Foundations of Computer Science Comp109

University of Liverpool

Boris Konev

konev@liverpool.ac.uk

Part 2. (Naive) Set Theory

Comp109 Foundations of Computer Science

Reading

- S. Epp. *Discrete Mathematics with Applications* Chapter 6
- K. H. Rosen. *Discrete Mathematics and Its Applications* Chapter 2

Contents

- Notation for *sets*.
- Important sets.
- What is a *subset* of a set?
- When are two sets *equal*?
- *Operations* on sets.
- *Algebra* of sets.
- Bit strings.
- *Cardinality* of sets.
- Russell's paradox.

Notation

A *set* is a collection of objects, called the *elements* of the set. For example:

- $\{7, 5, 3\}$;
- $\{\text{Liverpool}, \text{Manchester}, \text{Leeds}\}$.

We have written down the elements of each set and contained them between the *braces* $\{\ \}$.

We write $a \in A$ to denote that the object a is an element of the set A:

$$7 \in \{7, 5, 3\}, \quad 4 \notin \{7, 5, 3\}.$$

Notes

- The order of elements does not matter
- Repeatitions do not count

Notation

For a large set, especially an infinite set, we cannot write down all the elements. We use a predicate P instead.

$$A = \{x \in S \mid P(x)\}$$

denotes the set of objects x from S for which the predicate $P(x)$ is true.

Examples: Let $A = \{1, 3, 5, 7, \ldots\}$. Then

$$A = \{x \in \mathbb{Z} \mid \ x \text{ is odd}\}$$

Very informal notation:

$A = \{2n{-}1 \mid \ n \text{ is a positive integer } \} = \{m \in \mathbb{Z} \mid m = 2n{-}1 \text{ for some integer } n\}.$

More examples

Find simpler descriptions of the following sets by listing their elements:

- $A = \{x \in \mathbb{Z} \mid \; x^2 + 4x = 12\}$;
- $B = \{n^2 \mid \; n \text{ is an integer } \}$.
- $C = \{x \mid \; x \text{ a day of the week not containing "}u\text{" } \}$;

Important sets (notation)

The empty set has no elements. It is written as $\emptyset$ or as $\{\}$.

We have seen some other examples of sets in Part 1.

- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ (the natural numbers)
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ (the integers)
- $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ (the positive integers)
- $\mathbb{Q} = \{x/y \mid x \in \mathbb{Z}, y \in \mathbb{Z}, y \neq 0\}$ (the rationals)
- $\mathbb{R}$: (real numbers)
  - $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ the set of real numbers between a and b (inclusive)

Detour: Sets in python

Sets are the ‘most elementary’ data structures (though they don’t always map well into the underlying hardware).

Some modern programming languages feature sets.

- For example, in Python one writes

```
empty = set()
m = {'a', 'b', 'c'}
n = {1, 2}
print 'a' in m
```

(Computer) representation of sets

Only finite sets can be represented

- Number of elements not fixed: List (?) Java&Python do differently

- All elements of A are drawn from some ordered sequence $S = \langle s_1, \ldots, s_n \rangle$: the characteristic vector of A is the sequence $[b_1, \ldots, b_n]$ where

$$b_i = \begin{cases} 1 & \text{if} \quad s_i \in A \\ 0 & \text{if} \quad s_i \notin A \end{cases}$$

Sequences of zeros and ones of length n are called *bit strings* of length n. AKA *bit vectors* AKA *bit arrays*

Example

Let $S = \langle 1, 2, 3, 4, 5 \rangle$, $A = \{1, 3, 5\}$ and $B = \{3, 4\}$.

- The characteristic vector of A is $[1, 0, 1, 0, 1]$.
- The characteristic vector of B is $[0, 0, 1, 1, 0]$.

- The set characterised by $[1, 1, 1, 0, 1]$ is $\{1, 2, 3, 5\}$.
- The set characterised by $[1, 1, 1, 1, 1]$ is $\{1, 2, 3, 4, 5\}$.
- The set characterised by $[0, 0, 0, 0, 0]$ is $\ldots$

Subsets

Definition A set B is called a *subset* of a set A if every element of B is an element of A. This is denoted by $B \subseteq A$.

Examples:

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

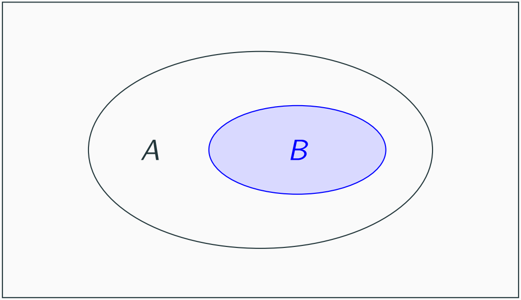


Figure 1: Venn diagram of $B \subseteq A$.

