Propositional Logic: Connectives

Attributed to Gottfried Wilhelm Leibniz (1646–1716).

"b if and only if d," –

\[ b \leftrightarrow d \]

Hyphothesis implies d

"b hypothosis implies d" –

\[ b \rightarrow d \]

Implication of the (material) implication

"b of or d," –

\[ b \lor d \]

Disjunction of statements and

"b and d," –

\[ b \land d \]

Conjunction of statements and

\[ \neg d \]

The negation of statement.
Ludwig Wittgenstein (1889-1951)

\[ \text{implies } b \iff d \text{ written as } d \iff (u_d \land \ldots \land v_d \land 1) \]

When \( d \) is a tautology, we say logically

\[ \text{premises } p_1, p_2, \ldots \]

is a tautology, then conclusion valid

\[ b \iff (u_d \lor \ldots \lor v_d \lor 1) \]

If

value assignments for its component statements.

A statement is a contradiction if it is false for all truth

value assignments for its component statements.

A statement is a tautology if it is true for all truth

and Contradiction
problem \( \text{coNP-complete} \), to be exact.

Verifying a tautology is a known computationally hard

A truth table with \( n \) basic variables has \( 2^n \) entries.

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>I</td>
<td>0</td>
<td>0</td>
<td>I</td>
</tr>
<tr>
<td>0</td>
<td>I</td>
<td>I</td>
<td>0</td>
<td>I</td>
<td>0</td>
</tr>
<tr>
<td>I</td>
<td>I</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ b \leftrightarrow d \quad b \leftrightarrow d \quad b \land d \quad b \lor d \quad b \quad d \]

Truth Tables
Is a tautology:

\[ b \leftarrow [\neg t \lor (d \leftarrow b) \lor (t \leftarrow d)] \]

Use a truth table to verify that

\[ \neg t \lor (d \leftarrow b) \lor (t \leftarrow d) \]

follows validly from \( b \)

Example of a Valid Argument
\[
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 \\
\end{array}
\]

\[
\begin{array}{cccc}
b \leftarrow d & b \wedge d & b & d \\
\end{array}
\]

For example, \( b \wedge d \leftrightarrow b \leftarrow d \)

Logical Equivalence

For each assignment for the component statements, the truth value assignments for the compounds have the same truth value as when \( b \leftrightarrow d \) were written (written \( d \leftrightarrow b \) are logically equivalent).
Reducio ad absurdum or rule of contradiction.

\[ d \iff (\text{false} \iff d) \]

Modus tollens.

\[ d \iff [b \iff (b \iff d)] \]

Law of the syllogism.

\[ (\mu \iff d) \iff [(\mu \iff b) \iff (b \iff d)] \]

Modus ponens or rule of detachment.

\[ b \iff [(b \iff d) \lor d] \]

\[ d \iff b \text{ and } b \iff d \iff b \iff d \]

\[ b \iff d \iff b \iff d \]

Some Easy Pieces
\[ ((\exists x \land \exists y) \lor (\exists z \land x) \lor (\exists y \land z)) = ((\exists x \land \exists y) \lor (\exists z \land x) \lor (\exists y \land z)) = ((\exists x \land \exists y) \lor (\exists z \land x) \lor (\exists y \land z)) \]

For example, an equivalent one where applies only to variables, can be used to transform any boolean expression into.

\[ b \land d = (b \lor d) \lor (b \land d) \]

\[ b \lor d = (b \land d) \lor (b \land d) \]

\text{DeMorgan's Laws}
The Principle of Duality: If \( s \), then \( \neg \neg s \).

- Note that \( 
eg \) is unchanged.
- False with true.
- True with false, and
  - \( \neg \) with \( \forall \).
  - \( \neg \) with \( \forall \).
  - \( \forall \) with \( \forall \).

Replacing each occurrence of \( p \) with \( s \) is the statement obtained from \( s \) by

The dual of \( s \) is the statement obtained from \( s \) by

Other than \( \forall \) and \( \forall \),

Let \( s \) be a statement and contain no logical connectives

Duality
For any set \( A \), \( \emptyset \subseteq A \).
- Is the empty set.

\( A \neq B \) but \( A \subseteq B \).
\( A \subseteq B \) and \( B \subseteq A \) means \( A = B \).

