CHAPTER 6

SET THEORY

Why do we study set theory?

Set Theory is the foundation of mathematics and many aspects of Computer Science and Data Analysis:

- **Binary Logic** (see equivalence between Boolean Algebra and operations on sets)
- Sets form the basis of many **data structure** used in programming, e.g. Set (Java).
- **Databases**: Set Theory determines which data will be included and excluded in searches and selections
- **Distribution lists** for messages such as email
- **Cryptography** for secure communications
- **Bayesian filtering** of junk email
- **Artificial-Intelligence**-based decision making
- **Image Processing** and **Recognition**

Cantorian Set Theory

- Georg Cantor (1845 – 1918)
- German Mathematician
- Defined the notion of a set, union, intersection **rigorously**.
  - He basically invented the **entirety** of Set Theory we know today

Basic Definition of Set

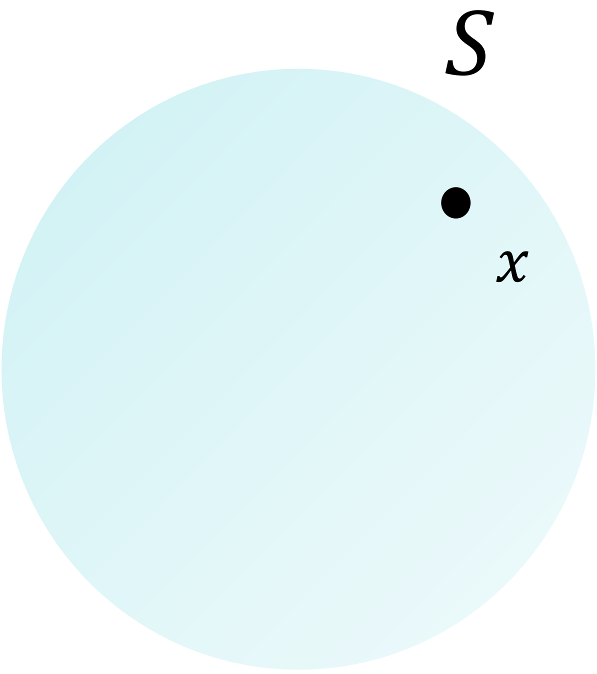
Cantor's definition of a set:

A set S is a “*collection into a whole S of definite and separate objects of our intuition or our thought. These objects are called the elements of S.*”

Basically, a set is a collection of **distinct** objects. That’s it. Nothing else.

Basic Definition of Set

- We will use the notation $\boldsymbol{x} \in \boldsymbol{S}$, which means that
  - “x is a member of S” or
  - “x is an element of S” or
  - “x is in S” or
  - “S contains x”.
- The above expressions are all equivalent.



Venn diagram of set S

Example – *Representation of Sets*

1. Through **enumeration** (“curly bracket” {} notation)
   - $A = \{-1, 2, 8\}$
   - $B = \{20\}$
   - $C = \{10, 20, 30, 40, \ldots\}$
   - $D = \{A, B, C\}$
   - $E = \{A, B, C, D, 1, 2, 3, \{-2, -10\}\}$

2. Through a **property**
   - $S_1 = \{x \mid (x \in \mathbf{R}) \wedge (x \geq 100)\}$
   - $S_2 = \{y \mid (y \in \mathbf{R}) \wedge (y^2 = 3)\}$
   - $S_3 = \{\ell \mid \ell$ is a string of at most 5 characters$\}$

3. Through an agreed upon symbol (**N**, **Z**, **Q**, **R**)

Exercise – *Set Identification*

Identify which set each expression belongs to (**N**, **Z**, **R**)

1. $\{x - 1 \mid x \in \mathbf{N}^{\geq 1}\} \rightarrow \mathbf{N}$

2. $\{x + y \mid x, y \in \mathbf{Z}\} \rightarrow \mathbf{Z}$

3. $\{x + y \mid x, y \in \mathbf{N}\} \rightarrow \mathbf{N}$

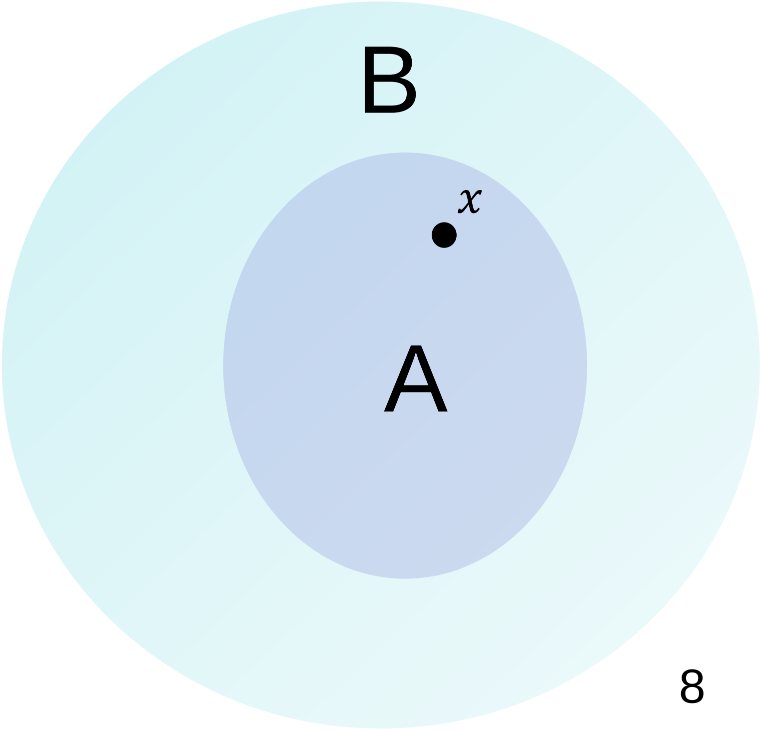
4. $\{x^2 \mid x \in \mathbf{R}\} \rightarrow \mathbf{R}^{\geq 0}$ (non-negative reals)

Definition: Subset of a Set

- We say that A is a **subset** of B ($A \subseteq B$) iff (e.g., if and only if) $\forall x \in A$ then $x \in B$

$$\boxed{A \subseteq B \iff \forall x,\ \text{if } x \in A \text{ then } x \in B.}$$

- We also then say that B is a **superset** of A ($B \supseteq A$)

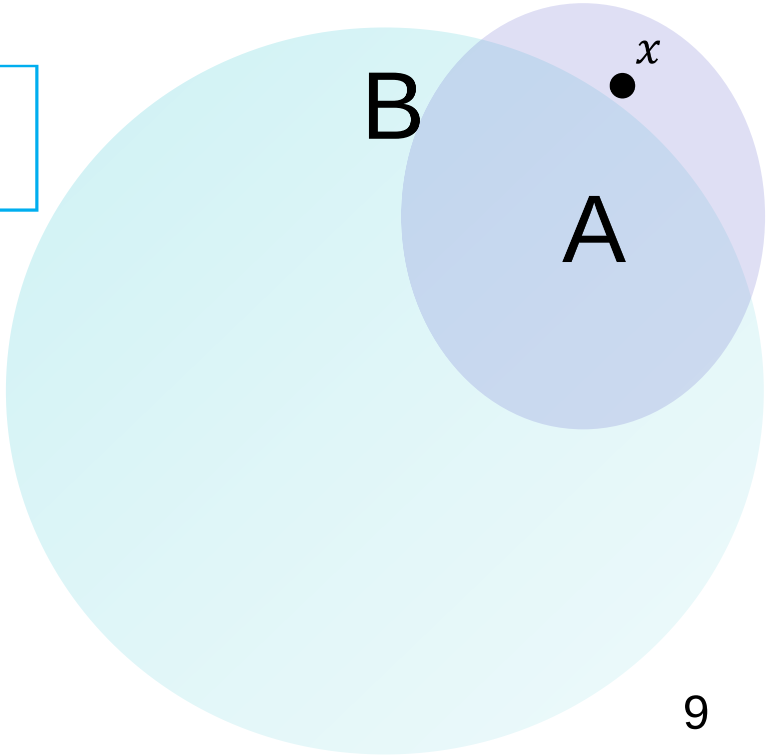


Definition: Not a Subset

- The negation of "being a subset" is existential:

  A is **not** a **subset** of B ($A \nsubseteq B$)
  if and only if there exists an element of A that is not in B

$$A \nsubseteq B \quad \Leftrightarrow \quad \exists x \text{ such that } x \in A \text{ and } x \notin B.$$



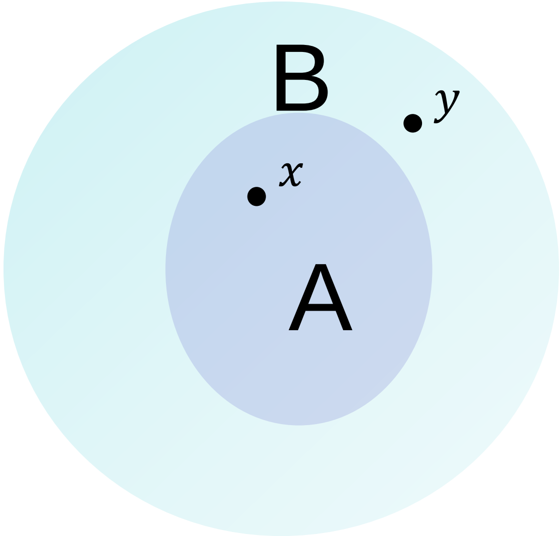
Definition: Proper Subset of a Set

We say that A is a *proper subset* of B ($A \subset B$) if and only if it is a subset that is not equal to its containing set. Thus

A is a **proper subset** of B $\Leftrightarrow$

(1) $A \subseteq B$, and

(2) there is at least one element in B that is not in A.



$A \subset B$

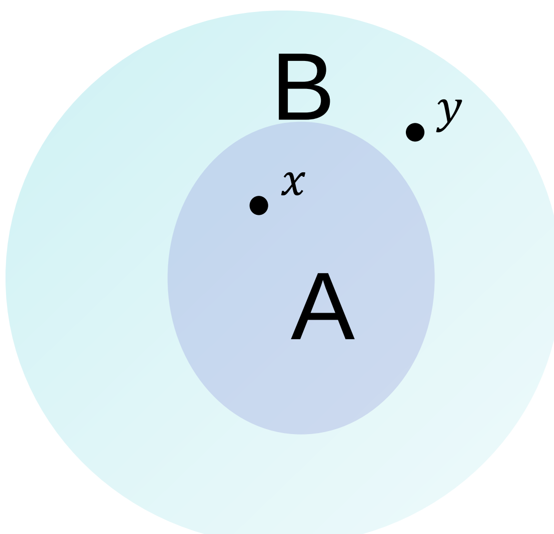
Definition: Proper Subset of a Set

We say that A is a *proper subset* of B ($A \subset B$) if and only if it is a subset that is not equal to its containing set. Thus

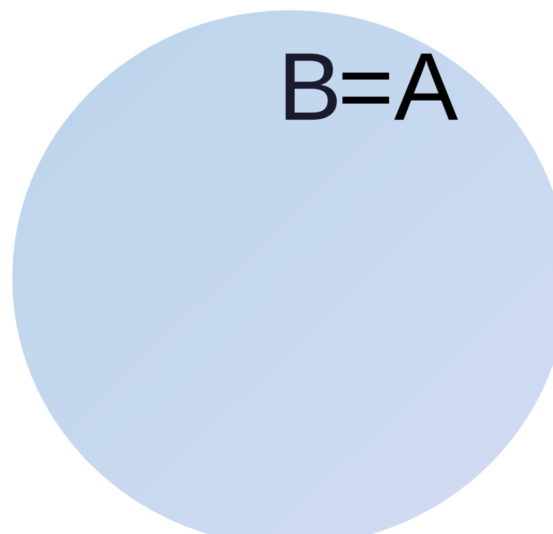
A is a **proper subset** of B $\Leftrightarrow$

(1) $A \subseteq B$, and

(2) there is at least one element in B that is not in A.



$A \subset B$



$A \not\subset B$ but $A \subseteq B$ because A=B

Exercise 1 – *Testing Whether One Set Is a Subset of Another*

Let $A = \{1\}$ and $B = \{1, 2\}$.

a. Is $A \subseteq B$?

b. If so, is A a proper subset of B?