Detour: Subsets in Python

```
def isSubset(A, B):
    for x in A:
        if x not in B:
            return False
    return True
```

Testing the method:

```
print isSubset(n,m)
```

But then there is a built-in operation:

```
print n<m
```

Subsets and bit vectors

Let $S = \langle 1, 2, 3, 4, 5 \rangle$, $A = \{1, 3, 5\}$ and $B = \{3, 4\}$.

- Is $A \subseteq B$?

- Is the set C, represented by $[1, 0, 0, 0, 1]$, a subset of the set D, represented by $[1, 1, 0, 0, 1]$?

Equality

Definition A set A is called *equal* to a set B if $A \subseteq B$ and $B \subseteq A$. This is denoted by $A = B$.

Examples:

$$\{1\} = \{1, 1, 1\},$$

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

$$\{5, 4, 4, 3, 5\} = \{3, 4, 5\}.$$

Equality and bit vectors

Let $S = \langle 1, 2, 3, 4, 5 \rangle$, $A = \{1, 3, 5\}$ and $B = \{3, 4\}$.

- Is $A = B$?

- Is the set C, represented by $[1, 0, 0, 0, 1]$, equual to the set D, represented by $[1, 1, 0, 0, 1]$?

Set operations

The union of two sets

Definition The union of two sets A and B is the set

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$

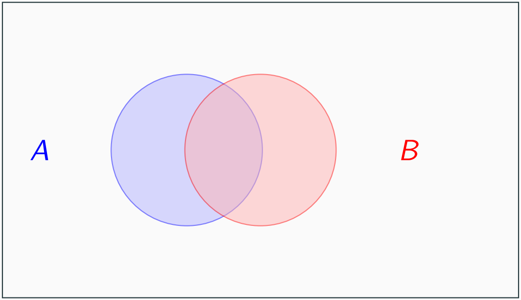


Figure 2: Venn diagram of $A \cup B$.

Example

Suppose

$$A = \{4, 7, 8\}$$

and

$$B = \{4, 9, 10\}.$$

Then

$$A \cup B = \{4, 7, 8, 9, 10\}.$$

Detour: Set union in Python

```
def union(A, B):
    result = set()
    for x in A:
        result.add(x)
    for x in B:
        result.add(x)
    return result
```

Testing the method:

```
print union(m, n)
```

But then there is a built-in operation:

```
print m.union(n)
```

Union of sets represented by bit vectors

Let $S = \langle 1, 2, 3, 4, 5 \rangle$, $A = \{1, 3, 5\}$ and $B = \{3, 4\}$.

- Compute $A \cup B$.

- Compute the union of the set C, represented by $[1, 0, 0, 0, 1]$, and the set D, represented by $[1, 1, 0, 0, 1]$.

The intersection of two sets

Definition The intersection of two sets A and B is the set

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$$

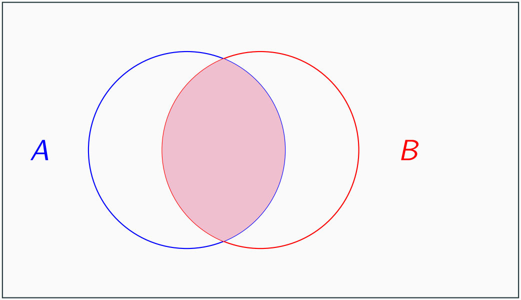


Figure 3: Venn diagram of $A \cap B$.

Example

Suppose

$$A = \{4, 7, 8\}$$

and

$$B = \{4, 9, 10\}.$$

Then

$$A \cap B = \{4\}$$

Detour: Set intersection in Python

```
def intersection(A, B):
    result = set()
    for x in A:
        if x in B:
            result.add(x)
    return result
```

Testing the method:

```
print intersection(m, n)
print intersection(n, {1})
```

But then there is a built-in operation:

```
print n.intersection({1})
```

Intersection of sets represented by bit vectors

Let $S = \langle 1, 2, 3, 4, 5 \rangle$, $A = \{1, 3, 5\}$ and $B = \{3, 4\}$.

- Compute $A \cap B$.

- Compute the intersection of the set C, represented by $[1, 0, 0, 0, 1]$, and the set D, represented by $[1, 1, 0, 0, 1]$.