\( B \subseteq A \) means every element of \( B \) is an element of \( A \).

\( A \not\in x \) means \( x \) is not an element of \( A \).

\( x \in A \) means \( x \) is an element of \( A \).

Let \( A \) and \( B \) be sets.

Set Theory
\( \emptyset = A \cup \emptyset \) •

\( A \text{ and } B \text{ are disjoint if } A \cup B = \emptyset. \) •

\( \{ (A \not\ni x \lor B \ni x) \land (B \not\ni x \lor A \ni x) : x \} \)

\( A \Delta B \) is the symmetric difference of \( A \) and \( B \), or

\( A \cap B \) is the intersection of \( A \) and \( B \). •

\( A \cup B \) is the union of \( A \) and \( B \). •

Set Operations
\[ \{ I \in \mathcal{F} \mid \text{for all} \, x : \mathcal{F} \in \mathcal{F} \} = \mathcal{F} \cap \mathcal{F} \] 

\[ \{ I \in \mathcal{F} \mid \text{for some} \, x : \mathcal{F} \in \mathcal{F} \} = \mathcal{F} \cap \mathcal{F} \] 

\[ \{ B \not\in x \lor \mathcal{F} \in \mathcal{F} \} = B - \mathcal{F} \] 

Set Operations (continued)
\[ I \subseteq A \bigcap \subseteq I \bigcup = I \bigcup \subseteq I \bigcap \subseteq A \bigcup = A \bigcup \subseteq A \bigcap \]

DeMorgan’s Laws
\[ \{ \cdots, 2, 1, 0, 1, -1, \cdots \} = \mathbb{Z} \]
\[ \{ \cdots, 1, 0, 1, \cdots \} = \mathbb{N} \]

Common Sets
The Well-Ordering Principle
Richard Dedekind (1831–1916) and Giuseppe Peano (1858–1932).

Then \( S(\forall u)(\exists z \in \mathbb{Z}^+) \) is true for all \( u \in \mathbb{Z}^+ \).

\( \forall z \in \mathbb{Z}^+ \) chosen

\( \forall z \in \mathbb{Z}^+ \) chosen

Whenever \( S(y)(\exists x \in \mathbb{Z}^+) \) is true for arbitrarily chosen \( u \in \mathbb{Z}^+ \),

\( \exists x \in \mathbb{Z}^+ \) denote an open mathematical statement

Mathematical Induction
\[ \emptyset = \mathcal{P} \]

So \( P \).

**It follows that** \( S(\emptyset) \) **is true, a contradiction.**

Because \( I \) \( \not\in \mathcal{P} \), \( \mathcal{P} \not\subset I \) **is true.**

Clearly \( I < I + 1 \) and, hence, \( I + 1 < I \) \( \in \mathbb{Z}^+ \).

\( \mathcal{P} \) has a least element \( I \) by the well-ordering principle.

**Assume that** \( \emptyset \not\in \mathcal{P} \).

**Let** \( \{ t \in \mathbb{Z}^+ : t \not\in \forall \} = \mathcal{P} \).

The proof
Mathematical induction is merely a property of integers.

"Everyday!"

Sun rises on Monday, on Tuesday, etc., so it must rise.

induction in the physical and empirical sciences.

Mathematical induction has nothing to do with

Philosophical Issues
\[ F_{1+\gamma H} = (1+\gamma H + \gamma H)_{1+\gamma H} = \]

\[ 1+\gamma H + 1+\gamma H = 1+\gamma H + 1+3 \]

Inductively, \[
F_{1+3} = 1 = 1+3, \quad F_{1+1} = 1+1 = 2, \quad F_{1+0} = 1+0 = 1
\]

Claim: \[
F_{1+u} = F_{1} + u \quad \text{for} \quad 3 < u < 1\]

Let \[
F_{1+u} + F_{1-u} = F_{1} + u \quad \text{and} \quad F_{1} = 1
\]

Fibonacci Numbers (1203)
There are infinitely many primes.

Divisors are itself and 1.

