Lecture 4 recap: Graphs

- Basic definitions: Degree, (Simple, closed) paths, cycles
- Trees, Complete \((k\text{-partite})\) graphs: \(K_n\), \(K_{m,n}\), \(K_{m,n,p}\), ...
- Eulerian paths and circuits
- Hamiltonian paths and circuits
- Graph colouring, chromatic number \(\chi(G)\)
- Cliques, clique number \(\kappa(G)\)
- Planarity

Example: Planar

Example: Clique number \(\kappa(G) = 4\)
Example: Chromatic number $\chi(G) = 4$

Overview

- what’s a proof?
- from English to propositional logic
- truth tables, validity, satisfiability and entailment
- *applications*: program logic, constraint satisfaction problems, reasoning about specifications, digital circuits
- proof methods
- generalisation: Boolean algebras

Proofs

A **mathematical proof** of a proposition $p$ is a chain of logical deductions leading to $p$ from a base set of axioms.

**Example**

**Proposition**: Every group of 6 people includes a group of 3 who each have met each other or a group of 3 who have not met a single other person in that group.

**Proof**: by case analysis.

But what are propositions, logical deductions, and axioms? And what is a sound case analysis?
The Real World vs Symbols

symbols ← symbolic manipulation → symbols

relationship ← physical operation → relationship

world ← world

NB

“Essentially, all models are wrong. But some are useful.” (G. Box)

The main relationship between symbols and the world of concern in logic is that of a sentence of a language being true in the world. A sentence of a natural language (like English, Cantonese, Warlpiri) is declarative, or a proposition, if it can be meaningfully be said to be either true or false.

Examples

- Richard Nixon was president of Ecuador.
- A square root of 16 is 4.
- Euclid’s program gets stuck in an infinite loop if you input 0.
- Whatever list of numbers you give as input to this program, it outputs the same list but in increasing order.
- $x^n + y^n = z^n$ has no nontrivial integer solutions for $n > 2$.
- 3 divides 24.
- $K_5$ is planar.

The following are not declarative sentences:

- Gubble gimble goo
- For Pete’s sake, take out the garbage!
- Did you watch MediaWatch last week?
- Please waive the prerequisites for this subject for me.
- $x$ divides $y$. — $R(x, y)$
- $x = 3$ and $x$ divides 24. — $P(x)$

The following are not declarative sentences:

- Gubble gimble goo
- For Pete’s sake, take out the garbage!
- Did you watch MediaWatch last week?
- Please waive the prerequisites for this subject for me.
- $x$ divides $y$. — $R(x, y)$
- $x = 3$ and $x$ divides 24. — $P(x)$
Declarative sentences in natural languages can be **compound** sentences, built out of other sentences. *Propositional Logic* is a formal representation of some constructions for which the truth value of the compound sentence can be determined from the truth value of its components.

- Chef is a bit of a Romeo and Kenny is always getting killed.
- Either Bill is a liar or Hillary is innocent of Whitewater.
- It is not the case that this program always halts.

Not all constructions of natural language are truth-functional:

- *Obama believes that* Iran is developing nukes.
- *Chef said* they killed Kenny.
- This program always halts *because* it contains no loops.
- The disk crashed *after* I saved my file.

**NB**

Various **modal logics** extend classical propositional logic to represent, and reason about, these and other constructions.

### The Three Basic Connectives of Propositional Logic

<table>
<thead>
<tr>
<th>symbol</th>
<th>text</th>
</tr>
</thead>
<tbody>
<tr>
<td>∧</td>
<td>“and”, “but”, “,”, “;”</td>
</tr>
<tr>
<td>∨</td>
<td>“or”, “either . . . or . . .”</td>
</tr>
<tr>
<td>¬</td>
<td>“not”, “it is not the case that”</td>
</tr>
</tbody>
</table>

**Truth tables:**

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A ∧ B</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A ∨ B</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>¬A</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
</tr>
</tbody>
</table>

### Applications I: Program Logic

**Example**

if \(x > 0 \text{ or } (x \leq 0 \text{ and } y > 100)\):

Let \(p \overset{\text{def}}{=} (x > 0)\) and \(q \overset{\text{def}}{=} (y > 100)\)

\(p \lor (\neg p \land q)\)

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>¬p</th>
<th>¬p ∧ q</th>
<th>p ∨ (¬p ∧ q)</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

This is equivalent to \(p \lor q\). Hence the code can be simplified to

\(\text{if } x > 0 \text{ or } y > 100:\)
Somewhat more controversially, consider the following constructions:
- if $A$ then $B$
- $A$ only if $B$
- $B$ if $A$
- $A$ implies $B$
- it follows from $A$ that $B$
- whenever $A$, $B$
- $A$ is a sufficient condition for $B$
- $B$ is a necessary condition for $A$

Each has the property that if the whole statement is true, and $A$ is true, then $B$ is true.

