Combinatorics and "Higher" Mathematics
For relaxation,

General Bradley did algebra problems,
and he worked at integral calculus
when he was flying an airplane
— or flying in his airplane.
He said it relaxed him, made him think.

— Chet Hansen, Major,
aide to 5-star General Omar Bradley (1893–1981)
### Growth of Factorials

<table>
<thead>
<tr>
<th>( n )</th>
<th>( n! )</th>
<th>( n )</th>
<th>( n! )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>8</td>
<td>40320</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>9</td>
<td>362880</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>10</td>
<td>3628800</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>11</td>
<td>39916800</td>
</tr>
<tr>
<td>4</td>
<td>24</td>
<td>12</td>
<td>479001600</td>
</tr>
<tr>
<td>5</td>
<td>120</td>
<td>13</td>
<td>6227020800</td>
</tr>
<tr>
<td>6</td>
<td>720</td>
<td>14</td>
<td>87178291200</td>
</tr>
<tr>
<td>7</td>
<td>5040</td>
<td>15</td>
<td>1307674368000</td>
</tr>
</tbody>
</table>
A Logplot (Base Two)

Logplot of $n!$
A Useful Lower Bound for $n!$

**Lemma 23** $n! > (n/e)^n$.

*Proof:*

$$\ln(n!) = \ln 1 + \ln 2 + \ln 3 + \cdots + \ln n$$

$$= \sum_{k=1}^{n} \ln k$$

$$> \sum_{k=1}^{n} \int_{k-1}^{k} \ln x \, dx \quad \text{as } \ln x \text{ is increasing}$$

$$= \int_{0}^{n} \ln x \, dx$$

$$= [x \ln x - x]_{x=0}^{n}$$

$$= n \ln n - n.$$
\[ \ln x \]
Conclusion: good but probably not of the same order as $n!$. 
A Marginally Better Bound

Lemma 24 \( n! > e^{(n/e)^n} \).

Proof:

\[
\ln(n!) = \ln 1 + \ln 2 + \ln 3 + \cdots + \ln n
\]

\[
= \sum_{k=2}^{n} \ln k
\]

\[
> \sum_{k=2}^{n} \int_{k-1}^{k} \ln x \, dx
\]

\[
> \int_{1}^{n} \ln x \, dx
\]

\[
= [x \ln x - x]_{x=1}^{n}
\]

\[
= n \ln n - n + 1.
\]
A Useful Upper Bound for $C(n, m)$

**Lemma 25** $C(n, m) < (ne/m)^m$ for any $0 < m < n$.\(^a\)

**Proof:**

\[
C(n, m) = \frac{n!}{(n-m)! \cdot m!} = \frac{n(n-1) \cdots (n-m+1)}{m!} \leq \frac{n^m}{m!} < \frac{n^m}{(m/e)^m} \text{ by Lemma 23 (p. 132)} = (ne/m)^m.
\]

\(^a\)Obtain the slightly tighter bound $(ne/m)^m/e$ with Lemma 24 (p. 135).
Stirling’s Formula\textsuperscript{a} (1730)

- The notation \( f(x) \sim g(x) \) means

\[
\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1,
\]

i.e.,

\[
f(x) = g(x) + o(g(x))
\]

as \( x \to \infty \).\textsuperscript{b}

- Stirling’s formula says:

**Theorem 26** \( n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \).

**Corollary 27** \( e = \lim_{n \to \infty} n / (n!)^{1/n} \).

\textsuperscript{a}James Stirling (1692–1770); but actually due to Abraham DeMoivre (1667–1754)!

\textsuperscript{b}It does not imply \( f(x) - g(x) \to 0 \).
Goodness of Approximation to $n!$
Approximation of $C(n, m)$

- Stirling’s formula can be used to approximate $C(n, m)$ better than Lemma 25 (p. 136) under some conditions.