A prime is a positive integer larger than 1 whose only

\[ a \neq q \text{ or } 0 \neq a \text{ where } a \in \mathbb{Z}, \text{where } gcd(a, q) < 0 \]

\[ \text{such that there exists unique } a, q \in \mathbb{Z} \text{ and } a \text{ is a divisor of } q \]

\[ q | a \text{ means that } q \text{ divides } a, \text{where } a, q \in \mathbb{Z} \text{ and } 0 \neq q \]

Fundamental Integer Arithmetics
\[
\mathcal{A} \times \cdots \times \mathcal{A} \times \mathcal{A} = \mathcal{A}^n \quad \mathcal{A}
\]

\[
\{ \cdots \mathcal{A} \ni a_1 \in (a_1, a_2, \cdots, a_n) \} = \mathcal{A} \times \cdots \times \mathcal{A}^2 \times \mathcal{A}
\]

In general,

\[u \times w = |\mathcal{B} \times \mathcal{A}|\]

then \(u = |\mathcal{B}|\) and \(w = |\mathcal{A}|\) if

\[
\{ B \ni q \ni q \ni a : (q, a) \} = B \times A
\]

The Cartesian product of \(A\) and \(B\) is

Let \(A\) and \(B\) be two sets.

Cartesian Products
Relations

- A subset of \( A \times B \) is called a relation from \( A \) to \( B \).
- Each one of the \( mn \) 2-tuples \((a, b) \in A \times B\) can be either in the relation or not.

- If \(|A| = m\) and \(|B| = n\), then there are \(2^{mn}\) relations from \( A \) to \( B \).
- For example, \(\{(a, b) : a < b, \text{ where } a, b \in \mathbb{N}\} \subset \mathbb{N} \times \mathbb{N} \).

- A relation can be \(\emptyset\).
- In particular, a subset of \( A \times A \) is called a binary relation on \( A \).
\{ x \in A : (\forall y \in B) \exists z \in A (x = f(z)) \} = (\forall y \in B) \exists z \in A (x = f(z))

In general, the image of a function under a relation $q$ is called the image of a function under $q$, whereas a is $q = (\forall y \in B) \exists z \in A (x = f(z))$.

A function is a relation from $A$ to $B$ in which is a function of $f$.

The codomain of $f$ is called the domain and is called the domain.

$A \leftarrow f : B \rightarrow A$ from $A$ to $B$ is denoted by $f$ (mapping). A function (mapping) is denoted by $f : A \rightarrow B$.

Let $A$, $B$ be nonempty sets.

Functions
\[ u^{\cdot} = u \times \ldots \times u \times u \]\n
Hence the desired number is

\[ q = (n) f \] in the codomain \( B \) to make

For each \( a \) in the domain \( A \), there are \( n \) choices of \( q \) functions from \( A \) to \( B \).

\[ u^{\cdot} \]

If \( u = |B| \) and \( u^{\cdot} = |A| \) then there are

Number of Functions
George Boole (1815–1864).

- Alternative proof: The truth table has \( 2^n \) rows.
- By the previous slide with \( m = 2^u \) and \( n = 2^v \).

Boolean functions.

\[ 2^u \times 2^v \]

- There are \( 2^m \) function from \( \{0, 1\}^m \) to \( \{0, 1\} \).
- For example, \( f(x_1, x_2) = \overline{x_1} \lor x_2 \) is a boolean function.

Application: Number of Boolean Functions

A function from \( \{0, 1\}^m \) to \( \{0, 1\}^n \) is called a boolean function.
\[ f \] is a function. Whenver \( f \geq (\ell) \), the function \( f \) is monotone increasing.

**Application:** Monotone Increasing Functions
\[
\text{The number is } u = \binom{n}{u} \text{ when } u \geq n-1.
\]

\[
v = 1 + (z)f = (z)f, \quad 3 = 0 + (1)f = (z)f
\]

\[
v = z + (0)f = (1)f, \quad 1 = (0)f
\]

For \( u = 3 \) and \( u = w \), \( u = 6 \) and \( u = w \), \( \sum \).

Each such function corresponds to a permutation of

\[
\begin{cases}
\cdots & I \mid \cdots & 1 \mid \cdots & I \\
I-1 & \cdots & I & 1 \cdots
\end{cases}
\]

There are \( (n-1)^{u+w} \) such functions.

