Name/DoB: Answer Key

IT University of Copenhagen

Foundations of Computing—Discrete Mathematics

Exam

January 3, 2017

Instructions (*read carefully*)

Contents: The exam contains 14 questions for the total of 34 points. The exam is divided into two parts: The first part has 10 multiple choice questions and the second part has 4 open ended questions.

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 9) 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* and your date of birth (DoB) on every page (top-right) including the front page.

—IMPORTANT—
Only information written on the pages 1–8 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.

S **1.** Which of the following statements is *true*?

A $\{a, b\} \times \{1, 2\} = \{(a, 1), (b, 2)\}$

☑ B $\emptyset \subseteq \{1, 2, 3, 4, 5, 6\}$

C $(\{1, 2\} \cup \{1, 3\}) \cap \{1, 3\} = (\{1, 2\} \cap \{1, 3\}) \cup \{1, 2\}$

D For any nonempty set A we have that $A \cap \emptyset = A$

NT **2.** What is the sum of the binary numbers $(11\,0110)_2$ and $(1111)_2$ as a binary expression?

☑ A $(100\,0101)_2$

B $(100\,1001)_2$

C $(100\,0001)_2$

D $(100\,1101)_2$

NT **3.** What is the hexadecimal expansion of $(100\,1111\,1100\,0111\,0110)_2$?

A $(9F8E6)_{16}$

B $(9F8EC)_{16}$

C $(4161476)_{16}$

☑ D $(4FC76)_{16}$

NT **4.** Which of the following statements is *true*?

A $3 \mid (5 \cdot c)$ for all positive integers c

B $(100)_2 > (10)_8$

☑ C $\gcd(9, 15) = \gcd(15, 21)$

D $12 \equiv 24 \pmod{24}$

F **5.** Let $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ be recursively defined by

$$f(1) = 1,$$
$$f(n) = nf(n-1).$$

What expression does the function calculate?

[A] $f(n) = \frac{n(n+1)}{2}$

[B ✓] $f(n) = n!$

[C] $f(n) = 2^n$

[D] $f(n) = n^n$

CP **6.** Assume that ITU user names must consist of either four or five characters, where each character is any of the 26 characters from `a` to `z`. To make user names easier to remember ITU is considering to introduce a policy where at least two of the characters in the user name must be identical:

- Examples of allowed user names are `azbz`, `azzz`, `zazz`, `zzzz`, `zazbz` and `zzzzz`.
- Examples of disallowed user names are `abcd` and `cegjk`.

What is the total number of allowed user names according to this policy?

[A] $2\,490\,519 = \frac{26^4}{4} + \frac{26^5}{5}$

[B] $80\,730 = \binom{26}{4} + \binom{26}{5}$

[C] $8\,252\,400 = 26 \cdot 25 \cdot 24 \cdot 23 + 26 \cdot 25 \cdot 24 \cdot 23 \cdot 22$

[D ✓] $4\,085\,952 = 26^4 - 26 \cdot 25 \cdot 24 \cdot 23 + 26^5 - 26 \cdot 25 \cdot 24 \cdot 23 \cdot 22$

CP **7.** Suppose that the probability of snow in Denmark is 10%. If it is snowing then 60% of all trains will be delayed. Otherwise, if it is not snowing then only 20% of the trains will be delayed. Given that a train is delayed, what is the probability of it is snowing?

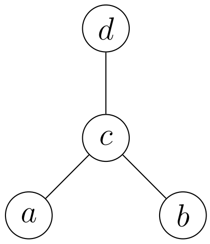
[A ✓] 25%

[B] 30%

[C] 60%

[D] 75%

S **8.** The following is the Hasse diagram for the partially ordered set $(\{a, b, c, d\}, \preccurlyeq)$.



Which of the following statements is *true*?

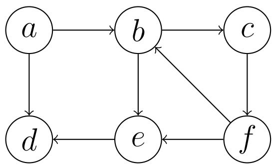
A $d \preccurlyeq c$

B $a \preccurlyeq b$

✔ There is no least element

D There is no greatest element

G **9.** Consider the following directed graph $G = (V, E)$.



Which of the following statements is *false*?

A G is a simple directed graph

✔ $H = (\{f\}, \{\})$ is a strongly connected component of G

C G is weakly connected

D The path b, c, f, b is a simple circuit of length 3

A **10.** Consider the grammar $G = (V, T, S, P)$, where P is the set of productions

$$P = \{S \to AB, B \to cBd, A \to aAb, A \to e, B \to e\}.$$

Which of the following statements is *true*?

$\boxed{\text{A}}$ The vocabulary is $V = \{a, b, c, d, e\}$

$\boxed{\text{B}}$ The language generated by G is $\{a^n e b^n c^m e d^m \mid n \geq 0, m \geq 0\}$

$\boxed{\text{C}}$ The language generated by G cannot be recognised by a Turing machine

$\boxed{\text{D}}$ The grammar G is right-linear (regular)

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

L **11.** Show that $\neg((q \to p) \to (p \vee \neg q))$ is a contradiction by constructing a truth table for all sub expressions.

