Kenmerk: EWI2016/TW/DMMP/MU/2016-2 (see page 4 for an English version)

Hertentamen 2, Module 7, Vakcode 201400433

Discrete Structuren & Efficiënte Algoritmes

Vrijdag 15 april 2016, 08:45 - 11:45

Alle antwoorden dienen te worden gemotiveerd. Gebruik van een rekenmachine is niet toegestaan. Gebruik van zelfgeschreven formulebladen, één dubbelzijdig A4, is wel toegestaan. Indien u een onderdeel niet kunt oplossen dan kunt 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. (8 punten) Beschouw de volgende contextvrije grammatica (CFG) G:

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

   (a) Transformeer G stapsgewijs naar een equivalente CFG G_1, zodat G_1 geen kettingregels en geen λ-regels bevat.

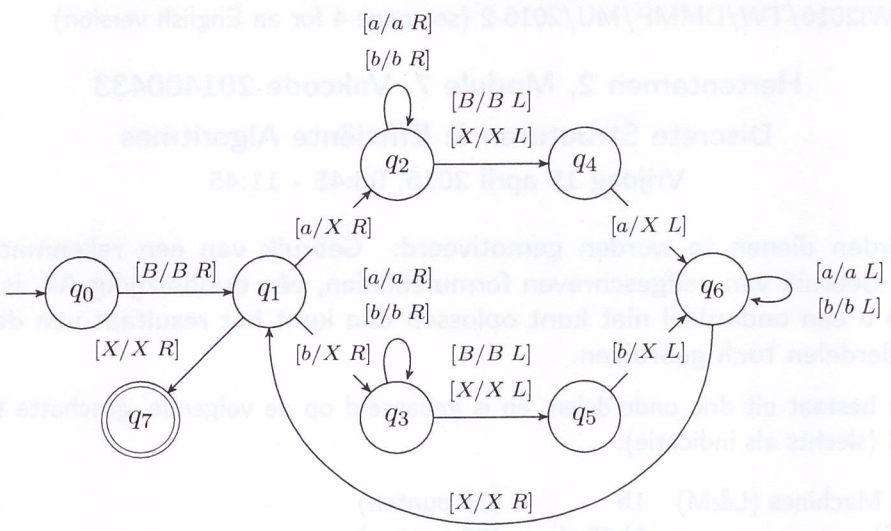
   (b) Geef een equivalente grammatica G_2 in Greibach Normaalvorm.

2. (12 punten) Beschouw de contextvrije taal $L := \{a^i\,b\,a^j \mid j \geq i \geq 0\}$.

   (a) Geef een *deterministische* PDA (stapelautomaat) voor L.
   Leg *kort* de werking van uw automaat uit.

   (b) Is de taal $L \cap \big((aaa)^*\,b\,(aaa)^*\big)$ contextvrij? Hoe volgt dat uit de geslotenheidseigenschappen van contextvrije talen?

3. (10 punten) Beschouw de volgende Turing Machine (TM) met twee tapes.



(a) Bij invoer $abaa$ schrijven we de start configuratie als $[q_0BabaaB]$.
Wat is de eind-configuratie na terminatie van de TM bij deze invoer?
Wordt het woord $abaa$ geaccepteerd door bovenstaande TM?

(b) Welke taal wordt door deze TM *beslist*? (leg kort uit)

Algebra

4. Zij $V = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, de viergroep van Klein. Zoals bekend is iedere eindige groep isomorf met een ondergroep van S_n (de permutatiegroep van n symbolen).

   (a) (4 punten) Waarom kan V niet isomorf zijn met een ondergroep van S_3?

   (b) (6 punten) Bepaal een ondergroep H van S_4 zodanig dat V isomorf is met H.

5. Zij $(G, \cdot)$ een groep. Definieer

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

   (a) (5 punten) Laat zien dat $Z(G)$ een ondergroep van G is.

   (b) (6 punten) Zij nu G de matrixgroep met als bewerking matrixvermenigvuldiging

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

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

   (c) (6 punten) Laat zien dat $\mathrm{Z}(G)$ uit onderdeel 5b isomorf is met $\mathbb{R}\backslash\{0\}$ met de gewone vermenigvuldiging.

6. Zij $p(x) \in \mathbb{Z}_5[x]$ gegeven door: $p(x) = x^3 + 2x^2 + 1$ en $I =< p(x) >$ het ideaal in $\mathbb{Z}_5[x]$ voortgebracht door $p(x)$.

(a) (3 punten) Laat zien dat $p(x)$ irreducibel is.

(b) (4 punten) Beargumenteer dat $\mathbb{F} = \mathbb{Z}_5[x]/I$ een lichaam is.

(c) (4 punten) Beschrijf de algemene vorm van de elementen van $\mathbb{F} = \mathbb{Z}_5[x]/I$. Hoeveel verschillende elementen zijn er?

(d) (8 punten) Bepaal de inverse van $2x + 3 + I$ in $\mathbb{F}$.

(e) (4 punten) Laat zien dat $\mathbb{F}$ isomorf is met $\mathbb{Z}_5[x]/< x^3 + 3x + 2 >$.

Discrete Wiskunde

7. (6 punten) Bekijk de RSA methode, en neem aan dat Alice de modulus $n = 55$ en de exponent $e = 7$ heeft gepubliceerd. Bob mailt het gecodeerde bericht $C = 2$ naar Alice. Beschrijf een manier voor afluisteraar Eve om C te decoderen, bepaal alle gegevens die Eve hiervoor nodig heeft, en bereken Bob's oorspronkelijke bericht M.