(continued)

Application: Monotone Increasing Functions
\[ x > (x)f \text{ satisfy } \{ 1 - u', \ldots, 1', 0 \} \leftarrow \{ u', \ldots, 2', 1 \} : f \]

Equivalently, how many monotone increasing functions

\[ x \geq (x)f \text{ satisfy } \{ u', \ldots, 2', 1 \} \leftarrow \{ u', \ldots, 2', 1 \} : f \]

How many monotone increasing functions

Application: Monotone Increasing Functions with
\[
\tau = \tau + (\tau)f = (\tau)f', \quad 0 = 0 + (0)f = (\tau)f
\]
\[
0 + (0)f = (0)f, \quad 0 = (0)f
\]

For \( u = 3, \tau = I, \tau = I' + I, \tau = I + I' + I', \tau = I' + I, \tau = I' + I'

Sums (p. 45).

Each such function corresponds to a permutation of such functions.

\[
\left( \begin{array}{c}
\binom{u}{u} \\
\binom{u}{1}
\end{array} \right) \frac{I + u}{I} = uq
\]

There are (continued)

Application: Monotone Increasing Functions with

\( x \geq (x)f\)
etc.

There are \( u \) choices for \( f \).

One-to-one functions from \( A \) to \( B \):

\[
(1 + u - u) \cdots (1 - u)u = (m; u)B
\]

Then there are

\[
w \geq u = |B| \text{ and } m = |A| \;
\]

If each element of \( B \) appears at most once as the image

\[
\text{of an element of } A
\]

A function \( B \mapsto f \) is called one-to-one or injective

One-to-One (Injective) Functions
\[ u > m \]

\( u \) equals \( 0 \) for \( m \).

- See p. 86 or p. 147 for proofs.

\[ \text{onto functions from } A \text{ to } B. \]

\[ w(\gamma - u)(\frac{\gamma - u}{u}) \gamma(1-\gamma) \sum_{u} \]

Then there are \( u = |B| \) and \( w = |V| \).

\[ x = (x)f \text{ where } \mathbb{R} \leftrightarrow \mathbb{R} : f - \]

Necessary.

\[ |\mathbb{V}| \geq |B| \quad B = (\mathbb{V})f \]

A function onto or surjective if

\[ \text{onto (Surjective Functions)} \]
\[ q = (n)f \]

- All the objects in the container labeled \( q \) singly
- Identity a distribution with an onto function.

Ways:

\[ u(y - u)\underbrace{(y - u)}_{u}(y - u)^{\sum_{0}^{y}} \]

- There are \( \bullet \)
- Left empty?
- How many ways are there to distribute \( m \) distinct objects into \( n \) distinct containers with no container empty?
- Distinct Objects into Distinct Containers with None Empty

Distinct Objects into Distinct Containers with None
James Stirling (1692-1770).

Simplify remove the labels on the containers.

(4) \( \sum_{u}^{\infty} (\gamma - u) \binom{\gamma - u}{u} \gamma (1 - \gamma)^{u} = \frac{1}{u} = (u, \gamma)_{S} \)

Then

- of the second kind
- The answer is denoted \( S(m, n) \), the Stirling number
- container left empty
- containers into \( m \) identical containers with no
- How many ways are there to distribute \( m \) distinct

Distinct Objects into Identical Containers
Stirling number of the second kind \( s(20, n) \)
Application: A Combinatorial Identity

\[ \sum_{k=0}^{n} (-1)^k \binom{n}{n-k} (n-k)^n = n!. \]

• There are

\[ \sum_{k=0}^{n} (-1)^k \binom{n}{n-k} (n-k)^n \]

number of onto functions from \( X \) to \( X \), where \(|X| = n\).

• But the number of such onto functions is also \( n! \).

• As the left-hand side of the identity equals \( n! S(n, n) \),

\[ S(n, n) = 1. \] (5)
other objects.

Object $a_{m+1}^+$ can be in a container all by itself or with

containers, with no containers left empty.

is distributed among identical

counts the number of ways

where $I \geq u > m$.

\[
(u, m) s_u + (1 - u, m) s = (u, I + w) s
\]

A Recurrence Relation for Stirling Numbers
A Recurrence Relation for Stirling Numbers (continued)

- \( S(m, n - 1) \) is the number of ways \( \{a_1, a_2, \ldots, a_m\} \) is distributed among \( n - 1 \) identical containers, with no containers left empty and with \( a_{m+1} \) alone in the remaining container.

