Name,DoB: Answer Key

IT University of Copenhagen

Discrete Mathematics, MSc SD

Re-exam

1 March, 2022

Instructions (Read Carefully)

Contents: The exam contains 13 questions for a total of 100 points. The exam is divided into two parts: The first part has 9 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 7) 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).

—IMPORTANT—
Only information written on the pages 1–6 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. (6 pts) Which of the following statements is **true**?

A $A \subseteq \emptyset$ for all A.

B $(A \cup A) - A = \emptyset$ for all A.

C $\{1, 2\} \times \{3, 4\} = \{(1, 3), (2, 4)\}$.

D $|\mathcal{P}(\{1, 2, 3\})| = 6$.

2. (6 pts) Below we define four functions from $\mathbb{Z}$ to $\mathbb{Z}$. Which of these functions is a one-to-one correspondence?

A $f(n) = 2$ for all $n \in \mathbb{Z}$.

B $g(n) = n + 2$ for all $n \in \mathbb{Z}$.

C $h(n) = 2n$ for all $n \in \mathbb{Z}$.

D $i(n) = n^2$ for all $n \in \mathbb{Z}$.

3. (6 pts) Consider the following binary relation R on the set $\{1, 2, 3\}$:

$$R = \{(1, 1), (1, 2), (2, 2), (3, 2)\}$$

Which of the following statements is **true**?

A R is transitive and antisymmetric.

B R is not transitive and not symmetric.

C R is symmetric and reflexive.

D R is not reflexive and not antisymmetric.

Solution: R is transitive because there are not three distinct elements a, b, c with $a\,R\,b$ and $b\,R\,c$. R is antisymmetric because for all distinct elements a, b with $a\,R\,b$, we do not have $b\,R\,a$. Specifically, we have $1\,R\,2$ and $3\,R\,2$, but we neither have $2\,R\,1$ nor $2\,R\,3$.

4. (6 pts) Let n be an integer such that $n \bmod 11 = 7$. Which of the following statements is **true**?

[A] 7 divides n.

[B] $(2n) \bmod 11 = 14$.

[✔] $(n + 11) \bmod 11 = 7$.

[D] n is odd.

Solution: One possible value for n is 18. That rules out A and D, because 7 does not divide 18, and 18 is not odd. We can also rule out B, because the remainder modulo 11 must be less than 11.

5. (6 pts) You have two fair dice. One die is blue, and the other one is red. You roll both dice simultaneously. Consider the following two events:

- Event A: The blue die comes up ⚁.
- Event B: The red die comes up ⚂ or ⚃.

Which of the following statements is **false**?

[A] $P(A|B) = P(A)$.

[B] $P(B|A) = P(B)$.

[C] $P(A \cap B) = P(A) \cdot P(B)$.

[✔] $P(A|B) = P(B|A)$.

Solution: The two events A and B are independent. Hence, A, B, and C must be true. Moreover, $P(A|B) = 1/6$ and $P(B|A) = 1/3$, so D must be false.

6. (6 pts) A three-digit PIN consists of three digits, each between 0 and 9. The order in which the digits appear matters, e.g. 123 and 321 are two different three-digit PINs. We are interested in three-digit PINs, where a digit appears more than once, e.g. 373 or 000. How many different such PINs are there?

[A] 120

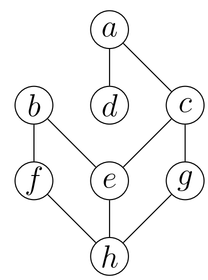
[✔] 280

[C] 720

[D] 840

Solution: There are $10^3 = 1000$ three-digit PINs in total. Out of those $10 \cdot 9 \cdot 8 = 720$ consists of three distinct digits. Hence, there are $1000 - 720 = 280$ three-digit PINs with a repeated digit.

7. (6 pts) Let $(\{a, b, c, d, e, f, g, h\}, \preceq)$ be the partially ordered set defined by the Hasse diagram below. Which of the following statements is **true**?



