

Kenmerk: EWI2016/TW/DMMP/MU (see page 4 for the English version)

Tentamen 2, Module 7, Vakcode 201400433

Discrete Structures & Efficiënte Algoritmes

Maandag 04 april 2016, 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!

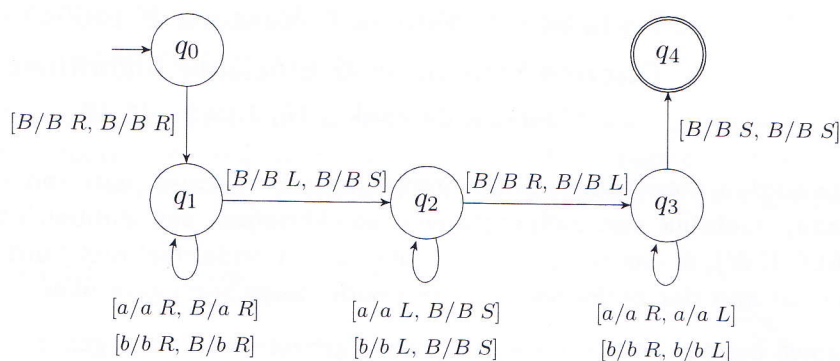
Languages & Machines

- (a) (6 pts) Transformeer de volgende contextvrije grammatica G stapsgewijs tot een equivalente contextvrije grammatica G' , zodat G' geen kettingregels en geen λ -regels meer bevat.

$$G = \begin{cases} S \rightarrow AB \\ A \rightarrow \lambda \mid aA \\ B \rightarrow C \mid bB \\ C \rightarrow c \mid cB \end{cases}$$

- (b) (2 pts) Is uw grammatica G' een reguliere grammatica? Waarom?
- (a) (8 pts) Beschouw de contextvrije taal $L = \{a^i (ba)^j \mid j > i > 0\}$. Geef een *deterministische* PDA (stapelautomaat) voor L . Leg *kort* de werking van uw automaat uit.
 - (b) (4 pts) Gegeven is een PDA P , een CFG G en een NFA M . Is de taal $(\mathcal{L}(P) \cap \mathcal{L}(M)) \cup \mathcal{L}(G)$ context-vrij? Waarom?

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



We zetten de invoer op tape 1 en tape 2 start blanco. Bij invoer aba noteren we de startconfiguratie als volgt, waarbij B een blanco symbool op de tape is, en $*$ de positie van de koppen weergeeft:

$$[q_0; *BabaB; *BBBBB]$$

- (5 pts) Geef de berekening van deze TM voor het invoerwoord aba (om schrijfwerk te besparen mag u stappen binnen een toestand q_i overslaan). Wordt het woord aba geaccepteerd door bovenstaande TM?
- (5 pts) Welke taal wordt door deze TM *beslist*? (leg kort uit)

Algebra

- Zij $G = U(14)$ (unitaire groep).
 - (3 pts) Bepaal de orde van $3 \in G$.
 - (3 pts) Is G cyclisch?
 - (5 pts) Bepaal een isomorfisme van G naar een ondergroep van S_6 , de groep van permutaties van zes symbolen, door van elk element van G het beeld in S_6 te geven. Schrijf deze beelden in disjuncte-cykel-vorm.
 - (5 pts) Bepaal met behulp van de vorige onderdelen, dus zonder verdere berekeningen, de ordes van de elementen van G .
- Zij $R = \{a + b\alpha \mid a, b \in \mathbb{Z}_3\}$, hierbij is α een symbool met de eigenschap: $\alpha^2 = 2$. Op R gebruiken we de voor de hand liggende optelling en vermenigvuldiging zodat R een ring is.
 - (3 pts) Geef de definitie van nuldeeler.
 - (6 pts) Ga na of R nuldelers heeft. Hint: beschouw $(a+b\alpha)(c+d\alpha) = 0$ en vermenigvuldig met $(a+2b\alpha)(c+2d\alpha)$ en werk uit.
 - (6 pts) Beredeneer dat R een lichaam is en bepaal $(1 + \alpha)^{-1}$.

6. (a) (3 pts) Geef de definitie van irreducibel polynoom in $\mathbb{F}[x]$.
- (b) (6 pts) Laat zien dat $g(x), h(x) \in \mathbb{Z}_3[x]$ met $g(x) = x^2 + 1$ en $h(x) = x^2 + 2x + 2$ de enige irreducibele monische polynomen, dwz leidende coëfficiënt gelijk aan één, van graad twee in $\mathbb{Z}_3[x]$ zijn.
- (c) (4 pts) Op hoeveel manieren kan een vierdegraadspolynoom *reducibel* zijn?
- (d) (4 pts) Laat zien dat $p(x) = x^4 + x^2 + x + 1 \in \mathbb{Z}_3[x]$ irreducibel is.
- (e) (2 pts) Construeer een lichaam van precies eenentachtig elementen en geef de algemene vorm van deze elementen.
-

Discrete Mathematics

7. Bekijk de RSA methode, en neem aan dat Alice de modulus $n = 55$ en de exponent $e = 3$ heeft gepubliceerd. Bob mailt het gecodeerde bericht $C = 2$ naar Alice.
- (a) (3 pts) Noem in het kort *alle* algoritmische problemen die afuisteraar Eve zou moeten oplossen om het oorspronkelijke bericht M van Bob te berekenen. Welke hiervan zijn efficient oplosbaar, en welke niet? Waarom wordt RSA dus in de praktijk als werkbare, en ook veilige methode beschouwd?
- (b) (7 pts) Bereken Bob's oorspronkelijke bericht M .

