Discrete Structures for Computer Science

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU CSci 341

Subsection 1

A Proof Primer

Statements and Negation

- A **proposition** or **sentence** is a statement that is either true or false.
- Example: The following are propositions:
  - The number 3 is odd.
  - It is now 3:00pm ET.

  "Painting x is beautiful" is not a proposition.
- Given a proposition S, the **negation** of S, denoted $\neg S$ and read "**not** S", is a proposition whose truth value is the opposite of that of S.
- Thus, the truth value of $\neg S$ is given in terms of the truth value of S by the following *truth table*:

S	$\neg S$
T	F
F	T

- The negation of "x is odd" is "not (x is odd)", which we write more naturally in English as "x is not odd".

Conjunction and Disjunction

- Let A and B be propositions.
- The **conjunction** of A and B, denoted $A \wedge B$ and read "A **and** B", is a proposition which is true when A and B are both true.
- Thus, the truth value of $A \wedge B$ in terms of those of A and B is given by the truth table on the left:

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

- The **disjunction** of A and B, denoted $A \vee B$ and read "A **or** B", is a proposition which is true when at least one of A or B is true.
- Thus, the truth value of $A \vee B$ in terms of those of A and B is given by the truth table on the right.

De Morgan's Laws

- Two propositions A and B are **equivalent**, written $A \equiv B$, if their truth tables are identical.
- Examples:

A	B	$A \wedge B$	$A \vee B$	$\neg A$	$\neg B$	$\neg(A \wedge B)$	$\neg A \vee \neg B$	$\neg(A \vee B)$	$\neg A \wedge \neg B$
T	T	T	T	F	F	F	F	F	F
T	F	F	T	F	T	T	T	F	F
F	T	F	T	T	F	T	T	F	F
F	F	F	F	T	T	T	T	T	T

- We showed:
  - $\neg(A \wedge B) \equiv \neg A \vee \neg B$
    The negation of a conjunction is a disjunction of negations.
  - $\neg(A \vee B) \equiv \neg A \wedge \neg B$
    The negation of a disjunction is a conjunction of negations.
- Example: "It is not the case that x is odd or y is odd" is equivalent to "x is not odd and y is not odd".

Conditional

- Let A and B be propositions.
- The **conditional**, written $A \to B$ and read "**If** A **then** B" or "A **implies** B", is a proposition that is true unless A is true and B is false.
- Thus, the truth value of $A \to B$ in terms of those of A and B is given by the truth table

A	B	$A \to B$
T	T	T
T	F	F
F	T	T
F	F	T

- In $A \to B$, the proposition
  - A is called the **hypothesis** or the **antecedent** of the conditional.
  - B is called the **conclusion** or **consequent** of the conditional.
- "If A then B" can also be read as:
  - "A is sufficient for B";
  - "B is necessary for A".

More on the Conditional

- Example: Evaluate the following conditionals:
  (a) "If Peru is in North America then $1 = 2$" True
  (b) "If $7 = 7$ then Chile is in Europe" False
  (c) "If $1 = 2$ then $39 = 12$" True
  (d) "If $1 = 2$ then $2 + 2 = 4$" True
- We say a conditional is **vacuously true** if its hypothesis is false.
  The conditionals (a), (c) and (d) above are vacuously true.
- We say that a conditional is **trivially true** if its conclusion is true.
  The conditional (d) above is trivially true.

Converse

- Let A and B be propositions.
- The conditional $B \to A$ is called the **converse** of the conditional $A \to B$.
- The following truth table shows that $(A \to B) \not\equiv (B \to A)$:

A	B	$A \to B$	$B \to A$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

- Consider the following conditionals, which are converses of each other:
  - "If x and y are odd then $x + y$ is even"
  - "If $x + y$ is even then x and y are odd"

  The first is true in general, but the second is not.

Contrapositive

- Let A and B be propositions.
- The conditional $\neg B \to \neg A$ is called the **contrapositive** of the conditional $A \to B$.
- The following truth table shows that $(A \to B) \equiv (\neg B \to \neg A)$:

A	B	$A \to B$	$\neg B$	$\neg A$	$\neg B \to \neg A$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

- Example: Consider the two contrapositive statements:
  - "If x and y are odd then $x + y$ is even";
  - "If $x + y$ is not even then not both x and y are odd".

  These are both true statements.

Biconditional

- Let A and B be propositions.
- The **biconditional**, written $A \leftrightarrow B$ and read "A **if and only if** B" (abbreviated "A **iff** B"), is a proposition that is true when A and B assume the same truth value.
- Thus, the truth value of $A \leftrightarrow B$ in terms of those of A and B is given by the truth table

A	B	$A \leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

- Sometimes "A iff B" is read "A is necessary and sufficient for B".
- Example: Consider the statement "x is even iff $x + 2$ is even".

  This is a true statement.

Integers and Divisibility

- The **integers** are the numbers

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

- For integers m and n, we say that m **divides** n, denoted $m \mid n$, if $m \neq 0$ and $n = m \cdot k$, for some integer k.
- The proposition "m divides n" can also be expressed by saying that "m **is a divisor of** n" or "n **is divisible by** m".
- Example: The number 9 has six divisors: $\pm 1, \pm 3$ and ± 9.
- If m does not divide n, we write $m \nmid n$.
- Example: We have the following:

$$3 \mid 12, \qquad 6 \mid 12, \qquad 5 \nmid 12.$$

Properties of Divisibility and Proofs

- The following two basic properties of divisibility hold:
  - (a) If $d \mid m$ and $m \mid n$, then $d \mid n$.
  - (b) If $d \mid m$ and $d \mid n$, then $d \mid (am + bn)$, for all integers a and b.
- Examples:
  - (a) $3 \mid 12$ and $12 \mid 72$. Therefore $3 \mid 72$.
  - (b) $7 \mid 14$ and $7 \mid 21$. Therefore $7 \mid (2 \cdot 14 + 3 \cdot 21) = 91$.
- We may prove (a) and (b) relatively easily:
  - (a) Assume $d \mid m$ and $m \mid n$. Then, there exist integers k and ℓ, such that $m = dk$ and $n = m\ell$. So, we have $n = m\ell = (dk)\ell = d(k\ell)$. This shows that $d \mid n$.
  - (b) Assume that $d \mid m$ and $d \mid n$. Then, there exist integers k and ℓ, such that $m = dk$ and $n = d\ell$. So we have

$$am + bn = a(dk) + b(d\ell) = d(ak + b\ell).$$

Therefore, we get $d \mid (am + bn)$.

