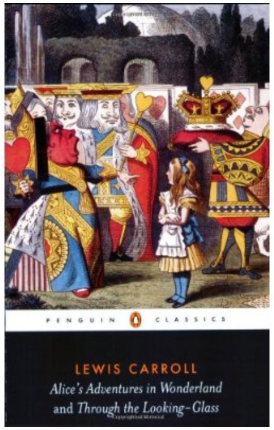
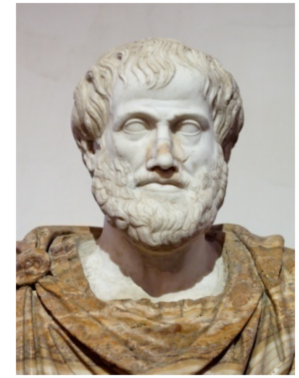


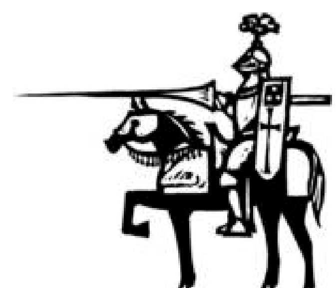


COMP 1002

Logic for Computer Scientists

Lecture 16

B 5 2 J



Admin stuff

- A2 due Feb 17th.
- Midterm March 2nd.

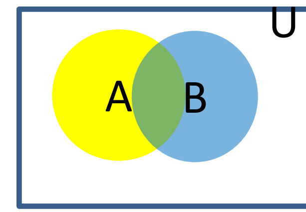
- Semester break next week!

Puzzle: the barber

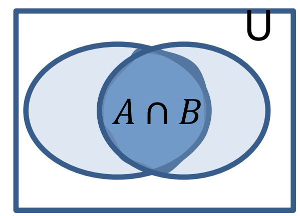
- In a certain village, there is a (male) barber who shaves all and only those men of the village who do not shave themselves.

- *Question: who shaves the barber?*

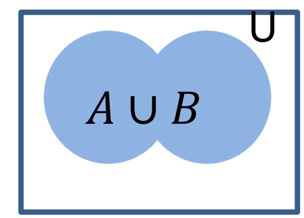
Operations on sets



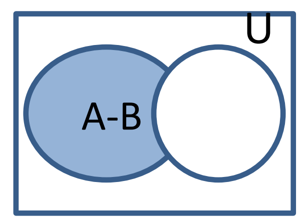
- Let A and B be two sets.
  - Such as A={1,2,3} and B={ 2,3,4}



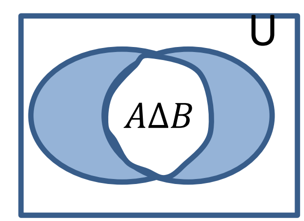
- **Intersection** $A \cap B = \{\, x \mid x \in A \land x \in B\}$
  - The green part of the picture above
  - $A \cap B = \{2,3\}$



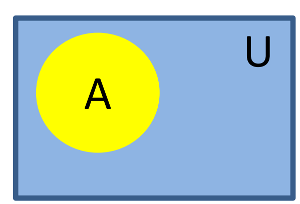
- **Union** $A \cup B = \{\, x \mid x \in A \lor x \in B\}$
  - The coloured part in the top picture.
  - $A \cup B = \{1,2,3,4\}$



- **Difference** $A - B = \{x \mid x \in A \land x \notin B\}$
  - The yellow part in the top picture.
  - $\mathrm{A} - B = \{1\}$



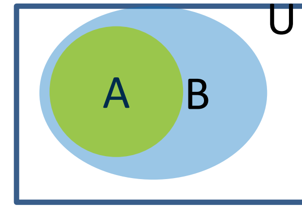
- **Symmetric difference** $A \,\Delta\, B = (A - B) \cup (B - A)$
  - The yellow and blue parts of the top picture.
  - $\mathrm{A}\Delta B = \{1,4\}$



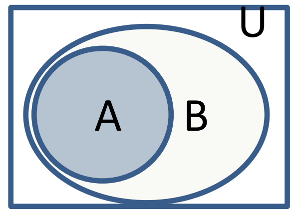
- **Complement** $\overline{A} = \{x \in U \mid x \notin A\}$
  - The blue part on the bottom Venn diagram
  - If universe U = ℕ, $\overline{A} = \{x \in \mathbb{N} \mid x \notin \{1,2,3\}\ \}$

