CMPUT 272 (Stewart) University of Alberta **Lecture 23**

Reading: Epp 9.2, 9.5

Counting binary relations and functions:

Let A and B be finite sets with $|A| = n$ and $|B| = m$. Let $A = \{a_1, a_2, \ldots, a_n\}$.

- The number of binary relations from A to B is 2^{nm}.

  A binary relation from A to B can be constructed in $|A \times B| = nm$ steps: for each ordered pair in $|A \times B|$, decide whether or not to include it in the relation. There are 2 choices at each step. The result follows by the multiplication rule.

- The number of functions from A to B is m^n.

  A function from A to B can be constructed in n steps:

$$\begin{array}{cccc} m & m & & m \\ \text{choices} & \text{choices} & & \text{choices} \\ \downarrow & \downarrow & & \downarrow \\ \{(a_1, \underline{\quad}), & (a_2, \underline{\quad}), & \ldots & , (a_n, \underline{\quad})\} \end{array}$$

  By the multiplication rule, the number of functions from A to B is m^n.

- The number of one-to-one functions from A to B

$$= \begin{cases} 0 & \text{if } n > m \\ P(m,n) & \text{if } n \leq m \end{cases}$$

  A one-to-one function from A to B can be constructed in n steps:

$$\begin{array}{cccc} m & m-1 & & m-n+1 \\ \text{choices} & \text{choices} & & \text{choices} \\ \downarrow & \downarrow & & \downarrow \\ \{(a_1, \underline{\quad}), & (a_2, \underline{\quad}), & \ldots & , (a_n, \underline{\quad})\} \end{array}$$

  By the multiplication rule, the number of one-to-one functions from A to B is

$$m(m-1)(m-2)\cdots(m-n+1) = \tfrac{m!}{(m-n)!} = P(m,n).$$

Let $S(n, r)$ be the number of partitions of an n-element set that have exactly r blocks. These are called *Stirling numbers of the second kind.*
[Epp pp 578-581, Grimaldi Chapter 5.3]

$$\begin{array}{rcll} S(n,1) & = & S(n,n) = 1 & \text{for } n \geq 1 \\ S(n,r) & = & S(n-1,r-1) + rS(n-1,r) & \text{for } 1 < r < n \\ & = & \dfrac{1}{r!}\displaystyle\sum_{i=0}^{r}(-1)^i\binom{r}{i}(r-i)^n & \end{array}$$

- The number of onto functions from A to B [Epp pp 578-580]

$$= \begin{cases} 0 & \text{if } n < m \\ S(n,m) \cdot m! & \text{if } n \geq m \end{cases}$$

If $n \geq m$, an onto function from A to B can be constructed in 2 steps:

1. Choose a partition of A into m blocks: $S(n, m)$ ways to do this.
2. Select a distinct element of B for each block of the partition (that each element of the block maps to).
There are $m!$ ways to do this:
Elements of block 1 map to _____ $\leftarrow m$ choices
Elements of block 2 map to _____ $\leftarrow m - 1$ choices
$\vdots$
Elements of block m map to _____ $\leftarrow 1$ choice

So the number of onto functions from A to B is: $S(n, m) \cdot m!$
or, equivalently

$$\sum_{i=0}^{m}(-1)^i\binom{m}{i}(m-i)^n$$

- The number of bijections from A to B

$$= \begin{cases} 0 & \text{if } n \neq m \\ m! & \text{if } n = m \end{cases}$$

- The number of relations on a finite n-element set (A002416[1]):

  Each of the n^2 entries of the incidence matrix can be 0 or 1.

  Therefore, by the multiplication rule, the number of relations is $2^{(n^2)}$.

- The number of reflexive binary relations on an n-element set (A053763):

  The n diagonal entries of the incidence matrix must all be 1, but the other $n^2 - n$ entries can be 0 or 1. Therefore, by the multiplication rule, the number of reflexive relations is 2^{n^2-n}.

- The number of symmetric binary relations on an n-element set (A006125 multiplied by 2^n):

  The $n+(n^2-n)/2 = (n^2+n)/2$ entries on and above the diagonal can be 0 or 1. After those entries are chosen, the rest are forced. Therefore, by the multiplication rule, the number of symmetric relations is $2^{(n^2+n)/2}$.

- The number of antisymmetric binary relations on an n-element set (A083667):

  The n diagonal entries can each be 0 or 1. For each of the $(n^2 - n)/2$ entries (i, j) where $i < j$, there are three choices for (i, j) and (j, i):

  $$\text{entry } (i,j) = 0 \text{ and entry } (j,i) = 0$$
  $$\text{entry } (i,j) = 0 \text{ and entry } (j,i) = 1$$
  $$\text{entry } (i,j) = 1 \text{ and entry } (j,i) = 0$$

  By the multiplication rule, the number of antisymmetric relations is $2^n \cdot 3^{(n^2-n)/2}$.

- The number of transitive binary relations on an n-element set (A006905):

  No simple formula is known.

[1] in the On-Line Encyclopedia of Integer Sequences at oeis.org

- The number of equivalence relations on an n-element set (equivalently, the number of partitions of an n-element set) (A000110): [Epp p 578]

$$S(n,1) + S(n,2) + \cdots + S(n,n).$$

- The number of partial order relations on an n-element set (A001035): No simple formula is known.

- The number of total order relations on an n-element set (A000142): $P(n) = n!$

CMPUT 272 (Stewart) University of Alberta **Lecture 22**

Reading: Epp 9.2, 9.5, 9.6, 9.7

Permutations of collections containing indistinguishable objects

Example: The number of distinguishable permutations of

I N V E N T I V E N E S S

is not 13!.

A permutation can be constructed in 6 steps:

1. Choose positions for the 2 I's: there are $\binom{13}{2}$ ways to perform this step
2. Choose positions for the 3 N's: $\binom{11}{3}$ ways
3. Choose positions for the 2 V's: $\binom{8}{2}$
4. Choose positions for the 3 E's: $\binom{6}{3}$
5. Choose positions for the 1 T: $\binom{3}{1}$
6. Choose positions for the 2 S's: $\binom{2}{2}$

By the multiplication rule, the number of distinguishable permutations of

I N V E N T I V E N E S S

is:

$$\binom{13}{2}\binom{11}{3}\binom{8}{2}\binom{6}{3}\binom{3}{1}\binom{2}{2} = \frac{13!}{2!11!}\cdot\frac{11!}{3!8!}\cdot\frac{8!}{2!6!}\cdot\frac{6!}{3!3!}\cdot\frac{3!}{1!2!}\cdot\frac{2!}{2!0!}$$

$$= \frac{13!}{2!3!2!3!1!2!}$$

Theorem. Suppose a collection consists of n objects of which

n_1 are of type 1 and are indistinguishable from each other,
n_2 are of type 2 and are indistinguishable from each other,
$\vdots$
n_k are of type k and are indistinguishable from each other,
and $n_1 + n_2 + \cdots + n_k = n$.

Then the number of distinguishable permutations of the n objects is

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k}$$

$$= \frac{n!}{n_1!(n-n_1)!} \cdot \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \cdot \cdots \cdot \frac{(n-n_1-n_2-\cdots-n_{k-1})!}{n_k!0!}$$

$$= \frac{n!}{n_1!n_2!n_3!\cdots n_k!}.$$

Example: Consider a robot moving in an $m \times n$ grid, where $m, n \in \mathbb{Z}^+$. At each step, the robot can move one square up or one square to the right. How many different ways can the robot travel from from the bottom left corner to the top right corner?

There must be $m-1$ steps moving up and $n-1$ steps moving right.

The total number of steps is $(m-1)+(n-1) = m+n-2$.

The number of ways we can arrange these moves is:

$$\frac{(m+n-2)!}{(m-1)!(n-1)!}$$

$$= \binom{m+n-2}{m-1} = \binom{m+n-2}{n-1}$$

Combinations with repetition allowed

Definition. An *r-combination with repetition allowed*, chosen from a set X of n elements, is an **unordered** selection of r (not necessarily distinct) elements of X. (a *multiset*)

Example: 7-combinations of $\{1,2,3,4\}$ with repetition allowed:

$$\begin{array}{lll}
[1,2,2,3,4,4,4] & & \\
[3,1,3,1,3,1,3] & = & [1,1,1,3,3,3,3] \\
[4,4,4,4,4,4,4] & & \\
\quad\vdots & &
\end{array}$$

There is a one-to-one correspondence between:

the 7-combinations of a 4-element set

and

permutations with repetition allowed of 7 $\times$'s and 3 $|$'s:

$$\begin{array}{ll}
[1,2,2,3,4,4,4] & \times| \times \times| \times | \times \times\times \\
[1,1,1,3,3,3,3] & \times \times \times| \, | \times \times \times \times| \\
[4,4,4,4,4,4,4] & | \, | \, | \times \times \times \times \times \times\times \\
\quad\vdots &
\end{array}$$

Therefore

the number of 7-combinations of a 4-element set with repetition allowed

is equal to

the number of distinguishable permutations of 7 $\times$'s and 3 $|$'s:

$$\frac{10!}{7!3!} = \binom{10}{7}$$

Theorem. The number of r-combinations, with repetition allowed, that can be selected from a set of n elements is

$$\binom{r+n-1}{r}.$$

Examples:

1. The number of ways of selecting 3 doughnuts from 20 different types, with repetition allowed: $n = 20$, $r = 3$

   $$\binom{r+n-1}{r} = \binom{22}{3} = \frac{22!}{3!19!} = 1540$$

   Note: $20 \cdot 20 \cdot 20 = 8000$ is not the right answer because, eg., $[1, 2, 3]$ is counted six times (once for each of its 6 permutations).

   $P(20, 3) = 20 \cdot 19 \cdot 18 = 6840$ is not correct either for the same reason and because $[1, 1, 1]$ is not counted at all.

   $\binom{20}{3} = 1140$ is not right: $[1, 1, 1]$ is not counted.

   Another way to count this: the number of selections with 3 distinct types plus the number of selections with 2 distinct types (choose 2 types and then duplicate one type or the other) plus the number of selections with 1 type $= \binom{20}{3}+2\cdot\binom{20}{2}+\binom{20}{1} = 1140+20\cdot19+20 = 1140+380+20 = 1540$.

   In general: For all integers n, r with $2 \le r \le n$,

   $$\binom{n+2}{r} = \binom{n}{r-2} + 2\binom{n}{r-1} + \binom{n}{r}.$$

2. The number of ways of distributing 16 identical balls into 5 distinct jars: $n = 5$, $r = 16$

$$\binom{r+n-1}{r} = \binom{20}{16} = \frac{20!}{16!4!} = 4845$$

3. If no jar can be empty:

   place one ball in each jar;

   then distribute the 11 remaining balls: $n = 5$, $r = 11$

$$\binom{r+n-1}{r} = \binom{15}{11} = \frac{15!}{11!4!} = 1365$$

4. The number of ways of distributing 16 *distinct* balls into 5 distinct jars:

   Choose a jar for each ball; apply the multiplication rule.

$$5 \cdot 5 \cdot \ \cdots \ \cdot 5 = 5^{16} = 152,587,890,625$$

5. The number of integer solutions to the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 16 \text{ where each } x_i \in \mathbb{Z}^{nonneg}.$$

$$\binom{20}{16}$$

6. The number of integer solutions to the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 16 \text{ where each } x_i \in \mathbb{Z}^{+}.$$

$$\binom{15}{11}$$

Theorem (Pascal's Formula). For all $r, n \in \mathbb{Z}^+$ with $r \leq n$,

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

Proof (combinatorial): Let $r, n \in \mathbb{Z}^+$ with $r \leq n$.

By the definition of combinations,

$$\binom{n+1}{r}$$

is equal to the number of r-element subsets of an $(n+1)$-element set.
Let $S = \{x_1, x_2, \ldots, x_n, x_{n+1}\}$ be an arbitrary $(n+1)$-element set.
Any r-element subset of S either contains x_{n+1} or not.

- If it contains x_{n+1}, then it consists of x_{n+1} and $r-1$ elements of $\{x_1, x_2, \ldots, x_n\}$: there are $\binom{n}{r-1}$ of these.
- If it does not contain x_{n+1}, then it consists of r elements of $\{x_1, x_2, \ldots, x_n\}$: there are $\binom{n}{r}$ of these.

So by the addition rule, the number of r-element subsets of S is equal to

$$\binom{n}{r-1} + \binom{n}{r}.$$

Therefore

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

□

Theorem (Pascal's Formula). For all $r, n \in \mathbb{Z}^+$ with $r \leq n$,

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

Proof (algebraic): Let $r, n \in \mathbb{Z}^+$ with $r \leq n$.

$$\begin{aligned}
\binom{n}{r-1} + \binom{n}{r} &= \frac{n!}{(r-1)!(n-(r-1))!} \;+\; \frac{n!}{r!(n-r)!} \\
&= \frac{n!}{(r-1)!(n-r+1)!} \;+\; \frac{n!}{r!(n-r)!} \\
&= \frac{n!}{(r-1)!(n-r+1)!} \cdot \frac{r}{r} \;+\; \frac{n!}{r!(n-r)!} \cdot \frac{n-r+1}{n-r+1} \\
&= \frac{n! \cdot r}{r!(n-r+1)!} \;+\; \frac{n!(n-r+1)}{r!(n-r+1)!} \\
&= \frac{n!(r+n-r+1)}{r!(n-r+1)!} \\
&= \frac{n!(n+1)}{r!(n-r+1)!} \\
&= \frac{(n+1)!}{r!((n+1)-r)!} \\
&= \binom{n+1}{r}
\end{aligned}$$

□

Using Pascal's formula: For all $r, n \in \mathbb{Z}^+$ with $r \leq n$,

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

Theorem. For all integers n, r with $2 \leq r \leq n$,

$$\binom{n+2}{r} = \binom{n}{r-2} + 2\binom{n}{r-1} + \binom{n}{r}.$$

Proof:

$$\begin{aligned}
\binom{n+2}{r} &= \qquad \binom{n+1}{r-1} \qquad + \qquad \binom{n+1}{r} && \text{by Pascal's formula} \\
&= \binom{n}{r-2} + \binom{n}{r-1} \;+\; \binom{n}{r-1} + \binom{n}{r} && \text{Pascal's formula twice} \\
&= \binom{n}{r-2} \qquad + \quad 2\binom{n}{r-1} \quad + \quad \binom{n}{r}
\end{aligned}$$

□

Pascal's triangle [Epp p 594]

Pascal's triangle is an arrangement of the values of $\binom{n}{r}$ for $0 \le r \le n$:

$$\binom{n}{0} = \binom{n}{n} = 1$$

and from Pascal's formula, for $0 < r < n$,

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

					r				
		0	1	2	3	4	5	6	7
	0	1							
	1	1	1						
	2	1	2	1					
	3	1	3	3	1				
n	4	1	4	6	4	1			
	5	1	5	10	10	5	1		
	6	1	6	15	20	15	6	1	
	7	1	7	21	35	35	21	7	1
					⋮				

$$\begin{tikzcd}
\binom{n-1}{r-1} \arrow[rrd] & + & \binom{n-1}{r} \arrow[d] \\
 & & \binom{n}{r}
\end{tikzcd}$$

Note: The horizontal symmetry is due to a fact that we saw before:

For $r, n \in \mathbb{Z}$ with $0 \le r \le n$,

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \binom{n}{n-r}$$

Binomial Theorem For any $a, b \in \mathbb{R}, n \in \mathbb{N}$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Proof by induction: see Epp pp 598-601

Proof sketch (combinatorial):

$$\begin{aligned}
(a+b)^2 &= (a+b)(a+b) \\
&= a^2 + ab + ba + b^2 \\
&= a^2 + 2ab + b^2
\end{aligned}$$

$$\begin{aligned}
(a+b)^3 &= (a+b)(a+b)(a+b) \\
&= aaa + aab + aba + abb + baa + bab + bba + bbb \\
&= a^3 + 3a^2b + 3ab^2 + b^3
\end{aligned}$$

$$\begin{aligned}
(a+b)^4 &= (a+b)(a+b)(a+b)(a+b) \\
&= aaaa + aaab + aaba + aabb + abaa + abab + abba + abbb \\
&\quad + baaa + baab + baba + babb + bbaa + bbab + bbba + bbbb \\
&= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \\
&= \binom{4}{0}a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + \binom{4}{4}b^4 \\
&\vdots
\end{aligned}$$

$$\begin{aligned}
(a+b)^n &= \underbrace{(a+b)(a+b)(a+b)\cdots(a+b)}_{n \text{ terms}} \\
&= \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n
\end{aligned}$$

For each k, $0 \le k \le n$, the coefficient of $a^{n-k}b^k$ is the number of ways of choosing k b's from n terms, that is $\binom{n}{k}$.

Using the Binomial Theorem: For any $a, b \in \mathbb{R}, n \in \mathbb{N}$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

1. expand powers of binomials:

$$\begin{aligned}(x+y)^7 &= \tbinom{7}{0}x^7+\tbinom{7}{1}x^6y+\tbinom{7}{2}x^5y^2+\tbinom{7}{3}x^4y^3+\tbinom{7}{4}x^3y^4+\tbinom{7}{5}x^2y^5+\tbinom{7}{6}xy^6+\tbinom{7}{7}y^7 \\ &= x^7+7x^6y+21x^5y^2+35x^4y^3+35x^3y^4+21x^2y^5+7xy^6+y^7\end{aligned}$$

2. derive identities: The number of subsets of an n-element set A:

$$\begin{aligned}|\mathcal{P}(A)| &= \sum_{k=0}^{n} \binom{n}{k} && \text{sum of the number of subsets of each size} \\ &= \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot 1^k && \text{multiply each term by 1} \\ &= (1+1)^n = 2^n && \text{Binomial theorem}\end{aligned}$$

3. simplify sums:

$$\begin{aligned}\sum_{k=0}^{n} \binom{n}{k} 9^k &= \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot 9^k \\ &= (1+9)^n \\ &= 10^n\end{aligned}$$

CMPUT 272 (Stewart) University of Alberta **Lecture 21**

Reading: Epp 9.2, 9.4, 9.5

Permutations

Recall:

- A *permutation* of a finite set is an ordering of its elements.
- The number of permutations of an n-element set is $n!$.

Definition. For $r, n \in \mathbb{Z}$ with $0 \leq r \leq n$, an r-*permutation* of a set of n elements is an **ordered** selection of r distinct elements from the set.

Notation:
$P(n, r)$ denotes the number of r-permutations of an n-element set.

Theorem. For $r, n \in \mathbb{Z}$ with $0 \leq r \leq n$,

$$P(n, r) = \frac{n!}{(n-r)!}.$$

Proof:

If $r \geq 1$, then an r-permutation of n elements can be constructed in r steps:

$$\begin{array}{cccc}
n & n-1 & & n-r+1 \\
\text{choices} & \text{choices} & & \text{choices} \\
\downarrow & \downarrow & & \downarrow \\
\underline{\qquad} & \underline{\qquad} & & \underline{\qquad} \\
1 & 2 & \ldots & r
\end{array}$$

By the multiplication rule,

$$\begin{aligned}
P(n, r) &= n(n-1)(n-2)\cdots(n-r+1) \\
&= n(n-1)(n-2)\cdots(n-r+1)\cdot\frac{(n-r)(n-r-1)\cdots 3\cdot\cdot 2\cdot 1}{(n-r)(n-r-1)\cdots 3\cdot\cdot 2\cdot 1} \\
&= \frac{n(n-1)(n-2)\cdots 3\cdot\cdot 2\cdot 1}{(n-r)(n-r-1)\cdots 3\cdot\cdot 2\cdot 1} \\
&= \frac{n!}{(n-r)!}
\end{aligned}$$

If $r = 0$ then there is one r-permutation (the empty string) and the number of r-permutations is $\frac{n!}{(n-0)!} = 1$ as required. □

Example: How many (ordered) playlists are there of 9 out of 40 songs?

$P(40,9) = \frac{40!}{31!} = 40 \cdot 39 \cdot 38 \cdot 37 \cdot 36 \cdot 35 \cdot 34 \cdot 33 \cdot 32 = 99,225,500,774,400$

Combinations

Definition. For $r, n \in \mathbb{Z}$ with $0 \le r \le n$, an r-*combination* of a set of n elements is an **unordered** selection of r distinct elements from the set, i.e. a subset of size r.

Notation: $\binom{n}{r}$ denotes the number of r-combinations of an n-element set.

(read as "n choose r")

Theorem. For $r, n \in \mathbb{Z}$ with $0 \le r \le n$,

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Proof: Among all r-permutations of n elements, each r-combination appears $r!$ times (once in each of its permutations). Therefore,

$$\binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}.$$

□

Examples:

1. On an exam with ten questions, where the order in which questions are answered is unimportant, how many ways are there to answer:

   - seven questions?

   $$\binom{10}{7} = \frac{10!}{7!3!} = \frac{10 \cdot 9 \cdot 8 \cdot 7!}{3 \cdot 2 \cdot 7!} = 10 \cdot 3 \cdot 4 = 120$$

   - three from questions 1-5 and four from questions 6-10?

     By the multiplication rule:

   $$\binom{5}{3}\binom{5}{4} = \frac{5!}{3!2!} \cdot \frac{5!}{4!1!} = 10 \cdot 5 = 50$$

   - seven questions, at least three of which are from questions 1-5?

     By the multiplication and addition rules:

   $$\binom{5}{3}\binom{5}{4} + \binom{5}{4}\binom{5}{3} + \binom{5}{5}\binom{5}{2} = 10 \cdot 5 + 5 \cdot 10 + 1 \cdot 10 = 110$$

2. How many eight-bit strings have exactly three 1's?

   The number of ways to choose three positions for the 1's:

   $$\binom{8}{3} = \frac{8!}{3!5!} = \frac{8 \cdot 7 \cdot 6 \cdot 5!}{3 \cdot 2 \cdot 5!} = 8 \cdot 7 = 56$$

   The number of ways to choose five positions for the 0's:

   $$\binom{8}{5} = \frac{8!}{5!3!} = \binom{8}{3} = 56$$

Note: For $r, n \in \mathbb{Z}$ with $0 \leq r \leq n$,

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n!}{(n-r)!r!} = \binom{n}{n-r}$$

In particular:

when $r = 0$:

$$\binom{n}{0} = \binom{n}{n} = 1$$

when $r = 1$:

$$\binom{n}{1} = \binom{n}{n-1} = n$$

when $r = 2$:

$$\binom{n}{2} = \binom{n}{n-2} = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}$$

The Pigeonhole Principle

If n pigeons fly into m pigeonholes and $n > m$ then at least one pigeonhole contains two or more pigeons. Equivalently, a function from a finite set to a smaller finite set cannot be one-to-one.

Proof: Suppose that n pigeons fly into m pigeonholes where $n > m$, and suppose that no pigeonhole contains more than one pigeon. Then the total number of pigeons is at most m. But this contradicts that the number of pigeons is $n > m$. □

How to use the Pigeonhole Principle:

Define a function from a finite set of n elements (the pigeons) to a finite set of m elements (the pigeonholes), where $n > m$. By the pigeonhole principle, two elements of the domain map to the same element of the co-domain.

Examples:

1. In any set of 13 people, 2 people have birthdays in the same month.

2. Among any six distinct integers from $\{1, 2, \ldots, 9\}$, there must be two whose sum is 10.

   Pigeons: the 6 integers
   Pigeonholes: $\{1, 9\}$, $\{2, 8\}$, $\{3, 7\}$, $\{4, 6\}$, $\{5\}$
   Function: maps each of the 6 integers to the set of which it is an element

3. Among any 101 elements of $\{1, 2, \ldots, 200\}$, there must be two integers such that one divides the other.

Proof: Let S be an arbitrary subset of $\{1, 2, \ldots, 200\}$ of size 101. Each integer from 1 through 200 can be written uniquely as

$$2^k \cdot y \text{ for some } k, y \in \mathbb{Z} \text{ where } 0 \leq k \leq 7, 1 \leq y \leq 199, \text{ and } y \text{ is odd.}$$

Pigeons: the 101 elements of S

Pigeonholes:

$$\begin{array}{l} \{x \in \{1, 2, \ldots, 200\} \mid x = 2^i \cdot 1 \quad \text{for some integer } i \text{ with } 0 \leq i \leq 7\} \\ \{x \in \{1, 2, \ldots, 200\} \mid x = 2^i \cdot 3 \quad \text{for some integer } i \text{ with } 0 \leq i \leq 7\} \\ \qquad \vdots \\ \{x \in \{1, 2, \ldots, 200\} \mid x = 2^i \cdot 199 \text{ for some integer } i \text{ with } 0 \leq i \leq 7\} \end{array}$$

Function: maps each element of S to the set containing it

There are 100 pigeonholes: one for each odd number y with $1 \leq y \leq 199$. There are 101 pigeons: the elements of S.

Therefore, by the Pigeonhole Principle, there exist distinct elements $x_1, x_2 \in S$ and odd integer y with $1 \leq y \leq 199$, such that

$$x_1 = 2^k \cdot y \text{ and } x_2 = 2^\ell \cdot y \text{ for some } k, \ell \in \mathbb{Z}, 0 \leq k < \ell \leq 7.$$

Then

$$\frac{x_2}{x_1} = \frac{2^\ell \cdot y}{2^k \cdot y} = 2^{\ell - k} \text{ which is an integer. Therefore } x_1 \text{ divides } x_2.$$

□

Can you prove this with $|S| < 101$? No: $\{101, 102, \ldots, 200\}$ is a set of 100 numbers, none of which divides any other.

4. During the first six weeks of winter term, a student sends out at least one resume per day but no more than 60 resumes in total. Show that there is a period of consecutive days during which she sends out exactly 23 resumes.

   Proof: For all $1 \leq i \leq 42$, let x_i equal the total number of resumes that the student sends out on days 1 through i. Then

   $$1 \leq x_1 < x_2 < \cdots < x_{42} \leq 60$$

   and adding 23 to each integer gives:

   $$24 \leq x_1 + 23 < x_2 + 23 < \cdots < x_{42} + 23 \leq 83.$$

   We have 42 distinct integers $x_1, x_2, \ldots, x_{42}$ and another 42 distinct integers $x_1 + 23, x_2 + 23, \ldots, x_{42} + 23$, and these 84 integers all lie between 1 and 83 inclusive. Therefore by the Pigeonhole Principle, $x_i + 23 = x_j$ for some $1 \leq i < j \leq 42$. So, on days $i + 1$ through j, the student sends out exactly 23 resumes. $\square$

Generalized Pigeonhole Principle

If n pigeons fly into m pigeonholes and $n > km$ for some $k \in \mathbb{Z}^+$, then at least one pigeonhole contains $k+1$ or more pigeons.

Proof: Suppose that n pigeons fly into m pigeonholes and $n > km$ for some $k \in \mathbb{Z}^+$, and suppose that no pigeonhole contains more than k pigeons. Then the total number of pigeons is at most km. But this contradicts that the number of pigeons is $n > km$. □

How to use the Generalized Pigeonhole Principle:

Define a function from a finite set of n elements (the pigeons) to a finite set of m elements (the pigeonholes), where $n > km$ for some $k \in \mathbb{Z}^+$. By the pigeonhole principle, $k+1$ elements of the domain map to the same element of the co-domain.

Example: In any set of 1100 people, four must have the same birthdate.

Proof:

Pigeons: 1100 people
Pigeonholes: 366 days of the year
Function: maps each person to his/her birthdate

Now $1100 > 3 \cdot 366 = 1098$ and therefore by the Generalized Pigeonhole Principle, at least four people have the same birthdate.

Alternate proof: Suppose no four have the same birthdate. Then at most three have the same birthdate and therefore the number of people is at most $3 \cdot 366 = 1098$, which contradicts that the number of people is 1100.

CMPUT 272 (Stewart) University of Alberta **Lecture 20**

Reading: Epp 9.1-9.3

Counting

Recall:

A set is *finite* if it has no elements or there is a one-to-one correspondence from $\{1, 2, \ldots, n\}$ to it for some $n \in \mathbb{Z}^+$.

If A is a finite set, then the number of elements in A, denoted $|A|$ or $N(A)$, is

$$|A| = \begin{cases} 0 & \text{if } A = \emptyset \\ n & \text{if there is a bijection from } \{1, 2, \ldots, n\} \text{ to } A, \text{ for some } n \in \mathbb{Z}^+ \end{cases}$$

Example:

For $m, n \in \mathbb{Z}$ with $m \leq n$, how many integers are there from m to n inclusive?