☑ b is a maximal element.

B $e \preceq d$.

C g and a are incomparable.

D h is the least element.

8. (6 pts) Consider a grammar (V, T, S, P), where $V = \{a, b, S, A, B\}$ and $T = \{a, b\}$. Below are four different choices for the set of productions P of this grammar. Which one results in a grammar that generates the language $\{a^{n+1}b^n \mid n \geq 0\}$?

A $P = \{S \to aA, \quad A \to aAb\}$.

B $P = \{S \to aSb, \quad S \to aS, \quad S \to \lambda\}$.

C $P = \{S \to aAB, \quad A \to \lambda, \quad A \to aA, \quad B \to \lambda, \quad B \to Bb\}$.

☑ $P = \{S \to aB, \quad S \to a, \quad B \to Sb, \quad B \to \lambda\}$.

9. (6 pts) Let S be a set of integers defined recursively as follows:

- I. BASE: $1 \in S$.
- II. RECURSION: If $n \in S$, then $5 - n \in S$.
- III. RESTRICTION: Nothing is in S other than objects defined in I and II above.

Which of the following statements is **true**?

☑ S is finite.

B If n is an integer with $n < 5$, then $n \in S$.

C If n is a positive integer, then $n \in S$.

D If $n \in S$, then n is odd.

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

10. (12 pts) Let the sequence $a_1, a_2, a_3, \ldots$ be given by the following recursive definition

$$\begin{aligned} a_k &= 2a_{k-1} + 3 \qquad \text{for all } k \geq 2 \\ a_1 &= 2 \end{aligned}$$

Prove by mathematical induction that $a_n = 5 \cdot 2^{n-1} - 3$ for all $n \geq 1$.

Solution: We want to prove the statement

$$a_n = 5 \cdot 2^{n-1} - 3 \tag{$P(n)$}$$

for all $n \geq 1$.
Basis step: Let $n = 1$. We have

$$a_1 = 5 \cdot 2^{1+1} - 3 = 5 \cdot 2^0 - 3 = 5 - 3 = 2$$

and, by definition $a_1 = 1$. Hence, the basis step is verified.

Inductive step:
Suppose that $k \geq 1$ and that $P(k)$ holds, that is,

$$a_k = 5 \cdot 2^{k-1} - 3 \tag{inductive hypothesis}$$

We must show that $P(k+1)$ holds, that is,

$$a_{k+1} = 5 \cdot 2^k - 3 \tag{$P(k+1)$}$$

The following calculation shows that $P(k+1)$ holds:

$$\begin{aligned} a_{k+1} &= 2a_k + 3 && \text{(by definition of the sequence)} \\ &= 2(5 \cdot 2^{k-1} - 3) + 3 && \text{(inductive hypothesis)} \\ &= 2 \cdot 5 \cdot 2^{k-1} - 6 + 3 \\ &= 5 \cdot 2 \cdot 2^{k-1} - 3 \\ &= 5 \cdot 2^k - 3 \end{aligned}$$

11. (12 pts) Use the logical equivalences on page 7 to prove the following logical equivalence:

$$(q \wedge {\sim}p) \to {\sim}p \equiv \mathbf{t}$$

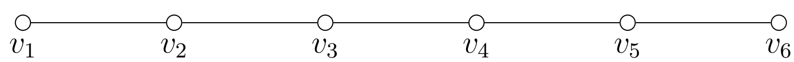
In each step, indicate (by number) which equivalence from page 7 you used.
Solution:

$$\begin{aligned}
& (q \wedge {\sim}p) \to {\sim}p \\
\equiv\ & {\sim}(q \wedge {\sim}p) \vee {\sim}p && (12)\\
\equiv\ & ({\sim}q \vee {\sim}({\sim}p)) \vee {\sim}p && (9)\\
\equiv\ & ({\sim}q \vee p) \vee {\sim}p && (6)\\
\equiv\ & {\sim}q \vee (p \vee {\sim}p) && (2)\\
\equiv\ & {\sim}q \vee \mathbf{t} && (5)\\
\equiv\ & \mathbf{t} && (8)
\end{aligned}$$

