Propositional Logic: a Connectives

- ¬p: the negation of statement p.
- p ∧ q: the conjunction of statements p and q.
  - “p and q.”
- p ∨ q: the disjunction of statements p and q.
  - “p or q.”
- p → q: the (material) implication of q by p.
  - “Hypothesis p implies conclusion q.”
- p ↔ q: the biconditional of p and q.
  - “p if and only if q.”

Attributed to Gottfried Wilhelm Leibniz (1646–1716).

Tautology and Contradiction

- A statement is a tautology if it is true for all truth value assignments for its component statements.
  - For example, p ∨ ¬p.
  - Note that tautology is a metalogical statement.
- A statement is a contradiction if it is false for all truth value assignments for its component statements.

“Ludwig Wittgenstein (1889–1951). He is one of the most important philosophers of all time. “God has arrived,” Keynes said of him on January 18, 1928. “I met him on the 5:15 train.”

Tautology and Contradiction (concluded)

- When p → q is a tautology, we say p logically implies q, written as p ⇒ q.
  - Note that p ⇒ q is a metalogical statement.
- If
  \[(p_1 ∧ p_2 ∧ \cdots ∧ p_n) \rightarrow q\]
  is a tautology, then conclusion q follows validly from premises p_1, p_2, ..., p_n.
### Truth Tables

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>p ∧ q</th>
<th>p ∨ q</th>
<th>p → q</th>
<th>p ↔ q</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

- A truth table with \( n \) basic variables has \( 2^n \) entries.
- Verifying a tautology is a known computationally hard problem (coNP-complete, to be exact).

### An Example of a Valid Argument

\( q \) follows validly from

\[(p → r) ∧ (¬q → p) ∧ ¬r.\]

- Write down the truth table for

\[\[(p → r) ∧ (¬q → p) ∧ ¬r]\] → q.

- Verify that it is a tautology.

### An Example of a Potentially Invalid Argument

“The premises he used were false, therefore his conclusions were false,” said Dudley Sharp of *Justice For All.*

---

---

### Logical Equivalence

- Statements \( p \) and \( q \) are logically equivalent (written as \( p \Leftrightarrow q \)) when \( p \) and \( q \) have the same truth value for all truth value assignments for the component statements.

- For example, \( p → q \Leftrightarrow ¬p ∨ q.\)

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>¬p ∨ q</th>
<th>p → q</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Some Easy Pieces

- $p \Rightarrow q$ if and only if $p \rightarrow q$ is a tautology.
- $p \iff q$ if and only if $p \Rightarrow q$ and $q \Rightarrow p$.
- $[p \land (p \rightarrow q)] \Rightarrow q$.
- Modus ponens or rule of detachment.
- $[(p \rightarrow q) \land (q \rightarrow r)] \Rightarrow (p \rightarrow r)$.
- Law of the syllogism.
- $[(p \rightarrow q) \land \neg q] \Rightarrow \neg p$.
- Modus tollens.
- $(\neg p \rightarrow \text{false}) \Rightarrow p$.
- Reductio ad absurdum or rule of contradiction.

Duality

- Let $s$ be a statement and contain no logical connectives other than $\lor$ and $\land$.
- The dual of $s$, $s^d$, is the statement obtained from $s$ by replacing each occurrence of
  - $\land$ with $\lor$,
  - $\lor$ with $\land$,
  - true with false, and
  - false with true.
- Note that $\neg$ is unchanged.
- The principle of duality: If $s \iff t$, then $s^d \iff t^d$.

DeMorgan’s Laws\textsuperscript{a}

- $\neg(p \lor q) = \neg p \land \neg q$.
- $\neg(p \land q) = \neg p \lor \neg q$.
- It can be used to transform any boolean expression into an equivalent one where $\neg$ applies only to variables.
  - For example,
    
    $\neg(x_1 \lor (x_2 \land \neg x_3)) = (\neg x_1) \land (\neg x_2 \lor \neg x_3)$
    
    $= (\neg x_1) \land (\neg x_2 \lor \neg x_3)$
    
    $= (\neg x_1) \land (\neg x_2 \lor x_3)$.

\textsuperscript{a}Augustus DeMorgan (1806–1871).

Set Theory\textsuperscript{a}

- Let $A$ and $B$ be sets.
- $x \in A$ means $x$ is an element of $A$.
- $x \notin A$ means $x$ is not an element of $A$.
- $A \subseteq B$ means every element of $A$ is an element of $B$.
- $A = B$ means $A \subseteq B$ and $B \subseteq A$.
- $A \subset B$ means $A \subseteq B$ but $A \neq B$.
- $\emptyset$ is the empty set, and $\emptyset \subseteq A$ for any set $A$.