Solution:

Yes because:

a. A only has the element 1, which is also an element of set B, hence $A \subseteq B$.

b. It is **proper** because there is at least one element in B that is not in A, which is the 2, since $1 \neq 2$

Exercise 2 – *True or False?*

- $\mathbf{N} \subseteq \mathbf{Z}$ $\rightarrow$ True
- $\mathbf{N} \subset \mathbf{Z}$ $\rightarrow$ True
- $\mathbf{Z}^{\geq 0} \subset \mathbf{N}$ $\rightarrow$ False ($\mathbf{Z}^{\geq 0} = \mathbf{N}$)
- $\mathbf{N} \subseteq \mathbf{N}$ $\rightarrow$ True
- $\{0, 1, 2, 3, \ldots\} \subset \mathbf{N}$ $\rightarrow$ False ($\{0, 1, 2, 3, \ldots\} = \mathbf{N}$)

Subsets: Proof and Disproof

How do we **proof mathematically** that a set A is a subset of another set B?

$$\boxed{A \subseteq B \quad \Leftrightarrow \quad \forall x,\ \text{if } x \in A \text{ then } x \in B.}$$

- **Solution**: pick a **particular but arbitrarily chosen** element x of A and show that it is also an element of B

Example – *Proving and Disproving Subset Relations*

Define sets *A* and *B* as follows:

$$A = \{m \in \mathbf{Z} \mid m = 6r + 12 \text{ for some } r \in \mathbf{Z}\}$$
$$B = \{n \in \mathbf{Z} \mid n = 3s \text{ for some } s \in \mathbf{Z}\}.$$

a. Prove that $A \subseteq B$.

b. Disprove that $B \subseteq A$.

Solution – *Proving and Disproving Subset Relations*

$$A = \{m \in \mathbf{Z} \mid m = 6r + 12 \text{ for some } r \in \mathbf{Z}\}$$
$$B = \{n \in \mathbf{Z} \mid n = 3s \text{ for some } s \in \mathbf{Z}\}.$$

a. Suppose x is an arbitrarily chosen element of A.
By definition, there is an integer r such that $x = 6r + 12$.
Let $s = 2r + 4$. It holds that

$$3s = 3(2r + 4) = 6r + 12 = x,$$

Thus, x is an element of B by definition of B.

b. Let $x = 3$. Then $x \in B$ because $3 = 3 \cdot 1$, but $x \notin A$ because there is no integer r such that $3 = 6r + 12$.
Thus, $B \not\subseteq A$.

Set Equality

Two sets A and B are equal iff every element of A is in B and every element in B is in A

- **Definition**

Given sets A and B, A **equals** B, written $\boldsymbol{A = B}$, if, and only if, every element of A is in B and every element of B is in A.

Symbolically:

$$A = B \quad \Leftrightarrow \quad A \subseteq B \text{ and } B \subseteq A.$$

Exercise – *Set Equality*

Define sets A and B as follows:

$$A = \{m \in \mathbf{Z} \mid m = 2a \text{ for some integer } a\}$$

$$B = \{n \in \mathbf{Z} \mid n = 2b - 2 \text{ for some integer } b\}$$

Is $A = B$?

Solution:

Yes. First, we show that $A \subseteq B$: Let $b = a + 1$ (b is an integer because it is a sum of integers).

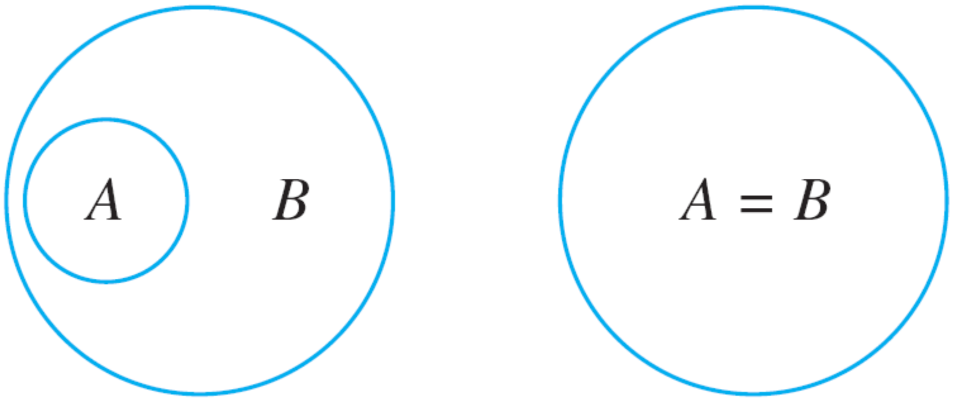
It holds that $2b - 2 = 2(a + 1) - 2 = 2a + 2 - 2 = 2a = x$, thus x is an element of B.

Similarly we can prove that $B \subseteq A$.
Hence $A = B$.

Venn Diagrams

If sets A and B are represented as regions in the plane, relationships between A and B can be represented by **Venn diagrams**, introduced by John Venn in 1881.

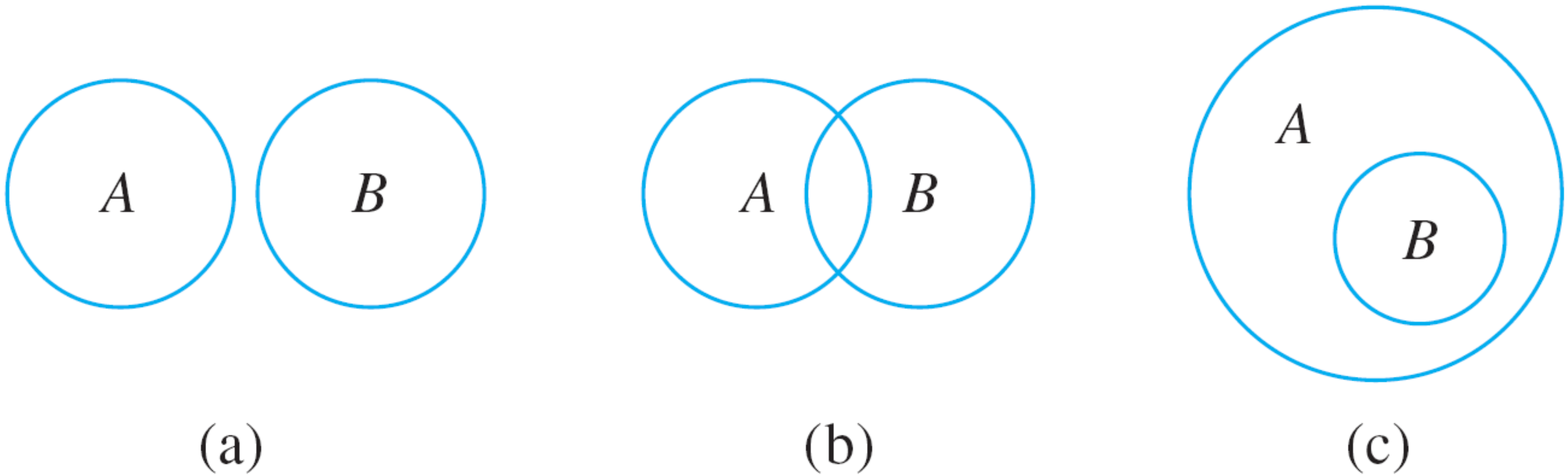
For example, the relationship $A \subseteq B$ can be pictured in one of two ways:



(a) (b)

Venn Diagrams

The relationship $A \not\subseteq B$ can be represented in three different ways with Venn diagrams:



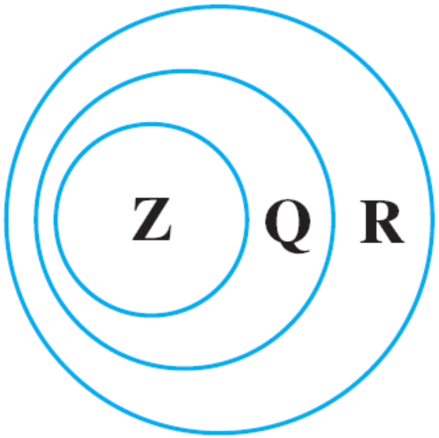
Example – *Relations among Sets of Numbers*

Z is a subset of **Q** because every integer is rational.

Q is a subset of **R** because every rational number is real.

Z is a proper subset of **Q** because there are rational numbers that are not integers (for example, 1/2).

Q is a proper subset of **R** because there are real numbers that are not rational (for example, $\sqrt{2}$).



The Empty Set (∅, { })

The empty set (or null set), denoted by ∅ or { }, is the **unique** set with **no elements**

- The **empty set is a subset of every set**, or alternatively, every set contains the empty set.

For example, $\{1, 3\} \cap \{2, 4\} = \varnothing$ and $\{x \in \mathbf{R} \mid x^2 = -1\} = \varnothing$.

Exercise: True or False?

1. $\emptyset \subseteq \mathbf{N}$ $\rightarrow$ **True**

2. $\emptyset \subseteq A$ for any set A $\rightarrow$ **True**

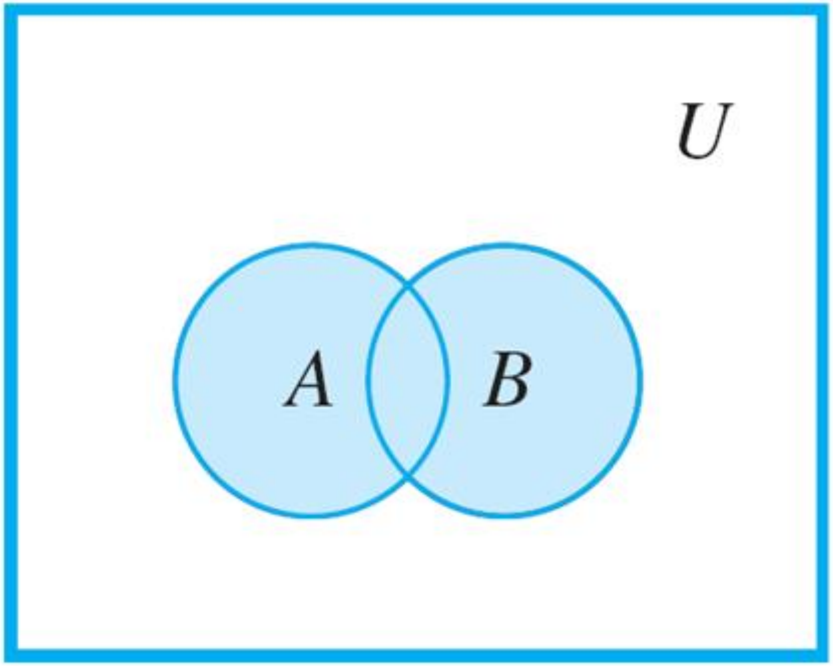
3. $\emptyset \subset A$ for any set A $\rightarrow$ **False** (if A is the empty set, then $\emptyset$ is not a proper set of itself)

4. $\emptyset \subseteq \emptyset$ $\rightarrow$ **True** because $\emptyset = \emptyset$

Operations on Sets: Union

- The **union** between two sets A and B, denoted $A \cup B$, is the **set of elements that belong either to A or to B:**

$$A \cup B = \{x \in U \mid (x \in A) \vee (x \in B)\}$$

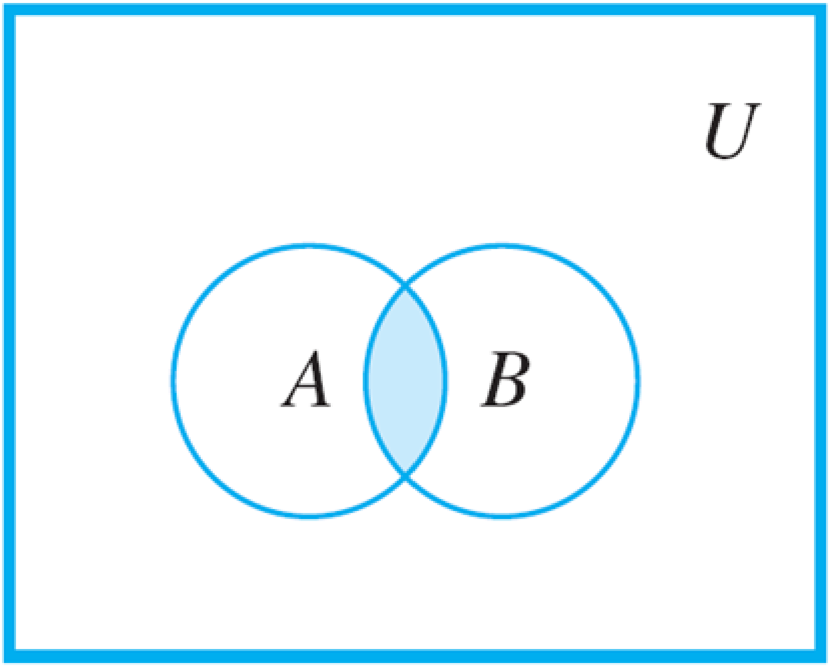


NB: U is the universal set (i.e., the set that includes all sets and all objects)

Operations on Sets: Intersection

- The **intersection** between A and B, denoted $A \cap B$, is the **set of elements that belong to both** A and B.