Let k be the number of integers from m to n inclusive.

We find a bijection from $\{1, 2, \ldots, k\}$ to $\{m, \ldots, n\}$
and then determine an expression for k in terms of m and n.

Consider mapping $\{1, 2, \ldots, k\}$ to $\{m, \ldots, n\}$ like this:

$$\begin{tikzcd}
1 \arrow[d] & 2 \arrow[d] & 3 \arrow[d] & \cdots & k \arrow[d] \\
m & m+1 & m+2 & & n
\end{tikzcd}$$

This mapping is described by the function $f : \{1, \ldots, k\} \mapsto \{m, \ldots, n\}$ where

$$f(x) = x + m - 1.$$

f is a bijection since each integer from m to n is mapped to exactly once.

Now $\quad f(k) = k + m - 1 = n \quad$ and therefore $\quad k = n - m + 1.$

So, the number of integers from m to n inclusive is $n - m + 1$.

Example: How many 3-digit positive integers are multiples of 5?

We find a bijection from $\{1, 2, \ldots, k\}$ to $\{100, 105, \ldots, 995\}$ and then determine the value of k.

Consider mapping $\{1, 2, \ldots, k\}$ to $\{100, 105, \ldots, 995\}$ like this:

$$\begin{tikzcd}
1 \arrow[dd] & 2 \arrow[dd] & 3 \arrow[dd] & & k \arrow[dd] \\
 & & & \cdots & \\
100 & 105 & 110 & & 995
\end{tikzcd}$$

We may think of this mapping as the composition of two functions:

$$\begin{tikzcd}
1 \arrow[d] & 2 \arrow[d] & 3 \arrow[d] & & k \arrow[d] \\
20 \arrow[d] & 21 \arrow[d] & 22 \arrow[d] & \cdots & 199 \arrow[d] \\
100 & 105 & 110 & & 995
\end{tikzcd}$$

The mapping is the bijection $f : \{1, 2, \ldots, k\} \mapsto \{100, 105, \ldots, 995\}$ where

$$f(x) = (x + 19) \times 5.$$

Now $\quad f(k) = (k + 19) \times 5 = 995 \quad$ and therefore $\quad k = 995/5 - 19 = 180.$

So, the number of 3-digit positive integers that are multiples of 5 is 180.

Rules for Counting (for finite sets)

The Addition Rule [Epp Theorem 9.3.1]
If a finite set A equals the union of k mutually disjoint subsets $A_1, A_2, \ldots, A_k$ then $|A| = |A_1| + |A_2| + \cdots + |A_k|$.

The Difference Rule [Epp Theorem 9.3.2]
If A is a finite set and B is a subset of A then $|A - B| = |A| - |B|$.

The Inclusion/Exclusion Rule [Epp Theorem 9.3.3]

If A and B are finite sets then $|A \cup B| = |A| + |B| - |A \cap B|$.

If A, B, and C are finite sets then
$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

If $A_1, A_2, \ldots, A_n$ are finite sets, then

$$\begin{aligned} |\bigcup_{1 \le i \le n} A_i| = & \sum_{1 \le i \le n} |A_i| \\ & - \sum_{1 \le i < j \le n} |A_i \cap A_j| \\ & + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| \\ & - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n|. \end{aligned}$$

The Multiplication Rule [Epp Theorem 9.2.1]
If an operation consists of k steps and
the first step can be performed in n_1 ways,
the second step can be performed in n_2 ways *regardless of how the first step was performed,*
$\vdots$
the kth step can be performed in n_k ways *regardless of how the preceding steps were performed,*
then the entire operation can be performed in $n_1 n_2 \ldots n_k$ ways.

Examples:

1. The number of bit strings of length n is 2^n.

$$\begin{array}{cccc} 2 & 2 & & 2 \\ \text{choices} & \text{choices} & & \text{choices} \\ \downarrow & \downarrow & & \downarrow \\ \underline{\qquad} & \underline{\qquad} & & \underline{\qquad} \\ 1 & 2 & \dots & n \end{array}$$

By the multiplication rule, the number of n-bit strings is $\underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{n \text{ times}} = 2^n$

2. Counting the number of iterations of a nested loop:

```
for $i := 1$ to $5$
    for $j := 4$ to $11$
        ⋮
    next $j$
next $i$
```

In an iteration of the inner loop, i has one of 5 values and j has one of $11 - 4 + 1 = 8$ values.

$$\begin{array}{cc} 5 & 8 \\ \text{choices} & \text{choices} \\ \downarrow & \downarrow \\ \underline{\qquad} & \underline{\qquad} \\ i & j \end{array}$$

By the multiplication rule, the inner loop executes $5 \times 8 = 40$ times.

3. $|A_1 \times A_2 \times \cdots \times A_n|$ where $A_1, \ldots, A_n$ are finite sets.

   An element of the cross product (an ordered n-tuple) can be constructed in n steps:

$$\begin{array}{ccccc}
 & |A_1| & |A_2| & & |A_n| \\
 & \text{choices} & \text{choices} & & \text{choices} \\
 & \downarrow & \downarrow & & \downarrow \\
(& \underline{\quad}, & \underline{\quad}, & \cdots & ,\underline{\quad}\ ) \\
 & 1 & 2 & & n
\end{array}$$

   By the multiplication rule, the number of ordered n-tuples is

$$|A_1| \cdot |A_2| \cdot \ \cdots \ \cdot |A_n|.$$

4. The number of

   - Boolean functions on n variables, i.e.,
   - functions from $\{0,1\}^n$ to $\{0,1\}$, i.e.,
   - distinct columns in a truth table with n variables.

   From above, $|\{0,1\}^n| = 2^n$.

   A function from $\{0,1\}^n$ to $\{0,1\}$ can be constructed in 2^n steps:

$$\begin{array}{ccccc}
2 & 2 & & 2 \\
\text{choices} & \text{choices} & & \text{choices} \\
\downarrow & \downarrow & & \downarrow \\
\{((0,0,\ldots,0),\underline{\quad}), & ((0,0,\ldots,1),\underline{\quad}), & \cdots & , \ ((1,1,\ldots,1),\underline{\quad})\} \\
1 & 2 & & 2^n
\end{array}$$

   By the multiplication rule, the number of Boolean functions on n variables is

$$2^{(2^n)}.$$

5. The number of strings of characters A-Z, 0-9:

- 4 symbols with repetition allowed $= 36^4$.

$$\begin{array}{cccc} 36 & 36 & 36 & 36 \\ \text{choices} & \text{choices} & \text{choices} & \text{choices} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ \rule{2em}{0.4pt} & \rule{2em}{0.4pt} & \rule{2em}{0.4pt} & \rule{2em}{0.4pt} \\ 1 & 2 & 3 & 4 \end{array}$$

  By the multiplication rule,
  the number of strings of length 4 is
  $36 \cdot 36 \cdot 36 \cdot 36 = 36^4$

- 1 to 4 symbols with repetition allowed $= 36^4 + 36^3 + 36^2 + 36^1$ (multiplication and addition rules).

- 4 symbols without repetition $= 36 \cdot 35 \cdot 34 \cdot 33$.

$$\begin{array}{cccc} 36 & 35 & 34 & 33 \\ \text{choices} & \text{choices} & \text{choices} & \text{choices} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ \rule{2em}{0.4pt} & \rule{2em}{0.4pt} & \rule{2em}{0.4pt} & \rule{2em}{0.4pt} \\ 1 & 2 & 3 & 4 \end{array}$$

  By the multiplication rule,
  the number of strings of length 4 is
  $36 \cdot 35 \cdot 34 \cdot 33$

- 1 to 4 symbols without repetition
  $36 \cdot 35 \cdot 34 \cdot 33 \quad + \quad 36 \cdot 35 \cdot 34 \quad + \quad 36 \cdot 35 \quad + \quad 36$
  (multiplication and addition rules).

- 4 symbols with at least one repetition:
  $36^4 - 36 \cdot 35 \cdot 34 \cdot 33$ (difference rule).

- 3 symbols with at least one A:

  Let S be the set of all 3-symbol strings.
  Let S_A be the set of 3-symbol strings that contain at least one A.
  Let S_{no} be the set of 3-symbol strings that contain no A.

  By the difference rule: $|S_A| = |S| - |S_{no}| = 36^3 - 35^3 = 3781$.

Let S_1	be the set of 3-symbol strings with an A in position(s)	1
S_2		2
S_3		3
$S_{1,2}$		1 and 2
$S_{1,3}$		1 and 3
$S_{2,3}$		2 and 3
$S_{1,2,3}$		1, 2, and 3

  By the inclusion/exclusion rule:
  $$\begin{aligned}|S_A| &= |S_1| + |S_2| + |S_3| - |S_{1,2}| - |S_{1,3}| - |S_{2,3}| + |S_{1,2,3}| \\ &= 36^2 + 36^2 + 36^2 - 36 - 36 - 36 + 1 = 3781.\end{aligned}$$

Connection to Probability

sample space: the set of all possible outcomes of a random process (finite)

event: a subset of a sample space

If S is a finite sample space in which all outcomes are equally likely, and E is an event in S, then the *probability of E*, denoted $P(E)$, is
$$P(E) = \frac{|E|}{|S|}.$$

Example: Suppose a 4 symbol string of characters A-Z, 0-9 is chosen at random with all outcomes equally likely. The sample space S is the set of all 4-symbol strings. Let E be the event of all strings without repetition. Then

$$P(E) = \frac{36 \cdot 35 \cdot 34 \cdot 33}{36^4} = \frac{1413720}{1679616} \approx 0.8417 \qquad P(S-E) = 1-P(E) \approx 0.1583$$

Permutations

Definition. The *factorial* function from $\mathbb{N}$ to $\mathbb{Z}^+$ is defined by:

$$0! = 1$$
$$n! = n(n-1)! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1 \text{ for all } n \in \mathbb{Z}^+$$

Definition. A *permutation* of a finite set is an ordering of its elements.

Theorem. The number of permutations of an n-element set is $n!$.

Proof:

If $n \geq 1$ then a permutation of n elements can be constructed in n steps:

$$\begin{array}{cccc} n & n-1 & & 1 \\ \text{choices} & \text{choices} & & \text{choice} \\ \downarrow & \downarrow & & \downarrow \\ \underline{\qquad} & \underline{\qquad} & & \underline{\qquad} \\ 1 & 2 & \dots & n \end{array}$$

By the multiplication rule, the number of permutations of n elements is

$$n(n-1)(n-2)\cdots 1$$
$$= n!$$

If $n = 0$, there is one permutation: the empty string, denoted ε. Therefore, the number of permutations of $n = 0$ elements is $n! = 1$. □

Examples:

1. The number of permutations of 50 elements is 50!

   = 30414093201713378043612608166064768844377641568960512000000000000

2. How many ways can the letters of the word Q U I C K be arranged in a row?

   $$5!$$

3. How many ways can the letters of the word Q U I C K be arranged in a row if the letters Q and U must remain next to each other ...

   - in the order QU?

     $$4!$$

   - in either order?

     $$2 \times 4!$$

4. The number of bijections from A to B where $|A| = |B| = n$ is:

   $$P(n) = n!$$

Theorem. The number of circular arrangements of $n \geq 1$ elements, where rotations are considered to be the same, is $(n-1)!$.

Proof idea: Each circular arrangement corresponds to n permutations. Therefore the number of circular arrangements is $n!/n = (n-1)!$.

Example: If two seatings around a circular table are considered the same if one is a rotation of the other,

- how many ways can four people be seated?
- five people?

CMPUT 272 (Stewart) University of Alberta **Lecture 19**

Reading: Epp 8.1-8.3, 8.5

Recall:

Properties of binary relations: Let R be a relation on a set A.

R is *reflexive* $\Leftrightarrow \forall x \in A$, $(x, x) \in R$.

R is *symmetric* $\Leftrightarrow \forall x, y \in A$, if $(x, y) \in R$ then $(y, x) \in R$.

R is *antisymmetric* $\Leftrightarrow \forall x, y \in A$, if $(x, y) \in R$ and $(y, x) \in R$ then $x = y$.

R is *transitive* $\Leftrightarrow \forall x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$.

R is an *equivalence relation* $\Leftrightarrow$ R is reflexive, symmetric, and transitive.

R is a *partial order relation* $\Leftrightarrow$ R is reflexive, antisymmetric, and transitive.

Partial Order Relations: reflexive, antisymmetric, and transitive

Recall: A relation R on a set A is
antisymmetric $\Leftrightarrow \forall x, y \in A$, if $(x, y) \in R$ and $(y, x) \in R$ then $x = y$.

Examples:

1. $\leq$ on $\mathbb{R}$
2. $\subseteq$ on $\mathcal{A}$, where $\mathcal{A}$ is a set of sets
3. $|$ on $\mathbb{Z}^+$ (In contrast, $|$ on $\mathbb{Z}$ is not antisymmetric since $1|-1$ and $-1|1$.)

Theorem. The relation R on $\mathbb{R} \times \mathbb{R}$ where, for all (a, b) and (c, d) in $\mathbb{R} \times \mathbb{R}$,

$$(a, b)\ R\ (c, d) \quad \Leftrightarrow \quad \text{either } a < c \text{ or both } a = c \text{ and } b \leq d$$

is a partial order relation.

Proof:

R is reflexive: Let $(a, b) \in \mathbb{R} \times \mathbb{R}$. $a = a$ and $b \leq b$; therefore $(a, b)\ R\ (a, b)$.

R is antisymmetric: Let $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$ such that $(a, b)\ R\ (c, d)$ and $(c, d)\ R\ (a, b)$. Then $a \leq c$ and $c \leq a$, which implies that $a = c$. But now $b \leq d$ and $d \leq b$, so $b = d$. Therefore $(a, b) = (c, d)$.

R is transitive: Let $(a, b), (c, d), (e, f) \in \mathbb{R} \times \mathbb{R}$ such that $(a, b)\ R\ (c, d)$ and $(c, d)\ R\ (e, f)$. Then $a \leq c$ and $c \leq e$, which implies that $a \leq e$.

Case 1 ($a < e$): Then, by the definition of R, $(a, b)\ R\ (e, f)$.

Case 2 ($a = e$): Then, since $a \leq c$ and $c \leq e$, it must be that $a = c$ and $c = e$. Then $b \leq d$ and $d \leq f$, so $b \leq f$. Therefore, by the definition of R, $(a, b)\ R\ (e, f)$.

In both cases, $(a, b)\ R\ (e, f)$ and therefore R is transitive.

R is reflexive, antisymmetric, and transitive and therefore R is a partial order relation. □

What does the directed graph of a partial order relation look like?

Example: $\subseteq$ on $\mathcal{P}(\{1, 2, 3\})$

Because a partial order relation is transitive and antisymmetric, its directed graph has no cycles except loops.

Definition. The *Hasse diagram* of a partial order relation R is the directed graph representation with

- loops omitted
- all arrows directed upward,
- arrowheads omitted, and
- edges implied by transitivity omitted.

Examples:

$\subseteq$ on $\mathcal{P}(\{1, 2, 3\})$ $\qquad$ $\mid$ on $\{2, 3, \ldots, 12\}$ $\qquad$ $\mid$ on $\{1, 2, 4, 8, 16\}$

Definitions. Let $\preceq$ be a partial order relation on a set A.

A is a *partially ordered set* or *poset* with respect to $\preceq$.

$x \in A$ is a *maximal* element of $A \Leftrightarrow \forall y \in A$, if $x \neq y$ then $x \not\preceq y$.

$x \in A$ is a *minimal* element of $A \Leftrightarrow \forall y \in A$, if $x \neq y$ then $y \not\preceq x$.

$x \in A$ is a *greatest* element of $A \Leftrightarrow \forall y \in A$, $y \preceq x$.

$x \in A$ is a *least* element of $A \Leftrightarrow \forall y \in A$, $x \preceq y$.

$B \subseteq A$ is a *chain* of $A \Leftrightarrow \forall x, y \in B$, $x \preceq y$ or $y \preceq x$.

$\preceq$ is a *total order relation* $\Leftrightarrow \forall x, y \in A$, $x \preceq y$ or $y \preceq x$.

Applications of partial order relations

1. Sorting
2. Scheduling: example (from Epp):

   At an automobile assembly plant, the job of assembling a car can be broken down into these tasks:

   1. Build frame
   2. Install engine, power train components, gas tank
   3. Install brakes, wheels, tires
   4. Install dashboard, floor, seats
   5. Install electrical lines
   6. Install gas lines
   7. Install brake lines
   8. Attach body panels to frame
   9. Paint body

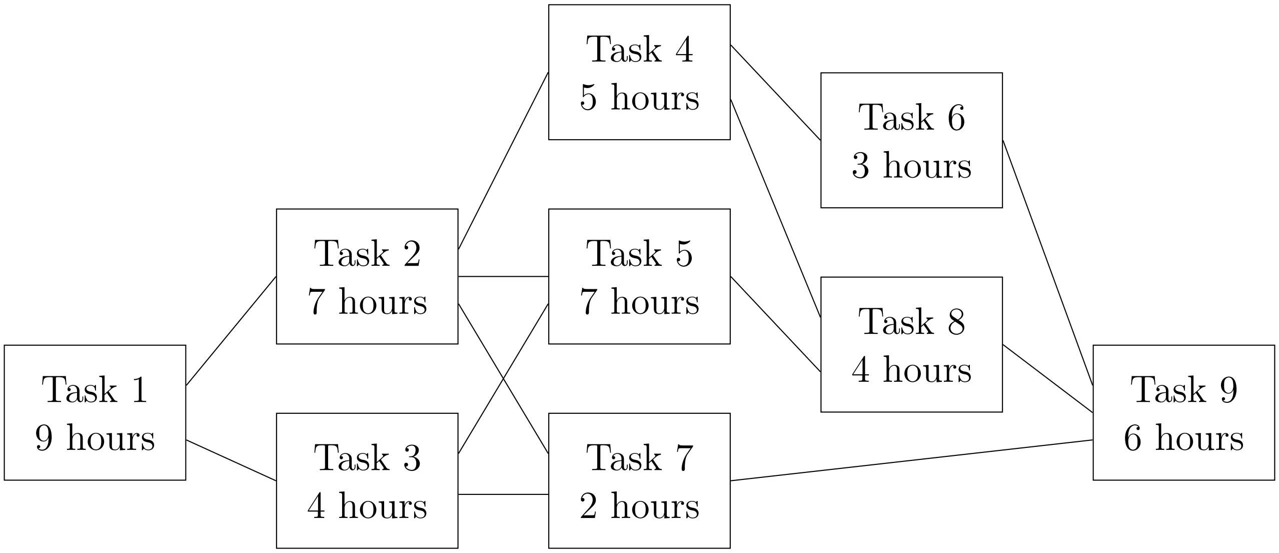
   Some tasks cannot be started until others are finished, and each task requires a certain amount of time:

Task	Immediately preceding tasks	Time needed to perform task
1		9 hours
2	1	7 hours
3	1	4 hours
4	2	5 hours
5	2, 3	7 hours
6	4	3 hours
7	2, 3	2 hours
8	4, 5	4 hours
9	6, 7, 8	6 hours

Define a partial order relation $\preceq$ on the set of tasks as follows:

$$\text{For all tasks } x \text{ and } y, \quad x \preceq y \quad \Leftrightarrow \quad x = y \quad \text{or} \quad x \text{ precedes } y.$$

Draw the Hasse diagram for $\preceq$ (with relations directed from left to right).



What is the minimum time required to assemble a car

with many robots? 33 hours

with one robot? 47 hours

Identify a *critical path*, that is, a longest path: 1 - 2 - 5 - 8 - 9

A *feasible schedule* for one robot: 1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9

Definition. A *topological sort* (or *linear extension*) of a partial order relation $\preceq$ on a set A is a total order on A that contains $\preceq$ as a subset.

(can be computed in linear time)

Precedence constrained multiprocessor scheduling problem:

Given a set of tasks, the time required for each, the partial order relation $\preceq$, the number of robots available, and a positive integer T, can a car be assembled in at most T hours?

- NP-complete even if all tasks require the same number of hours
- in P if the number of robots is 1, 2, or $\geq$ the number of tasks
- unknown for 3 robots

CMPUT 272 (Stewart) University of Alberta **Lecture 18**

Reading: Epp 8.1-8.3

Recall:

Properties of binary relations: Let R be a relation on a set A.

R is *reflexive* $\Leftrightarrow \forall x \in A$, $(x, x) \in R$.

R is *symmetric* $\Leftrightarrow \forall x, y \in A$, if $(x, y) \in R$ then $(y, x) \in R$.

R is *antisymmetric* $\Leftrightarrow \forall x, y \in A$, if $(x, y) \in R$ and $(y, x) \in R$ then $x = y$.

R is *transitive* $\Leftrightarrow \forall x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$.

R is an *equivalence relation* $\Leftrightarrow$ R is reflexive, symmetric, and transitive.

R is a *partial order relation* $\Leftrightarrow$ R is reflexive, antisymmetric, and transitive.

Equivalence Relations: reflexive, symmetric, and transitive

Examples:

1. $=$ on $\mathbb{R}$
2. the equality relation on any set

   Three properties of equality: For all objects A, B, and C: (1) $A = A$, (2) if $A = B$ then $B = A$, (3) if $A = B$ and $B = C$ then $A = C$
3. P on $\mathbb{Z}$ where $x\ P\ y \Leftrightarrow x$ and y are both even or both odd
4. S on $\mathcal{P}(\{a, b, c\})$ where $(A, B) \in S \Leftrightarrow |A| = |B|$

What does the directed graph of an equivalence relation look like?

Example: Draw the directed graph representation of S (#4 above):

Theorem. The relation R on $\mathbb{Z}$ where $xRy \Leftrightarrow 5|(x-y)$ is an equivalence relation. (The relation R is called *congruence modulo 5*.)

Proof:

R is reflexive: $\forall x \in \mathbb{Z}$, $x - x = 0$ and $5|0$, so $5|(x-x)$ and therefore xRx.

R is symmetric: Let $x, y \in \mathbb{Z}$ such that xRy. Then $5|(x-y)$ (by the definition of R), and therefore $x - y = 5a$ for some $a \in \mathbb{Z}$ (by the definition of divides). Now $y - x = -(x-y) = -5a = 5(-a)$ and so $5|(y-x)$ and therefore yRx.

R is transitive: Let $x, y, z \in \mathbb{Z}$ such that xRy and yRz. Then $5|(x-y)$ and $5|(y-z)$ and therefore $x - y = 5a$ and $y - z = 5b$ for some $a, b \in \mathbb{Z}$. So $x - z = x - y + y - z = 5a + 5b = 5(a+b)$ and so $5|(x-z)$ and therefore xRz.

R is reflexive, symmetric, and transitive and therefore R is an equivalence relation. $\square$

Theorem. For any positive integer n, the relation R on $\mathbb{Z}$ where $xRy \Leftrightarrow n|(x-y)$ is an equivalence relation. (*congruence modulo* n)

Proof: The proof is similar.

Draw part of the directed graph for R on $\mathbb{Z}$ where $xRy \Leftrightarrow 5|(x-y)$.

Definitions. Let R be an equivalence relation on a set A.

For each $a \in A$, the *equivalence class of a in R*, denoted $[a]_R$ or $[a]$, is:

$$\{x \in A \mid xRa\}.$$

If $A = \{\ldots, a_1, a_2, a_3, \ldots\}$ then the *equivalence classes of R* are:

$$\ldots, [a_1], [a_2], [a_3], \ldots$$

Example: For R on $\mathbb{Z}$ where $xRy \Leftrightarrow 5|(x-y)$:

$\vdots$

$[-1] = \{x \in \mathbb{Z} \mid 5|(x-(-1))\} = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$

$[0] = \{x \in \mathbb{Z} \mid 5|(x-0)\} = \{\ldots, -5, 0, 5, 10, 15, \ldots\}$

$[1] = \{x \in \mathbb{Z} \mid 5|(x-1)\} = \{\ldots, -4, 1, 6, 11, \ldots\}$

$[2] = \{x \in \mathbb{Z} \mid 5|(x-2)\} = \{\ldots, -3, 2, 7, 12, \ldots\}$

$[3] = \{x \in \mathbb{Z} \mid 5|(x-3)\} = \{\ldots, -2, 3, 8, 13, \ldots\}$

$[4] = \{x \in \mathbb{Z} \mid 5|(x-4)\} = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$

$[5] = \{x \in \mathbb{Z} \mid 5|(x-5)\} = \{\ldots, -5, 0, 5, 10, 15, \ldots\}$

$\vdots$

The equivalence classes of R are $\quad \ldots, [-1], [0], [1], [2], \ldots$

Many of the equivalence classes coincide. For example, $[-3] = [2] = [7]$.

The *distinct* equivalence classes of R are $[0], [1], [2], [3], [4]$.

Definition. A *partition of a set A* is a set of nonempty mutually disjoint subsets of A whose union is A.

Examples:

- Which of the following are partitions of $\{1, 2, 3, 4, 5\}$?

  $\{\{1, 3, 4\}, \{2, 5\}\}$

  $\{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}$

  $\{\{1, 2, 3, 4, 5\}\}$

  $\{\emptyset, \{1, 2, 3, 4, 5\}\}$

  $\{1\}, \{2\}, \{3\}, \{4\}, \{5\}$

  $\{\{1, 2\}, \{3, 5\}\}$

  $\{\{1, 2\}, \{2, 3\}, \{4, 5\}\}$

  $\{\{1, 2\}, \{2\}, \{4, 5\}\}$

- For R on $\mathbb{Z}$ where $xRy \Leftrightarrow 5|(x - y)$:

  $\{[0], [1], [2], [3], [4]\}$ is a partition of $\mathbb{Z}$.

Theorem. If R is an equivalence relation on A then the set of distinct equivalence classes of R is a partition of A.

Proof: Let R be an equivalence relation on a set A. The set of distinct equivalence classes of R is $\{\ [a] \in \mathcal{P}(A) \mid a \in A\}$.

By the definition of equivalence relation, R is reflexive, symmetric, and transitive. Since R is reflexive, $a \in [a]$ for all $a \in A$. Therefore each equivalence class is nonempty and their union is A.

We now show that the distinct equivalence classes of R are mutually disjoint. Suppose not, that is, suppose there are equivalence classes $[a]$ and $[b]$ such that $[a] \neq [b]$ and $[a] \cap [b] \neq \emptyset$. Let $x \in [a] \cap [b]$. Then

$(x, a) \in R$ by the definition of $[a]$,

$(x, b) \in R$ by the definition of $[b]$,

$(a, x) \in R$ because $(x, a) \in R$ and R is symmetric,

$(a, b) \in R$ because $(a, x) \in R$ and $(x, b) \in R$ and R is transitive, and therefore

$(b, a) \in R$ since $(a, b) \in R$ and R is symmetric.

Therefore $a \in [b]$ and $b \in [a]$.

Now, for every element $x \in [a]$ we have $(x, a) \in R$ and $(a, b) \in R$, and so $(x, b) \in R$ by transitivity, and therefore $x \in [b]$. This shows that $[a] \subseteq [b]$.

Similarly, for every element $x \in [b]$ we have $(x, b) \in R$ and $(b, a) \in R$, so $(x, a) \in R$ by transitivity, and therefore $x \in [a]$. This shows that $[b] \subseteq [a]$.

But $[a] \subseteq [b]$ and $[b] \subseteq [a]$ imply $[a] = [b]$, which contradicts that $[a] \neq [b]$. $\Box$

Definition. The *relation induced by a partition of a set A* is the relation R on A where

$$xRy \Leftrightarrow x \text{ and } y \text{ are in the same element of the partition.}$$

Theorem. The relation induced by a partition is an equivalence relation.

Proof: Let S be a partition of a set A and let R be the relation on A induced by S.

R is reflexive: Every element of A is in the same element of S as itself.

R is symmetric: Let $x, y \in A$ such that xRy. Then x and y are in the same element of S and therefore y and x are in the same element of S and therefore yRx.

