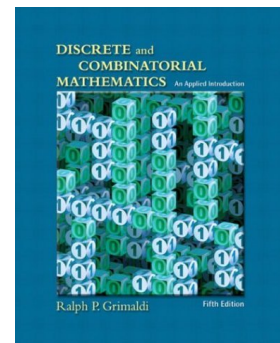
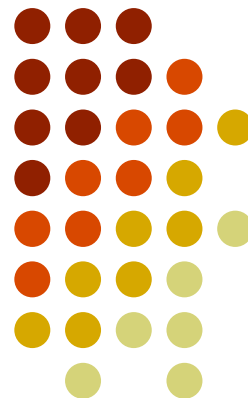


# Discrete Mathematics

## -- Chapter 3: Set Theory



*Hung-Yu Kao (高宏宇)*  
*Department of Computer Science and Information Engineering,*  
*National Cheng Kung University*

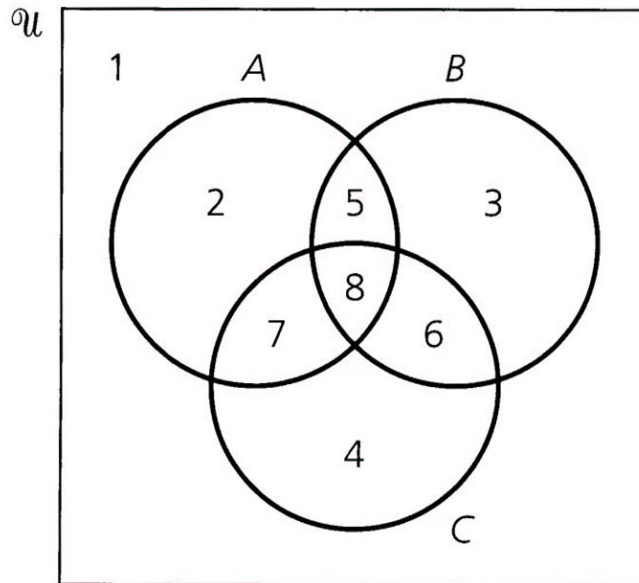




# Outline

- 3.1 Set and Subsets
- 3.2 Set Operations and the Laws of Set Theory
- 3.3 Counting and Venn Diagrams
- 3.4 A First Word on Probability
- 3.5 The Axioms of Probability
- 3.6 Conditional Probability: Independence
- 3.7 Discrete Random Variables

# Why Set?



- Sets are the most simple, yet non-trivial structures in mathematics.

- Many other mathematical objects and properties can be defined by them.

- For us, sets are useful to understand the principles of counting and probability theory.



## 3.1 Set and Subsets

- **Set**: should be a well-defined collection of objects.
- **Elements (members)**: These objects are called elements or members of the set.
  - could be another set,  $1 \neq \{1\} \neq \{\{1\}\}$
- Capital letters represent sets:  $A, B, C$   
lowercase letters represent elements:  $x, y$ 
  - E.g.,  $x \in A, y \notin B$
- A set can be designated by listing its elements within set braces “{“, ”}”.
  - E.g.,  $A = \{1, 2, 3, 4, 5\}, B = \{x \mid x \text{ is an integer, and } 1 \leq x \leq 5\}$
- **Cardinality (size)**:  $|A|$  denotes the number of elements in  $A$ .
  - for finite sets



# Set and Subsets

- **Universe (Universe of discourse):**  $\mathcal{U}$  denotes the range of all elements to form any set.
- Definition 3.1: If  $C$  and  $D$  are sets from a universe  $\mathcal{U}$ 
  - **Subset:**  $C \subseteq D$  ( $D \supseteq C$ ), if every element of  $C$  is an element of  $D$ .
  - **Proper subset:**  $C \subset D$  ( $D \subset C$ ) , if, in addition,  $D$  contains an element that is not in  $C$ .
  - $C \subseteq D \Leftrightarrow \forall x [x \in C \Rightarrow x \in D]$

$$\begin{aligned} C \not\subseteq D & \text{ (i.e., } C \text{ is not a subset of } D\text{)} \\ & \Leftrightarrow \neg \forall x [x \in C \Rightarrow x \in D] \\ & \Leftrightarrow \exists x \neg [x \in C \Rightarrow x \in D] \\ & \Leftrightarrow \exists x \neg [\neg(x \in C) \vee x \in D] \\ & \Leftrightarrow \exists x [\neg \neg(x \in C) \wedge \neg(x \in D)] \\ & \Leftrightarrow \exists x [x \in C \wedge x \notin D] \end{aligned}$$