12. (12 pts) In the following, you are given two descriptions a graph. For each of these, you are asked whether a graph of that description exists. To answer the question, give either an example of a graph that satisfies the condition, or a reason why no such graph exists. In order to give an example, either draw the corresponding graph or give the triple (V, E, f) of vertices, edges and edge-endpoint function.
Hint: Use the definitions and theorems about graphs and trees on pages 12–14.

(a) A graph with an Euler trail and a total degree of 10.

Solution: Such a graph does exist:



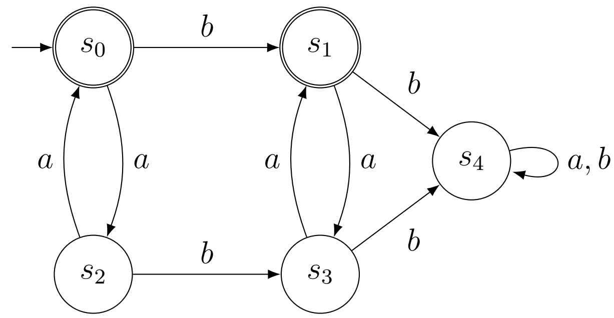
(b) A tree with 7 vertices and each vertex has degree 2.

Solution: No such tree exists. Assume that such a graph G exists. Then according to Theorem 14 G must have 6 edges. In turn, by the Handshake Theorem, this means that G has a total degree of 12. However, each of the 7 vertices of G has a degree of 2, the total degree of G must be $7 \cdot 2 = 14$. This is a contradiction.

13. (10 pts) Construct a finite-state automaton A with input alphabet $\{a, b\}$ that recognises the set of strings that contain an even number of 'a's and at most one 'b'. That is, A must satisfy

$$L(A) = \{w \in \{a, b\}^* \mid |w|_a \text{ even} \wedge |w|_b \leq 1\}$$

For example, A should accept the strings aa and aba, but should not accept the strings $abab$ and ab.
Describe the automaton A using a next-state table *or* a transition diagram.
Solution:



b
b
a
a
a
a
s_0
s_1
s_2
s_3
s_4
a, b
b
b

Definitions and theorems

Logic

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

p	q	$\sim p$	$p \vee q$	$p \wedge q$	$p \to q$	$p \leftrightarrow q$
T	**T**	**F**	**T**	**T**	**T**	**T**
T	**F**	**F**	**T**	**F**	**F**	**F**
F	**T**	**T**	**T**	**F**	**T**	**F**
F	**F**	**T**	**F**	**F**	**T**	**T**

A compound proposition is called a *tautology* if it is always true no matter what the truth values of the propositional variables are. 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.

Given any propositional variables p, q, r, a tautology $\mathbf{t}$ and a contradiction $\mathbf{c}$, the following logical equivalences hold:

1. Commutative laws: $p \wedge q \equiv q \wedge p$ $\quad$ $p \vee q \equiv q \vee p$
2. Associative laws: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $\quad$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$
3. Distributive laws: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $\quad$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4. Identity laws: $p \wedge \mathbf{t} \equiv p$ $\quad$ $p \vee \mathbf{c} \equiv p$
5. Negation laws: $p \vee \sim p \equiv \mathbf{t}$ $\quad$ $p \wedge \sim p \equiv \mathbf{c}$
6. Double negative law: $\sim(\sim p) \equiv p$
7. Idempotent laws: $p \wedge p \equiv p$ $\quad$ $p \vee p \equiv p$
8. Universal bound laws: $p \vee \mathbf{t} \equiv \mathbf{t}$ $\quad$ $p \wedge \mathbf{c} \equiv \mathbf{c}$
9. De Morgan's laws: $\sim(p \wedge q) \equiv \sim p \vee \sim q$ $\quad$ $\sim(p \vee q) \equiv \sim p \wedge \sim q$
10. Absorption laws: $p \vee (p \wedge q) \equiv p$ $\quad$ $p \wedge (p \vee q) \equiv p$
11. Negations of $\mathbf{t}$ & $\mathbf{c}$: $\sim\mathbf{t} \equiv \mathbf{c}$ $\quad$ $\sim\mathbf{c} \equiv \mathbf{t}$
12. Conditional: $\sim p \vee q \equiv p \to q$ $\quad$ $p \to q \equiv \sim q \to \sim p$
13. Biconditional: $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$ $\quad$ $p \leftrightarrow q \equiv \sim p \leftrightarrow \sim q$