R is transitive: Let $x, y, z \in A$ such that xRy and yRz. Then x and y are in the same element of S and y and z are in the same element of S. This implies that x, y, and z are all in the same element of S and therefore xRz. □

Applications of equivalence relations

1. Arithmetic with big numbers: modular arithmetic and RSA encryption

   Definition. For any $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}^+$, *a is congruent to b modulo n*, denoted $a \equiv b \pmod{n}$, if and only if

   $$n|(a-b).$$

   Congruence modulo n is an equivalence relation.

   $\forall a, b, c, d, n \in \mathbb{Z}$, $n > 1$, if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$ then

   $$(a+b) \equiv (c+d) \pmod{n}$$
   $$(a-b) \equiv (c-d) \pmod{n}$$
   $$ab \equiv cd \pmod{n}$$
   $$a^m \equiv c^m \pmod{n} \ \ \forall m \in \mathbb{Z}^+$$

2. Graph connectivity:

   Let S be a relation on the nodes of a *symmetric* graph where:

   $$xSy \Leftrightarrow \text{there is a path from } x \text{ to } y.$$

   S is an equivalence relation.

   The equivalence classes are the connected components of the graph.

   Kruskal's MST algorithm uses dynamic equivalence relations / union-find operations to compute a minimum spanning tree of a network.

   Let T be a relation on the nodes of an *arbitrary* directed graph where:

   $$xTy \Leftrightarrow \text{there is a path from } x \text{ to } y \text{ and a path from } y \text{ to } x.$$

   T is an equivalence relation.

   The equivalence classes are the *strongly* connected components.

3. Analysis of algorithms: Asymptotic notation

For function $g : \mathbb{N} \mapsto \mathbb{R}^{nonneg}$:

$$\Theta(g) = \{f : \mathbb{N} \mapsto \mathbb{R}^{nonneg} \mid \text{there exist } c_1, c_2 \in \mathbb{R}^+ \text{ and } n_0 \in \mathbb{N} \text{ such that } 0 \leq c_1 g(n) \leq f(n) \leq c_2 g(n) \text{ for all } n \geq n_0\}$$

$$O(g) = \{f : \mathbb{N} \mapsto \mathbb{R}^{nonneg} \mid \text{there exist } c_2 \in \mathbb{R}^+ \text{ and } n_0 \in \mathbb{N} \text{ such that } 0 \leq f(n) \leq c_2 g(n) \text{ for all } n \geq n_0\}$$

$$\Omega(g) = \{f : \mathbb{N} \mapsto \mathbb{R}^{nonneg} \mid \text{there exist } c_1 \in \mathbb{R}^+ \text{ and } n_0 \in \mathbb{N} \text{ such that } 0 \leq c_1 g(n) \leq f(n) \text{ for all } n \geq n_0\}$$

Let C be a relation on the set of all functions from $\mathbb{N}$ to $\mathbb{R}^{nonneg}$ where

$$f \; C \; g \Leftrightarrow f \in \Theta(g).$$

C is an equivalence relation.

The equivalence classes are sets of functions that all have the same growth rate.

CMPUT 272 (Stewart) University of Alberta **Lecture 17**

Reading: Epp 1.3, 8.1-8.3

Relations

Definition. If A and B are sets, then
a *(binary) relation on* $A \times B$ (also called a *relation from* A *to* B)
is a subset of $A \times B$.

The following all mean that ordered pair $(x, y) \in A \times B$ is in the relation R:

$$x \text{ is related to } y \text{ in } R$$

$$(x, y) \in R$$

$$xRy$$

Definition. An *n-ary relation on* $A_1 \times \cdots \times A_n$ is a subset of $A_1 \times \cdots \times A_n$ where $A_1, \ldots, A_n$ are sets and $n \geq 2$.

Examples:

1. R from $\{1,2,3,4,5\}$ to $\{1,2,3,4,5\}$ (R on $\{1,2,3,4,5\}$) where
   $R = \{(1,1),(1,2),(1,3),(3,4),(2,4),(4,5),(5,4)\}$.

2. LE from $\mathbb{R}$ to $\mathbb{R}$ (LE on $\mathbb{R}$) where $x\ LE\ y \Leftrightarrow x \leq y$
   $LE = \{(x,y) \in \mathbb{R}^2 \mid x \leq y\}$

3. P from $\mathbb{Z}$ to $\mathbb{Z}$ (P on $\mathbb{Z}$) where
   $x\ P\ y \Leftrightarrow x$ and y are both even or both odd
   $P = \{(x,y) \in \mathbb{Z}^2 \mid$ x and y are both even or both odd $\}$

4. T from $\mathcal{P}(\{a,b,c\})$ to $\mathbb{Z}$ where $(A,x) \in T \Leftrightarrow |A| \geq x$
   $\{a\}\ T\ 0 \qquad (\emptyset, 2) \notin T$

5. Every function is a binary relation but not every binary relation is a function. For example, binary relations 1-4 above are not functions.

6. B on $\mathbb{R}^3$ where $(x,y,z) \in B \Leftrightarrow y < x < z$ or $z < x < y$

7. relational databases

   Let $A_1 =$ the set of all student names
   $A_2 =$ the set of all student numbers
   $A_3 =$ the set of all courses
   $A_4 = \{$ A+, A, A-, B+, B, B-, C+, C, C-, D+, D, F $\}$

   Define R on $A_1 \times A_2 \times A_3 \times A_4$ as follows:

   $(w,x,y,z) \in R \Leftrightarrow$ the student with name w and student number x took course y and received a grade of z.

Let R be a relation from A to B. The *inverse relation of* R is the relation R^{-1} from B to A defined as follows:

$$R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}.$$

Every binary relation has an inverse relation.

(But only bijective functions have inverse functions.)

A binary relation R on a (small, finite) set A can be given as

- a set of ordered pairs
- a *directed graph*
  - like an arrow diagram of a function except each element of A is drawn only once
  - $\forall x, y \in A$, there is an arrow from x to $y \Leftrightarrow xRy \Leftrightarrow (x, y) \in R$
- a *Boolean matrix*
  - $|A| \times |A|$ square matrix
  - $\forall x, y \in A$, entry $(x, y) = \begin{cases} 1 & \text{if } (x, y) \in R \\ 0 & \text{if } (x, y) \notin R \end{cases}$

Example: Define a relation R on $\{1, 2, 3, 4, 5\}$ as

$$R = \{(1, 1), (1, 2), (1, 3), (3, 4), (2, 4), (4, 5), (5, 4)\}.$$

Give the directed graph representation of R.

Give the Boolean matrix representation of R.

What is R^{-1}, the inverse relation of R?

Is R a function? Is R^{-1} a function?

How many binary relations are there on $\{1, 2, 3, 4, 5\}$?

Answer: The Boolean matrix has 25 entries, each of which is 0 or 1. Therefore the number of binary relations on A is $2^{25} = 33,554,432$.

Properties of binary relations: Let R be a relation on a set A.

R is *reflexive* $\Leftrightarrow \forall x \in A$, $(x, x) \in R$.

R is *symmetric* $\Leftrightarrow \forall x, y \in A$, if $(x, y) \in R$ then $(y, x) \in R$.

R is *antisymmetric* $\Leftrightarrow \forall x, y \in A$, if $(x, y) \in R$ and $(y, x) \in R$ then $x = y$.

R is *transitive* $\Leftrightarrow \forall x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$.

R is an *equivalence relation* $\Leftrightarrow$ R is reflexive, symmetric, and transitive.

R is a *partial order relation* $\Leftrightarrow$ R is reflexive, antisymmetric, and transitive.

Reading: Epp 1.3, 7

Definition. A *function* from a set X to a set Y is a relation from X to Y such that:

- every element in X is related to some element in Y, and
- no element in X is related to more than one element in Y.

$f : X \mapsto Y$ means "f is a function from X to Y".
"f maps the set X to the set Y."
"f is a mapping from X to Y."

The *domain* of f is X.
The *co-domain* of f is Y.

For each $x \in X$, $f(x)$ denotes the (unique) element of Y that f maps x to.
"the *value* of f at x."
"the *image* of x (under f)."

The *image of* $A \subseteq X$ is

- the set of all elements of Y that are mapped to by at least one element of A.
- $f(A) = \{y \in Y \mid y = f(x) \text{ for some } x \in A\}$.

The *range* of f is the image of X.

The *preimage* (or *inverse image*) of $y \in Y$ is

- the set of all elements of X that map to y.
- $\{x \in X \mid f(x) = y\}$.

The *preimage* of $C \subseteq Y$ is

- the set of all elements of X that map to an element of C.
- $\{x \in X \mid f(x) \in C\}$.

Definition. Two functions are *equal* if and only if they have

- the same domain,
- the same co-domain, and
- the same value at each element of the domain.

Examples of functions:

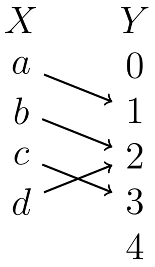
1. $f : X \mapsto Y$ where $X = \{a, b, c, d\}$, $Y = \{0, 1, 2, 3, 4\}$, and:

$f(a) = 1$
$f(b) = 2$
$f(c) = 3$
$f(d) = 2$

or

x	$f(x)$
a	1
b	2
c	3
d	2

or



or $\quad f = \{(a, 1), (b, 2), (c, 3), (d, 2)\}$

The domain of f is X.

The co-domain of f is Y.

The range of f is $\{1, 2, 3\}$.

2. The function computed by the Division Algorithm is:

   $D : \mathbb{N} \times \mathbb{Z}^+ \mapsto \mathbb{N}^2$ where each ordered pair $(a, d) \in \mathbb{N} \times \mathbb{Z}^+$ maps to the ordered pair $(q, r) \in \mathbb{N}^2$ such that

$$a = dq + r \text{ and } 0 \leq r < d.$$

   Every deterministic algorithm computes a function from the set of all inputs to the set of outputs.

3. $mod : \mathbb{Z} \times \mathbb{Z}^+ \mapsto \mathbb{Z}$ where for each integer n and positive integer d,

   $mod(n, d) = n \bmod d = r$ where $n = dq+r$, q and r are integers, and $0 \leq r < d$.

4. $gcd : \mathbb{Z}^2 - \{(0, 0)\} \mapsto \mathbb{Z}^+$ where, for all $a, b \in \mathbb{Z}$ that are not both zero,

$$gcd(a, b) = \text{ the largest integer that divides both } a \text{ and } b.$$

5. A sequence is a function: $\frac{1}{1^2}, \frac{1}{2^2}, \frac{1}{3^2}, \frac{1}{4^2}, \ldots$

   $f : \mathbb{Z}^+ \mapsto \mathbb{Q} \qquad f(n) = \frac{1}{n^2}$

6. $I_X : X \mapsto X \qquad I_X(x) = x$ for all $x \in X$ $\qquad$ The identity function on X

7. $C : \mathcal{P}(\{r, g, b\}) \mapsto \mathbb{N}$ where $C(X) = |X|$

8. $B : \{0, 1\}^4 \mapsto \{0, 1\}$ where $B(x_1, x_2, x_3, x_4) = (x_1 \vee x_2) \wedge \sim (x_3 \wedge x_4)$

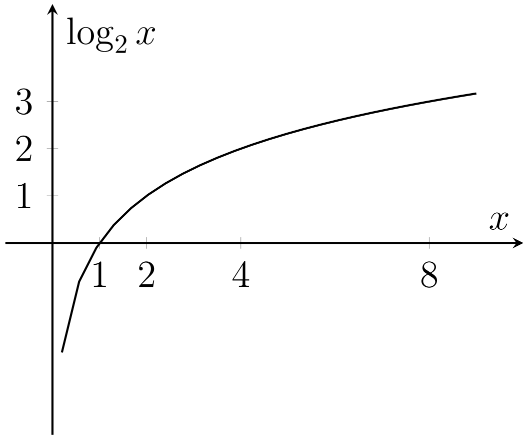
9. For $b \in \mathbb{R}^+$, $b \neq 1$, $x \in \mathbb{R}^+$, and $y \in \mathbb{R}$, the *logarithm* to the base b of x is the power to which b must be raised to equal x. That is,

$$\log_b x = y \;\Leftrightarrow\; b^y = x.$$

$\log_3 9 = 2$	For all $b \in \mathbb{R}^+$, $b \neq 1$, and all $x \in \mathbb{R}^+$:
$\log_2 1024 = 10$	$b^{\log_b x} = x$
$\log_2 \frac{1}{2} = -1$	$\log_b b^x = x$
$\log_{99} 1 = 0$	$\log_b 1 = 0$

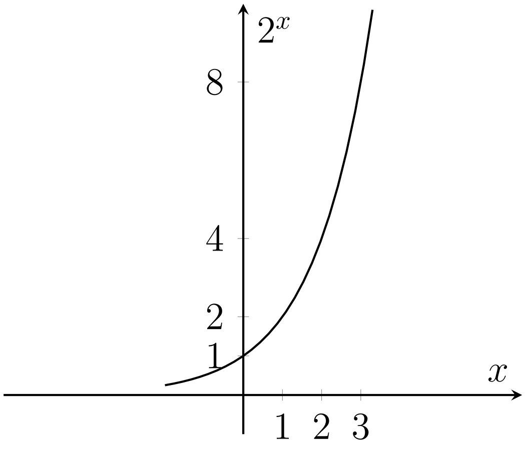
The *logarithmic function with base b* is the function from $\mathbb{R}^+$ to $\mathbb{R}$ that takes each positive real number x to $\log_b x$.

Graph of the logarithmic function with base 2:



10. The *exponential function with base b* is the function from $\mathbb{R}$ to $\mathbb{R}^+$ that takes each real number x to b^x.

Graph of the exponential function with base 2:



11. $f : \mathbb{R}^{nonneg} \mapsto \mathbb{R}^{nonneg}$ where $f(x) = \sqrt{x}$

    Every nonnegative real number has a unique nonnegative real square root: its *principle square root.*

But these are not functions:

$g : \mathbb{R}^{nonneg} \mapsto \mathbb{R}$ where $g(x) = y$ if and only if $x = y^2$

Not a function because, for example, 4 is related to both 2 and -2.

$h : \mathbb{R}^{nonneg} \mapsto \mathbb{Q}^{nonneg}$ where $h(x) = \sqrt{x}$

Not a function: since $\sqrt{2}$ is irrational, 2 does not map to any rational number.

Definitions. A function $F : X \mapsto Y$ is

one-to-one $\Leftrightarrow \forall x_1, x_2 \in X$, if $F(x_1) = F(x_2)$ then $x_1 = x_2$;

onto $\Leftrightarrow \forall y \in Y$, $\exists x \in X$ such that $F(x) = y$.

More examples:

12. Let $f : \mathbb{R} \mapsto \mathbb{R}$ where $f(x) = 4x - 1$ for all $x \in \mathbb{R}$.

Theorem. f is one-to-one.

Proof: Let $x_1, x_2 \in \mathbb{R}$ such that

$$f(x_1) = f(x_2).$$

Then

$$4x_1 - 1 = 4x_2 - 1$$

so

$$4x_1 = 4x_2$$

and therefore

$$x_1 = x_2.$$

□

Theorem. f is onto.

Proof: Let $y \in \mathbb{R}$.

Let $x = \frac{y+1}{4}$.

$x \in \mathbb{R}$ since sums and quotients of real numbers are real numbers.

$$\begin{aligned} f(x) &= f\left(\frac{y+1}{4}\right) \\ &= 4\left(\frac{y+1}{4}\right) - 1 \\ &= y + 1 - 1 \\ &= y. \end{aligned}$$

□

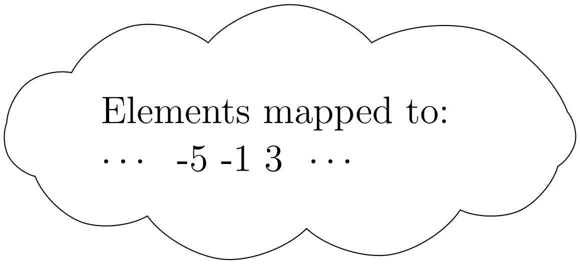
If $y = f(x)$ for some $x \in \mathbb{R}$
then $y = 4x - 1$
so $4x = y + 1$
and therefore $x = \frac{y+1}{4}$.

13. Let $h : \mathbb{Z} \mapsto \mathbb{Z}$ where $h(x) = 4x - 1$ for all $x \in \mathbb{Z}$.

    Note: $h \neq f$

    h **is one-to-one** by reasoning similar to the proof that f is one-to-one.

    h **is not onto.**



Proof: $0 \in \mathbb{Z}$, the co-domain of h. We prove by contradiction that 0 is not in the range of h. Suppose that 0 is in the range of h, that is, there is an $x \in \mathbb{Z}$ such that

$$h(x) = 0.$$

Then

$$4x - 1 = 0$$

so

$$4x = 1$$

and therefore

$$x = \frac{1}{4}.$$

But then $x \notin \mathbb{Z}$, a contradiction. □

14. The *floor function* is the function from $\mathbb{R}$ to $\mathbb{Z}$ that takes each real number x to $\lfloor x \rfloor$, the *floor of x*.

    not one-to-one: $\lfloor 2.9 \rfloor = \lfloor 2.1 \rfloor = 2$

    onto: For all $n \in \mathbb{Z}$, we have $n \in \mathbb{R}$ and $\lfloor n \rfloor = n$.

Definition: A function $F : X \mapsto Y$ is
one-to-one $\Leftrightarrow \forall x_1, x_2 \in X$, if $F(x_1) = F(x_2)$ then $x_1 = x_2$;
onto $\Leftrightarrow \forall y \in Y$, $\exists x \in X$ such that $F(x) = y$;
a *one-to-one correspondence (or bijection)* $\Leftrightarrow$ it is both one-to-one and onto.

The inverse function of a one-to-one correspondence $F : X \mapsto Y$:

- a function from Y to X that "undoes" the action of F, that is, it sends each element of Y back to the element of X that it came from.
- $\{(y, x) \mid y \in Y, x \in X, \text{ and } F(x) = y\}$
  - is a function because F is one-to-one and onto,
  - is one-to-one and onto because F is a function, and
  - maps each $y \in Y$ to the element $x \in X$ that F maps to y.

It follows from the second point above that

- Every bijection has an inverse function.
- The inverse function of a bijection is a bijection.

Definition: If $F : X \mapsto Y$ is a one-to-one correspondence, then the *inverse function* for F is the function $F^{-1} : Y \mapsto X$ such that for all $y \in Y$,

$$F^{-1}(y) = \text{the unique element } x \in X \text{ such that } y = F(x).$$

In other words, for all $x \in X$ and all $y \in Y$,

$$F^{-1}(y) = x \ \Leftrightarrow \ y = F(x).$$

Theorem. If $F : X \mapsto Y$ is a one-to-one correspondence, then $(F^{-1})^{-1} = F$.

Proof: Both functions have domain X and co-domain Y and, for all $x \in X$ and all $y \in Y$, $F(x) = y \ \Leftrightarrow \ F^{-1}(y) = x \ \Leftrightarrow \ (F^{-1})^{-1}(x) = y$. $\square$

Examples (from before):

6. $I_X : X \mapsto X$ where $I_X(x) = x$ for all $x \in X$. The identity function on X.

   I_X is a one-to-one correspondence and $I_X^{-1} = I_X$.

9. Let $L : \mathbb{R}^+ \mapsto \mathbb{R}$ be the function defined by $L(x) = \log_2 x$.

   Let $E : \mathbb{R} \mapsto \mathbb{R}^+$ be the function defined by $E(x) = 2^x$.

   L is a one-to-one correspondence; therefore L has an inverse function.

   $L^{-1} : \mathbb{R} \mapsto \mathbb{R}^+$ such that for all $x \in \mathbb{R}^+$, $y \in \mathbb{R}$,

   $$\begin{aligned} L^{-1}(y) = x &\Leftrightarrow y = L(x) \\ &\Leftrightarrow y = \log_2 x \\ &\Leftrightarrow 2^y = 2^{\log_2 x} \\ &\Leftrightarrow 2^y = x. \end{aligned}$$

   That is, $L^{-1}(y) = 2^y$ for all $y \in \mathbb{R}$. So $L^{-1} = E$. And $E^{-1} = L$.

11. Let $f : \mathbb{R}^{nonneg} \mapsto \mathbb{R}^{nonneg}$ where $f(x) = \sqrt{x}$.

    f is a one-to-one correspondence; therefore f has an inverse function.

    $f^{-1} : \mathbb{R}^{nonneg} \mapsto \mathbb{R}^{nonneg}$ such that for all $x, y \in \mathbb{R}^{nonneg}$,

    $$\begin{aligned} f^{-1}(y) = x &\Leftrightarrow y = f(x) \\ &\Leftrightarrow y = \sqrt{x} \\ &\Leftrightarrow y^2 = x. \end{aligned}$$

    That is, $f^{-1}(y) = y^2$ for all $y \in \mathbb{R}^{nonneg}$.

12. Let $f : \mathbb{R} \mapsto \mathbb{R}$ where $f(x) = 4x - 1$ for all $x \in \mathbb{R}$.

    f is a one-to-one correspondence; therefore f has an inverse function.

    $f^{-1} : \mathbb{R} \mapsto \mathbb{R}$ such that for all $x, y \in \mathbb{R}$,

    $$\begin{aligned} f^{-1}(y) = x &\Leftrightarrow y = f(x) \\ &\Leftrightarrow y = 4x - 1 \\ &\Leftrightarrow x = \frac{y+1}{4}. \end{aligned}$$

    That is, $f^{-1}(y) = \frac{y+1}{4}$ for all $y \in \mathbb{R}$.

Composition of functions.

Definition.[1]
Let $f : X \mapsto Y$ and $g : Y \mapsto Z$ be functions.
The *composition of f and g* is the function $g \circ f : X \mapsto Z$ where

$$(g \circ f)(x) = g(f(x)) \quad \text{for all } x \in X.$$

Example:

Let $f : \mathbb{R} \mapsto \mathbb{R}$ where $f(x) = x^2$ for all $x \in \mathbb{R}$

and $g : \mathbb{R} \mapsto \mathbb{R}$ where $g(x) = x + 5$ for all $x \in \mathbb{R}$.

Then $g \circ f : \mathbb{R} \mapsto \mathbb{R}$ where for all $x \in \mathbb{R}$,

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) \\ &= g(x^2) \\ &= x^2 + 5 \end{aligned}$$

and $f \circ g : \mathbb{R} \mapsto \mathbb{R}$ where for all $x \in \mathbb{R}$,

$$\begin{aligned} (f \circ g)(x) &= f(g(x)) \\ &= f(x + 5) \\ &= (x + 5)^2 \\ &= x^2 + 10x + 25. \end{aligned}$$

[1] The co-domain of f does not have to be equal to the domain of g. All that is required is that the range of f be a subset of the domain of g.

Theorem. If $f : X \mapsto Y$ is a bijection, then

$$(1)\ f^{-1} \circ f = I_X \qquad \text{and} \qquad (2)\ f \circ f^{-1} = I_Y.$$

Proof: Suppose $f : X \mapsto Y$ is a bijection.

1. Let $x \in X$ and let $y \in Y$ such that $f(x) = y$.

   By the definition of function composition, $f^{-1} \circ f$ is a function from X to X, and

   $$\begin{aligned}(f^{-1} \circ f)(x) &= f^{-1}(f(x)) \\ &= f^{-1}(y) \quad \text{since } f(x) = y \\ &= x \quad \text{by definition of inverse, since } f(x) = y.\end{aligned}$$

   Therefore $f^{-1} \circ f = I_X$ by the definition of the identity function.

2. Let $y \in Y$ and let $x \in X$ such that $f^{-1}(y) = x$.

   By the definition of function composition, $f \circ f^{-1}$ is a function from Y to Y, and

   $$\begin{aligned}(f \circ f^{-1})(y) &= f(f^{-1}(y)) \\ &= f(x) \quad \text{since } f^{-1}(y) = x \\ &= y \quad \text{by definition of inverse, since } f^{-1}(y) = x.\end{aligned}$$

   Therefore $f \circ f^{-1} = I_Y$ by the definition of the identity function. □

Theorem. If $f : X \mapsto Y$ and $g : Y \mapsto Z$ are both one-to-one functions, then $g \circ f$ is one-to-one.

Proof: Suppose $f : X \mapsto Y$ and $g : Y \mapsto Z$ are both one-to-one functions. Let $x_1, x_2 \in X$ such that

$$(g \circ f)(x_1) = (g \circ f)(x_2).$$

Then

$$g(f(x_1)) = g(f(x_2)) \qquad \text{by the definition of composition.}$$

So

$$f(x_1) = f(x_2) \qquad \text{since } g \text{ is one-to-one}$$

and therefore

$$x_1 = x_2 \qquad \text{since } f \text{ is one-to-one.}$$

This proves that $g \circ f$ is one-to-one. □

Theorem. If $f : X \mapsto Y$ and $g : Y \mapsto Z$ are both onto functions, then $g \circ f$ is onto.

Proof: Suppose $f : X \mapsto Y$ and $g : Y \mapsto Z$ are both onto functions.

Let $z \in Z$. [We need to show that $\exists x \in X$ such that $(g \circ f)(x) = z$.]

Since g is onto, it maps some element of Y to z; let $y \in Y$ such that $g(y) = z$. Since f is onto, it maps some element of X to y; let $x \in X$ such that $f(x) = y$.

Now

$$(g \circ f)(x) = g(f(x)) = g(y) = z.$$

Therefore $g \circ f$ is onto. □

Cardinality and infinite sets [Epp Chapter 7.4]

Definition. A set is:

- *finite* if it is the empty set, or there is a bijection from $\{1, 2, \ldots, n\}$ to it for some $n \in \mathbb{Z}^+$;
- *infinite* if it is not finite;
- *countable* if it is finite or there is a bijection from $\mathbb{Z}^+$ to it;
- *uncountable* if it is not countable.

Theorem. $\mathbb{Z}$ is countable.

Proof: Let $F : \mathbb{Z}^+ \mapsto \mathbb{Z}$ where

$$F(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is an even positive integer} \\ -\left(\frac{n-1}{2}\right) & \text{if } n \text{ is an odd positive integer} \end{cases}$$

F is one-to-one:
Let $n_1, n_2 \in \mathbb{Z}^+$ such that $F(n_1) = F(n_2)$.
If $F(n_1) > 0$ then $F(n_1) = \frac{n_1}{2} = F(n_2) = \frac{n_2}{2}$, and so $n_1 = n_2$.
If $F(n_1) \leq 0$ then $F(n_1) = -\left(\frac{n_1-1}{2}\right) = F(n_2) = -\left(\frac{n_2-1}{2}\right)$, and so $n_1 = n_2$.

F is onto:
Let $q \in \mathbb{Z}$. [We must find a positive integer that F maps to q.]
If $q > 0$ then $2q \in \mathbb{Z}^+$ and $F(2q) = \frac{2q}{2} = q$.
If $q \leq 0$ then $-2q + 1 \in \mathbb{Z}^+$ and $F(-2q+1) = -\left(\frac{(-2q+1)-1}{2}\right) = \frac{2q}{2} = q$.
□

Theorem. $\mathbb{Q}$ is countable.

Theorem. $\mathbb{R}$ is uncountable.

Reading: Epp 1.2, 1.3, 6, 7.1

A generalized distributive law for sets

Notation. For integers $m \leq n$ and sets $A_m, A_{m+1}, \ldots, A_n$:

$$\bigcup_{i=m}^{n} A_i = A_m \cup A_{m+1} \cup \cdots \cup A_n \qquad \text{and} \qquad \bigcap_{i=m}^{n} A_i = A_m \cap A_{m+1} \cap \ \cdots \ \cap A_n.$$

Use mathematical induction and set identities (Epp, Theorem 6.2.2) to prove the following generalized distributive law:

Theorem. For all integers $n \geq 1$, if A and $B_1, B_2, \ldots, B_n$ are any sets then

$$A \cap \left(\bigcup_{i=1}^{n} B_i \right) = \bigcup_{i=1}^{n} (A \cap B_i).$$

Proof (by induction): Let $P(n)$ mean $A \cap (\bigcup_{i=1}^{n} B_i) = \bigcup_{i=1}^{n}(A \cap B_i)$.
We prove $P(n)$ holds for all $n \geq 1$ by induction.
Basis step:
The LHS and RHS of $P(1)$ are both equal to $A \cap B_1$, so $P(1)$ holds.