# Set and Subsets

- Definition 3.2: The sets  $C$  and  $D$  are equal for a given universe  $\mathcal{U}$ ,  
$$C = D \Leftrightarrow (C \subseteq D) \wedge (D \subseteq C)$$
- Let  $A, B, C \subseteq \mathcal{U}$ ,
  - a) If  $A \subseteq B$  and  $B \subseteq C$ , then  $A \subseteq C$
  - b) If  $A \subset B$  and  $B \subseteq C$ , then  $A \subset C$
  - c) If  $A \subseteq B$  and  $B \subset C$ , then  $A \subset C$
  - d) If  $A \subset B$  and  $B \subset C$ , then  $A \subset C$
- Let  $\mathcal{U} = \{1, 2, 3, 4, 5\}$  with  $A = \{1, 2, 3\}$ ,  $B = \{3, 4\}$ , and  $C = \{1, 2, 3, 4\}$ . Then the following subset relations hold:
  - a)  $A \subseteq C$    b)  $A \subset C$    c)  $B \subset C$
  - d)  $A \subseteq A$    e)  $B \not\subseteq A$    f)  $A \not\subset A$   $\leftarrow$  *A is not a proper subset of A*



# Set and Subsets

- **Null set (empty set)**,  $\emptyset$  or  $\{ \}$ : is the set containing no elements.
  - $|\emptyset|=0$  but  $\{0\} \neq \emptyset$
  - $\emptyset \neq \{\emptyset\}$
- **Power set**,  $P(A)$ : is the collection (set) of all subsets of the set  $A$  from universe  $\mathcal{U}$ .
- Example:  $A = \{1, 2, 3\}$ 
  - $P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$
- For any finite set  $A$  with  $|A|=n$ 
  - $A$  has  $2^n$  subsets and  $|P(A)| = 2^n$
  - There are  $\binom{n}{k}$  subsets of size  $k$ ,  $0 \leq k \leq n$
  - Counting the subsets of  $A$  (binomial theorem)

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = \sum_{k=0}^n \binom{n}{k} = 2^n$$



# Set and Subsets

- Theorem 3.2

For any universe  $\mathcal{U}$ , let  $A \subseteq \mathcal{U}$ . Then  $\emptyset \subseteq A$ , and if  $A \neq \emptyset$ , then  $\emptyset \subset A$ .

**Proof:** If the first result is not true, then  $\emptyset \not\subseteq A$ , so there is an element  $x$  from the universe with  $x \in \emptyset$  but  $x \notin A$ . But  $x \in \emptyset$  is impossible. So we reject the assumption  $\emptyset \not\subseteq A$  and find that  $\emptyset \subseteq A$ . In addition, if  $A \neq \emptyset$ , then there is an element  $a \in A$  (and  $a \notin \emptyset$ ), so  $\emptyset \subset A$ .

$$\phi \subseteq \{\phi\} ? \text{ T } \quad \phi \subset \{\phi\} ? \text{ T }$$

$$\phi \subseteq \phi ? \text{ T } \quad \phi \subset \phi ? \text{ F }$$

$\phi \subseteq \{\phi\}$  :  $\phi$  is included in  $\{\phi\}$

$\phi \not\subset \phi$  :  $\phi$  is not subset of  $\phi$





# Set and Subsets

## ● Ex 3.11

26

Composition 有考慮位置的順序性(partition 無)