Sets

A *set* is an (unordered) collection of objects, called *elements* or *members*. We write $a \in A$ to indicate that a is an *element of* A

A set A is a *subset* of a set B, written $A \subseteq B$, if for all a, $a \in A$ implies $a \in B$.

Two sets A and B are equal if $A \subseteq B$ and $B \subseteq A$.

The *power set* of a set A, denoted $\mathcal{P}(A)$, is the set of all subsets of A. That is, $\mathcal{P}(A) = \{B \mid B \subseteq A\}$.

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 is the set $A - B = \{x \mid x \in A \wedge x \notin B\}$.

The *complement* of a set A is the set $A^c = \{x \in \mathcal{U} \mid x \notin A\}$, where $\mathcal{U}$ is the *universal set*.

The *Cartesian product* of A and B is the set $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$. That is, $A \times B$ is the set of all pairs (a, b) with $a \in A$ and $b \in B$.

Functions

Given two sets A and B, a *function* f from A to B (written $f : A \to B$) is an assignment of exactly one element of B to each element of A.

A function $f : A \to B$ is *onto* 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* if $f(a) = f(b)$ implies $a = b$ for all a and b in the domain of f.

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

Given two functions $g : A \to B$ and $f : B \to C$, the *composition* of f and g (written $f \circ g : A \to C$) is given by

$$(f \circ g)(a) = f(g(a)) \qquad \text{for all } a \in A$$

Let $f : X \to Y$. If $f(x) = y$ we say that y is the *image* of x and x is an *inverse image* (or *preimage*) of y. The *range* (or *image*) of f is the set of all values of f, i.e.

$$\mathsf{range}(f) = \{y \in Y \mid \exists x \in X. f(x) = y\}$$

The *inverse image* of an element $y \in Y$ is the set of all inverse images of y, i.e.

$$\text{inverse image of } y = \{x \in X \mid f(x) = y\}$$

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 binary 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 is called *antisymmetric* if whenever $(a, b) \in R$ and $(b, a) \in R$, then $a = b$, for all $a, b \in A$,.

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 *transitive closure* of a relation R is the smallest transitive relation T such that $R \subseteq T$.

A relation is an *equivalence relation* if it is reflexive, symmetric and transitive.

Let R be an equivalence relation on a set A. The *equivalence class* of $a \in A$ is the set $[a]_R = \{x \in A \mid x \; R \; a\}$.

A relation is a *partial order relation* if it is reflexive, antisymmetric and transitive.

A *partially ordered set* is a pair (A, R) consisting of a set A and a partial order relation R on A.

Elements a and b of a partially ordered set $(A, \preceq)$ are said to be *comparable* if $a \preceq b$ or $b \preceq a$. Otherwise, a and b are said to be *incomparable*.

Let $(A, \preceq)$ be a partially ordered set. An element $a \in A$ is called

- a *greatest element* of A, if $x \preceq a$ for all $x \in A$
- a *least element* of A, if $a \preceq x$ for all $x \in A$
- a *maximal element* of A if, for all $x \in A$, either $x \preceq a$ or a and x are incomparable
- a *minimal element* of A if, for all $x \in A$, either $a \preceq x$ or a and x are incomparable

Number Theory

Given two integers a and b, with $a \neq 0$, we say that a *divides* b (written $a \mid b$) if there exist an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer.