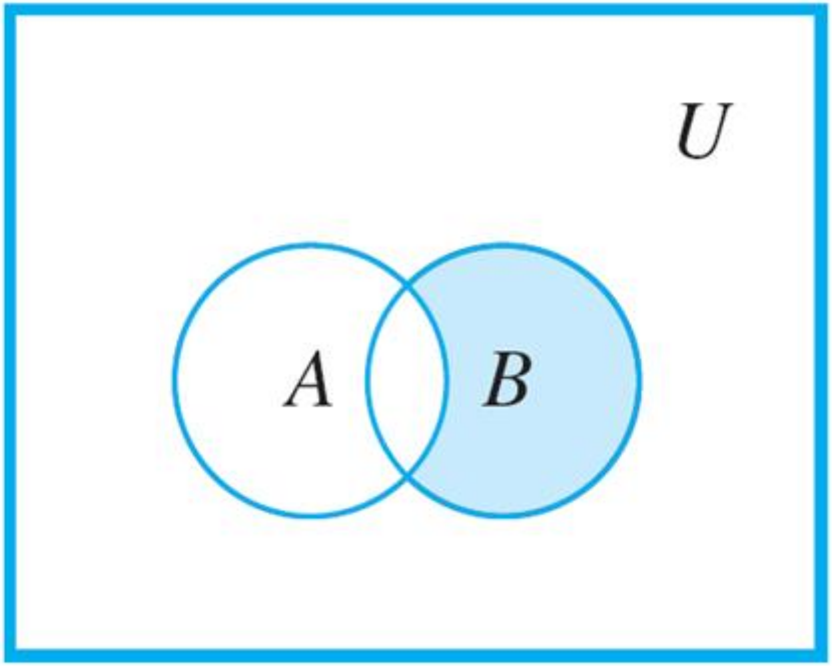
$$A \cap B = \{x \in U \mid (x \in A) \wedge (x \in B)\}$$



Operations on Sets: Difference

- The **difference** B−A is the set of all elements in B but not in A:

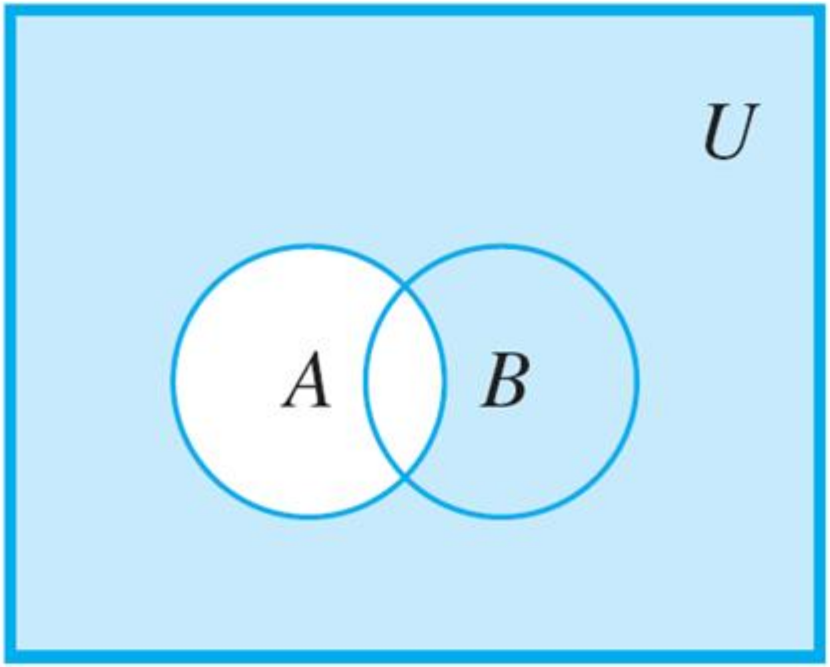
$$B - A = \{x \in U \mid (x \in B) \land (x \notin A)\}$$



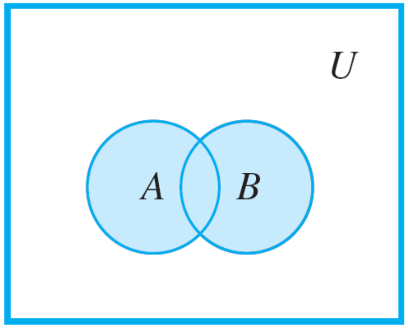
Operations on Sets: Complement

- The complement of A, denoted A^c, is the set of all elements that do **not** belong to A:

$$A^c = \{x \in U \mid x \notin A\}$$

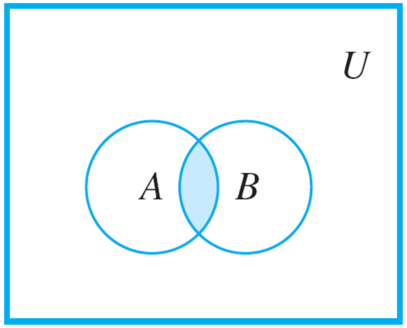


Operations on Sets: Recap



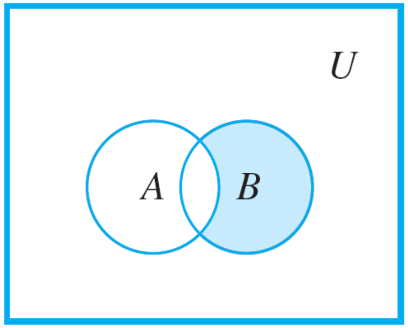
Shaded region represents *A* ∪ *B*.

$A \cup B = \{x \in U |$
$(x \in A) \vee (x \in B)\}$



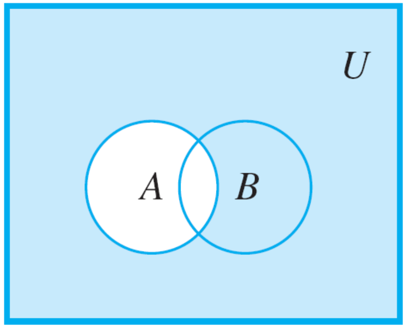
Shaded region represents *A* ∩ *B*.

$A \cap B = \{x \in U \mid$
$(x \in A) \wedge (x \in B)\}$



Shaded region represents *B* – *A*.

$B - A = \{x \in U \mid$
$(x \in B) \wedge (x \notin A)\}$



Shaded region represents A^c.

$A^c = \{x \in U \mid x \notin A\}$

Exercise 1 – *Unions, Intersections, Differences, and Complements*

Let the universal set be the set $U = \{a, b, c, d, e, f, g\}$ and let $A = \{a, c, e, g\}$ and $B = \{d, e, f, g\}$. Find $A \cup B$, $A \cap B$, $B - A$, and A^c.

Solution:

$$A \cup B = \{a, c, d, e, f, g\}$$

$$A \cap B = \{e, g\}$$

$$B - A = \{d, f\}$$

$$A^c = \{b, d, f\}$$

Exercise 2 – *Unions, Intersections, Differences, and Complements*

1. $\mathrm{A} \cup \mathrm{U} = \mathrm{U}$
2. $A \cap \mathrm{U} = \mathrm{A}$
3. $A \cup \emptyset = \mathrm{A}$
4. $A \cap \emptyset = \emptyset$
5. $A - A = \emptyset$
6. $A - \mathrm{U} = \emptyset$
7. $\mathrm{U}^c = \emptyset$
8. $\emptyset^c = \mathrm{U}$

Interval Sets

- **Notation**

Given real numbers a and b with $a \leq b$:

$$(a, b) = \{x \in \mathbf{R} \mid a < x < b\} \qquad [a,\ b] = \{x \in \mathbf{R} \mid a \leq x \leq b\}$$
$$(a, b] = \{x \in \mathbf{R} \mid a < x \leq b\} \qquad [a,\ b) = \{x \in \mathbf{R} \mid a \leq x < b\}.$$

The symbols ∞ and $-\infty$ are used to indicate intervals that are unbounded either on the right or on the left:

$$(a, \infty) = \{x \in \mathbf{R} \mid x > a\} \qquad [a, \infty) = \{x \in \mathbf{R} \mid x \geq a\}$$
$$(-\infty, b) = \{x \in \mathbf{R} \mid x < b\} \qquad [-\infty, b) = \{x \in \mathbf{R} \mid x \leq b\}.$$

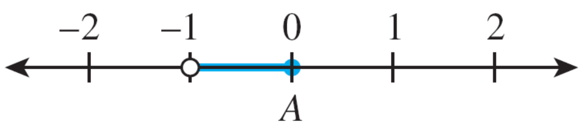
NB: Note that the notation for the interval (a, b) is identical to the notation for the ordered pair (a, b). However, context makes it unlikely that the two will be confused.

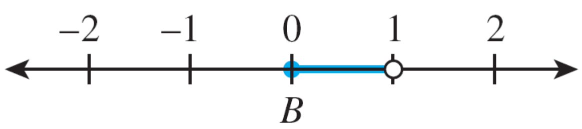
Exercise – *An Example with Intervals*

Let the universal set be **R** and let

$$A = (-1,\ 0] = \{x \in \mathbf{R} \mid -1 < x \leq 0\} \text{ and } B = [0,\ 1) = \{x \in \mathbf{R} \mid 0 \leq x < 1\}.$$

Graphically:

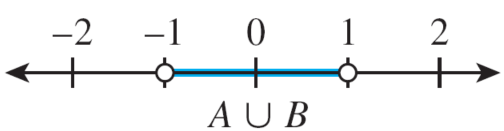




Find $A \cup B$, $A \cap B$, $B - A$, and A^c.

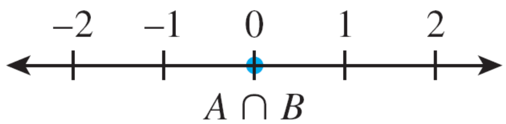
Solution:

$$A \cup B = \{x \in \mathbf{R} \mid x \in (-1,\ 0] \text{ or } x \in [0,\ 1)\} = \{x \in \mathbf{R} \mid x \in (-1,\ 1)\} = (-1,\ 1).$$

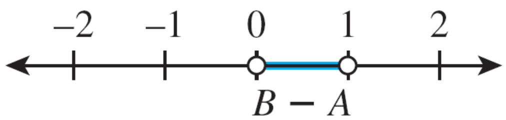


Solution – *An Example with Intervals*

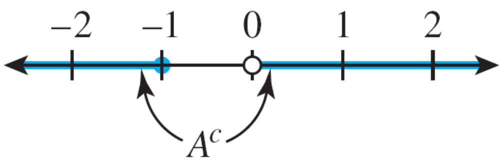
$$A \cap B = \{x \in \mathbf{R} \mid x \in (-1,\ 0] \text{ and } x \in [0,\ 1)\} = \{0\}.$$



$$B - A = \{x \in \mathbf{R} \mid x \in [0,\ 1) \text{ and } x \notin (-1,\ 0]\} = \{x \in \mathbf{R} \mid 0 < x < 1\} = (0, 1)$$



$$A^c = \{x \in \mathbf{R} \mid \text{it is not the case that } x \in (-1,\ 0]\}$$



Operations on Sets

- **Definition**

Unions and Intersections of an Indexed Collection of Sets

Given sets $A_0,\ A_1,\ A_2, \ldots$ that are subsets of a universal set U and given a nonnegative integer n,

$$\bigcup_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for at least one } i = 0, 1, 2, \ldots, n\}$$

$$\bigcup_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for at least one nonnegative integer } i\}$$

$$\bigcap_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for all } i = 0, 1, 2, \ldots, n\}$$

$$\bigcap_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for all nonnegative integers } i\}.$$

Exercise – *Finding Unions and Intersections of More than Two Sets*

For each positive integer *i*, let

$$A_i = \left\{x \in \mathbf{R} \mid -\frac{1}{i} < x < \frac{1}{i}\right\} = A_i = \left(-\frac{1}{i}, \frac{1}{i}\right).$$

Find $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$.