\textsuperscript{a}Founded by Georg Cantor (1845–1918) in 1874. Set theory is the cornerstone of all modern mathematics.
Set Operations

- $A \cup B$ is the union of $A$ and $B$.
- $A \cap B$ is the intersection of $A$ and $B$.
- $A \Delta B$ is the symmetric difference of $A$ and $B$, or
  \[ \{x : (x \in A \land x \notin B) \lor (x \in B \land x \notin A)\}. \]
- $A$ and $B$ are disjoint if $A \cap B = \emptyset$.
- $\bar{A}$ is the complement of $A$.

Set Operations (concluded)

- $A - B = \{x : x \in A \land x \notin B\}$.
- $\bigcup_{i \in I} A_i = \{x : x \in A_i \text{ for some } i \in I\}$.
- $\bigcap_{i \in I} A_i = \{x : x \in A_i \text{ for all } i \in I\}$.

Interesting Relations

- $A \Delta B = B \Delta A$.
- In general, $A - B \neq B - A$.
- $A \Delta B = (A \cup B) - (A \cap B)$.
- $A \Delta B = (A - B) \cup (B - A)$.

*Contributed by Ms. Chiyoko Yamazaki (B92902108) on October 4, 2004.

Russell’s* Paradox (1901)

- Consider the set
  \[ R = \{A : A \notin A\}. \]
- If $R \in R$, then $R \notin R$ by the definition.
- If $R \notin R$, then $R \in R$ also by the definition.
- What gives?

*Bertrand Russell (1872–1970), the most important logician of the 20th century if not of all time.
DeMorgan’s Laws

\( \bigcup_{i \in I} A_i = \bigcap_{i \in I} A_i \),

\( \bigcap_{i \in I} A_i = \bigcup_{i \in I} A_i \).

And though the holes were rather small,
they had to count them all.

More Combinatorics

Common Sets

\( \mathbb{N} = \{0, 1, \ldots\} \),
\( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \),
\( \mathbb{Z}^+ = \{1, 2, \ldots\} \),
\( \mathbb{R} = \) set of real numbers,
\( \mathbb{Q} = \) set of rational numbers.

\(^a0\) is a natural number!
The Well-Ordering Principle

**Theorem 34** Every nonempty subset of \( \mathbb{Z}^+ \) contains a smallest element. (\( \mathbb{Z}^+ \) is said to be well-ordered.)

- Real numbers are not well-ordered.
  - \( \{x \in \mathbb{R} : x > 1\} \) does not contain a smallest element.
- Rational numbers are not well-ordered.
  - \( \{x \in \mathbb{Q} : x > 1\} \) does not contain a smallest element.

---

Mathematical Induction^a

**Theorem 35** Let \( S(n) \) denote an (open) mathematical statement containing references to a positive integer \( n \) such that

- \( S(1) \) is true and
- \( S(k + 1) \) is true whenever \( S(k) \) is true for arbitrarily chosen \( k \in \mathbb{Z}^+ \).

Then \( S(n) \) is true for all \( n \in \mathbb{Z}^+ \).

---

^aRichard Dedekind (1831–1916) and Giuseppe Peano (1858–1932).

---

The Proof

- Let \( F = \{t \in \mathbb{Z}^+ : S(t) \text{ is false}\} \).
- Assume that \( F \neq \emptyset \).
- \( F \) has a least element \( \ell \) by the well-ordering principle.
- Clearly \( \ell > 1 \) and, hence, \( \ell - 1 \in \mathbb{Z}^+ \).
- Because \( \ell - 1 \notin F \), \( S(\ell - 1) \) is true.
- It follows that \( S(\ell) \) is true, a contradiction.
- So \( F = \emptyset \).

---

Mathematical Induction and the Well-Ordering Principle

- The proof of induction says that the well-ordering principle (p. 146) implies mathematical induction.
- Now we prove the converse.
- Let \( T \subseteq \mathbb{Z}^+ \) and \( T \neq \emptyset \).
- It suffices to show that \( T \) contains a smallest element.
- Let \( S(n) \) be the statement that no element of \( T \) is smaller than \( n \).
The Proof (continued)

- $S(1)$ is true as no positive integers are smaller than 1.
- Suppose $S(k + 1)$ holds whenever $S(k)$ does.
- By mathematical induction, $S(n)$ is true for all $n \in \mathbb{Z}^+$.
- This means for any $n \in \mathbb{Z}^+$, no element of $T$ is smaller than $n$.
- But this is impossible as any integer in $T$ must be smaller than some integer.
- Hence there is a $k \in \mathbb{Z}^+$ such that $S(k)$ is true but $S(k + 1)$ is not.

