Notes on Discrete Mathematics

Department of Computer Science
Professor Goldberg

Textbooks:  
Introduction to the Theory of Computation  
by Michael Sipser

Elements of the Theory of Computation  
by H. Lewis and C. Papadimitriou

Discrete Mathematics with Algorithms  
by M. Albertson and J. Hutchinson

These notes contain the material from Discrete Mathematics that you need to know in order to take the course in Computability and Complexity. Try to solve all problems. Most of them are simple; their purpose is just to refresh you memory. If you cannot solve many of them, I would strongly recommend that you take a course in Discrete Mathematics.

1 Logic

Problem 1 Which of the following statements are true?

<table>
<thead>
<tr>
<th>Dogs have wings only if cats have wings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Birds have wings only if cats have wings.</td>
</tr>
<tr>
<td>If dogs have wings, then birds have wings.</td>
</tr>
<tr>
<td>Snakes have legs iff cats have wings.</td>
</tr>
<tr>
<td>If frogs have hair or mice have eyes, then sharks do not have teeth.</td>
</tr>
<tr>
<td>If frogs have hair and mice have eyes, then sharks do not have teeth.</td>
</tr>
</tbody>
</table>
Problem 2 Fill in the truth tables:

<table>
<thead>
<tr>
<th></th>
<th>P ∧ Q</th>
<th>P is true</th>
<th>P is false</th>
<th></th>
<th>P ∨ Q</th>
<th>P is true</th>
<th>P is false</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q is true</td>
<td></td>
<td></td>
<td></td>
<td>Q is true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q is false</td>
<td></td>
<td></td>
<td></td>
<td>Q is false</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>If Q then P</th>
<th>P is true</th>
<th>P is false</th>
<th>true</th>
<th>false</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q is true</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q is false</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Problem 3 Write the truth table for \((p ∧ q) ∨ (q ∨ p)\).

Problem 4 Assuming that \(p\) and \(r\) are false, and that \(q\) and \(s\) are true, find the truth value of the following propositions:

1. \(p → q\);
2. \(\overline{p} → q\);
3. \(\overline{p} → q\);
4. \((p → q) ∧ (q → r)\);
5. \((p → q) → r\);
6. \((p → (q → r))\).

2 Set theory

Definition 1 A set \(A = \{a_0, a_1, \ldots\}\); empty set: \(\emptyset\); \(A\) is a subset of \(B\): \(A ⊆ B\); \(x\) is an element of \(A\): \(x ∈ A\); \(2^A = \{\text{the set of all subsets of } A\}\); Cartesian product of two sets: \(A × B = \{(a, b) : a ∈ A ∧ b ∈ B\}\).
Problem 5 Which of the following statements are true?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$\emptyset \subseteq \emptyset$</td>
<td>✗</td>
</tr>
<tr>
<td>$\emptyset \in \emptyset$</td>
<td>✗</td>
</tr>
<tr>
<td>$\emptyset \subseteq {\emptyset}$</td>
<td>✗</td>
</tr>
<tr>
<td>$\emptyset \in {\emptyset}$</td>
<td>✗</td>
</tr>
<tr>
<td>${a, b} \subseteq {a, b, {a, b}}$</td>
<td>✗</td>
</tr>
<tr>
<td>${a, b} \in {a, b, {a, b}}$</td>
<td>✗</td>
</tr>
<tr>
<td>${a, b} \in 2^{{a, b, {a, b}}}$</td>
<td>✗</td>
</tr>
<tr>
<td>${a, b} \subseteq 2^{{a, b, {a, b}}}$</td>
<td>✗</td>
</tr>
</tbody>
</table>

Problem 6 Prove the following identities.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Idempotency</td>
<td>$A \cup A = A; \ A \cap A = A$</td>
</tr>
<tr>
<td>Commutativity</td>
<td>$A \cup B = B \cup A; \ A \cap B = B \cap A$</td>
</tr>
<tr>
<td>Associativity</td>
<td>$(A \cup B) \cup C = A \cup (B \cup C)$</td>
</tr>
<tr>
<td></td>
<td>$(A \cap B) \cap C = A \cap (B \cap C)$</td>
</tr>
<tr>
<td>Distributivity</td>
<td>$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$</td>
</tr>
<tr>
<td></td>
<td>$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$</td>
</tr>
<tr>
<td>DeMorgan’s Laws</td>
<td>$U - (B \cup C) = (U - B) \cap (U - C)$</td>
</tr>
<tr>
<td></td>
<td>$U - (B \cap C) = (U - B) \cup (U - C)$</td>
</tr>
</tbody>
</table>

Problem 7 If $X = \{1, 2, 3\}$ and $Y = \{a, b\}$, then what are $X \times Y; Y \times X; X \times X; 2^X$?

Definition 2

A partition of a nonempty set $A$ is a subset $\Pi$ of $2^A$ such that $\emptyset$ is not an element of $\Pi$ and each element of $A$ is in one and only one set in $\Pi$.

Problem 8 Rephrase the definition of a partition in a simpler language. Enumerate all partitions of $Y \times Y$ for $Y = \{1, 2\}$. 

3
Problem 9

Let $S = \{1, 2, 3, 4, 5\}$.

(a) What partition of $S$ has the most (the fewest) members?

(b) List all partitions of $S$ with exactly two (three) members.

Definition 3

Binary relation $R$ is a subset of $A \times B$.

Inverse $R^{-1}$ of $R$; if $R$ is a binary relation between $A$ and $B$ then $R^{-1} \subseteq B \times A$; $(b, a) \in R^{-1}$ iff $(a, b) \in R$.