Inductive Step: Let $k \geq 1$ be an arbitrary integer and assume that $P(k)$ holds. We prove $P(k+1)$.

$$\begin{aligned} A \cap \left(\bigcup_{i=1}^{k+1} B_i \right) &= A \cap \left(\left(\bigcup_{i=1}^{k} B_i \right) \cup B_{k+1} \right) && \text{by the definition of } \bigcup \\ &= \left(A \cap \left(\bigcup_{i=1}^{k} B_i \right) \right) \cup (A \cap B_{k+1}) && \text{distributive law} \\ &= \left(\bigcup_{i=1}^{k} (A \cap B_i) \right) \cup (A \cap B_{k+1}) && \text{inductive hypothesis} \\ &= \bigcup_{i=1}^{k+1} (A \cap B_i) && \text{definition of } \bigcup \end{aligned}$$

□

The Number of Subsets of a Set

Theorem. For all $n \in \mathbb{N}$, if a set X has $|X| = n$, then $|\mathcal{P}(X)| = 2^n$.
That is, for all $n \in \mathbb{N}$, if a set has (exactly) n elements, then it has (exactly) 2^n subsets.

Proof (by mathematical induction):

Basis step: [We have to show that every set with zero elements has 2^0 subsets.] The only set with zero elements is the empty set, which has $2^0 = 1$ subset, namely the empty set.

Inductive step: Let $k \in \mathbb{N}$ such that every set with k elements has 2^k subsets. [We must show that every set with $k+1$ elements has 2^{k+1} subsets.]

Let X be a set with $k+1$ elements.

Since $k \in \mathbb{N}$, we know that $k + 1 \geq 1$. Therefore X has at least one element and we may let z be an element of X.

Observe that any subset of X either contains z or not.

And any subset A of X that does not contain z can be matched up with a subset B, equal to $A \cup \{z\}$, of X that contains z. This means that there are as many subsets of X that contain z as there are subsets of X that do not contain z.

Finally, note that the subsets of X that do not contain z are precisely the subsets of $X - \{z\}$.

Combining these facts, we see that the number of subsets of X is equal to

$$\begin{aligned}
|\mathcal{P}(X)| &= \text{the number of subsets of } X \text{ that do not contain } z \\
&\qquad + \text{ the number of subsets of } X \text{ that contain } z \\
&= 2 \cdot |\mathcal{P}(X - \{z\})| \\
&= 2 \cdot 2^k \qquad\qquad \text{by the inductive hypothesis} \\
&= 2^{k+1}
\end{aligned}$$

□

Russell's paradox [Epp Chapter 6.4]

Let S be the set of all sets that are not elements of themselves:

$$S = \{A \mid A \text{ is a set and } A \notin A\}.$$

$\emptyset \in S$
$\{1, 2, 3\} \in S$
$\mathbb{Z} \in S$
the set of all sets $\notin S$

$S \in S$?

The Barber Puzzle

In a certain town there is a male barber who shaves all those men, and only those men, who do not shave themselves.

Does the barber shave himself?

In both cases, the situation cannot exist:
- there cannot be such a barber
- S is not a set

Halting Problem. Given an algorithm X and an input D, does X halt when run on input D?

Theorem. [Alan Turing, 1936] There cannot exist a computer algorithm for solving the halting problem.

Proof (by contradiction): Suppose there is an algorithm, CheckHalt, such that for a given algorithm X and input D:

```
CheckHalt($X, D$):
    prints "halts" if $X$ halts on input $D$;
    prints "loops forever" if $X$ does not halt on input $D$.
```

Note that the sequence of characters making up an algorithm X can be regarded as input to another algorithm (eg. a compiler) or even to X itself.

Now define a new algorithm, Test, such that, for any input algorithm X:

```
Test($X$):
    loops forever if CheckHalt($X, X$) prints "halts";
    stops if CheckHalt($X, X$) prints "loops forever".
```

Now, what happens when Test is run on input Test?

If Test(Test) halts then it doesn't, and if it doesn't halt, then it does! This is a contradiction, which proves the theorem. □

Ordered tuples

Definition. Let $n \in \mathbb{Z}^+$. An *ordered n-tuple* is
a sequence (an ordered list) of n (not necessarily distinct) elements.

Examples:

$(x_1, x_2, \ldots, x_n)$ an ordered n-tuple

$(0, 1, 0, 0, 1)$ an ordered 5-tuple

$(5, 11, 5)$ an ordered triple

$(1, 11)$ an ordered pair

$(x, (y, z))$ another ordered pair

Equality of ordered n-tuples:

$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \Leftrightarrow x_1 = y_1$, $x_2 = y_2$, $\ldots$, and $x_n = y_n$

Examples:

$(3, (-2)^2, \frac{1}{2}) = (\sqrt{9}, 4, \frac{3}{6})$

$(0, 1, 0, 0, 1) \neq (1, 1, 0, 0, 0)$

$(x, (y, z)) \neq ((x, y), z)$

$(x, (y, z)) \neq (x, y, z)$

Cartesian products

Definition. The *Cartesian product* of $n \geq 2$ sets $A_1, A_2, \ldots A_n$, is
$A_1 \times A_2 \times \cdots \times A_n = \{\ (a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$.

Examples:

$\{3, 4\} \times \{a, b, c\} = \{(3, a), (3, b), (3, c), (4, a), (4, b), (4, c)\}$

$\{0, 1\} \times \{0, 1\} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$

For any set A, $A \times \emptyset = \emptyset \times A = \emptyset$

For nonempty sets A, B, and C, these are all different:

$$(A \times B) \times C \qquad\qquad A \times (B \times C) \qquad\qquad A \times B \times C$$

Definition. For any set A: $A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ times}}$ for $n \geq 2$.

Examples:

$\{0, 1\}^3 = \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}$

$\mathbb{Z}^2$ is the set of all ordered pairs of integers

$\mathbb{R}^2$ is the set of all ordered pairs of real numbers: points in the plane

Relations

Definition. A *relation* from a set A to a set B is a subset of $A \times B$.

If R is a relation from A to B:

$R \subseteq A \times B$

$(a, b) \in R$ means "a is related to b" in R

Examples: A few relations from $\{a, b, c, d\}$ to $\{0, 1, 2, 3, 4\}$:

$\{(a, 0), (c, 2), (d, 4)\}$
$\{(a, 0), (a, 4), (d, 1), (b, 3), (c, 3)\}$
$\{(a, 1), (b, 2), (c, 3), (d, 2)\}$
$\{a, b, c, d\} \times \{0, 1, 2, 3, 4\}$

Functions

Definition. A *function* from a set X to a set Y is a relation from X to Y such that:

- every element in X is related to some element in Y, and
- no element in X is related to more than one element in Y.

$f : X \mapsto Y$ means "f is a function from X to Y".
"f maps the set X to the set Y."
"f is a mapping from X to Y."

The *domain* of f is X.

The *co-domain* of f is Y.

For each $x \in X$, $f(x)$ denotes the (unique) element of Y that f maps x to.
"the *value* of f at x."
"the *image* of x (under f)."

The *range* of f is $\{\ y \in Y \mid y = f(x) \text{ for some } x \in X\}$.

Examples of functions:

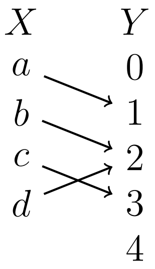
1. $f : X \mapsto Y$ where $X = \{a, b, c, d\}$, $Y = \{0, 1, 2, 3, 4\}$, and:

$f(a) = 1$
$f(b) = 2$
$f(c) = 3$
$f(d) = 2$

or

x	$f(x)$
a	1
b	2
c	3
d	2

or



or $\quad f = \{(a, 1), (b, 2), (c, 3), (d, 2)\}$

The domain of f is X.

The co-domain of f is Y.

The range of f is $\{1, 2, 3\}$.

2. The function computed by the Division Algorithm is:
$D : \mathbb{N} \times \mathbb{Z}^+ \mapsto \mathbb{N}^2$ where each ordered pair $(a, d) \in \mathbb{N} \times \mathbb{Z}^+$ maps to the ordered pair $(q, r) \in \mathbb{N}^2$ such that

$$a = dq + r \text{ and } 0 \leq r < d.$$

Every deterministic algorithm computes a function from the set of all inputs to the set of outputs.

3. $mod : \mathbb{Z} \times \mathbb{Z}^+ \mapsto \mathbb{Z}$ where for each integer n and positive integer d,

$mod(n, d) = n \bmod d = r$ where $n = dq+r$, q and r are integers, and $0 \leq r < d$.

4. $gcd : \mathbb{Z}^2 - \{(0, 0)\} \mapsto \mathbb{Z}^+$ where, for all $a, b \in \mathbb{Z}$ that are not both zero,

$$gcd(a, b) = \text{ the largest integer that divides both } a \text{ and } b.$$

5. A sequence is a function: $\frac{1}{1^2}, \frac{1}{2^2}, \frac{1}{3^2}, \frac{1}{4^2}, \ldots$
$f : \mathbb{Z}^+ \mapsto \mathbb{Q} \qquad f(n) = \frac{1}{n^2}$

6. $I_X : X \mapsto X \qquad I_X(x) = x$ for all $x \in X \qquad$ The identity function on X

CMPUT 272 (Stewart) University of Alberta **Lecture 14**

Reading: Epp Chapter 1.2, Chapter 6

Set Theory

Definition. A *set* is an unordered collection of distinct elements.

Notation:

$S = \{1, 2, 5, 10, 4\}$	set-roster notation
$1 \in S, 2 \in S, 3 \notin S$	element / member / in / not in
$\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$	set-builder notation
$\emptyset = \{\}$	empty set: the set with no elements

Definitions. For sets A and B:

A is a *subset* of B :	$A \subseteq B \;\Leftrightarrow\; \forall x, (x \in A \to x \in B)$
A is a *proper subset* of B :	$A \subset B \;\Leftrightarrow\; A \subseteq B$ and $\exists x, (x \notin A$ and $x \in B)$
A is *equal* to B :	$A = B \;\Leftrightarrow\; A \subseteq B$ and $B \subseteq A$

Definition.
For a set A, the *power set* of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

Examples:

$\{2\} \subseteq \{1, 2\}$

$\{1, 2\} \subseteq \{1, 2\}$ every set is a subset of itself

$\emptyset \subseteq \{1, 2\}$ the empty set is a subset of every set

$\emptyset \subseteq \emptyset$

$\emptyset \notin \emptyset$

$\emptyset \in \{\{1, 2\}, \emptyset, 1\}$

$2 \notin \{\{1, 2\}, \emptyset, 1\}$

$\{1, 2\} \in \{\{1, 2\}, \emptyset, 1\}$

$\{1, 2\} \not\subseteq \{\{1, 2\}, \emptyset, 1\}$

$\{\{1, 2\}\} \subset \{\{1, 2\}, \emptyset, 1\}$

$\{1, 3, 4, 2\} = \{2, 3, 1, 4\}$

$\{a \in \mathbb{Z} \mid a = 5p + 2 \text{ for some } p \in \mathbb{Z}\} = \{b \in \mathbb{Z} \mid b = 5q - 3 \text{ for some } q \in \mathbb{Z}\}$

$\mathcal{P}(\{1, 2, 3\}) = \{\ \emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\ \}$

$\mathcal{P}(\emptyset) = \{\emptyset\}$

Definitions (repeated from last page). For sets A and B:

A is a *subset* of B :	$A \subseteq B \;\Leftrightarrow\; \forall x, (x \in A \to x \in B)$
A is a *proper subset* of B :	$A \subset B \;\Leftrightarrow\; A \subseteq B$ and $\exists x, (x \notin A$ and $x \in B)$
A is *equal* to B :	$A = B \;\Leftrightarrow\; A \subseteq B$ and $B \subseteq A$

Theorem. For sets A and B, $A = B \;\Leftrightarrow\; \forall x, (x \in A \leftrightarrow x \in B)$.

Proof:
The proof uses definitions and logical equivalences, including (see Epp 3.3.55):

$$(\forall x, (P(x)) \wedge (\forall x, Q(x)) \;\equiv\; \forall x, (P(x) \wedge Q(x))$$

$$\begin{aligned}
A = B &\Leftrightarrow A \subseteq B \;\wedge\; B \subseteq A && \text{by the definition of set equality}\\
&\Leftrightarrow (\forall x, (x \in A \to x \in B)) \;\wedge\; (\forall x, (x \in B \to x \in A)) && \text{definition of } \subseteq\\
&\Leftrightarrow \forall x, ((x \in A \to x \in B) \wedge (x \in B \to x \in A)) && \text{above logical equivalence}\\
&\Leftrightarrow \forall x, (x \in A \leftrightarrow x \in B) && \text{biconditional as and of conditionals} \qquad \square
\end{aligned}$$

Notation. For any finite set A, the number of elements of A (also called the *cardinality of* A) is denoted by $|A|$ or $N(A)$.

Examples:

$N(\{5, 1, 3, 7\}) = 4$

$|\{1, 2, 3, 4, \{1, 2\}, \{1, 2, 3\}, \emptyset\}| = 7$

$|\emptyset| = 0$

$|\mathcal{P}(\emptyset)| = 1$

Definition. A *universal set* or *universe of discourse* is the set of all elements under discussion in a particular context.

- When using set-builder notation, a universal set must be specified.

  $\{x \mid x \notin \{1,2,3,4\}\}$ not a set

  $\{x \in \mathbb{Z} \mid x \notin \{1,2,3,4\}\}$ a set

  $\{x \in \mathbb{Z}^+ \mid x \notin \{1,2,3,4\}\}$ a different set

Set operations: Let A and B be subsets of a universal set U.

The *union* of A and B : $A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$

The *intersection* of A and B : $A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$

The *set difference* B minus A : $B - A = \{x \in U \mid x \in B \text{ and } x \notin A\}$

The *complement* of A : $A^c = \{x \in U \mid x \notin A\}$

Example: Let $U = \{1,2,3,4,5,6,7\}$ be the universal set,

$V = \{4\}$, $W = \{7\}$, $X = \{1,2,3\}$, $Y = \{2,3,4\}$, $Z = \{4,5,6\}$.

$X \cap Z = \emptyset$ disjoint sets

W, X, and Z pairwise disjoint or mutually disjoint sets

$Y^c = \{1,5,6,7\}$

$X \cup Y \cup Z = \{7\}^c$

$|X \cup Y \cup Z| = 6$

$|X \cap Y \cap Z| = 0$

$Y \cap Z = V$

$Y - Z = \{2,3\}$

A Venn diagram may help to:

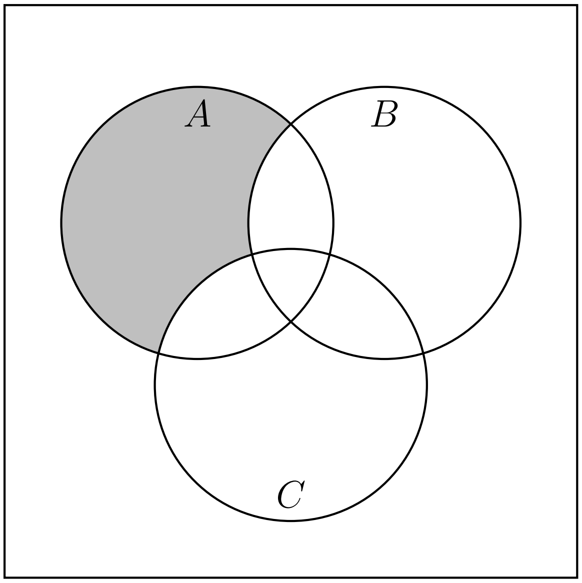
- determine whether a claim is true or false
- find a counterexample to a false universal claim

Methods of proof in set theory:

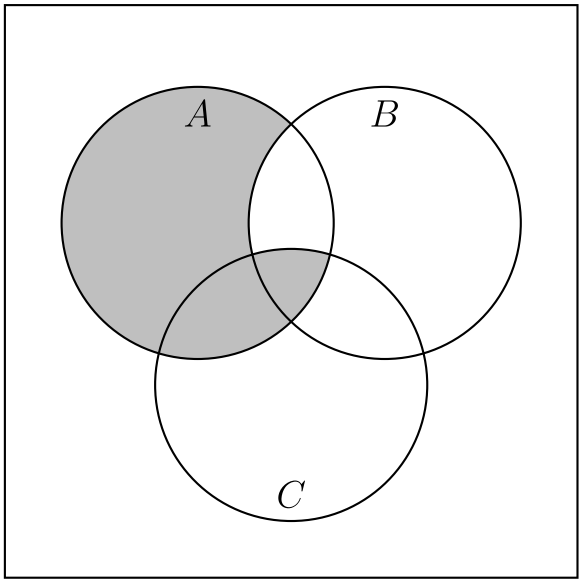
- element method:
  - prove that one set is a subset of another
  - prove set identities
  - prove that a set is equal to $\emptyset$ (by contradiction)
- known (famous) set identities:
  - simplify set expressions
  - give algebraic proofs of other set identities
- mathematical induction

Prove or disprove: For all sets A, B, and C, $(A - B) - C = A - (B - C)$.

Draw Venn diagrams for the LHS and the RHS.

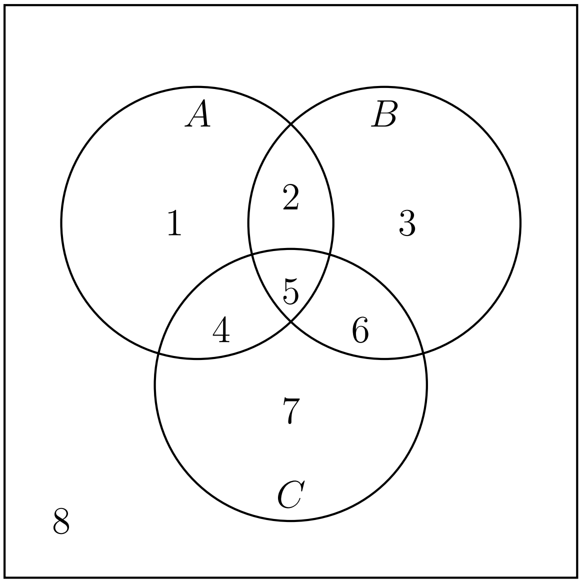


Shaded region
represents $(A - B) - C$



Shaded region
represents $A - (B - C)$

Disprove the statement by constructing a counterexample.



Let $A = \{1, 2, 4, 5\}$, $B = \{2, 3, 5, 6\}$, and $C = \{4, 5, 6, 7\}$.
Then
$A - B = \{1, 4\}$ and $B - C = \{2, 3\}$,
so
$(A - B) - C = \{1, 4\} - \{4, 5, 6, 7\} = \{1\}$
and
$A - (B - C) = \{1, 2, 4, 5\} - \{2, 3\} = \{1, 4, 5\}$.
Since $\{1\} \neq \{1, 4, 5\}$, it follows that $(A - B) - C \neq A - (B - C)$.

Prove or disprove: For all sets A, B, and C, $(A-B)\cup(C-B) = (A\cup C)-B$.

Proof (by element method): Let A, B, and C be arbitrary sets.

By the definition of set equality, we must prove:
$(A-B)\cup(C-B) \subseteq (A\cup C)-B$ and $(A\cup C)-B \subseteq (A-B)\cup(C-B)$.

Proof that $(A-B)\cup(C-B) \subseteq (A\cup C)-B$:

Let $x \in (A-B)\cup(C-B)$.

Then $x \in A-B$ or $x \in C-B$ by the definition of union.

If $x \in A-B$ then $x \in A$ and if $x \in C-B$ then $x \in C$, by the definition of set difference. So $x \in A$ or $x \in C$ and therefore $x \in A\cup C$ by the definition of union.

In both cases, $x \notin B$ by the definition of set difference.

Therefore, $x \in (A\cup C)-B$ by the definition of set difference.

Now, by the definition of subset, $(A-B)\cup(C-B) \subseteq (A\cup C)-B$.

Proof that $(A\cup C)-B \subseteq (A-B)\cup(C-B)$:

Let $x \in (A\cup C)-B$.

Then $x \in A\cup C$ and $x \notin B$ by the definition of set difference.

So $x \in A$ or $x \in C$ by the definition of union, and $x \notin B$.

If $x \in A$ then $x \in A-B$ by the definition of set difference.

If $x \in C$ then $x \in C-B$ by the definition of set difference.

Therefore, $x \in A-B$ or $x \in C-B$, and so by the definition of union, $x \in (A-B)\cup(C-B)$.

Now, by the definition of subset, $(A\cup C)-B \subseteq (A-B)\cup(C-B)$.

Finally, by the definition of set equality, $(A-B)\cup(C-B) = (A\cup C)-B$.
□

Prove or disprove: For all sets A, B, and C, if $C \subseteq B - A$ then $A \cap C = \emptyset$.

Proof (by element method):

Let A, B, and C be arbitrary sets such that $C \subseteq B - A$.

Suppose that $A \cap C \neq \emptyset$. Then there is an element x such that $x \in A \cap C$. By definition of intersection, $x \in A$ and $x \in C$.

Since $C \subseteq B - A$, then $x \in B - A$ and therefore $x \in B$ and $x \notin A$.

But now we have $x \in A$ and $x \notin A$, which is a contradiction.

Therefore $A \cap C = \emptyset$. $\square$

Set Identities [Epp, Theorem 6.2.2]
Let all sets referred to below be subsets of a universal set U.

1. *Commutative Laws:* For all sets A and B,
   (a) $A \cup B = B \cup A$ and (b) $A \cap B = B \cap A$.
2. *Associative Laws:* For all sets A, B, and C,
   (a) $(A \cup B) \cup C = A \cup (B \cup C)$ and (b) $(A \cap B) \cap C = A \cap (B \cap C)$.
3. *Distributive Laws:* For all sets A, B, and C,
   (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
4. *Identity Laws:* For all sets A,
   (a) $A \cup \emptyset = A$ and (b) $A \cap U = A$.
5. *Complement Laws:* For all sets A,
   (a) $A \cup A^c = U$ and (b) $A \cap A^c = \emptyset$.
6. *Double Complement Law:* For all sets A,
   $(A^c)^c = A$.
7. *Idempotent Law:* For all sets A,
   (a) $A \cup A = A$ and (b) $A \cap A = A$.
8. *Universal Bound Laws:* For all sets A,
   (a) $A \cup U = U$ and (b) $A \cap \emptyset = \emptyset$.
9. *De Morgan's Laws:* For all sets A and B,
   (a) $(A \cup B)^c = A^c \cap B^c$ and (b) $(A \cap B)^c = A^c \cup B^c$.
10. *Absorption Laws:* For all sets A and B,
    (a) $A \cup (A \cap B) = A$ and (b) $A \cap (A \cup B) = A$.
11. *Complements of U and $\emptyset$:*
    (a) $U^c = \emptyset$ and (b) $\emptyset^c = U$.
12. *Set Difference Law:* For all sets A and B,
    $A - B = A \cap B^c$.

Set Identities can be verified by the element method. For example:

Set Difference Law. For all sets A and B, $A - B = A \cap B^c$.

Proof (by element method): Let A and B be arbitrary sets.

Proof that $A - B \subseteq A \cap B^c$:

> Let $x \in A - B$.
>
> Then $x \in A$ and $x \notin B$ by the definition of set difference, and so $x \in A$ and $x \in B^c$ by the definition of complement. Therefore, $x \in A \cap B^c$ by the definition of intersection.

Proof that $A \cap B^c \subseteq A - B$:

> Let $x \in A \cap B^c$.
>
> Then $x \in A$ and $x \in B^c$ by the definition of intersection. So $x \in A$ and $x \notin B$ by definition of complement. Thus, $x \in A - B$ by the definition of set difference.

By the definition of set equality, we have shown that $A - B = A \cap B^c$. □

Give an algebraic proof (i.e. using the set identities of Theorem 6.2.2 of the textbook) of the following statement. (We proved this earlier using the element method.)

For all sets A, B, and C, $(A - B) \cup (C - B) = (A \cup C) - B$.

Proof:

$(A - B) \cup (C - B)$

$= (A \cap B^c) \cup (C \cap B^c)$ set difference law (twice)

$= (B^c \cap A) \cup (B^c \cap C)$ commutative law (twice)

$= B^c \cap (A \cup C)$ distributive law

$= (A \cup C) \cap B^c$ commutative law

$= (A \cup C) - B$ set difference law

Simplify the given expression for sets A, B, and C.

$(\ ((A \cup B) \cap C)^c\ \cup\ B^c\ )^c$

$=\ (((A \cup B) \cap C)^c)^c\ \cap\ (B^c)^c$	De Morgan's law
$=\ ((A \cup B) \cap C)\ \cap\ B$	Double complement law twice
$=\ (A \cup B)\ \cap\ (C\ \cap B)$	Associative law
$=\ (A \cup B)\ \cap\ (B\ \cap\ C)$	Commutative law
$=\ ((A \cup B)\ \cap\ B) \cap\ C$	Associative law
$=\ ((B \cup A)\ \cap\ B) \cap\ C$	Commutative law
$=\ (B\ \cap\ (B \cup A)) \cap\ C$	Commutative law
$=\ B\ \cap\ C$	Absorption law

CMPUT 272 (Stewart) University of Alberta **Lecture 13**

Reading: Epp Chapter 5.5

Correctness of Algorithms [Floyd, Dijkstra, Hoare, late 1960's]

A *specification* of an algorithm is given by two statements describing the input and output and the relationship between them:

a *pre-condition* and a *post-condition*.

Example: For an algorithm to sort a one-dimensional array of real numbers:

Pre-condition: Input is an array $A[1..n]$ of real numbers.

Post-condition: Output is an array $B[1..n]$ of real numbers with the same elements as $A[1..n]$ satisfying: $B[i] \leq B[j]$ for all $1 \leq i \leq j \leq n$.

An algorithm is *correct* if, whenever it is executed on input that satisfies the pre-condition, the post-condition is true.

To prove correctness of an algorithm:

- Can we run the algorithm on all possible inputs? NO!

  Suppose the input size is 40 bytes = 320 bits.

  Then the number of distinct inputs is 2^{320}. ← a 91-digit number

  number of protons in the known universe ← 79 digits

  number of microseconds since the big bang ← 24 digits

- Can we at least run it through a program that checks whether or not it halts on a given input? NO!

  The halting problem is undecidable: no such program can exist.

- Overall strategy:

  - Divide the algorithm into parts, each with a pre-condition and post-condition.
  - Prove the correctness of each part.
  - Show that the post-condition of each part implies the pre-condition of the next part, etc.

- It's easy to reason about parts that don't contain a loop.

- To reason about a loop:

  Define a *loop invariant*, $I(n)$: a predicate that describes how the values of the variables relate to each other after each iteration n (i.e., just before iteration $n+1$ if the loop executes again). Then

  I. prove that $I(0)$ is true before the first iteration of the loop,

  II. prove that for an arbitrary iteration $k \geq 0$ of the loop, if $I(k)$ is true after the kth iteration and the loop executes again, then $I(k+1)$ is true after the next iteration,

  III. show that the loop terminates, and

  IV. prove that when the loop terminates, the post-condition is true.

Recall the Quotient-Remainder Theorem:
Given any integer a and positive integer d, there exist unique integers q and r such that

$$a = dq + r \text{ and } 0 \leq r < d.$$

Example: Division Algorithm (described in Epp, p 218-219, Chapter 5.5)

The division algorithm is supposed to take a nonnegative integer a and positive integer d and compute nonnegative integers q and r such that

$$a = dq + r \text{ and } 0 \leq r < d.$$

Input: $a \in \mathbb{N}$, $d \in \mathbb{Z}^+$

Algorithm Body:

```
r := a, q := 0

Pre-condition: $a \in \mathbb{N}$, $d \in \mathbb{Z}^+$, $r = a$, and $q = 0$.
while ($r \geq d$)
    $r := r - d$
    $q := q + 1$
end while
Post-condition: $q, r \in \mathbb{Z}$ and $a = qd + r$ and $0 \leq r < d$.
```

Output: $q, r \in \mathbb{N}$

Loop guard:

$$G\colon\ r \geq d$$

Loop invariant:

$$I(n)\colon\ r = a - nd \text{ and } r \geq 0 \text{ and } q = n.$$

Theorem. The Division Algorithm is correct.

Proof:
I. Basis step: [We must prove that $I(0)$ is true before the first iteration.] By the pre-condition: $a \geq 0$, $r = a$, and $q = 0$. Therefore

$$r = a - 0 \cdot d, \quad r \geq 0, \quad \text{and} \quad q = 0,$$

that is, $I(0)$ is true.

