Identity Matrices

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

$$A = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

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

$AI_n = I_mA = A$

Powers and Transposes of Matrices

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

$A^0 = I_n$,
$A^r = AAA\dots A$ (r times the letter A)

The **transpose** of an m×n matrix $A = [a_{ij}]$, denoted by A^t, is the n×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, …, n and j = 1, 2, …, m.

Powers and Transposes of Matrices

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

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, …, n and j = 1, 2, …, n.

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

A is symmetric, B is not.

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:

a	b	a∧b
0	0	0
0	1	0
1	0	0
1	1	1

a	b	a∨b
0	0	0
0	1	1
1	0	1
1	1	1

Zero-One Matrices

Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be m×n zero-one matrices.

Then the **join** of A and B is the zero-one matrix with (i, j)th entry $a_{ij} \vee b_{ij}$. The join of A and B is denoted by $A \vee B$.

The **meet** of A and B is the zero-one matrix with (i, j)th entry $a_{ij} \wedge b_{ij}$. The meet of A and B is denoted by $A \wedge B$.

Zero-One Matrices

Example: $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$ $B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 0 \end{bmatrix}$

Join: $$A \vee B = \begin{bmatrix} 1\vee 0 & 1\vee 1 \\ 0\vee 1 & 1\vee 1 \\ 1\vee 0 & 0\vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Meet: $$A \wedge B = \begin{bmatrix} 1\wedge 0 & 1\wedge 1 \\ 0\wedge 1 & 1\wedge 1 \\ 1\wedge 0 & 0\wedge 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$$

Zero-One Matrices

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

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

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

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 ∧ instead of the product and ∨ instead of the sum.

Zero-One Matrices

Example:

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

$$A \circ B = \begin{bmatrix} (1 \wedge 0) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) \\ (1 \wedge 0) \vee (1 \wedge 0) & (1 \wedge 1) \vee (1 \wedge 1) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

Zero-One Matrices

Let A be a square zero-one matrix and r be a positive integer.

The **r-th Boolean power** of A is the Boolean product of r factors of A. The r-th Boolean power of A is denoted by $A^{[r]}$.

$A^{[0]} = I_n$,
$A^{[r]}$ = A∘A∘…∘A (r times the letter A)

Let's proceed to…

Mathematical Reasoning

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 $(p \wedge (p \rightarrow q)) \rightarrow q$. We write it in the following way:

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

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

The general form of a rule of inference is:

$$\begin{array}{l} p_1 \\ p_2 \\ \vdots \\ p_n \\ \hline \therefore q \end{array}$$

The rule states that if p_1 **and** p_2 **and** … **and** p_n are all true, then q is true as well.

These rules of inference can be used in any mathematical argument and do not require any proof.

Rules of Inference

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

$$\begin{array}{l} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$$ Modus tollens

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

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$$ Hypothetical syllogism

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

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

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.

Arguments

Example:

"If 101 is divisible by 3, then 101^2 is divisible by 9. 101 is divisible by 3. Consequently, 101^2 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 102^2 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."

$$\begin{array}{l} p \\ p \to q \\ \hline \therefore q \end{array} \quad \text{Modus ponens}$$

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:

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array} \quad \text{Hypothetical syllogism}$$

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."

Arguments

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:	$i \to c$	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 $((p \to q) \land q) \to p$.

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 ∀:
∀x P(x) "for all x P(x)" or "for every x P(x)"

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

Universal Quantification

Example:
S(x): x is a UMB student.
G(x): x is a genius.

What does ∀x (S(x) → 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 ∃:
∃x P(x) "There is an x such that P(x)."
"There is at least one x such that P(x)."

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

Existential Quantification

Example:
P(x): x is a UMB professor.
G(x): x is a genius.

What does ∃x (P(x) ∧ 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 ∀x∃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

¬(∀x P(x)) is logically equivalent to ∃x (¬P(x)).

¬(∃x P(x)) is logically equivalent to ∀x (¬P(x)).

Quantification

Introducing the **universal quantifier** ∀ and the **existential quantifier** ∃ facilitates the translation of world knowledge into predicate calculus.

Examples:

Paul beats up all professors who fail him.
∀x([Professor(x) ∧ Fails(x, Paul)] → BeatsUp(Paul, x))

All computer scientists are either rich or crazy, but not both.
∀x (CS(x) → [Rich(x) ∧ ¬Crazy(x)] ∨ [¬Rich(x) ∧ Crazy(x)])

Or, using XOR:
∀x (CS(x) → [Rich(x) ⊕ Crazy(x)])