Name/DoB/Room: Answer Key

IT University of Copenhagen

Foundations of Computing—Discrete Mathematics BSc

Midterm Assignment

October 8, 2019

Instructions (*read carefully*)

Contents: The midterm contains 8 questions for the total of 19 points. The midterm is divided into two parts: The first part has 4 multiple choice questions and the second part has 4 open ended questions (some of the open ended questions have subquestions).

What to check: In the multiple choice questions, there is one and only one correct answer. You should only check 1 box.

Definitions and theorems: At the end of this document (page 5) you can find some definitions and theorems that could be useful for answering some of the questions.

Info about you: Write *clearly* your *full name*, your date of birth (DoB) and the room that you normally go to exercises in (i.e. 2A52, 2A54, or 4A16) on every page (top-right) including the front page.

—IMPORTANT—
Only information written on the pages 1–5 will be evaluated.
Anything else that you hand-in will NOT be considered for the final evaluation!

Part I. Answer the following multiple choice questions.

1. (2 pts) Which of the following statements is *true*?

☑ $\{(2,4),(2,6),(2,8),(3,6),(3,9),(4,8)\} \subset \mid \cap (\{2\ldots9\} \times \{2\ldots9\})$
where $\mid$ is the "divides" relation

B $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$ for arbitrary sets A, B

C $\{3, \sqrt{10}, 24 \textbf{ mod } 7\} \subseteq \{8 \textbf{ mod } 5\}$

D $(A - C) \cap (B - C) = \emptyset$ for arbitrary sets A, B, C

2. (2 pts) Which one is a valid representation of $(E74)_{16}$?

A $(3900)_{10}$

☑ $(111001110100)_2$

C $(7174)_8$

D $(11011011)_2$

3. (2 pts) Let $a_k = a_{k-1} + 2a_{k-2}, a_0 = -1, a_1 = 2$. Which of the following statements is *true*?

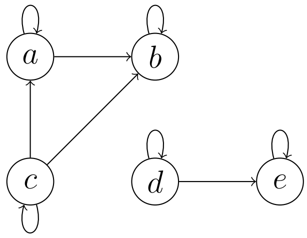
A $a_0 = a_3$

B $a_k + a_{k+1} = a_k - a_{k-1}$ for all k

☑ $a_k \cdot a_{k+1} = a_k^2 + 2 \cdot a_k \cdot a_{k-1}$ for all k

D $\sum_{i=1}^{4} a_k = a_5$

4. (2 pts) Consider the following directed graph representing the relation R on the set $\{a, b, c, d, e\}$.



Which of the following statements is *true*?

$\boxed{\text{A}}$ R is antisymmetric and transitive, but not reflexive

$\boxed{\text{B}}$ R is transitive, but neither reflexive nor antisymmetric

$\boxed{\text{C}}$ R is antisymmetric, but neither reflexive nor transitive

$\boxed{\text{D}}$ R is reflexive and antisymmetric and transitive

Part II. Answer the following questions. Be brief but precise, your correct use of mathematical notation is an important aspect of your answer.

5. (a) (3 pts) Construct a valid judgment (derivation) for the following predicate:

$$\exists x(\neg Q(x)) \to (\forall y(P(y) \to Q(y))) \to \neg\forall z(P(z))$$

Solution:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\exists x\ (\neg Q(x))}\ h1 \qquad \dfrac{\dfrac{}{\neg Q(a)}\ h4 \qquad \dfrac{\dfrac{\dfrac{}{\forall y\ (P(y) \to Q(y))}\ h2}{P(a) \to Q(a)}\ \forall E \qquad \dfrac{\dfrac{}{\forall z\ (P(z))}\ h3}{P(a)}\ \forall E}{Q(a)}\ \to E}{\mathbf{F}}\ \neg E}{\dfrac{\mathbf{F}}{\neg\forall z\ (P(z))}\ \neg I^{h3}}\ \exists E^{a,h4}}{\forall y\ (P(y) \to Q(y)) \to \neg\forall z\ (P(z))}\ \to I^{h2}}{\exists x\ (\neg Q(x)) \to \forall y\ (P(y) \to Q(y)) \to \neg\forall z\ (P(z))}\ \to I^{h1}$$

(b) (1 pt) Is this predicate valid in intuitionistic logic, classical logic, or both? Explain your answer.