Composition $QR$; if $Q \subseteq A \times C$ and $R \subseteq C \times B$ is defined by $(a, b) \in QR$ iff $(a, c) \in Q$ and $(c, b) \in R$ for some $c \in C$.

Problem 10 Define an $n$-ary relation.

Definition 4 A binary relation $R \subseteq A \times A$ is called

- reflexive if $(a, a) \in R$ for all $a \in A$.
- symmetric if $(a, b) \in R$ whenever $(b, a) \in R$;
- antisymmetric if $(a, b) \in R$ and $(b, a) \in R$, then $a = b$
- transitive if $(a, b)$ and $(b, c)$ imply $(a, c)$;
- equivalence if it is reflexive, symmetric, and transitive.
- partial order if it is reflexive, antisymmetric, and transitive.
- total order if it is a partial order and $\forall a, b$, either $(a, b) \in R$ or $(b, a) \in R$. 
Definition 5

Function from a set $A$ into a set $B$ is a binary relation $R$ on $A$ and $B$ such that for each element $a \in A$, there exists exactly one element $b \in B$ with $(a, b) \in R$.

$f : A \to B$; $A$ is the domain of $f$; $f(A) \subseteq B$ is the range of $f$.

A function is **one-to-one** if for any two distinct elements $a$ and $b$, $f(a) \neq f(b)$.

**onto** if each element of $B$ is the image of an element of $A$ under $f$.

**bijection** between $A$ and $B$, if it is one-to-one and onto $B$.

Definition 6

Let $D$ be a set, $n \geq 0$, and $R \subseteq D^{n+1}$ be an $(n + 1)$-ary relation on $D$. Then $B \subseteq D$ is said to be **closed under** $R$ if

$$\forall b_1, \ldots, b_n \in B, \ (b_1, \ldots, b_n, b_{n+1}) \in R \text{ implies } b_{n+1} \in B.$$ 

Let $D$ be a set, $n \geq 0$, and $f : D^n \to D$. A subset $B \subseteq D$ is **closed under** $f$ if $f(b_1, \ldots, b_n) \in B$ for all $b_1, \ldots, b_n \in B$.

Problem 11 Fix $|D| = 5$. Construct an example of a relation $R \subseteq D^3$ and a subset $B \subset D$ which is closed under $R$.

Problem 12

Is a set closed under a function $f$ also closed under an appropriately defined relation $R$? How to define $R$?

Problem 13

Given a set $A \subseteq D$ and a relation $R$ on $D$, is there a subset $B \subseteq D$ which contains $A$ and is closed under $R$?

Problem 14
Given a set $A \subseteq D$ and a relation $R$ on $D$, is there a subset $B \subseteq D$ which (1) contains $A$; (2) closed under $R$; (3) is minimal in some natural sense?

**Theorem 1**

Let $R$ be a relation on $D$ and let $A \subseteq D$. Then there is a set $B \subseteq D$ such that

- $A \subseteq B$;
- $B$ is closed under $R$;
- for any $C \subseteq D$ satisfying the previous two conditions, $B \subseteq C$.

**Definition 7**

The set $B$ described in the previous theorem is called the *closure* of $A$ under relations $R_1, \ldots, R_n$.

**Reflexive, Transitive Closure of a Binary Relation**

**Definition 8**

Let $A$ be a finite set, $D = A \times A$, and $R \subseteq D$. Let also $Q$ and $Q'$ be a 3-ary and unary relation on $D$, respectively, given by $Q = \{((a, b), (b, c), (a, c)) : a, b, c \in A\}$ and $Q' = \{(a, a) : a \in A\}$. Then the closure of $R$ under $Q$ and $Q'$ is called the reflexive, transitive closure of $R$ and is denoted $R^*$.

**Theorem 2**

The reflexive, transitive closure $R^*$ of a binary relation $R$ is equal to

$$R \cup \{(a, b) : \exists \text{ a chain in } R \text{ from } a \text{ to } b\}.$$  

**Problem 15**

Prove theorem 2.17.
3 Principle of Mathematical Induction

Let $A$ be a set of nonnegative integers such that

1. $0 \in A$;
2. $\forall n \in \mathbb{N}$, if $\{0, \ldots, n\} \subseteq A$, then $n + 1 \in A$.

Then $A = \mathbb{N}$.

---

Applying Mathematical Induction

**The task:** Given property $P = P(n)$, prove that it holds for all integers $n \geq 0$.

**Basis:** show that $P(0)$ is correct;

**Induction hypothesis:** $P$ holds for all integers $0, 1, \ldots, n$

**Induction step:** prove that the induction hypothesis, $P(n)$, implies that $P$ is true of $n + 1$: $P(n) \implies P(n + 1)$

**Conclusion:** using the principle of Mathematical Induction conclude that $P(n)$ is true for arbitrary $n \geq 0$.

**Problem 16** Prove that for all $n > 10$

$$n - 2 < \frac{n^2 - n}{12}.$$

**Proof:** Define property $P(n)$ by

$$P(n) : \forall k \leq n \ (k > 10; \ n > 10), \ k - 2 < \frac{k^2 - k}{12}.$$
Then,

**Basis:** for \( n = 11, \)

\[
11 - 2 < \frac{11^2 - 11}{12} \implies 9 < \frac{110}{12} = \frac{55}{6} = 9 + \frac{1}{6}.
\]

Notice that the base of the induction proof start with \( n = 11, \) rather than with \( n = 0. \) Such a shift happens often, and it does not change the principle, since this is nothing more than the matter of notations. One can define a property \( Q(m) \) by \( Q(m) = P(n - 11), \) and consider \( Q \) for \( m \geq 0. \)