II. Inductive step: [We must prove: For arbitrary $k \in \mathbb{N}$, if $I(k)$ and G are true after the kth iteration, then $I(k+1)$ is true after the $(k+1)$st iteration.] Let $k \in \mathbb{N}$ such that $I(k)$ and G are true after the kth iteration. Then

$$r_{old} \geq d \quad \text{by } G$$

$$\text{and} \qquad r_{old} = a - kd \quad \text{and} \quad r_{old} \geq 0 \quad \text{and} \quad q_{old} = k \qquad \text{by } I(k).$$

After the $(k+1)$st iteration:

$$\begin{aligned} r_{new} &= r_{old} - d \\ &= (a - kd) - d \quad && \text{by } I(k) \\ &= a - (k+1)d \\ r_{new} &= r_{old} - d \geq 0 && \text{by } G \\ q_{new} &= q_{old} + 1 \\ &= k + 1 && \text{by } I(k) \end{aligned}$$

Therefore $I(k+1)$ is true after the $(k+1)$st iteration.

III. The loop terminates: If $r \geq d$, then the loop executes and the value of r is decreased. But the value of r never goes below zero (by the loop invariant). Therefore, eventually $r < d$ and the loop terminates.

IV. Correctness of the Post-condition: When the loop terminates,

$$r = a - qd \quad \text{and} \quad r \geq 0 \quad \text{by the loop invariant}$$

and $r < d$ by the loop guard. Combining these facts gives the post-condition:

$$a = qd + r \quad \text{and} \quad 0 \leq r < d. \qquad \square$$

Example: Euclid's Algorithm (described in Epp, p 220-224, Chapter 5.5)

Recall the Definition of divides. For integers n and $d \neq 0$,

$$d \mid n \quad (\text{“}d\text{ divides }n\text{”}) \quad \Leftrightarrow \quad \exists k \in \mathbb{Z} \text{ such that } n = dk.$$

$$\Leftrightarrow \quad \frac{n}{d} \in \mathbb{Z}.$$

Definition. Let a and b be integers that are not both zero. The *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is the largest integer that divides both a and b.

Example:

$\gcd(49, 70) = 7$

For all integers a and b that are not both zero:

$\gcd(a, b) = \gcd(b, a)$

For all integers $a \neq 0$:

$\gcd(a, a) = a$

$\gcd(a, 0) = a$

Recall: Theorem (Properties of Integer Division). For all $a, b, c, d \in \mathbb{Z}$,

1. $1|a$ and, if $a \neq 0$ then $a|0$ and $a|a$;
2. if $a|b$ then $a|bc$;
3. if $a|b$ and $b|c$ then $a|c$; (Transitivity of Division)
4. if $a = b + c$ and d divides two of a,b, and c, then d divides all of a,b, and c;
5. if a and b are positive, and $a|b$, then $a \leq b$;
6. if $a|b$ then $(-a)|b$;
7. if $a|b$ and $b|a$ then $a = \pm b$.

Lemma. For all integers a and b with $a > b \geq 0$,

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

(Recall: $a \bmod b = r$ where $a = bq + r$ and $0 \leq r < b$, for some $q \in \mathbb{Z}$.)

Proof: Let $a, b \in \mathbb{Z}$ with $a > b \geq 0$. By the Q-R Theorem, there exist integers q and r such that

$$a = bq + r \quad \text{and} \quad 0 \leq r < b.$$

By the definition of mod,

$$a \bmod b = r$$

or equivalently

$$a \bmod b = a - bq.$$

By properties of integer division:

- every divisor of b is also a divisor of $-bq$ (property 2);
- every common divisor of a and b is also a divisor of $a \bmod b$ (2 and 4);
- every common divisor of b and $a \bmod b$ is also a divisor of a (2 and 4).

So $\{x \in \mathbb{Z} \mid x \text{ divides both } a \text{ and } b\} = \{x \in \mathbb{Z} \mid x \text{ divides both } b \text{ and } a \bmod b\}$ and the largest element of that set is $\gcd(a, b) = \gcd(b, a \bmod b)$. □

Euclid's Algorithm

Given two integers A and B with $A > B \geq 0$, compute $\gcd(A, B)$.

Input: $A, B \in \mathbb{Z}$ with $A > B \geq 0$

Algorithm Body:

```
    $a := A$, $b := B$, $r := B$

    Pre-condition: $A$ and $B$ are integers satisfying $A > B \geq 0$,
                   $a = A$, $b = B$, and $r = B$.
    while ($b \neq 0$)
        $r := a \bmod b$
        $a := b$
        $b := r$
    end while
    Post-condition: $a = \gcd(A, B)$.
```

Output: a

Loop guard:

$$G\colon\ b \neq 0$$

Loop invariant:

$$I(n)\colon\ \gcd(a, b) = \gcd(A, B) \text{ and } 0 \leq b < a.$$

Theorem. Euclid's Algorithm is correct.

Proof:
I. Basis step: [We must prove that $I(0)$ is true before the first iteration.] By the pre-condition: $a = A$, $b = B$, $r = B$, and $0 \leq B < A$. Therefore

$$\gcd(a, b) = \gcd(A, B) \quad \text{and} \quad 0 \leq b < a,$$

that is, $I(0)$ is true.

II. Inductive step: [We must prove: For arbitrary $k \in \mathbb{N}$, if $I(k)$ and G are true after the kth iteration, then $I(k+1)$ is true after the $(k+1)$st iteration.] Let $k \in \mathbb{N}$ such that $I(k)$ and G are true after the kth iteration. Then

$$b_{old} \neq 0 \qquad \text{by } G$$

$$\text{and} \qquad \gcd(a_{old}, b_{old}) = \gcd(A, B) \quad \text{and} \quad 0 \leq b_{old} < a_{old} \qquad \text{by } I(k).$$

After the $(k + 1)$st iteration:

$$\begin{aligned} r_{new} &= a_{old} \bmod b_{old} \\ a_{new} &= b_{old} \\ b_{new} &= r_{new} = a_{old} \bmod b_{old} \end{aligned}$$

Therefore

$$\begin{aligned} \gcd(a_{new}, b_{new}) &= \gcd(b_{old}, a_{old} \bmod b_{old}) \\ &= \gcd(a_{old}, b_{old}) && \text{by Lemma, since } a_{old} > b_{old} \geq 0 \\ &= \gcd(A, B) && \text{by } I(k) \end{aligned}$$

and $0 \leq a_{old} \bmod b_{old} < b_{old}$ by the definition of mod, that is, $0 \leq b_{new} < a_{new}$. Therefore $I(k + 1)$ is true after the $(k + 1)$st iteration.

III. The loop terminates: If $b \neq 0$, then the loop executes and the value of b is decreased. But the value of b never goes below zero (by the loop invariant). Therefore, eventually $b = 0$ and the loop terminates.

IV. Correctness of the Post-condition: When the loop terminates, $\gcd(a, b) = \gcd(A, B)$ by the loop invariant and $b = 0$ by the loop guard. Therefore

$$\gcd(A, B) = \gcd(a, b) = \gcd(a, 0) = a$$

which is the post-condition. □

CMPUT 272 (Stewart) University of Alberta **Lecture 12**

Reading: Epp Chapter 5.4, Theorems 4.3.4 and 4.3.5, Chapter 4.4, p 210

More Number Theory

Definition. For all integers $n > 1$,

n is *prime*
$\Leftrightarrow \forall\ r, s \in \mathbb{Z}^+$, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$;

n is *composite*
$\Leftrightarrow \exists\ r, s \in \mathbb{Z}^+$ such that $n = rs$ and $1 < r, s < n$.

Theorem. Every integer greater than 1 is prime or composite but not both.

Proof: Let n be an integer that is greater than 1. If the only positive integers r and s such that $n = rs$ are $r = 1$, $s = n$ and $r = n$, $s = 1$, then n is prime by the definition of prime. Otherwise, there are positive integers r and s such that $n = rs$ and $1 < r, s < n$. Therefore n is composite. □

Recall:

Theorem (Properties of Integer Division). For all $a, b, c, d \in \mathbb{Z}$,

1. $1|a$ and, if $a \neq 0$ then $a|0$ and $a|a$;
2. if $a|b$ then $a|bc$;
3. if $a|b$ and $b|c$ then $a|c$; (Transitivity of Division)
4. if $a = b + c$ and d divides two of a,b, and c, then d divides all of a,b, and c;
5. if a and b are positive, and $a|b$, then $a \leq b$;
6. if $a|b$ then $(-a)|b$;
7. if $a|b$ and $b|a$ then $a = \pm b$.

Theorem. Every integer greater than 1 is divisible by a prime number.

Proof (by strong mathematical induction):

Basis step: The integer 2 is a prime number and it is divisible by itself. Therefore 2 is divisible by a prime number.

Inductive step: Let k be any integer with $k \geq 2$ and suppose that every integer from 2 through k is divisible by a prime number. We must show that $k + 1$ is divisible by a prime number.

Case 1 ($k + 1$ is prime): In this case, $k + 1$ is divisible by a prime number, namely, itself.

Case 2 ($k + 1$ is not prime): In this case, $k + 1$ is composite and therefore $k + 1 = ab$ for positive integers a and b with $1 < a, b < k + 1$. So $2 \leq a \leq k$ and therefore by the inductive hypothesis, a is divisible by a prime number, p. Since $p|a$ and $a|(k+1)$, we have that $p|(k+1)$ by the transitivity of division. Therefore, $k + 1$ is divisible by a prime number. □

Theorem (Unique Factorization of Integers).

For any integer $n > 1$,

there exist:

- a positive integer k,
- distinct prime numbers $p_1, p_2, \ldots, p_k$, and
- positive integers $e_1, e_2, \ldots, e_k$

such that

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Any other expression for n as a product of prime numbers is identical to this, except possibly for the order in which the factors are written.

Proof: The proof is outlined in Exercises 5.4.13, 5.4.20, and 8.4.41 of the textbook. The proof of the uniqueness part uses this lemma:

$$\text{For } a, b \in \mathbb{N}, p \in \mathbb{P}, \ \text{ if } p|ab \text{ then } p|a \text{ or } p|b.$$

Definition: For any integer $n > 1$, the *standard factored form* of n is the expression

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \quad \text{where}$$

$$k, e_1, e_2, \ldots, e_k \text{ are positive integers,}$$

$$p_1, p_2, \ldots, p_k \text{ are prime numbers, and}$$

$$p_1 < \cdots < p_k.$$

Notes: Suppose that in standard factored form

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \quad \text{where}$$

$$k, e_1, e_2, \ldots, e_k \text{ are positive integers,}$$

$$p_1, p_2, \ldots, p_k \text{ are prime numbers, and}$$

$$p_1 < \cdots < p_k.$$

Then

- n is a perfect square if and only if $e_1, e_2, \ldots, e_k$ are all even;
- a positive integer m is a factor of n if and only if

$$m = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \quad \text{where}$$

$f_1, f_2, \ldots, f_k$ are integers such that $0 \leq f_1 \leq e_1, 0 \leq f_2 \leq e_2, \ldots, 0 \leq f_k \leq e_k$.

Using unique factorization to solve problems:

1. Find the least positive integer n such that $1176n$ is a perfect square.

$$1176 \ = 2^3 3^1 7^2$$

We need to add one to the exponents of 2 and 3 to make all exponents even.
So, when $n = 2 \times 3 = 6$,

$$1176n \ = 2^4 3^2 7^2 \text{ is a perfect square.}$$

2. How many zeros are at the end of $45^8 \cdot 88^5$, or equivalently,
what is the largest k such that 10^k divides $45^8 \cdot 88^5$.

$$10 = 2^1 5^1$$
$$45^8 \cdot 88^5 = (3^2 5^1)^8 \cdot (2^3 11^1)^5 = 3^{16} 5^8 2^{15} 11^5$$

So $5^8 2^8$ is a factor of $45^8 \cdot 88^5$ but $5^9 2^9$ is not.
There are 8 zeros are at the end of $45^8 \cdot 88^5$.

Recall:

Theorem (Properties of Integer Division). For all $a, b, c, d \in \mathbb{Z}$,

1. $1|a$ and, if $a \neq 0$ then $a|0$ and $a|a$;
2. if $a|b$ then $a|bc$;
3. if $a|b$ and $b|c$ then $a|c$; (Transitivity of Division)
4. if $a = b + c$ and d divides two of a,b, and c, then d divides all of a,b, and c;
5. if a and b are positive, and $a|b$, then $a \leq b$;
6. if $a|b$ then $(-a)|b$;
7. if $a|b$ and $b|a$ then $a = \pm b$.

Theorem. There are infinitely many prime numbers.

Proof (by contradiction): Suppose not. Let $\{p_1, p_2, \ldots, p_k\}$ be the finite set of prime numbers. Let

$$N = p_1 p_2 \cdots p_k + 1.$$

Then $N > 1$ and every integer greater than 1 is divisible by a prime number by an earlier theorem, so N is divisible by some prime number p. Since p is prime, it is one of $p_1, p_2, \ldots, p_k$ and therefore $p \mid p_1 p_2 \cdots p_k$. Now $p \mid N$ and $p \mid p_1 p_2 \cdots p_k$ so, by property 4 of integer division, $p \mid 1$. But then $p = 1$ by property 5 of integer division, which contradicts the fact that p is a prime number. $\square$

Well-Ordering Principle for Integers

Let S be a nonempty set of integers, all of which are greater than some fixed integer. Then S has a least element.

Earlier, we proved the following theorem by strong mathematical induction. Now we look at a proof by the well-ordering principle.

Theorem. Every integer greater than 1 is divisible by a prime number.

Proof (by contradiction and the well-ordering principle):
Suppose not. Then some integer greater than 1 is not divisible by a prime number. Let $S = \{n \in \mathbb{Z} \mid n > 1 \text{ and } n \text{ is not divisible by a prime number}\}$. Now $S \neq \emptyset$ (since we are supposing that the theorem is not true) and every element of S is greater than 1. Therefore the well-ordering principle implies that S has a least element ℓ.

Case 1 (ℓ is prime): In this case, ℓ is divisible by a prime number (itself) but this contradicts that $\ell \in S$.

Case 2 (ℓ is not prime): In this case, ℓ is composite and therefore $\ell = ab$ for some positive integers a and b with $1 < a, b < \ell$. Since $1 < a < \ell$ and ℓ is the smallest element of S, a is not in S and therefore a is divisible by a prime number, p. Since $p|a$ and $a|\ell$, we have that $p|\ell$ by the transitivity of division. But this contradicts that ℓ is in S. $\square$

Theorem (Quotient-Remainder).
Given any integer n and positive integer d,
there exist unique integers q and r such that

$$n = dq + r \text{ and } 0 \leq r < d.$$

Examples:

n	d	q	r
48	5	9	3
-48	5	-10	2
3	10	0	3
-3	10	-1	7

Definition. For $n, q, r \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, where $0 \leq r < d$,

$$n \ div \ d = q \text{ and } n \ mod \ d = r \ \Leftrightarrow \ n = dq + r.$$

Examples:

$$48 \ div \ 5 = 9$$
$$48 \ mod \ 5 = 3$$

Theorem (Quotient-Remainder).
Given any integer n and positive integer d,
there exist unique integers q and r such that

$$n = dq + r \text{ and } 0 \leq r < d.$$

First prove it **without uniqueness** and **without the second condition**:

Given any integer n and positive integer d,
there exist ~~unique~~ integers q and r such that

$n = dq + r$ ~~and $0 \leq r < d$.~~

Easy proof: Let $q = 0$ and $r = n$. □

In fact: Given any integer n and positive integer d,
there exist an infinite number of pairs of integers q and r such that

$$n = dq + r \qquad \text{(equivalently, } r = n - dq\text{)}.$$

Examples:

$n = 33, d = 5$:

q	⋯	8	7	6	5	4	3	2	1	0	-1	⋯
r	⋯	-7	-2	3	8	13	18	23	28	33	38	⋯

$n = -33, d = 5$:

q	⋯	1	0	-1	-2	-3	-4	-5	-6	-7	-8	⋯
r	⋯	-38	-33	-28	-23	-18	-13	-8	-3	2	7	⋯

In each case, only one pair satisfies $0 \leq r < d$.

Idea for proof of the Q-R Theorem:

- Consider such a pair, q and r, with smallest nonnegative r value.
- Show that $0 \leq r < d$ and that q and r are unique.

Theorem (Quotient-Remainder).
Given any integer n and positive integer d,
there exist unique integers q and r such that

$$n = dq + r \text{ and } 0 \leq r < d.$$

Proof (by well-ordering principle):

Let $S = \{n - dk \mid k \in \mathbb{Z} \text{ and } n - dk \geq 0\}$. To show that $S \neq \emptyset$, we note that

- if $n \geq 0$ then $n - d \cdot 0 \in S$, and
- if $n < 0$ then $n - d \cdot n \in S$ since $d \in \mathbb{Z}^+$.

Now S is a nonempty set of integers, each of which is greater than or equal to 0. Therefore, by the well-ordering principle, S contains a least element, r. Since $r \in S$, $r = n - dq$ for some integer q, and $r \geq 0$.

[We need to show that $r < d$.] Suppose that $r \geq d$. Then

$$r - d \geq 0$$

and

$$r - d = n - dq - d = n - d(q + 1).$$

So $r - d \in S$, which contradicts that r is the smallest element of S. This contradiction proves that $r < d$.

So far, we have proved: there exist integers q and r such that

$$n = dq + r \text{ and } 0 \leq r < d.$$

We now have to show that q and r are unique.

So far, we have proved: there exist integers q and r such that

$$n = dq + r \text{ and } 0 \leq r < d.$$

We now have to show that q and r are unique.

Suppose not.

Then there exist integers q_1, r_1, q_2, r_2 such that

$$n = dq_1 + r_1, \quad 0 \leq r_1 < d, \quad n = dq_2 + r_2, \quad 0 \leq r_2 < d, \quad \text{and} \quad r_1 < r_2.$$

Now

$$dq_1 + r_1 = dq_2 + r_2.$$

Therefore

$$dq_1 - dq_2 = r_2 - r_1$$

and

$$d(q_1 - q_2) = r_2 - r_1.$$

Now we derive a contradiction by showing that this equation cannot hold. First, consider the left-hand side. Since $q_1 - q_2$ is an integer and d is a positive integer,

$$d(q_1 - q_2) \leq 0 \qquad \text{or} \qquad d(q_1 - q_2) \geq d.$$

Next, consider the right-hand side. Since $0 \leq r_1 < r_2 < d$,

$$0 < r_2 - r_1 < d.$$

Therefore

$$d(q_1 - q_2) \neq r_2 - r_1,$$

a contradiction. Since the supposition that q and r are not unique leads to a contradiction, we conclude that q and r are unique. □

Theorem. Every integer is even or odd but not both.

Proof: Let n be an integer. By the Q-R Theorem, there exist unique integers q and r such that

$$n = 2q + r \quad \text{and} \quad 0 \leq r < 2.$$

Thus, $r = 0$ or $r = 1$.
If $r = 0$, then $n = 2q$ and therefore by the definition of even, n is even.
If $r = 1$, then $n = 2q + 1$ and therefore by the definition of odd, n is odd.
Therefore, n is even or n is odd. Because r is unique, n cannot be both even and odd. □

Theorem. For all $n \in \mathbb{Z}^+$, $n^2 - 1$ is a multiple of 3 if and only if n is not a multiple of 3.

Proof: Let $n \in \mathbb{Z}^+$.

Suppose that n is a multiple of 3, that is,

$$n = 3a \quad \text{for some } a \in \mathbb{Z}.$$

Then

$$n^2 - 1 = (3a)^2 - 1 = 9a^2 - 1.$$

If $3|(n^2 - 1)$ then, since $3|9a^2$, it must be that $3|1$, a contradiction. Therefore if n is multiple of 3 then $n^2 - 1$ is not a multiple of 3.

Suppose that n is not a multiple of 3. Then by the Q-R Theorem, there exist unique integers q and r such that

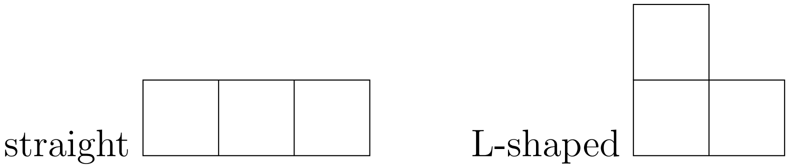
$$n = 3q + r \text{ and } 0 < r < 3.$$

Thus, $r = 1$ or $r = 2$.
If $r = 1$, then $n^2 - 1 = (3q+1)^2 - 1 = 9q^2 + 6q + 1 - 1 = 9q^2 + 6q = 3(3q^2 + 2q)$.
If $r = 2$, then $n^2 - 1 = (3q + 2)^2 - 1 = 9q^2 + 12q + 4 - 1 = 9q^2 + 12q + 3 = 3(3q^2 + 4q + 1)$.
In both cases, $n^2 - 1$ is a multiple of 3. Therefore if n is not a multiple of 3 then $n^2 - 1$ is a multiple of 3. □

Reading: Epp Chapter 5.1-5.3

Tromino Puzzle [Golomb, 1954]

A *tromino* is a generalized domino made up of three attached squares. There are two types:



Question. Which rectangles can be covered by both types of trominoes? by just one type?

Such coverings by various shapes, called *tilings* or *tessellations*, have applications in:
- manufacturing
- art and design
- biology, e.g., honeycombs
- algorithms: approximation, dynamic programming, divide-and-conquer

Theorem. For any rectangle, the following are equivalent:

1. it can be covered by trominoes
2. its area is a multiple of 3
3. it can be covered by straight trominoes

Theorem. [Chu and Johnsonbaugh, 1985-86] A rectangle can be covered by L-shaped trominoes if its area is a multiple of 3, except when one dimension is 3 and the other is odd.

$\underbrace{\textit{Deficient checkerboards}}$ *and L-shaped trominoes*

↖ a square of any size from which a unit square has been removed

Question. Which deficient checkerboards can be covered with L-shaped trominoes?

Theorem. [Golomb, 1954] For any $n \in \mathbb{Z}^+$, if any square is removed from a $2^n \times 2^n$ checkerboard, then the remaining squares can be covered by L-shaped trominoes.

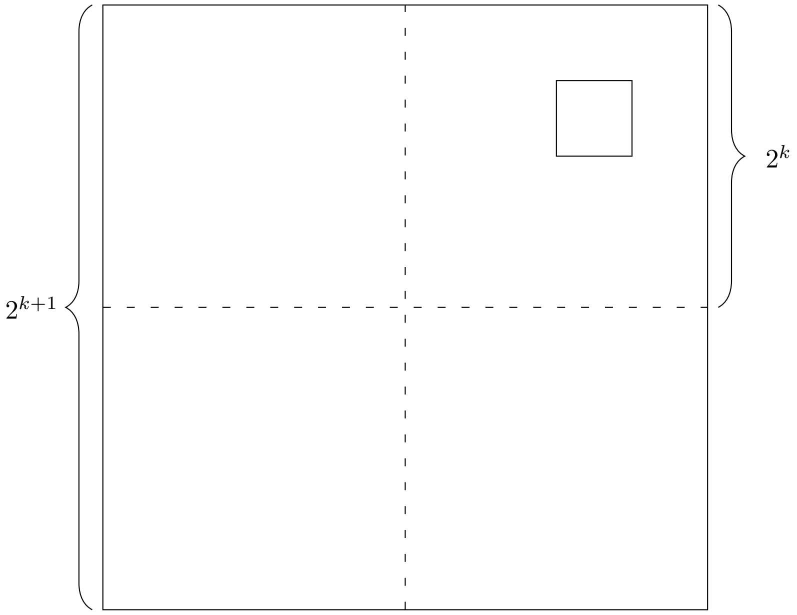
Proof (by mathematical induction):

Let $P(n)$ be the statement:

> If any square is removed from a $2^n \times 2^n$ checkerboard, then the remaining squares can be covered by L-shaped trominoes.

Basis step: Show that $P(1)$ is true.
A $2^1 \times 2^1$ checkerboard has four squares; removing any one square leaves a region that can be covered by one L-shaped tromino.

Inductive step: Show that $\forall k \in \mathbb{Z}^+, (P(k) \to P(k+1))$.
Let $k \in \mathbb{Z}^+$ such that after removing any one square from a $2^k \times 2^k$ checkerboard, the remaining squares can be covered by L-shaped trominoes. Consider a $2^{k+1} \times 2^{k+1}$ checkerboard with an arbitrary square removed. Divide it into quadrants:



The quadrant from which a square has been removed can be covered by L-shaped trominoes by the inductive hypothesis. The centre squares of the other three quadrants can be covered by one tromino. The remaining squares of those three quadrants can also be covered by trominoes, by the inductive hypothesis. Therefore, after an arbitrary square is removed from a $2^{k+1} \times 2^{k+1}$ checkerboard, the remaining squares can be covered by L-shaped trominoes. So $P(k+1)$ is true. □

Theorem. [Chu and Johnsonbaugh, 1986]
If $n \neq 5$ then a deficient $n \times n$ board can be tiled with L-shaped trominoes if and only if $n^2 - 1$ is a multiple of 3.

Proving a property of a sequence by mathematical induction

Define a sequence $a_1, a_2, a_3, \ldots$ as follows: [Epp p 263]

$$\begin{aligned} a_1 &= 2 \\ a_k &= 5a_{k-1} \quad \text{for all integers } k \geq 2. \end{aligned}$$

Theorem. For all $n \in \mathbb{Z}^+, a_n = 2 \cdot 5^{n-1}$.

Proof (by mathematical induction):

Let $P(n)$ be: $a_n = 2 \cdot 5^{n-1}$.

Basis step: $a_1 = 2$ and $2 \cdot 5^{1-1} = 2 \cdot 5^0 = 2$. Therefore $a_1 = 2 \cdot 5^{1-1}$ and $P(1)$ is true.

Inductive step: Let k be an arbitrary positive integer such that $P(k)$ is true, that is

$$a_k = 2 \cdot 5^{k-1}. \qquad \leftarrow \text{inductive hypothesis}$$

Now

$$\begin{aligned} a_{k+1} &= 5a_k && \text{by the definition of the sequence } a_1, a_2, \ldots \text{ since } k+1 \geq 2 \\ &= 5 \cdot 2 \cdot 5^{k-1} && \text{by the inductive hypothesis} \\ &= 2 \cdot 5^k \end{aligned}$$

Thus $P(k+1)$ holds. $\square$

Another recursively defined sequence:

$$\begin{aligned} e_0 &= 12 \\ e_1 &= 29 \\ e_k &= 5\,e_{k-1} - 6\,e_{k-2} \quad \text{for all integers } k \geq 2 \end{aligned}$$

Try to prove: For all $n \in \mathbb{N}$, $e_n = 5 \cdot 3^n + 7 \cdot 2^n$.

Proof by induction: Let $P(n)$ be: $e_n = 5 \cdot 3^n + 7 \cdot 2^n$.

Basis step:

$e_0 = 12$ and $5 \cdot 3^0 + 7 \cdot 2^0 = 5 + 7 = 12$; therefore $P(0)$ is true.

Inductive step: Let $k \in \mathbb{N}$ and suppose that $P(k)$ is true, that is,

$$e_k = 5 \cdot 3^k + 7 \cdot 2^k. \qquad \leftarrow \text{inductive hypothesis}$$

Now

$$\begin{aligned} e_{k+1} &= 5\,e_k && -6\,e_{k-1} && \text{if } k \geq 1 \\ &= 5(5 \cdot 3^k + 7 \cdot 2^k) && -6\,(???) && \text{by the inductive hypothesis} \end{aligned}$$

Problem: The inductive hypothesis doesn't tell us anything about e_{k-1}.

Principle of Strong Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

1. $P(a), P(a+1), \ldots, P(b)$ are all true.
2. For all integers $k \geq b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true.

Then the statement for all integers $n \geq a$, $P(n)$ is true.