Solution: Since we do not resort to the law of excluded middle, this argument is valid both in classical and intuitionistic logic.

6. (3 pts) Assume that A and B are non-empty sets and that $f : A \to B$ is a bijective function. Let $g : A \to \mathcal{P}(B)$ be the function defined as $g(a) = \{f(a)\}$ for all $a \in A$. One of the following statements is true, and one is false.

1. g is injective.
2. g is surjective.

Write which statement is true and prove it. Write which statement is false and find a counter example. (Just answering which is true and which is false gives no points.)

Solution: The function g is injective but not surjective.
To prove g injective we need to prove $\forall x, y \in A\ (g(x) = g(y) \to x = y)$. Take two arbitrary elements a, b and assume $g(a) = g(b)$, to prove $a = b$. By definition of g, $g(a) = \{f(a)\} = \{f(b)\} = g(b)$, and hence $f(a) = f(b)$ since they are the only elements in the two sets. Since f is injective, we can conclude $a = b$, proving our result.
As a counterexample to point (2), the image of g does not contain $\emptyset$.

7. (2 pts) Let A, B and C be sets. Show that if $A \subseteq B$ and $B \subseteq \overline{C}$, then $A \cap C = \emptyset$.

Solution: We take an arbitrary element a and assume $a \in A \cap C$ to reach a contradiction. If $a \in A \cap C$ then $a \in A$ and $a \in C$. Because $A \subseteq B$ then $a \in B$, and because $B \subseteq \overline{C}$ then $a \in \overline{C}$. Hence we have that $a \in C$ and $a \in \overline{C}$, which is a contradiction. Therefore $A \cap C = \emptyset$.

8. (2 pts) Let $a, b \in \mathbb{Z}$ be integers, and assume that $a \mid b$. Prove that $a \mid 5b + a$.

Solution: By definition $a \mid b$ iff there exists $k \in \mathbb{Z}$ such that $b = k \cdot a$. Therefore $5b + a = 5(k \cdot a) + a = (5k + 1) \cdot a$. Hence we found an integer $(5k + 1)$ that multiplied by a gives us $5b + a$, therefore $a \mid 5b + a$.

Definitions and theorems

Logic

The logic rules for propositional and predicate logics are given below.

Conjunction:

$$\frac{A\ \mathsf{true} \quad B\ \mathsf{true}}{A \wedge B\ \mathsf{true}}\ \wedge I \qquad \frac{A \wedge B\ \mathsf{true}}{A\ \mathsf{true}}\ \wedge E_1 \qquad \frac{A \wedge B\ \mathsf{true}}{B\ \mathsf{true}}\ \wedge E_2$$

Implication:

$$\frac{\begin{array}{c}\overline{A\ \mathsf{true}}^{\ u}\\ \vdots\\ B\ \mathsf{true}\end{array}}{A \to B\ \mathsf{true}}\ {\to}I^u \qquad \frac{A \to B\ \mathsf{true} \quad A\ \mathsf{true}}{B\ \mathsf{true}}\ {\to}E$$

Disjunction:

$$\frac{A\ \mathsf{true}}{A \vee B\ \mathsf{true}}\ \vee I_1 \qquad \frac{B\ \mathsf{true}}{A \vee B\ \mathsf{true}}\ \vee I_2 \qquad \frac{A \vee B\ \mathsf{true} \quad \begin{array}{c}\overline{A\ \mathsf{true}}^{\ u}\\ \vdots\\ C\ \mathsf{true}\end{array} \quad \begin{array}{c}\overline{B\ \mathsf{true}}^{\ v}\\ \vdots\\ C\ \mathsf{true}\end{array}}{C\ \mathsf{true}}\ \vee E^{u,v}$$

True and false:

$$\frac{}{\mathbf{T}\ \mathsf{true}}\ \mathbf{T}I \qquad \frac{\mathbf{F}\ \mathsf{true}}{C\ \mathsf{true}}\ \mathbf{F}E$$