**Induction step.** Suppose, given \( n \geq 11, \) \( P \) holds true for all integers up \( n. \) Then

\[
P(n) \implies n - 2 < \frac{n^2 - n}{12} \implies (n + 1) - 2 - 1 < \frac{(n+1)^2 - (n+1) - 2n - 1 + 1}{12} \implies (n + 1) - 2 < \frac{(n+1)^2 - (n+1) - 2n + 1}{12} \implies (n + 1) - 2 < \frac{(n+1)^2 - (n+1)}{12} \text{ (since } n > 10).\]

The last inequality is \( P(n + 1). \)

**Problem 17** (*Ramsey Theorem*) Let \( G \) be a graph. A **clique** (resp. **independent set**) in \( G \) is a subgraph in which any two vertices are adjacent (respectively, no two are adjacent). Denote \( R(p, q) \) the smallest integer \( N \) such that every graph with \( N \) vertices either contains a clique of size \( p, \) or an independent set of size \( q. \) Prove that

\[
R(p, q) \leq R(p - 1, q) + R(p, q - 1).
\]

Then prove that every graph with \( \binom{2n}{n} \) vertices either contains a clique of size \( n, \) or an independent set of size \( n. \)

**Problem 18** Prove that for all \( n \geq 0 \)

\[
1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{2n} \leq 1 + n.
\]

**Problem 19** A set with an even number of elements is called even. Guess a formula for the number of even subsets of a set with \( n \) elements and prove the formula by induction.
4 Pigeonhole principle

1st form: If \( n \) pigeons fly into \( k \) pigeonholes and \( k < n \), then some pigeonhole contains at least two pigeons.

2nd form: If \( A \) and \( B \) are nonempty finite sets and \( |A| > |B| \), then for any function \( f : A \rightarrow B \), \( \exists a, b \in A \), such that \( f(a) = f(b) \).

3rd form: Let \( f \) be a function from a finite set \( A \) to a finite set \( B \), let \( |A| = n \), \( |B| = m \), and \( k = \lceil n/m \rceil \). If \( k \geq 1 \), then there are at least \( k \) values \( a_1, \ldots, a_k \) such that \( f(a_1) = \ldots = f(a_k) \).

Problem 20 Prove that every sequence of \( n^2 + 1 \) distinct numbers has either an increasing subsequence of length \( n + 1 \) or a decreasing subsequence of length \( n + 1 \).

Proof. Consider an arbitrary sequence \( S = \{a_i\} (i \in [1, n^2 + 1]) \) of distinct numbers and define \( t_i \) to be the length of the longest increasing subsequence starting at \( a_i \).

If no monotone increasing subsequence \( S \) of length \( n + 1 \) exists, then

\[
\forall i = 1, \ldots, n^2 + 1, t_i \leq n.
\]

To use the Pigeonhole Principle, we now define function \( F : [1, n^2 + 1] \rightarrow [1, n] \) by

\[
F(i) = t_i \ (i = 1, 2, \ldots, n^2 + 1).
\]

Since the domain \( A \) of \( F \) is of size \( n^2 + 1 \) and the range \( B \) is of size \( n \), by the Pigeonhole Principle (3rd form) there are at least \( \lceil n^2 + 1/n \rceil = n + 1 \) indices \( i_1, i_2, \ldots, i_{n+1} \) for which \( F \) takes the same value. Let

\[
F(i_1) = F(i_2) = \ldots F(i_{n+1}) = L.
\]

Claim: for every \( j = i_1, i_2, \ldots, i_{n+1}, a_{i_j} > a_{i_{j+1}} \).

Indeed, suppose \( a_{i_j} < a_{i_{j+1}} \) for some \( j \in \{1, 2, \ldots, n + 1\} \). Then every monotone increasing subsequence \( R \) starting with \( a_{i_{j+1}} \) can be included into a longer monotone increasing subsequence starting with \( a_{i_j} \), by simply making \( a_{i_j} \) the first member and appending \( R \) to it. If \( R \) is the longest monotone
increasing subsequence starting at $i_{j+1}$, its length is $L$, which yields a length $L + 1$ monotone increasing subsequence starting at $a_{i_j}$. This contradicts the conclusion from the Pigeonhole Principle, and thus, proves the claim.

Finally, we see that

$$a_{i_1} > a_{i_1} > \ldots > a_{n+1},$$

which proves the theorem.

**Problem 21** Prove that any subset $A$ of a set \{1, 2, 3, \ldots, 2n\} which has at least $n+1$ elements, contains two numbers such that one of them is a multiple of the other.

**Proof.** Define $\text{odd}(x)$ to be the largest odd divisor of $x$. Let $R$ be an equivalence defined by

$$R = \{(a, b) : \text{odd}(a) = \text{odd}(b)\}$$

There are $n$ classes of $R$ in $[1, \ldots, 2n]$ and there are $n + 1$ numbers. By pigeonhole principle, two of the numbers are in the same class; this implies that one of them is a multiple of the other.

5 Strings and languages

**Terminology:**
- alphabet $\Sigma$: a finite set of symbols; binary alphabet: \{0, 1\};
- string over $\Sigma$: a finite sequence of symbols from $\Sigma$;
- empty string $e$: \;
- $\Sigma^*$: the set of all strings over an alphabet $\Sigma$;
- length of a string: the number of symbols in the string;
- occurrences: COMMITTEE;
- position $w(i)$: ranges from 1 to the length of the string;
- substring: COMMITTEE — MIT;
- suffix (prefix): COMMITTEE — TEE (COM);
Operations on strings:

Concatenation: \( \text{MUSH} \circ \text{ROOM} \rightarrow \text{MUSHROOM} \);

concatenation is associative: \( (uv)w = u(vw) \).