Strong Mathematical Induction as a formal rule of inference

$$\begin{array}{l} \quad P(a) \\ \quad P(a+1) \\ \quad\ \ \vdots \\ \quad P(b) \\ \ \forall k \geq b, (\ (\forall i, a \leq i \leq k, P(i)) \rightarrow P(k{+}1)\ ) \\ \therefore \forall n \geq a, P(n) \end{array}$$

Compare with Mathematical Induction

$$\begin{array}{l} \quad P(a) \\ \quad \forall k \geq a, (\ P(k) \rightarrow P(k{+}1)\ ) \\ \therefore \forall n \geq a, P(n) \end{array}$$

Method of Proof by Strong Mathematical Induction

Define a suitable predicate $P(n)$.

To prove

$$\text{For all integers } n \geq a, P(n):$$

Basis step: Show that all of the following are true: $P(a), P(a+1), \ldots, P(b)$.

Inductive step: Show that for arbitrary integer $k \geq b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true.

Let k be an integer $\geq b$.
Suppose that $P(i)$ is true for all integers i from a through k.
Show that $P(k+1)$ is true.

We can complete the proof from before using strong mathematical induction.

The sequence $e_0, e_1, \ldots$ is defined as:

$$\begin{aligned} e_0 &= 12 \\ e_1 &= 29 \\ e_k &= 5\,e_{k-1} - 6\,e_{k-2} \quad \text{for all integers } k \geq 2 \end{aligned}$$

Theorem. For all $n \in \mathbb{N}$, $e_n = 5 \cdot 3^n + 7 \cdot 2^n$.

Proof by (strong) mathematical induction: Let $P(n)$ be: $e_n = 5 \cdot 3^n + 7 \cdot 2^n$.

Basis step:
$e_0 = 12$ and $5 \cdot 3^0 + 7 \cdot 2^0 = 5 + 7 = 12$; therefore $P(0)$ is true.
$e_1 = 29$ and $5 \cdot 3^1 + 7 \cdot 2^1 = 15 + 14 = 29$; therefore $P(1)$ is true.

Inductive step:

~~Let $k \in \mathbb{N}$ and suppose that $P(k)$ is true, that is,~~

~~$e_k = 5 \cdot 3^k + 7 \cdot 2^k$. ← inductive hypothesis~~

Let $k \in \mathbb{N}$, $k \geq 1$, and suppose that $P(i)$ is true for all i from 0 through k, that is,

$$e_i = 5 \cdot 3^i + 7 \cdot 2^i \text{ for all } i \text{ with } 0 \leq i \leq k. \qquad \leftarrow \text{inductive hypothesis}$$

Now

$$\begin{aligned} e_{k+1} &= 5\,e_k \qquad\qquad - 6\,e_{k-1} && \text{by definition of the sequence, since } k \geq 1 \\ &= 5(5 \cdot 3^k + 7 \cdot 2^k) - 6\,(5 \cdot 3^{k-1} + 7 \cdot 2^{k-1}) && \text{by the inductive hypothesis} \\ &= 25 \cdot 3^k + 35 \cdot 2^k \ - 30 \cdot 3^{k-1} - 42 \cdot 2^{k-1} \\ &= 25 \cdot 3^k + 35 \cdot 2^k \ - 10 \cdot 3 \cdot 3^{k-1} - 21 \cdot 2 \cdot 2^{k-1} \\ &= 25 \cdot 3^k + 35 \cdot 2^k \ - 10 \cdot 3^k - 21 \cdot 2^k \\ &= 15 \cdot 3^k + 14 \cdot 2^k \\ &= 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1} \end{aligned}$$

□

CMPUT 272 (Stewart) University of Alberta **Lecture 10**

Reading: Epp Chapter 5.1-5.3

Mathematical Induction

- an additional rule of inference
- for proving facts about all integers greater than or equal to a certain value

When do we use mathematical induction? Consider the following theorem.

Theorem. For all $n \in \mathbb{Z}^+$, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

How to prove it?

It's easy to check for the first few numbers:
$n = 1$: $1 = \frac{1(1+1)}{2}$
$n = 2$: $1 + 2 = \frac{2(2+1)}{2}$
$n = 3$: $1 + 2 + 3 = \frac{3(3+1)}{2}$
$\vdots$
But we can't check all positive integers!

To prove the theorem, we prove:

(1) the equality is true for $n = 1$, and

(2) **IF** the equality holds for an arbitrary positive integer
THEN it holds for the next integer, which means:

- if it is true for $n = 1$ then it is true for $n = 2$
- if it is true for $n = 2$ then it is true for $n = 3$

$\vdots$

Together, these facts show that the equality holds *for all* $n \geq 1$.

(1) **Prove** that the equality holds for $n = 1$:
When $n = 1$, the LHS of the equality is 1 and the RHS is $\frac{1(1+1)}{2} = 1$. Since the LHS and RHS are both equal to 1, the equality holds for $n = 1$.

(2) **Prove** that
IF the equality holds for an arbitrary positive integer
THEN it holds for the next integer.

That is, **prove**:

$$\textbf{for all } k \in \mathbb{Z}^+\text{: } \textbf{IF } 1 + 2 + \cdots + k = \tfrac{k(k+1)}{2}$$
$$\textbf{THEN } 1 + 2 + \cdots + (k+1) = \tfrac{(k+1)(k+2)}{2}.$$

Let $k \in \mathbb{Z}^+$. **Suppose** the equality holds for $n = k$:

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

We want to prove that the equality holds for $n = k + 1$, that is:

$$1 + 2 + \cdots + (k+1) = \frac{(k+1)(k+2)}{2}.$$

Strategy: Write the LHS of what we want to prove in terms of the LHS of the supposition:

$$\begin{aligned}
1 + 2 + \cdots + (k+1) &= 1 + 2 + \cdots + k \quad + (k+1) \\
&= \frac{k(k+1)}{2} \quad + (k+1) && \text{use the equality for } n = k \\
&= (k+1)\left(\frac{k}{2} + 1\right) \\
&= \frac{(k+1)(k+2)}{2} && \text{the equality holds for } n = k+1
\end{aligned}$$

(1) and (2) combined show that the equality holds for all positive integers.

Principle of Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the following two statements are true:

1. $P(a)$ is true.
2. For all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

Then the statement for all integers $n \geq a$, $P(n)$ is true.

Mathematical Induction as a formal rule of inference

$$
\begin{array}{ll}
 & P(a) \\
 & \forall k \geq a, (P(k) \to P(k+1)) \\
\therefore & \forall n \geq a, P(n)
\end{array}
$$

Method of Proof by Mathematical Induction

Define a suitable predicate $P(n)$.

To prove

$$\text{For all integers } n \geq a, P(n):$$

Basis step: Show that $P(a)$ is true.

Inductive step:
Show that for all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

Let k be an arbitrary integer $\geq a$.

Suppose that $P(k)$ is true. $P(k)$ is the *inductive hypothesis*

Show that $P(k+1)$ is true. $P(k+1)$ is the *inductive consequent*

Sequences

A *sequence* is an ordered list of terms indexed by consecutive integers, for example:

$$a_m, a_{m+1}, a_{m+2}, \ldots, a_n$$

or

$$a_m, a_{m+1}, a_{m+2}, \ldots$$

The terms of a sequence may be defined by a general formula.
For example, the first few terms of the sequence $a_1, a_2, \ldots$ defined by

$$a_i = \frac{i}{i+1} \qquad \text{for all integers } i \geq 1$$

are

$$\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5} \cdots$$

Summation and Product Notation

For integers m and n:

$$\sum_{i=m}^{n} a_i = \begin{cases} a_m + a_{m+1} + \cdots + a_n & \text{if } m \leq n \\ 0 & \text{if } m > n \end{cases}$$

$$\prod_{i=m}^{n} a_i = \begin{cases} a_m \times a_{m+1} \times \ \cdots \ \times a_n & \text{if } m \leq n \\ 1 & \text{if } m > n \end{cases}$$

Examples:

$$\sum_{i=1}^{4} i^2 = 1 + 4 + 9 + 16 = 30$$

$$\prod_{k=1}^{7} k = 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 = 5040$$

$$\sum_{i=1}^{n} i = \begin{cases} 1 + 2 + \cdots + n & \text{if } n \geq 1 \\ 0 & \text{if } n \leq 0 \end{cases}$$

See Epp Chapter 5.1 for more about sequences, and Σ and Π notation.

Theorem. $\forall n \in \mathbb{Z}^+,\ \sum_{i=1}^{n} i \ = \ \frac{n(n+1)}{2}.$

Proof (by mathematical induction):
Let $P(n)$ be the predicate:

$$\sum_{i=1}^{n} i \ = \ \frac{n(n+1)}{2}.$$

Basis step: [We need to prove $P(1)$, that is, $1 = \frac{1(1+1)}{2}$.]
The right-hand side of the equation is

$$\frac{1(1+1)}{2} = \frac{2}{2} = 1$$

which is equal to the left-hand side. Therefore $P(1)$ is true.

Inductive step: [We need to prove $\forall k \in \mathbb{Z}^+, (P(k) \to P(k+1))$.]
Let k be an arbitrary positive integer such that $P(k)$ is true, that is

$$\sum_{i=1}^{k} i \ = \ \frac{k(k+1)}{2}. \qquad \leftarrow \text{ inductive hypothesis}$$

[Now we must show that $P(k+1)$ is true.]

Now

$$\begin{aligned}
\sum_{i=1}^{k+1} i \ &= \ \sum_{i=1}^{k} i && + (k+1) \\
&= \frac{k(k+1)}{2} && + (k+1) \qquad \text{by the inductive hypothesis} \\
&= (k+1)\left(\frac{k}{2}+1\right) \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

which shows that $P(k+1)$ is true.
[Since we have proved the basis step and the inductive step, we conclude that the theorem is true.] □

Theorem. $\forall n \in \mathbb{N}$, $2^{2n} - 1$ is divisible by 3.

Proof (by mathematical induction):

Let $P(n)$ mean that $2^{2n} - 1$ is divisible by 3.

Basis step: [Need to prove $P(0)$, that is, that $2^{2\cdot 0} - 1$ is divisible by 3.]
Now

$$\begin{aligned} 2^{2\cdot 0} - 1 &= 2^0 - 1 \\ &= 1 - 1 \\ &= 0 \end{aligned}$$

which is divisible by 3 since $0 = 3 \cdot 0$. Therefore $P(0)$ is true.

Inductive step: [Need to prove $\forall k \in \mathbb{N}, (P(k) \to P(k+1))$.]
Let k be an arbitrary natural number such that $P(k)$ is true, that is,

$$2^{2k} - 1 \text{ is divisible by 3.}$$

That is, by the definition of divides,

$$2^{2k} - 1 = 3r \text{ for some integer } r.$$

We need to prove that $P(k+1)$ is true, that is, that $2^{2(k+1)} - 1$ is divisible by 3.
Now

$$\begin{aligned} 2^{2(k+1)} - 1 &= 2^{2k+2} - 1 \\ &= 2^{2k} \cdot 2^2 - 1 \qquad \text{[Write } 2^{2(k+1)} - 1 \text{ in terms of } 2^{2k} - 1\text{]} \\ &= 2^{2k} \cdot 4 - 1 \\ &= 3 \cdot 2^{2k} + 2^{2k} - 1 \\ &= 3 \cdot 2^{2k} + 3r \;\; \text{for some integer } r \\ &= 3(2^{2k} + r) \end{aligned}$$

Therefore, since $2^{2k} + r$ is an integer, $2^{2(k+1)} - 1$ is divisible by 3, that is, $P(k+1)$ is true.
[Since we have proved the basis step and the inductive step, we conclude that the theorem is true.] □

Theorem. For all integers $n \geq 3$, $2n + 1 < 2^n$.

Proof (by mathematical induction):

Let the property $P(n)$ be the inequality $2n + 1 < 2^n$.

Basis step: We need to show that $P(3)$ is true, that is, that

$$2(3) + 1 < 2^3.$$

Now $2(3) + 1 = 7$ and $2^3 = 8$ and $7 < 8$. Therefore $P(3)$ is true.

Inductive step: [Need to prove: for all integers $k \geq 3, (P(k) \to P(k+1))$.]
Let k be an arbitrary integer, $k \geq 3$, such that $P(k)$ is true, that is,

$$2k + 1 < 2^k.$$

Now

$$\begin{aligned}2(k+1) + 1 &= 2k + 2 + 1\\ &= (2k + 1) + 2\\ &< 2^k + 2^k \quad \text{by the inductive hypothesis and since } 2 < 2^k\ \forall k \geq 3\end{aligned}$$

and

$$2^k + 2^k = 2 \cdot 2^k = 2^{k+1}.$$

Therefore

$$2(k+1) + 1 < 2^{k+1}$$

that is, $P(k+1)$ is true.
We have proved the basis step and the inductive step; therefore the theorem is true by the principle of mathematical induction. □

CMPUT 272 (Stewart) University of Alberta **Lecture 9**

Reading: Epp 4.5, 4.6, 4.7

Number Theory and Methods of Proof

Theorem. Every integer is even or odd but not both.

Proof: We'll prove this later. For now, we take it for granted.

Theorem. For all integers n, if n^2 is even then n is even.

Proof: We prove the contrapositive. Let n be an odd integer. By the definition of odd, $n = 2k + 1$ for some integer k. Thus

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Thus since $2k^2 + 2k$ is an integer, n^2 is odd by the definition of odd. □

Recall: For all $r \in \mathbb{R}$,

r is *rational* if and only if $\exists\ a, b \in \mathbb{Z}$ such that $b \neq 0$ and $r = a/b$;
r is *irrational* if and only if it is not rational.

Theorem (Irrationality of $\sqrt{2}$). $\sqrt{2}$ is irrational.

Proof (by contradiction): Suppose the claim is false, that is, $\sqrt{2}$ is rational. Then there exist integers m and n such that $n \neq 0$ and

$$\sqrt{2} = \frac{m}{n}.$$

Let m and n be such that they have no common factors greater than 1, by dividing m and n by any such common factors if necessary. Squaring both sides of the equality gives

$$2 = \frac{m^2}{n^2}$$

or equivalently

$$2n^2 = m^2.$$

This implies that m^2 is even and therefore, by the preceding theorem, m is even. Thus $m = 2k$ for some integer k. Substituting into the above equality gives

$$\begin{aligned} 2n^2 &= (2k)^2 \\ &= 4k^2 \end{aligned}$$

and dividing both sides by 2 gives

$$n^2 = 2k^2.$$

Thus, n^2 is even and therefore by the preceding theorem, n is even. But then m and n are both even which contradicts that they have no common factor greater than 1. □

Definition. For any real number x, the *floor* of x, denoted $\lfloor x \rfloor$, is defined as:

$$\lfloor x \rfloor = \text{ that unique integer } n \text{ such that } n \leq x < n+1.$$

For any real number x, the *ceiling* of x, denoted $\lceil x \rceil$, is defined as:

$$\lceil x \rceil = \text{ that unique integer } n \text{ such that } n-1 < x \leq n.$$

Symbolically, for all $x \in \mathbb{R}$, $n \in \mathbb{Z}$,

$$\begin{aligned} \lfloor x \rfloor = n &\Leftrightarrow n \leq x < n+1 \\ \lceil x \rceil = n &\Leftrightarrow n-1 < x \leq n \end{aligned}$$

Theorem. For any integer n,

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Proof: Let $n \in \mathbb{Z}$.
Case 1 (n is odd): Then $n = 2k+1$ for some integer k. Then

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k+1}{2} \right\rfloor = \left\lfloor \frac{2k}{2} + \frac{1}{2} \right\rfloor = \left\lfloor k + \frac{1}{2} \right\rfloor = k$$

because k is an integer and $k \leq k + \frac{1}{2} < k+1$. And

$$\frac{n-1}{2} = \frac{2k+1-1}{2} = \frac{2k}{2} = k.$$

Therefore $\lfloor \frac{n}{2} \rfloor = \frac{n-1}{2}$ if n is odd.
Case 2 (n is even): Then $n = 2k$ for some integer k. Then

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k}{2} \right\rfloor = \lfloor k \rfloor = k$$

because k is an integer and $k \leq k < k+1$. And

$$\frac{n}{2} = \frac{2k}{2} = k.$$

Therefore $\lfloor \frac{n}{2} \rfloor = \frac{n}{2}$ if n is even.
In both cases, the equality holds. □

"Both discovery and proof are integral parts of problem solving. When you think you have discovered that a certain statement is true, try to figure out why it is true. If you succeed, you will know that your discovery is genuine. Even if you fail, the process of trying will give you insight into the nature of the problem and may lead to the discovery that the statement is false."
[Epp, p 146]

How to write a proof

Adapted from *How to Solve It* by G. Polya (1945)

1. Understand what is to be proven.

   What is the logic of the statement? What are the definitions? What are the conditions? Work through some examples (eg. simple cases, boundary conditions). Are you sure it is true?

2. Devise a plan.

   What do you know about the concepts? Have you seen something similar? Do you know a theorem that could be useful? What can you easily deduce from the conditions? From what could you easily deduce the conclusion? Can you restate what is to be proven (eg. contrapositive)? Can you prove it by contradiction? Can you break the proof into cases? Can you prove it by mathematical induction?

3. Carry out the plan.

   Check and justify each step.

4. Look back.

   Can you derive the result differently? Can you find a simpler proof?

“To be understandable and helpful, more is required of a proof than just logical correctness: a good proof must also be clear.”
[MIT course notes, p 40]

- Directions for writing proofs [Epp p 155-156]
- Good proofs in practice [MIT course notes, p 40-42]

  State your game plan.
  Keep a linear flow.
  A proof is an essay, not a calculation.
  Avoid excessive symbolism.
  Revise and simplify.
  Introduce notation thoughtfully.
  Structure long proofs.
  Be wary of the “obvious”.
  Finish.

CMPUT 272 (Stewart) University of Alberta **Lecture 8**

Reading: Epp 4.1, 4.2, 4.3

Number Theory and Methods of Proof

A *mathematical proof* is a carefully reasoned argument to convince a skeptical reader (often yourself) that a given statement is true. [Epp, p 145]

- It is written in English.
- Logic provides the framework.
- The level of detail depends on the reader.
- Basic mathematical axioms and definitions are taken for granted:
  - Laws of basic algebra and real numbers that you learned in school (For the complete list see Epp Appendix A). A few examples are:
    - *Cancellation Law for Multiplication:*
For $a, b, c \in \mathbb{R}$, if $ab = ac$ and $a \neq 0$, then $b = c$.
    - *Real Number Division:*
For $a, b \in \mathbb{R}$ with $a \neq 0$, there is exactly one $x \in \mathbb{R}$ such that $ax = b$. This x is denoted by b/a (or $\frac{b}{a}$) and is called the **quotient** of b and a.
    - For $a, b \in \mathbb{R}$,
      - if $ab = 0$ then $a = 0$ or $b = 0$
      - if $ab > 0$ then both a and b are positive or both are negative
      - $(-a)b = a(-b) = -(ab)$
      - $(-a)(-b) = ab$
  - Equality of objects A, B, and C: (1) $A = A$, (2) if $A = B$ then $B = A$, (3) if $A = B$ and $B = C$ then $A = C$
  - The integers form a subset of the real numbers.
  - The set of integers is closed under addition, subtraction, and multiplication, but not division!

Definition.

An integer n is even if and only if $n = 2k$ for some integer k.
An integer n is odd if and only if $n = 2k + 1$ for some integer k.

Symbolically:

for all integers n,

n is *even* $\Leftrightarrow \exists$ an integer k such that $n = 2k$;

n is *odd* $\Leftrightarrow \exists$ an integer k such that $n = 2k + 1$.

Theorem. The sum of any two even integers is even.

Proof: Let m and n be even integers. By the definition of even, there exist integers r and s such that $m = 2r$ and $n = 2s$. Then

$$m + n = 2r + 2s = 2(r + s).$$

Let $t = r + s$. t is an integer because it is the sum of two integers. Therefore

$$m + n = 2t \text{ where } t \text{ is an integer.}$$

So, by the definition of even, $m + n$ is even.
□

↖

QED (**quod erat demonstrandum**)

Notation (see Epp page 104).
$\Leftrightarrow$ "if and only if"
$\Rightarrow$ "if - then"

Definition.

A real number r is *rational* if and only if it can be expressed as a ratio of two integers with a nonzero denominator. A real number that is not rational is *irrational.*

Symbolically:

For all $r \in \mathbb{R}$,

r is *rational* $\Leftrightarrow \exists\ a, b \in \mathbb{Z}$ such that $b \neq 0$ and $r = a/b$.

Theorem. The sum of any two rational numbers is rational.

Proof: Let r and s be rational numbers. Then, by the definition of rational, $r = a/b$ and $s = c/d$ for some integers a, b, c and d where $b \neq 0$ and $d \neq 0$. Thus

$$\begin{aligned} r + s &= \frac{a}{b} + \frac{c}{d} \\ &= \frac{ad + bc}{bd}. \end{aligned}$$

Both $ad + bc$ and bd are integers because products and sums of integers are integers, and $bd \neq 0$ because it is the product of nonzero integers. Therefore, $r + s$ is rational by the definition of a rational number. $\square$

Integer Division

Definition of divides. For integers n and $d \neq 0$,

$$\begin{aligned} d \mid n \quad (\text{“}d \text{ divides } n\text{”}) \quad &\Leftrightarrow \quad \exists k \in \mathbb{Z} \text{ such that } n = dk. \\ &\Leftrightarrow \quad \frac{n}{d} \in \mathbb{Z}. \end{aligned}$$

Examples: $1|-4$ $\qquad$ $99|0$ $\qquad$ $7|-7$ $\qquad$ $-7|7$

Negation of divides: For integers n and $d \neq 0$,

$$\begin{aligned} d \not| \, n \quad (\text{“}d \text{ does not divide } n\text{”}) \quad &\Leftrightarrow \quad \forall k \in \mathbb{Z},\ n \neq dk. \\ &\Leftrightarrow \quad \frac{n}{d} \notin \mathbb{Z}. \end{aligned}$$

Examples: $7 \not| \, 13$ $\qquad$ $50 \not| \, 99$ $\qquad$ $2 \not| \, 1$

Theorem (Properties of Integer Division). For all $a, b, c, d \in \mathbb{Z}$,

1. $1|a$ and, if $a \neq 0$ then $a|0$ and $a|a$;
2. if $a|b$ then $a|bc$;
3. if $a|b$ and $b|c$ then $a|c$; (Transitivity of Division)
4. if $a = b + c$ and d divides two of a,b, and c, then d divides all of a,b, and c;
5. if a and b are positive, and $a|b$, then $a \leq b$;
6. if $a|b$ then $(-a)|b$;
7. if $a|b$ and $b|a$ then $a = \pm b$.

Proof:

1. Let $a \in \mathbb{Z}$. Then $1|a$ since $a = 1 \cdot a$. If $a \neq 0$ then $a|0$ since $0 = a \cdot 0$ and $a|a$ since $a = a \cdot 1$.

2. Let a, b, and c be integers such that $a|b$. Then $a \neq 0$ and there exists an integer r such that

   $$ar = b.$$

   Multiplying both sides of the equality by c gives

   $$arc = bc.$$

   Now rc is an integer since it is the product of two integers, and $a \neq 0$. Therefore, $a|bc$.

3. Let a, b, and c be integers such that $a|b$ and $b|c$. Then $a \neq 0$, $b \neq 0$, and there exist integers r and s such that

   $$ar = b \text{ and } bs = c.$$

   Combining the two equalities gives

   $$c = bs = ars.$$

   Now rs is an integer since it is the product of two integers, and $a \neq 0$. Therefore, $a|c$.

4. Let a, b, c, and d be integers such that $a = b + c$ and d divides two of a,b, and c. By the definition of divides, $d \neq 0$. *[The proof is by division into cases.]*

   Case 1 ($d|a$ and $d|b$): In this case, there exist integers r and s such that

   $$a = dr \text{ and } b = ds.$$

   Then

   $$c = a - b = dr - ds = d(r - s),$$

   $r - s$ is an integer since it is the difference of two integers, and $d \neq 0$. Therefore $d|c$.

   Case 2 ($d|a$ and $d|c$): In this case, there exist integers r and s such that

   $$a = dr \text{ and } c = ds.$$

   Then

   $$b = a - c = dr - ds = d(r - s),$$

   $r - s$ is an integer since it is the difference of two integers, and $d \neq 0$. Therefore $d|b$.

   Case 3 ($d|b$ and $d|c$): In this case, there exist integers r and s such that

   $$b = dr \text{ and } c = ds.$$

   Then

   $$a = b + c = dr + ds = d(r + s),$$

   $r + s$ is an integer since it is the sum of two integers, and $d \neq 0$. Therefore $d|a$.

   No matter which case occurs, d divides all of a,b, and c.

5. Let a and b be positive integers such that $a|b$. Then there exists an integer r such that

   $$b = ar.$$

   Now ar is positive, since b is positive. It follows that r is positive since a is positive and the product of two integers is positive if and only if both integers are positive or both are negative. Therefore

   $$1 \leq r.$$

Multiplying both sides of this inequality by a, and combining with the equality gives

$$a \leq ar = b.$$

6. Let a and b be integers such that $a|b$. By the definition of divides, $a \neq 0$ and there exists an integer r such that

$$ar = b.$$

So

$$(-a)(-r) = b.$$

Now $-r$ is an integer since r is an integer, and $-a \neq 0$ because $a \neq 0$. Therefore, $(-a)|b$.

7. Let a and b be integers such that $a|b$ and $b|a$. By the definition of divides, $a \neq 0$, $b \neq 0$, and there exist integers r and s such that

$$ar = b \text{ and } bs = a.$$

Combining the two equalities gives

$$a = bs = ars$$

and therefore, since $a \neq 0$, by the Cancellation Law for Multiplication,

$$rs = 1.$$

Since $1 = 1 \cdot 1 = (-1)(-1)$, both 1 and -1 are divisors of 1. By (5), 1 is the only positive divisor of 1. If there were a negative divisor of 1 other than -1, (6) would imply the existence of a positive divisor of 1 other than 1, a contradiction. Therefore, the only negative divisor of 1 is -1. This implies that $r = s = 1$ or $r = s = -1$ and therefore $a = \pm b$.

□

Reading: Epp 3.4

Rules of inference and formal proofs in predicate logic

To **prove** that X logically implies Y,

show that every interpretation that makes X true also makes Y true

by giving:

an informal argument or

a formal proof using rules of inference and logical equivalences.

Valid Rules of Inference for Quantifiers [Epp 3.4, Grimaldi 2.5]

1. *Universal Instantiation (Specification)*

$$\begin{array}{lll} & \forall x \in D, P(x) & \\ \therefore & P(a) & \text{where } a \text{ is any particular element of } D \end{array}$$

2. *Universal Generalization*

$$\begin{array}{lll} & P(a) & \text{where } a \text{ is an } \textit{arbitrary} \text{ element of } D \\ \therefore & \forall x \in D, P(x) & \end{array}$$

3. *Existential Instantiation (Specification)*

$$\begin{array}{lll} & \exists x \in D \text{ such that } P(x) & \\ \therefore & P(a) & \text{for } \textit{some } a \text{ in } D \end{array}$$

4. *Existential Generalization*

$$\begin{array}{lll} & P(a) & \text{where } a \text{ is an element of } D \\ \therefore & \exists x \in D \text{ such that } P(x) & \end{array}$$

5. *Universal Modus Ponens*

$$\begin{array}{lll} & \forall x \in D, (P(x) \to Q(x)) & \\ & P(a) & \text{where } a \text{ is an element of } D \\ \therefore & Q(a) & \end{array}$$

6. *Universal Modus Tollens*

$$\begin{array}{lll} & \forall x \in D, (P(x) \to Q(x)) & \\ & \sim Q(a) & \text{where } a \text{ is an element of } D \\ \therefore & \sim P(a) & \end{array}$$

7. *Universal Transitivity*

$$\begin{array}{ll} & \forall x \in D, (P(x) \to Q(x)) \\ & \forall x \in D, (Q(x) \to R(x)) \\ \therefore & \forall x \in D, (P(x) \to R(x)) \end{array}$$

Proofs in Predicate Logic

Example: The domain of all variables is D.

$$\begin{array}{ll} & \forall x, (P(x) \vee \sim Q(x)) \\ & \forall x, (P(x) \rightarrow R(x)) \\ & \forall x, (\sim Q(x) \rightarrow R(x)) \\ \therefore & \forall x, R(x) \end{array}$$

1.	$\forall x, (P(x) \vee \sim Q(x))$	Premise
2.	$\forall x, (P(x) \rightarrow R(x))$	Premise
3.	$\forall x, (\sim Q(x) \rightarrow R(x))$	Premise
4.	$P(a) \vee \sim Q(a)$	1, Universal Instantiation a is an *arbitrary* element of the domain (↑ needed later for step 8)
5.	$P(a) \rightarrow R(a)$	2, Universal Instantiation
6.	$\sim Q(a) \rightarrow R(a)$	3, Universal Instantiation
7.	$R(a)$	4, 5, 6, Proof by Division into Cases
8.	$\therefore \forall x, R(x)$	7, Universal Generalization

Example: The domain of all variables is D.