Table 3.1

Composition of 7		Determining Subset of {1, 2, 3, 4, 5, 6}	
(i)	$1 + 1 + 1 + 1 + 1 + 1 + 1$	(i)	$\emptyset$
(ii)	$1 + 2 + 1 + 1 + 1 + 1$	(ii)	$\{2\}$
(iii)	$1 + 1 + 3 + 1 + 1$	(iii)	$\{3, 4\}$
(iv)	$2 + 3 + 2$	(iv)	$\{1, 3, 4, 6\}$
(v)	$4 + 3$	(v)	$\{1, 2, 3, 5, 6\}$
(vi)	$7$	(vi)	$\{1, 2, 3, 4, 5, 6\}$

3 + 4 : 1, 2, 4, 5, 6



# Set and Subsets

## • Ex 3.12

Let  $A = \{x, a_1, a_2, \dots, a_n\}$  and consider all subsets of  $A$  that contain  $r$  elements.

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

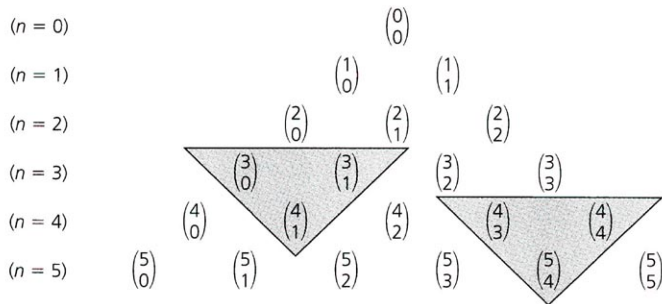


Figure 3.3

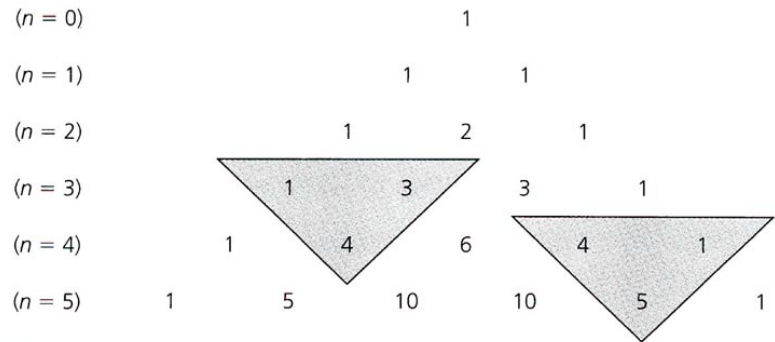


Figure 3.4



# Set and Subsets

- **Ex 3.13** the number of nonnegative integer solutions of the inequality  $x_1 + x_2 + \cdots + x_6 < 10$

$\forall k, 0 \leq k \leq 9$ , the number of solution to  $x_1 + x_2 + \cdots + x_6 = k$  is

$$\binom{6+k-1}{k} = \binom{5+k}{k}$$

in chapter 1,  $\binom{7+9-1}{9} = \binom{15}{9}$

$$\begin{aligned} & \binom{5}{0} + \binom{6}{1} + \binom{7}{2} + \binom{8}{3} + \cdots + \binom{14}{9} \\ &= \left[ \binom{6}{0} + \binom{6}{1} \right] + \binom{7}{2} + \binom{8}{3} + \cdots + \binom{14}{9}, \quad \text{since } \binom{5}{0} = 1 = \binom{6}{0} \\ &= \left[ \binom{7}{1} + \binom{7}{2} \right] + \binom{8}{3} + \cdots + \binom{14}{9}, \quad \text{since } \binom{6}{0} + \binom{6}{1} = \binom{7}{1} \\ &= \left[ \binom{8}{2} + \binom{8}{3} \right] + \binom{9}{4} + \cdots + \binom{14}{9}, \quad \text{since } \binom{7}{1} + \binom{7}{2} = \binom{8}{2} \\ &= \left[ \binom{9}{3} + \binom{9}{4} \right] + \cdots + \binom{14}{9} = \cdots = \binom{14}{8} + \binom{14}{9} = \binom{15}{9} = 5005. \end{aligned}$$