The relative complement

Definition The relative complement of a set B relative to a set A is the set

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}.$$

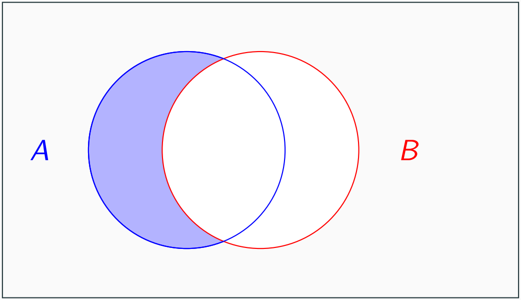


Figure 4: Venn diagram of $A - B$.

Example

Suppose

$$A = \{4, 7, 8\}$$

and

$$B = \{4, 9, 10\}.$$

Then

$$A - B = \{7, 8\}$$

Detour: Set complement in Python

```
def complement(A, B):
    result = set()
    for x in A:
        if x not in B:
            result.add(x)
    return result
```

Testing the method:

```
print complement(m, {'a'})
```

But then there is a built-in operation:

```
print m−{'a'}
```

Relative complement and bit vectors

Let $S = \langle 1, 2, 3, 4, 5 \rangle$, $A = \{1, 3, 5\}$ and $B = \{3, 4\}$.

- Compute $A - B$.

- Compute the relative complement of the set C, represented by $[1, 0, 0, 0, 1]$, related to the set D, represented by $[1, 1, 0, 0, 1]$.

The complement

When we are dealing with subsets of some large set U, then we call U the *universal set* for the problem in question.

Definition The complement of a set A is the set

$$\sim A = \{x \mid x \notin A\} = U - A.$$

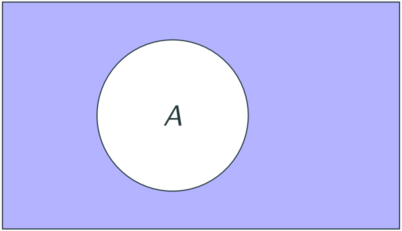


Figure 5: Venn diagram of $\sim A$. (The rectangle is U)

Complement and bit vectors

Let $S = \langle 1, 2, 3, 4, 5 \rangle$, $A = \{1, 3, 5\}$ and $B = \{3, 4\}$.

- Compute $\sim A$.

- Compute $\sim B$.

- Compute the complement of the set C, represented by $[1, 0, 0, 0, 1]$.

The symmetric difference

Definition The symmetric difference of two sets A and B is the set

$$A \Delta B = \{x \mid (x \in A \text{ and } x \notin B) \text{ or } (x \notin A \text{ and } x \in B)\}.$$

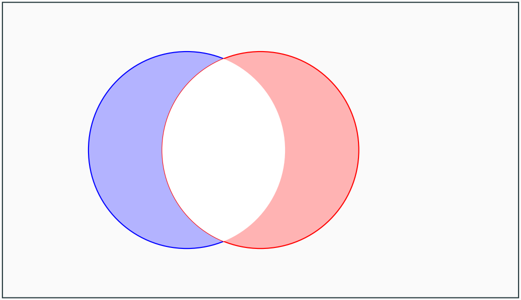


Figure 6: Venn diagram of $A \Delta B$.

Example

Suppose

$$A = \{4, 7, 8\}$$

and

$$B = \{4, 9, 10\}.$$

Then

$$A \Delta B = \{7, 8, 9, 10\}$$

Proving identities: $A \Delta B = (A \cup B) - (A \cap B)$

Proof continues

The algebra of sets

The algebra of sets (1)

Suppose that A, B, C, U are sets with $A \subseteq U,\ B \subseteq U,\ C \subseteq U$

Commutative laws (a) $A \cup B = B \cup A$ and (b) $A \cap B = B \cap A$.

Associative laws (a) $A \cup (B \cup C) = (A \cup B) \cup C$ and
(b) $A \cap (B \cap C) = (A \cap B) \cap C$.

Distributive laws (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and
(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Identity laws (a) $A \cup \emptyset = A$ and (b) $A \cap U = A$

Complement laws (a) $A \cup \sim A = U$ and (b) $A \cap \sim A = \emptyset$.

The algebra of sets (2)

Double complement law	$\sim(\sim A) = A$.
Idempotent laws	(a) $A \cup A = A$ and (b) $A \cap A = A$.
Universal bound laws	(a) $A \cup U = U$ and (b) $A \cap \emptyset = \emptyset$.
De Morgan's law	(a) $\sim(A \cup B) = \sim A \cap \sim B$ and (b) $\sim(A \cap B) = \sim A \cup \sim B$
Absorption laws	(a) $A \cup (A \cap B) = A$ and (b) $A \cap (A \cup B) = A$
Complement of U and $\emptyset$	(a) $\sim U = \emptyset$ and (b) $\sim \emptyset = U$
Set difference law	$A - B = A \cap \sim B$

Proving the commutative law $A \cup B = B \cup A$

Definition: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$ $B \cup A = \{x \mid x \in B \text{ or } x \in A\}$.