Prime Numbers

- Any *positive* integer $n > 1$ has at least two *positive* divisors: 1 and n.
- A positive integer p is said to be **prime** if $p > 1$ and its only positive divisors are 1 and p.
- Example:
  - 2 is prime.
  - 9 is not prime.
  - The first eight prime numbers are:

$$2, 3, 5, 7, 11, 13, 17, 19.$$

Decomposition into Product of Primes

- Every integer greater than 1 is a product of primes.
- This is proven by induction.
  - **Basis of the Induction:** 2 is a prime.
  - **Induction Hypothesis:** Suppose that every integer k, with $1 < k < n$ is a product of primes.
  - **Induction Step:** We must prove that $n > 1$ is a product of primes.
    - If n is prime, then n is a product of primes $n = n$.
    - If n is not prime, there exist $1 < k, \ell < n$, such that $n = k\ell$. By the Induction Hypothesis, each of k, ℓ is a product of primes, say

$$k = p_1 \cdots p_i \quad \text{and} \quad \ell = q_1 \ldots q_j.$$

But then

$$n = k\ell = p_1 \cdots p_i q_1 \cdots q_j$$

is also a product of primes.

Infinity of Primes

- There are infinitely many prime numbers.
- This is Euclid's famous proof by contradiction:

  Suppose there exist only finitely many primes, say $p_1, p_2, \ldots, p_n$. Consider the number

  $$k = p_1 p_2 \cdots p_n + 1.$$

  Since it is larger than all of $p_1, \ldots, p_n$, it cannot be a prime.

  By the Decomposition into Primes, it is a product of primes, say $k = p_{i_1} \cdots p_{i_\ell}$. Now we have

  $$p_1 p_2 \cdots p_n + 1 = p_{i_1} \cdots p_{i_\ell}.$$

  This gives $1 = p_{i_1} \cdots p_{i_\ell} - p_1 p_2 \cdots p_n$. But the right hand side is divisible by p_{i_1} (since it is a prime and, therefore, among the $p_1, \ldots, p_n$). Thus, $p_{i_1} \mid 1$, a contradiction.

Proof by Example and by Counterexample

- A Proof by Example can be used to show the claimed existence of a certain object.
- Example: "There exists a prime number between 80 and 88" is true.

  The number 83 is a prime.
- A Proof by Counterexample can be used to disprove (show the falsity) of a given statement.
- Example: "Every prime number is odd" is false.

  2 is a prime number and it is even.

Proof by Exhaustive Checking

- Proof by Exhaustive Checking is checking of all possibilities, showing that each satisfies the claimed conclusion.
- Example: Show that the sum of any two of the numbers 1, 3 and 5 is an even number.

  All sums

  $$1+1,\ 1+3,\ 1+5,\ 3+3,\ 3+5,\ 5+5,$$

  are even numbers.
- Exhaustive checking cannot be done if there are infinitely many things to check.
- Exhaustive checking is also impracticable even in the finite case, if the number of things that need to be checked is large.

Proof Using Variables

- Using variables is a convenient way to overcome the difficulty of having to check an infinite number of cases.
- Example: Show that the sum of any two odd integers is even.

  Let m and n be two odd integers.

  Then, there exist integers k and ℓ, such that

  $$m = 2k + 1 \quad \text{and} \quad n = 2\ell + 1.$$

  Therefore, we get

  $$m + n = (2k + 1) + (2\ell + 1) = 2k + 2\ell + 2 = 2(k + \ell + 1).$$

  Thus, $m + n$ is even.

Direct Proofs

- A Direct Proof of a statement of the form $A \to B$ (If A then B) starts with A and inserts intermediate steps in a sequence of valid logical implications that lead from A to B:
$$A \to C_1 \to C_2 \to \cdots \to B.$$
- Sometimes, it is useful to work at both sides and close the chain in the middle:
$$A \to C_1 \to C_2 \to \cdots \to C_{n-2} \to C_{n-1} \to B.$$
- Example: Prove that if x is odd and y is even, then $x^2 + 3y$ is odd.
Suppose that x is odd and y is even.
Then there exist integers k and ℓ, such that $x = 2k + 1$ and $y = 2\ell$.
Then, we have
$$\begin{aligned} x^2 + 3y &= (2k+1)^2 + 3(2\ell) = 4k^2 + 4k + 1 + 6\ell \\ &= 2(2k^2 + 2k + 3\ell) + 1. \end{aligned}$$
This shows that $x^2 + 3y$ is odd.

Indirect Proofs: Proof by Contraposition

- We saw that $A \to B$ and $\neg B \to \neg A$ are equivalent propositions.
- A Proof by Contraposition of $A \to B$ is a direct proof of $\neg B \to \neg A$:

$$\neg B \to C_1 \to C_2 \to \cdots \to \neg A.$$

- Example: Let x be an an integer.

  Show that if x^2 is even, then x is even.

  We prove the contrapositive: "If x is odd, then x^2 is odd."

  Suppose x is odd.

  Then, there exists an integer k, such that $x = 2k + 1$.

  Thus, $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

  So x^2 is odd.

Indirect Proofs: Proof by Contradiction

- A Proof by Contradiction of A assumes $\neg A$ and shows that it leads to a contradiction (an obviously false statement).
- Example: Show that there are no integers a and b, such that $4a + 6b = 1$.

  We proceed by contradiction.

  Assume that there exist integers a and b, such that

$$4a + 6b = 1.$$

  Then, we get that $2a + 3b = \frac{1}{2}$.

  This is a contradiction, since $2a + 3b$ is an integer, but $\frac{1}{2}$ is not an integer.

  So there cannot exist integers a and b, such that $4a + 6b = 1$.

