Foundations of Computer Science Comp109

University of Liverpool

Boris Konev

konev@liverpool.ac.uk

Olga Anosova

O.Anosova@liverpool.ac.uk

Last lecture recap: algebra on sets

Proving with sets often includes consideration of several cases, knowing the main laws can speed up the process:

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

Commutative laws

Associative laws

Distributive laws

Identity laws

Complement laws

Cardinality of sets

Cardinality of finite sets

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

Examples:

- $|\{4, 5\}| =$
- $|\emptyset| =$
- $|\{\emptyset\}| =$
- $|\{1, 1\}| =$
- $|\{1, 3, 5\} \cap \{3, 4\}| =$
- $|\{1, 3, 5\} \cup \{3, 4\}| =$

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,

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

Examples

- $A = \{a\}$. Then all subsets of A are:
- $B = \{a, b\}$. Then all subsets of B are:
- $C = \{a, b, c\}$. Then the number of subsets is

Cardinality of a power set

$|A| = n \Longrightarrow |Pow(A)| = ??$

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

We prove the statement by induction.

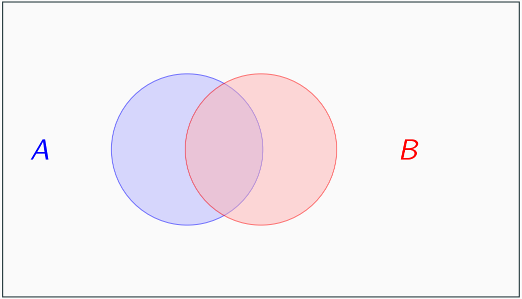
Base Case:

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

Computing the cardinality of a union of two sets

If A and B are sets then

$$|A \cup B| =$$

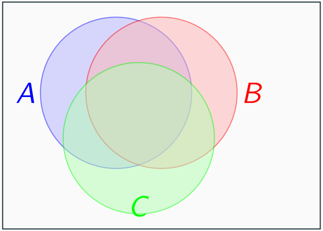


Example

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

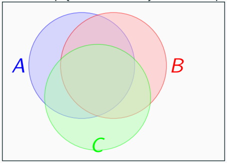
$$|A \cup B \cup C| =$$



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 general 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 Is $A \in A$?

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

- If $A \in A$, then (from the definition of P),
- If $A \notin A$, then (from the definition of P),

Gödel's puzzle

There are exactly two types of people on an island: Truthers and Liars. Truthers always say true statements, and Liars always say false statements. One day Alice, a perfectly sound reasoner who never proves anything that is false comes to visit the island.

She meets Bob, who lives on the island, who claims to Alice:
"You never prove that I am a truther."
Is he right?

Gödel's impossibility theorem(s)

Summary

- The cardinality $|A|$ of a *finite* set A is the number of distinct elements in A.
- If $|A| = n \in \mathbb{Z}^+$, then the number of all subsets $=$
- *Inclusion-exclusion principle* for 3 events:
  $|A \cup B \cup C| =$
- Russel's paradox and Gödel's theorems prove that axiomatic theory is not a perfect final solution.