These are the same set. To see this, check all possible cases.

Case 1: Suppose $x \in A$ and $x \in B$. Since $x \in A$, the definitions above show that x is in both $A \cup B$ and $B \cup A$.

Case 2: Suppose $x \in A$ and $x \notin B$. Since $x \in A$, the definitions above show that x is in both $A \cup B$ and $B \cup A$.

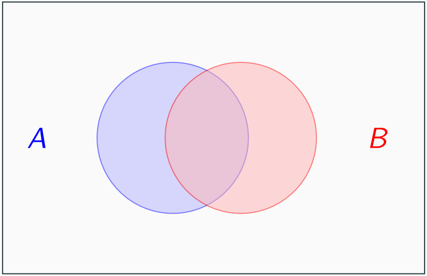
Case 3: Suppose $x \notin A$ and $x \in B$. Since $x \in B$, the definitions above show that x is in both $A \cup B$ and $B \cup A$.

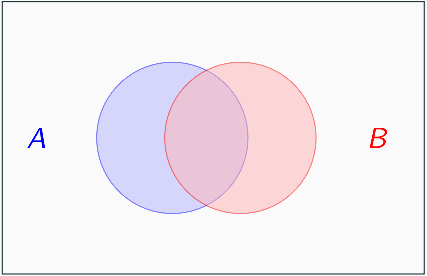
Case 4: Suppose $x \notin A$ and $x \notin B$. The definitions above show that x is not in $A \cup B$ and x is not in $B \cup A$.

So, for all possible x, either x is in both $A \cup B$ and $B \cup A$, or it is in neither. We conclude that the sets $A \cup B$ and $B \cup A$ are the same.

De Morgan's laws

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





A proof of De Morgan's law $\sim (A \cap B) = \sim A \cup \sim B$

Case 1: Suppose $x \in A$ and $x \in B$. From the definition of $\cap$, $x \in A \cap B$. So from the definition of $\sim$, $x \notin \sim (A \cap B)$. From the definition of $\sim$, $x \notin \sim A$ and also $x \notin \sim B$. So from the definition of $\cup$, $x \notin \sim A \cup \sim B$.

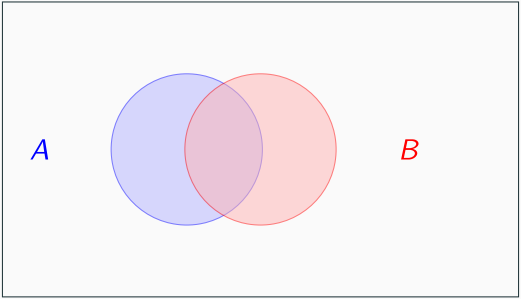
Case 2: Suppose $x \in A$ and $x \notin B$. From the definition of $\cap$, $x \notin A \cap B$. So from the definition of $\sim$, $x \in \sim (A \cap B)$. From the definition of $\sim$, $x \notin \sim A$ but $x \in \sim B$. So from the definition of $\cup$, $x \in \sim A \cup \sim B$.

Case 3: Suppose $x \notin A$ and $x \in B$. From the definition of $\cap$, $x \notin A \cap B$. So from the definition of $\sim$, $x \in \sim (A \cap B)$. From the definition of $\sim$, $x \in \sim A$ but $x \notin \sim B$. So from the definition of $\cup$, $x \in \sim A \cup \sim B$.

Case 4: Suppose $x \notin A$ and $x \notin B$. From the definition of $\cap$, $x \notin A \cap B$. So from the definition of $\sim$, $x \in \sim (A \cap B)$. From the definition of $\sim$, $x \in \sim A$ and $x \in \sim B$. So from the definition of $\cup$, $x \in \sim A \cup \sim B$.

Using the algebra of sets

Prove that $(A \cap \sim B) \cup (B \cap \sim A) = (A \cup B) \cap \sim (A \cap B)$.