Indirect Proofs: Proof by Contradiction (Cont'd)

- A Proof by Contradiction of $A \to B$ assumes $\neg(A \to B) \equiv (A \wedge \neg B)$ and shows that it leads to a contradiction (an obviously false statement).
- Example: Show that if $n^3 + 5$ is odd, then n is even.

  We prove the statement by contradiction.

  Assume $n^3 + 5$ is odd and n is odd.

  Then, there exist integers k and ℓ such that $n^3 + 5 = 2k + 1$ and $n = 2\ell + 1$.

  Thus, we get

$$\begin{aligned} 5 &= 2k + 1 - n^3 = 2k + 1 - (2\ell + 1)^3 \\ &= 2k + 1 - (8\ell^3 + 12\ell^2 + 6\ell + 1) \\ &= 2(k - 4\ell^3 - 6\ell^2 - 3\ell). \end{aligned}$$

  This is a contradiction, since the right-hand side is an even integer.

"If and only if" Proofs

- To prove $A \leftrightarrow B$, we must show:
  - $A \rightarrow B$ **and**
  - $B \rightarrow A$.
- Example: Show that x is even if and only if x^2 is even.
  - We first show "if x is even, then x^2 is even using a direct proof.
    Suppose x is even.
    Then, there exists integer k, such that $x = 2k$.
    Thus, we get $x^2 = (2k)^2 = 4k^2 = 2(2k^2)$.
    Therefore x^2 is even.
  - Next we show "If x^2 is even, then x is even" by contraposition.
    That is, we show "If x is odd, then x^2 is odd".
    Suppose that x is odd.
    Then, there exists an integer k, such that $x = 2k + 1$.
    Thus, we get $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.
    Therefore x^2 is odd.

Subsection 2

Sets

Sets and Membership

- A **set** is a collection of things, called its **elements** or **members**.
- A set is also called a **collection** or a **family**.
- A set **contains** its elements.
- An element **belongs to**, **is a member of** or **is in** the set.
- If an element x is in a set S, we write

$$x \in S.$$

- If x is not an element of a set S, we write $x \notin S$.
- The notation $x, y \in S$, means $x \in S$ and $y \in S$.

Notation for Sets

- One way to define a set is by explicitly listing its elements (note how braces and commas are used, and learn the notation!).
- Example: The set S whose elements are the letters x, y and z is denoted by
$$S = \{x, y, z\}.$$
- Example: The set $S = \{x, \{x, y\}\}$ has two elements:
  - The letter x;
  - The set $\{x, y\}$, with elements the letters x, y.
- Sometimes ellipsis, $\ldots$, are used to informally denote a sequence of elements.
- Example: The set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ may be denoted by $\{1, 2, 3, \ldots, 12\}$ or by $\{1, 2, 3, \ldots, 11, 12\}$.
- Use this notation with caution, only when the meaning of the ellipses is clear!

Empty Set and Singleton Sets

- The set with no elements in it is called the **empty set** or the **null set**.
- The empty set is denoted most commonly by $\emptyset$ or, more rarely, by $\{\}$.
- A set with one element is called a **singleton**.
- Example: The following sets are singletons:

$$\{a\}, \quad \{z\}, \quad \{\{x, y\}\}, \quad \{\emptyset\}.$$

  - $\{a\}$ contains only the letter a;
  - $\{z\}$ contains only the letter z;
  - $\{\{x, y\}\}$ contains only one element, the set $\{x, y\}$;
  - $\{\emptyset\}$ contain only one element, the empty set.

Equality of Sets

- Two sets A and B are **equal**, written $A = B$, if:
  - Each element of A is an element of B; and
  - Each element of B is an element of A.
- We can use equality to demonstrate two important properties of sets:
  - There is no particular order or arrangement of the elements.
  - There are no redundant elements (repetitions do not count).
- Example: The set whose elements are g, h and u can be represented in many ways, e.g.,

$$\{u, g, h\} = \{h, u, g\} = \{h, u, g, h\} = \{u, g, h, u, g\}.$$

  So there are many ways to represent the same set.
- If the sets A and B are not equal, we write $A \neq B$.
- Example: $\{a, b, c\} \neq \{a, b\}$ because $c \in \{a, b, c\}$, but $c \notin \{a, b\}$.
- Example: $\{a\} \neq \emptyset$ because the empty set does not contain a.

Finite versus Infinite Sets

- Suppose we start counting the elements of a set S.
- If $S = \emptyset$, then we don't need to start, because there are no elements to count.
- If $S \neq \emptyset$, and the counting stops at a finite positive natural number when all elements of S have been counted, then we say that S is a **finite set**.
- If the counting never stops, then S is an **infinite set**.

Familiar Sets of Numbers and Notation

- Set of **natural numbers**:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\};$$

- Set of **integers**:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\};$$

- Set of **rational numbers**:

$$\begin{array}{lcl} \mathbb{Q} & = & \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\} \\ & = & \{x \in \mathbb{R} : x \text{ has a terminating} \\ & & \text{or repeating decimal representation}\}; \end{array}$$

- Set of **real numbers**: $\mathbb{R}$.

Sets Defined by Properties

- Ay set can be defined by stating a property that the elements of the set must satisfy.
- If P is some property, then there is a set S (with elements in a universe U) whose elements have property P, and we write
$$S = \{x \in U : x \text{ has property } P\},$$
read as "S is the set of all $x \in U$, such that x has property P".
- Example: $\text{Odd} = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$ of odd integers can be defined by
$$\text{Odd} = \{x \in \mathbb{Z} : x = 2k + 1 \text{ for some } k \in \mathbb{Z}\}.$$
- Example: Similarly, the set $\{1, 2, \ldots, 12\}$ can be defined by writing
$$\{x \in \mathbb{N} : 1 \leq x \leq 12\}.$$

Subsets

- A set A is called a **subset** of a set B, written $A \subseteq B$, if every element of A is also an element of B.
- Example: $\{a, b\} \subseteq \{a, b, c\}$, $\{0, 1, 2\} \subseteq \mathbb{N}$, and $\mathbb{N} \subseteq \mathbb{Z}$.
- Every set A is a subset of itself: $A \subseteq A$.
- The empty set is a subset of any set A: $\emptyset \subseteq A$.
- A set A is called a **proper subset** of B, written $A \subset B$, if:
  - $A \subseteq B$; and
  - There is some element in B that does not belong to A.
- Example: $\{a, b\} \subset \{a, b, c\}$.
- Example: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.
- If A is not a subset of B, we sometimes write $A \nsubseteq B$.
- Example: $\{a, b\} \nsubseteq \{a, c\}$ and $\{-1, -2\} \nsubseteq \mathbb{N}$.