We can *approximate* the English meaning of these by “not ( $A$ and not $B$ )”, written $A \rightarrow B$, which has the following truth table:

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$A \rightarrow B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
</tbody>
</table>

How to interpret $A \rightarrow B$ when $A$ is false?

E.g. “If I am the president of Australia, then I have blue eyes”

“All presidents of Australia have blue eyes” vs. “All presidents of Australia do not have blue eyes”

“If false then true” and “If false then false” are vacuously true
How to interpret $A \rightarrow B$ when $A$ is false?

E.g. “If I am the president of Australia, then I have blue eyes”

“All presidents of Australia have blue eyes” vs. “All presidents of Australia do not have blue eyes”

“If false then true” and “If false then false” are vacuously true

We can approximate the English meaning of these by “not ( A and not B)”, written $A \rightarrow B$, which has the following truth table:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>$A \rightarrow B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

While only an approximation to the English, 100+ years of experience have shown this to be adequate for capturing mathematical reasoning.

(Moral: mathematical reasoning does not need all the features of English.)

Examples

LLM: Problem 3.2

Let $p = “you get an HD on your final exam”$,
$q = “you do every exercise in the book”$,
$r = “you get an HD in the course”$.

Translate into logical notation:

(a) You get an HD in the course although you do not do every exercise in the book.
   $r \land \neg q$

(c) To get an HD in the course, you must get an HD on the exam.
   $r \rightarrow p$

(d) You get an HD on your exam, but you don’t do every exercise in this book; nevertheless, you get an HD in this course.
   $p \land \neg q \land r$
Unless

A unless B can be approximated as $\neg B \rightarrow A$

E.g.

I go swimming unless it rains = If it is not raining I go swimming.

Correctness of the translation is perhaps easier to see in:

I don’t go swimming unless the sun shines = If the sun does not shine then I don’t go swimming.

Note that “I go swimming unless it rains, but sometimes I swim even though it is raining” makes sense, so the translation of “A unless B” should not imply $B \rightarrow \neg A$.

Propositional Logic as a Formal Language

Let $Prop = \{p, q, r, \ldots\}$ be a set of basic propositional letters.
Consider the alphabet

$$\Sigma = Prop \cup \{\top, \bot, \neg, \land, \lor, \rightarrow, \leftrightarrow, (, )\}$$

The set of formulae of propositional logic is the smallest set of words over $\Sigma$ such that

- $\top$, $\bot$, and all elements of $Prop$ are formulae
- If $\phi$ is a formula, then so is $\neg \phi$
- If $\phi$ and $\psi$ are formulae, then so are $(\phi \land \psi)$, $(\phi \lor \psi)$, $(\phi \rightarrow \psi)$, and $(\phi \leftrightarrow \psi)$.

Convention: we often drop parentheses when there is no ambiguity.

$\neg$ binds more tightly than $\land$ and $\lor$, which in turn bind more tightly than $\rightarrow$ and $\leftrightarrow$.

Just in case

A just in case B usually means A if, and only if, B; written $A \leftrightarrow B$

The program terminates just in case the input is a positive number.

= The program terminates if, and only if, the input is positive.

I will have an entree just in case I won’t have desert.

= If I have desert I will not have an entree and vice versa.

It has the following truth table:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A $\leftrightarrow$ B</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

Same as $(A \rightarrow B) \land (B \rightarrow A)$

Logical Equivalence

Two formulas $\phi, \psi$ are logically equivalent, denoted $\phi \equiv \psi$ if they have the same truth value for all values of their basic propositions.

Application: If $\phi$ and $\psi$ are two formulae such that $\phi \equiv \psi$, then the digital circuits corresponding to $\phi$ and $\psi$ compute the same function. Thus, proving equivalence of formulas can be used to optimise circuits.
Some Well-Known Equivalences

Excluded Middle  \( p \lor \neg p \equiv \top \)
Contradiction       \( p \land \neg p \equiv \bot \)
Identity          \( p \lor \bot \equiv p \)
                    \( p \land \top \equiv p \)
                    \( p \lor \top \equiv \top \)
                    \( p \land \bot \equiv \bot \)
Idempotence        \( p \lor p \equiv p \)
                    \( p \land p \equiv p \)
Double Negation    \( \neg \neg p \equiv p \)
Commutativity      \( p \lor q \equiv q \lor p \)
                    \( p \land q \equiv q \land p \)