# Set and Subsets

$$\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$$

- a)  $\mathbf{Z}$  = the set of *integers* =  $\{0, 1, -1, 2, -2, 3, -3, \dots\}$  ✗  $N^+, N^0$
  - b)  $\mathbf{N}$  = the set of *nonnegative integers* or *natural numbers* =  $\{0, 1, 2, 3, \dots\}$
  - c)  $\mathbf{Z}^+$  = the set of *positive integers* =  $\{1, 2, 3, \dots\} = \{x \in \mathbf{Z} \mid x > 0\}$
  - d)  $\mathbf{Q}$  = the set of *rational numbers* =  $\{a/b \mid a, b \in \mathbf{Z}, b \neq 0\}$
  - e)  $\mathbf{Q}^+$  = the set of *positive rational numbers* =  $\{r \in \mathbf{Q} \mid r > 0\}$
  - f)  $\mathbf{Q}^*$  = the set of *nonzero rational numbers*
  - g)  $\mathbf{R}$  = the set of *real numbers*
  - h)  $\mathbf{R}^+$  = the set of *positive real numbers*
  - i)  $\mathbf{R}^*$  = the set of *nonzero real numbers*
  - j)  $\mathbf{C}$  = the set of *complex numbers* =  $\{x + yi \mid x, y \in \mathbf{R}, i^2 = -1\}$
  - k)  $\mathbf{C}^*$  = the set of *nonzero complex numbers*
  - l) For each  $n \in \mathbf{Z}^+$ ,  $\mathbf{Z}_n = \{0, 1, 2, \dots, n-1\}$
  - m) For real numbers  $a, b$  with  $a < b$ ,  $[a, b] = \{x \in \mathbf{R} \mid a \leq x \leq b\}$ ,  
 $(a, b) = \{x \in \mathbf{R} \mid a < x < b\}$ ,  $[a, b) = \{x \in \mathbf{R} \mid a \leq x < b\}$ ,  
 $(a, b] = \{x \in \mathbf{R} \mid a < x \leq b\}$ . The first set is called a *closed interval*, the second set an *open interval*, and the other two sets *half-open intervals*.
- $\mathbf{Z}^+ \subseteq \mathbf{Q}^+$

○  $\mathbf{R}^+ \cap \mathbf{C} = \mathbf{R}^+$

✗  $\mathbf{R}^+ \subseteq \mathbf{Q}$

✗  $\mathbf{Q}^* \cap \mathbf{Z} = \mathbf{Z}$

○  $\mathbf{Z}^+ \cup \mathbf{R}^+ = \mathbf{R}^+$

## 3.2 Set Operations and the Laws of Set Theory



- Definition 3.5: For  $A$  and  $B \subseteq \mathcal{U}$

a)  $A \cup B$  (the union of  $A$  and  $B$ ) =  $\{x \mid x \in A \vee x \in B\}$

b)  $A \cap B$  (the intersection of  $A$  and  $B$ ) =  $\{x \mid x \in A \wedge x \in B\}$

c)  $A \Delta B$  (the symmetric difference of  $A$  and  $B$ )

$$= \{x \mid (x \in A \vee x \in B) \wedge x \notin A \cap B\} = \{x \mid x \in A \cup B \wedge x \notin A \cap B\}$$

Union - intersection

- Definition 3.6: The sets  $S, T \subseteq \mathcal{U}$  are called disjoint (mutually disjoint), when  $S \cap T = \phi$ . 無交集

# Set Operations and the Laws of Set Theory



- Theorem 3.3: If  $S, T \subseteq \mathcal{U}$  are disjoint if and only if  $S \cup T = S \Delta T$