Subsets and operations

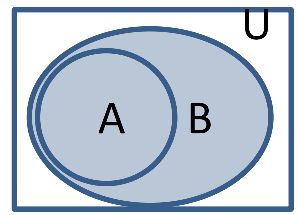
- If $A \subseteq B$ then



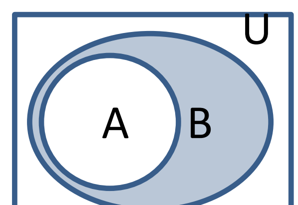
  - Intersection $A \cap B =$
    - A



  - Union $A \cup B =$
    - B



  - Difference $A - B =$
    - $\emptyset$
  - Difference B – A =
    - $\overline{\mathrm{A}} - \overline{B}$

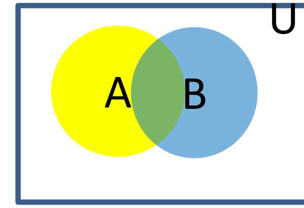


Size (cardinality)

- If a set A has n elements, for a natural number n, then A is a **finite** set and its **cardinality** is |A|=n.
  - $|\{1,2,3\}| = 3$
  - $|\emptyset| = 0$

- Sets that are not finite are **infinite**. More on cardinality of infinite sets in a couple of lectures…
  - $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$
  - $\mathbb{R}, \mathbb{C}$
  - $\{0,1\}^*$: set of all finite-length binary strings.

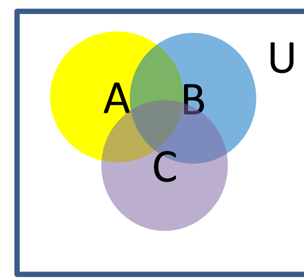
Rule of inclusion-exclusion



- Let A and B be two sets. Then

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

  - Proof idea: notice that elements in $|A \cap B|$ are counted twice in |A|+|B|, so need to subtract one copy.
  - If A and B are disjoint, then $|A \cup B| = |A| + |B|$
  - If there are 112 students in COMP 1001, 70 in COMP 1002, and 12 of them are in both, then the total number of students in 1001 or 1002 is 112+70-12=170.

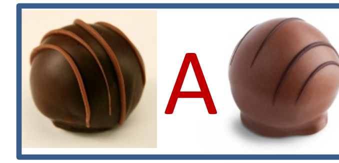


- For three sets (and generalizes)
- $|A \cup B \cup C| = |A| + |B| + |C|$

$$-|A \cap B| - |A \cap C| - |B \cap C|$$

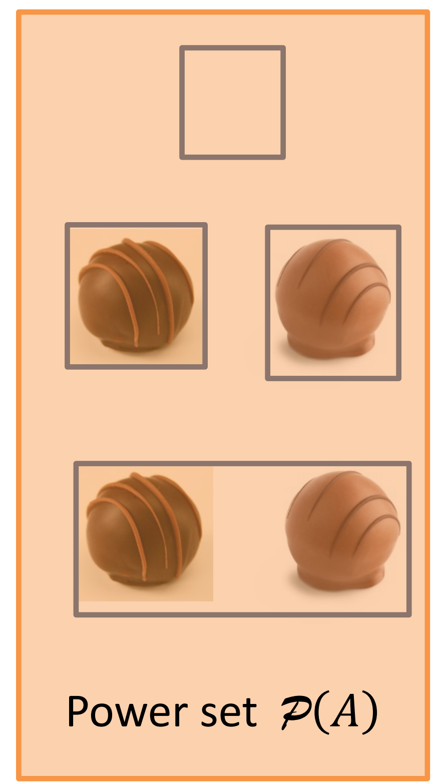
$$+|A \cap B \cap C|$$

Power sets



- A **power set** of a set A, $\mathcal{P}(A)$, is a set of all subsets of A.
  - Think of sets as boxes of elements.
  - A subset of a set A is a box with elements of A (maybe all, maybe none, maybe some).
  - Then $\mathcal{P}(A)$ is a box containing boxes with elements of A.
  - When you open the box $\mathcal{P}(A)$, you don't see chocolates (elements of A), you see boxes.
  - A={1,2}, $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$
  - $A = \emptyset, \quad \mathcal{P}(A) = \{\emptyset\}$.
    - They are not the same! There is nothing in A, and there is one element, an empty box, in $\mathcal{P}(A)$
- If A has n elements, then $\mathcal{P}(A)$ has 2^n elements.

