

Exam 2, Module 7, Code 201700304
Discrete Structures & Efficient Algorithms
Friday April 6, 2018, 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 of points divided by 10.

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

Languages & Machines

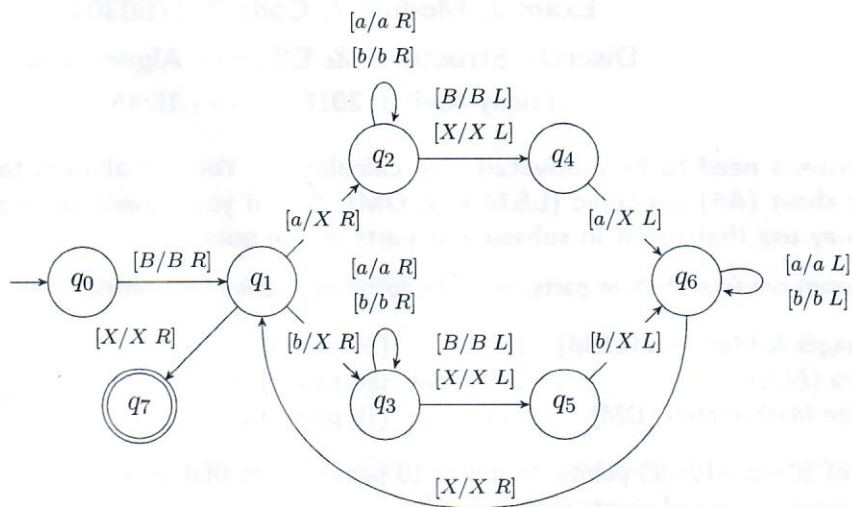
1. (5 points) Which variables can be derived by chain rules from C in the following grammar G_1 ? Provide an equivalent grammar without chain rules.

$$G_1 = \begin{cases} S \rightarrow AB \mid C \\ A \rightarrow aA \mid B \\ B \rightarrow bB \mid C \\ C \rightarrow cC \mid a \mid A \end{cases}$$

2. (5 points) Provide a *regular* grammar, equivalent to the following context-free grammar G_2 :

$$G_2 = \begin{cases} S \rightarrow BS \mid AB \\ A \rightarrow Aaa \mid \lambda \\ B \rightarrow b \end{cases}$$

3. (5 points) Consider the context-free language $L = \{a^i b^{i+j} c^j \mid i, j > 0\}$. Give a DPDA (*deterministic pushdown automaton*) for L . Provide a *short* explanation.
4. (5 points) Let G be a context-free grammar in Greibach Normal Form. Let P be a deterministic pushdown automaton, and let E be a regular expression. Is the language $\mathcal{L}(G) \cup (\mathcal{L}(P) \cap \mathcal{L}(E))$ context-free? (prove)
5. (5 points) Is the class of recursive languages closed under complement? (prove)
6. (5 points) Consider the following Turing Machine with a single tape. Which language is *decided* by this TM? (explain shortly)



Algebra

5. Are $U(14)$ and $U(18)$ isomorphic?

6. (a) Let $\sigma \in S_8$ be given by

$$\sigma = (1586)(23)$$

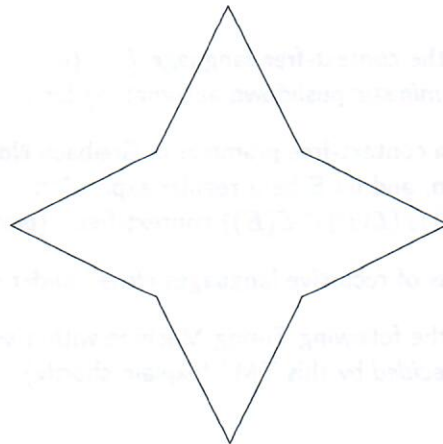
Determine whether σ is even or odd.

(b) Let $\tau \in S_5$ be given by

$$\tau = (12)(134)(152)$$

What is the order of τ ?

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



8. (a) Show that $a(x) = x^2 + x + 1$ is the only irreducible polynomial of degree two in $\mathbb{Z}_2[x]$.
(b) Expand $(a(x))^2$ in $\mathbb{Z}_2[x]$.
(c) Show that $p(x) = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$ is irreducible.
(d) Define

$$\mathbb{F} = \mathbb{Z}_2[x] / \langle x^4 + x^3 + 1 \rangle .$$

Argue that \mathbb{F} is a field.

- (e) How many elements does \mathbb{F} have?
(f) Determine the multiplicative order of $x + \langle x^4 + x^3 + 1 \rangle \in \mathbb{F}$.

Points: Ex 5: 10; Ex 6: a: 4, b: 6; Ex 7: 12, Ex 8: a: 3, b: 2, c: 4, d: 2, e: 3, f: 4.

Discrete Mathematics

9. (7 points) Consider the RSA method, and assume that Alice has published the modulus $n = 91$ and the exponent $e = 35$. Bob emails the cipher text $C = 3$ to Alice. Compute everything that Alice needs to compute Bob's original message M , and also compute M .
10. (3 points) In the year 2002 the indian researcher Agrawal together with his BSc students Kayal and Saxena published a breakthrough paper in which they solve a long-standing open problem, namely a polynomial time algorithm that correctly solves the following decision problem: Given a number $n \in \mathbb{N}$, is n a prime or not? Does that put the RSA crypto system in danger? (Please give a *short* but conclusive answer; "yes" or "no" does not suffice.)