Example
((r \land \neg p) \lor (r \land q)) \lor ((\neg r \land \neg p) \lor (\neg r \land q))
≡ (r \land (\neg p \lor q)) \lor (\neg r \land (\neg p \lor q)) \quad \text{Distrib.}
≡ (r \lor \neg r) \land (\neg p \lor q) \quad \text{Distrib.}
≡ \top \land (\neg p \lor q) \quad \text{Excl. Mid.}
≡ \neg p \lor q \quad \text{Ident.}

Examples
2.2.18 Prove or disprove:
(a) \( p \rightarrow (q \rightarrow r) \equiv (p \rightarrow q) \rightarrow (p \rightarrow r) \)
(c) \( (p \rightarrow q) \rightarrow r \equiv p \rightarrow (q \rightarrow r) \)
Examples

2.2.18 Prove or disprove:
(a) \((p \rightarrow q) \rightarrow (p \rightarrow r)\)
\equiv \neg(p \rightarrow q) \lor \neg p \lor r 
\equiv (p \lor \neg q) \lor \neg p \lor r 
\equiv (p \lor \neg p \lor q) \land (\neg q \lor \neg p \lor r) 
\equiv T \land (\neg p \lor \neg q \lor r) 
\equiv p \lor (\neg q \lor r) 
\equiv p \rightarrow (\neg q \lor r) 
\equiv p \rightarrow (q \rightarrow r) 

(c) \((p \rightarrow q) \rightarrow r \equiv p \rightarrow (q \rightarrow r)\)

Counterexample:

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>r</th>
<th>(p \rightarrow q) \rightarrow r</th>
<th>p \rightarrow (q \rightarrow r)</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Satisfiability of Formulas

A formula is **satisfiable**, if it evaluates to T for some assignment of truth values to its basic propositions.

Example

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>\neg(A \rightarrow B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
</tbody>
</table>

Applications II: Constraint Satisfaction Problems

These are problems such as timetabling, activity planning, etc. Many can be understood as showing that a formula is satisfiable.

Example

You are planning a party, but your friends are a bit touchy about who will be there.
1. If John comes, he will get very hostile if Sarah is there.
2. Sarah will only come if Kim will be there also.
3. Kim says she will not come unless John does.

Who can you invite without making someone unhappy?

Translation to logic: let \(J, S, K\) represent “John (Sarah, Kim) comes to the party”. Then the constraints are:

\[ J \rightarrow \neg S \]
\[ S \rightarrow K \]
\[ K \rightarrow J \]

Thus, for a successful party to be possible, we want the formula \(\phi = (J \rightarrow \neg S) \land (S \rightarrow K) \land (K \rightarrow J)\) to be satisfiable.

Truth values for \(J, S, K\) making this true are called **satisfying assignments**, or **models**.
We figure out where the conjuncts are false, below. (so blank = T)

<table>
<thead>
<tr>
<th>J</th>
<th>K</th>
<th>S</th>
<th>J → ¬S</th>
<th>S → K</th>
<th>K → J</th>
<th>ϕ</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td></td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Conclusion: a party satisfying the constraints can be held. Invite nobody, or invite John only, or invite Kim and John.

---

**Exercise**

2.7.14 (supp)

Which of the following formulae are *always* true?

(a) \((p \land (p \rightarrow q)) \rightarrow q\) — always true

(b) \(((p \lor q) \land \neg p) \rightarrow \neg q\) — not always true

(e) \(((p \rightarrow q) \lor (q \rightarrow r)) \rightarrow (p \rightarrow r)\) — not always true

(f) \((p \land q) \rightarrow q\) — always true

---

**Validity, Entailment, Arguments**

An *argument* consists of a set of declarative sentences called *premises* and a declarative sentence called the *conclusion*.

**Example**

Premises: Frank took the Ford or the Toyota.  
If Frank took the Ford he will be late.  
Frank is not late.

Conclusion: Frank took the Toyota
An argument is **valid** if the conclusions are true whenever all the premises are true. Thus: if we believe the premises, we should also believe the conclusion.
(Note: we don’t care what happens when one of the premises is false.)

Other ways of saying the same thing:
- The conclusion **logically follows** from the premises.
- The conclusion is a **logical consequence** of the premises.
- The premises **entail** the conclusion.