Membership versus Subsets

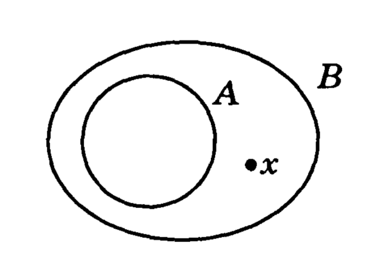
- Consider the set $A = \{a, b, c\}$.
  We have
  - $\{a\} \subseteq A$;
  - $a \in A$;
  - $\{a\} \notin A$;
  - $a \not\subseteq A$.
- Consider $A = \{a, \{b\}\}$.
  We have:
  - $a \in A$;
  - $\{b\} \in A$;
  - $\{a\} \subseteq A$;
  - $\{\{b\}\} \subseteq A$;
  - $b \notin A$;
  - $\{b\} \not\subseteq A$.

Power Sets

- The **power set** of a set S, denoted by $\mathcal{P}(S)$ or power(S), is the collection of all subsets of S.
- Example:
  - $\mathcal{P}(\emptyset) = \{\emptyset\}$;
  - $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$;
  - $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$;
  - $\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Venn Diagrams

- A **Venn diagram** consists of one or more closed curves in which the interior of each curve represents a set.
- Example: The Venn diagram below reflects the facts that:
  - A is a proper subset of B;
  - x is an element of B that does not occur in A.



Proof Techniques

- Recall that two sets A and B are **equal** if:
  - Every element of A belongs to B;
  - Every element of B belongs to A.
- Rephrasing the definition, we get that

$$A = B \quad \text{iff} \quad (A \subseteq B \quad \text{and} \quad B \subseteq A).$$

- In dealing with sets we use the following proof techniques:
  - To prove that $A \subseteq B$:

    Let $x \in A$. Show that $x \in B$.
  - To prove that $A \nsubseteq B$:

    Find an element $x \in A$ such that $x \notin B$.
  - To show that $A = B$:
    - First show that $A \subseteq B$;
    - Then show that $B \subseteq A$.

Example

- Let
$$\begin{array}{rcl} A & = & \{x \in \mathbb{N} : x \text{ is prime and } 42 \leq x \leq 51\}; \\ B & = & \{x : x = 4k + 3 \text{ and } k \in \mathbb{N}\}. \end{array}$$
  Show that $A \subseteq B$.
  Let $x \in A$.
  Then $x = 43$ or $x = 47$.
  - If $x = 43$, then $x = 4 \cdot 10 + 3$. So $x \in B$.
  - If $x = 47$, then $x = 4 \cdot 11 + 3$. So $x \in B$.

  So in either case, $x \in B$.
  We conclude that $A \subseteq B$.

Example

- Suppose that

$$A = \{3k+1 : k \in \mathbb{N}\} \quad \text{and} \quad B = \{4k+1 : k \in \mathbb{N}\}.$$

Show that $A \not\subseteq B$ and $B \not\subseteq A$.

By listing a few elements from each set we can write A and B as follows:

$$\begin{array}{lcl} A & = & \{1,4,7,10,13,\ldots\}; \\ B & = & \{1,5,9,13,17,\ldots\}. \end{array}$$

  - $A \not\subseteq B$: $4 \in A$, but $4 \notin B$.
  - $B \not\subseteq A$: $5 \in B$, but $5 \notin A$.

Example

- Consider the sets

$$\begin{aligned} A &= \{x \in \mathbb{N} : x \text{ is prime and } 12 \leq x \leq 18\}; \\ B &= \{x \in \mathbb{N} : x = 4k+1 \text{ and } k \in \{3,4\}\}. \end{aligned}$$

Show that $A = B$.

We must show that $A \subseteq B$ and $B \subseteq A$.

$A \subseteq B$: Let $x \in A$. Then $x = 13$ or $x = 17$. We have $13 = 4 \cdot 3 + 1$ and $17 = 4 \cdot 4 + 1$. It follows that $x \in B$. We conclude that $A \subseteq B$.

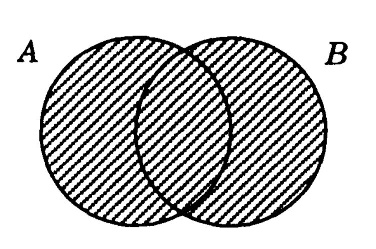
$B \subseteq A$: Let $x \in B$. Then $x = 4 \cdot 3 + 1 = 13$ or $x = 4 \cdot 4 + 1 = 17$. Thus, in either case, x is a prime number between 12 and 18. It follows that $x \in A$. We conclude that $B \subseteq A$.

Union of Sets

- If A and B are sets, then the **union** of A and B, writen $A \cup B$, is the set of all elements that either are in A or in B or in both A and B.
- Formally (recall the connective "or", $\vee$)

$$A \cup B = \{x : x \in A \ \vee \ x \in B\}.$$

- The union of two sets A and B is represented by the shaded regions of the following Venn diagram:



- Example: If $A = \{a, b, c\}$ and $B = \{c, d\}$, then $A \cup B = \{a, b, c, d\}$.

Properties of Union

- The union operation satisfies the following properties:
  - $A \cup \emptyset = A$ (**identity element**)
  - $A \cup B = B \cup A$ (**commutativity**)
  - $A \cup (B \cup C) = (A \cup B) \cup C$ (**associativity**)
  - $A \cup A = A$ (**idempotency**)
  - $A \subseteq B$ iff $A \cup B = B$ (**order**)
- We prove the last property:
  - Suppose, first, that $A \subseteq B$. We must show $A \cup B = B$.