- Proof: (1)  $\underline{x \in S \cup T} \Rightarrow x \in S \cup x \in T$

But  $S$  and  $T$  disjoint, i.e.,  $x \notin S \cap T, \Rightarrow \underline{x \in S \Delta T}$

$$\therefore S \cup T \subseteq S \Delta T$$

$$(2) \underline{y \in S \Delta T} \Rightarrow y \in S \cup y \in T$$

$$\Rightarrow \underline{y \in S \cup T}$$

$$\therefore S \Delta T \subseteq S \cup T$$

$$\therefore S \cup T \subseteq S \Delta T \text{ and } S \Delta T \subseteq S \cup T$$

$$\therefore S \cup T = S \Delta T$$

*Prove the converse by the method of proof by contradiction*

# Set Operations and the Laws of Set Theory



補集

- Definition 3.7: For a set  $A \subseteq \mathcal{U}$ , the **complement** of  $A$ , denoted  $\mathcal{U} - A$  or  $\bar{A}$ , is given by  $\{x \mid x \in \mathcal{U} \wedge x \notin A\}$
- Definition 3.8: For  $A, B \subseteq \mathcal{U}$ , the (relative) complement of  $A$  in  $B$ , denoted  $B - A$  or, is given by  $\{x \mid x \in B \wedge x \notin A\}$  即  $B - A = B \cap \bar{A}$
- **Ex 3.18**: For  $\mathcal{U} = \mathbf{R}$ ,  $A = [1, 2]$ ,  $B = [1, 3)$ 
  - a)  $A = \{x \mid 1 \leq x \leq 2\} \subseteq \{x \mid 1 \leq x < 3\} = B$
  - b)  $A \cup B = ? = \{x \mid 1 \leq x < 3\} = B$
  - c)  $A \cap B = ? = \{x \mid 1 \leq x \leq 2\} = A$
  - d)  $\bar{B} = (-\infty, 1) \cup [3, +\infty) \subseteq (-\infty, 1) \cup (2, +\infty) = \bar{A}$
- Theorem 3.4: The following statements are equivalent:

$$(a) A \subseteq B \quad (b) A \cup B = B \quad (c) A \cap B = A \quad (d) \bar{B} \subseteq \bar{A}$$

$$(a) = (b) = (c) = (d)$$



# Sets and Logic

Logic and set theory go very well together.

The previous definitions can be made very succinct:

$x \notin A$  if and only if  $\neg(x \in A)$

$A \subseteq B$  if and only if  $(x \in A \rightarrow x \in B)$  is True

$x \in (A \cap B)$  if and only if  $(x \in A \wedge x \in B)$

$x \in (A \cup B)$  if and only if  $(x \in A \vee x \in B)$

$x \in A - B$  if and only if  $(x \in A \wedge x \notin B)$

$x \in A \Delta B$  if and only if  $(x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)$

$x \in \bar{A}$  if and only if  $\neg(x \in A)$

$X \in P(A)$  if and only if  $X \subseteq A$





# The Laws of Set Theory

1) Law of *Double Complement*:  $\overline{\overline{A}} = A$

2) *DeMorgan's Laws*:  $\begin{cases} \overline{A \cup B} = \overline{A} \cap \overline{B} \\ \overline{A \cap B} = \overline{A} \cup \overline{B} \end{cases}$  3) *Commutative Laws*:  $\begin{cases} A \cup B = B \cup A \\ A \cap B = B \cap A \end{cases}$

4) *Associative Laws*:  $\begin{cases} A \cup (B \cap C) = (A \cup B) \cap C \\ A \cap (B \cup C) = (A \cap B) \cup C \end{cases}$

5) *Distributive Laws*:  $\begin{cases} A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \end{cases}$

6) *Idempotent Laws*:  $\begin{cases} A \cup A = A \\ A \cap A = A \end{cases}$  7) *Identity Laws*:  $\begin{cases} A \cup \phi = A \\ A \cap U = A \end{cases}$

8) *Inverse Laws*:  $\begin{cases} A \cup \overline{A} = U \\ A \cap \overline{A} = \phi \end{cases}$  9) *Domination Laws*:  $\begin{cases} A \cup U = U \\ A \cap \phi = \phi \end{cases}$