$\quad\exists x$ such that $(C(x) \wedge \sim B(x))$
$\quad\forall x, (C(x) \to P(x))$
$\therefore\ \exists x$ such that $(P(x) \wedge \sim B(x))$

1.	$\exists x$ such that $(C(x) \wedge \sim B(x))$	Premise
2.	$\forall x, (C(x) \to P(x))$	Premise
3.	$C(a) \wedge \sim B(a)$	1, EI
4.	$C(a)$	3, Specialization
5.	$P(a)$	2, 4, Universal Modus Ponens
6.	$\sim B(a)$	3, Specialization
7.	$P(a) \wedge \sim B(a)$	5, 6, Conjunction
8.	$\therefore\ \exists x$ such that $(P(x) \wedge \sim B(x))$	7, EG

Example: The domain of all variables is D.

$\forall x, (P(x) \vee Q(x))$
$\forall x, ((\sim P(x) \wedge Q(x)) \rightarrow R(x))$
$\therefore\ \forall x, (\sim R(x) \rightarrow P(x))$

1.	$\forall x, (P(x) \vee Q(x))$	Premise
2.	$\forall x, ((\sim P(x) \wedge Q(x)) \rightarrow R(x))$	Premise
3.	$\sim R(a)$	Assume for Hypothetical Reasoning, a is arbitrary (needed later for step 13)
4.	$\sim (\sim P(a) \wedge Q(a))$	2, 3, Universal Modus Tollens
5.	$\sim\sim P(a) \vee \sim Q(a)$	4, De Morgan's law
6.	$P(a) \vee \sim Q(a)$	5, Double Negation
7.	$P(a) \vee Q(a)$	1, Universal Instantiation
8.	$(P(a) \vee Q(a)) \wedge (P(a) \vee \sim Q(a))$	6, 7, Conjunction
9.	$P(a) \vee (Q(a) \wedge \sim Q(a))$	8, Distributive law
10.	$P(a) \vee \mathbf{c}$	9, Negation law
11.	$P(a)$	10, Identity law
12.	$\sim R(a) \rightarrow P(a)$	3-11, Hypothetical Reasoning
13.	$\therefore\ \forall x, (\sim R(x) \rightarrow P(x))$	12, Universal Generalization

Logic and Theoretical Computer Science

Reading: Mathematics for Computer Science MIT (2010) Readings Chapter 1.5, Epp 6.4

The problem SAT: Is a given propositional logic statement form satisfiable?

- *decidable*, that is, there is an algorithm that gives a yes/no answer:
  - compute the truth table
  - check if there is a T in at least one row
- But there are 2^n rows in the truth table for a statement form with n variables.
  - 2^{100} is a 31 digit number
  - At 1 microsecond / row, it would take 400 trillion centuries
    to compute a truth table with 2^{100} rows
- Is there a more efficient algorithm?
  - No one knows!
  - SAT plays an important role the theory of NP-completeness
  - P (polynomial) $\subseteq$ NP (nondeterministic polynomial)
  - Is P = NP? ($\$1,000,000$ prize: Clay Mathematics Institute Cambridge MA)
  - SAT solvers can solve *any* NP problem
    (but not in polynomial time)

Another problem: Is a given predicate logic statement satisfiable?

- *undecidable*: there cannot exist an algorithm that gives a yes/no answer.
- related to the Entscheidungsproblem: Is a given predicate logic statement true under all interpretations? which was posed by Hilbert in 1928 and shown to be undecidable by Turing and Church in 1936.
- related to the halting problem

Example: Transforming an instance of exam scheduling to a SAT instance

The problem:
Given integers n and k, and a set of conflicts: $C = \{(i,j) \mid$ where $1 \leq i < j \leq n$ and exam i cannot be scheduled at the same time as exam $j\}$,
can n exams be scheduled in k timeslots such that no conflicting exams are scheduled in the same timeslot?

We construct a statement form in propositional logic that is satisfiable if and only if the answer to the exam scheduling problem is yes.

There are nk variables: x_{ij} where $1 \leq i \leq n$ and $1 \leq j \leq k$.
Variable x_{ij} means "Exam i is scheduled in timeslot j."

The statement form is the conjunction of the following subformulas:

Each exam is scheduled into a timeslot:

$$\begin{array}{l} x_{11} \vee x_{12} \vee \cdots \vee x_{1k} \\ x_{21} \vee x_{22} \vee \cdots \vee x_{2k} \\ \qquad\qquad \vdots \\ x_{n1} \vee x_{n2} \vee \cdots \vee x_{nk} \end{array}$$

No exam is scheduled in two timeslots:

$$\begin{array}{ll} \sim (x_{1i} \wedge x_{1j}) & \\ \sim (x_{2i} \wedge x_{2j}) & \qquad\text{for all } 1 \leq i < j \leq k \\ \qquad \vdots & \\ \sim (x_{ni} \wedge x_{nj}) & \end{array}$$

No conflicting exams are scheduled in the same timeslot:

$$\begin{array}{ll} \sim (x_{i1} \wedge x_{j1}) & \\ \sim (x_{i2} \wedge x_{j2}) & \qquad\text{for all } (i,j) \in C \\ \qquad \vdots & \\ \sim (x_{ik} \wedge x_{jk}) & \end{array}$$

Reading: Epp 1.1, 1.2, 3.1, 3.2, 3.3

Interpretations, logical equivalence, and logical implication

Recall that, in propositional logic:

- a truth assignment of a propositional logic statement form is an assignment of truth values to the variables
- a truth table lists all possible truth assignments

But in predicate logic:

- each predicate has a truth value for each element of the domain
- so if the domain is large or infinite, we can't list all possibilities

Definition. An *interpretation* of a predicate logic statement is a specification of:

$$\underline{\text{(nonempty) domains}} \text{ and } \underline{\text{meanings}} \text{ of the predicates.}$$

- A *satisfying* interpretation is one under which the statement evaluates to true.
- A *falsifying* interpretation is one under which the statement evaluates to false.

Example: $\forall x, (P(x) \vee Q(x))$

- a falsifying interpretation:

  domain: $\mathbb{Z}$, $P(x)$: $x < 0$, $Q(x)$: $x > 0$
- a satisfying interpretation:

  domain: $\{a, b\}$, $P(a) : T$, $P(b) : T$, $Q(a) : T$, $Q(b) : F$

Definition. A statement in predicate logic is

- *satisfiable* if it has a satisfying interpretation;
- *falsifiable* if it has a falsifying interpretation;
- a *tautology*, denoted by **t**, if it is true under every interpretation;
- a *contradiciton*, denoted by **c**, if it is false under every interpretation.

Definition. For predicate logic statements X and Y:

- X is *logically equivalent* to Y, written $X \equiv Y$, if X and Y have the same truth value under all interpretations.
- X *logically implies* Y if, under every interpretation that makes X true, Y is also true.

Note: $X \equiv Y$ if and only if X logically implies Y and Y logically implies X.

Logical Equivalences involving $\forall$ and $\exists$ [Epp 3.2, Grimaldi 2.4]

Given predicates $P(x)$ and $Q(x)$, and domain D, the following logical equivalences hold.

1. *Negation of a universal statement:*

   $\sim(\forall x \in D, Q(x)) \equiv \exists x \in D$ such that $\sim Q(x)$

2. *Negation of an existential statement:*

   $\sim(\exists x \in D$ such that $Q(x)) \equiv \forall x \in D, \sim Q(x)$

3. *Negation of a universal conditional statement:*

   $\sim(\forall x \in D, (P(x) \to Q(x))) \equiv \exists x \in D$ such that $(P(x) \wedge \sim Q(x))$

4. *Contrapositive of a universal conditional statement:*

   $\forall x \in D, (P(x) \to Q(x)) \equiv \forall x \in D, (\sim Q(x) \to \sim P(x))$

Reasoning about logical equivalence and logical implication:

- To **prove** that X logically implies Y, show that every interpretation that makes X true also makes Y true.
  - Use an informal argument: Example:
    $\exists x \in D$ such that $(P(x) \wedge Q(x))$ logically implies
    $(\exists x \in D$ such that $P(x)) \wedge (\exists x \in D$ such that $Q(x))$
  - or give a proof using rules of inference.

- To **prove** that $X \equiv Y$, show that under each interpretation, X and Y are both true or both false.
  - Use known logical equivalences:
    Example: Simplify the negation of Goldbach's conjecture:

    $\sim \forall n \in \mathbb{N}, ((n > 2 \wedge n \text{ even}) \to (\exists p, q \in \mathbb{P} \text{ such that } n = p + q))$
    $\equiv \exists n \in \mathbb{N} \text{ such that } \sim ((n > 2 \wedge n \text{ even}) \to (\exists p, q \in \mathbb{P} \text{ such that } n = p + q))$
    negation of universal
    $\equiv \exists n \in \mathbb{N} \text{ such that } ((n > 2 \wedge n \text{ even}) \wedge \sim (\exists p, q \in \mathbb{P} \text{ such that } n = p + q))$
    negation of conditional
    $\equiv \exists n \in \mathbb{N} \text{ such that } ((n > 2 \wedge n \text{ even}) \wedge (\forall p, q \in \mathbb{P}, n \neq p + q))$
    negation of existential

  - or prove that X logically implies Y and Y logically implies X.

- To **disprove** that X logically implies Y, give a counterexample, that is, an interpretation under which X is true and Y is false.

  Example: Disprove the following statement:

  $(\exists x \in D$ such that $P(x)) \wedge (\exists x \in D$ such that $Q(x))$ logically implies
  $\exists x \in D$ such that $(P(x) \wedge Q(x))$

- To **disprove** that $X \equiv Y$, give a counterexample, that is, an interpretation under which X and Y have different truth values.

CMPUT 272 (Stewart) University of Alberta **Lecture 5**

Reading: Epp 1.1, 1.2, 3.1, 3.2, 3.3

Predicate Logic

Definition. A *set* is an unordered collection of distinct elements.

Examples and Notation:

$S = \{1, 5, 10, 2, 4\}$	set-roster notation
$1 \in S$, $5 \in S$, $3 \notin S$	element
$\{1, 5\} \subseteq S$, $\{1, 5, 3\} \not\subseteq S$	subset
$T = \{x \in S \mid x \text{ is even}\}$	set-builder notation
$\{\} = \emptyset$	empty set
$\mathbb{R}$	real numbers
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$	integers
$\mathbb{Z}^+ = \{1, 2, \ldots\}$	positive integers
$\mathbb{Z}^{nonneg} = \{0, 1, 2, \ldots\}$	nonnegative integers
$\mathbb{N} = \{0, 1, 2, \ldots\}$	natural numbers
$\mathbb{Q}$	rational numbers
$\mathbb{P}$	prime numbers

Predicate Logic

- propositional logic with the addition of predicates, quantifiers, $=$, $\neq$
- allows us to express facts about all or some elements of sets

Definition. A *predicate* is a sentence that contains one or more variables where

- each variable is associated with a nonempty set, called its *domain* or *universe of discourse*, and
- the sentence becomes a statement when each variable is replaced by an element of its domain.

Examples:

Predicate: x lives in Alberta. Let the domain of x be the set of all people.
Statement: Mary lives in Alberta. (Mary is a person.)
Predicate symbol: Let A stand for "lives in Alberta".
Predicate: $A(x)$ is formal notation for "x lives in Alberta".
Statement: $A(\text{Mary})$ is formal notation for "Mary lives in Alberta".

Let $T(p, q)$ be "p is at least q centimetres tall",
where the domain of p is the set of all people and the domain of q is $\mathbb{Z}^+$.

Let $S(x, y, z)$ be "$x + y = z$" where the domain of all variables is $\mathbb{Z}$.

Quantifiers are combined with predicates to say something about *all* or *some* elements of a domain.

Universal Quantifier: $\forall$ "For all ... "

$\forall x \in D$, $Q(x)$ universal statement

- Truth value
  - T if and only if $Q(x)$ is T for every $x \in D$
    - $*$ To show that a universal statement is true, show that the quantified statement is true for *every* element of the domain.
  - F if and only if $Q(x)$ is F for at least one $x \in D$
    - $*$ To show that a universal statement is false,
      give a *counterexample.*
- Relation between $\forall$ and $\wedge$: If $D = \{x_1, x_2, \ldots x_n\}$ then

$$\forall x \in D, Q(x) \quad \text{means} \quad Q(x_1) \wedge Q(x_2) \wedge \cdots \wedge Q(x_n)$$

Existential Quantifier: $\exists$ "There exists ... "

$\exists x \in D$ such that $Q(x)$ existential statement

- Truth value
  - T if and only if $Q(x)$ is T for at least one $x \in D$
    - $*$ To show that an existential statement is true, give an *example.*
  - F if and only if $Q(x)$ is F for all $x \in D$
    - $*$ To show that an existential statement is false, show that the quantified statement is false for *every* element of the domain.
- Relation between $\exists$ and $\vee$: If $D = \{x_1, x_2, \ldots x_n\}$ then

$$\exists x \in D \text{ such that } Q(x) \quad \text{means} \quad Q(x_1) \vee Q(x_2) \vee \cdots \vee Q(x_n)$$

Note: $Q(x)$ (the quantified statement) can be a complicated logical expression involving many predicates, quantifiers, and logical connectives.

Definition. The *truth set* of a predicate $P(x)$ on domain D is $\{x \in D \mid P(x) \text{ is true}\}$.

Example:
Let $E(x)$ be "x is even" on domain $\{x \in \mathbb{Z}^+ \mid x \leq 20\}$.
The truth set of $E(x)$ is $\{2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$.

These two statements always have the same truth value:

$$\sim\ \forall x \in D, Q(x)$$
$$\exists x \in D \text{ such that } \sim Q(x)$$

and so do these:

$$\sim\ \exists x \in D \text{ such that } Q(x)$$
$$\forall x \in D, \sim Q(x)$$

For u and v representing elements of a domain,

$u = v$ means that u and v denote the same element of the domain, and
$u \neq v$ means that u and v denote two distinct elements of the domain.

Think of $=$ and $\neq$ as special predicates.

Translating between English and predicate logic

$\forall$: all, every, each

$\exists$: there exists, there is at least one, some

Combine predicates and quantified statements with $\wedge$, $\vee$, $\sim$, $\rightarrow$, $\leftrightarrow$

Examples:

1. $A(x)$: x lives in Alberta
   $C(x)$: x is a student in this class
   P: the set of all people
   S: the set of all students in this class

   Every student in this class lives in Alberta.

   $\forall x \in S, A(x)$

   $\forall x \in P, (C(x) \rightarrow A(x))$

   Some student in this class lives in Alberta.

   $\exists x \in S$ such that $A(x)$

   $\exists x \in P$ such that $(C(x) \wedge A(x))$

   No student in this class lives in Alberta.

   $\forall x \in S, \sim A(x)$

   $\forall x \in P, (C(x) \rightarrow \sim A(x))$

   $\forall x \in P, (C(x) \wedge A(x))$

   Every person is in this class and lives in Alberta.

   $\exists x \in P$ such that $(C(x) \rightarrow A(x))$

   There is a person such that if he is in this class then he lives in Alberta.

2. Write the following statements in symbolic form using the predicates:

   $P(x)$: $x > 0$
   $Q(x)$: x is even
   $R(x)$: x is divisible by 5

   There exists a positive integer that is even.

   $\exists x \in \mathbb{Z}$ such that $(P(x) \wedge Q(x))$

   $\exists x \in \mathbb{Z}^+$ such that $Q(x)$

   If an integer is even, then it is not divisible by 5.

   $\forall x \in \mathbb{Z}, (Q(x) \to \sim R(x))$

   No even integer is divisible by 5.

   $\forall x \in \mathbb{Z}, (Q(x) \to \sim R(x))$

   $\sim \exists x \in \mathbb{Z}$ such that $(Q(x) \wedge R(x))$

   There exists an even integer that is divisible by 5.

   $\exists x \in \mathbb{Z}$ such that $(Q(x) \wedge R(x))$

   If x is a positive, even integer then x is divisible by 5.

   $\forall x \in \mathbb{Z}, ((P(x) \wedge Q(x)) \to R(x))$

At least one integer is even.

$\exists x \in \mathbb{Z}$ such that $Q(x)$

At least two integers are even.

$\exists x, y \in \mathbb{Z}$ such that $(Q(x) \wedge Q(y) \wedge x \neq y)$

At most one integer is even.

$\forall x, y \in \mathbb{Z}, (Q(x) \wedge Q(y) \rightarrow x = y)$

Exactly one integer is even.

$\exists x \in \mathbb{Z}$ such that $(Q(x) \wedge \forall y \in \mathbb{Z}, (Q(y) \rightarrow x = y))$

Using mathematical notation as predicates

Stating the domain only once when variables have the same domain

Multiple Quantifiers: Order is important! Domain is important!

Examples:

- $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}$ such that $x + y = 0$ T
- $\exists y \in \mathbb{Z}$ such that $\forall x \in \mathbb{Z}$, $x + y = 0$ F
- $\forall x \in \mathbb{Z}^+, \exists y \in \mathbb{Z}^+$ such that $x + y = 0$ F

- $\forall q \in \mathbb{Z}$, $\exists p \in \mathbb{P}$ such that $p > q$

  infinitely many prime numbers exist (known since Euclid's time)

- $\forall a, b, c, n \in \mathbb{Z},\ ((a, b, c > 0 \wedge n > 2) \to a^n + b^n \neq c^n)$

  Fermat's last theorem, proved by Andrew Wiles in 1994

- $\forall n \in \mathbb{N}, ((n > 2 \wedge n$ even$) \to (\exists p, q \in \mathbb{P}$ such that $n = p + q))$

  Goldbach's conjecture (1742): Every even integer greater than 2 can be written as the sum of two primes. Unproven; holds up to $4 \cdot 10^{18}$.

CMPUT 272 (Stewart) University of Alberta **Lecture 4**

Reading: Epp 2.4, 2.5

Positional Number Systems [Epp 2.5] (nonnegative numbers)

The decimal (base 10) number system that we use every day is a positional number system: a string of digits represents a value that depends on the positions of the digits.

Example. The value of "85921" is:

$$8 \times 10^4 + 5 \times 10^3 + 9 \times 10^2 + 2 \times 10^1 + 1 \times 10^0$$

In the base 10 number system:

- digits are $0, 1, \ldots, 9$

- the value of the base 10 number $d_k d_{k-1} \ldots d_2 d_1 d_0$ is

$$d_k \times 10^k \ + \ d_{k-1} \times 10^{k-1} \ + \ \ldots \ + \ d_2 \times 10^2 \ + \ d_1 \times 10^1 \ + \ d_0 \times 10^0$$

In the base b number system (for integer $b \geq 2$):

- digits are $0, 1, \ldots, b-1$

- the value of the base b number $d_k d_{k-1} \ldots d_2 d_1 d_0$ is

$$d_k \times b^k \ + \ d_{k-1} \times b^{k-1} \ + \ \ldots \ + \ d_2 \times b^2 \ + \ d_1 \times b^1 \ + \ d_0 \times b^0$$

Converting a base b number to base 10

Evaluate the expression using base 10 arithmetic.

Examples:

$$\begin{aligned}2102_3 &= 2 \times 3^3 + 1 \times 3^2 + 0 \times 3^1 + 2 \times 3^0\\ &= 2 \times 27 + 1 \times 9 \ + 0 \times 3 \ + 2 \times 1\\ &= 54 + 9 + 2\\ &= 65_{10}\end{aligned}$$

$$\begin{aligned}101110_2 &= 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0\\ &= 32 + 8 + 4 + 2\\ &= 46_{10}\end{aligned}$$

Addition in other bases works the same as in base 10.

Example:

$$\begin{array}{rcccccccc} & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0\\ + & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0\end{array}$$

To convert a base 10 number n to base b,

find the sequence of base b digits $d_k\ d_{k-1}\ \ldots\ d_2\ d_1\ d_0$ such that

$$n \ = \ d_k \times b^k \ + \ d_{k-1} \times b^{k-1} \ + \ \ldots \ + \ d_2 \times b^2 \ + \ d_1 \times b^1 \ + \ d_0 \times b^0.$$

One method:

1. Find the largest k such that $b^k \leq n$.

2. Find the largest d_k such that $d_k \times b^k \leq n$.

Now, $n = d_k \times b^k \ + \ \underbrace{\ \ldots\ \ }$ i.e., d_k is the leftmost digit of n.

The remaining digits ↑ have to represent the value:

$$\underbrace{n - d_k \times b^k}.$$

So, find the leftmost digit of ↑ and so on.

Another method:

1. Divide n by b to obtain the quotient q and remainder r such that

$$n = bq + r, \quad 0 \leq r < b.$$

2. We want to find $d_k d_{k-1} \ldots d_2 d_1 d_0$ such that

$$\begin{aligned} n = & \ d_k \times b^k \ + \ d_{k-1} \times b^{k-1} \ + \ \ldots \ + \ d_1 \times b^1 \ + \ d_0 \times b^0 \\ = & \ b \ (\underbrace{d_k \times b^{k-1} \ + \ d_{k-1} \times b^{k-2} \ + \ \ldots \ + \ d_1}_{q}) \ + \ \underbrace{d_0}_{r} \end{aligned}$$

So the base b representation of n is $\underbrace{d_k\ d_{k-1}\ \ldots\ d_2\ d_1}\underbrace{d_0}$

base b representation of q ↑ r

So, find the rightmost digit of q and so on.

Example. Convert 51_{10} to base 3

$$
\begin{aligned}
51_{10} &= 1 \times 3^3 + (51 - 27) \\
&= 1 \times 3^3 \ + \ 24 \\
&= 1 \times 3^3 \ + \ 2 \times 3^2 \ + \ 6 \\
&= 1 \times 3^3 \ + \ 2 \times 3^2 \ + \ 2 \times 3^1 \\
&= 1 \times 3^3 \ + \ 2 \times 3^2 \ + \ 2 \times 3^1 \ + \ 0 \times 3^0 \\
&= 1220_3
\end{aligned}
$$

Example. Convert 77_{10} to binary

$$
\begin{aligned}
77_{10} &= 2^6 + (77 - 64) \\
&= 2^6 + 13 \\
&= 2^6 + 2^3 + 5 \\
&= 2^6 + 2^3 + 2^2 + 1 \\
&= 2^6 + 2^3 + 2^2 + 2^0 \\
&= 1001101_2
\end{aligned}
$$

Hexadecimal number system Base 16

Digits are: $0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ A\ B\ C\ D\ E\ F$

Hex	Decimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Example:

$$B49F_{16} = 11 \times 16^3 \ + \ 4 \times 16^2 \ + \ 9 \times 16^1 \ + \ 15 \times 16^0 = 46239_{10}$$

Converting between two bases when one is a power of the other

Example: $5E2B_{16} = 101\ 1110\ 0010\ 1011_2$

5	E	2	B
101	1110	0010	1011

Why does it work?

$$
\begin{aligned}
5\mathrm{E}2\mathrm{B}_{16} &= 5 \times 16^3 \ + \ 14 \times 16^2 \ + \ 2 \times 16^1 \ + \ 11 \times 16^0 \\
&= (2^2 + 2^0)2^{12} + (2^3 + 2^2 + 2^1)2^8 + (2^1)2^4 + (2^3 + 2^1 + 2^0)2^0
\end{aligned}
$$

$$
\begin{array}{ccccccccccccccccc}
= & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
+ & & & & & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
+ & & & & & & & & & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
+ & & & & & & & & & & & & & 1 & 0 & 1 & 1 \\
\hline
= & & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1_2
\end{array}
$$

Computer Arithmetic

- numbers are represented in binary
- stored in fixed size registers / memory locations
  - An 8-bit register can store 2^8 distinct numbers:

$$\begin{array}{ll} 00000000_2 & \\ \quad\text{to} & \\ 11111111_2 & = 2^8 - 1 = 255_{10} \end{array}$$

  - In reality, registers are 32 or 64 bits.
    $2^{32} - 1 > 4$ billion (a 10-digit number)
    $2^{64} - 1 > 18$ million trillion (a 20-digit number)
    and bigger numbers can be represented in multiple registers.
- to represent negative numbers
  - sign bit
  - two's complement notation:
    reduces subtraction to addition and allows for overflow detection
- contents of memory can be represented succinctly in hexadecimal notation

Digital Logic Circuits

A *switching device* is a basic electrical or electronic device for making, breaking, or changing the connections in a circuit.

A *digital logic circuit* is an arrangement of switching devices that transforms combinations of input signal bits to an output signal bit (0 or 1).

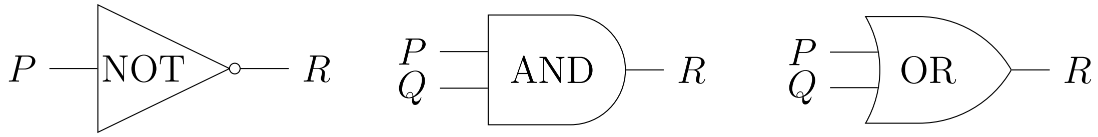
inputs
output

The *Input/Output table* of a circuit gives the output for each combination of input signals.

Two circuits are *equivalent* if their I/O tables are identical.

Logic gates

- three simple circuits that are combined to form more complex circuits
- correspond to the logical connectives ∼, ∧, and ∨ (0/F, 1/T)
- Symbols and Input/Output tables:



Input	Output
P	R
0	1
1	0

Input		Output
P	Q	R
0	0	0
0	1	0
1	0	0
1	1	1

Input		Output
P	Q	R
0	0	0
0	1	1
1	0	1
1	1	1

Note: Since ∧ and ∨ are associative,

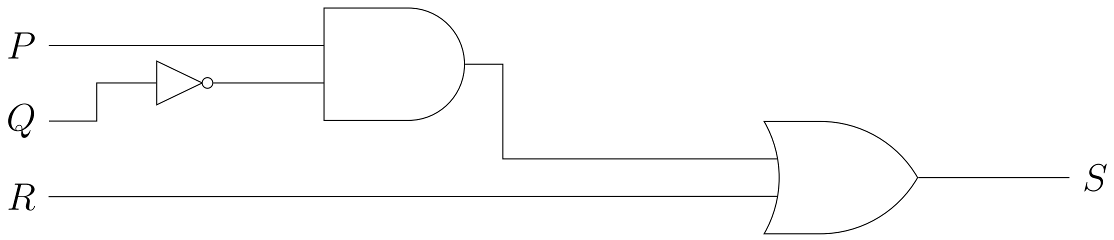
- we often write a logical statement form containing only the connective ∧ or only the connective ∨ without parentheses, and
- AND and OR gates can have three or more inputs.

A circuit composed of AND, OR, and NOT gates corresponds to a statement form containing only the connectives $\wedge$, $\vee$, and $\sim$: this is called a *Boolean expression* (FT / 01) [after George Boole, English mathematician, 1800's].

So the transformation of a circuit can be described using logic
[Shannon (MIT) 1930's]:

Inputs: statement variables
Output: a compound statement form on the input variables

Example Circuit:



Converting between circuits, Boolean expressions, and I/O tables
(see examples in textbook):

- To determine the output of a circuit for a given input, follow signals from left to right.
- To construct the I/O table of a circuit, determine the output for all possible inputs.
- To find a Boolean expression for a circuit, combine inputs from left to right.
- To find a circuit that corresponds to a given a Boolean expression, use a logic gate for each connective.
- To find a circuit that corresponds to a given I/O table, construct a Boolean expression (see p 72 of the textbook).

Circuit for binary addition

Example:

$$\begin{array}{cc} & 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0 \\ + & 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0 \end{array}$$

To add the rightmost pair of bits, we add two 1-bit numbers. For the other pairs, we need to add three 1-bit numbers to accommodate possible carries.