Algebraic proof

$$
\begin{aligned}
(A \cup B) \cap \sim (A \cap B) &= (A \cup B) \cap (\sim A \cup \sim B) \text{ De Morgan} \\
&= ((A \cup B) \cap \sim A) \cup ((A \cup B) \cap \sim B) \text{ distributive} \\
&= (\sim A \cap (A \cup B)) \cup (\sim B \cap (A \cup B)) \text{ commutative} \\
&= ((\sim A \cap A) \cup (\sim A \cap B)) \cup ((\sim B \cap A) \cup (\sim B \cap B)) \text{ distributive} \\
&= ((A \cap \sim A) \cup (B \cap \sim A)) \cup ((A \cap \sim B) \cup (B \cap \sim B)) \text{ commutative} \\
&= (\emptyset \cup (B \cap \sim A)) \cup ((A \cap \sim B) \cup \emptyset) \text{ complement} \\
&= (A \cap \sim B) \cup (B \cap \sim A) \text{ commutative and identity}
\end{aligned}
$$

Cardinality of sets

Cardinality of sets

Definition The cardinality of a *finite* set A is the number of distinct elements in A, and is denoted by $|A|$.

Example: The cardinality of the set of all subsets

Definition The **power set** $Pow(A)$ of a set A is the set of all subsets of A. In other words,

$$Pow(A) = \{C \mid C \subseteq A\}.$$

For all $n \in \mathbb{Z}^+$ and all sets A: if $|A| = n$, then $|Pow(A)| = 2^n$.

Power set and bit vectors

We use the correspondence between bit vectors and subsets: $|Pow(A)|$ is the number of bit vectors of length n.

The number of n-bit vectors is 2^n

We prove the statement by induction.

Base Case:

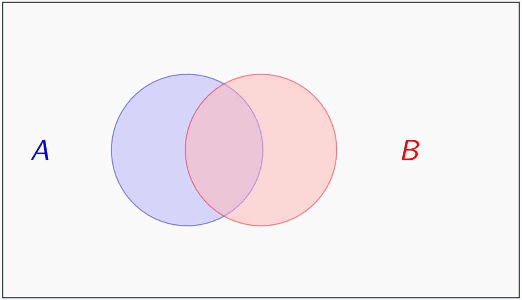
The number of n-bit vectors is 2^n

Inductive Step: Assume that the property holds for $n = m$, so the number of m-bit vectors is 2^m. Now consider the set B of all $(m+1)$-bit vectors. We must show that $|B| = 2^{m+1}$.

Computing the cardinality of a union of two sets

If A and B are sets then

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

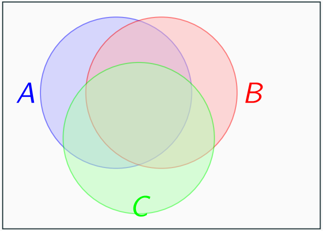


Example

Suppose there are 100 third-year students. 40 of them take the module "Sequential Algorithms" and 80 of them take the module "Multi-Agent Systems". 25 of them took both modules. How many students took neither modules?

Computing the cardinality of a union of three sets

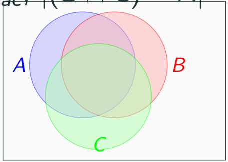
$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$



Proof (optional)

We need lots of notation.

- $|A - (B \cup C)| = n_a$, $|B - (A \cup C)| = n_b$, $|C - (A \cup B)| = n_c$,
- $|(A \cap B) - C| = n_{ab}$, $|(A \cap C) - B| = n_{ac}$, $|(B \cap C) - A| = n_{bc}$,
- $|A \cap B \cap C| = n_{abc}$.



Then

$$\begin{aligned} |A \cup B \cup C| &= n_a + n_b + n_c + n_{ab} + n_{ac} + n_{bc} + n_{abc} \\ &= (n_a + n_{ab} + n_{ac} + n_{abc}) + (n_b + n_{ab} + n_{bc} + n_{abc}) \\ &+ (n_c + n_{ac} + n_{bc} + n_{abc}) - (n_{ab} + n_{abc}) \\ &- (n_{ac} + n_{abc}) - (n_{bc} + n_{abc}) + n_{abc} \end{aligned}$$

These are special cases of the principle of inclusion and exclusion

Principle of inclusion and exclusion

Let $A_1, A_2, \ldots, A_n$ be sets.

Then

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

Russel’s paradox

Why is this set theory “naive”

It suffers from paradoxes.

A leading example:

> *A barber is the man who shaves all those, and only those, men who do not shave themselves.*

- Who shaves the barber?

Russell's Paradox

Russell's paradox shows that the 'object' $\{x \mid P(x)\}$ is not always meaningful.

Set $A = \{B \mid B \notin B\}$

Problem: do we have $A \in A$?

Abbreviate, for any set C, by $P(C)$ the statement $C \notin C$. Then $A = \{B \mid P(B)\}$.

- If $A \in A$, then (from the definition of P), not $P(A)$. Therefore $A \notin A$.
- If $A \notin A$, then (from the definition of P), $P(A)$. Therefore $A \in A$.