10) *Absorption Laws*:  $\begin{cases} A \cup (A \cap B) = A \\ A \cap (A \cup B) = A \end{cases}$



# The Laws of Set Theory

- Ex 3.20

- Simplify the expression  $\overline{\overline{(A \cup B) \cap C} \cup \overline{B}}$

$$\overline{\overline{(A \cup B) \cap C} \cup \overline{B}}$$

$$= \overline{\overline{((A \cup B) \cap C)} \cap \overline{\overline{B}}}$$

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

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

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

$$= [(A \cup B) \cap B] \cap C$$

$$= B \cap C$$

Reasons

DeMorgan's Law

Law of Double Complement

Associative Law of Intersection

Commutative Law of Intersection

Associative Law of Intersection

Absorption Law

How about expressing  $\overline{A - B}$  in terms of  $\cup$  and  $\overline{\phantom{x}}$ ?  $\overline{A \cap \overline{B}} = \overline{A} \cup B$

# Set Operations and the Laws of Set Theory



- Definition 3.9: The **dual** of  $s$ ,  $s^d$  can be replaced mutually.
  - (1)  $\cup$  and  $\cap$  (2)  $\phi$  and  $\mathcal{U}$
- Theorem 3.5: **The Principle of Duality**, let  $s$  denote **a theorem** dealing with the equality of two set expressions. Then  $s^d$  is also a theorem.
- **Ex 3.19** : find a dual for statement  $A \subseteq B$  (Th. 3.4)
  - $A \cup B = B \rightarrow A \cap B = B$  (duality)  
But  $A \cap B = B \Leftrightarrow B \subseteq A$  (the dual of  $A \subseteq B$ )
  - or  $A \cap B = A \rightarrow A \cup B = A \Leftrightarrow B \subseteq A$

# Set Operations and the Laws of Set Theory

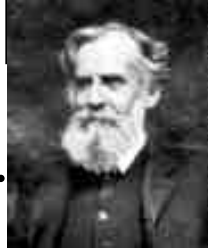


- Theorem 3.6: **Generalized DeMorgan's Laws**, let  $I$  be an index set, then

$$(1) \overline{\bigcup_{i \in I} A_i} = \bigcap_{i \in I} \overline{A_i} \quad (2) \overline{\bigcap_{i \in I} A_i} = \bigcup_{i \in I} \overline{A_i}$$

- Proof:

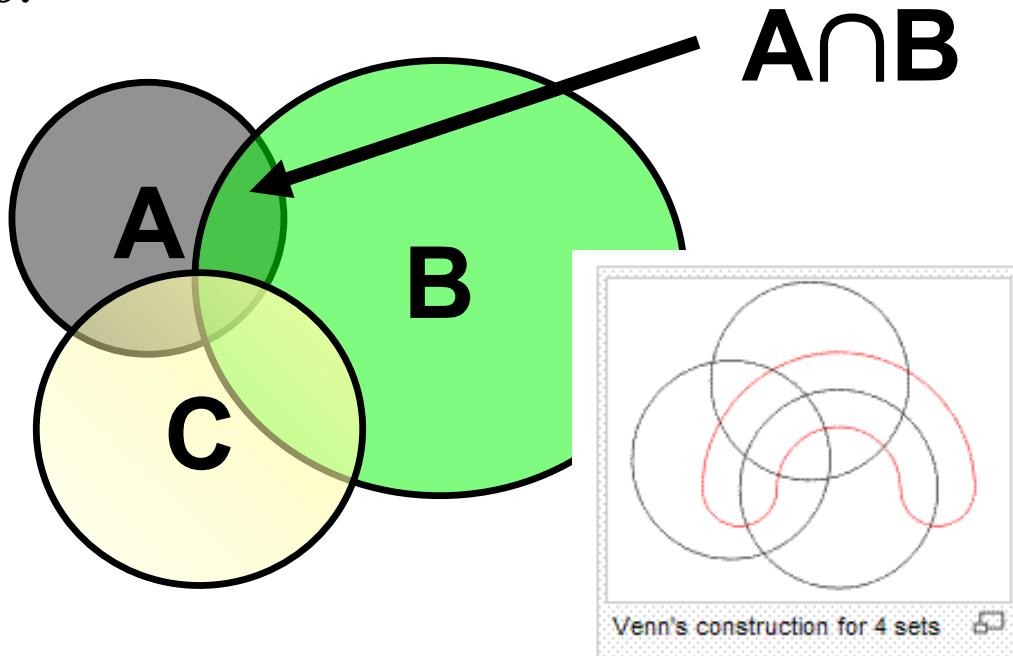
$$(1) x \in \overline{\bigcup_{i \in I} A_i} \Leftrightarrow x \notin \bigcup_{i \in I} A_i \Leftrightarrow x \notin A_i \text{ for all } i \in I \Leftrightarrow x \in \overline{A_i} \text{ for all } i \in I \Leftrightarrow x \in \bigcap_{i \in I} \overline{A_i}$$