- For that purpose, a more refined Stirling’s formula is stated below without proof:

$$\sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\frac{1}{12n}}. \quad (20)$$

---

<sup>a</sup>Robbins (1955).
The Proof (concluded)

• Now from inequalities (20) on p. 139,

\[
C(n, m) = \frac{n!}{(n-m)! \cdot m!} < \sqrt{\frac{2\pi n}{n}} \left( \frac{n}{e} \right)^n e^{\frac{1}{12n}} \frac{\sqrt{2\pi (n-m)}}{\sqrt{2\pi m}} \left( \frac{m}{e} \right)^m e^{\frac{1}{12m+1}} \\
= \frac{1}{\sqrt{2\pi}} \left( \frac{n}{m} \right)^m \left( \frac{n}{n-m} \right)^{n-m} \sqrt{\frac{n}{m(n-m)}} \times e^{\frac{1-12n-144(m-n)^2-144mn}{(\ldots)(\ldots)(\ldots)}} \sqrt{\frac{n}{m(n-m)}}.
\]
Approximation of $C(n, m)$, $1 \leq m \leq n/2$

\[
C(n, m) \geq \frac{1}{\sqrt{2\pi}} \left( \frac{n}{m} \right)^m \left( \frac{n}{n-m} \right)^{n-m} \sqrt{\frac{n}{m(n-m)}} e^{\frac{1}{12n+1} - \frac{1}{12(n-m)} - \frac{1}{12m}}
\]

\[
= \frac{1}{\sqrt{2\pi}} \left( \frac{n}{m} \right)^m \left( \frac{n}{n-m} \right)^{n-m} \sqrt{\frac{n}{m(n-m)}} e^{-\frac{12m-1}{12(n-m)(12n+1)} - \frac{1}{12m}}
\]

\[
\geq \frac{1}{\sqrt{2\pi}} \left( \frac{n}{m} \right)^m \left( \frac{n}{n-m} \right)^{n-m} \sqrt{\frac{n}{m(n-m)}} e^{\frac{-12m-1}{12m(24m+1)} - \frac{1}{12m}}
\]

\[
= \frac{1}{\sqrt{2\pi}} \left( \frac{n}{m} \right)^m \left( \frac{n}{n-m} \right)^{n-m} \sqrt{\frac{n}{m(n-m)}} e^{-\frac{1}{6m} + \frac{1}{(24m+1)}}
\]

\[
\geq \frac{1}{\sqrt{2\pi}} \left( \frac{n}{m} \right)^m \left( \frac{n}{n-m} \right)^{n-m} \sqrt{\frac{n}{m(n-m)}} e^{-\frac{1}{6m}}. \quad (22)
\]
The Proof (continued)

- Combining inequalities (21) on p. 140 and (22) on p. 141 under $1 \leq m \leq n/2$, we conclude that

$$e^{-\frac{1}{6m}} \frac{1}{\sqrt{2\pi}} \left( \frac{n}{m} \right)^m \left( \frac{n}{n-m} \right)^{n-m} \sqrt{\frac{n}{m(n-m)}}$$

$$< C(n, m)$$

$$< \frac{1}{\sqrt{2\pi}} \left( \frac{n}{m} \right)^m \left( \frac{n}{n-m} \right)^{n-m} \sqrt{\frac{n}{m(n-m)}}.$$
The Proof (concluded)

• So

\[
C(n, m) \sim \frac{1}{\sqrt{2\pi}} \left( \frac{n}{m} \right)^m \left( \frac{n}{n - m} \right)^{n-m} \sqrt{\frac{n}{m(n-m)}}
\]  

(23)

as \(m \to \infty\) and \(n - m \to \infty\).

• An alternative formulation is

\[
C(n, m) \sim \frac{1}{\sqrt{2\pi pq n}} (pq)^{-n},
\]

where \(p \triangleq \frac{m}{n}\) and \(q \triangleq 1 - p\).
Application: Probability of Return to Origin

• Suppose the binomial random walk has a probability of $2^{-1} = 0.5$ of going in either direction (p. 47).
  – This is called a symmetric random walk.