Solution:

p	q	$q \to p$	$\neg q$	$p \vee \neg q$	$(q \to p) \to (p \vee \neg q)$	$\neg((q \to p) \to (p \vee \neg q))$
T	T	T	F	T	T	F
T	F	T	T	T	T	F
F	T	F	F	F	T	F
F	F	T	T	T	T	F

Since $\neg((q \to p) \to (p \vee \neg q))$ always is false for all true values of p og q the proposition is a contradiction.

L **12.** Prove, using induction, that

$$\sum_{i=1}^{n}\left(i-\frac{1}{2}\right)=\frac{n^2}{2}$$

for all integers $n \geq 1$.

Solution: We want to verify the statement

$$P(n) := \sum_{i=1}^{n}\left(i-\frac{1}{2}\right)=\frac{n^2}{2}$$

where n is an integer of value at least 1. So our base case is when $n = 1$.

Base case: Let $n = 1$. We have

$$\sum_{i=1}^{1}\left(i-\frac{1}{2}\right)=\left(1-\frac{1}{2}\right)=\frac{1}{2}=\frac{1^2}{2}.$$

Induction step: Suppose we know that $P(n)$ is true for some integer n that is equal or greater than 1. We now show that this implies $P(n+1)$ is true. We have that

$$\sum_{i=1}^{n+1}\left(i-\frac{1}{2}\right)=\left(\sum_{i=1}^{n}\left(i-\frac{1}{2}\right)\right)+\left((n+1)-\frac{1}{2}\right)=\frac{n^2}{2}+\frac{2n+1}{2}=\frac{(n+1)^2}{2}.$$

N **13.** Use the Euclidean algorithm to compute the greatest common divisor of 4 260 and 432.

Solution: If $a = q \cdot b + r$ then $\gcd(a,b) = \gcd(b,r)$. It then follows that

$$\begin{aligned} 4260 &= 9 \cdot 432 + 372 \\ 432 &= 1 \cdot 372 + 60 \\ 372 &= 6 \cdot 60 + 12 \\ 60 &= 5 \cdot 12 + 0 \end{aligned}$$

Thus

$$\gcd(4260, 432) = \gcd(432, 372) = \gcd(372, 60) = \gcd(60, 12) = \gcd(12, 0) = 12.$$

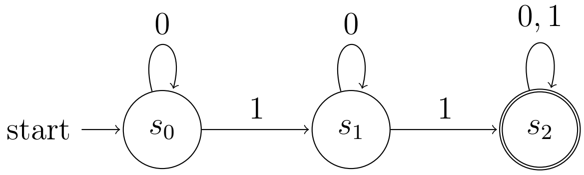
A **14.** Make a deterministic finite state automaton to recognise the regular set denoted by the regular expression:

$$(0 \cup 1)^*1(0 \cup 1)^*1(0 \cup 1)^*$$

Be sure to specify the entire machine formally.

Solution: A picture of an automaton or a table and set specification are two possible solutions. Please note that these are not the only possible solutions.

Possibility 1:



Possibility 2: $M = (S, I, f, s_0, F)$, where

- $S = (s_0, s_1, s_2)$,
- $I = \{0, 1\}$,
- $f : S \times I \to S$ is given by

	Input	
state	0	1
s_0	s_0	s_1
s_1	s_1	s_2
s_2	s_2	s_2

- $F = \{s_2\}$

Definitions and theorems

Logic

The truth table for a number of logical operators are given below.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \to q$	$p \leftrightarrow q$
T	T	F	T	T	F	T	T
T	F	F	F	T	T	F	F
F	T	T	F	T	T	T	F
F	F	T	F	F	F	T	T

A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it, is called a *tautology*. A compound proposition that is always false is called a *contradiction*.

The compound propositions p and q are called *logically equivalent* if $p \leftrightarrow q$ is a tautology. The notation $p \equiv q$ denotes that p and q are logically equivalent.

Below are given some of the rules of inference for propositional logic.

Modus Ponens
$$\begin{array}{rl} & p \\ & p \to q \\ \hline \therefore & q \end{array}$$

Modus Tollens
$$\begin{array}{rl} & \neg q \\ & p \to q \\ \hline \therefore & \neg p \end{array}$$

Addition
$$\begin{array}{rl} & p \\ \hline \therefore & p \vee q \end{array}$$

Simplification
$$\begin{array}{rl} & p \wedge q \\ \hline \therefore & p \end{array}$$

Conjunction
$$\begin{array}{rl} & p \\ & q \\ \hline \therefore & p \wedge q \end{array}$$

Disjunctive syllogism
$$\begin{array}{rl} & p \vee q \\ & \neg q \\ \hline \therefore & p \end{array}$$

Sets

A set is an (unordered) collection of objects, called *elements* or *members*.