8. (4 punten) We nemen aan dat we divisie met rest (integer division) van twee getallen $n, a \in \mathbb{Z}$, $n \geq a$ in tijd $O(\log n)$ kunnen doen. Dat wil zeggen dat we in $O(\log n)$ tijd $q, a \in \mathbb{Z}$ kunnen berekenen zodat $n = qa + r$, met $0 \leq r < a$. Noem de functie die de rest r in $n = qa + r$ terug geeft `r(n,a)` (in python `r(n,a) = n % a`).

   Geef in pseudocode (geen python vereist) een algoritme dat bepaalt of een gegeven getal $k \in \mathbb{Z}$ een priemgetal is of niet. Geef ook een bovengrens voor de rekentijd van je algoritme (in $O(\,)$-notatie). Is je algoritme een polynomiale tijd algoritme?

Re-Exam 2, Module 7, Code 201400433

Discrete Structures & Efficient Algorithms

Friday, April 15, 2016, 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. 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. (8 points) Consider the following context-free grammar (CFG) G:

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

   (a) Transform G stepwise to an equivalent CFG G_1, such that G_1 contains neither chain rules, nor λ-rules.

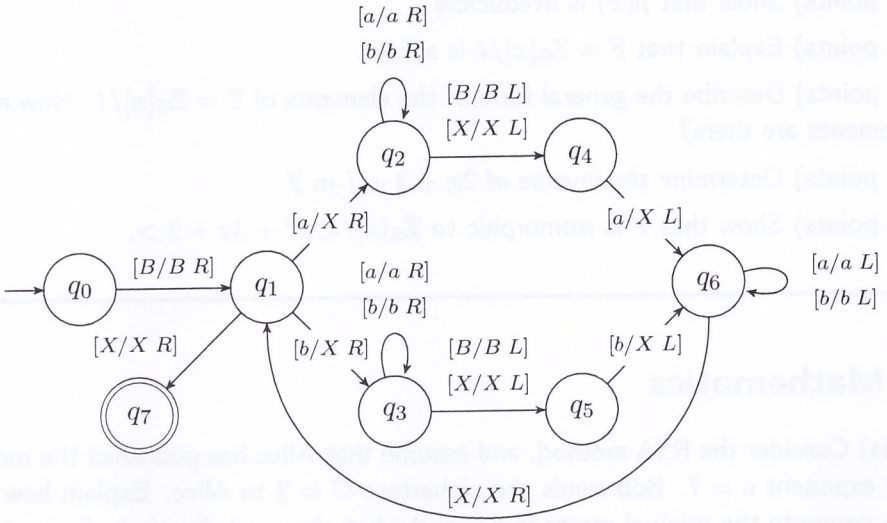
   (b) Provide an equivalent grammar G_2 in Greibach Normal Form.

2. (12 points) Consider the context-free language $L := \{a^i\,b\,a^j \mid j \geq i \geq 0\}$.

   (a) Provide a *deterministic* PDA (stack automaton) for L.
   Explain *shortly* the working of your automaton.

   (b) Is the language $L \cap \big((aaa)^*\,b\,(aaa)^*\big)$ context-free? How does this follow from the closure properties of context-free languages?

3. (10 points) Consider the following Turing Machine (TM).



(a) Given input $abaa$, we write the start configuration as $[q_0BabaaB]$.
What is the end configuration after the TM halts on this input?
Will the word $abaa$ be accepted by this TM?

(b) Which language will be *decided* by this TM? (Explain shortly).

Algebra

4. Let $V = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, be the Klein four-group . As is well-known, each finite group is isomorphic to a subgroup of S_n (the permutationgroup of n symbols).

   (a) (4 points) Why can V not be isomorphic to a subgroup of S_3?

   (b) (6 points) Determine a subgroup H of S_4 such that V is 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) (5 points) Show that $Z(G)$ is a subgroup of G.

   (b) (6 points) Now let G be the matrixgroup with as operation matrixmultiplication

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

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

   (c) (6 points) 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) (3 points) Show that $p(x)$ is irreducible.

(b) (4 points) Explain that $\mathbb{F} = \mathbb{Z}_5[x]/I$ is a field.

(c) (4 points) Describe the general form of the elements of $\mathbb{F} = \mathbb{Z}_5[x]/I$. How many different elements are there?

(d) (8 points) Determine the inverse of $2x + 3 + I$ in $\mathbb{F}$.

(e) (4 points) Show that $\mathbb{F}$ is isomorphic to $\mathbb{Z}_5[x]/< x^3 + 3x + 2 >$.

Discrete Mathematics

1. (6 points) Consider the RSA method, and assume that Alice has published the modulus $n = 55$ and the exponent $e = 7$. Bob sends the ciphertext $C = 2$ to Alice. Explain how eavesdropper Eve can compute the original message M, and what she needs for that. Compute M.

2. (4 points) Assume we can do integer division w. rest for any $n, a \in \mathbb{Z}$, $n \geq a$ in time $O(\log n)$. That means we can compute, in $O(\log n)$ time, $q, a \in \mathbb{Z}$ with $n = qa + r$, with $0 \leq r < a$. Denote the function that returns r in $n = qa + r$, `r(n,a)` (in python `r(n,a) = n % a`).

   Describe in pseudocode (no python necessary) an algorithm that determines, for any input $k \in \mathbb{Z}$, if k is a prime or not. Also give an upper bound on the computation time (use $O(\ )$-notation). Is this a polynomial time algorithm?