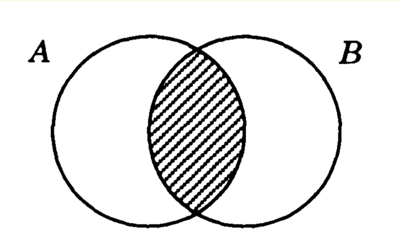
$A \cup B \subseteq B$: Let $x \in A \cup B$. Then $x \in A$ or $x \in B$. If $x \in A$, since $A \subseteq B$, we get $x \in B$. Thus, in either case, $x \in B$. We conclude $A \cup B \subseteq B$.

$B \subseteq A \cup B$: Suppose $x \in B$. Then $x \in A$ or $x \in B$. Thus, $x \in A \cup B$. We conclude that $B \subseteq A \cup B$.

  - Suppose, conversely, that $A \cup B = B$. We must show that $A \subseteq B$. Suppose $x \in A$. Then $x \in A$ or $x \in B$. Thus, $x \in A \cup B$. Since $A \cup B = B$, we get $x \in B$. We conclude $A \subseteq B$.

Intersection of Sets

- If A and B are sets, then the **intersection** of A and B, writen $A \cap B$, is the set of all elements that are in both A and B.
- Formally (recall the connective "and", $\wedge$)
$$A \cap B = \{x : x \in A \ \wedge \ x \in B\}.$$
- The intersection of two sets A and B is represented by the shaded regions of the following Venn diagram:



- Example: If $A = \{a, b, c\}$ and $B = \{c, d\}$, then $A \cap B = \{c\}$.

Properties of Intersection

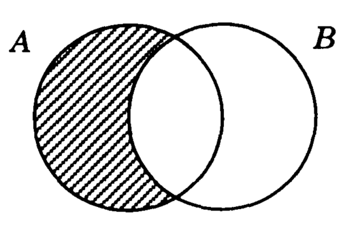
- The intersection operation satisfies the following properties:
  - $A \cap \emptyset = \emptyset$ (**absorption element**)
  - $A \cap B = B \cap A$ (**commutativity**)
  - $A \cap (B \cap C) = (A \cap B) \cap C$ (**associativity**)
  - $A \cap A = A$ (**idempotency**)
  - $A \subseteq B$ iff $A \cap B = A$ (**order**)

Distributive Laws

- The **Distributive Laws** relate Union and Intersection:
  (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ($\cap$ **distributes over** $\cup$);
  (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ ($\cup$ **distributes over** $\cap$).
- We prove part (b).
  $\subseteq$: Suppose $x \in A \cup (B \cap C)$. Then $x \in A$ or $x \in B \cap C$. Thus, $x \in A$ or ($x \in B$ and $x \in C$). So ($x \in A$ or $x \in B$) and ($x \in A$ or $x \in C$). We get $x \in A \cup B$ and $x \in A \cup C$. So $x \in (A \cup B) \cap (A \cup C)$. This shows that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.
  $\supseteq$: Suppose $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$. This implies that ($x \in A$ or $x \in B$) and ($x \in A$ or $x \in C$). So $x \in A$ or ($x \in B$ and $x \in C$). Therefore, $x \in A \cup (B \cap C)$. This proves that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

Difference or Relative Complement

- If A and B are sets, then the **difference** A **minus** B, or the **relative complement of** B **in** A, denoted by $A - B$ or $A \backslash B$, is the set of elements in A that are not in B.
- In formal notation
$$A - B = \{x : x \in A \ \wedge \ x \notin B\}.$$
- The Venn diagram depicting $A - B$ is:



- Example: If $A = \{a, b, c\}$ and $B = \{c, d\}$, then $A - B = \{a, b\}$.

Intersection and Difference

- Let A and B be sets.

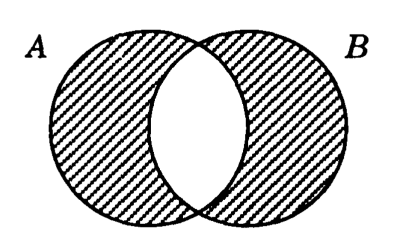
  Show that $A \cap B = A - (A - B)$.

$\subseteq$: Suppose $x \in A \cap B$. Then $x \in A$ and $x \in B$. This implies that $x \in A$ and $x \notin A - B$. So $x \in A - (A - B)$. We conclude that $A \cap B \subseteq A - (A - B)$.

$\supseteq$: Suppose $x \in A - (A - B)$. Then $x \in A$ and $x \notin A - B$. So $x \in A$ and it is not the case that ($x \in A$ and $x \notin B$). Therefore, $x \in A$ and ($x \notin A$ or $x \in B$). So $x \in A$ and $x \in B$. This shows that $x \in A \cap B$. We conclude that $A - (A - B) \subseteq A \cap B$.

Symmetric Difference

- The **symmetric difference** of sets A and B, denoted $A \oplus B$, is the union of $A - B$ with $B - A$.
- The symmetric difference is defined by using the "exclusive or" as follows:
$$A \oplus B = \{x : x \in A \text{ or } x \in B \text{ but not both}\}.$$
- The set $A \oplus B$ is represented by the shaded regions of the following Venn diagram:



Symmetric Difference, Union and Intersection

- Let A and B be sets.

  Show that $A \oplus B = (A \cup B) - (A \cap B)$.

$\subseteq$: Suppose $x \in A \oplus B$.

Then $x \in A$ or $x \in B$, but x is not in both A and B.

Thus, $x \in A \cup B$, but $x \notin A \cap B$.

So $x \in (A \cup B) - (A \cap B)$.

We conclude $A \oplus B \subseteq (A \cup B) - (A \cap B)$.

$\supseteq$: Suppose $x \in (A \cup B) - (A \cap B)$.

The $x \in A \cup B$ and $x \notin A \cap B$.

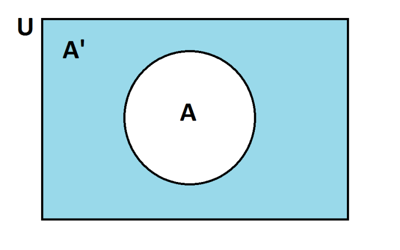
So $x \in A$ or $x \in B$, but x is not in both A and B.

We conclude $x \in A \oplus B$.

So $(A \cup B) - (A \cap B) \subseteq A \oplus B$.