The argument above is valid. The following is invalid:

**Example**

**Premises:** Frank took the Ford or the Toyota.
If Frank took the Ford he will be late.
Frank is late.

**Conclusion:** Frank took the Ford.

For arguments in propositional logic, we can capture validity as follows:
Let $\phi_1, \ldots, \phi_n$ and $\phi$ be formulae of propositional logic. Draw a truth table with columns for each of $\phi_1, \ldots, \phi_n$ and $\phi$.

The argument with premises $\phi_1, \ldots, \phi_n$ and conclusion $\phi$ is valid, denoted

$$\phi_1, \ldots, \phi_n \models \phi$$

if in every row of the truth table where $\phi_1, \ldots, \phi_n$ are all true, $\phi$ is true also.

---

<table>
<thead>
<tr>
<th>Frd</th>
<th>Tyta</th>
<th>Late</th>
<th>Frd $\lor$ Tyta</th>
<th>Frd $\rightarrow$ Late</th>
<th>$\neg$Late</th>
<th>Tyta</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

This shows $\text{Frd} \lor \text{Tyta}, \text{Frd} \rightarrow \text{Late}, \neg\text{Late} \models \text{Tyta}$
The following row shows Frd ∨ Tyta, Frd → Late, Late ̸|= Frd

<table>
<thead>
<tr>
<th>Frd</th>
<th>Tyta</th>
<th>Late</th>
<th>Frd ∨ Tyta</th>
<th>Frd → Late</th>
<th>Late</th>
<th>Frd</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
</tbody>
</table>

Applications III:
Reasoning About Requirements/Specifications

Suppose a set of English language requirements \( R \) for a software/hardware system can be formalised by a set of formulae \( \{ \phi_1, \ldots, \phi_n \} \).

Suppose \( C \) is a statement formalised by a formula \( \psi \). Then

1. The requirements cannot be implemented if \( \phi_1 \wedge \ldots \wedge \phi_n \) is not satisfiable.
2. If \( \phi_1, \ldots, \phi_n \models \psi \) then every correct implementation of the requirements \( R \) will be such that \( C \) is always true in the resulting system.
3. If \( \phi_1, \ldots, \phi_{n-1} \models \phi_n \), then the condition \( \phi_n \) of the specification is redundant and need not be stated in the specification.

Example

Requirements \( R \): A burglar alarm system for a house is to operate as follows. The alarm should not sound unless the system has been armed or there is a fire. If the system has been armed and a door is disturbed, the alarm should ring. Irrespective of whether the system has been armed, the alarm should go off when there is a fire.

Conclusion \( C \): If the alarm is ringing and there is no fire, then the system must have been armed.

Questions
- Will every system correctly implementing requirements \( R \) satisfy \( C \)?
- Is the final sentence of the requirements redundant?

Expressing the requirements as formulas of propositional logic, with

- \( S \) = the alarm sounds = the alarm rings
- \( A \) = the system is armed
- \( D \) = a door is disturbed
- \( F \) = there is a fire

we get

Requirements:
1. \( S \rightarrow (A \lor F) \)
2. \((A \land D) \rightarrow S \)
3. \( F \rightarrow S \)

Conclusion: \((S \land \neg F) \rightarrow A \)
Our two questions then correspond to

1. Does \( S \to (A \lor F), (A \land D) \to S, F \to S \models (S \land \neg F) \to A \)?
2. Does \( S \to (A \lor F), (A \land D) \to S \models F \to S \)?

Answers: problem set 2, exercise 2

Validity of Formulas

A formula \( \phi \) is valid, or a tautology, denoted \( \models \phi \), if it evaluates to \( T \) for all assignments of truth values to its basic propositions.

Example

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>((A \to B) \to (\neg B \to \neg A))</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>(T)</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>(T)</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>(T)</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>(T)</td>
</tr>
</tbody>
</table>

Validity, Equivalence and Entailment

Theorem

The following are equivalent:

- \( \phi_1, \ldots, \phi_n \models \psi \)
- \( \models (\phi_1 \land \ldots \land \phi_n) \to \psi \)
- \( \models \phi_1 \to (\phi_2 \to \ldots (\phi_n \to \psi) \ldots) \)

Theorem

\( \phi \equiv \psi \) if and only if \( \models \phi \leftrightarrow \psi \)

Quantifiers

We’ve made quite a few statements of the kind

“If there exists a satisfying assignment …”

or

“Every natural number greater than 2 …”

without formally capturing these quantitative aspects.