Theorem 1. *Let a, b, and c be any integers.*

1. *If $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.*

2. *If* $a \mid b$ *then* $a \mid bc$.

3. *If* $a \mid b$ *and* $b \mid c$ *then* $a \mid c$.

Theorem 2 (The Quotient/Remainder Theorem)**.** *Given any integer a and a positive integer d, there exist unique integers q and r such that*

$$a = dq + r \qquad \text{and } 0 \leq r < d$$

In Theorem 2 the value d is called the *divisor*, a is the *dividend*, q is the *quotient*, and r is the *remainder*. Then div and mod are defined as a div $d = q$, $a \bmod d = r$. Remember that the remainder cannot be negative.

Let n and m be any integers and d a positive integer. We write $n \equiv m \pmod{d}$ if

$$(n \bmod d) = (m \bmod d)$$

Theorem 3. *Let n and m be any integers and d a positive integer then*

$$n \equiv m \pmod{d} \quad \text{if and only if} \quad d \mid (n - m)$$

Let n be a nonnegative integer and $b_r b_{r-1} ... b_0$ a finite sequence of binary digits, i.e. $b_i \in \{0, 1\}$ for $0 \leq i \leq r$. The sequence $b_r b_{r-1} ... b_0$ is a binary representation of n if

$$n = b_r \cdot 2^r + b_{r-1} 2^{r-1} + ... + b_1 \cdot 2 + b_0$$

For example 101101 is the binary representation of $1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1 = 45$

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 *least common multiple* of two positive integers a and b is denoted by $\text{lcm}(a, b)$ and is the smallest positive integer c such that $a \mid c$ and $b \mid c$.

Theorem 4. *If a and b integer, not both zero, then*

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Counting

The table below states how many different ways there are to order n distinct objects, and how many ways there are to choose r objects out of n distinct objects (depending on whether the order matters or repetition is allowed).

Order n objects (permutation)	$P(n) = n! = n \cdot (n-1) \ldots 2 \cdot 1$	
Choose r objects from n	without repetition	with repetition
- order matters (r-permutation)	$P(n,r) = \frac{n!}{(n-r)!}$	n^r
- order doesn't matter (r-combination)	$\binom{n}{r} = \frac{n!}{r!\,(n-r)!}$	$\binom{n+r-1}{r}$

Theorem 5 (Binomial Theorem)**.** *Given real numbers a and b, and non-negative integer n,*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Let A be a finite set. We write $N(A)$ to denote the number of elements in A. We say A has $N(A)$ elements or A is a set of size $N(A)$

Theorem 6. *If A and B are finite sets, then*

$$N(A \cup B) = N(A) + N(B) - N(A \cap B)$$

Theorem 7 (Difference Rule)**.** *If A is a finite set and B is a subset of A, then*

$$N(A - B) = N(A) - N(B).$$

Probability

A *sample space* is the set of all possible outcomes of a random process or experiment. An *event* is a subset of a sample space. The probability of an event E is denoted $P(E)$. If S is a finite sample space in which all outcomes are equally likely and E is an event in S, then the probability of E is

$$P(E) = \frac{N(E)}{N(S)}$$

Let S be a sample space. A *probability function* P is a function from the set of all events in S to the set of real numbers satisfying

1. $0 \leq P(A) \leq 1$ for all events A in S.
2. $P(\emptyset) = 0$ and $P(S) = 1$.
3. If A and B are disjoint events in S, i.e. $A \cap B = \emptyset$, then $P(A \cup B) = P(A) + P(B)$.