Universe and Complements

- Suppose the discussion always refers to sets that are subsets of a particular set U, called the **universe** of discourse.
- The difference $U - A$ is called the **complement** of A, denoted by A'.
- The Venn diagram pictures the universe U as a rectangle (encompassing "everything under discussion"), and the region corresponding to A' is shaded.



Properties of Complement

- The following are properties of complement:
  - $(A')' = A$;
  - $\emptyset' = U$ and $U' = \emptyset$;
  - $A \cap A' = \emptyset$ and $A \cup A' = U$;
  - $A \subseteq B$ if and only if $B' \subseteq A'$;
  - $(A \cup B)' = A' \cap B'$ and $(A \cap B)' = A' \cup B'$ (**De Morgan's Laws**).
- We prove the first De Morgan Law

$$(A \cup B)' = A' \cap B'.$$

$\subseteq$: Suppose $x \in (A \cup B)'$. Then $x \notin A \cup B$. So $x \notin A$ and $x \notin B$. Thus, $x \in A'$ and $x \in B'$. So $x \in A' \cap B'$. We conclude $(A \cup B)' \subseteq A' \cap B'$.

$\supseteq$: Suppose $x \in A' \cap B'$. Then $x \in A'$ and $x \in B'$. So $x \notin A$ and $x \notin B$. Thus $x \notin A \cup B$. Therefore $x \in (A \cup B)'$. We conclude that $A' \cap B' \subseteq (A \cup B)'$.

Subsection 3

Ordered Structures

Tuples

- A **tuple** is a collection of things, called its **elements**, characterized by the properties:
  - There is an order or arrangement of the elements;
  - There may be multiple occurrences of each element.
- The elements of a tuple are also called **members**, **objects** or **components**.
- We denote a tuple by writing down its elements, separated by commas, and surrounding everything with parentheses (and).
- Example: The tuple $(12, R, 9)$ has three elements:
  - The first element is 12;
  - The second element is the letter R;
  - The third element is 9.

Length of a Tuple

- If a tuple has n elements, we say that its **length** is n, and we call it an ***n*-tuple**.
- Example:
  - The tuple $(8, k, \text{hello})$ is a 3-tuple;
  - $(x_1, \ldots, x_8)$ is an 8-tuple.
- The 0-tuple is denoted by $()$, and we call it the **empty tuple**.
- For $n = 2, 3, 4, 5$, we often use the terms **(ordered) pair**, **triple**, **quadruple**, **quintuple**, respectively.
- Other words used for “tuple” are **vector** and **sequence**.

Equality of Tuples

- Two n-tuples $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ are said to be **equal**, written
$$(x_1, \ldots, x_n) = (y_1, \ldots, y_n),$$
if $x_i = y_i$, for $1 \leq i \leq n$.
- Example: $(3, 7) \neq (7, 3)$.
- Since in tuples order matters and repetitions are allowed, they are different from sets.
- Example:
$$\begin{array}{ll} \text{Sets:} & \{h, u, g, h\} = \{h, u, g\} = \{u, g, h\}. \\ \text{Tuples:} & (h, u, g, h) \neq (h, h, g, u), \quad (h, u, g) \neq (u, g, h). \end{array}$$

Cartesian Product of Sets

- Let A and B be sets.
- The (**Cartesian**) **product** of A and B, denoted $A \times B$, is the set of all pairs with first components from A and second components from B.
- Formally we have

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.$$

- Example: If $A = \{x, y\}$ and $B = \{0, 1\}$, then we have

$$A \times B = \{(x, 0), (x, 1), (y, 0), (y, 1)\}.$$

- If $A = \emptyset$ or $B = \emptyset$, then $A \times B = \emptyset$.
- Example: If $A = \{x, y\}$ and $B = \emptyset$, then $A \times B = \emptyset$.

Cartesian Product of Sets Generalized

- The **product** of n sets $A_1, \ldots, A_n$, written $A_1 \times A_2 \times \cdots \times A_n$, is defined by
$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) : x_i \in A_i, i = 1, 2, \ldots, n\}.$$
- If all the sets A_i in a product are the same set A, then we use the abbreviated notation $A^n = A \times \cdots \times A$.
- With this notation we have the following definitions for the sets A^1 and A^0:
$$\begin{array}{lcl} A^1 & = & \{(a) : a \in A\}; \\ A^0 & = & \{()\}. \end{array}$$
- Example: Let $A = \{a, b, c\}$. Then we have:
$$\begin{array}{lcl} A^0 & = & \{()\}; \\ A^1 & = & \{(a), (b), (c)\}; \\ A^2 & = & \{(a,a), (a,b), (a,c), (b,a), (b,b), (b,c), \\ & & (c,a), (c,b), (c,c)\}. \end{array}$$

Representations

- The components of an n-tuple can be indexed in several different ways depending on context.
- Example: If $t \in A \times B \times C$, then we might represent t in any of the following ways:
  - (t_1, t_2, t_3);
  - $(t(1), t(2), t(3))$;
  - $(t[1], t[2], t[3])$;
  - $(t(A), t(B), t(C))$;
  - $(A(t), B(t), C(t))$.

Arrays, Matrices and Records

- A **1-dimensional array** of size n with elements in the set A can be represented by an n-tuple in the product A^n.

  If $x = (x_1, \ldots, x_n)$, then the component x_i is usually denoted in programming languages by $x[i]$.
- A **2-dimensional array** also called a **matrix** can be thought of as a table of objects that are indexed by rows and columns.

  If x is a matrix with m rows and n columns, we say that x is an $m \times n$ **matrix**, read "m by n matrix".
- Example: If x is a 3×4 matrix, then x can be represented by the following diagram:

$$x = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{34} \end{bmatrix}.$$

Arrays, Matrices and Records (Cont'd)

- We can also represent x as a 3-tuple whose components are 4-tuples as follows:

$$x = ((x_{11}, x_{12}, x_{13}, x_{14}), (x_{21}, x_{22}, x_{23}, x_{24}), (x_{31}, x_{32}, x_{33}, x_{34})).$$

- In programming, the component x_{ij} is usually denoted by $x[i, j]$.
- We can also think of the product $A \times B$ as the set of all **records**, or **structures**, having two fields A and B.
- For a particular record $r = (a, b) \in A \times B$ the components a and b are normally denoted by $r.A$ and $r.B$:
  - The A-component of the record r;
  - The B-component of the record r.