Solution – *Finding Unions and Intersections of More than Two Sets*

$$\bigcup_{i=1}^{\infty} A_i = \{x \in \mathbf{R} \mid x \text{ is in at least one of the intervals } \left(-\frac{1}{i}, \frac{1}{i}\right),$$

$$= \{x \in \mathbf{R} \mid -1 < x < 1\}$$

because all the elements in every interval $\left(-\frac{1}{i}, \frac{1}{i}\right)$ are in $(-1, 1)$

$$= (-1, 1)$$

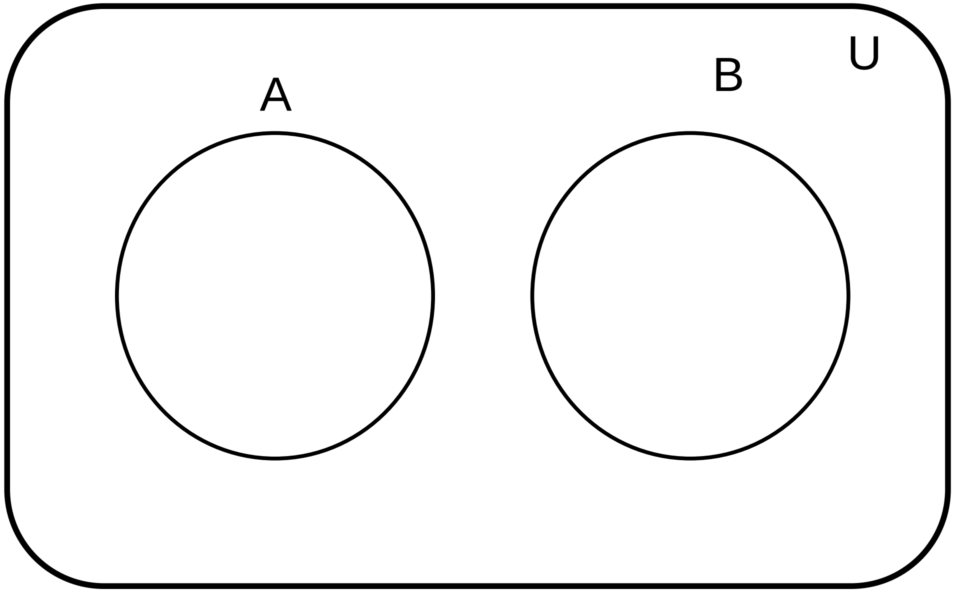
$$\bigcap_{i=1}^{\infty} A_i = \{x \in \mathbf{R} \mid x \text{ is in all of the intervals } \left(-\frac{1}{i}, \frac{1}{i}\right), \text{ where } i \text{ is}$$

$$= \{0\}$$

because the only element in every interval is 0

Mutually Disjoint Sets

Two sets A, B are called **mutually disjoint** (or just disjoint) iff they have no elements in common or $A \cap B = \emptyset$



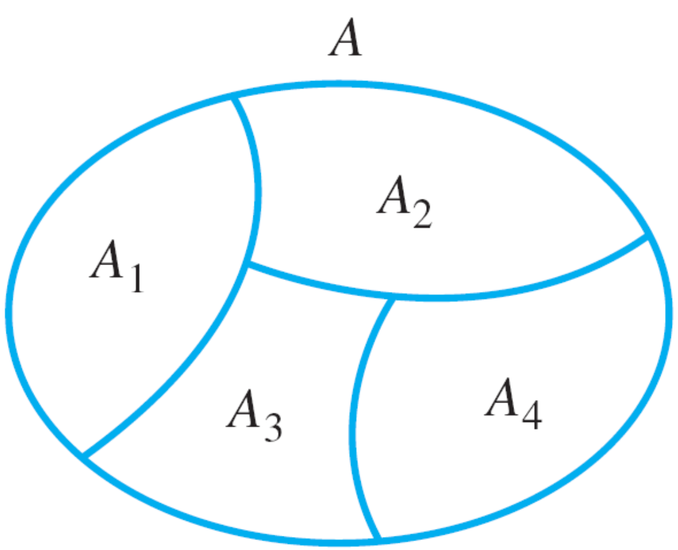
Example: $A = \{1, 3, 5\}$ and $B = \{2, 4, 6\}$ are disjoint because $\{1, 3, 5\} \cap \{2, 4, 6\} = \emptyset$.

Partitions of Sets

- Let A be a set. $P = \{A_1, A_2, \ldots A_n\}$ is a **partition of A** iff
  - A_i and A_j are **mutually disjoint**, for all i, j with $i \neq j$
  - $A_1 \cup A_2 \cup \cdots \cup A_n = A$

Example – Partitions of Sets

Suppose A, A_1, A_2, A_3, and A_4 are the sets of points represented by the following regions:



$\{A_1, A_2, A_3, A_4\}$ is a partition of A because A_1, A_2, A_3, and A_4 are disjoint and $A = A_1 \cup A_2 \cup A_3 \cup A_4$.

Exercise: True or False?

1. $\{\mathbf{Z}^{<0}, \{0\}, \mathbf{N}^{>0}\}$ is a partition of $\mathbf{Z}$ $\rightarrow$ **True**

2. $\{\mathbf{Z}^{<0}, \{0\}, \mathbf{N}\}$ is a partition of $\mathbf{Z}$ $\rightarrow$ **False**

3. $\{\mathbf{Q}, \mathbf{R} - \mathbf{Q}\}$ is a partition of $\mathbf{R}$ $\rightarrow$ **True**

Exercise – Partitions of Sets

Let **Z** be the set of all integers and let

$$T_0 = \{n \in \mathbf{Z} \mid n = 3k, \text{ for some integer } k\},$$
$$T_1 = \{n \in \mathbf{Z} \mid n = 3k + 1, \text{ for some integer } k\}, \text{ and}$$
$$T_2 = \{n \in \mathbf{Z} \mid n = 3k + 2, \text{ for some integer } k\}.$$

Is $\{T_0, T_1, T_2\}$ a partition of **Z**?

Solution:

Yes, by the quotient-remainder theorem, every integer n can be represented in exactly one of the three forms

$$n = 3k \quad \text{or} \quad n = 3k + 1 \quad \text{or} \quad n = 3k + 2,$$

and thus $T_0 \cap T_1 \cap T_2 = \emptyset$ and $\mathbf{Z} = T_0 \cup T_1 \cup T_2$.

Ordered Tuples

Let n be a positive integer and $x_1, x_2, \ldots, x_n$ elements, the following ordered set is called

- ordered n-tuple $(x_1, x_2, \ldots, x_n)$.
- If n=2, (x_1, x_2) is called an **ordered pair.**
- If n=3, (x_1, x_2, x_3) is called an **ordered triple.**

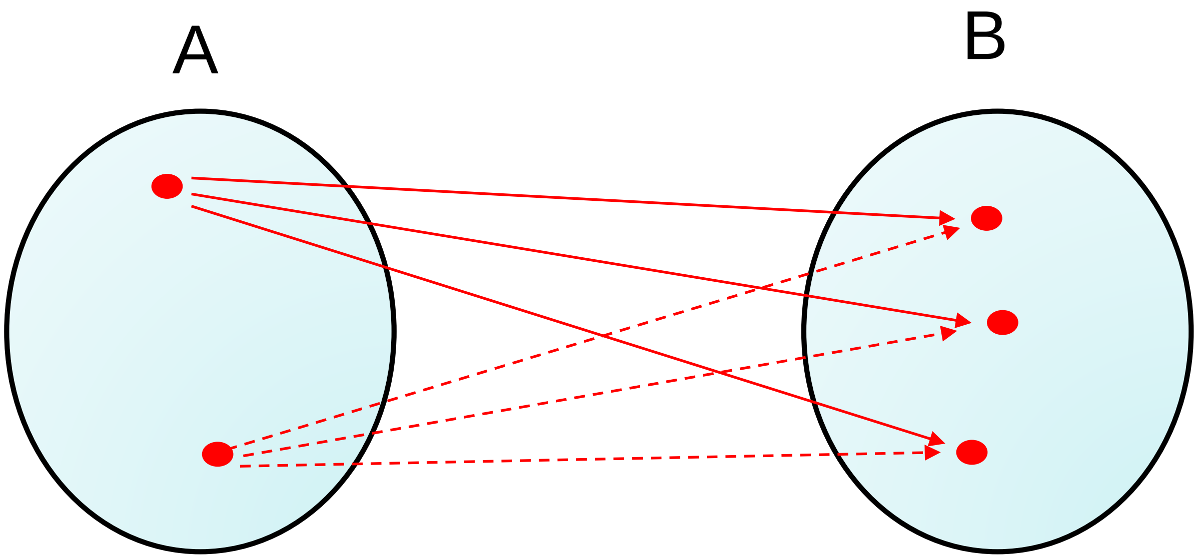
Two ordered n-tuples $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ are equal iff $x_1 = y_1$, $x_2 = y_2$, …, $x_n = y_n$.

Example: $(a, b) = (c, d)$ iff $(a = c)$ and $(b = d)$.

Cartesian Products between two sets

Denoted $A \times B$, the **Cartesian product** between A and B is the set of **ordered pairs** of elements of A and B:

$$\{(a, b) | (a \in A) \wedge (b \in B)\}$$



Cartesian Products between n sets

More generally, given the sets $A_1, A_2, \ldots, A_n$, the **Cartesian product** $A_1 \times A_2 \ldots \times A_n$ is the set of **ordered $\boldsymbol{n}$-tuples**

$$\{(a_1, a_2, \ldots, a_n) | (a_1 \in A_1) \wedge (a_2 \in A_2) \wedge \cdots \wedge (a_n \in A_n)\}$$

Cartesian Products os Sets with Themselves

- A shorthand notation for $\underbrace{\mathrm{A} \times A \times \ldots \times A}_{n \text{ times}}$ is A^n.

- Examples:
  - if $A = \{a, b, c\}$, then

    $A^3 = \{(a,a,a),(a,a,b),(a,a,c),(a,b,a),\ldots,(c,c,b),(c,c,c)\}$
  - **$\mathbf{R}^2$ (Cartesian plane)**
  - **$\mathbf{R}^3$ (3D Space)**
  - $\{(x,y) \mid (x,y) \in \mathbf{R}^2 \wedge (x^2+y^2 \leq 1)\}$ = Two-dimensional disk of radius 1, centered at the origin

Cardinality

- For a **finite set A**, its cardinality, denoted |A|, is the number of its elements.
- For an **infinite set A,** the definition is more complicated (we will see this in Chapter 7).
- The cardinality of the Cartesian products of two sets is the product between the cardinality of the two sets.