Reversal: \( \text{MUSHROOM}^R = \text{MOORHSUM} \);

Statement: For any two strings \( u \) and \( v \), \( (uv)^R = v^R u^R \).

Operations on languages:

Complement \( \overline{A} = \Sigma^* - A \);

Union: \( L \cup M \);

Concatenation: \( LM = \{ w : w = uv; u \in L, v \in M \} \);

\( L^k = LL \ldots L \);

Closure (Kleene star) \( L^* \)

\( L^* = \{ e \} \cup L \cup L^2 \cup \ldots ; \)

\( L^+ = L \cup L^2 \cup \ldots . \)

Problem 22 What is \( \emptyset^* \)?

Problem 23 What is \( (L^*)^* \)?

Problem 24 Is it true that \( L \subseteq M \) implies \( L^* \subseteq M^* \)?

Problem 25 Is it true that \( L \subseteq M \) implies \( L^+ \subseteq M^+ \)?

Problem 26 Prove that \( (w^R)^R = w \)

Problem 27 Prove that if \( v \) is a substring of \( w \), then \( v^R \) is a substring of \( w^R \).
Problem 28 Prove that \((w^R)^R = w\)

Problem 29 Under what circumstances is \(L^+ = L^* - \{e\}\)?
Problem 30 Prove that \( \{a, b\}^* = \{a\}^* \{\{b\} \{a\}^*\}^* \).

Proof. The inclusion

\[
\{a, b\}^* \supseteq \{a^*ba^*\}^*
\]

is obvious since the left part is the set of all strings in \( a \) and \( b \).

The non-trivial part of our task is to prove that

\[
\{a, b\}^* \subseteq a^* \{ba^*\}^*.
\]

The left part of \( B \) consists of all strings in the alphabet \( \{a, b\} \); every such a string can be written as \( a^{p_0}b^{q_0}a^{p_1}b^{q_1} \ldots a^{p_n}b^{q_n-1} \), for \( n \geq 0 \) and non-negative integers \( p_0, q_0, p_1, q_1, \ldots \).

The right part of \( B \) can be re-written as follows:

\[
a^* \{ba^*\}^* = (e \cup a \cup a^2 \ldots) \{e \cup L \cup L^2 \ldots\}^* = \bigcup a^sL^t,
\]

where \( s, t \geq 0 \) are integers and \( L = ba^* = b \cup ba \cup ba^2 \cup \ldots \).

Thus, to prove \( B \), we need to find, for every \( p_0, q_0, p_1, q_1, \ldots \), integers \( s \) and \( t \) such that \( a^sL^t \) contains

\[
a^{p_0}b^{q_0}a^{p_1}b^{q_1} \ldots a^{p_n}b^{q_n-1}.
\]

Claim: \( s = p_0 \); and \( t = q_0 + q_1 + \ldots + q_{n-1} \) are such integers.

\[
a^{p_0}L^{(q_0+q_1+\ldots+q_{n-1})}
\]

\[
= a^{p_0} (b \cup ba \cup ba^2 \ldots) \ldots (b \cup ba \cup ba^2 \ldots) (b \cup ba \cup ba^2 \ldots)
\]

\[
(b \cup ba \cup ba^2 \ldots) \ldots (b \cup ba \cup ba^2 \ldots) (b \cup ba \cup ba^2 \ldots)
\]

\[
(b \cup ba \cup ba^2 \ldots) \ldots (b \cup ba \cup ba^2 \ldots) (b \cup ba \cup ba^2 \ldots).
\]

The first factor gives \( a^{p_0} \); each next \( q_0 - 1 \) factor gives a \( b \); the factor which follows gives \( ba^{p_1} \), and so on: on every line, the factors above the braces give \( b \) each, and the last factor gives the concatenation of \( b \) and \( a \) in the corresponding degree.

\[\square\]
FINITE REPRESENTATION OF LANGUAGES.

THE CENTRAL ISSUE IN THE THEORY OF COMPUTATION IS THE REPRESENTATION OF LANGUAGES BY FINITE SPECIFICATIONS

\[ \cup \text{ the union operation; } \]
\[ \circ \text{ the concatenation operation; } \]
\[ * \text{ the closure operation; } \]

Regular Language (informal definition): any language that can be obtained by a finite application of the three operations above to a given finite set of words.

Regular expression over an alphabet \( \Sigma \) is a string over the alphabet

\[ \Sigma \cup \{\epsilon, \), ( , \emptyset, \cup, * \} \]

such that the following holds

1. \( \emptyset, \epsilon \) and each member of \( \Sigma \) is a regular expression.
2. If \( \alpha \) and \( \beta \) are regular expressions, then so is \( (\alpha \beta) \).
3. If \( \alpha \) and \( \beta \) are regular expressions then so is \( (\alpha \cup \beta) \).
4. If \( \alpha \) is a regular expressions then so is \( \alpha^* \).
5. Only an expression which can be obtained by applying (1) through (4) is regular.

The class of regular languages (sets) over an alphabet \( \Sigma \) is the minimal collection of sets containing \( \emptyset \) and the set \( \{a\} \) for every \( a \in \Sigma \), and closed under the operations of union, concatenation, and Kleene star.

Standard convention. Parentheses in an expression may be omitted.