• The number of ways it is at the origin after $2n$ steps is $\binom{2n}{n}$ by Eq. (4) on p. 44.\textsuperscript{a}

• The probability for this to happen is

$$
\frac{\binom{2n}{n}}{2^{2n}} \approx \frac{1}{\sqrt{2\pi}} \frac{2^n 2^n}{2^{2n}} \sqrt{\frac{2}{n}} \approx \sqrt{\frac{1}{\pi n}} = O \left( \frac{1}{\sqrt{n}} \right)
$$

by Eq. (23) on p. 143.

\textsuperscript{a}We have seen $\binom{2n}{n}$ many times before (e.g., p. 57, p. 61, p. 119, and p. 123). We will continue to encounter it.
Application: Probability of Return to Origin (concluded)

- Suppose 100 U.S. Senators vote on a bill randomly.¹
- What is the probability of a tie (which has to be broken by the Vice President)?
- By Eq. (24), it equals

\[ \frac{\binom{100}{50}}{2^{100}} = 0.0795892 \approx \frac{1}{12}. \]

- The probability is surprisingly high.
- It rises to 0.176197 with 20 Senators in late 18th century.

Application: Deviation

• Consider the symmetric random walk again.

• Its average position at the end is 0.

• Assume $n$ is even.

• Given $c > 0$, after $n$ steps what is the probability for the walk to end at a position $\geq c\sqrt{n}$ for $n$ sufficiently large?
Application: Deviation (continued)

- The probability that the walk ends at position $k$ after $n$ steps is

$$\left( \frac{n}{n+k} \right)^2 2^{-n}$$

by Eq. (4) on p. 44, where $k$ is even.

- The probability that $k \geq c\sqrt{n}$ is about

$$\sum_{k=\lceil c\sqrt{n} \rceil}^{n} \left( \frac{n}{n+k} \right)^2 2^{-n} \approx \frac{1}{2} - \sum_{k=2}^{\lfloor c\sqrt{n} \rfloor} \left( \frac{n}{n+k} \right)^2 2^{-n}$$

by Eq. (9) on p. 58.

- The integer $k$ must also be even.
Application: Deviation (concluded)

• But

\[
\frac{1}{2} - \sum_{k=2}^{\lfloor c\sqrt{n} \rfloor} \left( \frac{n}{n+k} \right)^2 - n \geq \frac{1}{2} - 2^n \frac{c\sqrt{n}}{2} \left( \frac{n}{2} \right)
\]

according to the unimodal property (p. 28).\(^a\)

– That \(k\) is even accounts for the 2 in the denominator.

• Finally, the desired probability is

\[
\frac{1}{2} - 2^n \frac{c\sqrt{n}}{2} \left( \frac{n}{2} \right) \geq \frac{1}{2} - c\sqrt{\frac{1}{2\pi}}
\]

by Eq. (24) on p. 144 for \(n\) sufficiently large.

\(^a\)Corrected by Mr. Gong-Ching Lin (B00703082) on March 8, 2012 and Mr. Rajon Geng (B03902010) on March 5, 2016.
An Upper Bound for $C(2n, n)$

**Lemma 28** \( \binom{2n}{n} < \frac{4^n}{\sqrt{n\pi}} \).

Proof: From inequality (21) on p. 140,

\[
\binom{2n}{n} < \frac{1}{\sqrt{2\pi}} \left( \frac{2n}{n} \right)^n \left( \frac{2n}{2n-n} \right)^{2n-n} \sqrt{\frac{2n}{n(2n-n)}}
\]

\[= \frac{1}{\sqrt{n\pi}} 4^n.\]

Note that Lemma 25 (p. 136) gives a much looser upper bound of $(2e)^n \sim 5.43656^n$. 
A Tight Bound for $C(2n, n)$

Lemma 29 $\binom{2n}{n} \sim 4^n / \sqrt{n\pi}$.