- \( nS(m, n) \) is the number of ways \( \{a_1, a_2, \ldots, a_m\} \) is distributed among \( n \) identical containers, with no containers left empty and with \( a_{m+1} \) put in any of the \( n \) containers.
Therefore, they must be identical.

Therefore, they must be identical.

This proves the identity for \( x \in \mathbb{Z} \).

\( x = \left| \mathcal{B} \right| \) and \( w = \left| \mathcal{A} \right| \)

The number of functions from \( \mathcal{A} \) to \( \mathcal{B} \), which is \( \sum_{w}^{\mathcal{B}} \), is the number of functions of the form \( (1 + \gamma - x) \cdot \cdots \cdot (1 - x)x(\gamma,w)\).

\( w_{x} = (1 + \gamma - x) \cdot \cdots \cdot (1 - x)x(\gamma,w)\).

\( x = \sum_{w}^{\mathcal{B}} \)

An Identity for Stirling Numbers
\[(u', w)S = \sum_{u} \frac{u}{(u', w)S} = \sum_{u} \frac{i(u)}{(u', w)S} = \sum_{u} i(u) = \sum_{u} \frac{u}{(u', w)S} \]

\[(\ell - u) \sum_{\ell} \frac{i(\ell - u)}{(u', w)S} = \sum_{\ell} \frac{i(\ell - u)}{(u', w)S} \sum_{u} \frac{\ell}{(u', w)S} = \sum_{\ell} \frac{i(\ell - u)}{(u', w)S} \sum_{u} \frac{\ell}{(u', w)S} \]

\[\frac{i(u)}{I} \sum_{u} \frac{0 = u}{I} \sum_{u} \frac{0 = u}{I} = \sum_{u} \frac{0 = u}{I} \sum_{u} \frac{0 = u}{I} \]

\[(\ell - u) \sum_{\ell} \frac{i(u)}{(u', w)S} \sum_{\ell} \frac{u}{(u', w)S} = \sum_{\ell} \frac{i(u)}{(u', w)S} \sum_{\ell} \frac{u}{(u', w)S} \]

\[\sum_{u} \frac{u}{I} = \frac{1}{I} \sum_{u} u \]

\[\sum_{u} \frac{u}{I} \]

It suffices to prove Eq. (4).

Finally, proof of Eq. (3) with Eq. (6).
Indeed, $P^3 = 5$.

\[
\sum_{m=0}^{\infty} P^{\lambda} = \sum_{m=0}^{\infty} P^{\lambda} = u P
\]

Clearly, $\bullet$

\[
\begin{align*}
\{\{3\}\} & \{\{1\}\} \{\{2\}\} \{\{2\}\} \{\{3\}\} \{\{1\}\} \\
\{\{3\}\} & \{\{1\}\} \\
\{\{3\}\} & \{\{2\}\} \{\{1\}\} \\
\{\{3\}\} & \{\{2\}\} \{\{1\}\}
\end{align*}
\]

There are 5 ways to partition 3 distinct objects:

There are 5 distinct objects.

The $m$th Bell number $P^m$ is the number of partitions of $\bullet$

Bell Numbers
(7) \[
\frac{\mathcal{D}}{I} \frac{i\mathcal{L}}{u_{m}\mathcal{L}} \sum_{0}^{\infty} = \\
\frac{i(\mathcal{L} - \mathcal{Y})}{\mathcal{L} - \mathcal{Y}(I-I)} \sum_{\infty}^{0} \frac{i\mathcal{L}}{u_{m}\mathcal{L}} \sum_{0}^{\infty} = \\
\frac{u_{m}\mathcal{L}\left(\begin{array}{c}
\mathcal{L}\\
\mathcal{Y}
\end{array}\right)}{\mathcal{L} - \mathcal{Y}(I-I)} \sum_{\mathcal{Y}}^{0} \frac{i\mathcal{Y}}{I} \sum_{\infty}^{0} = u_{m}P
\]