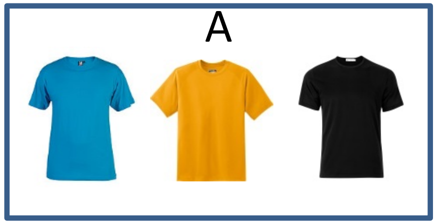
Subsets of A:



Cartesian products

- **Cartesian product** of A and B is a set of all pairs of elements with the first from A, and the second from B:
  - A x B = $\{(x, y) | x \in A,\ \ y \in B\}$
  - A={1,2,3}, B={a,b}
  - $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$
  - A={1,2}, $A \times A\ = \{(1,1), (1,2), (2,1), (2,2)\}$

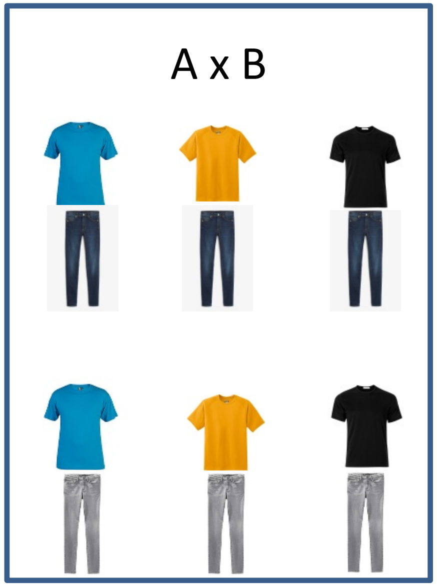
	a	b
1	(1,a)	(1,b)
2	(2,a)	(2,b)
3	(3,a)	(3,b)



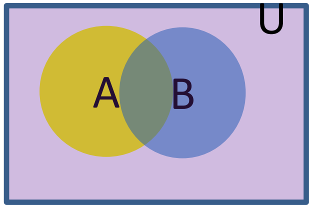
- Order of pairs does not matter, order within pairs does: $A \times B \neq B \times A$.

- Number of elements in $A \times B$ is $|A \times B| = |A| \cdot |B|$

- Can define the Cartesian product for any number of sets:
  - $A_1 \times A_2 \times \cdots \times A_k = \{(x_1, x_2, \ldots x_k) |\ x_1 \in A_1 \ldots x_k \in A_k\}$
  - $A = \{1,2,3\}$, B ={a,b}, C={3,4}
  - $A \times B \times C = \{(1, a, 3), (1, a, 4),\ (1, b, 3), (1, b, 4),$ $(2, a, 3), (2, a, 4),\ (2, b, 3), (2, b, 4),$ $(3, a, 3), (3, a, 4),\ (3, b, 3), (3, b, 4)\}$

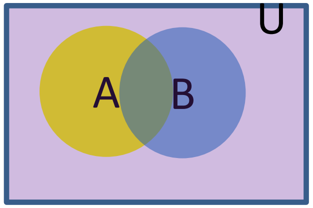


Proofs with sets



- Two ways to describe the purple area
- $\overline{A \cup B}$, $\overline{A} \cap \overline{B}$
  - $x \in \overline{A \cup B}$ when $x \notin A \cup B$
  - This happens when $x \notin A \wedge x \notin B$.
  - So $x \in \overline{A} \cap \overline{B}$. Since we picked an arbitrary x, then $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$
  - Not quite done yet… Now let $x \in \overline{A} \cap \overline{B}$
  - Then $x \in \overline{A} \wedge x \in \overline{B}$. So $x \notin A \wedge x \notin B$.
  - $x \notin A \wedge x \notin B \equiv \neg(x \in A \vee x \in B)$. So $x \notin A \cup B$. Thus $x \in \overline{A \cup B}$.
  - Since x was an arbitrary element of $\overline{A} \cap \overline{B}$, then $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$.
  - Therefore $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Laws of set theory



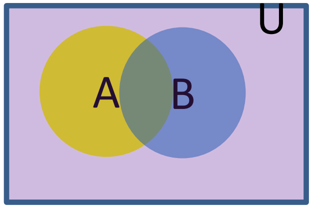
- Two ways to describe the purple area
  - $\overline{A \cup B} = \overline{A} \cap \overline{B}$
- By similar reasoning,
  - $\overline{A \cap B} = \overline{A} \cup \overline{B}$

- Does this remind you of something?...
  - $\neg(p \lor \mathrm{q}) \equiv \neg p \ \land \neg\, q$
  - DeMorgan’s law works in set theory!
  - What about other equivalences from logic?