- From inequality (22) on p. 141,

\[
\binom{2n}{n} > \frac{1}{\sqrt{2\pi}} \left( \frac{2n}{n} \right)^n \left( \frac{2n}{2n-n} \right)^{2n-n} \sqrt{\frac{2n}{n(2n-n)}} e^{-\frac{1}{6n}}
\]

\[
= \frac{1}{\sqrt{n\pi}} 4^n e^{-\frac{1}{6n}}.
\]

- Finally, recall Lemma 28 (p. 149).
A Tight Bound for $C'(2n, n)$ (concluded)

$\binom{2n}{n}/(4^n/\sqrt{n\pi})$
First Return to Origin

What is the probability a symmetric binomial random walk returns to the origin the first time at step $2n$?

- From Eq. (19) on p. 125, the probability is
  \[ 2^{-2n} \frac{1}{2n - 1} \binom{2n}{n}. \]
- The above probability is asymptotically
  \[ \sim \frac{1}{2\sqrt{n^3\pi}} \]
  by Lemma 29 (p. 150).

\(^a\)Recall p. 124.
Analytic Number Theory
A proof is that which convinces a reasonable man; a rigorous proof is that which convinces an unreasonable man.

— Mark Kac (1914–1984)
There Are an Infinite Number of Primes

Theorem 30 (Euclid, 300 B.C.) There are infinitely many primes.

- A prime is a positive integer larger than 1 whose only divisors are itself and 1.
- Suppose $p_1, p_2, \ldots, p_k$ are all the primes.
- Let $B = p_1 p_2 \cdots p_k + 1$.
- Because $B > p_i$ for all $i$, $B$ cannot be a prime.

---

Euclid (325 B.C.–265 B.C.). Some claim this is the most important result in all mathematics, such as Calude (1994).
The Proof (concluded)

- So there must be a prime $p_j$ such that $p_j$ divides $B = p_1p_2 \cdots p_k + 1$.
- But that implies $p_j$ must divide 1, a contradiction.
There Are an Infinite Number of Primes: An Alternative Proof\textsuperscript{a}

- Every number $n$ can be uniquely factorized into prime factors $p_1^{k_1} p_2^{k_2} \cdots$.

- So

  \[
  \left( \sum_{k=0}^{\infty} \frac{1}{2^k} \right) \left( \sum_{k=0}^{\infty} \frac{1}{3^k} \right) \left( \sum_{k=0}^{\infty} \frac{1}{5^k} \right) \cdots
  \]

  \[
  = \sum_{n \geq 1} \frac{1}{n}.
  \]

\textsuperscript{a}Leonhard Euler (1707–1783) in 1737.
The Proof (concluded)

• The right-hand side is an infinite number (why?).

• The left-hand side equals

\[
\frac{1}{1 - (1/2)} \frac{1}{1 - (1/3)} \frac{1}{1 - (1/5)} \cdots
\]

• It is an infinite number only if the number of primes is infinite.
Leonhard Euler (1707–1783)
The Prime Number Theorem\textsuperscript{a}

Let $\pi(n)$ stand for the number of primes up to $n$.

**Theorem 31** $\pi(n) \sim n/\ln n$.

**Corollary 32** The average density of primes from 1 to $n$ is $1/\ln n$.

**Corollary 33** The $n$th prime number is about $n \ln n$.

What is truth?
— John 18:38

Probably only a person with some mathematical knowledge would think of beginning with 0 instead of with 1.
Propositional Logic: Connectives

- \( \neg p \): the negation of statement \( p \).
- \( p \land q \): the **conjunction** of statements \( p \) and \( q \).
  - “\( p \) and \( q \)”
- \( p \lor q \): the **disjunction** of statements \( p \) and \( q \).
  - “\( p \) or \( q \)”
- \( p \rightarrow q \): the (material) **implication** of \( q \) by \( p \).
  - “Hypothesis \( p \) implies conclusion \( q \)” ; “if \( p \), then \( q \)”.
- \( p \leftrightarrow q \): the **biconditional** of \( p \) and \( q \).
  - “\( p \) if and only if \( q \)”

\(^{a}\)Attributed to Gottfried Wilhelm Leibniz (1646–1716).
Gottfried Wilhelm Leibniz (1646–1716)
Truth Table\textsuperscript{a}

- A truth table with \textit{n primitive statements} or boolean variables has $2^n$ rows or truth assignments.
  - For example, the compound statement
    \[ (p \lor (p \land q)) \land \neg r \]
    contains 3 primitive statements $p, q, r$.