A Formula for Bell Numbers
\[ d \left( \frac{\gamma}{1-u} \right) \text{ containing } \gamma \text{ elements is} \]
\[ = \frac{\gamma-\gamma_d}{1-u} \]
\[ \text{So the number of partitions in which the class} \]
\[ \text{space } \gamma \text{ ways.} \]
\[ \text{The remaining } \gamma - u \text{ elements can be partitioned in} \]
\[ = (1-u)^{\gamma-\gamma_d} \]
\[ \text{ways.} \]
\[ \text{A class with } \gamma \text{ elements and containing } x \text{ can be chosen} \]
\[ \text{Let } u = |S| \text{ and } \gamma \in S. \]
\[ (8) \quad \gamma_0 d \left( \frac{\gamma}{1-u} \right) = \gamma_0 d \left( \frac{\gamma}{1-u} \right) \]
\[ \text{A Recurrence Relation for Bell Numbers} \]
From $A$ to $B$. If $m = |\mathcal{B}| = |A|$ then there are $m$ bijective functions.

$|A| = |\mathcal{B}|$.

Necessarily, $\mathcal{B}$ is one-to-one and one-to-one correspondence if it is one-to-one and a function $f : A \rightarrow \mathcal{B}$ is called bijective or a

Bijective Functions
Set of squares integers: \[ \ldots, 1, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \ldots \]

Set of rational numbers.

Set of odd integers.

Set of positive integers \( \mathbb{Z}^+ \).

Set of integers \( \mathbb{Z} \).

A set is countable if it is finite or if it can be put in one-to-one correspondence with \( \mathbb{N} \), the set of natural numbers.

Infinite Sets
\[ |B| \neq |A| \text{ but } |B| \geq |A| \text{ if } |B| > |A| \]

and \( B \) is subset of \( A \) if there exists a one-to-one correspondence between \( A \) and \( B \).

\[ |B| \geq |A| \text{ if there exists a one-to-one correspondence between their elements.} \]

Two sets are said to have the same cardinality (written as \(|C| \neq |D| \) for any set \( C \), define \(|C| \) as \( C \)'s cardinality (size)).

- If \( |A| = \mathbb{Z}_+ \) and \( |A| = \mathbb{Z}_- \), then:
  \[ \mathbb{Z} = \mathbb{Z}_+ \cup \mathbb{Z}_- \]
- \( \mathbb{Z} \) denotes the power set of \( \mathbb{Z} \), that is \( \{ A \subseteq \mathbb{Z} : \mathbb{Z} \} \).
- Let \( A \) denote a set.

Cardinality
A lot of "paradoxes":

- The set of odd integers.
  - But the set of integers has the same cardinality as the set of odd integers.
  - The set of integers properly contains the set of odd integers.

\[ |B| = |A| \]

If \( A \) and \( B \) are infinite sets, it is possible that \( A \subset B \).
is not a bijection, a contradiction.

Hence $B$ for any $u$.

If $u \in B$, then $u \not\in B$ by $B$'s definition.

If $u \not\in B$, then $u \not\in B$ by $B$'s definition.

Suppose that $B = (u)f$.

Consider the set $B = \{ (u)f \not\in N : N \in \mathcal{B} \}$.

Suppose it is countable with $f : \mathbb{N} \rightarrow \mathbb{N}$ being a bijection.

The set of all subsets of $\mathbb{N}$ is infinite and

Cantor's Theorem
As there are functions for which there are no \( f \in \mathbb{N} \), the \( |\mathbb{N}| > |\mathbb{N}| \).

\[ \mathbb{N} \ni \{ i = (\forall)f : ? \} - \]

Cardinality is a subset of \( \mathbb{N} \).

As each function uniquely defines a subset of \( \mathbb{N} \),

\( \{0, 1\} \) Now consider functions from \( \mathbb{N} \) to \( \{0, 1\} \).

It follows that the set of programs is as large as \( \mathbb{N} \).

Every program is a series of 0s and 1s, thus a nonnegative integer.

Application: Existence of Uncomputable Problems
Hilbert’s Paradox of the Grand Hotel

David Hilbert (1862–1943).

The new customer occupies Room 1.

"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 ....

A new guest comes and asks for a room.

Now let us imagine a hotel with an infinite number of rooms, and all the rooms occupied, a new guest will be turned away.

For a hotel with a finite number of rooms with all the rooms occupied, a new guest will be turned away.
(John 14:3).

There are many rooms in my Father’s house, and I am

infinite or new guests can be accommodated in them.

Now all odd-numbered rooms become free and the

occupant of Room 2 into Room 4, and so on.

