CS2209A 2017
Applied Logic for Computer Science

Lecture 13

Set Theory

Instructor: Yu Zhen Xie

Midterm

- **Midterm 7:00pm-8:50pm, Wed., October 25th**
  - Closed-book; no electronic devices are allowed.
  - Two exam papers (take A or B); Covers lectures 1 to 12.
    - Question formats are the same as those for quizzes, exercises and assignments.
  - Study guide posted to help you study
    - **not** to bring to the midterm itself.
  - The table for laws of propositional logic will be provided with the exam paper for your reference.
- Assignment 1 marked.
  - Solution sheet posted at OWL.
  - Let us know as soon as possible if you have questions about your mark.
- We will do our best to return the marked Assignment 2 before the midterm

A review for the work of
Assignment 2 and Quiz 2

Arguments and validity

- An argument is **valid** if whenever all premises are true, the conclusion is also true.
  - So if premises are $P_1, \ldots, P_n$, and conclusion is P_{n+1} ,
  - then the argument is valid

    $\Updownarrow$ if and only if
  - $\boldsymbol{P_1 \wedge P_2 \wedge \cdots P_n \rightarrow P_{n+1}}$ is a **tautology**

$$\begin{array}{c} \boldsymbol{P_1} \\ \boldsymbol{P_2} \\ \vdots \\ \boldsymbol{P_n} \\ \hline \therefore \boldsymbol{P_{n+1}} \end{array}$$

Rules of inference

- Can apply **tautologies** of the form $\mathbf{F} \rightarrow \boldsymbol{G}$
  - so that if F is an **AND** of several formulas derived so far, then we get G, and **add G to the premises**.
  - Such as from $((\boldsymbol{p} \rightarrow \boldsymbol{q}) \wedge \boldsymbol{p}) \rightarrow \boldsymbol{q}$ we can deduce q. Now we can add q to the list of premises.
- Keep going until we get the conclusion.

- If Socrates is a man, then Socrates is mortal
- Socrates is a man

____

∴ Socrates is mortal

Modus ponens: treasure hunt

- **If** $\boldsymbol{p}$ **then** $\boldsymbol{q}$
- $\boldsymbol{p}$

$\underline{\hspace{10em}}\ \therefore$

$\boldsymbol{q}$

- If house is next to the lake then the treasure is not in the kitchen
- The house is next to the lake
- Therefore, the treasure is not in the kitchen.

➢ **Here, p is “the house is next to the lake”, and q is “the treasure is not in the kitchen”.**

Resolution rule

- Middle ground between truth tables and natural deduction
  - Basis for many practical provers (SAT solvers).
  - Used in verification, scheduling, etc...

$$\begin{array}{c} C \lor x \\ D \lor \neg x \\ \hline \therefore C \lor D \end{array}$$

- $(C \lor x) \land (D \lor \neg x) \rightarrow (C \lor D)$ is a tautology

Resolution rule

$$\frac{\begin{array}{c} C \lor x \\ D \lor \neg x \end{array}}{\therefore\ C \lor D} \qquad \frac{\begin{array}{c} y \lor \neg z \ \lor w \\ u \ \lor \neg w \end{array}}{\therefore\ y \lor \neg z \ \lor u} \qquad \frac{\begin{array}{c} y \lor w \lor \neg z \\ \neg z \ \lor \neg w \end{array}}{\therefore\ y \lor \neg z}$$

- Ignore order in an **OR** and remove duplicates.
- *C* and *D* are possibly empty
  - $\boldsymbol{x \land \neg x \equiv False}$ (same as saying it is a contradiction)

$$\frac{\begin{array}{c} x \\ \neg x \end{array}}{\therefore\ False}$$

Resolution proofs

- Rather than proving that F is a tautology, prove that $\neg \boldsymbol{F} \equiv \boldsymbol{FALSE}$. That is, a proof of F is a **refutation** of $\neg F$
  - To check that an formula A is a tautology, refute $\neg A$
  - To check that an **argument** is valid, refute AND of premises AND NOT conclusion.