Theorem 8. *If A is any event in a sample space S then the probability of the complement event $A^c = S - A$ is*

$$P(A^c) = 1 - P(A)$$

Theorem 9. *If A and B are events in a sample space S then*

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Suppose the sample space of an experiment or a random process is given by $S = \{a_1, ..., a_n\}$ where a_i is a real number for all $1 \leq i \leq n$. Suppose that each a_i occur with probability p_i for $1 \leq i \leq n$. The *expected value* of the process is

$$\sum_{i=1}^{i=n} a_i p_i = a_1 p_1 + a_2 p_2 + ... + a_n p_n$$

Let A and B be events in a sample space S. If $P(A) \neq 0$, then the *conditional probability of B given A*, denoted $P(B|A)$, is

$$P(B|A) = \frac{P(A \cap B)}{P(A)}$$

Theorem 10 (Bayes' Theorem)**.** *Suppose that a sample space S is the union of mutually disjoint events $B_1, ..., B_n$ where $P(B_i) \neq 0$ for all $1 \leq i \leq n$. Suppose that A is an event in S and that $P(A) \neq 0$. Then*

$$P(B_k|A) = \frac{P(A|B_k)P(B_k)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + ... + P(A|B_n)P(B_n)}$$

Graphs & Trees

A *graph* is a triple (V, E, f) consisting of: a finite, nonempty set V of *vertices*; a finite set E of *edges*; and a function $f : E \to \{\{x, y\} \mid x, y \in V\}$, which assigns one or two *endpoints* to each edge.

An edge with only one endpoint is called a *loop.* Two edges with the same set of endpoints are called *parallel.* Vertices are called *adjacent* if they are endpoints of the same edge (if the edge is a loop, its endpoint is called *adjacent to itself*). We say that an edge is *incident on* its endpoints. Two edges with a common endpoint are called *adjacent.* A vertex on which no edge is incident is called *isolated.*

A graph is called *simple* if it has no loops or parallel edges.

Let G be a graph and v a vertex of G. The *degree of v*, denoted $\deg(v)$, is the number of edges that are incident on v, with an edge that is a loop counted twice. The *total degree of G* is the sum of the degrees of all vertices in G.

Theorem 11 (Handshake Theorem)**.** *A graph with m edges has total degree $2m$.*

A *walk* from v to w is a finite sequence $v_0e_1v_1e_2\ldots v_{n-1}e_nv_n$ such that $v = v_0$, $w = v_n$, and $f(e_i) = \{v_{i-1}, v_i\}$ for all $1 \leq i \leq n$. The table below gives an overview over the different kinds of walks in a graph:

	repeated edge	**repeated vertex**	**same start & end vertex**	**must contain at least 1 edge**
Walk	allowed	allowed	allowed	no
Trail	no	allowed	allowed	no
Path	no	no	no	no
Closed walk	allowed	allowed	yes	no
Circuit	no	allowed	yes	yes
Simple Circuit	no	first and last only	yes	yes

A *subgraph* of G is a graph (V', E', f') with $V' \subseteq V$, $E' \subseteq E$ and $f'(e) = f(e)$ for all $e \in E'$.

A graph (V, E, f) is *connected* if there exists a walk from u to v for all $u, v \in V$. A *connected component* of a graph G is a maximal connected subgraph C of G (i.e. every connected subgraph of G is either a subgraph of C or has no common vertices with C).

An *Euler circuit* of a graph G is a circuit that contains every edge and every vertex of G.

An *Euler trail* of a graph G is a trail that contains every edge and every vertex of G.