He moves the occupant Room 1 into Room 2, the

minute.

Certainly, gentlemen,” says the proprietor, “just wait a

guests who come in and ask for rooms.

Let us imagine now a hotel with an infinite number of

Hilbert’s Paradox of the Grand Hotel (continued)
Galileo (1564–1642), mathematicians.

Resolution of paradoxes: Which notion results in better

greater than any of its proper parts.

This is contrary to the axiom of Euclid that the whole is

Correspondence with all the positive integers.

The squares of the positive integers can be placed in 1–1

Galileo's Paradox (1638)
What gives?

But Cantor’s theorem says $|L| < |\mathcal{P}(L)|$.

We conclude that $|L| \geq |\mathcal{P}(L)|$.

$\mathcal{P}(L)$ is a set of sets, hence $\mathcal{P}(L) \subseteq \mathcal{P}(\mathcal{P}(L))$.

Any set imaginable: set of apples, set of cars, etc. —

Let $L$ be the set of all sets.

Cantor’s Paradox (1899)

If $S \notin S$, then $S \notin S$ by the definition.

If $S \notin S$, then $S \notin S$ by the definition.

Consider the set $\{x \notin x : x \in x\} = S$.
For the other \( m \)\(^2 \) \( \neq m \) pairs of \( A \times A \) is arbitrary.

\( \forall R \in \mathcal{R} \), membership in \( R \) is reflexive relations on \( A \),

\[
\exists m \in \mathbb{Z} - m
\]

If \( m = |A| \) then there are \( 2^{|A|^2} - m \) is reflexive.

\[ \subseteq \text{ is reflexive if } R \ (x, x) \ (x, x) \text{ for all } x \in A. \]

\( \forall \ R \in \mathcal{R} \) \( R \) is reflexive if \( A \times A \subseteq R \) is a relation on \( A \).
There are \( 2^{(m^2 - m)} \) reflexive, symmetric relations on \( A \). \( \therefore \)

\[
\frac{2}{(m + m^2)} = \frac{2}{(m - m^2)} + m
\]

\[
\frac{2}{(m + m^2)} = \frac{2}{(m - m^2)} + m
\]

\[
\]
to derive, unfortunately.

Number of transitive relations on a finite set is not easy.

\[ \Rightarrow \text{is transitive.} \]

\[ x, y, z \in A. \]

\[ \forall y \in \mathcal{R} \quad \mathcal{R}(z, x) \iff \mathcal{R}(z', y) \quad (\mathcal{R}, x) \quad \text{is transitive.} \]

Transitive Relations
Peter Gustave Lejeune Dirichlet (1805–1859).

With \( m < n \), at least one pigeon is “homeless.” With \( m \) pigeons and \( n \) single-occupancy pigeonholes

- exist a student with a score at least 70.
- If the average score in a class is 70, then there must
  - If \( n \) pigeons occupy \( m \) pigeonholes and \( m < n \), at least
  - If \( m \) pigeons occupy two or more pigeonholes roosting in it.

The Pigeonhole Principle
Pick \( u = t - s \) to finish the proof.

Because \( m \) is odd,

\( m \mid 2^{t-s} - 1 \), i.e., \( m \mid (2^{t-s} - 1)2^s \).

Therefore exist \( s > t \) such that \( 2^s \equiv 1 \mod m \).

Consider \( m + 1 \) integers \( \{2^1 - 1, 2^2 - 1, \ldots, 2^m + 1 - 1\} \).

Integer \( u \) such that \( m \mid 2^u - 1 \).

**Lemma 4.** Let \( m \in \mathbb{Z}^+ \) be odd. Then there exists a positive divisor.
transitive subtournament on \( m \) of the \( n \) players?

What is a number \( m \) that guarantees the existence of a

\[ \binom{n}{2} \]


game.

There are \( \binom{n}{2} \) games.

Consider an arbitrary tournament with \( n \) players.

Players can be ranked.

If a tournament is furthermore transitive, then the

\( \text{is not reflexive} \)

\[ \forall x \in \mathcal{R}, (x, h) \in \mathcal{R} \]

or \( (h, x) \in \mathcal{R} \), either \( x \neq h \).