Negation:

$$\frac{\begin{array}{c}\overline{A\ \mathsf{true}}^{\ u}\\ \vdots\\ \mathbf{F}\ \mathsf{true}\end{array}}{\neg A\ \mathsf{true}}\ \neg I^u \qquad \frac{\neg A\ \mathsf{true} \quad A\ \mathsf{true}}{C\ \mathsf{true}}\ \neg E$$

Classical rules:

$$\frac{}{A \vee \neg A\ \mathsf{true}}\ LEM \qquad \frac{\neg\neg A\ \mathsf{true}}{A\ \mathsf{true}}\ \neg\neg C \qquad \frac{\begin{array}{c}\overline{\neg A\ \mathsf{true}}^{\ u}\\ \vdots\\ \mathbf{F}\ \mathsf{true}\end{array}}{A\ \mathsf{true}}\ \mathbf{F}_C^u$$

Quantifiers:

$$\frac{A[a/x]\ \mathsf{true}}{\forall x(A)\ \mathsf{true}}\ \forall I^a \qquad \frac{\forall x(A)\ \mathsf{true}}{A[t/x]\ \mathsf{true}}\ \forall E$$

$$\frac{A[t/x]\ \mathsf{true}}{\exists x(A)\ \mathsf{true}}\ \exists I \qquad \frac{\exists x(A)\ \mathsf{true} \quad \begin{array}{c}\overline{A[a/x]\ \mathsf{true}}^{\ u}\\ \vdots\\ C\ \mathsf{true}\end{array}}{C\ \mathsf{true}}\ \exists E^{a,u}$$

Sets

Size of a set $|A|$ denotes the number of elements of A

Emptyset $\forall x(x \notin \emptyset)$

Equality $A = B$ iff $\forall x(x \in A \leftrightarrow x \in B)$

Subset $A \subseteq B$ iff $\forall x(x \in A \rightarrow x \in B)$

Union $A \cup B = \{x \mid x \in A \vee x \in B\}$ Property: $\forall x(x \in A \cup B \leftrightarrow x \in A \vee x \in B)$

Intersection $A \cap B = \{x \mid x \in A \wedge x \in B\}$ Property: $\forall x(x \in A \cap B \leftrightarrow x \in A \wedge x \in B)$

Difference $A - B = \{x \mid x \in A \wedge x \notin B\}$ Property: $\forall x(x \in A - B \leftrightarrow x \in A \wedge x \notin B)$

Complement $\bar{A} = U - A$ Property: $\forall x(x \in \bar{A} \leftrightarrow x \in U \wedge x \notin A)$

Cartesian product $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$

Relations

Binary relation from A to B is a subset of $A \times B$

Relation on a set A is a relation from A to A (subset of $A \times A$)

Reflexive relation R on set A satisfies $\forall x \in A((x, x) \in R)$
Digraphs: loops on every vertex

Symmetric relation satisfies $\forall x, y \in A((x, y) \in R \leftrightarrow (y, x) \in R)$
Digraphs: every edge has the corresponding edge in the opposite direction

Antisymmetric relation satisfies $\forall x, y \in A((x, y) \in R \wedge (y, x) \in R \rightarrow x = y)$
Digraphs: never two edges in the opposite direction

Transitive relation satisfies $\forall x, y, z \in A((x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R)$
Digraphs: an edge $a \rightarrow b$ and an edge $b \rightarrow c$ implies an edge $a \rightarrow c$

Composing relations $S \circ R = \{(x, y) \mid (x, z) \in R \wedge (z, y) \in S\}$
Property: $\forall x, y((x, y) \in S \circ R \leftrightarrow \exists z((x, z) \in R \wedge (z, y) \in S))$

Partial ordering R on S iff R is reflexive, antisymmetric and transitive.

Poset $(S, \preceq)$ is a poset iff $\preceq$ is a partial ordering on S.