- A truth table gives a statement a truth value under all possible truth assignments.
  - The truth table for $p \lor (p \land q) \land \neg r$ contains $2^3 = 8$ truth assignments.

\textsuperscript{a}Post (1921); Wittgenstein (1922). 1 and $T_0$ are used to denote true; 0 and $F_0$ are used to denote false.
Truth Tables of Connectives\(^a\)

<table>
<thead>
<tr>
<th></th>
<th>(p)</th>
<th>(\neg p)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>(p)</th>
<th>(q)</th>
<th>(p \land q)</th>
<th>(p \lor q)</th>
<th>(p \rightarrow q)</th>
<th>(p \leftrightarrow q)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</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>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<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>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

\(^a\)They are definitions.
### The Truth Table for \((p \lor (p \land q)) \land \neg r\)

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(p)</td>
<td>(q)</td>
<td>(r)</td>
<td>(p \land q)</td>
<td>(\neg r)</td>
<td>(p \lor (p \land q))</td>
<td>((p \lor (p \land q)) \land \neg r)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Tautology\textsuperscript{a} and Contradiction

- A statement is a \textit{tautology} if it is true for all truth assignments for its component primitive statements.
  - For example, $p \lor \neg p$.
  - Note that tautology is a \textit{metalogical} statement.

\textsuperscript{a}Wittgenstein (1889–1951) in 1922. Wittgenstein is one of the most important philosophers of all time. Russell (1919), “The importance of ‘tautology’ for a definition of mathematics was pointed out to me by my former pupil Ludwig Wittgenstein, who was working on the problem. I do not know whether he has solved it, or even whether he is alive or dead.” “God has arrived,” the great economist Keynes (1883–1946) said of him on January 18, 1928. “I met him on the 5:15 train.”
Tautology and Contradiction (continued)

- A statement is a **contradiction** if it is false for all truth assignments for its component primitive statements.

- When \( p \rightarrow q \) is a tautology, we say \( p \) **logically implies** \( q \), written as \( p \Rightarrow q \).
  
  - Note that \( p \Rightarrow q \) is a metalogical statement.

- If

\[
(p_1 \land p_2 \land \cdots \land p_n) \rightarrow q
\]

is a tautology, we say conclusion \( q \) follows **validly** from premises \( p_1, p_2, \ldots, p_n \).
Tautology and Contradiction (concluded)

- Verifying a tautology can be done by checking if all entries of the truth table give a true.

- Verifying a contradiction can be done by checking if all entries of the truth table give a false.

- But neither is efficient: Both take an exponential amount of time.\(^a\)

- A statement is a \textit{contingency} if it is neither a tautology nor a contradiction.

\(^a\)Both are known computationally hard problems; they are \texttt{coNP-complete} (Cook, 1971).
Ludwig Wittgenstein (1889–1951)

Wittgenstein (1922),
“Whereof one cannot speak, thereof one must be silent.”
Richard Karp, “It is to our everlasting shame that we were unable to persuade the math department [of UC-Berkeley] to give him tenure.”