For all \( x \), either \( x \neq h \).

\[ \mathcal{R} \text{ is a tournament} \]

Application: Tournaments
\( \sum_{\log_2 n} u \geq 1 \). 

This establishes the theorem because then \( u(n) \).

\[ L_{\text{transitive tournament on } n \text{ players}} \]

We shall show that a tournament on \( n \) players exists.

\[ \left\lfloor \log_2 n \right\rfloor + 1 \geq u(n) \]

Theorem 5 (Bridges and Moser, 1964)

Subtournament on \( m \) players.

Tournament on \( n \) players contains a transitive tournament on \( n \) players, and there exists an integer \( m \) such that every tournament on \( m \) players contains a transitive tournament on \( m \) players.

Let \( u(n) \) be the largest integer \( m \) such that every tournament on \( m \) players contains a transitive tournament on \( m \) players.

Application: Tournaments (continued)
transitive subtournament on \( n \) players.

So there exists a tournament on \( n \) players without a

the total number of tournaments on \( n \) players.

\[
\binom{\frac{n}{2}}{\frac{n}{2}} > \binom{\frac{n}{2}}{\frac{n}{2}} - \frac{n}{2}! \binom{n}{n}\]

contains a transitive subtournament on \( n \) players.

The total number of tournaments on \( n \) players that

possible tournaments on \( n \) players.

with a subtournament on \( n \) players fixed, there are

there are \( \frac{n}{2} \) possible tournaments on \( n \) players.

The Proof (continued)
Theorem 6

There exists a constant $c$ such that

$\exists (x_1, x_2, \ldots, x_u)$ has formula size at most $cn \log n$.

We can do much better.

$$(\forall x \lor \exists x \lor \forall x) \land \cdots \land (\forall x_1 \lor \exists x_2 \lor \forall x_3) = (x_1, x_2, \ldots, x_u) \leq cn \log n$$

One possible formula

at least 3 of the $x_i$'s are 1's and 0 otherwise.

Define the boolean function $\exists (x_1, x_2, \ldots, x_u)$ to be 1 if

Application: Compact Threshold Boolean Formulas
The total number of possible $\mathcal{F}$ is $3^m$.

- Each $\mathcal{F}$ has exactly $m$ variables.

\[ (\bigwedge x \land \bigvee \bar{x}) \lor (\forall x \land \exists \bar{x}) \lor (\exists \bar{x} \land \forall x \land \bigvee \bar{x}) = \mathcal{F} \]

For example,

- Each $x$ is placed within one of the brackets.

\[ (\cdots \land) \lor (\cdots \land) \lor (\cdots \land) = \mathcal{F} \]

Form

Construct formula $\mathcal{F} \land \cdots \land \mathcal{F} = \mathcal{F}$

The Proof
is correct if every possible \( x \) appears in it.

\[
(\forall x \lor \exists x \lor \exists x) \land \cdots \land
(\forall x \lor \exists x \lor \exists x) \land (\exists x \lor \exists x \lor \exists x) =
(\forall x \land \exists x) \lor (\exists x \land \exists x) \lor (\exists x \land \exists x \land \exists x)
\]

For example, \( q \), \( r \), \( c \).

The proof (continued)
\[ u \left( \frac{d}{\partial x} \right) \]

The number of ways that \( x^a, x^b, x^c \) do not appear in any

\[ u \left( \frac{d}{\partial x} \right) = u \left( \frac{d}{\partial x} \right) - \]

That number equals

not thrown into distinct brackets.

appears in \( \mathcal{H} \) if the number of ways that \( x^a, x^b, x^c \) are

The number of ways that any given \( x^a \) or \( x^b \) does not
\[ \text{Pick } t = \log u, \quad \log(\nu) = (\frac{\nu}{2})^{6/7} \]

The ensuing formula has size \( (u, \nu) \).

The ensuing formula makes \( H \) includes all \( \frac{\nu}{u} \) monomials, making \( H \) correct.

There must exist a choice of \( H, H', \ldots \) that

\[ \nu \varepsilon > \nu(\frac{\nu}{u})^{\frac{6}{7}} \nu \]

Then \( \nu \)** \( (6/7) \nu \). Suppose \( \nu \geq 1 \).

Suppose \( \nu \geq (\frac{6}{7}) \nu \).

The number of ways that at least one of the \( \nu \geq \)(continued)