Identity Matrices

The identity matrix of order $n$ is the $n \times n$ matrix $I_n = [\delta_{ij}]$, where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$:

$$
A = \begin{bmatrix}
1 & 0 & \ldots & 0 \\
0 & 1 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & 1
\end{bmatrix}
$$

Multiplying an $m \times n$ matrix $A$ by an identity matrix of appropriate size does not change this matrix:

$A I_n = I_m A = A$

Powers and Transposes of Matrices

The power function can be defined for square matrices. If $A$ is an $n \times n$ matrix, we have:

$$
A^0 = I_n, \\
A^r = AAA\ldots A \text{ (r times the letter } A)$$

The transpose of an $m \times n$ matrix $A = [a_{ij}]$, denoted by $A^t$, is the $n \times m$ matrix obtained by interchanging the rows and columns of $A$.

In other words, if $A^t = [b_{ij}]$, then $b_{ij} = a_{ji}$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$.

Zero-One Matrices

A matrix with entries that are either 0 or 1 is called a zero-one matrix. Zero-one matrices are often used like a “table” to represent discrete structures.

We can define Boolean operations on the entries in zero-one matrices:

$$
\begin{array}{c|c|c}
 & a & b \\
\hline
a \land b & 0 & 0 \\
0 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 1
\end{array} \quad \begin{array}{c|c|c}
 & a \lor b & a \land b \\
\hline
0 & 0 & 0 \\
0 & 1 & 0 \\
1 & 0 & 1 \\
1 & 1 & 1
\end{array}
$$

Example:

$$
A = \begin{bmatrix} 2 & 1 \\ 0 & -1 \\ 3 & 4 \end{bmatrix}, \quad A^t = \begin{bmatrix} 2 & 0 & 3 \\ -1 & 1 & 4 \end{bmatrix}
$$

A square matrix $A$ is called symmetric if $A = A^t$.

Thus $A = [a_{ij}]$ is symmetric if $a_{ij} = a_{ji}$ for all $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, n$.

$$
A = \begin{bmatrix} 5 & 1 & 3 \\ 1 & 2 & -9 \\ 3 & -9 & 4 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 3 & 1 \\ 1 & 3 & 1 \end{bmatrix}
$$

A is symmetric, $B$ is not.
Zero-One Matrices

Let $A = [a_{ij}]$ be an $m \times k$ zero-one matrix and $B = [b_{ij}]$ be a $k \times n$ zero-one matrix.

Then the **Boolean product** of $A$ and $B$, denoted by $A \odot B$, is the $m \times n$ matrix with $(i,j)$th entry $c_{ij}$, where

$$c_{ij} = (a_{i1} \land b_{1j}) \lor (a_{i2} \land b_{2j}) \lor \ldots \lor (a_{ik} \land b_{kj}).$$

Note that the actual Boolean product symbol has a dot in its center.

Basically, Boolean multiplication works like the multiplication of matrices, but with computing $\land$ instead of the product and $\lor$ instead of the sum.

**Example:**

\[
A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}
\]

\[
A \odot B = \begin{bmatrix} (1 \land 0) \lor (0 \land 0) & (1 \land 0) \lor (0 \land 1) \\ (1 \land 0) \lor (1 \land 0) & (1 \land 0) \lor (1 \land 1) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}
\]

---

**Mathematical Reasoning**

We need mathematical reasoning to

- determine whether a mathematical argument is correct or incorrect and
- construct mathematical arguments.

Mathematical reasoning is not only important for conducting proofs and program verification, but also for artificial intelligence systems (drawing inferences).

**Terminology**

An **axiom** is a basic assumption about mathematical structures that needs no proof.

We can use a **proof** to demonstrate that a particular statement is true. A proof consists of a sequence of statements that form an argument.

The steps that connect the statements in such a sequence are the **rules of inference**.

Cases of incorrect reasoning are called **fallacies**.

A **theorem** is a statement that can be shown to be true.
Terminology

A **lemma** is a simple theorem used as an intermediate result in the proof of another theorem.

A **corollary** is a proposition that follows directly from a theorem that has been proved.

A **conjecture** is a statement whose truth value is unknown. Once it is proven, it becomes a theorem.

Rules of Inference

**Rules of inference** provide the justification of the steps used in a proof.

One important rule is called **modus ponens** or the **law of detachment**. It is based on the tautology $(p \rightarrow (p \rightarrow q)) \rightarrow q$. We write it in the following way:

\[
p \\
\rightarrow \ (p \rightarrow q) \\
\therefore q
\]

The two hypotheses $p$ and $p \rightarrow q$ are written in a column, and the conclusion below a bar, where $\therefore$ means “therefore”.

### Rules of Inference

- **Addition**: $p$ and $q$ are both true, then their disjunction $p \lor q$ is true.
- **Simplification**: If $p \land q$ is true, then $p$ is true.
- **Conjunction**: If $p$ is true, then $p \land q$ is true.
- **Modus tollens**: If $p \rightarrow q$ is true, and $q$ is false, then $p$ must be false.
- **Hypothetical syllogism**: If $p \rightarrow q$ and $q \rightarrow r$ are true, then $p \rightarrow r$ is true.
- **Disjunctive syllogism**: If $p \lor q$ is true and $p$ is false, then $q$ must be true.