- Last step of the resolution refutation of $\neg F$:
  - from x and $\neg x$ derive FALSE, for some variable x.
  - If you cannot derive anything new, then the formula is satisfiable.

$$(y \vee \neg z) \wedge \quad (\neg y) \wedge \quad (y \vee z)$$

$$(\neg z) \qquad\qquad (z)$$

$$FALSE$$

Exp. Prove Modus Ponens by resolution

- **If** $\boldsymbol{p}$ **then** $\boldsymbol{q}$
- $\boldsymbol{p}$

$\underline{\hspace{6cm}} \therefore$

$\boldsymbol{q}$

$$\boldsymbol{(p \rightarrow q) \wedge p \rightarrow q}$$

is a tautology

➢ Prove by resolution refutation:
$(p \rightarrow q) \wedge p \wedge (\neg q\ )$ is false

$$\boldsymbol{(\neg p \vee q) \wedge p \wedge \neg q}$$

$$(\neg p \vee q) \wedge\ p \wedge\ (\neg q)$$

$$q$$

$$FALSE$$

Predicate logic (first-order formula)

- A formula $\forall x \in S,\ F(x)$, where $F(x)$ is a formula containing predicates, is true (on the domain of predicates) if it is true on every value of x from the domain. Here, $\forall$ is called a ***universal quantifier***, usually pronounced as “for all ...".

- A formula $\exists x \in S,\ F(x)$, where $F(x)$ is a formula containing predicates, is true (on the domain of predicates) if it is true on some value of x from the domain. Here, $\exists$ is called an ***existential quantifier***, usually pronounced as “exists ...".

- Universal and existential quantifiers are **opposites** of each other.
  - $\neg\big(\forall \boldsymbol{x} \in \boldsymbol{S}, \boldsymbol{F}(\boldsymbol{x})\big) \equiv \exists \boldsymbol{x} \in \boldsymbol{S},\ \neg \boldsymbol{F}(\boldsymbol{x})$
  - $\neg\big(\exists \boldsymbol{x} \in \boldsymbol{S}, \boldsymbol{F}(\boldsymbol{x})\big) \equiv \forall \boldsymbol{x} \in \boldsymbol{S},\ \neg \boldsymbol{F}(\boldsymbol{x})$

Scope of quantifiers

- Like in programming, a **scope** of a quantified variable continues until a new variable with the same name **is** introduced.
  - $\forall x \left(\exists y \; P(x, y)\right) \wedge \left(\exists y \, Q(x, y)\right)$
    - For everybody there is somebody who loves them and somebody who hates them.
  - Not the same as $\forall x \left(\exists y \; P(x, y) \wedge Q(x, y)\right)$
    - For everybody there is somebody who both loves and hates them.

- Better to avoid using same names for different variables since it is confusing.
  - $\forall x \left(\exists y \; P(x, y)\right) \wedge \left(\exists y \, Q(x, y)\right)$

    $\equiv$
  - $\forall x \left(\exists y \, P(x, y)\right) \wedge \left(\exists z \, Q(x, z)\right)$

    $\equiv$
  - $\forall x \, \exists y \, \exists z \, P(x, y) \wedge Q(x, z)$

    $\equiv$
  - $\forall x \, \exists z \, \exists y \, P(x, y) \wedge Q(x, z)$

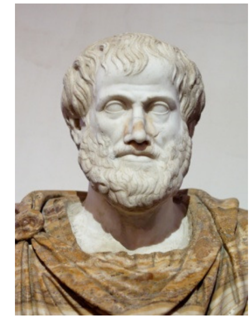
Prenex normal form

- When all quantified variables have different names, can move all quantifiers to the front of the formula, and get an equivalent formula: this is called **prenex normal form**.
  - $\forall x\ \exists y\ \exists z\ P(x,y) \wedge Q(x,z)$ is in prenex normal form
  - $\forall x\ \left(\exists\ y\ P(x,y)\right) \wedge \left(\exists z\ Q(x,z)\right)$ is not in prenex normal form.