Problem 31 For each of the sets below, give examples of strings in and not in the sets \( (\Sigma = \{a, b\}) \)
(a) \{w : \text{for some } u \in \Sigma, w = uu^Ru\}

(b) \{w : ww = wwww\}

(c) \{w : \text{for some } u \text{ and } v, uvw = wvu\}

(d) \{w : \text{for some } u, www = uu\}

Problem 32 Rewrite each of the regular expressions as a simpler expression representing the same set.

(a) \emptyset^* \cup a^* \cup b^* \cup (a \cup b)^*

(b) ((a^*b)^*(b^*a)^*)^*

(c) (a^*b)^* \cup (b^*a)^*

(d) (a \cup b)^*a(a \cup b)^*

Problem 33 A regular expression is in disjunctive normal form if it is of the form $(\alpha_1 \cup \alpha_2 \ldots \cup \alpha_n)$ for some $n \geq 0$, where none of the $\alpha_i$ contains an occurrence of $\sqcup$. Show that every regular language is represented by an expression in disjunctive normal form.

6 Principle of Mathematical Induction

Let $A$ be a set of nonnegative integers such that

1. $0 \in A$;
2. $\forall n \in \mathcal{N}$, if $\{0, \ldots, n\} \subseteq A$, then $n + 1 \in A$.

Then $A = \mathcal{N}$.

Applying Mathematical Induction
The task: Given property $P = P(n)$, prove that it holds for all integers $n \geq 0$.

Basis: show that $P(0)$ is correct;

Induction hypothesis: $P$ holds for all integers $0, 1, \ldots, n$

Induction step: prove that the induction hypothesis, $P(n)$, implies that $P$ is true of $n + 1$: $P(n) \implies P(n + 1)$

Conclusion: using the principle of Mathematical Induction conclude that $P(n)$ is true for arbitrary $n \geq 0$.

Problem 34 Prove that for all $n > 10$

$$n - 2 < \frac{n^2 - n}{12}.$$ 

Proof: Define property $P(n)$ by

$$P(n): \forall k \leq n \ (k > 10; \ n > 10), \ k - 2 < \frac{k^2 - k}{12}.$$ 

Then,

Basis: for $n = 11$,

$$11 - 2 < \frac{11^2 - 11}{12} \implies 9 < \frac{110}{12} = \frac{55}{6} = 9 + \frac{1}{6}.$$ 

Notice that the base of the induction proof start with $n = 11$, rather than with $n = 0$. Such a shift happens often, and it does not change the principle, since this is nothing more than the matter of notations. One can define a property $Q(m)$ by $Q(m) = P(n - 11)$, and consider $Q$ for $m \geq 0$.  

16
**Induction step.** Suppose, given $n \geq 11$, $P$ holds true for all integers up $n$. Then

$$
P(n) \implies n - 2 < \frac{n^2 - n}{12}
$$

$$
\implies (n + 1) - 2 - 1 < \frac{(n+1)^2-(n+1)-2n-1+1}{12}
$$

$$
\implies (n + 1) - 2 < \frac{(n+1)^2-(n+1)}{12} - \frac{2n}{12} + 1
$$

$$
\implies (n + 1) - 2 < \frac{(n+1)^2-(n+1)}{12} \quad (\text{since } n > 10)
$$

The last inequality is $P(n + 1)$.

**Problem 35** (Ramsey Theorem) Let $G$ be a graph. A clique (resp. independent set) in $G$ is a subgraph in which any two vertices are adjacent (respectively, no two are adjacent). Denote $R(p, q)$ the smallest integer $N$ such that every graph with $N$ vertices either contains a clique of size $p$, or an independent set of size $q$. Prove that

$$
R(p, q) \leq R(p - 1, q) + R(p, q - 1).
$$

Then prove that every graph with $\binom{2n}{n}$ vertices either contains a clique of size $n$, or an independent set of size $n$.

**Problem 36** Prove that for all $n \geq 0$

$$
1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{2n} \leq 1 + n.
$$

**Problem 37** A set with an even number of elements is called even. Guess a formula for the number of even subsets of a set with $n$ elements and prove the formula by induction.

7 **Pigeonhole principle**

1st form: If $n$ pigeons fly into $k$ pigeonholes and $k < n$, then some pigeonhole contains at least two pigeons.

2nd form: If $A$ and $B$ are nonempty finite sets and $|A| > |B|$, then for any function $f : A \to B$, $\exists a, b \in A$, such that $f(a) = f(b)$.
3rd form: Let \( f \) be a function from a finite set \( A \) to a finite set \( B \), let \( |A| = n \), \( |B| = m \), and \( k = \lceil n/m \rceil \). If \( k \geq 1 \), then there are at least \( k \) values \( a_1, \ldots, a_k \) such that \( f(a_1) = \cdots = f(a_k) \).

Problem 38 Prove that every sequence of \( n^2 + 1 \) distinct numbers has either an increasing subsequence of length \( n+1 \) or a decreasing subsequence of length \( n+1 \).

Proof. Consider an arbitrary sequence \( S = \{a_i\} (i \in [1, n^2 + 1]) \) of distinct numbers and define \( t_i \) to be the length of the longest increasing subsequence starting at \( a_i \).

If no monotone increasing subsequence \( S \) of length \( n+1 \) exists, then

\[
\forall i = 1, \ldots, n^2 + 1, t_i \leq n.
\]

To use the Pigeonhole Principle, we now define function \( F : [1, n^2+1] \to [1, n] \) by

\[
F(i) = t_i \ (i = 1, 2, \ldots, n^2 + 1).
\]

Since the domain \( A \) of \( F \) is of size \( n^2 + 1 \) and the range \( B \) is of size \( n \), by the Pigeonhole Principle (3rd form) there are at least \( \lceil n^2 + 1/n \rceil = n + 1 \) indices \( i_1, i_2, \ldots, i_{n+1} \) for which \( F \) takes the same value. Let

\[
F(i_1) = F(i_2) = \ldots F(i_{n+1}) = L.
\]

Claim: for every \( j = i_1, i_2, \ldots, i_{n+1}, a_{i_j} > a_{i_{j+1}} \).