Philosophical Issues

- Mathematical induction has nothing to do with induction in the physical and empirical sciences.
  - Sun rises on Monday, on Tuesday, etc., so it must rise everyday from now?
- Mathematical induction is merely a property of integers.

Compositions of Positive Integers Revisited

- As $S(k)$ holds, no element of $T$ is smaller than $k$.
- As $S(k + 1)$ does not hold, some elements of $T$ are smaller than $k + 1$.
- But as $S(k)$ holds, these elements must equal $k$.
- Hence the smallest element of $T$ exists and is $k$. 

- Next we use mathematical induction to reprove the fact that the number of compositions for $m$ is $2^{m-1}$.
- The statement clearly holds when $m = 1$.
- So assume it holds for general $m$ and now consider the compositions of $m + 1$. 

The Proof (continued)

• Suppose the last summand is \( n > 1 \).
  – Replace the last summand by \( n – 1 \).
  – The result is a composition of \( m \).
  – This correspondence is also one-to-one.
  – So there are \( 2^{m-1} \) compositions in this case.

• In the proof that the total number of compositions of \( m \) is \( 2^{m-1} \), induction was used.
• Can we do away with it by, say, an indirect proof?
• So we set out to obtain a contradiction by assuming the desired number is not \( 2^{m-1} \).
• What next?

Do You Really Need Induction?

• It is typical to work on the smallest \( m \) such that the desired number does not equal \( 2^{m-1} \).
• This \( m \) cannot be 1 by inspection.
• But if \( m > 1 \), we obtain another contradiction because ...
• This proof relies on the well-ordering principle (p. 146), which is equivalent to mathematical induction (p. 149)!
• The same thing can be said of the alternative proof on pp. 76ff.

The Proof (concluded)

• Now suppose the last summand is \( n = 1 \).
  – Remove the last summand.
  – The result is a composition of \( m \).
  – This correspondence is also one-to-one.
  – So there are \( 2^{m-1} \) compositions in this case.
• The total number of compositions of \( m + 1 \) is hence
  \[ 2^{m-1} + 2^{m-1} = 2^m. \]
• This is consistent with Theorem 22 (p. 76).
Fibonacci Numbers (1202)

- Let $F_0 = 0$ and $F_1 = 1$.
- Let $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.
  - $F_2 = 0 + 1 = 1$.
  - $F_3 = 1 + 1 = 2$.
  - $F_4 = 1 + 2 = 3$.
- Innumerable applications in surprisingly diverse fields.

\*Leonardo Fibonacci (1175–1250).

Another Identity for Fibonacci Numbers

**Theorem 37** $\sum_{i=0}^{n} F_i = F_{n+2} - 1$ for $n \in \mathbb{N}$.

- For $n = 0$, $F_0 = 0 = 1 - 1 = F_2 - 1$.
- Inductively,
  
  \[
  \begin{align*}
  \sum_{i=0}^{k+1} F_i &= \sum_{i=0}^{k} F_i + F_{k+1} \\
  &= F_{k+2} - 1 + F_{k+1} \\
  &= F_{k+3} - 1.
  \end{align*}
  \]

An Identity for Fibonacci Numbers

**Theorem 36** $\sum_{i=0}^{n} F_i^2 = F_n F_{n+1}$ for $n \in \mathbb{Z}^+$.

- For $n = 1$, $F_0^2 + F_1^2 = 1 = F_1 F_2$.
- Inductively,
  
  \[
  \begin{align*}
  \sum_{i=0}^{k+1} F_i^2 &= \sum_{i=0}^{k} F_i^2 + F_{k+1}^2 \\
  &= \left( \sum_{i=0}^{k} F_i^2 \right) + F_{k+1}^2 \\
  &= F_{k+1}(F_k + F_{k+1}) = F_{k+1}F_{k+2}.
  \end{align*}
  \]

Identities for Summations

For $n \in \mathbb{Z}^+$,

\[
\frac{n^2(n+1)^2}{4} = \sum_{i=1}^{n} i^3 = \left( \sum_{i=1}^{n} i \right)^2.
\]