Lists

- A **list** is a finite sequence of zero or more elements that is ordered and where repetitions are allowed.
- To denote lists we use $\langle$ and $\rangle$, with elements separated by commas.
- The **empty list** is $\langle\rangle$.
- The number of elements in a list is called its **length**.
- The difference between tuples and lists is the following:
  - In tuples we can randomly access any component.
  - In the case of lists we can randomly access only two things:
    - The first component of a list, which is called its **head**;
    - The list made up of everything except the first component, which is called its **tail**.
- An important property of lists is the ability to easily **construct** a new list from an element and another list.

Destructors and Constructors for Lists

- Given a list, two operators, called **destructors**, deconstruct the list:
  - head takes a list and produces its head;
  - tail takes a list and produces its tail.
- Example:
  - $\text{head}(\langle x, y, z \rangle) = x$;
  - $\text{tail}(\langle x, y, z \rangle) = \langle y, z \rangle$.
- A **constructor** cons constructs a list, given its parts.
- Example: Given the element x and the list $\langle y, z \rangle$, we can apply cons:

$$\text{cons}(x, \langle y, z \rangle) = \langle x, y, z \rangle.$$

- For every list L, we have

$$\text{cons}(\text{head}(L), \text{tail}(L)) = L..$$

Lists over a Set

- A **list over the set** A is a list whose components are in A.
- We denote the collection of all lists over A by Lists$[A]$.
- Example: If $A = \{a, b, c\}$, then three of the lists in Lists$[A]$ are

$$\langle\rangle, \quad \langle a, a, b\rangle, \quad \langle b, c, a, b, c\rangle.$$

List with Lists as Elements

- There is no restriction on the kind of object that a list can contain.
- It is often useful to represent information in the form of lists whose elements may be lists, and the elements of those lists may be lists, and so on.
- Example: The following list contain lists as components:

List L	head(L)	tail(L)
$\langle a, \langle b\rangle\rangle$	a	$\langle\langle b\rangle\rangle$
$\langle\langle a\rangle, \langle b, a\rangle\rangle$	$\langle a\rangle$	$\langle\langle b, a\rangle\rangle$
$\langle\langle\langle\rangle, a, \langle\rangle\rangle, b, \langle\rangle\rangle$	$\langle\langle\rangle, a\langle\rangle\rangle$	$\langle b, \langle\rangle\rangle$

Strings

- An **alphabet** A is a set of **symbols**.
- A **string** over the alphabet A is a finite sequence of zero or more symbols from A that are placed next to each other in juxtaposition.
- Example: Consider the alphabet $\{a, b, c\}$.

  $aacabb$ is a string over the alphabet $\{a, b, c\}$.
- The string with no elements is called the **empty string**, and we denote it by (the Greek capital letter lambda) Λ.
- The number of elements that occur in a string is called the **length** of the string.
- We denote the length of a string s by $|s|$.
- Example: Over the alphabet $\{a, b, c\}$, the string $aacabb$ has length $|aacabb| = 6$.

Concatenation of Strings

- The operation of placing two strings s and t next to each other to form a new string st is called **concatenation**, denoted by cat.
- Example: If aab and ba are two strings over the alphabet $\{a, b\}$, then

$$\text{cat}(aab, ba) = aabba.$$

- If the empty string occurs as part of another string, then it does not contribute anything new to the string:

$$s\Lambda = \Lambda s = s$$
$$\text{cat}(s, \Lambda) = s$$

Languages over an Alphabet

- If A is an alphabet, then the set of all strings over A is denoted by A^*.
- Example: If $A = \{a\}$, then we have

$$A^* = \{\Lambda, a, aa, aaa, \ldots\}.$$

- A **language** L over A is a set of strings over A, i.e., $L \subseteq A^*$.
- Example:
  - For any alphabet A, four languages over A are $\emptyset$, $\{\Lambda\}$, A and A^*.
  - If $A = \{a\}$, then, the corresponding languages are $\emptyset$, $\{\Lambda\}$, $\{a\}$ and $\{\Lambda, a, aa, aaa, \ldots\}$.
- For a natural number n and a string s, s^n denotes the string of n s's:
  - $s^0 = \Lambda$;
  - $s^1 = s$;
  - $s^2 = ss$.
- Example: If $A = \{a\}$, then we can write $A^* = \{a^n : n \in \mathbb{N}\}$.

Example

- Suppose $A = \{a, b\}$.
- Then A^* can be described by writing down a few strings of small length followed by an ellipsis:

$$\begin{array}{rcl} A^* & = & \{\Lambda, a, b, aa, ab, ba, bb, \\ & & aaa, aab, aba, baa, baa, bab, bba, bbb, \ldots\}. \end{array}$$

- Some languages over A can be represented concisely by using exponents:
  - $\{ab^n : n \in \mathbb{N}\} = \{a, ab, abb, abbb, \ldots\}$;
  - $\{a^n b^n : n \in \mathbb{N}\} = \{\Lambda, ab, aabb, aaabbb, \ldots\}$;
  - $\{(ab)^n : n \in \mathbb{N}\} = \{\Lambda, ab, abab, ababab, \ldots\}$.

Example: Numerals

- A **numeral** is a nonempty string of symbols that represents a number.
- We are familiar with the following three numeral systems:
  - The **Roman numerals** represent the nonnegative integers by using the alphabet {I, V, X, L, C, D, M}.
  - The **decimal numerals** represent the natural numbers by using the alphabet $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
  - The **binary numerals** represent the natural numbers by using the alphabet $\{0, 1\}$.
- Example: The following numerals all represent the same number:
  - The Roman numeral MDCLXVI;
  - The decimal numeral 1666;
  - The binary numeral 11010000010.

Products of Languages

- Let L and M be languages.
- The **product** of L and M, denoted LM is the set of all concatenations of strings in L with strings in M:

$$LM = \{st : s \in L \text{ and } t \in M\}.$$

- Example: Let $A = \{a, b, c\}$ and consider the languages $L = \{ab, ac\}$ and $M = \{a, bc, abc\}$ over A.

