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

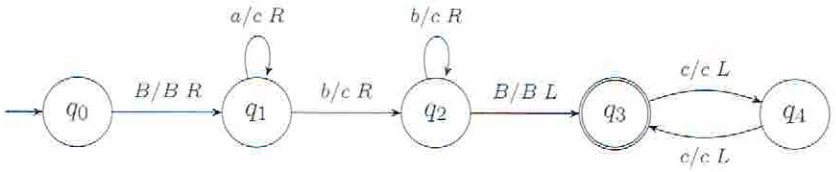
1. (a) (6 points) Transform the following contextfree grammar G step by step to an equivalent grammar G' in Chomsky Normal Form.

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

   (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:

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

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:

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

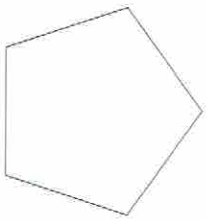
Write α, β and $\beta\alpha$ as:

(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 $a(x) = x^2 + a_1 x + a_0 \in \mathbb{Z}_2[x]$. 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).

Kenmerk: EWI2017/TW/DMMP/MU (see page 4 for the English version)

Tentamen 2, Module 7, Vakcode 201600270

Discrete Structuren & Efficiënte Algoritmes

Vrijdag 07 april 2017, 13:45 - 16:45

Alle antwoorden dienen te worden gemotiveerd. Gebruik van een rekenmachine is niet toegestaan. Gebruik van zelfgeschreven spiekbriefjes, één dubbelzijdig A4 per onderdeel (L&M,ALG,DW), is wel toegestaan. Indien u een onderdeel niet kunt oplossen dan kunt u het resultaat van dat onderdeel in latere onderdelen toch gebruiken.

Dit tentamen bestaat uit drie onderdelen, en is gebaseerd op de volgende, geschatte tijdsbesteding per onderdeel (slechts als indicatie):

Languages & Machines (L&M)	1h	(30 punten)
Algebra (ALG)	1h40min	(50 punten)
Discrete Mathematics (DW)	20 min	(10 punten)

Dus in totaal 30+50+10=90 punten. Incl. de 10 gratis punten zijn het 100 punten. Het tentamencijfer is het totaal aantal punten gedeeld door 10.

Gebruik aub per onderdeel (L&M/ALG/DW) een nieuw vel!

Languages & Machines

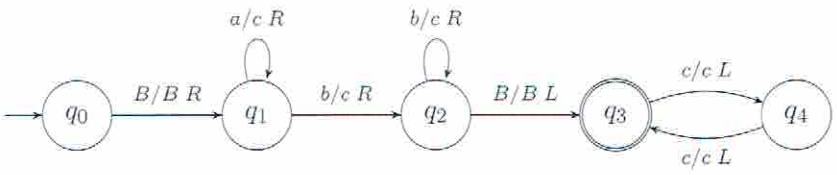
1. (a) (6 punten) Transformeer de volgende contextvrije grammatica G stapsgewijs tot een equivalente grammatica G' in Chomsky Normaalvorm.

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

   (b) (6 punten) Laat $w = aacc$. Pas het CYK-algoritme (genoemd naar Cocke-Younger-Kasami) toe om te beslissen of $w \in \mathcal{L}(G')$. Geef ook een afleidingsboom voor w weer.

2. (6 punten) Beschouw de contextvrije taal $L = \{a^{2i}\,b^i\,c \mid i \geq 0\}$. Geef een *deterministische* PDA (stapelautomaat) voor L. Geef een *korte* toelichting.

3. (6 punten) Welke taal wordt *beslist* door de volgende Turing Machine (alleen q_3 is accepterend)? Licht uw antwoord *kort* toe.



4. (6 punten, elk fout antwoord kost 2 punten) Geef van de volgende beweringen aan of ze WAAR of ONWAAR zijn. (Een toelichting is niet nodig).

(a) Voor elke contextvrije grammatica (CFG) bestaat een Turing Machine (TM) die dezelfde taal accepteert.

(b) Voor elke contextvrije grammatica (CFG) bestaat een equivalente uitgebreide stapelautomaat (extended PDA) met twee toestanden.

(c) De klasse van contextvrije talen is gesloten onder complement.

(d) De klasse van contextvrije talen is gesloten onder vereniging.

(e) Voor elke PDA bestaat een equivalente deterministische PDA.

(f) Voor elke TM bestaat een equivalente deterministische TM.

(g) De taal van (gecodeerde) terminerende Turing Machines is niet recursief maar wel recursief opsombaar.

(h) Gegeven een grammatica G in Chomsky Normaalvorm en een woord w, dan kunnen we in polynomiale tijd testen of $w \in \mathcal{L}(G)$.

Algebra

5. Zij G de verzameling matrices gegeven door:

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

Op G beschouwen we de bewerking matrixvermenigvuldiging.

(a) Laat zien dat G met matrixvermenigvuldiging een groep is.

(b) Zij $\mathbb{F} = \mathbb{Z}_3[x]/ < x^2 + 1 >$. Laat zien dat $\phi : G \to \mathbb{F} \backslash \{0\}$ gedefinieerd door

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

een groepsisomorfisme tussen G en de vermenigvuldigingsgroep van het lichaam $\mathbb{F}$ definieert.

6. Gegeven de permutaties:

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

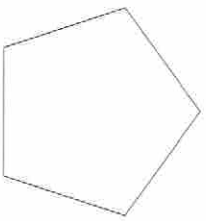
Schrijf α, β en $\beta\alpha$ als:

(a) Produkt van disjunkte cycels.

(b) Produkt van 2-cycels.

(c) Wat is de orde van α?

7. Bepaal met behulp van de stelling van Burnside op hoeveel verschillende manieren de zijden van een in de vorm van een regelmatige vijfhoek (zie afbeelding) gevouwen koperdraad gekleurd kunnen worden met twee kleuren.



8. (a) Laat $a(x) = x^2 + a_1x + a_0 \in \mathbb{Z}_2[x]$. Bepaal alle mogelijke waarden van a_0 en a_1 waarvoor $a(x)$ irreducibel is.

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

   (b) Bewijs dat $p(x)$ irreducibel is.

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

   (c) Is $\mathbb{F}$ een lichaam?

   (d) Hoeveel elementen heeft $\mathbb{F}$?

Punten: **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 punten) Bekijk de RSA methode, en neem aan dat Alice de modulus $n = 65$ en de exponent $e = 11$ heeft gepubliceerd. Bob mailt het gecodeerde bericht $C = 2$ naar Alice. Bereken alle gegevens die Alice nodig heeft om Bob's oorspronkelijke bericht M te berekenen, en bereken ook M.

10. (3 punten) Laat zien dat $15^{17} = 15 \pmod{17}$ (zonder veel rekenwerk).