Notation: \( \forall \) means “for all” and \( \exists \) means “there exist(s)”

Example

Goldbach’s conjecture

\[ \forall n \in 2\mathbb{N} \hspace{2pt} (n > 2 \to \exists p, q \in \mathbb{N} \hspace{2pt} (p, q \in \text{Primes} \land n = p + q)) \]
Proof Rules and Methods:
Proof of the Contrapositive

We want to prove $A \rightarrow B$.
To prove it, we show $\neg B \rightarrow \neg A$ and invoke the equivalence
$(A \rightarrow B) \equiv (\neg B \rightarrow \neg A)$.

Example
$\forall m, n \in \mathbb{N} \ (m + n \geq 73 \rightarrow m \geq 37 \lor n \geq 37)$

Proof Rules and Methods:
Proof by Contradiction

We want to prove $A$.
To prove it, we assume $\neg A$, and derive both $B$ and $\neg B$ for some proposition $B$.
(Hard part: working out what $B$ should be.)

Examples
- $\sqrt{2}$ is irrational
- There exist an infinite number of primes

Proof Rules and Methods:
Proof by Cases

We want to prove that $A$. To prove it, we find a set of cases $B_1, B_2, \ldots, B_n$ such that
- $B_1 \lor \ldots \lor B_n$, and
- $B_i \rightarrow A$ for each $i = 1, \ldots, n$.
(Hard Part: working out what the $B_i$ should be.)
(Comment: often $n = 2$ and $B_2 = \neg B_1$, so $B_1 \lor B_2 = B_1 \lor \neg B_1$ holds trivially.)

Example
$|x + y| \leq |x| + |y|$ for all $x, y \in \mathbb{R}$.
Recall:
$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$

Substitution

Substitution is the process of replacing every occurrence of some symbol by an expression.

Examples
The result of substituting 3 for $x$ in
$x^2 + 7y = 2xz$
is
$3^2 + 7y = 2 \cdot 3 \cdot z$
The result of substituting $2k + 3$ for $x$ in
$x^2 + 7y = 2xz$
is
$(2k + 3)^2 + 7y = 2 \cdot (2k + 3) \cdot z$
We can substitute logical expressions for logical variables:

**Example**
The result of substituting $P \land Q$ for $A$ in

$$(A \land B) \rightarrow A$$

is

$$(P \land Q) \rightarrow (P \land Q)$$

---

**Substitution Rules**

(a) If we substitute an expression for *all* occurrences of a logical variable in a tautology then the result is still a tautology.

If $\models \phi(P)$ then $\models \phi(\alpha)$.

**Examples**

$\models P \rightarrow (P \lor Q)$, so

$\models (A \lor B) \rightarrow ((A \lor B) \lor Q)$

$\models \neg Q \rightarrow (Q \rightarrow P)$, so

$\models \neg(P \rightarrow Q) \rightarrow ((P \rightarrow Q) \rightarrow P)$

(b) If a logical formula $\phi$ contains a formula $\alpha$, and we replace (an occurrence of) $\alpha$ by a logically equivalent formula $\beta$, then the result is logically equivalent to $\phi$.

If $\alpha \equiv \beta$ then $\phi(\alpha) \equiv \phi(\beta)$.

**Example**

$P \rightarrow Q \equiv \neg P \lor Q$, so

$$Q \rightarrow (P \rightarrow Q) \equiv Q \rightarrow (\neg P \lor Q)$$

---

COMP9020 Lecture 6
Session 2, 2017
Logic cont’d
Lecture 5 recap: Logical connectives

- AND — conjunction, ∧, &
- OR — disjunction, ∨, ||
- NOT — negation
- Implication, →, ⊃ (IF-THEN)
- Bi-implication, ↔ (IF AND ONLY IF)

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A ∧ B</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A ∨ B</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>¬A</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
</tr>
</tbody>
</table>

Lecture 5 recap: Propositional formulae

The set of formulae of propositional logic is the smallest set of words over Σ such that

- T, ⊥ and all elements of Prop are formulae
- If φ is a formula, then so is ¬φ
- If φ and ψ are formulae, then so are (φ ∧ ψ), (φ ∨ ψ), (φ → ψ), and (φ ↔ ψ).

Lecture 5 recap: Truth tables

- Row for every truth assignment — assignment of T/F to elements of Prop
- Columns for subformulae
- Truth assignments can also map formulae to T/F: be careful!

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>¬p</th>
<th>¬p ∧ q</th>
<th>p ∨ (¬p ∧ q)</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>¬p</th>
<th>¬p ∧ q</th>
<th>p ∨ (¬p ∧ q)</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>
A truth assignment is a function \( \nu : \text{Prop} \rightarrow \{T, F\} \).

