Re-Exam 2, Module 7, Code 201700304

Discrete Structures & Efficient Algorithms

Thursday, April 19, 2018, 08:45 - 11:45

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 an 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. Your exam grade is the total number of points plus 10, then divided by 10, rounded to one digit.

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

Languages & Machines

1. (*6 points*) Transform the following context-free grammar G step by step into an equivalent grammar G' in Chomsky Normal Form.

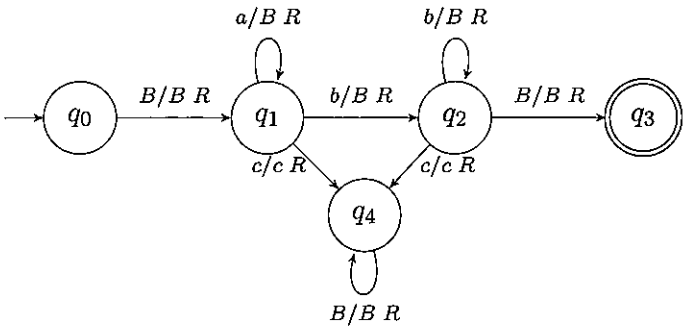
$$G = \begin{cases} S & \to & b\,X \mid a\,Y \\ X & \to & Y \mid b\,S \\ Y & \to & a\,Y \mid \lambda \end{cases}$$

2. (*6 points*) Consider the context-free language

$$L = \left\{ w\,w' \mid w \in \{a,b\}^*, w' \in \{b,c\}^*, \#_a(w) = \#_c(w') \right\} .$$

(where $\#_x(z)$ denotes the number of x-symbols in word z).
Provide a *deterministic* PDA (push-down automaton) for L.

3. (*6 points*) Which language is *accepted* by the following Turing Machine?
Does this Turing Machine also *decide* that language?



4. (*6 points*) Assume languages L_1 and L_2 are context-free and L_3 is regular.
   Which of the following statements hold necessarily? Explain your answers.

   (a) $(L_1 \cup L_3) \cap L_2$ is context-free

   (b) $(L_1 \cap L_3) \cup L_2$ is context-free

5. (*6 points*) Provide a context-free grammar in *Greibach Normal Form* that generates the following language:

$$\{a^i b^i c^+ \mid i \geq 0\}$$

   Shortly explain how you obtained your GNF.

Algebra

6. Let $G = U(9)$.

   (a) Determine the order of $2 \in G$.

   (b) Is G cyclic?

   (c) Construct an isomorphism from G to a subgroup of S_6, the permutation group of six symbols, by providing the image of each element of G in S_6. Write these images in disjoint cycle form.

   (d) Derive, without direct calculations, the orders of all elements of G by using the previous parts.

7. Let $R = \{a + b\alpha \mid a, b \in \mathbb{Z}_3\}$, here α is a symbol with the property: $\alpha^2 = 2$. On R we use the obvious addition and multiplication so that R becomes a ring.

   (a) Give the definition of zero divisor.

   (b) Investigate the existence of zero divisors in R. Hint: consider $(a + b\alpha)(c + d\alpha) = 0$ and multiply with $(a + 2b\alpha)(c + 2d\alpha)$.

   (c) Argue that R is a field and write $(1 + \alpha)^{-1}$ in the form $a + b\alpha$ with $a, b \in \mathbb{Z}_3$.

8. We want to paint the wheel depicted in Figure 1 using two colors. The wheel is constructed from iron wire and the spokes, the inner wheel and the outer wheel are considered separate parts. Use Burnside's theorem to determine the number of different ways in which the wheel may be painted.

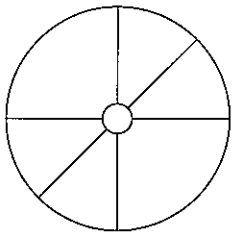


Figure 1: Wheel with spokes

9. (a) Provide the definition of irreducible polynomial in $\mathbb{F}[x]$.
   (b) Show that $f(x), g(x), h(x) \in \mathbb{Z}_3[x]$ with $f(x) = x^2 + x + 2$, $g(x) = x^2 + 1$ and $h(x) = x^2 + 2x + 2$ are the only irreducible monic polynomials, that is with leading coefficient equal to one, of degree two in $\mathbb{Z}_3[x]$.
   (c) In which ways can we write a polynomial of degree four as a product of nontrivial factors?
   (d) Show that $p(x) = x^4 + x^2 + x + 1 \in \mathbb{Z}_3[x]$ is irreducible.
   (e) Construct a field consisting of exactly 81 elements and give the general form of these elements.

Points: **Ex 6**: a: 3, b: 2, c: 4, d: 3. **Ex 7**: a: 2, b: 4, c: 4. **Ex 8**: 12. **Ex 9**: a: 2, b: 4, c: 2, d: 4, e: 4.

Discrete Mathematics

10. (6 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.

11. (4 points) Argue that for any prime $p > 2$, we have that

$$(p-1)! = p - 1 \pmod{p}.$$

(Hint: Recall that the equation $x^2 = 1$ has exactly two solutions in $\mathbb{Z}_p$, which are 1 and $p-1$.)