The *union* of two sets A and B is the set

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

The *intersection* of A and B is the set

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

The *difference* of two sets A and B, denoted by $A - B$ (or by $A \setminus B$), is the set containing those elements in A but not in B, i.e.

$$A - B = \{x \mid x \in A \land x \notin B\}.$$

Given n sets $A_1, A_2, \ldots, A_n$,

$$\bigcup_{i=1}^{n} A_i = A_1 \cup \ldots \cup A_n \qquad \bigcap_{i=1}^{n} A_i = A_1 \cap \ldots \cap A_n.$$

The *Cartesian product* of two or more sets $A_1, A_2, \ldots, A_n$, denoted by $A_1 \times A_2 \times \ldots \times A_n$, is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$, where $a_i \in A_i$ for $1 \leq i \leq n$.

Functions

Given two non-empty sets A and B, a *function* f from A to B is an assignment of exactly one element of B to each element of A.

A function $f : A \to B$ is *onto* (or a surjection) if and only if for every element $b \in B$ there is an element $a \in A$ such that $f(a) = b$.

A function $f : A \to B$ is *one-to-one* (or an injunction) if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f.

A function f is a *bijection* if it is both one-to-one and onto.

Relations

Let A and B be sets. A *binary relation* from A to B is a subset of $A \times B$.

A *relation on a set* A is a relation from A to A.

A relation R on a set A is called *reflexive* if $(a, a) \in R$ for every element $a \in A$.

A relation R on a set A is called *symmetric* if $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$.

A relation R on a set A such that for all $a, b \in A$, if $(a, b) \in R$ and $(b, a) \in R$, then $a = b$ is called *antisymmetric.*

A relation R on a set A is called *transitive* if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$.

The *reflexive closure* of a binary relation R on A is the smallest reflexive relation on A that contains R.

The *symmetric closure* of a binary relation R on A is the smallest symmetric relation on A that contains R.

The *transitive closure* of a binary relation R on A is the smallest transitive relation on A that contains R.

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

Counting

Choose r objects from n	Order matters, not all elements (r-permutations)	Order matters, all elements (permutations)	Order does not matter, not all elements (combinations)
Without repetitions	$P(n, r) = \frac{n!}{(n-r)!}$	$P(n, n) = n!$	$C(n, r) = \binom{n}{r} = \frac{n!}{r!\,(n-r)!}$
With repetitions	n^r	$\frac{n!}{n_1!n_2!\cdots n_k!}$, where $n = n_1 + n_2 + \ldots + n_k$	$\binom{n+r-1}{r}$

Probability Theory

Theorem 2 (Bayes' Theorem)**.** *Let E and F be events from a sample space S such that $p(E) \neq 0$ and $p(F) \neq 0$. Then*

$$p(F|E) = \frac{p(E|F)p(F)}{p(E)}\,. \tag{1}$$

The denominator in equation (1) can be expressed as

$$p(E) = p(E|F)p(F) + p(E|\bar{F})p(\bar{F})\,.$$

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 3 (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.

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

Definition 1 (Paths in undirected graphs)**.** *Let n be a nonnegative integer and G an undirected graph. A* path *of length n from x_0 to x_n in G is a sequence of n edges $e_1 = \{x_0, x_1\}, e_2 = \{x_1, x_2\}, \ldots, e_n = \{x_{n-1}, x_n\}$. When the graph is simple, we denote this path by its vertex sequence $x_0, x_1, \ldots, x_n$.*

The path is a circuit *if it begins and ends at the same vertex, that is, if $u = v$, and has length greater than zero. A path or circuit is* simple *if it does not contain the same edge more than once.*

Definition 2 (Paths in directed graphs)**.** *Let n be a nonnegative integer and G a directed graph. A* path *of length n from x_0 to x_n in G is a sequence of n edges $e_1 = (x_0, x_1), e_2 = (x_1, x_2), \ldots, e_n = (x_{n-1}, x_n)$. When there are no multiple edges in the directed graph, this path is denoted by its vertex sequence $x_0, x_1, x_2, \ldots, x_n$.*

A path of length greater than zero that begins and ends at the same vertex is called a circuit *or* cycle*. A path or circuit is called* simple *if it does not contain the same edge more than once.*

Definition 3 (Connectedness in undirected graphs)**.** *An undirected graph is called* connected *if there is a path between every pair of distinct vertices of the graph. An undirected graph that is not connected is called* disconnected*.*

A connected component *of a graph G is a connected subgraph of G that is not a proper subgraph of another connected subgraph of G. That is, a connected component of a graph G is a* maximal connected subgraph *of G.*

Definition 4 (Connectedness in directed graphs)**.** *A directed graph is* strongly connected *if there is a path from a to b and from b to a whenever a and b are vertices in the graph. A directed graph is* weakly connected *if there is a path between every two vertices in the* underlying undirected graph*.*

The subgraphs of a directed graph G that are strongly connected but not contained in larger strongly connected subgraphs, that is, the maximal strongly connected subgraphs*, are called the* strongly connected components *of G.*