Can extend truth assignments to formulae:
- \( \nu(\top) = T \), \( \nu(\bot) = F \)
- \( \nu(\neg \varphi) = \neg \nu(\varphi) \)
- \( \nu(\varphi \land \psi) = \nu(\varphi) \land \nu(\psi) \), ...

Two formulas, \( \varphi \) and \( \psi \), are logically equivalent, \( \varphi \equiv \psi \), if \( \nu(\varphi) = \nu(\psi) \) for all truth assignments \( \nu \).

A list of formulae, \( \varphi_1, \ldots, \varphi_n \) entail a single formula, \( \psi \), written \( \varphi_1, \ldots, \varphi_n \models \psi \) if \( \nu(\psi) = T \) for all truth assignments \( \nu \) where \( \nu(\varphi_1) = \ldots = \nu(\varphi_n) = T \). If the list is empty, we say \( \psi \) is a tautology.

Theorem
- \( \phi_1, \ldots, \phi_n \models \psi \) if, and only if, \( \models (\phi_1 \land \ldots \land \phi_n) \rightarrow \psi \)
- \( \phi \equiv \psi \) if, and only if, \( \models \phi \leftrightarrow \psi \)

Formulae can be viewed as Boolean functions mapping valuations of their propositional letters to truth values.

A Boolean function of one variable is also called unary.
A function of two variables is called binary.
A function of \( n \) input variables is called \( n \)-ary.

Question
- How many unary Boolean functions are there?
- How many binary functions? \( n \)-ary?

Question
What connectives do we need to express all of them?
Boolean Arithmetic

Consider truth values with operations $\land, \lor, \neg$ as an algebraic structure:

- $\mathbb{B} = \{0, 1\}$ with 'Boolean' arithmetic

$$a \land b, \ a \lor b, \ \overline{a} = 1 - a$$

**NB**

We often write $pq$ for $p \land q$.

In electrical and computer engineering, the notation $\overline{p}$ is more common than $p'$, which is often used in mathematics.

Observe that using $(·)$ obviates the need for some parentheses.

---

Applications IV: Digital Circuits

A formula can be viewed as defining a digital circuit, which computes a Boolean function of the input propositions. The function is given by the truth table of the formula.

**NB**

Common usage: $+\ $ for or, $\cdot$ for and, $\overline{x}$ for $\neg x$

---

Definition: Boolean Algebra

Every structure consisting of a set $T$ with operations $\lor$, $\land$ and $\neg$ is called a Boolean algebra if it satisfies the following laws, for all $x, y, z \in T$:

- **commutative**: $x \lor y = y \lor x$
- $x \land y = y \land x$
- **associative**: $(x \lor y) \lor z = x \lor (y \lor z)$
- $(x \land y) \land z = x \land (y \land z)$
- **distributive**: $x \lor (y \land z) = (x \lor y) \land (x \lor z)$
- $x \land (y \lor z) = (x \land y) \lor (x \land z)$
- **identity**: $x \lor 0 = x, \ x \land 1 = x$
- **complementation**: $x \lor \overline{x} = 1, \ x \land \overline{x} = 0$

---

Terminology and Rules

- A literal is an expression $p$ or $\overline{p}$, where $p$ is a propositional atom.
- An expression is in CNF (conjunctive normal form) if it has the form

$$\bigwedge_i C_i$$

where each clause $C_i$ is a disjunction of literals e.g. $p \lor q \lor \overline{r}$.

- An expression is in DNF (disjunctive normal form) if it has the form

$$\bigvee_i C_i$$

where each clause $C_i$ is a conjunction of literals e.g. $p \land q \land \overline{r}$.
- CNF and DNF are named after their top level operators; no deeper nesting of $\land$ or $\lor$ is permitted.
- We can assume in every clause (disjunct for the CNF, conjunct for the DNF) any given variable (literal) appears only once; preferably, no literal and its negation together.
  - $x \lor x = x$, $x \land x = x$
  - $x \land \overline{x} = 0$, $x \lor \overline{x} = 1$
  - $x \land 0 = 0$, $x \land 1 = x$, $x \lor 0 = x$, $x \lor 1 = 1$
- A preferred form for an expression is DNF, with as few terms as possible. In deriving such minimal simplifications the two basic rules are **absorption** and **combining the opposites**.

**Fact**

1. $x \lor (x \land y) = x$ (absorption)
2. $(x \land y) \lor (x \land \overline{y}) = x$ (combining the opposites)

**Theorem**

For every Boolean expression $\phi$, there exists an equivalent expression in conjunctive normal form and an equivalent expression in disjunctive normal form.