An Example of a Valid Argument

$q$ follows validly from

$$(p \rightarrow r) \land (\neg q \rightarrow p) \land \neg r.$$

- Write down the truth table for

$$[(p \rightarrow r) \land (\neg q \rightarrow p) \land \neg r] \rightarrow q.$$

- Verify that it is true under all possible truth assignments for $p, q, r$ (see next page).
An Example of a Valid Argument (concluded)

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$r$</th>
<th>$p \rightarrow r$</th>
<th>$\neg q \rightarrow p$</th>
<th>$\neg r$</th>
<th>$[(p \rightarrow r) \land (\neg q \rightarrow p) \land \neg r] \rightarrow q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
An Example of a Potentially Invalid Argument\textsuperscript{a}

“The premises he used were false, therefore his conclusions were false.”
— Dudley Sharp of \textit{Justice For All}

\textsuperscript{a}“Federal judge rules U.S. death penalty is unconstitutional,” \textit{The Star-Ledger}, Tuesday, July 2, 2002.
Statement, Meta-statement, and What?

• “Einstein was born in Japan.”
• “It is not true that Einstein was born in Japan.”
• “This sentence is false.”$^a$
• “Both of us had said the very same thing. Did we both speak the truth—or one of us did—or neither?”$^b$
• No Name Restaurant (Boston).

$^a$Called liar’s paradox.
$^b$Joseph Conrad (1900), *Lord Jim.*
Logical Equivalence

• Statements $p$ and $q$ are **logically equivalent** (written as $p \iff q$) when $p$ and $q$ have the same truth value for all truth value assignments for the primitive statements.

• For example, $p \rightarrow q \iff \neg p \lor q$.\(^a\)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>$p \rightarrow q$</th>
<th>$\neg p \lor q$</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>

• **Rule of replacement**: $p \rightarrow q$ can be replaced by $\neg p \lor q$.

\(^a\)Frege (1879).
More Logical Equivalences (Prove Them)

- $p \leftrightarrow q \iff (p \land q) \lor (\neg p \land \neg q)$.
- $\neg(p \leftrightarrow q) \iff p \leftrightarrow \neg q$.
- $p \rightarrow q \iff \neg q \rightarrow \neg p$.
- $\neg p \leftrightarrow q \iff p \leftrightarrow \neg q$.
- $\neg(p \leftrightarrow q) \iff \neg p \leftrightarrow q$.
- $(p \rightarrow q) \lor (p \rightarrow r) \iff p \rightarrow (q \lor r)$.
- $(p \rightarrow r) \lor (q \rightarrow r) \iff (p \land q) \rightarrow r$. 
More Logical Equivalences (concluded)

- \( \neg p \rightarrow (q \rightarrow r) \iff q \rightarrow (p \lor r) \).
- \( p \leftrightarrow q \iff (p \rightarrow q) \land (q \rightarrow p) \).
- \( p \leftrightarrow q \iff \neg p \leftrightarrow \neg q \).
More on Material Implication

- Note that

\[ p \rightarrow q \iff \neg p \lor q \]
\[ \iff q \lor \neg p \]
\[ \iff \neg(q \lor \neg p) \]
\[ \iff \neg q \rightarrow \neg p. \]

- This is a standard proof method in mathematics.
- But there are controversies surrounding it called the paradoxes of material implication.
  - “If the pig can fly, then Paris is in China” is true.

\(^a\)The term is due to Russell.
DeMorgan’s Laws

• \((p \lor q) \iff \neg p \land \neg q\).

• \((p \land q) \iff \neg p \lor \neg q\).

• It can be used to transform any statement into an equivalent one where \(\neg\) applies only to primitive statements.

  – For example,

\[
\neg(x_1 \lor (x_2 \land \neg x_3)) \iff \neg x_1 \land \neg (x_2 \land \neg x_3)
\]
\[
\iff \neg x_1 \land (\neg x_2 \lor \neg x_3)
\]
\[
\iff \neg x_1 \land (\neg x_2 \lor x_3).
\]

\(^a\)Augustus DeMorgan (1806–1871) or William of Ockham (1288–1348).
DeMorgan’s Laws (concluded)

- Here is a proof of the second law:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$\neg(p \land q)$</th>
<th>$\neg p \lor \neg q$</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>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Other Laws of Logic

• $\neg\neg p \iff p$.
  - Law of double negation.