John Venn  
(1834~1923)

## 3.3 Counting and Venn Diagrams

- **Venn diagrams** are used to depict the various unions, subsets, complements, intersections etc. of sets:



# Venn Diagrams

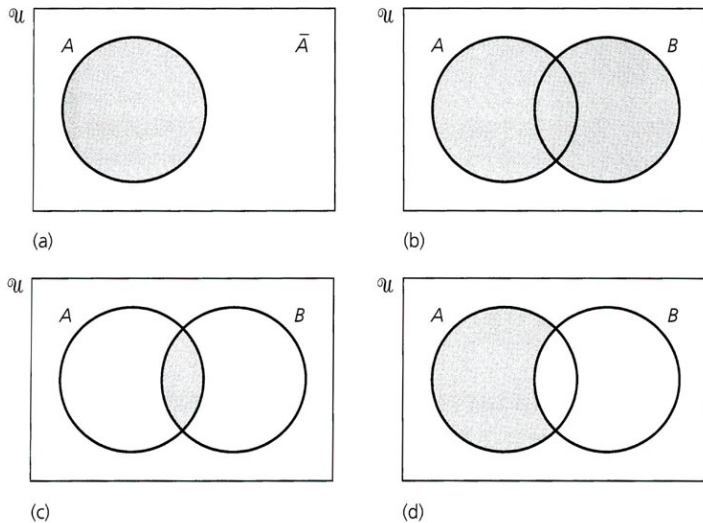


Figure 3.6

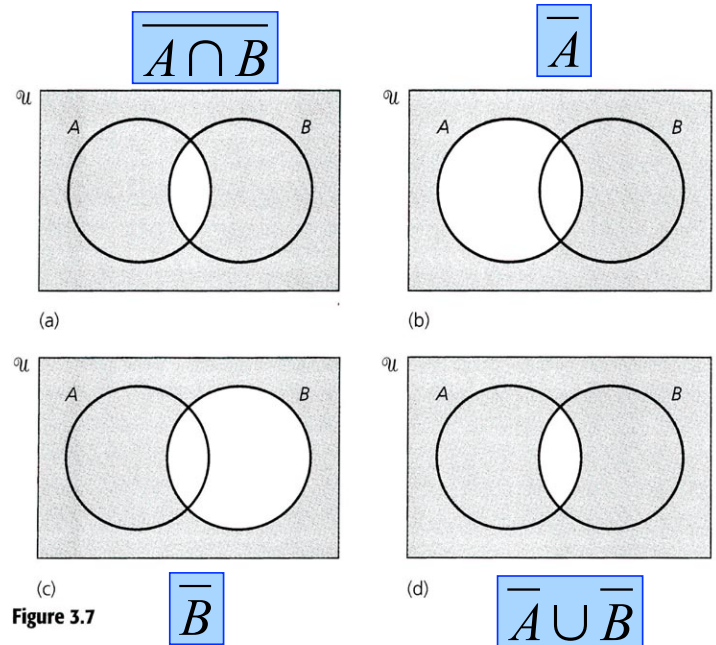


Figure 3.7

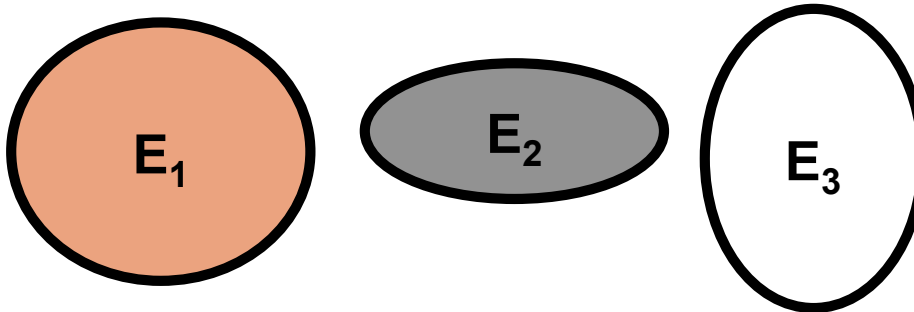


# Remember the Sum Rule

If we have sets of mutually disjoint **events**  $E_1, E_2, \dots, E_m$ , where  $E_j$  can occur in  $n_j$  ways (with  $E_j \cap E_k = \emptyset$  for all  $j \neq k$ ), then there are  $n_1 + n_2 + \dots + n_m$  possible events.

Think union of sets:

Let  $|E_j| = n_j$  for all  $1 \leq j \leq m$ ,  
then  $E_1 \cup E_2, \dots \cup E_m$  has  $n_1 + n_2 + \dots + n_m$  elements.





# Inclusion and Exclusion (排容原理)

- The Principle of Inclusion and Exclusion generalizes the Sum Rule to the cases where the events are not disjoint.
- We can use it when solving counting problems...





## 3.3 Counting and Venn Diagrams

$$(1) |A \cup B| = |A| + |B| - |A \cap B|$$

$$(2) |\overline{A \cap B}| = |\overline{A \cup B}|$$

$$= |U| - |A \cup B|$$

$$= |U| - |A| - |B| + |A \cap B|$$