**Proof.**

We show how to apply the equivalences already introduced to convert any given formula to an equivalent one in CNF, DNF is similar.

---

**Step 1: Push Negations Down**

Using De Morgan’s laws and the *double negation* rule

\[
\overline{x \lor y} = \overline{x} \land \overline{y} \\
\overline{x \land y} = \overline{x} \lor \overline{y} \\
\overline{x} = x
\]

we push negations down towards the atoms until we obtain a formula that is formed from literals using only $\land$ and $\lor$.

---

**Step 2: Use Distribution to Convert to CNF**

Using the distribution rules

\[
x \lor (y_1 \land \ldots \land y_n) = (x \lor y_1) \land \ldots \land (x \lor y_n) \\
(y_1 \land \ldots \land y_n) \lor x = (y_1 \lor x) \land \ldots \land (y_n \lor x)
\]

we obtain a CNF formula.
CNF/DNF in Propositional Logic

Using the equivalence
\[ A \rightarrow B \equiv \neg A \lor B \]
we first eliminate all occurrences of \( \rightarrow \)

**Example**
\[ \neg (\neg p \land ((r \land s) \rightarrow q)) \equiv \neg (\neg p \land (\neg (r \land s) \lor q)) \]

Step 1:

**Example**
\[ \overline{p(r \land s \lor q)} = \overline{p} \lor \overline{r} \lor \overline{s} \lor q \]
\[ = p \lor \overline{r} \lor \overline{s} \lor q \]

Step 2:

**Example**
\[ p \lor rsq = (p \lor r)(p \lor sq) \]
\[ = (p \lor r)(p \lor s)(p \lor q) \quad \text{CNF} \]

Canonical Form DNF

Given a Boolean expression \( E \), we can construct an equivalent
DNF \( E^{dnf} \) from the lines of the truth table where \( E \) is true:

Given an assignment \( \pi \) of 0,1 to variables \( x_1 \ldots x_i \), define the literal
\[ \ell_i = \begin{cases} x_i & \text{if } \pi(x_i) = 1 \\ \overline{x_i} & \text{if } \pi(x_i) = 0 \end{cases} \]
and a product \( t_{\pi} = \ell_1 \cdot \ell_2 \cdot \ldots \cdot \ell_n \).

**Example**
If \( \pi(x_1) = 1 \) and \( \pi(x_2) = 0 \) then \( t_{\pi} = x_1 \cdot \overline{x_2} \)

The canonical DNF of \( E \) is
\[ E^{dnf} = \sum_{E(\pi) = 1} t_{\pi} \]

**Example**
If \( E \) is defined by
\[
\begin{array}{c|c|c}
 x & y & E \\
 0 & 0 & 1 \\
 0 & 1 & 0 \\
 1 & 0 & 1 \\
 1 & 1 & 0 \\
\end{array}
\]
then \( E^{dnf} = xy + xy + xy \)
Note that this can be simplified to either
\[ y + xy \]
or
\[ xy + x \]
Exercise

10.2.3 Find the canonical DNF form of each of the following expressions in variables \( x, y, z \):

- \( xy \)
- \( \bar{z} \)
- \( xy + \bar{z} \)
- \( 1 \)

Karnaugh Maps

For up to four variables (propositional symbols) a diagrammatic method of simplification called Karnaugh maps works quite well. For every propositional function of \( k = 2, 3, 4 \) variables we construct a rectangular array of \( 2^k \) cells. We mark the squares corresponding to the value 1 with eg “+” and try to cover these squares with as few rectangles with sides 1 or 2 or 4 as possible.

Example

10.4.2 Use a K-map to find an optimised form.

Example

For optimisation, the idea is to cover the + squares with the minimum number of rectangles. One cannot cover any empty cells (they indicate where \( f(w, x, y, z) = 0 \)).

- The rectangles can go ‘around the corner’/the actual map should be seen as a torus.
- Rectangles must have sides of 1, 2 or 4 squares (three adjacent cells are useless).

Example

\[
\begin{array}{cccc}
xyz & y\bar{z} & \bar{y}\bar{z} & \bar{y}z \\
x & + & + & + \\
\bar{x} & + & + & +
\end{array}
\]

\( f = xy + \bar{y}z \)

Canonical form would consist of writing all cells separately:

\[
xyz + xy\bar{z} + \bar{x}y\bar{z} + \bar{x}\bar{y}z + \bar{x}y\bar{z} + \bar{x}\bar{y}z
\]
For optimisation, the idea is to cover the + squares with the minimum number of rectangles. One cannot cover any empty cells (they indicate where $f(w, x, y, z)$ is 0).