• $p \lor q \iff q \lor p$; $p \land q \iff q \land p$.
  - Commutative laws.

• $p \lor (q \lor r) \iff (p \lor q) \lor r$; $p \land (q \land r) \iff (p \land q) \land r$.
  - Associative laws.

• $p \lor (q \land r) \iff (p \lor q) \land (p \lor r)$;
  $p \land (q \lor r) \iff (p \land q) \lor (p \land r)$.
  - Distributive laws.
Other Laws of Logic (continued)

- $p \lor p \Leftrightarrow p$; $p \land p \Leftrightarrow p$.
  - Idempotent laws.

- $p \lor \text{false} \Leftrightarrow p$; $p \land \text{true} \Leftrightarrow p$.
  - Identity laws.

- $p \lor \neg p \Leftrightarrow \text{true}$; $p \land \neg p \Leftrightarrow \text{false}$.
  - Inverse laws.

- $p \lor \text{true} \Leftrightarrow \text{true}$; $p \land \text{false} \Leftrightarrow \text{false}$.
  - Domination laws.

- $p \lor (p \land q) \Leftrightarrow p$; $p \land (p \lor q) \Leftrightarrow p$.
  - Absorption laws.
Other Laws of Logic (continued)

• $p \iff q$ 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 or law of contrapositive.

• $(\neg p \rightarrow \text{false}) \Rightarrow p$.
  
  – Reductio ad absurdum or rule of contradiction.
Other Laws of Logic (concluded)

• \[ (p \lor q) \land \neg p \] \Rightarrow q.
  – Disjunctive syllogism.

• \( p \Rightarrow (p \lor q). \)
  – Addition.

• \( (p \land q) \Rightarrow p. \)
  – Simplification.

• \[ (p) \land (q) \] \Rightarrow (p \land q).
  – Conjunction.

• \[ (p \lor q) \land (\neg p \lor r) \] \Rightarrow (q \lor r).
  – Resolution.
Law of Double Negation (P. 183) in Practice

“I ain’t never done no harm to no one.”
— Bertrand Russell (1957),
“Mr. Strawson on referring”
Duality

- Let \( s \) be a statement and contain no logical connectives other than \( \neg, \lor, \) 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,
  - false with true.

- But \( \neg \) is unchanged.
Duality (concluded)

- For example, the dual of \((p \land \neg q) \lor (r \land \text{true})\) is
  \[ (p \lor \neg q) \land (r \lor \text{false}). \]

- DeMorgan’s laws (p. 181) are duality pairs.

- All the laws from the commutative laws (p. 183) to the absorption laws are duality pairs.

**Theorem 34 (The principle of duality)** If \(s \Leftrightarrow t\), then \(s^d \Leftrightarrow t^d\).
Set Theory
The point of philosophy is to start with something so simple as not to seem worth stating, and to end with something so paradoxical that no one will believe it.

— Bertrand Russell (1872–1970)
Set Theory

- 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 $A$.
- $A \subseteq B$ (A is a subset of $B$) means every element of $A$ is an element of $B$.
- $A = B$ means $A \subseteq B$ and $B \subseteq A$.
- $A \subset B$ (A is a proper subset of $B$) means $A \subseteq B$ but $A \neq B$.
- $\emptyset$ is the empty set, and $\emptyset \subseteq A$ for any set $A$.

*aFounded by Georg Cantor (1845–1918) in 1874. Set theory is the cornerstone of 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

\[
\{ x : (x \in A \land x \notin B) \lor (x \in B \land x \notin A) \}. \tag{25}
\]

- E.g., $\{1, 2, 3, 4\} \Delta \{3, 4, 5, 6\} = \{1, 2, 5, 6\}$.
- $A$ and $B$ are **disjoint** if $A \cap B = \emptyset$.
- $\bar{A}$ is the **complement** of $A$. 