$$(3) |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

$$(4) |\overline{A \cap B \cap C}| = |\overline{A \cup B \cup C}|$$

$$= |U| - |A \cup B \cup C|$$

$$= |U| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C|$$

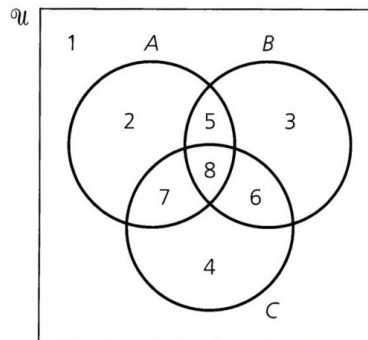


Figure 3.8



# How to Derive the 3 Set Case

Using the various Laws for Sets:

$$\begin{aligned} |A \cup B \cup C| &= |A \cup (B \cup C)| \\ &= |A| + |B \cup C| - |A \cap (B \cup C)| \\ &= |A| + |B| + |C| - |B \cap C| - |A \cap (B \cup C)| \\ &= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)| \\ &= |A| + |B| + |C| - |B \cap C| - |A \cap B| - |A \cap C| + |A \cap B \cap C| \\ &= |A| + |B| + |C| - |B \cap C| - |A \cap B| - |A \cap C| + |A \cap B \cap C| \end{aligned}$$



# Examples

兩個不同骰子

Throw two dice, how many ways of throwing:  
a total of 8, value 6+not value 6, or two identical values?

Counting the possibilities: (2,6), (3,5), (5,3), (6,2), (4,4)

a total of eight: 5

value 6+not value 6: 10

two identical values: 6

total 8 and 6+not 6: 2

total 8 and two id-vs: 1

6+not 6 and two id-vs: 0

6+not 6, two id-vs, total 8: 0

**Total:**

$$5+10+6-2-1-0+0 = 18$$