Recap Quiz

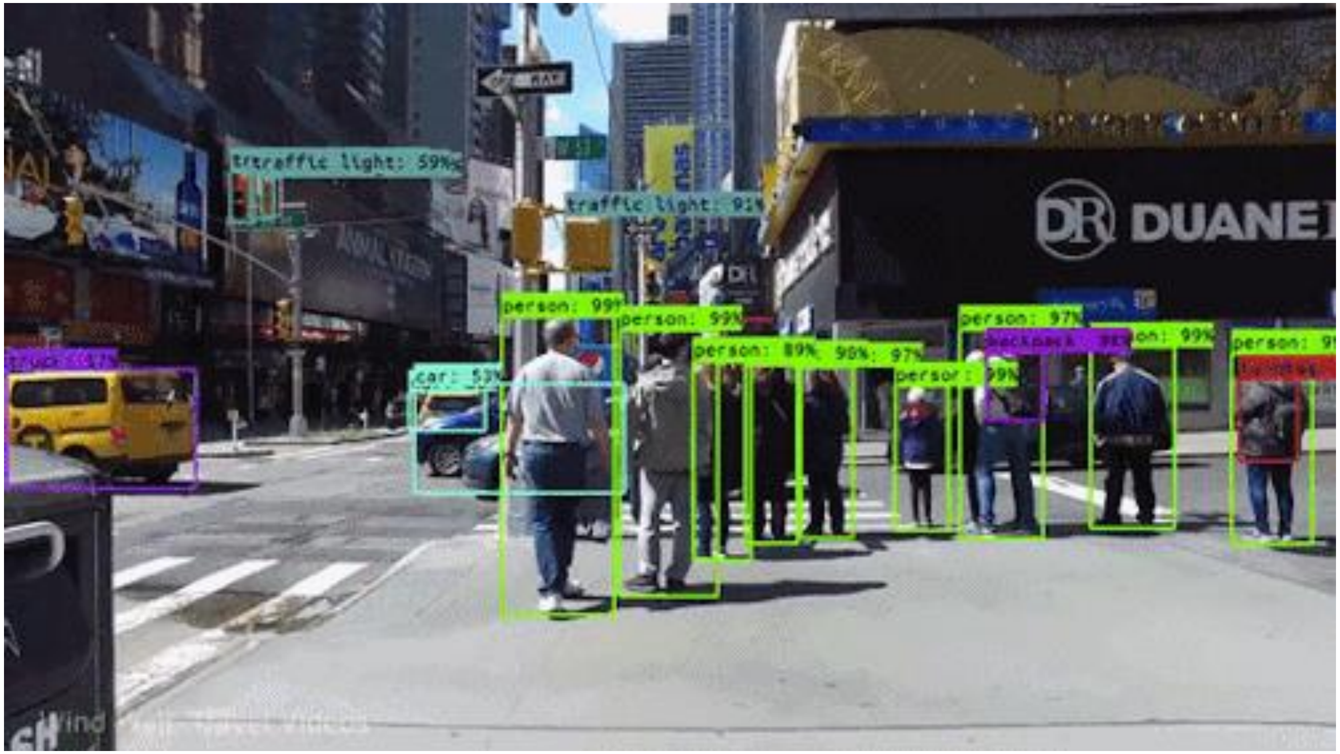
1. $(A \cap B) \subseteq (A \cup B)$ → True
2. $A - B$ and B are mutually disjoint. → True
3. $(A \subset B) \Rightarrow (A \subseteq B)$ → True
4. $\{\mathbf{R}^{\neq 0}, \{0\}\}$ is a partition of $\mathbf{R}$ → True
5. $\emptyset \subseteq \{\ \}$ → True
6. $|A^n| = |A|^n, n \in \mathbf{N}$ → True

Extra

Set Theory applied to Digital Image Processing

Digital Image Processing

- In computer science, digital image processing is the use of computer algorithms to process digital images

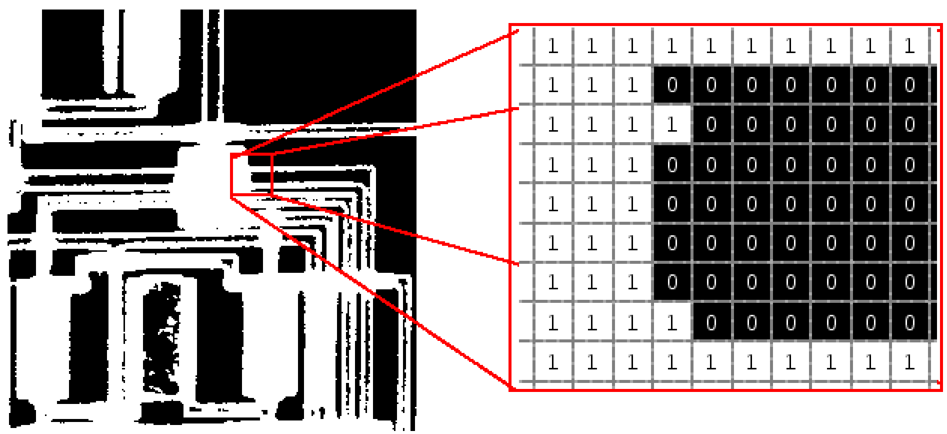


Binary Images

- Because image processing is outside the scope of this course, we will consider **binary images** for now
- A binary image is an image whose **pixels values can either be 0** (black) **or 1** (white), e.g., bar codes, text, etc.

0 36000 29145 2

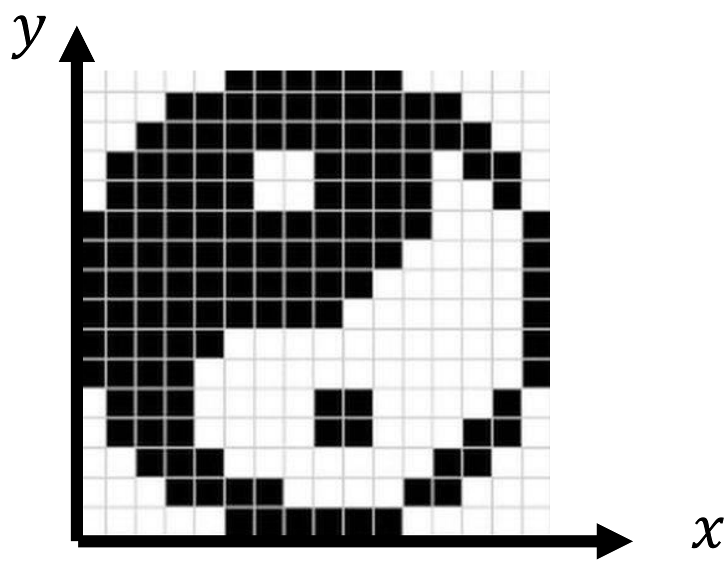
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae



Binary Images as Sets

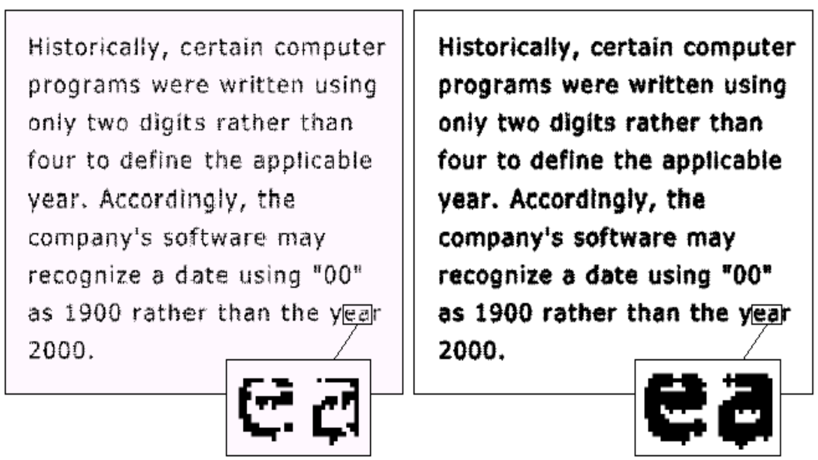
- A binary image A can be defined as the set of grid elements, whose coordinates are the ordered pairs (x, y) of the **2-D integer space N²** such that the pixel value (i.e., grid value) $I(x, y) = 0$:

$$A = \{(x, y) \in N^2 \,|I(x, y) = 0\}$$



Dilation

- Dilation is popular image processing operation that **grows and thickens** objects of a binary image
- The extent of the thickening is controlled by a **shape** called **structuring element**, which is **carefully designed**
- A structuring element is also a binary image



0	1	0
1	1	1
0	1	0

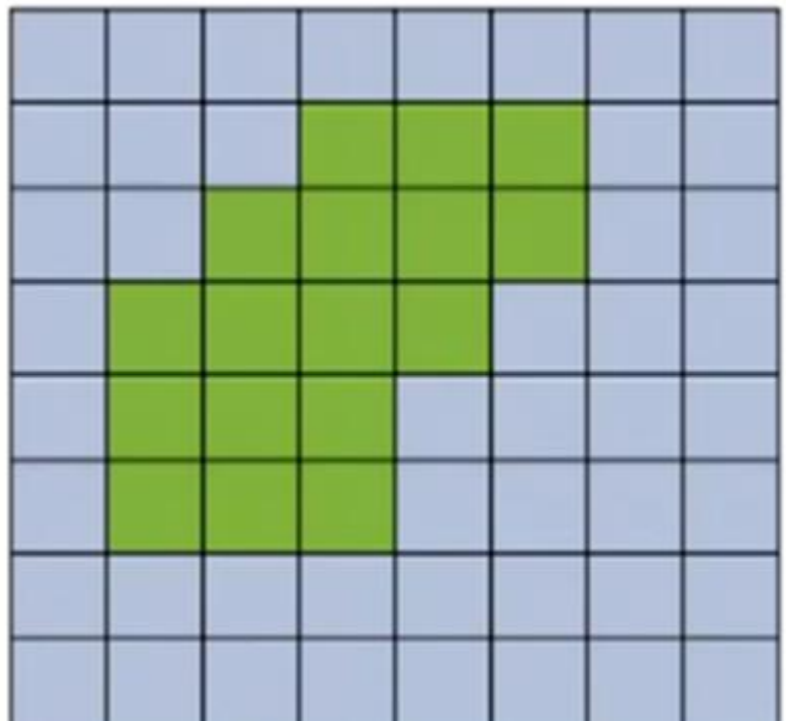
a c
b

FIGURE 9.5 (a) Sample text of poor resolution with broken characters (magnified view). (b) Structuring element. (c) Dilation of (a) by (b). Broken segments were joined.

Dilation

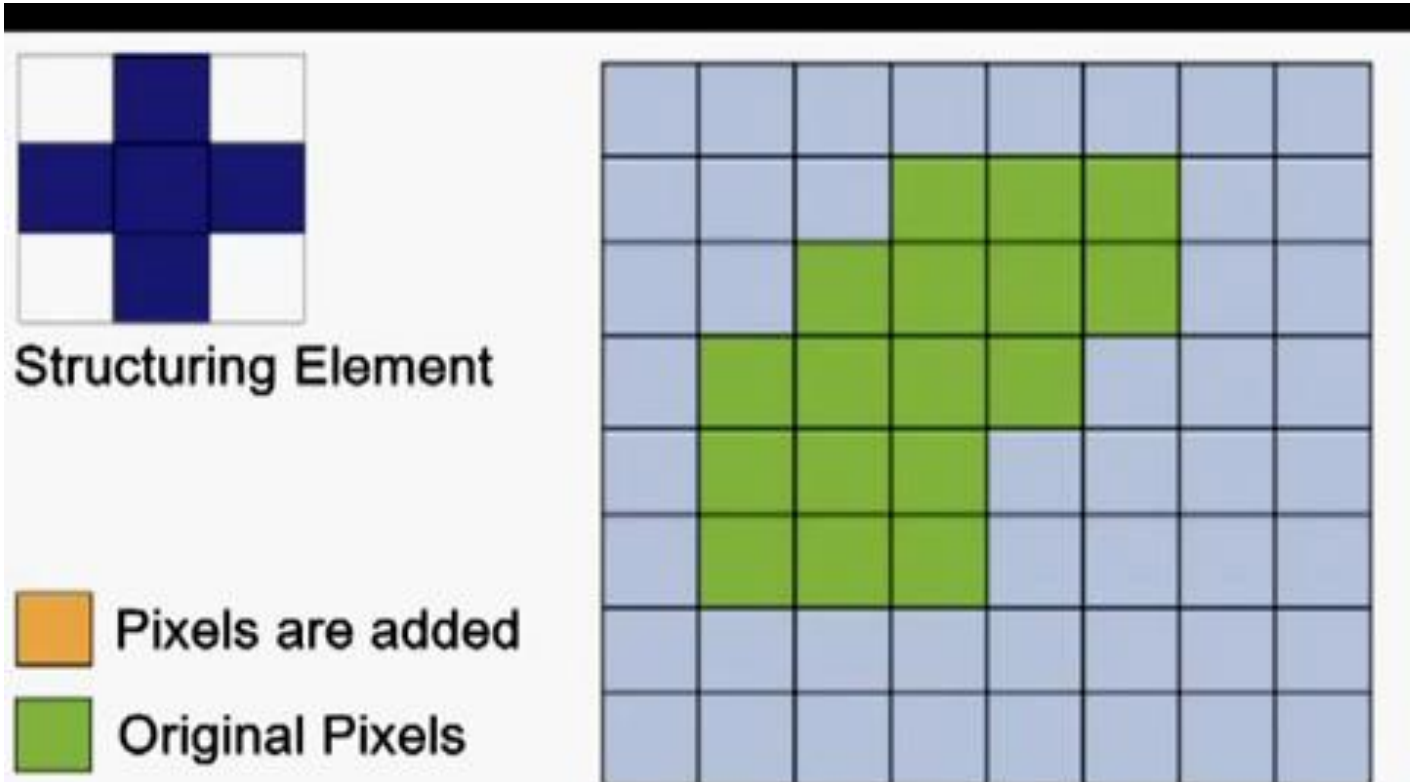
- The dilation of A by B is the set consisting of all the **structuring element "origin" locations** where the translated B overlaps at least one element of A