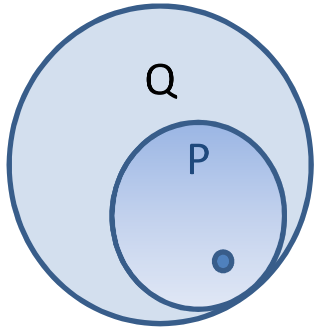
- Order of variables under the same quantifier does not matter. Under different ones does.
  - $\forall x\ \exists y\ \exists z\ P(x,y) \wedge Q(x,z)$ and $\exists y\ \forall x\ \exists z\ P(x,y) \wedge Q(x,z)$ are not equivalent

- Be careful with implications: when in doubt, open into $\neg A \vee B$. Move all negations inside.
  - $\forall x\ \ (\left(\exists y\ P(x,y)\right) \rightarrow Q(x)\ )$ actually has two universal quantifiers!
  - Its equivalence in prenex normal form is $\forall x\ \forall y\ \left(\neg P(x,y) \vee Q(x)\right)$

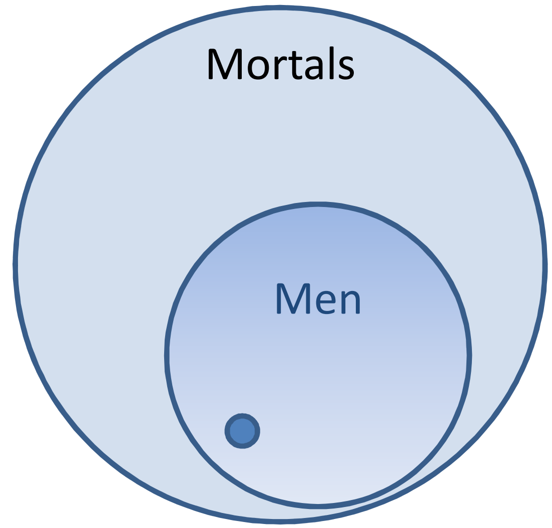
Universal Modus Ponens



- $\forall x,\ P(x)\ \rightarrow Q(x)$
- $P(a)$
- -------------------------
- $Q(a)$



- All men are mortal $(\forall x,\ Man(x) \rightarrow Mortal(x))$
- Socrates is a man $(Man(Socrates))$
- Therefore, Socrates is mortal $(Mortal(Socrates))$



- All numbers are either odd or even
- 2 is a number
- Therefore, 2 is either odd or even.

- All trees drop leaves
- Pine does not drop leaves
- Therefore, pine is not a tree

Counterexamples

- To disprove a statement, enough to give a counterexample: a scenario where it is false
  - To **disprove** that $A \to B \equiv B \to A$
    - Take $A = true, B = false,$
    - Then $A \to B$ is false, but $\mathrm{B} \to A$ is true.
  - To **disprove** that if $\forall x\, \exists y\, P(x, y),$ then $\exists y\, \forall x\, P(x, y)$,
    - Set the domain of x and y to be {0,1}
    - Set P(0,0) and P(1,1) to true, and P(0,1), P(1,0) to false.
    - Then $\forall x\, \exists y\, P(x, y)$ is true, but $\exists y\, \forall x\, P(x, y)$ is false.
      - Because $\big(P(0,0) \vee P(1,0)\big) \wedge \big(P(0,1) \vee P(1,1)\big)$ is true,
      - But $(P(0,0) \wedge P(1,0)) \vee (P(0,1) \wedge P(1,1))$ is false.

Constructive proofs

- To prove a statement of the form $\exists x$, sometimes can just find that x
  - $\exists x \in \mathbb{N}\ Even(x) \wedge Prime(x)$
    - Set $x = 2$.
    - Even(x) holds.
    - Prime(x) holds.
    - Therefore, $Even(x) \wedge Prime(x)$ holds.
    - Done.
  - This proof is **constructive**, because we constructed an x which makes the formula $Even(x) \wedge Prime(x)$ true.