Comparable a and b are comparable iff $a \preceq b$ or $b \preceq a$

Total order $(S, \preceq)$ iff all elements are comparable

Maximal element a is maximal iff $\neg\exists x \in S(a \prec x)$

Minimal element a is minimal iff $\neg\exists x \in S(x \prec a)$

Greatest element a is greatest iff $\forall x \in S(x \preceq a)$

Least element a is least iff $\forall x \in S(a \preceq x)$

Upper bound u of A iff $\forall x \in A(x \preceq u)$

Lower bound l of A iff $\forall x \in A(l \preceq x)$

Functions

Function $f : A \to B$ assigns exactly one element of B to each element of A.
A is the **domain** and of f B is the **codomain** of f.

Image, preimage Let $f(a) = b$, then b is the **image** and a is the **preimage**.

Image of a set $S \subseteq A$: $f(S) = \{y \in B \mid x \in S, y = f(x)\}$

One-to-one/injective function $\forall x, y \in A(f(x) = f(y) \to x = y)$

Onto/surjective function $\forall y \in B\ \exists x \in A(f(x) = y)$

One-to-one correspondence / bijection is both one-to-one and onto.

Function composition $\forall x((f \circ g)(x) = f(g(x)))$
$\forall x, y((f \circ g)(x) = y \leftrightarrow \exists z(f(x) = z \wedge g(z) = y))$

Sequences and Summations

Geometric progression A sequence of the form $a, ar, ar^2, \ldots, ar^n, \ldots$, where $a \in \mathbb{R}$ is the *initial term* and $r \in \mathbb{R}$ is the *common ratio*.

Arithmetic progression A sequence of the form $a, a + d, a + 2d, \ldots, a + nd, \ldots$, where $a \in \mathbb{R}$ is the *initial term* and $d \in \mathbb{R}$ is the *common difference*.

Some Useful Summation Formulae

Sum	Closed form	Sum	Closed form
$\sum_{k=0}^{n} ar^k (r \neq 0)$	$\frac{ar^{n+1} - a}{r - 1}, r \neq 1$	$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$	$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=1}^{\infty} x^k, \lvert x\rvert < 1$	$\frac{1}{1-x}$	$\sum_{k=1}^{\infty} kx^{k-1}, \lvert x\rvert < 1$	$\frac{1}{(1-x)^2}$

Number Theory

Given two integers a and b, with $a \neq 0$, we say that a *divides* b if there exist an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. If a divides b then a is a *factor* (or *divisor*) of b, and b is said to be a *multiple* of a.

Theorem 1 (Division algorithm)**.** *Let a be an integer and d a positive integer. Then there exist unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.*

In theorem 1 the value d is called the *divisor*, a is the *dividend*, q is the *quotient*, and r is the *remainder*. Then $q = a \textbf{ div } d$, $r = a \textbf{ mod } d$. Remember that the remainder cannot be negative.

If a and b are integers and m is a positive integer, then a *is congruent to* b *modulo* m if $m \mid a - b$ and we write $a \equiv b \pmod{m}$.

The *greatest common divisor* of two integers a and b, not both zero, is denoted by $\gcd(a, b)$ and is the largest integer that both divides a and divides b.

The *Euclidean algorithm* provides a efficient way to compute the greatest common divisor of two integers. The algorithm is based on the following lemma.

Lemma 1. *Let $a = bq + r$ where a, b, q and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.*

Hexadecimal, octal and binary representation of integers 0 through 15

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Graph Theory

A *graph* $G = (V, E)$ consists of V, a nonempty set of *vertices* (or nodes) and E, a set of *edges*. Each edge has either one or two vertices associated with it, called its *endpoints*. An edge is said to *connect* its endpoints.

Theorem 2 (Handshaking theorem)**.** *Let $G = (V, E)$ be an undirected graph with m edges, then*

$$2m = \sum_{v \in V} \deg(v)$$

Note that this applies even if multiple edges and loops are present.

Theorem 3. *Let $G = (V, E)$ be a graph with directed edges, then $\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = |E|$.*

Graph terminology

Type	*Edges*	*Multiple edges are allowed?*	*Loops are allowed?*
Simple graph	Undirected	No	No
Multigraph	Undirected	Yes	No
Pseudograph	Undirected	Yes	Yes
Simple directed graph	Directed	No	No
Directed multigraph	Directed	Yes	Yes
Mixed graph	Directed and undirected	Yes	Yes