Indeed, suppose \( a_{i_j} < a_{i_{j+1}} \) for some \( j \in \{1, 2, \ldots, n+1\} \). Then every monotone increasing subsequence \( R \) starting with \( a_{i_{j+1}} \) can be included into a longer monotone increasing subsequence starting with \( a_{i_j} \), by simply making \( a_{i_j} \) the first member and appending \( R \) to it. If \( R \) is the longest monotone increasing subsequence starting at \( i_{j+1} \), its length is \( L \), which yields a length \( L + 1 \) monotone increasing subsequence starting at \( a_{i_j} \). This contradicts the conclusion from the Pigeonhole Principle, and thus, proves the claim.

Finally, we see that

\[
a_{i_1} > a_{i_1} > \ldots > a_{n+1},
\]

which proves the theorem.
**Problem 39** Prove that any subset $A$ of a set \{1, 2, 3, \ldots, 2n\} which has at least $n+1$ elements, contains two numbers such that one of them is a multiple of the other.

**Proof.** Define $\text{odd}(x)$ to be the largest odd divisor of $x$. Let $R$ be an equivalence defined by

$$R = \{(a, b) : \text{odd}(a) = \text{odd}(b)\}.$$  

There are $n$ classes of $R$ in $[1, \ldots, 2n]$ and there are $n + 1$ numbers. By pigeonhole principle, two of the numbers are in the same class; this implies that one of them is a multiple of the other.

### 8 Strings and languages

**Terminology:**

- alphabet $\Sigma$: a finite set of symbols; binary alphabet: \{0,1\};
- string over $\Sigma$: a finite sequence of symbols from $\Sigma$;
- empty string $\epsilon$;
- $\Sigma^*$: the set of all strings over an alphabet $\Sigma$;
- length of a string: the number of symbols in the string;
- occurrences: COMMITTEE;
- position $w(i)$: ranges from 1 to the length of the string;
- substring: COMMITTEE —— MIT;
- suffix (prefix): COMMITTEE —— TEE (COM);

**Operations on strings:**

- Concatenation: $\text{MUSH \circ ROOM} \rightarrow \text{MUSHROOM}$;
  - concatenation is associative: $(uv)w = u(vw)$.
- Reversal: $\text{MUSHROOM}^R = \text{MOORHSUM}$;
- Statement: For any two strings $u$ and $v$, $(uv)^R = v^R u^R$. 

19
Operations on languages:

Complement \( \overline{A} = \Sigma^* - A \);

Union: \( L \cup M \);

Concatenation: \( LM = \{ w : w = uv; u \in L, v \in M \} \);

\( L^k = LL \ldots L \);

Closure (Kleene star) \( L^* \)

\( L^* = \{ e \} \cup L \cup L^2 \cup \ldots \);

\( L^+ = L \cup L^2 \cup \ldots \).

Problem 40 What is \( \emptyset^* \)?

Problem 41 What is \((L^*)^*\)?

Problem 42 Is it true that \( L \subseteq M \) implies \( L^* \subseteq M^* \)?

Problem 43 Is it true that \( L \subseteq M \) implies \( L^+ \subseteq M^+ \)?

Problem 44 Prove that \((w^R)^R = w\)

Problem 45 Prove that if \( v \) is a substring of \( w \), then \( v^R \) is a substring of \( w^R \).

Problem 46 Under what circumstances is \( L^+ = L^* - \{ e \} \)?

Additional Problems in Discrete mathematics.

Problem 47 Let \( A = \{ a_1, a_2, \ldots, a_p \} \) \((p \geq 3)\) and let \( N_k \) denote the number of subsets of \( A \) whose size is \( k \) \((k = 1, 2, \ldots, p)\). Which of the following three statements is correct:

(a) \( N_2 > N_{p-2} \); (b) \( N_2 < N_{p-2} \); (c) \( N_2 = N_{p-2} \)? Explain.
Problem 48 How many eight digit numbers are there that contain a 5 and a 6? Explain.

Problem 49 Prove by induction that

\[ 1 + 5 + \ldots + (4n - 3) = n(2n - 1). \]

Problem 50 Find the smallest value of \( n \) for which

(a) \( 2^{2n} > 1,000,000 \);
(b) \( (n!)! > 1,000,000 \). Explain.

Problem 51 Describe an algorithm which computes \( x^{96} \) using at most seven multiplications.

Problem 52 Determine whether the following is true or false:

(a) \( (n + 1)! = O(n!) \); (b) \( n^3 = O(500n^2) \); Explain.

Problem 53 What are the coefficients of the terms \( \frac{1}{x}, \frac{1}{x^2} \) in the expansion of \( (x + \frac{1}{x})^n \), where \( (n > 2) \)? Explain.

Problem 54 The Euclidean algorithm is based on the theorem stating that the last nonzero remainder produced in the set of Euclidean equations equals \( \gcd(b, c) \). A corollary to this theorem is: if \( g = \gcd(b, c) \), then there are integers \( x \) and \( y \) such that \( g = xb + yc \). Write a formal induction proof of this Corollary.

Problem 55 Find pairs \( (b, c) \) such that \( \gcd(b, c) \) equals (a) \( b/2 \); (b) \( b/3 \).

Problem 56 Let \( a, b, t \) be positive integers. Which of the following statements is correct? Explain.