Existential instantiation/generalization

- If you can find an element $a \in S$ such that $F(a)$, then $\exists x \in S, F(x)$
  - This is called **existential generalization**.

- Alternatively, if $\exists\ x \in S\ \ F(x)$ is true, then you can give that element of S for which $F(x)$ is true **a name**, as long as that name has not been used elsewhere.
  - This is called the **existential instantiation** rule.
    - $\exists x \in \mathbb{N}\ \ (x - 5 = 0)$
    - $\therefore\ \ k = 0 + 5$

Proof of the form $\forall x\ F(x)$

- To prove that something of the form $\forall x\ F(x)$:
  - Make sure it holds in every scenario (method of exhaustion)
    - For all possible values of A and B, $\neg B \rightarrow \neg A$ is equivalent to $A \rightarrow B$, by checking the truth table.
  - But there can be too many scenarios!
    - For any integer, there is a larger integer which is a prime.
    - For any two reals, there is a real between them.
  - Instead, use **axioms and rules of inference** to derive it.

    $\neg B \rightarrow \neg A \equiv \neg\neg B \vee \neg A \equiv B \vee \neg A \equiv \neg A \vee B \equiv A \rightarrow B$
    - So $(\neg B \rightarrow \neg A) \leftrightarrow (A \rightarrow B)$ is a tautology.
    - And, therefore, $\forall A, B \in \{True, False\}$, $\neg B \rightarrow \neg A \equiv A \rightarrow B$

Universal instantiation/generalization

- In general, if $\forall\ x \in S\ \ F(x)$ is true for some formula $F(x)$, if you take any specific element $a \in S$, then $F(a)$ must be true.
  - This is called the **universal instantiation** rule.
    - $\forall x \in \mathbb{N}\ \ (x > -1)$
    - $\therefore\ \ 5 > -1$

- If you prove $F(a)$ without any assumptions about a other than $a \in S$, then $\forall x \in S, F(x)$
  - This is called **universal generalization**.

Types of proofs

- **Direct proof of $\forall x\, F(x)$**
  - Show that $F(x)$ holds for arbitrary x, then use universal generalization.
    - Often, $F(x)$ is of the form $G(x) \rightarrow H(x)$
  - Example: A sum of two even numbers is even.
- **Proof by cases**
  - If can write $\forall x\, F(x)$ as $\forall x(G_1(x) \vee G_2(x) \vee \cdots \vee G_k(x)) \rightarrow H(x)$, prove $\big(G_1(x) \rightarrow H(x)\big) \wedge (G_2(x) \rightarrow H(x)) \wedge \cdots \wedge (G_k(x) \rightarrow H(x))$
  - Example: Sum of an integer with a consecutive integer is odd.
- **Proof by contraposition**
  - To prove $\forall x\ \ G(x) \rightarrow H(x)$, prove $\forall x\, \neg H(x) \rightarrow \neg G(x)$
  - Example: If square of an integer is even, then this integer is even.

    Example: The Pigeonhole Principle
- **Proof by contradiction:** To prove $\forall x\, F(x)$, prove $\forall x\, \neg F(x) \rightarrow FALSE$
  - Example: To prove "$\sqrt{2}$ is not a rational number", we prove that "$\sqrt{2}$ is rational" leads to a contradiction.
  - Example: To prove $((C \vee x) \wedge (D \vee \neg x) \rightarrow (C \vee D))$ is a tautology, we can prove $\neg((C \vee x) \wedge (D \vee \neg x) \rightarrow (C \vee D))$ is false.