- The identities are clearly true when $n = 1$.
- Assume the identities are true for $n = k$.
- Note that
  \[
  \frac{(k+1)^2(k+2)^2}{4} = \frac{k^2(k+1)^2}{4} + (k+1)^3.
  \]
- So the first identity holds.
The Proof (concluded)

- As for the second identity,
  \[
  \left( \sum_{i=1}^{k+1} i \right)^2 = \left( \sum_{i=1}^{k} i \right)^2 + 2(k+1) \sum_{i=1}^{k} i + (k+1)^2 \\
  = \left( \sum_{i=1}^{k} i \right)^2 + 2(k+1) \frac{k(k+1)}{2} + (k+1)^2 \\
  = \left( \sum_{i=1}^{k} i \right)^2 + (k+1)^3 \\
  = \sum_{i=1}^{k} i^3 + (k+1)^3 = \sum_{i=1}^{k+1} i^3.
  \]

Fundamental Integer Arithmetics

- \( b \mid a \) means that \( b \) divides \( a \), where \( a, b \in \mathbb{Z} \) and \( b \neq 0 \).
  - \( b \) is a divisor or factor of \( a \); \( a \) is a multiple of \( b \).
- If \( a, b \in \mathbb{Z} \) with \( b > 0 \), then there exist unique \( q, r \in \mathbb{Z} \) such that \( a = qb + r \), where \( 0 \leq r < b \).
- \( \gcd(a, b) > 0 \) denotes the greatest common divisor of \( a, b \in \mathbb{Z} \), where \( a \neq 0 \) or \( b \neq 0 \) (hence \( \gcd(a, 0) = |a| \)).
- A prime is a positive integer larger than 1 whose only divisors are itself and 1.
- There are infinitely many primes.a

Application: \( d(n) \), Number of Positive Divisors

**Theorem 38** Let \( n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} \) be the prime factorization of \( n \). Then the number of positive divisors of \( n \) equals \( d(n) = (e_1 + 1)(e_2 + 1) \cdots (e_t + 1) \).

- A positive divisor of \( n \) is of form \( n = p_1^{s_1} p_2^{s_2} \cdots p_t^{s_t} \), where \( 0 \leq s_i \leq e_i \).
- There are \( e_1 + 1 \) choices for \( s_1 \), \( e_2 + 1 \) choices for \( s_2 \), etc.

Countability

---

[a] Euclid. Maybe the greatest theorem in mathematics.
Infinite Sets

- A set is **countable** if it is finite or if it can be put in one-to-one correspondence with \( \mathbb{N} \) (in which case it is called **countably infinite**).
  - Set of integers \( \mathbb{Z} \).
    - \( 0 \leftrightarrow 0, 1 \leftrightarrow 1, 2 \leftrightarrow 3, 3 \leftrightarrow 5, \ldots, -1 \leftrightarrow 2, -2 \leftrightarrow 4, -3 \leftrightarrow 6, \ldots \)
  - Set of positive integers \( \mathbb{Z}^+ \): \( i - 1 \leftrightarrow i \).
  - Set of odd integers: \( (i - 1)/2 \leftrightarrow i \).
  - Set of rational numbers: See next page.
  - Set of squared integers: \( i \leftrightarrow \sqrt{i} \).

Rational Numbers Are Countable

\[
\begin{array}{cccccc}
1/1 & 1/2 & 1/3 & 1/4 & 1/5 & 1/6 \\
2/1 & 2/2 & 2/3 & 2/4 & 2/5 & 2/6 \\
4/1 & 4/2 & 4/3 & 4/4 & 4/5 & 4/6 \\
5/1 & 5/2 & 5/3 & 5/4 & 5/5 & 5/6 \\
6/1 & & & & & \\
\end{array}
\]

Algebraic Numbers

- A number is called **algebraic** if it is a root of a polynomial equation with integer coefficients.
  - For example, \( \sqrt{2} \) is an algebraic number because it satisfies \( x^2 - 2 = 0 \).
- A real number that is not algebraic is called **transcendental**.
  - \( e = 2.718281828459045 \ldots \) is transcendental.
  - \( \pi \) is transcendental.

---

.brand.

a– Leonhard Euler.
b– Charles Hermite (1873).
c– Ferdinand Lindemann (1882).