Structuring Element



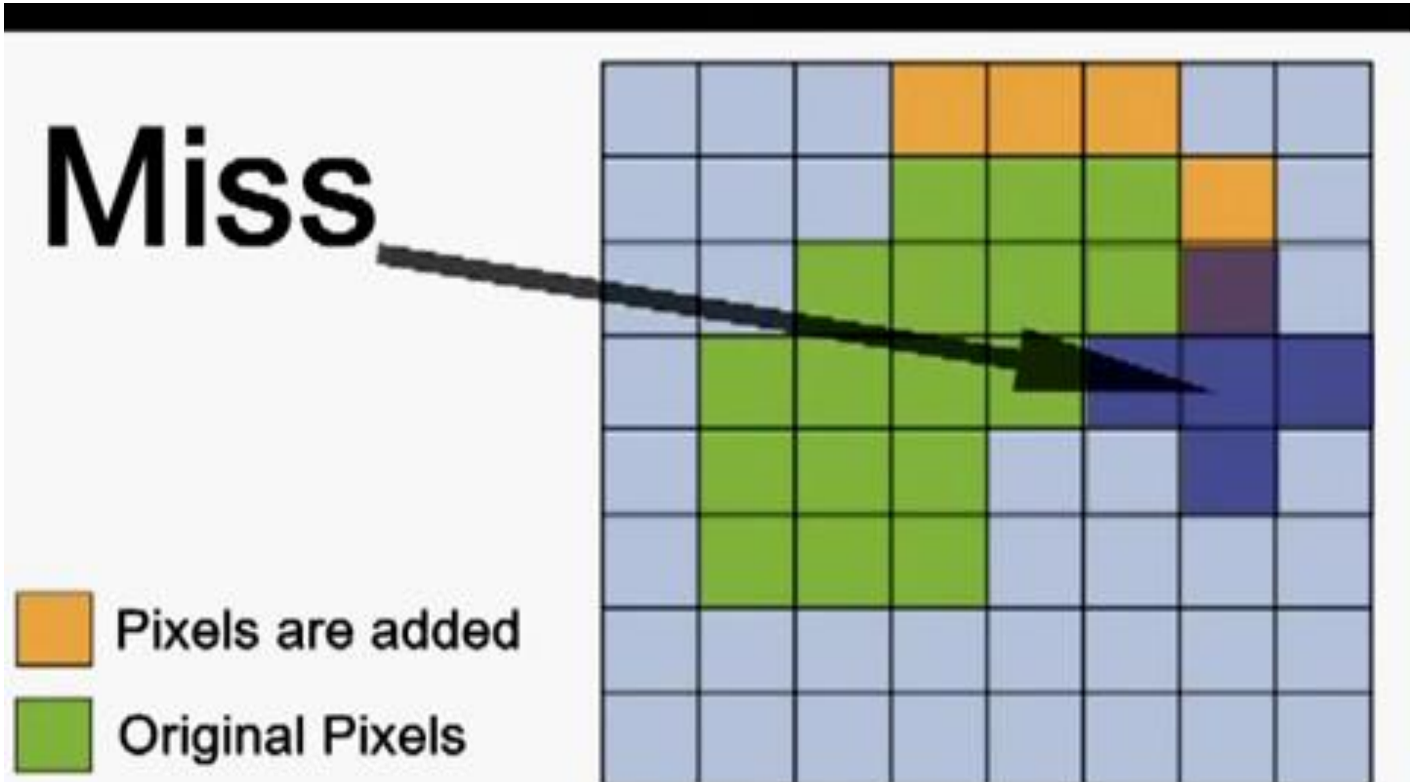
Dilation

- The dilation of A by B is the set consisting of all the **structuring element "origin" locations** where the translated B overlaps at least one element of A



Dilation

- The dilation of A by B is the set consisting of all the **structuring element “origin” locations** where the translated B overlaps at least one element of A



Dilation

- Dilation can be formally defined using the following set operation:

$$A \oplus B = \{(x, y) \in N^2 | \hat{B}_{(x,y)} \cap A \neq \emptyset\}$$

- In other words, the dilation of A by B is the set consisting of all the **structuring element origin locations** (x, y) where the translated B (indicated by $\hat{B}_{(x,y)}$) overlaps at least one element of A

Erosion

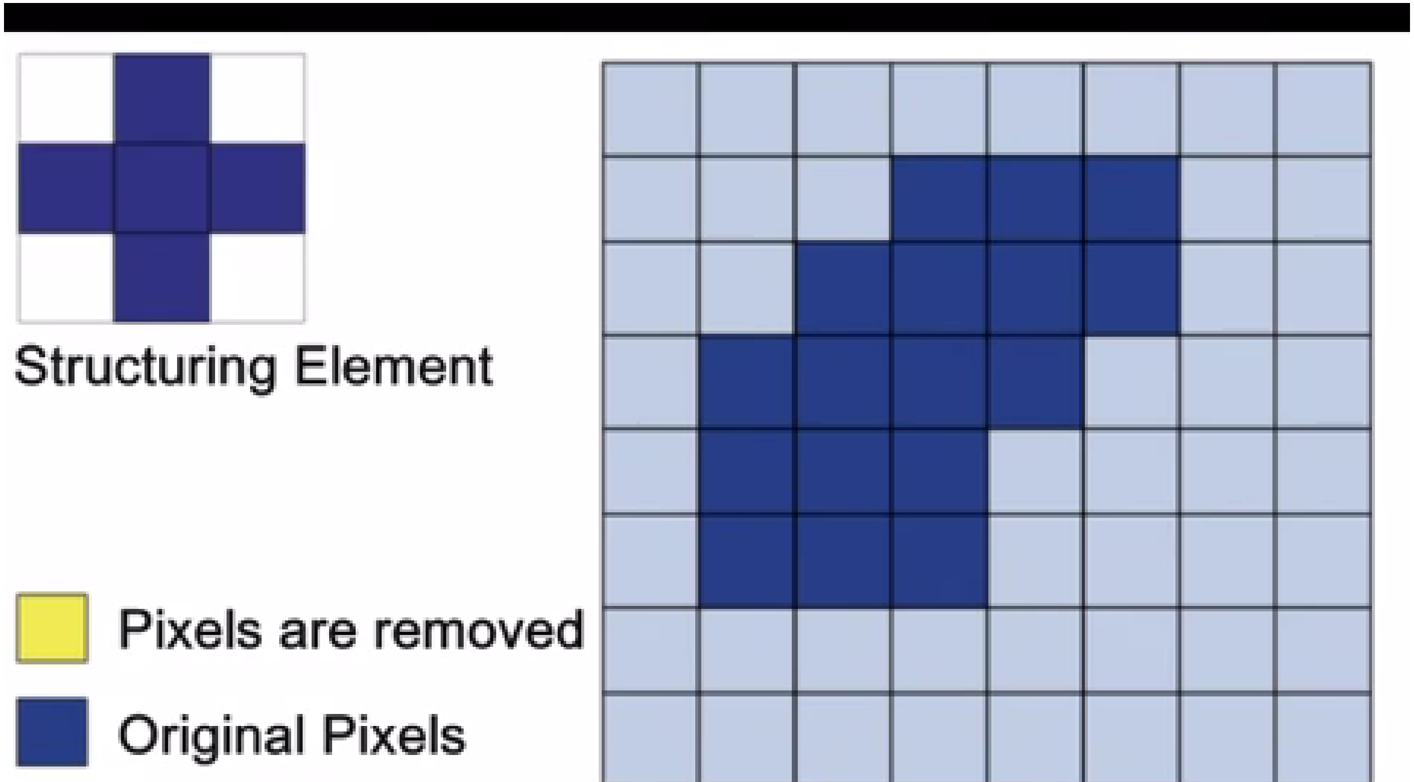
- Erosion is the opposite of dilation: it **shrinks** or **thins** objects in a binary image.
- As for dilation, the manner and amount of shrinking is controlled by a **structuring element**.
- Erosion can be formally defined using the following set operation:

$$A \ominus B = \{(x, y) \in N^2 | \hat{B}_{(x,y)} \subseteq A\}$$

- The erosion of A by B is the set consisting of all the **structuring element "origin" locations** where the translated B is a subset of A (or completely overlaps with of A).

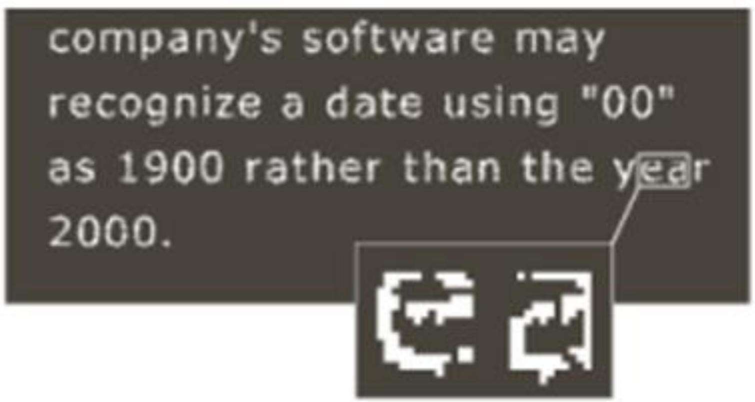
Erosion

- The erosion of A by B is the set consisting of all the **structuring element "origin" locations** where the translated B is a subset of A (or completely overlaps with of A).