  Then we have

$$\begin{aligned} LM &= \{aba, abbc, ababc, aca, acbc, acabc\}; \\ ML &= \{aab, aac, bcab, bcac, abcab, abcac\}. \end{aligned}$$

- Simple properties of the product:
  - $L\{\Lambda\} = \{\Lambda\}L = L$;
  - $L\emptyset = \emptyset L = \emptyset$;
  - $L(MN) = L(MN)$.

Product of a Language with Itself

- For any natural number n, the product of a language L with itself n times is denoted by L^n:
$$L^n = \{s_1 s_2 \cdots s_n : s_k \in L, k = 1, \ldots, n\}.$$
- The special case when $n = 0$ has the following definition.
$$L^0 = \{\Lambda\}.$$
- Example: If $L = \{a, bb\}$, then we have the following four products.
$$\begin{array}{lcl} L^0 & = & \{\Lambda\}; \\ L^1 & = & L = \{a, bb\}; \\ L^2 & = & LL = \{aa, abb, bba, bbbb\}; \\ L^3 & = & LL^2 = \{aaa, aabb, abba, abbbb, \\ & & \qquad bbaa, bbabb, bbbba, bbbbbb\}. \end{array}$$

Closure

- If L is a language, then the **closure** of L, denoted by L^*, is the set of all possible concatenations of (zero or more) strings from L:
$$L^* = L^0 \cup L^1 \cup L^2 \cup \cdots \cup L^n \cup \cdots .$$
- We have $x \in L^*$ if and only if $x \in L^n$ for some n.
It follows that
$$x \in L^* \text{ if and only if either } x = \Lambda \text{ or } x = \ell_1 \ell_2 \cdots \ell_n,$$
for some $n \geq 1$, where $\ell_k \in L$, for $k = 1, \ldots, n$.
- If L is a language, then the **positive closure** of L, which is denoted by L^+, is defined by
$$L^+ = L^1 \cup L^2 \cup L^3 \cup \cdots .$$
- It follows from the definition that $L^* = L^+ \cup \{\Lambda\}$.
- It is not necessarily true that $L^+ = L^* - \{\Lambda\}$.
- Example, if $L = \{\Lambda, a\}$, then $L^+ = L^*$.

Properties of Closure

- Let A be an alphabet.

  Then A^* has two meanings:
  - A^* is the set of all strings over A;
  - A^* is the closure of the language A.

  Fortunately, the two meanings coincide!
- The following are properties of the closure of languages:
  (a) $\{\Lambda\}^* = \emptyset^* = \{\Lambda\}$;
  (b) $\Lambda \in L$ if and only if $L^+ = L^*$;
  (c) $L^* = L^*L^* = (L^*)^*$;
  (d) $(L^*M^*)^* = (L^* \cup M^*)^* = (L \cup M)^*$;
  (e) $L(ML)^* = (LM)^*L$.

Proof of Property (e)

- We first show $L(ML)^* \subseteq (LM)^*L$.
  Suppose $x \in L(ML)^*$.
  Then $x = \ell y$, $\ell \in L$, $y \in (ML)^*$.
  So $x = \ell y$, $\ell \in L$, $y \in (ML)^n$, for some $n \geq 0$.
  - If $n = 0$, $x = \ell\Lambda = \ell = \Lambda\ell \in (LM)^*L$;
  - If $n > 0$, $x = \ell w_1 \ldots w_n$, $\ell \in L$, $w_i \in ML$.
    So $x = \ell m_1 \ell_1 \cdots m_n \ell_n$, $\ell \in L$, $m_i \in M$, $\ell_i \in L$.
    But, then
$$x = (\ell m_1)(\ell_1 m_2) \cdots (\ell_{n-1} m_n)\ell_n \in (LM)^*L.$$

The reverse inclusion $(LM)^*L \subseteq L(ML)^*$ can be proved similarly.

Relations

- An n-**ary relation** R over the product set $A_1 \times \cdots \times A_n$ is just a subset of $A_1 \times \cdots \times A_n$.
- The smallest n-ary relation over over $A_1 \times \cdots \times A_n$ is $\emptyset$.
- The largest n-ary relation over $A_1 \times \cdots \times A_n$ is $A_1 \times \cdots \times A_n$ itself, called the **universal relation**.
- If R is a binary relation over $A \times B$, we sometimes say "R is a binary relation **from** A **to** B".
- If R is an n-ary relation over $A \times \cdots \times A$, i.e., a subset of the product A^n, then R is called an n-**ary relation on** A.
- If R is a binary relation and $(x, y) \in R$, we often denote this fact by writing:
  - the **prefix expression** $R(a, b)$; or
  - the **infix expression** $x \ R \ y$.

Examples

- The "less than" relation is a binary relation on $\mathbb{N}$, defined as follows:

$$< = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x < y\}.$$

We have $(1, 2) \in <$. We write this as $1 < 2$.

Moreover $(5, 2) \notin <$. We write this as $5 \not< 2$.

- A ternary relation P on $\mathbb{R}$ is defined as follows:

$$P = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 = z^2\}.$$

We have:

  - $(3, 4, 5) \in P$;
  - $(6, 8, 10) \in P$;
  - $(2, 1, \sqrt{5}) \in P$;
  - $(1, 2, 5) \notin P$.

More on Relations

- The **equality relation** on a set A is the binary relation on A defined as follows:
$$= \ := \ \{(a,a) : a \in A\} \text{ of } A^2.$$
- Example: If $A = \{a, b, c\}$, then the equality relation on A is the set $\{(a,a),(b,b),(c,c)\}$.
  In this case we normally write $a = a$ instead of $=(a,a)$.
- A unary relation is similar to a test for membership in a set:
  Suppose R is a unary relation over the set A.
  Then R can be viewed as a subset of A:
$$\{x \in A : R(x)\}.$$
- Example: Suppose $A = \{1, 2, \ldots, 9\}$.
  Consider the unary relation R on A: $R = \{(2),(3),(5),(7)\}$.
  Then $\{x \in A : R(x)\} = \{2, 3, 5, 7\}$.