©2018 Prof. Yuh-Dauh Lyuu, National Taiwan University
Set Operations (concluded)

- $A - B = \{ x : x \in A \land x \notin B \}$.
  - E.g., $\{1, 2, 3, 4\} - \{3, 4, 5, 6\} = \{1, 2\}$.
  - In general, $A - B \neq B - A$.

- $\bigcup_{i \in I} A_i = \{ x : x \in A_i \text{ for some } i \in I \}$.
  - For example, if $I = \mathbb{N}$, then
  \[ \bigcup_{i \in I} A_i = A_0 \cup A_1 \cup \cdots. \]

- $\bigcap_{i \in I} A_i = \{ x : x \in A_i \text{ for all } i \in I \}$.
Interesting Relations\textsuperscript{a}

- \( A \Delta B = B \Delta A \).
- \( A \Delta B = (A \cup B) - (A \cap B) \).
- \( A \Delta B = (A - B) \cup (B - A) \).

\textsuperscript{a}Contributed by Ms. Chiyoko Yamazaki (B92902108) on October 4, 2004.
DeMorgan’s Laws

\[
\bigcup_{i \in I} A_i = \bigcap_{i \in I} \overline{A_i},
\]

\[
\bigcap_{i \in I} A_i = \bigcup_{i \in I} \overline{A_i}.
\]
Russell’s\textsuperscript{a} 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.

- So what is a set?

\textsuperscript{a}Bertrand Russell (1872–1970), the most important logician of the 20th century if not of all time, won the Nobel Prize in Literature in 1950.
Bertrand Russell (1872–1970)

Karl Popper (1974), “perhaps the greatest philosopher since Kant.”
Properties of Integers: Mathematical Induction
The conclusions which it draws from considering one circle are the same which it would form upon surveying all the circles in the universe.

— David Hume (1711–1776),

*An Enquiry Concerning Human Understanding* (1748)

A finite number means one to which mathematical induction applies[.]

— Bertrand Russell (1872–1970),

“Science and Hypothesis” (1905)
Common Sets in Mathematics

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

\[ ^a \] 0 is a natural number; \( \mathbb{Z} \) is from the German Zahl (meaning number); \( \mathbb{Q} \) is from the word “quotient.”
The Well-Ordering Principle

Axiom 1 (The well-ordering principle)  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.

---

*Defined by Cantor in 1883 and proved by Ernst Zermelo (1871–1953) in 1904 based on his proposed axiom of choice.*
Mathematical Induction\textsuperscript{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 $n \in \mathbb{Z}^+$.

\textsuperscript{a}Dedekind and Peano.
Richard Dedekind (1831–1916)
Giuseppe Peano (1858–1932)
The Proof

• Intuitively,
  – If $S(1)$ is true, then $S(2)$ is true.
  – But if $S(2)$ is true, then $S(3)$ is true.
  – …
  – So $S(n)$ must be true for all $n \in \mathbb{Z}^+$?

• We need a proof based on more foundational principles.
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.
  - So \( S(\ell) \) is false.

• Clearly \( \ell > 1 \) and, hence, \( \ell - 1 \in \mathbb{Z}^+ \).\(^a\)

• Because \( \ell - 1 \notin F \), \( S(\ell - 1) \) is true.

• It follows that \( S(\ell) \) is true, a contradiction.

• So \( F = \emptyset \).

\(^a\)We assume the standard properties of integers. Thanks to a lively after-class discussion on March 9, 2017.
Mathematical Induction and the Well-Ordering Principle

- The proof of induction says that the well-ordering principle (p. 202) 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 (open) statement:
  
  "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: Any integer in $T$ must be smaller than some integer.
- Hence there must be a $k \in \mathbb{Z}^+$ such that $S(k)$ is true but $S(k + 1)$ is not.
The Proof (concluded)

• 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 $k$.\(^a\)
• Hence the smallest element of $T$ exists and is $k$.

\(^a\)Again, we assume the standard properties of integers.