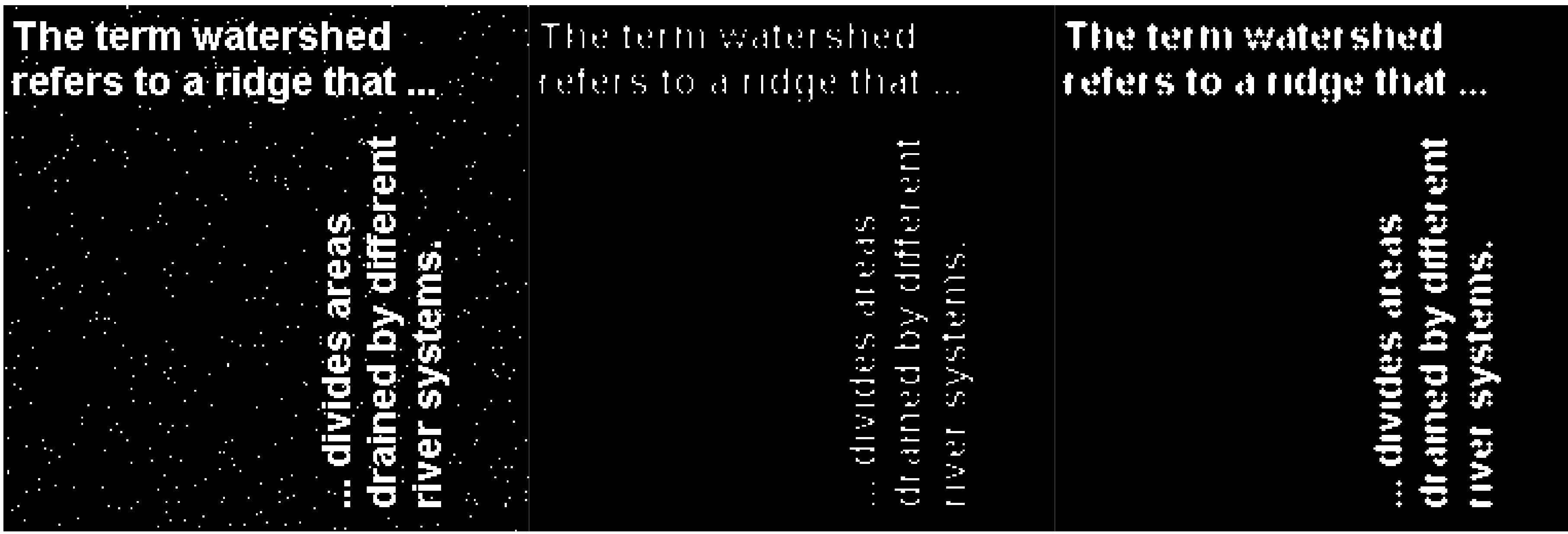
Dilation & Erosion have many applications

- Examples of dilation applied to text and fingerprint enhancement (preprocessing step before recognition)



Dilation & Erosion have many applications

- Examples of erosion and dilation applied consecutively to first remove noise and then enhance text:



Original noisy image | Eroded image (with disk of radius = 1) | Delated image with disk of radius = 1

SECTION 6.2

Properties of Sets

Properties of Sets

Theorem 6.2.1 Some Subset Relations

1. *Inclusion of Intersection:* For all sets A and B,

$$\text{(a) } A \cap B \subseteq A \quad \text{and} \quad \text{(b) } A \cap B \subseteq B.$$

2. *Inclusion in Union:* For all sets A and B,

$$\text{(a) } A \subseteq A \cup B \quad \text{and} \quad \text{(b) } B \subseteq A \cup B.$$

3. *Transitive Property of Subsets:* For all sets A, B, and C,

$$\text{if } A \subseteq B \text{ and } B \subseteq C, \text{ then } A \subseteq C.$$

Properties of Sets

Procedural Versions of Set Definitions

Let X and Y be subsets of a universal set U and suppose x and y are elements of U.

1. $x \in X \cup Y \quad \Leftrightarrow \quad x \in X$ or $x \in Y$
2. $x \in X \cap Y \quad \Leftrightarrow \quad x \in X$ and $x \in Y$
3. $x \in X - Y \quad \Leftrightarrow \quad x \in X$ and $x \notin Y$
4. $x \in X^c \quad \Leftrightarrow \quad x \notin X$
5. $(x, y) \in X \times Y \quad \Leftrightarrow \quad x \in X$ and $y \in Y$

Exercise – *Proof of a Subset Relation*

Prove that for all sets A and B, $A \cap B \subseteq A$.

Solution:

Let x is any element of $A \cap B$.

Then $x \in A$ and $x \in B$ by definition of intersection.

In particular, $x \in A$ and thus $A \cap B \subseteq A$.

Set Identities

Theorem 6.2.2 Set Identities

Let all sets referred to below be subsets of a universal set U.

1. *Commutative Laws:* For all sets A and B,

$$\text{(a) } A \cup B = B \cup A \quad \text{and} \quad \text{(b) } A \cap B = B \cap A.$$

2. *Associative Laws:* For all sets A, B, and C,

$$\text{(a) } (A \cup B) \cup C = A \cup (B \cup C) \quad \text{and}$$
$$\text{(b) } (A \cap B) \cap C = A \cap (B \cap C).$$

3. *Distributive Laws:* For all sets, A, B, and C,

$$\text{(a) } A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{and}$$
$$\text{(b) } A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

4. *Identity Laws:* For all sets A,

$$\text{(a) } A \cup \emptyset = A \quad \text{and} \quad \text{(b) } A \cap U = A.$$

5. *Complement Laws:*

$$\text{(a) } A \cup A^c = U \quad \text{and} \quad \text{(b) } A \cap A^c = \emptyset.$$

6. *Double Complement Law:* For all sets A,

Set Identities

3. *Distributive Laws:* For all sets, A, B, and C,

$$\text{(a) } A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{and}$$
$$\text{(b) } A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

4. *Identity Laws:* For all sets A,

$$\text{(a) } A \cup \emptyset = A \quad \text{and} \quad \text{(b) } A \cap U = A.$$

5. *Complement Laws:*

$$\text{(a) } A \cup A^c = U \quad \text{and} \quad \text{(b) } A \cap A^c = \emptyset.$$

6. *Double Complement Law:* For all sets A,

$$(A^c)^c = A.$$

7. *Idempotent Laws:* For all sets A,

$$\text{(a) } A \cup A = A \quad \text{and} \quad \text{(b) } A \cap A = A.$$

8. *Universal Bound Laws:* For all sets A,

$$\text{(a) } A \cup U = U \quad \text{and} \quad \text{(b) } A \cap \emptyset = \emptyset.$$

9. *De Morgan's Laws:* For all sets A and B,

$$\text{(a) } (A \cup B)^c = A^c \cap B^c \quad \text{and} \quad \text{(b) } (A \cap B)^c = A^c \cup B^c.$$

Example – *Proof of a Distributive Law*

Prove that for all sets A, B, and C,

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

Solution:

Suppose that A, B, and C are arbitrary sets. We must prove that

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C) \quad (1)$$

and that

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C). \quad (2)$$

Solution – *Proof of a Distributive Law*

First, we prove that

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C) \quad (1)$$

Let x be an arbitrary element in $A \cup (B \cap C)$.

By definition of union, $x \in A$ or $x \in B \cap C$.

Case 1: $x \in A$

By definition of union, $x \in A \cup B$ and $x \in A \cup C$.

By definition of intersection, $x \in (A \cup B) \cap (A \cup C)$.

Case 2: $x \in B \cap C$

By definition of intersection, $x \in B$ and $x \in C$.

By definition of union, $x \in A \cup B$ and $x \in A \cup C$.

By definition of intersection, $x \in (A \cup B) \cap (A \cup C)$.

Solution – *Proof of a Distributive Law*

Next, we prove that

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C). \quad (2)$$

Let x be an arbitrary element in $(A \cup B) \cap (A \cup C)$.

By definition of intersection, $x \in A \cup B$ and $x \in A \cup C$.

Case 1: $x \in A$

By the definition of union, $x \in A \cup (B \cap C)$.

Case 2: $x \notin A$

Since $x \in A \cup B$ and $x \in A \cup C$, $x \in B$ and $x \in C$.

By definition of intersection, $x \in B \cap C$.

By definition of union, $x \in A \cup (B \cap C)$.

“Algebraic” Proofs of Set Identities

Given the commutative laws, associative laws, distributive laws, identity laws, and complement,
any other identity involving only unions, intersections, and complements can be proven.

With the addition of complements of U and Ø, the set difference law, any set identity involving unions, intersections, complements, and set differences can be established.

Example – *Deriving a Set Identity Using Properties of ∅*

Construct an algebraic proof that for all sets *A* and *B*,

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

Solution – *Deriving a Set Identity Using Properties of ∅*

Solution: Suppose *A* and *B* are any sets.

$A - (A \cap B) = A \cap (A \cap B)^c$ by the set difference law

$= A \cap (A^c \cup B^c)$ by De Morgan's laws

$A - (A \cap B) = A \cap (A \cap B)^c$ by the set difference law

$= A \cap (A^c \cup B^c)$ by De Morgan's laws

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

$= \emptyset \cup (A \cap B^c)$ by the complement law

$= (A \cap B^c) \cup \emptyset$ by the commutative law

$= A \cap B^c$ by the identity law for $\cup$

$= A \cap (A^c \cup B^c)$ by De Morgan's laws

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

$= A \cap (A^c \cup B^c)$ by De Morgan's laws

$\cup$

The Empty Set

Theorem 6.2.4 A Set with No Elements Is a Subset of Every Set

If E is a set with no elements and A is any set, then $E \subseteq A$.

Corollary 6.2.5 Uniqueness of the Empty Set

There is only one set with no elements.

Element Method for Proving a Set Equals the Empty Set

To prove that a set X is equal to the empty set $\emptyset$, prove that X has no elements. To do this, suppose X has an element and derive a contradiction.

Example – *A Proof for a Conditional Statement*

Prove that for all sets A, B, and C, if $A \subseteq B$ and $B \subseteq C^c$, then $A \cap C = \varnothing$.

Solution:

Suppose A, B, and C are arbitrarily chosen sets that satisfy the conditions $A \subseteq B$ and $B \subseteq C^c$.

Suppose there is an element $x \in A \cap C$.

By definition of intersection, $x \in A$ and $x \in C$.
Since $A \subseteq B$, $x \in B$ by definition of subset.
Since $B \subseteq C^c$, then $x \in C^c$ by definition of subset.

By definition of complement, $x \notin C$. Thus, $x \in C$ and $x \notin C$, which is a contradiction.
We can conclude that there is no such element x.

SECTION 6.3

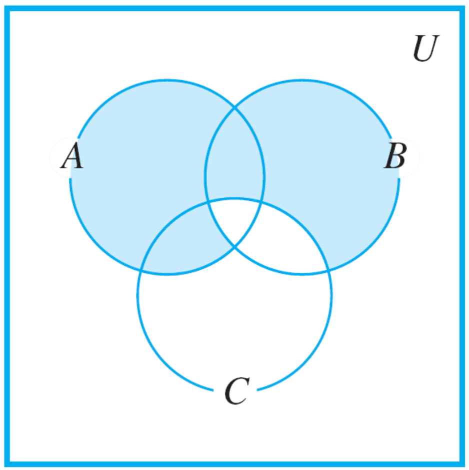
Disproofs, Algebraic Proofs, and Boolean Algebras

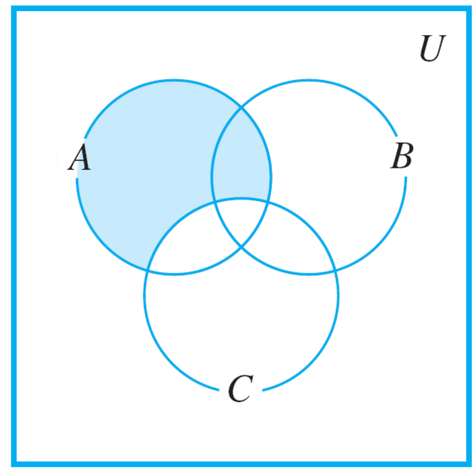
Exercise – *Finding a Counterexample for a Set Identity*

Is it true that for all sets A, B, and C:

$$(A - B) \cup (B - C) = A - C \quad ?$$

Solution:





No. The example above is a **counterexample** for which the identity does not hold; indeed,

$x \in B - C$ and thus $x \in (A - B) \cup (B - C)$

but clearly, $x \notin A - C$.

Power Sets

- **Definition**

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

Exercise – *Power Set of a Set*

Find the power set of the set $\{x, y\}$, i.e., find $\mathscr{P}(\{x, y\})$.

How many elements does it contain?

Solution:

$$\mathscr{P}(\{x, y\}) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}.$$

It contains 4 elements.

The Number of Subsets of a Set

Theorem 6.3.1

For all integers $n \geq 0$, if a set X has n elements, then $\mathscr{P}(X)$ has 2^n elements.

Proof (by mathematical induction):

Let the property *P*(*n*) be the sentence

Any set with *n* elements has 2^n subsets. $\leftarrow P(n)$

***P*(0):**

The only set with zero elements is the empty set, a
only subset of the empty set is itself. Thus, any set with 1
element has $2^0 = 1$ subsets.

The Number of Subsets of a Set

***P*(*k*) → *P*(*k* + 1):**

Let X be a set with $k + 1$ elements. Since $k + 1 \geq 1$, X is not empty and we may pick an element $z \in X$.

Observe that any subset of X either contains z or not. Moreover, any subset of $A = X - \{z\}$ can be matched up with a subset that is $A \cup \{z\}$.