- The rectangles can go ‘around the corner’/the actual map should be seen as a torus.
- Rectangles must have sides of 1, 2 or 4 squares (three adjacent cells are useless).

**Example**

\[
\begin{array}{cccc}
  yz & y\bar{z} & \bar{y}z & \bar{y}z \\
  x & + & + & + \\
 \bar{x} & + & + & +
\end{array}
\]

$f = xy + \bar{x}\bar{y} + z$

Canonical form would consist of writing all cells separately:

\[xyz + xy\bar{z} + x\bar{y}z + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}\bar{y}z\]

---

**Supplementary Exercise**

10.6.6(c)

\[
\begin{array}{cccc}
  yz & y\bar{z} & \bar{y}z & \bar{y}z \\
  wx & + & + & + \\
  w\bar{x} & + & + & + \\
  \bar{w}x & + & + & + \\
  \bar{w}x & + & + & +
\end{array}
\]

$f = wy + \bar{x}\bar{y} + xz$

Note: trying to use \( w\bar{x} \) or \( \bar{y}z \) doesn’t give as good a solution

---

**Boolean Algebras in Computer Science**

Several data structures have natural operations following essentially the same rules as logical \( \land \), \( \lor \) and \( \neg \).

- \( n \)-tuples of 0’s and 1’s with Boolean operations, e.g.

\[
\begin{array}{cc}
  \text{join: } & (1,0,0,1) \lor (1,1,0,0) = (1,1,0,1) \\
  \text{meet: } & (1,0,0,1) \land (1,1,0,0) = (1,0,0,0) \\
  \text{complement: } & (1,0,0,1) = (0,1,1,0)
\end{array}
\]

- \( \text{Pow}(S) \) — subsets of \( S \)

\[
\begin{array}{cc}
  \text{join: } & A \cup B, \quad \text{meet: } A \cap B, \quad \text{complement: } A^c = S \setminus A
\end{array}
\]
Example

10.1.1 Define a Boolean algebra for the power set Pow(S) of 
S = \{a, b, c\}
join: X, Y ↦→ X ∪ Y
meet: X, Y ↦→ X ∩ Y
complementation: X ↦→ (a, b, c) \ X
0 def = ∅
1 def = \{a, b, c\}

Exercise:
Verify that all Boolean algebra laws (cf. slide 65) hold for 
X, Y, Z ∈ Pow(\{a, b, c\})

More Examples of Boolean Algebras in CS

- Functions from any set S to B; their set is denoted Map(S, B)
  If f, g : S −→ B then
  - (f ∨ g) : S −→ B is defined by s ↦→ f(s) ∨ g(s)
  - (f ∧ g) : S −→ B is defined by s ↦→ f(s) ∧ g(s)
  - ̅f : S −→ B is defined by s ↦→ ̅f(s)
  There are 2^n such functions for |S| = n

- All Boolean functions of n variables, e.g.
  (p_1, p_2, p_3) ↦→ (p_1 ∨ p_2) ∧ (p_1 ∨ p_3) ∨ p_2 ∨ p_3
  There are 2^n of them; their collection is denoted BOOL(n)

Every finite Boolean algebra satisfies: |T| = 2^k for some k.
All algebras with the same number of elements are isomorphic,
meaning “structurally similar”, written ≃. Therefore, studying one such
algebra describes properties of all.
A cartesian product of Boolean algebras is again a Boolean
algebra. We write

B^k = B × ... × B

The algebras mentioned above are all of this form
- n-tuples ≃ B^n
- Pow(S) ≃ B^|S|
- Map(S, B) ≃ B^|S|
- BOOL(n) ≃ B^{2^n}

NB

Boolean algebra as the calculus of two values is fundamental to
computer circuits and computer programming.
Example: Encoding subsets as bit vectors.
Summary

- Logic: syntax, truth tables; $\land$, $\lor$, $\neg$, $\rightarrow$, $\leftrightarrow$, $\top$, $\bot$
- Valid formulae (tautologies), satisfiable formulae
- Entailment $\models$, equivalence $\equiv$
  - some well-known equivalences (slides 23 and 24)
- Proof methods: contrapositive, by contradiction, by cases
- Boolean algebra
- CNF, DNF, canonical form

Supplementary reading [LLM]
- Ch. 1, Sec. 1.5-1.9 (more about good proofs)
- Ch. 3, Sec. 3.3 (more about proving equivalences of formulae)