Set Theory

Sets

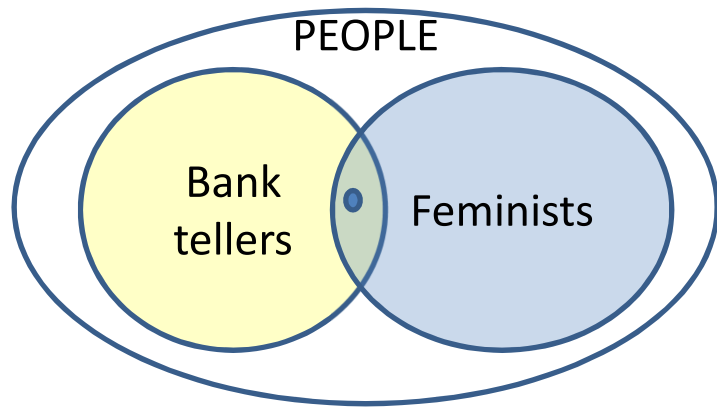
- A **set** is a collection of objects.
  - S_1={1, 2, 3}, S_2 = {Cathy, Alan, Keiko, Daniela}
  - S_3 = [-1, 2] (real numbers from -1 to 2, inclusive)
  - PEOPLE = {x | x is a person living on Earth now}
    - {x | such that x ... } is called **set builder notation**
  - S_4 = { (x,y) | x and y are people, and x is a parent of y}
  - BANKTELLERS = { x | x is a person who is a bank teller}
- The order of elements does not matter.
- There are no duplicates.

Special sets

- Notation for some **special sets** (much of which you are likely to have seen):
  - **Empty set** $\emptyset$
  - **Natural numbers** $\mathbb{N} = \{1, 2, 3, \dots\}$ (sometimes with 0)
  - **Integers** $\mathbb{Z} = \{\dots -2, -1, 0, 1, 2, \dots\}$
  - **Rational numbers** $\mathbb{Q} = \left\{\frac{m}{n} \;\middle|\; m, n \; in \; \mathbb{Z}, n \neq 0\right\}$
  - **Real numbers** $\mathbb{R}$
  - **complex numbers** $\mathbb{C}$

Set elements

- $\boldsymbol{a} \in \boldsymbol{S}$ means that an element a is in a set S, and $\boldsymbol{a} \notin \boldsymbol{S}$ that a is not in S.
  That is, $\boldsymbol{a} \in \boldsymbol{S} \equiv \neg\,(\boldsymbol{a} \notin \boldsymbol{S})$
  – Susan ∈ PEOPLE,
    Susan ∉ BANKTELLERS
  – $0.23 \ \in [-1, 2]$. $\ 3.14 \notin [-1, 2]$

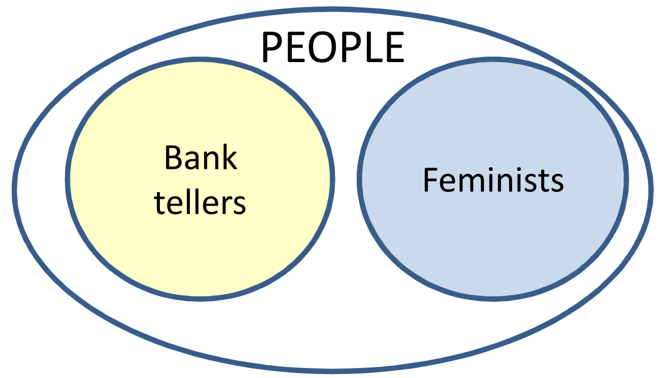


- Also, write $\boldsymbol{x} \in \boldsymbol{S}$ for **a variable $\boldsymbol{x}$**.
  – BANKTELLERS = { $x \in PEOPLE$ | x is a bank teller}

- How do we generalize sentences like “x is a bank teller”, where x is an element of some set?

Set inclusion.