(a) \( \gcd(a, b) < \gcd(at, bt) \); (b) \( \gcd(a, b) = \gcd(at, bt) \); (c) \( \gcd(a, b) > \gcd(at, bt) \).

Problem 57 Using the Euclidean algorithm, find the greatest common divisor of (1) 1008 and 539; (2) 662 and 414. Show all stages of the algorithm in both cases.
Problem 58 If \(a, b, x, y\) are nonzero integers such that \(ax + by = 3\), is \(\gcd(a, b) = 3\)? Explain.

Problem 59 Prove by induction that

\[
F_1 + F_3 + \ldots + F_{2n-1} = F_{2n},
\]

where \(F_i\) denotes the \(i^{th}\) Fibonacci number.

Problem 60 Suppose that the sequence \(G_i\) is defined by \(G_0 = 0; G_1 = 1; G_n = G_{n-1} + 2G_{n-2}\). Determine which of the following propositions are true:

(a) \(G_n = O(n^2)\)
(b) \(G_n = G_0 + G_1 + \ldots G_{n-1}\)
(c) \(G_n < 2^n\) \((n = 0, 1, \ldots)\)

Problem 61 Let \(\Sigma\) be an alphabet and \(L\) be a language over \(\Sigma\). Prove that if \(L^2 \subseteq L\), then \(L^+ \subseteq L\).

\(L^+ = L \cup L^2 \cup L^3 \cup \ldots\)

Problem 62 Prove that for every integer \(n > 0\), \(5^n - 2^n\) is divisible by 3.

Problem 63 For every integer \(n \geq 0\),

\[
\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.
\]

Prove.

Problem 64 For every integer \(n \geq 0\),

\[
\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}.
\]

Prove.

Problem 65 For any \(n \geq 4\), \(n! > 2^n\).
Problem 66 For any $w \in \{0, 1\}^*$, if $w$ starts with 0 and ends with 1, then it contains a substring 01.

Problem 67 For any integers $a$ and $b$ with $0 \leq a \leq b$, and every integer $n \geq 1$, $b^n - a^n$ is divisible by $b - a$. 
Problem 68 For every integer \( n \geq 1 \),
\[
\sum_{i=1}^{n} \sqrt{i} > 2n\sqrt{n}/3.
\]

Proof. We prove it by induction on \( n \).

Base. For \( n = 1 \), the left part is 1 and the right part is 2/3: \( 1 > 2/3 \).

Inductive step. Suppose the statement is correct for some \( n \geq 1 \); we prove that it is correct for \( n + 1 \). Thus,

Given: \( \sum_{i=1}^{n} \sqrt{i} > 2n\sqrt{n}/3 \); \hspace{1cm} Prove: \( \sum_{i=1}^{n+1} \sqrt{i} > 2(n+1)\sqrt{n+1}/3 \).

Using the given inequality, we evaluate the right part of (1)
\[
\left(\sum_{i=1}^{n} \sqrt{i}\right) + \sqrt{n+1} \geq 2n\sqrt{n}/3 + \sqrt{n+1}.
\]

The following sequence of equivalent inequalities completes the proof:
\[
2n\sqrt{n}/3 + \sqrt{n+1} \geq 2(n+1)\sqrt{n+1}/3 \quad (3)
\]
\[
2n\sqrt{n} + 3\sqrt{n+1} \geq 2(n+1)\sqrt{n+1} \quad (4)
\]
\[
2n\sqrt{n} \geq (2n-1)\sqrt{n+1} \quad (5)
\]
\[
4n^2n \geq (2n-1)^2(n+1) \quad (6)
\]
\[
4n^3 \geq (4n^2 - 4n + 1)(n+1) = 4n^3 - 3n + 1 \quad (7)
\]
\[
0 \geq -3n + 1. \quad (8)
\]
The last inequality holds true for any \( n > 0 \).

Problem 69 Prove that for every \( n \geq 1 \) and every \( m \geq 1 \), the number of functions from \( \{1, 2, \ldots, n\} \) to \( \{1, 2, \ldots, m\} \) is \( m^n \).

Problem 70 The numbers \( a_n \), for \( n \geq 0 \), are defined recursively as follows:
\[
a_0 = -2; \hspace{1cm} a_1 = -2; \hspace{1cm} \text{for } n \geq 2, \hspace{1cm} a_n = 5a_{n-1} - 6a_{n-2}.
\]
Show that for every \( n \geq 0 \), \( a_n = 2 \times 3^n - 4 \times 2^n \).
Problem 71 Let $\Sigma$ be an alphabet. Under what conditions two distinct non-empty strings $x, y$ satisfy $xy = yx$? Either prove it cannot occur, or describe precisely the circumstances under which it can.

Problem 72 For a finite set $S$, $|S|$ denotes the number of elements of $S$. Is it always true that for finite languages $A$ and $B$,

$$|AB| = |A| \times |B|?$$

Either prove it or find a counterexample.

Problem 73 Let $L$ be a language over an alphabet $\Sigma$. Under what circumstances $L^+ = L^*$?

Problem 74 Give an example of two non-empty languages $L_1$ and $L_2$ that satisfy the following two conditions:

1. $L_1 L_2 = L_2 L$, and
2. Neither language is a subset of the other.