Thus, there are as many subsets of X that contain z as do not. We get that

$$\text{the number of subsets of } X - \{z\} = 2^k \qquad \text{by inductive hypothesis.}$$

$$\begin{aligned}\text{the number of subsets of } X &= 2 \cdot (\text{the number of subsets of } X - \{z\}) \\ &= 2 \cdot (2^k) \\ &= 2^{k+1}\end{aligned}$$

Example – The Number of Subsets of a Set

For instance, if $X = \{x, y, z\}$, the following table shows the correspondence between subsets of X that do not contain z and subsets of X that contain z.

Subsets of X That Do Not Contain z		**Subsets of X That Contain z**
$\emptyset$	$\longleftrightarrow$	$\emptyset \cup \{z\} = \{z\}$
$\{x\}$	$\longleftrightarrow$	$\{x\} \cup \{z\} = \{x, z\}$
$\{y\}$	$\longleftrightarrow$	$\{y\} \cup \{z\} = \{y, z\}$
$\{x, y\}$	$\longleftrightarrow$	$\{x, y\} \cup \{z\} = \{x, y, z\}$

SECTION 6.4

Boolean Algebras, Russell’s Paradox, and the Halting Problem

Boolean Algebras, Russell's Paradox, and the Halting Problem

Logical Equivalences	**Set Properties**
For all statement variables p, q, and r:	For all sets A, B, and C:
a. $p \vee q \equiv q \vee p$ b. $p \wedge q \equiv q \wedge p$	a. $A \cup B = B \cup A$ b. $A \cap B = B \cap A$
a. $p \wedge (q \wedge r) \equiv p \wedge (q \wedge r)$ b. $p \vee (q \vee r) \equiv p \vee (q \vee r)$	a. $A \cup (B \cup C) \equiv A \cup (B \cup C)$ b. $A \cap (B \cap C) \equiv A \cap (B \cap C)$
a. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ b. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	a. $A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C)$ b. $A \cup (B \cap C) \equiv (A \cup B) \cap (A \cup C)$
a. $p \vee \mathbf{c} \equiv p$ b. $p \wedge \mathbf{t} \equiv p$	a. $A \cup \emptyset = A$ b. $A \cap U = A$

Logical Equivalences	Set Properties
b. $p \vee (q \vee r) \equiv p \vee (q \vee r)$	b. $A \cap (B \cap C) \equiv A \cap (B \cap C)$
a. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ b. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	a. $A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C)$ b. $A \cup (B \cap C) \equiv (A \cup B) \cap (A \cup C)$
a. $p \vee \mathbf{c} \equiv p$ b. $p \wedge \mathbf{t} \equiv p$	a. $A \cup \emptyset = A$ b. $A \cap U = A$
a. $p \vee \sim p \equiv \mathbf{t}$ b. $p \wedge \sim p \equiv \mathbf{c}$	a. $A \cup A^c = U$ b. $A \cap A^c = \emptyset$
$\sim(\sim p) \equiv p$	$(A^c)^c = A$
a. $p \vee p \equiv p$ b. $p \wedge p \equiv p$	a. $A \cup A = A$ b. $A \cap A = A$
a. $p \vee \mathbf{t} \equiv \mathbf{t}$ b. $p \wedge \mathbf{c} \equiv \mathbf{c}$	a. $A \cup U = U$ b. $A \cap \emptyset = \emptyset$
a. $\sim(p \vee q) \equiv \sim p \wedge \sim q$ b. $\sim(p \wedge q) \equiv \sim p \vee \sim q$	a. $(A \cup B)^c = A^c \cap B^c$ b. $(A \cap B)^c = A^c \cup B^c$

Boolean Algebras, Russell's Paradox, and the Halting Problem

$\vee$ (*or*) corresponds to $\cup$ (union)
$\wedge$ (*and*) corresponds to $\cap$ (intersection)
t (tautology) corresponds to *U* (universal set)
c (contradiction) corresponds to ∅ (empty set)
~ (negation) corresponds to ^{c} (complementation)

→ Structure of the set of statement forms with operations $\vee$ and $\wedge$ is essentially identical to the structure of the set of subsets of a universal set with operations $\cup$ and $\cap$.

Both are special cases of the same general structure known as a *Boolean algebra*.

Boolean Algebras, Russell's Paradox, and the Halting Problem

- **Definition: Boolean Algebra**

A **Boolean algebra** is a set B together with two operations, generally denoted $+$ and $\cdot$, such that for all a and b in B both $a + b$ and $a \cdot b$ are in B and the following properties hold:

1. *Commutative Laws:* For all a and b in B,

$$\text{(a) } a + b = b + a \quad \text{and} \quad \text{(b) } a \cdot b = b \cdot a.$$

2. *Associative Laws:* For all a, b, and c in B,

$$\text{(a) } (a + b) + c = a + (b + c) \quad \text{and} \quad \text{(b) } (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

3. *Distributive Laws:* For all a, b, and c in B,

$$\text{(a) } a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad \text{(b) } a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

4. *Identity Laws:* There exist distinct elements 0 and 1 in B such that for all a in B,

$$\text{(a) } a + 0 = a \quad \text{and} \quad \text{(b) } a \cdot 1 = a.$$

5. *Complement Laws:* For each a in B, there exists an element in B, denoted $\overline{a}$ and called the **complement** or **negation** of a, such that

$$\text{(a) } a + \overline{a} = 1 \quad \text{and} \quad \text{(b) } a \cdot \overline{a} = 0.$$

Theorem 6.4.1 Properties of a Boolean Algebra

Let B be any Boolean algebra.

1. *Uniqueness of the Complement Law:* For all a and x in B, if $a + x = 1$ and $a \cdot x = 0$ then $x = \overline{a}$.
2. *Uniqueness of* 0 *and* 1: If there exists x in B such that $a + x = a$ for all a in B, then $x = 0$, and if there exists y in B such that $a \cdot y = a$ for all a in B, then $y = 1$.
3. *Double Complement Law:* For all $a \in B$, $\overline{(\overline{a})} = a$.

4. *Idempotent Law:* For all $a \in B$,

$$\text{(a) } a + a = a \quad \text{and} \quad \text{(b) } a \cdot a = a.$$

5. *Universal Bound Law:* For all $a \in B$,

$$\text{(a) } a + 1 = 1 \quad \text{and} \quad \text{(b) } a \cdot 0 = 0.$$

6. *De Morgan's Laws:* For all a and $b \in B$,

$$\text{(a) } \overline{a + b} = \overline{a} \cdot \overline{b} \quad \text{and} \quad \text{(b) } \overline{a \cdot b} = \overline{a} + \overline{b}.$$

7. *Absorption Laws:* For all a and $b \in B$,

$$\text{(a) } (a + b) \cdot a = a \quad \text{and} \quad \text{(b) } (a \cdot b) + a = a.$$

8. *Complements of* 0 *and* 1:

$$\text{(a) } \overline{0} = 1 \quad \text{and} \quad \text{(b) } \overline{1} = 0.$$

All parts of the definition of a Boolean algebra contain paired statements. For example the identity laws state that for all a in B,

(a) $a + 0 = a$ and (b) $a \cdot 1 = a$.

Each of the paired statements can be obtained from the other by interchanging all + and · signs and 1s and 0s. Such interchanges transform any Boolean identity into its dual identity.

It can be proved that the dual of any Boolean identity is also an identity. This fact is often called the duality principle for a Boolean algebra.

Example – *Proof of the Double Complement Law*

Theorem 6.4.1(3) Double Complement Law

For all elements a in a Boolean algebra B, $\overline{(\overline{a})} = a$.

Proof:

Suppose B is a Boolean algebra and a is any element of B.

$$\begin{aligned} \overline{a} + a &= a + \overline{a} && \text{by the commutative law} \\ &= 1 && \text{by the complement law for 1} \end{aligned}$$

and

$$\begin{aligned} \overline{a} \cdot a &= a \cdot \overline{a} && \text{by the commutative law} \\ &= 0 && \text{by the complement law for 0.} \end{aligned}$$

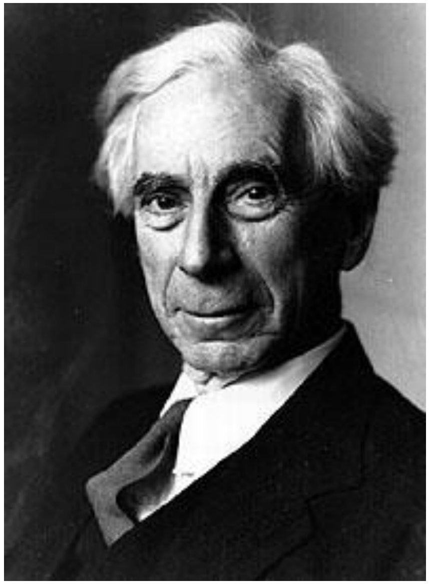
Thus, a satisfies the two equations (S.64, Law 5) for the complement of $\overline{a}$. Since the complement is unique, $\overline{(\overline{a})} = a$.

Recall Cantor's definition of sets

A set is a "collection into a whole *M* of definite and separate objects of our intuition or our thought. These objects are called the elements of *M*."

At the beginning of 20th century, abstract set theory had gained such popularity that many mathematicians started to show that all mathematics could be built upon the foundation of set theory. Until English mathematician and philosopher Bertrand Russel (Nobel Prize in Literature, 1950) discovered a set that creates a paradox, thus "shaking" Cantor's definition of a set.

Russell's Paradox



Most sets are not elements of themselves. For instance, the set of all integers is not an integer.

However, a set *could be* an element of itself. For instance, the set of all abstract ideas might be considered an abstract idea.

If we are allowed to use any defining property of a set, let *S* be the set of all sets that are not elements of themselves:

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

Russell's Paradox

Is S an element of itself? The answer is neither yes nor no.

If $S \in S$, then S satisfies the defining property for S, and hence $S \notin S$, which contradicts the assumption.

But if $S \notin S$, then S is a set such that $S \notin S$ and so S satisfies the defining property for S,

which implies that $S \in S$, which contradicts the assumption.

Thus, neither $S \in S$ nor $S \notin S$ holds.

Russell devised a puzzle, the barber puzzle, whose solution exhibits the same logic as his paradox.

Exercise – *The Barber Puzzle*

In a 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?

Solution:

Neither yes nor no.

If the barber shaves himself, he is a member of the class of men who shave themselves, so the barber does *not* shave himself.

If the barber does not shave himself, he belongs to the class of men who do not shave themselves. The barber shaves every man in this class, so the barber *does* shave himself.

Russell’s Paradox

We conclude that ”The barber shaves himself” is neither true nor false.

The sentence arose from a description of a situation.

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

If the situation actually existed, then the sentence would have to be true or false. Thus, the situation described in the puzzle cannot exist.

The conclusion for Russell’s paradox itself is that S is not a set. (If it were a set, then it either would be either an element of itself or not)

Russell’s Paradox

Despite Russel’s paradox, Cantor’s definition still holds. In 1931, Kurt Gödel showed that it is not possible to prove, mathematically, that mathematics is free of contradictions!

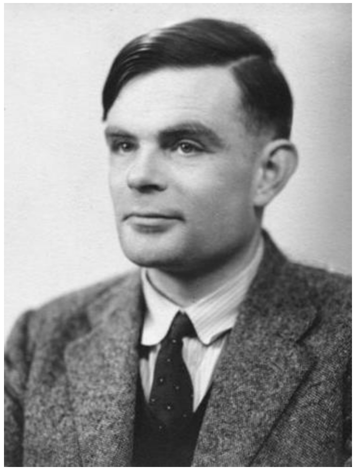
The Halting Problem

Given a computer program, it would be useful to be able to preprocess a program and its data set by running it through a checking program that determines whether execution of the given program with the given data set would result in an infinite loop.

Can an algorithm for such a program be written?

The Halting Problem

Can an algorithm be written that will accept any algorithm *X* and any data set *D* as input and will print “halts” or “loops forever” to indicate whether *X* terminates in a finite number of steps or loops forever when run with data set *D*?



In the 1930s, Alan Turing proved that the answer to this question is No.

Theorem 6.4.2

There is no computer algorithm that will accept any algorithm X and data set D as input and then will output “halts” or “loops forever” to indicate whether or not X terminates in a finite number of steps when X is run with data set D.