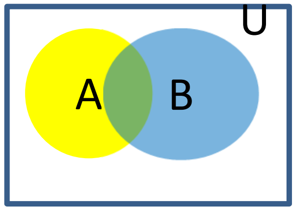
- Let A and B be two sets.
  - Such as A={2,3,4} and B= {1,2,3,4,5}
- A is a **subset** of B:
  - $A \subseteq B$ iff $\forall x\ (x \in A \rightarrow x \in B)$
    - $A \subseteq B.\ FEMINISTS \subseteq PEOPLE$
  - A is a **strict subset** of B:
    - $A \subset B$ iff $\forall x\ (x \in A \rightarrow x \in B) \land \exists\, y\ (y \in B \land y \notin A)$
    - $A \subset B.\ FEMINISTS \subset PEOPLE$
  - **When both $\boldsymbol{A \subseteq B}$ and $\boldsymbol{B \subseteq A}$, then $\boldsymbol{A = B}$**



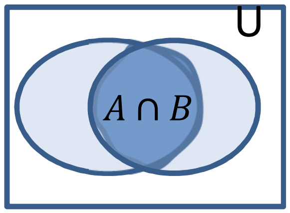
- A and B are **disjoint** iff $\forall x\ (x \notin A \lor x \notin B)$
  - {1,5} and {2,3,6,9} are disjoint. So are BANKTELLERS and FEMINISTS in the diagram above.

Operations on sets

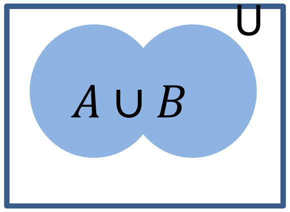
- Let A and B be two sets.
  - Such as A={1,2,3} and B={ 2,3,4}



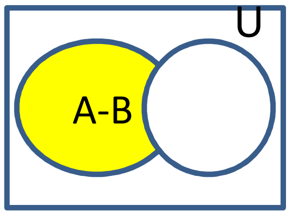
- **Intersection** $A \cap B = \{ x \mid x \in A \land x \in B\}$
  - The blue part in the picture
  - $A \cap B = \{2,3\}$



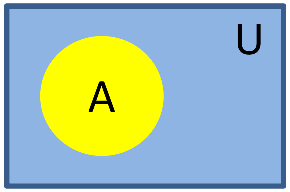
- **Union** $A \cup B = \{ x \mid x \in A \lor x \in B\}$
  - The blue part in the picture.
  - $A \cup B = \{1,2,3,4\}$



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

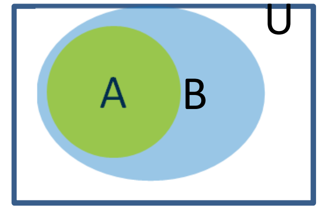


- **Complement** $\overline{A} = \{x \in U \mid x \notin A\}$
  - The blue part on the bottom diagram
  - If universe U = ℕ, $\overline{A} = \{x \in \mathbb{N} \mid x \notin \{1,2,3\} \}$

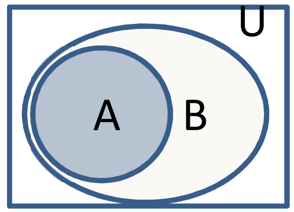


Subsets and operations

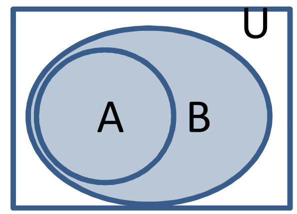
- If $A \subseteq B$ then



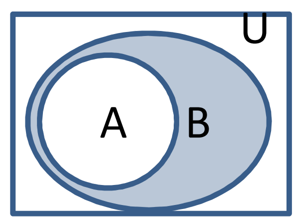
  - Intersection $A \cap B =$
    - **A**



  - Union $A \cup B =$
    - $\boldsymbol{B}$



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

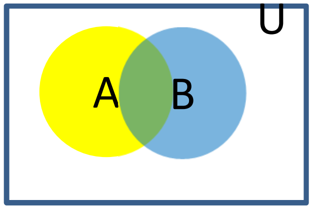


Size (cardinality)

- 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

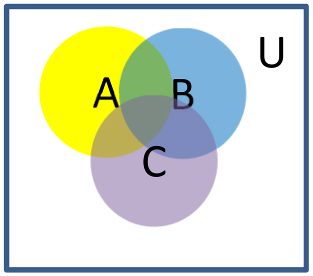


- Let A and B be two sets. Then the cardinality:

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

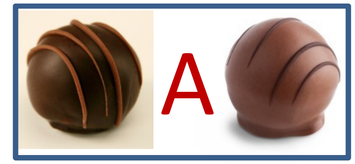
  - **Proof idea**: notice that elements in $|A \cap B|$ are counted twice in |A|+|B|, so need to subtract one copy.
  - If A and B are **disjoint**, then $|A \cup B| = |A| + |B|$
  - If there are 220 students in CS2209A, 100 in CS2210A, and 50 of them are in both, then the total number of students in 2209 or 2210 is 220+100-50=270.

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

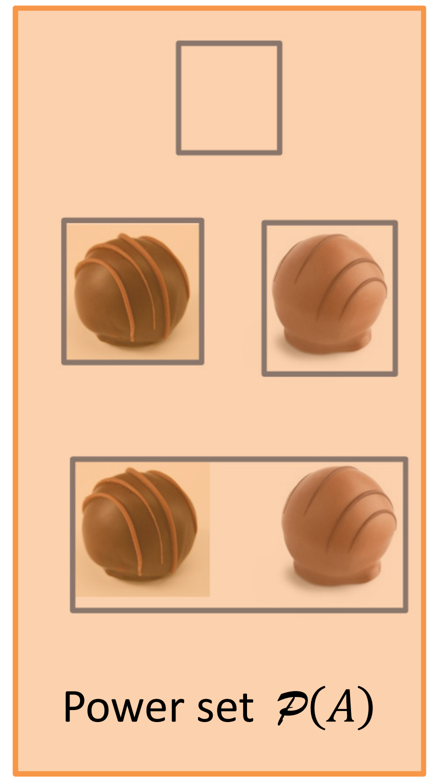


Power sets

- 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}, $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$
  - $A = \emptyset$, $\mathcal{P}(A) = \{\emptyset\}$.
    - 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.



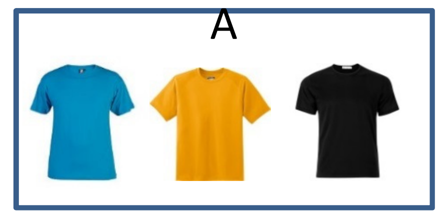
Subsets of A:



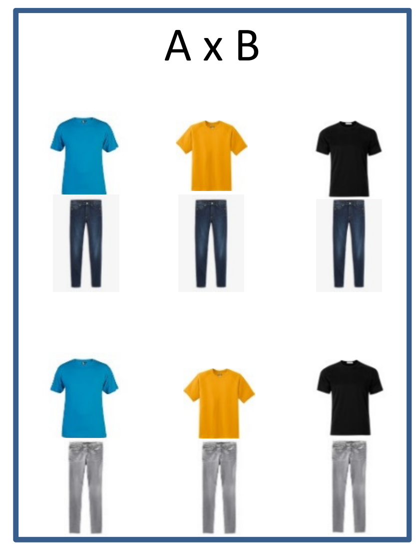
Cartesian products

- **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 = $\{(x, y) \mid x \in A,\ y \in B\}$
  - 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}, $A \times A = \{(1,1), (1,2), (2,1), (2,2)\}$

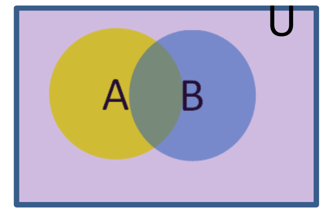
	a	b
1	(1,a)	(1,b)
2	(2,a)	(2,b)
3	(3,a)	(3,b)



- 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:
  - $A_1 \times A_2 \times \cdots \times A_k = \{(x_1, x_2, \ldots x_k) \mid x_1 \in A_1 \ldots x_k \in A_k\}$
  - $A = \{1,2,3\}$, 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 $\overline{A \cup B} = \overline{A} \cap \overline{B}$