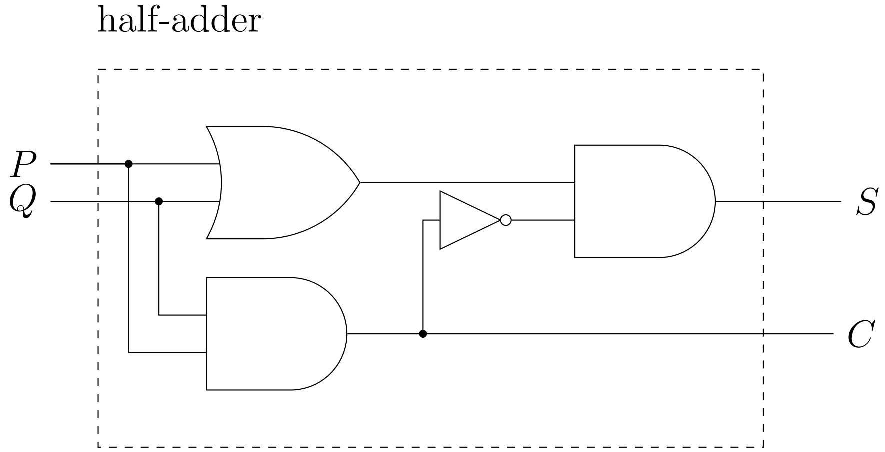
I/O table for adding two 1-bit numbers:

$$\begin{array}{cc} & P \\ + & Q \\ \hline C & S \end{array}$$

P	Q	C	S
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

$$\begin{aligned} &S = (P \vee Q) \wedge \sim (P \wedge Q) \\ &C = P \wedge Q \end{aligned}$$

Circuit for adding two 1-bit numbers:

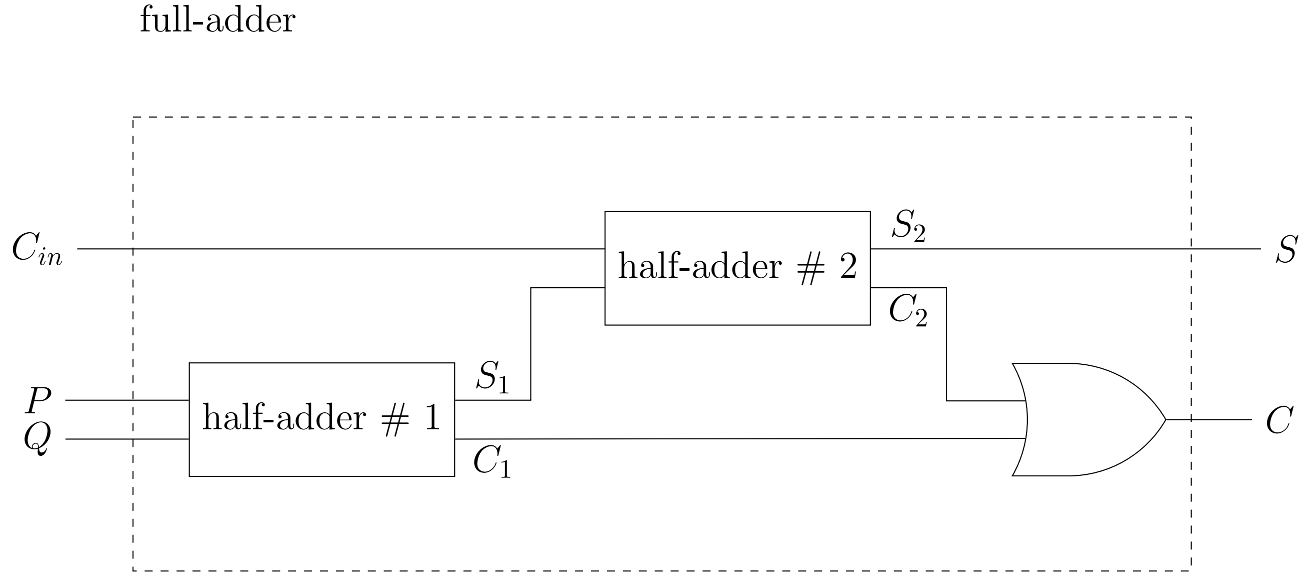


I/O table for adding three 1-bit numbers:

$$\begin{array}{cc} & C_{in} \\ & P \\ + & Q \\ \hline C & S \end{array}$$

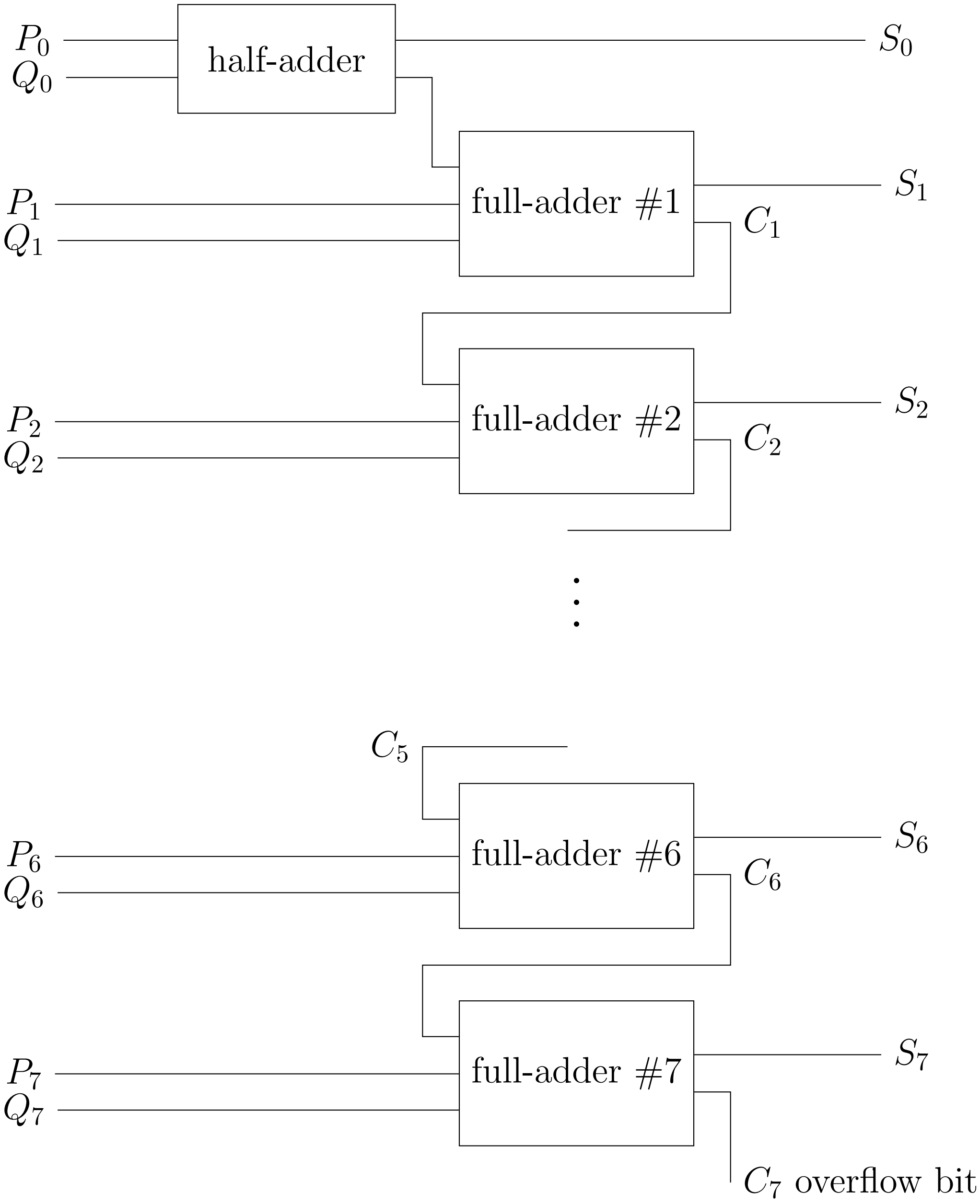
P	Q	C_{in}	C	S
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Circuit for adding three 1-bit numbers:



To add two 8-bit numbers:

$$\begin{array}{ccccccccc}
C_7 & C_6 & C_5 & C_4 & C_3 & C_2 & C_1 & C_0 & \\
 & P_7 & P_6 & P_5 & P_4 & P_3 & P_2 & P_1 & P_0 \\
+ & Q_7 & Q_6 & Q_5 & Q_4 & Q_3 & Q_2 & Q_1 & Q_0 \\
\hline
 & S_7 & S_6 & S_5 & S_4 & S_3 & S_2 & S_1 & S_0
\end{array}$$



CMPUT 272 (Stewart) University of Alberta **Lecture 3**

Reading: Epp 2.3

Arguments and Proofs

Definition. An *argument* is a sequence of statements. The last statement of an argument is the *conclusion*; each other statement is called a *premise*.

Definition. An *argument form* is a sequence of statement forms. The last statement form of an argument form is the *conclusion*; each other statement form is called a *premise*.

Example:

If Rex is a dog then Rex barks.	$p \to q$
Rex is a dog.	p
$\therefore$ Rex barks.	$\therefore\ q$

Definition. An argument (or argument form) is *valid* if, whenever the premises are true, the conclusion is also true. Otherwise, it is *invalid.*

In other words, the argument form
$$\begin{array}{rl} & p_1 \\ & p_2 \\ & \vdots \\ & p_n \\ \therefore & q \end{array}$$
is valid

if and only if $(p_1) \wedge (p_2) \wedge \cdots \wedge (p_n)$ logically implies q,

or equivalently,

if and only if $(p_1) \wedge (p_2) \wedge \cdots \wedge (p_n) \to q$ is a tautology,

or equivalently,

if and only if in each row of the truth table where all premises are true, the conclusion is also true.

An argument form is invalid

if and only if there is a row in the truth table where all premises are true and the conclusion is false.

Table 2.3.1 Valid Argument Forms (Rules of inference) [Epp Ch 2.3]
Valid argument forms that are frequently used in deductive reasoning.

Modus Ponens	$p \to q$ p $\therefore q$	Elimination	a. $p \vee q$ $\sim q$ $\therefore p$ b. $p \vee q$ $\sim p$ $\therefore q$
Modus Tollens	$p \to q$ $\sim q$ $\therefore \sim p$	Transitivity	$p \to q$ $q \to r$ $\therefore p \to r$
Generalization	a. p $\therefore p \vee q$ b. q $\therefore p \vee q$	Proof by Division into Cases	$p \vee q$ $p \to r$ $q \to r$ $\therefore r$
Specialization	a. $p \wedge q$ $\therefore p$ b. $p \wedge q$ $\therefore q$		
Conjunction	p q $\therefore p \wedge q$	Contradiction Rule	$\sim p \to \mathbf{c}$ $\therefore p$

Definition. A *formal proof* is a numbered sequence of statement forms, each with a justification, where each statement form is

- a premise (Justification "Premise"),
- an assumption (Justification "Assumption for Hypothetical Reasoning"),
- or is obtained by applying a logical equivalence or a rule of inference to previous statement forms (Justification: line numbers of the previous statement forms used, and the name of the law or rule applied),

and the last statement form is the conclusion.

Because the logical equivalences and rules of inference are valid, each statement form in a proof, including the conclusion, is logically implied by the premises.

$$\text{A formal proof} \quad \begin{array}{rl} & p_1 \\ & p_2 \\ & \vdots \\ & p_n \\ & \vdots \\ & \vdots \\ \therefore & q \end{array} \quad \text{guarantees the validity of the argument form} \quad \begin{array}{rl} & p_1 \\ & p_2 \\ & \vdots \\ & p_n \\ \therefore & q \end{array}$$

Example: Verify the validity of the following argument form:

$\sim p \leftrightarrow q$
$q \to r$
$\sim r$
$\therefore\ p$

1.	$\sim p \leftrightarrow q$	Premise
2.	$q \to r$	Premise
3.	$\sim r$	Premise
4.	$\sim q$	2, 3, Modus Tollens
5.	$(\sim p \to q) \wedge (q \to \sim p)$	1, Biconditional as and of conditionals
6.	$\sim p \to q$	5, Specialization
7.	$\sim\sim p$	4, 6, Modus Tollens
8.	$\therefore\ p$	7, Double negative law

Example: Verify the validity of the following argument form:

$$\begin{array}{ll} & p \to q \\ & q \to (r \wedge s) \\ & \sim r \vee (\sim y \vee u) \\ & p \wedge y \\ \therefore & u \end{array}$$

1.	$p \to q$	Premise
2.	$q \to (r \wedge s)$	Premise
3.	$\sim r \vee (\sim y \vee u)$	Premise
4.	$p \wedge y$	Premise
5.	p	4, Specialization
6.	q	1, 5, Modus Ponens
7.	$r \wedge s$	2, 6, Modus Ponens
8.	r	7, Specialization
9.	$\sim\sim r$	8, Double negative law
10.	$\sim y \vee u$	3, 9, Elimination
11.	y	4, Specialization
12.	$\sim\sim y$	11, Double negative law
13.$\therefore$	u	10, 12, Elimination

Hypothetical Reasoning: an additional rule of inference [Grimaldi Chap 2.3]

$$\begin{array}{rl} & p_1 \\ & p_2 \\ & \vdots \\ & p_n \\ \therefore & q \to r \end{array} \qquad \text{is valid} \qquad \text{if and only if} \qquad \begin{array}{rl} & p_1 \\ & p_2 \\ & \vdots \\ & p_n \\ & q \\ \therefore & r \end{array} \qquad \text{is valid.}$$

To prove that **if** $p_1, p_2, \ldots, p_n$ are all true **then** $q \to r$ is true,

we prove that **if** $p_1, p_2, \ldots, p_n, q$ are all true **then** r is true.

Assume that q is true and deduce that r is true **under that assumption**.

Then $q \to r$ is true **without the assumption**.

In a proof, write:

1.	p_1	
2.	p_2	
	$\vdots$	
n.	p_n	
	$\vdots$	
j.	$\quad q$	Assume for Hypothetical Reasoning
	$\quad \vdots$	
k.	$\quad r$	
	$q \to r$	j-k, Hypothetical Reasoning
	$\vdots$	

Example: Verify the validity of the following argument form:

$u \to r$
$r \wedge s \to p \vee y$
$\sim y$
$q \to u \wedge s$
$\therefore\ q \to p$

1.	$u \to r$	Premise
2.	$r \wedge s \to p \vee y$	Premise
3.	$\sim y$	Premise
4.	$q \to u \wedge s$	Premise
5.	q	Assume for Hypothetical Reasoning
6.	$u \wedge s$	4, 5, Modus Ponens
7.	u	6, Specialization
8.	r	1, 7, Modus Ponens
9.	s	6, Specialization
10.	$r \wedge s$	8, 9, Conjunction
11.	$p \vee y$	2, 10, Modus Ponens
12.	p	3,11, Elimination
13.$\therefore$	$q \to p$	5-12, Hypothetical Reasoning

Example: Knights and Knaves

On the island of knights and knaves, every inhabitant is a knight or a knave, and knights always tell the truth and knaves always lie.

Suppose A says: "If I am a knight then so is B."

Is there enough information to determine what A and B are?
knights, knaves, or one of each?

Answer: Yes, A and B must both be knights.

The argument is:

A says: "If I am a knight then so is B."
Therefore A and B are both knights.

or, equivalently,

A is a knight iff the statement "If A is a knight then B is a knight" is true.
$\therefore$ A is a knight and B is a knight.

or, equivalently,

$a =$ "A is a knight."
$b =$ "B is a knight."

$$\begin{array}{ll} & a \leftrightarrow (a \to b) \\ \therefore & a \wedge b \end{array}$$

Verify that the argument form is valid:

$$\begin{array}{ll} & a \leftrightarrow (a \to b) \\ \therefore & a \wedge b \end{array}$$

1.	$a \leftrightarrow (a \to b)$	Premise
2.	$(a \to (a \to b)) \wedge ((a \to b) \to a)$	1, Biconditional as and of conditionals
3.	$\quad \sim a$	Assume for Hypothetical Reasoning
4.	$\quad \sim a \vee b$	3, Generalization
5.	$\quad a \to b$	4, If-then as or
6.	$\quad (a \to b) \to a$	2, Specialization
7.	$\quad a$	5, 6, Modus Ponens
8.	$\quad a \wedge \sim a$	3, 7, Conjunction
9.	$\quad \mathbf{c}$	8, Negation laws
10.	$\sim a \to \mathbf{c}$	3-9, Hypothetical Reasoning
11.	a	10, Contradiction rule
12.	$a \to (a \to b)$	2, Specialization
13.	$a \to b$	11, 12, Modus Ponens
14.	b	11, 13, Modus Ponens
15. $\therefore$	$a \wedge b$	11, 14, Conjunction

Another proof of the validity of
$$\begin{array}{rl} & a \leftrightarrow (a \to b) \\ \therefore & a \wedge b \end{array}$$

1.	$a \leftrightarrow (a \to b)$	Premise
2.	$(a \to (a \to b)) \wedge ((a \to b) \to a)$	1, Biconditional as and of conditionals
3.	$\quad a$	Assume for Hypothetical Reasoning
4.	$\quad a \to (a \to b)$	2, Specialization
5.	$\quad a \to b$	3, 4, Modus Ponens
6.	$\quad b$	3, 5, Modus Ponens
7.	$a \to b$	3-7, Hypothetical Reasoning
8.	$(a \to b) \to a$	2, Specialization
9.	a	7, 8, Modus Ponens
10.	b	7, 9, Modus Ponens
11.$\therefore$	$a \wedge b$	9, 10, Conjunction

In fact, $a \leftrightarrow (a \rightarrow b) \equiv a \wedge b$, which implies the validity of both of the following argument forms:

$$\begin{array}{rl} & a \leftrightarrow (a \rightarrow b) \\ \therefore & a \wedge b \end{array} \qquad\qquad \begin{array}{rl} & a \wedge b \\ \therefore & a \leftrightarrow (a \rightarrow b) \end{array}$$

Exercise: Verify the logical equivalence $a \leftrightarrow (a \rightarrow b) \equiv a \wedge b$

- using logical equivalences from the handout
- using a truth table

CMPUT 272 (Stewart) University of Alberta **Lecture 2**

Reading: Epp 2.1, 2.2

$$p \to q$$

antecedent - consequent
hypothesis - conclusion
LHS - RHS

Truth tables for some statement forms involving →

			inverse of $p \to q$	converse of $p \to q$	contra-positive of $p \to q$	negation of $p \to q$		
p	q	$p \to q$	$\sim p \to \sim q$	$q \to p$	$\sim q \to \sim p$	$\sim (p \to q)$	$\sim p \vee q$	$p \wedge \sim q$
F	F							
F	T							
T	F							
T	T							

Definition. A *truth assignment* of a statement form is a specification of the truth values of the variables.

- A *satisfying* truth assignment is one under which the statement form evaluates to true.
- A *falsifying* truth assignment is one under which the statement form evaluates to false.

Definition. A statement form is

- *satisfiable* if it has a satisfying truth assignment;
- *falsifiable* if it has a falsifying truth assignment;
- a *tautology*, denoted by $\mathbf{t}$, if it is true under every truth assignment;
- a *contradiciton*, denoted by $\mathbf{c}$, if it is false under every truth assignment.

Definition. For statement forms r and s:

- r is *logically equivalent* to s, denoted $r \equiv s$, if r and s have the same truth value under every truth assignment.
- r *logically implies* s if every truth assignment that makes r true also makes s true.

Note: $r \equiv s$ if and only if $r \leftrightarrow s$ is a tautology.
Note: r logically implies s if and only if $r \to s$ is a tautology.
Note: $r \equiv s$ if and only if r logically implies s and s logically implies r.

To verify, use truth tables.

Another way to verify tautologies, contradictions, and logical equivalences: use the following established logical equivalences : the laws of logic

Theorem 2.1.1 Logical Equivalences involving $\wedge$, $\vee$, and $\sim$ [Epp]
Given any statement variables p, q, and r, a tautology $\mathbf{t}$ and a contradiction $\mathbf{c}$, the following logical equivalences hold.

1. *Commutative laws:*	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2. *Associative laws*	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3. *Distributive laws:*	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4. *Identity laws:*	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
5. *Negation laws:*	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
6. *Double negative law:*	$\sim (\sim p) \equiv p$	
7. *Idempotent laws:*	$p \wedge p \equiv p$	$p \vee p \equiv p$
8. *Universal bound laws:*	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
9. *De Morgan's laws:*	$\sim (p \wedge q) \equiv \sim p \vee \sim q$	$\sim (p \vee q) \equiv \sim p \wedge \sim q$
10. *Absorption laws:*	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11. *Negations of* $\mathbf{t}$ *and* $\mathbf{c}$*:*	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

Logical equivalences involving $\rightarrow$ [Epp Chapter 2.2]

12. *Division into cases:*	$p \vee q \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$
13. *If-then as or:*	$p \rightarrow q \ \equiv \sim p \vee q$
14. *Negation of conditional:*	$\sim (p \rightarrow q) \equiv \ p \wedge \sim q$
15. *Contrapositive of conditional:*	$p \rightarrow q \ \equiv \sim q \rightarrow \sim p$

Logical equivalences involving $\leftrightarrow$

16. *Biconditional as and of conditionals:*	$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
17. *Biconditional as or of ands:*	$p \leftrightarrow q \equiv (p \wedge q) \vee (\sim p \wedge \sim q)$

Simplifying statement forms / verifying logical equivalences

Example. Verify the logical equivalence $\sim(\sim p \wedge q) \wedge (p \vee q) \equiv p$

$\sim(\sim p \wedge q) \wedge (p \vee q) \equiv (\sim\sim p \vee \sim q) \wedge (p \vee q)$ by DeMorgan's law

$\equiv (p \vee \sim q) \wedge (p \vee q)$ by the double negative law

$\equiv p \vee (\sim q \wedge q)$ by the distributive law

$\equiv p \vee (q \wedge \sim q)$ by the commutative law

$\equiv p \vee \mathbf{c}$ by the negation law

$\equiv p$ by the identity law

Example. Verify the logical equivalence $p \to (q \to r) \equiv (p \wedge q) \to r$

$p \to (q \to r) \equiv \sim p \vee (q \to r)$ by if-then as or

$\equiv \sim p \vee (\sim q \vee r)$ by if-then as or

$\equiv (\sim p \vee \sim q) \vee r$ by the associative law

$\equiv \sim(p \wedge q) \vee r$ by DeMorgan's law

$\equiv (p \wedge q) \to r$ by if-then as or

CMPUT 272 (Stewart) University of Alberta **Lecture 1**

Reading: Epp 2.1, 2.2

Symbolic / Formal Logic : reasoning about statements

Definition. A *statement* (or *proposition*) is a sentence that is true or false.

Examples: The earth is a sphere.
$3 < 2$
The earth is a sphere or $3 < 2$.
The earth is not a sphere and $3 < 2$.

The last two examples are *compound statements*: made up of simpler ones.

Whether a compound statement is true or false depends on whether the simpler statements are true or false, and how they are combined.

A system of formal logic consists of:

- a language of symbolic statement forms, and
- rules for deducing symbolic statement forms from other symbolic statement forms.

Logic is the theoretical basis for:

- reasoning: constructing and analyzing arguments
- many areas of computer science including:
  - digital logic circuit design
  - relational database theory
  - automata theory and computability
  - artificial intelligence

Propositional logic: the logic of compound statements

The symbolic form of a simple statement is a statement variable, eg.

$p =$ "The earth is a sphere."
$q =$ "$3 < 2$"

To construct the symbolic form of a compound statement, we combine the variables of its component statements with logical connectives.

The logical connectives (operators) are:

$\wedge$	and	
$\vee$	or	
$\sim$	not	in some textbooks the symbol $\neg$ is used for not
$\rightarrow$	if-then	sometimes called implies
$\leftrightarrow$	if-and-only-if	

Example:

If
$p =$ "The earth is a sphere."
and
$q =$ "$3 < 2$"
then

"The earth is not a sphere and $3 < 2$."

can be written in symbolic form as

$\sim p \wedge q$

Definition. A *statement form* is an expression made up of statement variables, logical constants, logical connectives, and parentheses, as follows:

1. Each statement variable is a statement form.
2. Each logical constant (**t**, **c**) is a statement form.
3. If p is a statement form then so is $\sim p$. *negation*
4. If p and q are statement forms then so are

   $(p \wedge q)$ *conjunction*
   $(p \vee q)$ *disjunction*
   $(p \rightarrow q)$ *implication / conditional*
   $(p \leftrightarrow q)$ *equivalence / biconditional*

5. All statement forms of propositional logic are obtained as above.

Example: Show that this is a statement form:

$$(\ (\ p \quad \wedge \quad q\ ) \quad \vee \quad (\ \sim r \quad \wedge \quad (\ r \quad \leftrightarrow \quad p\ )\ )\ )$$

The *main connective* of a statement form is

- the last connective added in a construction of the statement form according to the definition.

Each statement form has a *truth value*, T (true) or F (false), which depends on the truth values of the logical constants, the meanings of the logical connectives ($\sim$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$), and the truth values of the variables.

- The truth value of the logical constant **t** is T.
- The truth value of the logical constant **c** is F.
- The truth values of all other statement forms depend on
  - the definitions of the logical connectives, and
  - the truth values of the variables.

Each logical connective is defined by a *truth table*:

not – negation

p	$\sim p$
F	T
T	F

and – conjunction

p	q	$(p \wedge q)$
F	F	F
F	T	F
T	F	F
T	T	T

or – disjunction

p	q	$(p \vee q)$
F	F	F
F	T	T
T	F	T
T	T	T

if-then / implies – conditional / implication

p	q	$(p \rightarrow q)$
F	F	T
F	T	T
T	F	F
T	T	T

if and only if / iff – biconditional / equivalence

p	q	$(p \leftrightarrow q)$
F	F	T
F	T	F
T	F	F
T	T	T

The truth value of a compound statement form can be evaluated by substituting in the truth values of the logical constants and statement variables, and combining them using the truth tables for the logical connectives.

Example:

Suppose the statement variables p, q, and r have the following truth values:

$$p \text{ is } T,\ q \text{ is } F, \text{ and } r \text{ is } T.$$

What is the truth value of the following statement form?

$$(\quad (\quad p \quad \wedge \quad q \quad) \quad \vee \quad (\quad \sim r \quad \wedge \quad (\quad r \quad \leftrightarrow \quad p \quad) \quad) \quad)$$

The *main connective* of a statement form is

- the last connective added in a construction of the (fully parenthesized) statement form according to the definition, or equivalently,
- the last connective to be evaluated when determining the truth value of the statement form.

From now on, we will allow ourselves to omit unnecessary parentheses.
But we must use enough parentheses to avoid ambiguity!
When in doubt, include parentheses.

We adopt the following *order of evaluation* of the connectives.

$\sim$	evaluate first
$\wedge$, $\vee$	
$\rightarrow$, $\leftrightarrow$	evaluate last

To express the truth values of a statement form under *all possible truth values of the statement variables*, use a *truth table*.

Example.

p	q	r	$p \wedge q$	$\sim r$	$r \leftrightarrow p$	$\sim r \wedge (r \leftrightarrow p)$	$(p \wedge q) \vee (\sim r \wedge (r \leftrightarrow p))$
F	F	F					
F	F	T					
F	T	F					
F	T	T					
T	F	F					
T	F	T					
T	T	F					
T	T	T					

If a statement form has k variables, then its truth table has 2^k rows.

Logical connectives and natural language

Statement form	A few corresponding English phrases
$\sim p$	not
$p \vee q$	inclusive or
$p \wedge q$	and, but, in addition to, as well as
$p \to q$	if p then q q if p p only if q p is a sufficient condition for q q is a necessary condition for p
$p \leftrightarrow q$	p if and only if q p is a necessary and sufficient condition for q

Examples:

- If you get 90% then you pass the course.
- If the candy bar is labelled peanut-free then it is peanut-free.
- If 0=1 then 5=7.
- x is even or x is odd but not both.
- $x < 3$ if $x < 2$.
- $1 < y < 2$
- $n > 1$ is a sufficient condition for $n > 0$.
- $n > 1$ is a necessary condition for $n > 0$.
- I don't eat cookies unless I have milk.

$\sim q \to p$	p unless q p if not q if not q then p