Exam 2, Module 7, Code 201600270

Discrete Structures & Efficient Algorithms

Friday April 7, 2017, 13:45 - 16:45

All answers need to be motivated. No calculators. You are allowed to use a handwritten cheat sheet (A4) per topic (L&M,ALG,DM). Also if you cannot solve a part of a question you may use that result in subsequent parts of the question.

This exam consists of three parts, with the following (estimated) times:

Languages & Machines (L&M)	1h	(30 points)
Algebra (ALG)	1h 40 min	(50 points)
Discrete Mathematics (DM)	20 min	(10 points)

Total of 30+50+10=90 points. Including 10 bonus points that makes 100 points. Your exam grade is the total number pf points divided by 10.

Please use a new sheet of paper for each part (L&M/ALG/DW)!

Languages & Machines

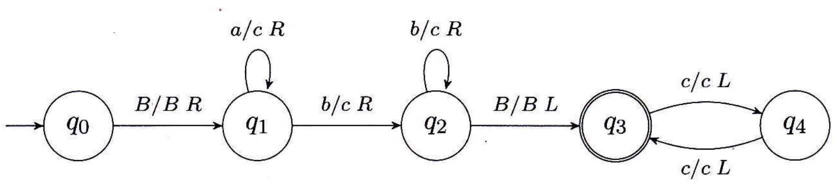
1. (a) (6 points) Transform the following contextfree grammar G step by step to an equivalent grammar G' in Chomsky Normal Form.

$$G = \left\{ \begin{array}{lcl} S & \to & a\,A \\ A & \to & \lambda \mid B \mid a\,A \\ B & \to & c \mid B\,c \end{array} \right.$$

   (b) (6 points) Let $w = aacc$. Apply the CYK-algorithm (after Cocke-Younger-Kasami) to decide whether $w \in \mathcal{L}(G')$. Provide a derivation tree for w as well.

2. (6 points) Consider the contextfree language $L = \{a^{2i}\, b^i\, c \mid i \geq 0\}$. Give a *deterministic* PDA (stack automaton) for L. Provide a *short* explanation.

3. (6 points) Which language is *decided* by the following Turing Machine? (only q_3 is accepting)? Explain your answer *shortly*.



4. (6 points, every wrong answer costs 2 points) Indicate for each of the following statements if they are TRUE or FALSE. (No explanation required).

   (a) Every contextfree grammar (CFG) has a Turing Machine (TM) accepting the same language.

   (b) Every contextfree grammar (CFG) has an equivalent extended PDA with two states.

(c) The class of contextfree languages is closed under complement.

(d) The class of contextfree languages is closed under union.

(e) To every PDA there exists a equivalent deterministic PDA.

(f) To every TM there exists an equivalent deterministic TM.

(g) The language of (encoded) terminating Turing Machines is not recursief, but it is recursive enumerable.

(h) Given a grammar G in Chomsky Normal Formal Form and a word w, one can decide in polynomial time whether $w \in \mathcal{L}(G)$.

Algebra

5. Let G be the set of matrices given by:

$$G = \{\begin{bmatrix} \alpha & \beta \\ 2\beta & \alpha \end{bmatrix} \mid \alpha, \beta \in \mathbb{Z}_3 \ \ (\alpha, \beta) \neq (0,0)\}.$$

On G we consider the operation matrix multiplication.

(a) Show that G with matrix multiplication forms a group.

(b) Let $\mathbb{F} = \mathbb{Z}_3[x]/ < x^2 + 1 >$. Show that $\phi : G \to \mathbb{F}\backslash\{0\}$ defined by

$$\phi\left(\begin{bmatrix} \alpha & \beta \\ 2\beta & \alpha \end{bmatrix}\right) = \alpha + \beta x + < x^2 + 1 >$$

is a group isomorphism from G to the multiplicative group of the field $\mathbb{F}$.

6. Given the permutations:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{bmatrix} \quad \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}$$

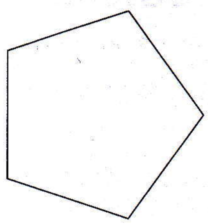
Write α, β and $\beta\alpha$ as:

(a) Product of disjoint cycles.

(b) Product of 2-cycles.

(c) Determine the order of α.

7. Use Burnside's theorem to determine the number of different ways in which the edges of a regular pentagon (see figure), made of copper wire, can be colored using two colors.



8. (a) Let $a(x) = x^2 + a_1x + a_0 \in \mathbb{Z}_2[x]$. Determine all values of $a_0, a_1 \in \mathbb{Z}_2$ for which $a(x)$ is irreducible.

   Let $p(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$.

   (b) Prove that $p(x)$ is irreducible.

   Let $\mathbb{F} = \mathbb{Z}_2[x]/{<}p(x){>}$.

   (c) Is $\mathbb{F}$ a field?

   (d) What is the number of elements of $\mathbb{F}$?

Points: **Ex 5**, a: 6, b: 6, **Ex 6**: a: 5, b: 5, c: 4, **Ex 7**: 10, **Ex 8**: a: 3, b: 4, c: 3, d: 4.

Discrete Mathematics

9. (7 points) Consider the RSA method, and assume that Alice has published the modulus $n = 65$ and the exponent $e = 11$. Bob emails the cipher text $C = 2$ to Alice. Compute everything that Alice needs to compute Bob's original message M, and also compute M.

10. (3 points) Show that $15^{17} = 15 \pmod{17}$ (without much calculation).