Kenmerk: EWI2018/TW/DMMP/MU/003

Test Exam 2, Module 7
Discrete Structures & Efficient Algorithms

All answers need to be motivated. No calculators. You are allowed to use a handwritten cheat sheet (A4, both sides) per topic (L&M, ALG, DM).

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

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

Total of 30+50+10=90 points. Your exam grade is the maximum of 1 and the total number of points divided by 9, rounded to one digit.

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

Languages & Machines

1. Transform the following contextfree grammar G step by step into Chomsky Normal Form. Clearly indicate the steps you take, including the intermediary results.

$$G = \begin{cases} S & \rightarrow & A\,B \mid B\,C\,S \\ A & \rightarrow & a\,A \mid C \\ B & \rightarrow & b\,B \mid \lambda \\ C & \rightarrow & c\,C \mid \lambda \end{cases}$$

2. Consider the contextfree language $L = \{a^i\, b^*\, c^j \mid j \geq i \geq 0\}$.
   Provide a *deterministic* PDA (pushdown automaton) for this language.

3. A 2-tape Turing Machine (TM) has two tapes. At the start, the input word is on tape 1 and tape 2 is empty. So, for word $aabcbaa$ the start configuration is

$$[q_0; *BaabcbaaB; *BBBBB]$$

   where B denotes the blank symbol, and $*$ denotes the position of the head on the tapes.

   (a) Provide a 2-tape Turing Machine (TM) that *recognizes* the language $\{w\,c\,w^R \mid w \in \{a, b\}^*\}$.

   (b) Explain shortly the working of your machine, inluding a computation from the start configuration for the word $aabcbaa$.

(c) Does your TM also *decide* this language? (explain)
(d) Is your TM deterministic? (explain)

Algebra

4. Let $V = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, the Klein four-group. As we know, every finite group is isomorphic to a subgroup of S_n, the permutation group of n symbols.

   (a) Why can V not be isomorphic to a subgroup of S_3?

   (b) Determine a subgroup H of S_4 such that V isomorphic to H.

5. Let $(G, \cdot)$ be a group. Define

$$\mathrm{Z}(G) = \{h \in G \mid \forall g \in G : \quad g \cdot h = h \cdot g\}.$$

   (a) Show that $Z(G)$ is a subgroup of G.

   (b) Now, let G be the group of matrices equiped with matrix multiplication

$$G = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \quad ad - bc \neq 0\}.$$

   Determine $\mathrm{Z}(G)$.

   (c) Show that $\mathrm{Z}(G)$ from Part 5b is isomorphic to $\mathbb{R}\backslash\{0\}$ with the usual multiplication.

6. Let $p(x) \in \mathbb{Z}_5[x]$ be given by: $p(x) = x^3 + 2x^2 + 1$ and $I =< p(x) >$ the ideal in $\mathbb{Z}_5[x]$ generated by $p(x)$.

   (a) Demonstrate that $p(x)$ is irreducible.

   (b) Argue that $\mathbb{F} = \mathbb{Z}_5[x]/I$ is a field.

   (c) Decribe the general form of the elements of $\mathbb{F} = \mathbb{Z}_5[x]/I$. How many different elements are there in $\mathbb{F}$?

   (d) Calculate the inverse of $2x + 3 + I$ in $\mathbb{F}$.

   (e) Show that $\mathbb{F}$ is isomorphic to $\mathbb{Z}_5[x]/< x^3 + 3x + 2 >$.

7. Use Burnside's theorem to calculate the number of different ways in which the edges of a square made of iron wire can be painted using five colors.

8. Write the permutation $\alpha \in S_5$ as product of disjoint cycles and a product of 2-cycle respectively.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{bmatrix}$$

Points: 1a: 3, b: 5; 2a: 5, b: 5, c: 5; 3a: 3, b: 4, c: 4, d: 6, e: 4; 4: 3; 5: 3.

Discrete Mathematics

9. (3 points) Compute 3^{20} (mod 5).

10. (7 points) The RSA method has been used with as modulus $n = 55$ and with exponent $e = 7$ to encode the secret message M to $C = M^e = 2$. Compute M.