Exam 2, Module 7, Code 201400433
 Discrete Structures & Efficient Algorithms
 Monday, April 4, 2016, 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 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 of points divided by 10.

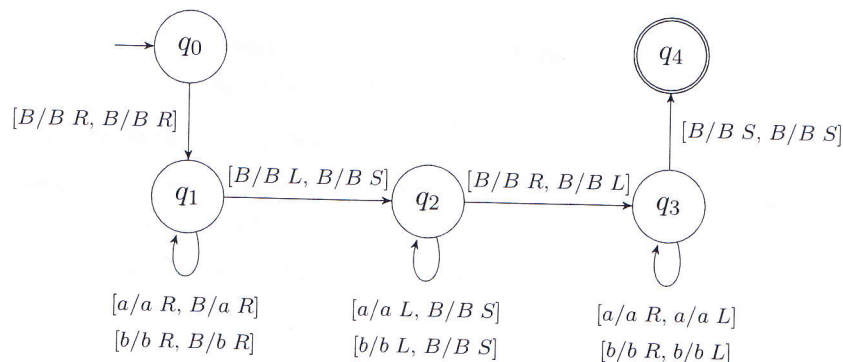
Please use a new sheet of paper for each part (L&M/ALG/DW)!

Languages & Machines

1. (a) (6 pts) Transform the following context-free grammar G stepwise to an equivalent context-free grammar G' , such that G' contains neither chain rules, nor λ -rules.

$$G = \begin{cases} S \rightarrow AB \\ A \rightarrow \lambda \mid aA \\ B \rightarrow C \mid bB \\ C \rightarrow c \mid cB \end{cases}$$

- (b) (2 pts) Is your grammar G' a regular grammar? Why?
2. Consider the context-free language $L = \{a^i (ba)^j \mid j > i > 0\}$.
- (a) (8 pts) Provide a *deterministic* PDA (stack automaton) for L . Explain *shortly* the working of your automaton.
- (b) (4 pts) Given are an arbitrary PDA P , a CFG G and an NFA M . Is the language $(\mathcal{L}(P) \cap \mathcal{L}(M)) \cup \mathcal{L}(G)$ context-free? Why?
3. Consider the following Turing Machine (TM) with two tapes.



The input is placed on tape 1, and tape 2 initially contains only blanks. Given input aba , we write the start configuration as follows, where B denotes the blank symbol, and $*$ shows the position of the tape heads:

$$[q_0; *BabaB; *BBBBB]$$

- (a) (5 pts) Provide the computation for this TM on the input word aba (to save writing, you may skip steps that stay in a state q_i).
Will the word aba be accepted by the given TM?
 - (b) (5 pts) Which language will be *decided* by this TM? (explain shortly)
-

Algebra

4. Let $G = U(14)$ (unitary group).
 - (a) (3 pts) Determine the order of $3 \in G$.
 - (b) (3 pts) Is G cyclic?
 - (c) (5 pts) 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) (5 pts) Derive, without any calculations, the orders of all elements of G by using the previous parts.
5. 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) (3 pts) Give the definition of zero divisor.
 - (b) (6 pts) 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) (6 pts) Argue that R is a field and calculate $(1 + \alpha)^{-1}$.
6.
 - (a) (3 pts) Provide the definition of irreducible polynomial in $\mathbb{F}[x]$.
 - (b) (6 pts) Show that $g(x), h(x) \in \mathbb{Z}_3[x]$ with $g(x) = x^2 + 1$ 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) (4 pts) In how many ways can we write a polynomial of degree four as a product of nontrivial factors?
 - (d) (4 pts) Show that $p(x) = x^4 + x^2 + x + 1 \in \mathbb{Z}_3[x]$ is irreducible.
 - (e) (2 pts) Construct a field consisting of exactly 81 elements and give the general form of these elements.

Discrete Mathematics

7. Consider the RSA method, and assume that Alice has published modulus $n = 55$ and exponent $e = 3$. Bob emails ciphertext $C = 2$ to Alice.
- (a) (3 pts) Name briefly *all* algorithmic problems that an eavesdropper Eve needs to solve in order to compute Bob's original message M . Which of these can be efficiently solved, and which of them cannot? Argue why is RSA considered to be a practical, yet safe cryptosystem.
 - (b) (7 pts) Compute Bob's original message M .