More useful equivalences

- For any formulas A, B, C:
  - A $\vee \neg A \equiv True$ $\quad\quad$ $A \wedge \neg A \equiv False$
  - $True \vee A \equiv True$. $\quad\quad$ $True \wedge A \equiv A$
  - $False \vee A \equiv A$. $\quad\quad$ $False \wedge A \equiv False$
  - A$\vee$ $A \equiv A \wedge A \equiv A$
- Also, like in arithmetic (with ∨ as +, ∧ as *)
  - $A \vee B \equiv B \vee A \quad and \quad (A \vee B) \vee C \equiv A \vee (B \vee C)$
  - Same holds for ∧.
  - Also, $(A \vee B) \wedge C \equiv (A \wedge C) \vee (B \wedge C)$
- And unlike arithmetic
  - $(A \wedge B) \vee C \equiv (A \vee C) \wedge (B \vee C)$

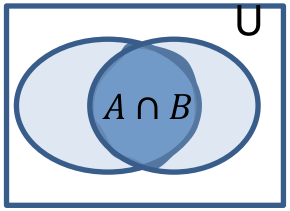
Propositions vs. sets



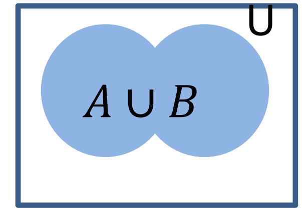
Propositional logic	Set theory
Negation $\neg p$	Complement $\overline{A}$
$AND\ \ p \wedge q$	Intersection $A \cap B$
OR $p \vee q$	Union $A \cup B$
FALSE	Empty set $\emptyset$
TRUE	Universe U

More useful equivalences

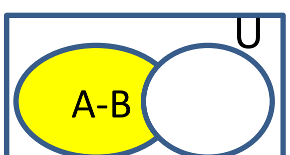
- For any formulas A, B, C:
  - $A \vee \neg A \equiv True$ $\qquad A \wedge \neg A \equiv False$
  - $True \vee A \equiv True.$ $\qquad True \wedge A \equiv A$
  - $False \vee A \equiv A.$ $\qquad False \wedge A \equiv False$
  - $A \vee A \equiv A \wedge A \equiv A$
- Also, like in arithmetic (with ∨ as +, ∧ as *)
  - $A \vee B \equiv B \vee A \quad and \;\; (A \vee B) \vee C \equiv A \vee (B \vee C)$
  - Same holds for ∧.
  - Also, $(A \vee B) \wedge C \equiv (A \wedge C) \vee (B \wedge C)$
- And unlike arithmetic
  - $(A \wedge B\,) \vee C \equiv \;\; (A \vee C) \wedge (B \vee C)$

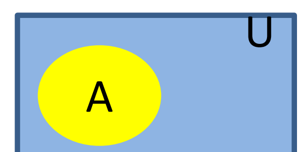


Laws of set theory



- For any sets A, B, C:
  - $A \cup \overline{A} = U$ $\qquad$ $A \cap \overline{A} = \emptyset$
  - $U \cup A = U$. $\qquad$ $U \cap A = A$
  - $\emptyset \cup A = A$. $\qquad$ $\emptyset \cap A = \emptyset$
  - $A \cup A = A \cap A = A$
- Also, like in arithmetic (with ∨ as +, ∧ as *)
  - $A \cup B = B \cup A \quad and \quad (A \cup B) \cup C = A \cup (B \cup C)$
  - Same holds for ∩.
  - Also, $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
- And unlike arithmetic
  - $(A \cap B) \cup C \equiv (A \cup C) \cap (B \cup C)$





Boolean algebra

- The “algebra” of both propositional logic and set theory is called **Boolean algebra** (as opposed to algebra on numbers).

Propositional logic	Set theory	Boolean algebra
Negation $\neg p$	Complement $\overline{A}$	$\overline{a}$
AND $p \wedge q$	Intersection $A \cap B$	$a \cdot b$
OR $p \vee q$	Union $A \cup B$	$a + b$
FALSE	Empty set $\emptyset$	0
TRUE	Universe U	1

Axioms of Boolean algebra

1. $a + b = b + a,$ $\qquad a \cdot b = b \cdot a$
2. (a+b)+c=a+(b+c) $\qquad (\mathrm{a} \cdot b\ ) \cdot c = a \cdot (b \cdot c)$
3. $a + (b \cdot c) = (a + b) \cdot (a + c)$
   $a \cdot (b + c) = (a \cdot b) + (a \cdot c\ )$
4. There exist distinct elements 0 and 1 (among underlying set of elements B of the algebra) such that for all $a \in B$,
   $$a + 0 = a \qquad a \cdot 1 = a$$
5. For each $a \in B$ there exists an element $\overline{a} \in B$ such that
   $$a + \overline{a} = 1 \qquad a \cdot \overline{a} = 0$$

How about DeMorgan, etc? They can be derived from the axioms!

Puzzle: the barber club

- In a certain barber's club,
  - Every member has shaved at least one other member
  - No member shaved himself
  - No member has been shaved by more than one member
  - There is a member who has never been shaved.

- *Question: how many barbers are in this club?*