z < \underline{\mathtt{a}} \Rightarrow ggT(z, \underline{\mathtt{m}}) = 1) \wedge \underline{\mathtt{a}} \neq \underline{\mathtt{m}} \wedge ggt(\underline{\mathtt{a}}, \underline{\mathtt{m}}) = 1 \rangle$
$\Downarrow$
$\langle \underline{\mathtt{m}} \geq n \wedge \forall z \in \mathbb{N} : (0 < z < \underline{\mathtt{a}} \Rightarrow ggT(z, \underline{\mathtt{m}}) = 1) \wedge ggt(\underline{\mathtt{a}}, \underline{\mathtt{m}}) = 1 \rangle$
$\Downarrow$
$\langle \underline{\mathtt{m}} \geq n \wedge \forall z \in \mathbb{N} : (0 < z < \underline{\mathtt{a}} + 1 \Rightarrow ggT(z, \underline{\mathtt{m}}) = 1) \rangle$
$\mathtt{a} \leftarrow \mathtt{a} + 1;$
$\langle \underline{\mathtt{m}} \geq n \wedge \forall z \in \mathbb{N} : (0 < z < \underline{\mathtt{a}} \Rightarrow ggT(z, \underline{\mathtt{m}}) = 1) \rangle$
fi
$\langle \underline{\mathtt{m}} \geq n \wedge \forall z \in \mathbb{N} : (0 < z < \underline{\mathtt{a}} \Rightarrow ggT(z, \underline{\mathtt{m}}) = 1) \rangle$
od
$\langle \underline{\mathtt{m}} \geq n \wedge \forall z \in \mathbb{N} : (0 < z < \underline{\mathtt{a}} \Rightarrow ggT(z, \underline{\mathtt{m}}) = 1) \wedge (\underline{\mathtt{a}} = \underline{\mathtt{m}}) \rangle$
$\Downarrow$
$\langle \underline{\mathtt{m}} \geq n \wedge \forall z \in \mathbb{N} : (0 < z < \underline{\mathtt{m}} \Rightarrow ggT(z, \underline{\mathtt{m}}) = 1) \rangle$

b) Welche Zahl berechnet obiges Programm bei Eingabe von n?

Das Programm berechnet die kleinste Primzahl, die größer oder gleich n ist.