---

Algebraic Numbers Are Countable

- Consider any polynomial with integer coefficients,
  \[
a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0.
\]
  - This polynomial corresponds uniquely to the rational number
    \[
    a_n a_{n-1} \cdots a_0 < 1.
    \]
      - Above, treat each \( a_i \) as a string of numbers between 0 and 9 whose leading number is nonzero.
- As rational numbers are countable, so are algebraic numbers.

---

a– Georg Cantor (1874).
Cardinality

• For any set $A$, define $|A|$ as $A$'s cardinality (size).
• Two sets are said to have the same cardinality (written as $|A| = |B|$ or $A \sim B$) if there exists a one-to-one correspondence between their elements.
• $2^A$ denotes set $A$'s power set, that is $\{B : B \subseteq A\}$.
  - If $|A| = k$, then $|2^A| = 2^k$.
  - So $|A| < |2^A|$ when $A$ is finite (see p. 172 for proof).

Cardinality (concluded)

• $|A| \leq |B|$ if there is a one-to-one correspondence between $A$ and one of $B$’s subsets.
• $|A| < |B|$ if $|A| \leq |B|$ but $|A| \neq |B|$.
• If $A \subseteq B$, then $|A| \leq |B|$.
• But if $A \subset B$, then $|A| < |B|$?

A Combinatorial Proof for $k < 2^k$

• Let $A = \{1, 2, \ldots, k\}$
  be a set with $k$ elements.
• $|2^A| = 2^k$.
• But
  \[2^A = \{\{1\}, \{2\}, \ldots, \{k\}, \{1, 2\}, \ldots, \{1, 2, \ldots, k\}\}.\]
• Hence $k < |2^A| = 2^k$.

Cardinality and Infinite Sets

• Suppose $A$ and $B$ are infinite sets.
• Then it is possible that $A \subset B$ and yet $|A| = |B|$.
  - The set of integers properly contains the set of odd integers.
  - But the set of integers has the same cardinality as the set of odd integers.
• A lot of “paradoxes.”
Cantor’s Theorem

**Theorem 39** The set of all subsets of \( \mathbb{N} \) \( (2^\mathbb{N}) \) is infinite and not countable.

- Suppose it is countable with \( f : \mathbb{N} \to 2^\mathbb{N} \) being a bijection.
- Consider the set \( B = \{ k \in \mathbb{N} : k \not\in f(k) \} \subseteq \mathbb{N} \).
- Suppose \( B = f(n) \) for some \( n \in \mathbb{N} \).

"Georg Cantor (1845–1918). According to Kac and Ulam, ‘[If] one had to name a single person whose work has had the most decisive influence on the present spirit of mathematics, it would almost surely be Georg Cantor.’"

---

Other Uncountable Sets

- Real numbers are not countable.
  - So there are real numbers that cannot be defined in a finite number of words.
- Transcendental numbers are not countable (p. 169).
- So in a sense, most real numbers are transcendental.

"Georg Cantor.

---

Application: Existence of Uncomputable Problems

- Every program with a binary output is a finite sequence of 0s and 1s, thus a nonnegative integer.
- It follows that the set of programs is as large as \( \mathbb{N} \).
- Now consider functions from \( \mathbb{N} \) to \( \{0, 1\} \).
- As each function uniquely defines a subset of \( \mathbb{N} \), their cardinality is \( |2^\mathbb{N}| \).
  - \( \{ i : f(i) = 1 \} \subseteq \mathbb{N} \).
- As \( |\mathbb{N}| < |2^\mathbb{N}| \) (p. 174), there are functions for which there are no programs.
Hilbert’s Paradox of the Grand Hotel

- For a hotel with a finite number of rooms with all the rooms occupied, a new guest will be turned away.

- Now let us imagine a hotel with an infinite number of rooms, and all the rooms are occupied.

- A new guest comes and asks for a room.

- “But of course!” exclaims the proprietor, and he moves the person previously occupying Room 1 into Room 2, the person from Room 2 into Room 3, and so on . . .

- The new customer occupies Room 1.

*David Hilbert (1862–1943).

Hilbert’s Paradox of the Grand Hotel (concluded)

- Let us imagine now a hotel with an infinite number of rooms, all taken up, and an infinite number of new guests who come in and ask for rooms.

- “Certainly, gentlemen,” says the proprietor, “just wait a minute.”

- He moves the occupant of Room 1 into Room 2, the occupant of Room 2 into Room 4, and so on.

- Now all odd-numbered rooms become free and the infinity of new guests can be accommodated in them.

- (“There are many rooms in my Father’s house, and I am going to prepare a place for you.” John 14:3.)