Problem 75 Show that for any language $L$, $L^* = (L^+)^* = (L^*)^* = (L^*)^+$. Does $L^+ = L^*$?
9 Order of functions

Notations:

\[ N \] (resp. \( N^+ \)) set of natural (resp. positive natural) numbers;

\[ \mathcal{R} \) (resp. \( \mathcal{R}^+ \)) set of real (resp. positive real) numbers;
Floors and ceilings: \([x]; \lceil x \rceil;\)
Polynomials: \( q_0 + q_1 n + \ldots + q_b n^b; \) exponentials: \( a^n; \)
\[ \lim_{n \to \infty} \frac{n^b}{a^n} = 0; \quad e^x = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \ldots; \]
Logarithms: \( \lg n = \log_2 n, \) (binary logarithm); \( \ln n = \log_e n; \)

Factorials: \( n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n.\)

\[ \sqrt{2\pi n} \left( \frac{n}{e} \right)^n \leq n! \leq \sqrt{2\pi n} \left( \frac{n}{e} \right)^{n+1/12}; \]

\[ n! \approx \sqrt{2\pi n} \left( \frac{n}{e} \right)^n (1 + \Theta(\frac{1}{n})); \]
Fibonacci numbers: \( F_0 = 0; F_1 = 1; F_i = F_{i-1} + F_{i-2}. \)
If \( \phi = \frac{1+\sqrt{5}}{2} \approx 1.61803 \ldots \) and \( \hat{\phi} = \frac{1-\sqrt{5}}{2} \approx -0.61803 \ldots, \) then \( F_i = \frac{\phi^i - \hat{\phi}^i}{\sqrt{5}}. \)

Frequently occurring complexity functions:

\( O(n) \) Linear function; when the size of the input doubles the amount of work doubles;

\( N \log N \) often arises when the algorithm breaks up the problem into small subproblems; when the data doubles, the function more than doubles, but not by much;

\( N^2 \) (resp. \( N^3 \)) Quadratic (resp. Cubic) order; doubling the data size quadruples (resp. increases by a factor of 8) the work;

\( 2^N \) Exponential order assumed to be impractical.
Given two functions $f, g : \mathcal{R}^+ \rightarrow \mathcal{R}^+$

$g = O(f) \equiv \exists C > 0, n_0 > 0$

such that $g(n) \leq Cf(n)$ for all $n > n_0$
Function $g(n)$ does not grow at a faster rate than $f(n)$

$g = \Omega(f) \equiv \exists C > 0, n_0 > 0$

such that $g(n) \geq Cf(n)$ for all $n > n_0$
Function $g(n)$ grows at least as fast as $f(n)$ does

$g = \Theta(f) \equiv (g = O(f)) \& (g = \Omega(f))$
$g(n)$ and $f(n)$ grow at the same rate

$f(n) = o(g(n)) \equiv \forall c > 0, \exists n_1 > 0$

such that $\forall n > n_1, 0 < f(n) < cg(n)$;
equivalently, $\lim_{n \to \infty} \frac{f(n)}{g(n)} = 0$.

$f(n)$ is growing asymptotically slower than $g(n)$.

$g(n) = \omega(f(n))$ iff $f(n) = o(g(n))$.
$g(n)$ is growing asymptotically faster than $f(n)$. 

27
Problem 76

Which of the statements below is correct and which is false?

1. \( n^2 = O(n^3); \)
2. \( n^3 = O(n^2); \)
3. \( 2^{n+3} = O(2^n); \)
4. \( (n + 1)! = O(n!); \)
5. if \( f(n) = O(n) \) then \( [f(n)]^2 = O(n^2); \)
6. if \( f(n) = O(n) \) then \( 2^{f(n)} = O(2^n); \)
7. if \( f(n) = O(g(n)) \) and \( g(n) = O(h(n)) \) then \( f(n) = O(h(n)); \)
8. there are two functions \( f(n) \) and \( g(n) \) such that \( f(n) \neq O(g(n)) \) and \( g(n) \neq O(f(n)). \)
Problem 77

Prove that

1. \( f(n) = \Theta(g(n)) \) and \( g(n) = \Theta(h(n)) \) imply \( f(n) = \Theta(h(n)) \);
2. \( f(n) = \Theta(g(n)) \) and \( g(n) = O(h(n)) \) imply \( f(n) = O(h(n)) \);
3. \( f(n) = \Omega(g(n)) \) and \( g(n) = \Omega(h(n)) \) imply \( f(n) = \Omega(h(n)) \);
4. \( f(n) = o(g(n)) \) and \( g(n) = o(h(n)) \) imply \( f(n) = o(h(n)) \);
5. \( f(n) = \omega(g(n)) \) and \( g(n) = \omega(h(n)) \) imply \( f(n) = \omega(h(n)) \);
6. \( f(n) = O(g(n)) \) iff \( g(n) = \Omega(f(n)) \);
7. \( e^x = 1 + x + \Theta(x^2) \) when \( x \to 0 \);
8. \( (n + a)^b = \Omega(n^b) \) (\( a \) and \( b \) are constants);
9. Is \( 2^{n+1} = O(2^n) \)? Is \( 2^{2n} = O(2^n) \)?
10. \( n! = o(n^n) \); \( n! = \omega(2^n) \); \( \log(n!) = \Omega(n \log n) \).
Problem 78

Prove by induction that $i$th Fibonacci number satisfies the equality

$$F_i = (\phi^i - \overline{\phi}^i)/\sqrt{5},$$

where $\phi = \frac{1+\sqrt{5}}{2}$ (the golden ratio) and $\overline{\phi} = \frac{1-\sqrt{5}}{2}$ (the conjugate) of $\phi$.

Problem 79

Prove by induction that $\forall i > 0$, $F_i \leq \phi^i$.

Problem 80

Show that quicksort’s best running time is $\Theta(n \log n)$.

Problem 81

Construct a linear algorithm for sorting $n$ non-negative integers of size $\leq Cn$ for some constant $C$. 