Arguments

Just like a rule of inference, an **argument** consists of one or more hypotheses and a conclusion.

We say that an argument is **valid**, if whenever all its hypotheses are true, its conclusion is also true.

However, if any hypothesis is false, even a valid argument can lead to an incorrect conclusion.

Example:

“If 101 is divisible by 3, then 101² is divisible by 9. 101 is divisible by 3. Consequently, 101² is divisible by 9.”

Although the argument is **valid**, its conclusion is **incorrect**, because one of the hypotheses is false (“101 is divisible by 3”).

If in the above argument we replace 101 with 102, we could correctly conclude that 102² is divisible by 9.
Arguments
Which rule of inference was used in the last argument?

p: “101 is divisible by 3.”
q: “101^2 is divisible by 9.”

\[ p \rightarrow q \]

\[ \therefore q \]

Unfortunately, one of the hypotheses (p) is false. Therefore, the conclusion q is incorrect.

Arguments
Another example:

“If it rains today, then we will not have a barbeque today. If we do not have a barbeque today, then we will have a barbeque tomorrow. Therefore, if it rains today, then we will have a barbeque tomorrow.”

This is a valid argument: If its hypotheses are true, then its conclusion is also true.

Arguments
Let us formalize the previous argument:

p: “It is raining today.”
q: “We will not have a barbecue today.”
r: “We will have a barbecue tomorrow.”

So the argument is of the following form:

\[ p \rightarrow q \]

\[ q \rightarrow r \]

\[ \therefore p \rightarrow r \]

Arguments
Another example:

Gary is either intelligent or a good actor.
If Gary is intelligent, then he can count from 1 to 10.
Gary can only count from 1 to 2.
Therefore, Gary is a good actor.

i: “Gary is intelligent.”
a: “Gary is a good actor.”
c: “Gary can count from 1 to 10.”

Step 1: \( \neg c \) Hypothesis
Step 2: \( i \rightarrow c \) Hypothesis
Step 3: \( \neg i \) Modus Tollens Steps 1 & 2
Step 4: \( a \lor i \) Hypothesis
Step 5: \( a \) Disjunctive Syllogism Steps 3 & 4

Conclusion: a (“Gary is a good actor.”)

Arguments
Yet another example:

If you listen to me, you will pass CS 320L.
You passed CS 320L.
Therefore, you have listened to me.

Is this argument valid?

No, it assumes \(((p \rightarrow q) \land q) \rightarrow p\).
This statement is not a tautology. It is false if p is false and q is true.
To understand certain forms of arguments, we need some...

**Predicate Calculus**

**Universal Quantification**

Let $P(x)$ be a propositional function.

**Universally quantified sentence:**
For all $x$ in the universe of discourse $P(x)$ is true.

Using the universal quantifier $\forall$:

$\forall x \ P(x)$ “for all $x$ $P(x)$” or “for every $x$ $P(x)$”

(Note: $\forall x \ P(x)$ is either true or false, so it is a proposition, not a propositional function.)

**Example:**

$S(x)$: $x$ is a UMB student.

$G(x)$: $x$ is a genius.

What does $\forall x \ (S(x) \rightarrow G(x))$ mean?

“If $x$ is a UMB student, then $x$ is a genius.”

or

“All UMB students are geniuses.”

**Existential Quantification**

**Existentially quantified sentence:**
There exists an $x$ in the universe of discourse for which $P(x)$ is true.

Using the existential quantifier $\exists$:

$\exists x \ P(x)$ “There is an $x$ such that $P(x)$.”

“$x$ is at least one $x$ such that $P(x)$.”

(Note: $\exists x \ P(x)$ is either true or false, so it is a proposition, but no propositional function.)

**Example:**

$P(x)$: $x$ is a UMB professor.

$G(x)$: $x$ is a genius.

What does $\exists x \ (P(x) \land G(x))$ mean?

“There is an $x$ such that $x$ is a UMB professor and $x$ is a genius.”

or

“At least one UMB professor is a genius.”

**Quantification**

Another example:

Let the universe of discourse be the real numbers.

What does $\forall x \exists y \ (x + y = 320)$ mean?

“For every $x$ there exists a $y$ so that $x + y = 320$.”

Is it true? yes

Is it true for the natural numbers? no
Negation

\neg (\forall x \ P(x)) \text{ is logically equivalent to } \exists x \ (\neg P(x)).

\neg (\exists x \ P(x)) \text{ is logically equivalent to } \forall x \ (\neg P(x)).

Quantification

Introducing the universal quantifier \( \forall \) and the existential quantifier \( \exists \) facilitates the translation of world knowledge into predicate calculus.

Examples:

Paul beats up all professors who fail him.

\forall x (\text{Professor}(x) \land \text{Fails}(x, \text{Paul}) \rightarrow \text{BeatsUp}(\text{Paul}, x))

All computer scientists are either rich or crazy, but not both.

\forall x (\text{CS}(x) \rightarrow [\text{Rich}(x) \land \neg \text{Crazy}(x)] \lor [\neg \text{Rich}(x) \land \text{Crazy}(x)])

Or, using XOR:

\forall x (\text{CS}(x) \rightarrow [\text{Rich}(x) \oplus \text{Crazy}(x)])