Theorem 12. *A graph has an* Euler circuit *if and only if it is connected and every vertex has positive even degree.*

Theorem 13. *Given two distinct vertices u and v in a graph G, there exists an Euler trail from u to v if and only if G is connected, u and v have odd degree, and all other vertices have positive even degree.*

A graph is called *circuit-free* if it has no circuits. A *tree* is a connected and circuit-free graph. In a tree, a vertex is called a *leaf* if it has degree 1, and an *internal vertex* if it has degree 2 or greater. A tree which consists of only one vertex is called *trivial.*

Theorem 14. *Let n be a positive integer. A tree with n vertices has $n - 1$ edges.*

A *rooted tree* is a tree in which one vertex is distinguished from the others and is called the *root.* The *level* of a vertex in a rooted tree is the number of edges on the unique path from that vertex to the root. Given two adjacent vertices v and w such that the level of w is one greater than the level of v, then we call w a *child* of v and v the *parent* of w. In a rooted tree, a vertex with one or more children is called an *internal vertex*, and a vertex with no children is called a *leaf*. A *binary tree* is a rooted tree in which every parent has at most two children. A *full binary tree* is a binary tree in which each parent has *exactly* two children.

Theorem 15. *A full binary tree with n internal vertices has $n + 1$ leaves.*

Automata, Regular Expressions, Grammars

An *alphabet* Σ is a finite set of *symbols*.

A *string* (or *word*) w over Σ is a finite sequence of symbols from Σ.

A *language* A is a set of strings over some Σ.

λ is the *empty string*.

The *length* of w, written $|w|$, is the number of symbols that w contains. We write $|w|_a$ for the number of times the symbol a occurs in w.

Given words $w_1 = a_1 a_2 \ldots a_m$ and $w_2 = b_1 b_2 \ldots b_n$, we write $w_1 w_2$ to mean their *concatenation*: $a_1 a_2 \ldots a_m b_1 b_2 \ldots b_n$.

The concatenation of two languages L_1 and L_2 is defined as the language

$$L_1 L_2 = \{w_1 w_2 \mid w_1 \in L_1 \text{ and } w_2 \in L_2\}$$

The *Kleene closure* of a language L is the language $L^* = \{\lambda\} \cup L \cup LL \cup LLL \cup \ldots$

A *finite-state automaton* is a 5-tuple (S, I, N, s_0, F) consisting of: a finite set of states S; a finite set I (the input alphabet); a transition function $N : S \times I \to S$; an initial state s_0; and a set $F \subseteq S$ of accepting states.

The language accepted by an automaton A is denoted by $L(A)$:

$$L(A) = \{w \mid w \in I^* \text{ and } N^*(s_0, w) \in F\}$$

where $N^* : S \times I^* \to S$ is defined by

$$\begin{aligned} N^*(s, \lambda) &= s \\ N^*(s, aw) &= N^*(s', w) \qquad \text{where } s' = N(s, a) \end{aligned}$$

A *regular expression* r over an alphabet Σ can be built using: $\emptyset$; λ; a symbol $a \in \Sigma$; concatenation $r\,s$ and union $r \,|\, s$ of regular expressions r, s; and Kleene closure r^* of a regular expression r.

The language $L(r)$ defined by a regular expression r is

$$L(\emptyset) = \emptyset \qquad L(a) = \{a\} \qquad L(r \,|\, t) = L(r) \cup L(r)$$
$$L(\lambda) = \{\lambda\} \qquad L(r\,t) = L(r)\,L(r) \qquad L(r^*) = L(r)^*$$

A *grammar* $G = (V, T, S, P)$ consists of: A set of symbols V called *vocabulary*; a set $T \subset V$ of terminal symbols (symbols in $N = V - T$ are called *non-terminal*); a starting symbol $S \in V$; and a set P of productions of the form $z_0 \rightarrow z_1$, where $z_0, z_1 \in V^*$ and z_0 must contain at least one non-terminal symbol.

Given a grammar G and two strings $s, t \in V^*$, we write $s \Rightarrow t$, if s can be rewritten to t by applying one production from P. We write $s \overset{*}{\Rightarrow} t$, and say that t is derivable from s, if s can be rewritten to t by applying several productions from P. The language defined by the grammar G is the set of strings over T derivable from S:

$$L(G) = \left\{ w \mid w \in T^* \text{ and } S \overset{*}{\Rightarrow} w \right\}$$