CS TBC: Theory Bridge Course

Instructor: Kevin Milans

Website: http://www.cs.uiuc.edu/class/su07/cstbc

- No Grades
- 3 lectures / wk for 9 weeks
- Exercises after each class
- 3 "exams"; graded if you wish

GOAL: Think clearly and logically.

Keys to success: patience and practice.

- Do not expect to solve every problem.
- But, attack all of them.
- You should be confident your answers are correct.

How can we be confident?

- Have patience to check all details of your solution carefully, several times.
- Even if a step is not worth writing down, check it in your head.
- Tinker with your solution. Ask:
  - Which steps are necessary?
  - Does it still work if I make small changes?
  - Am I using all the given information?
  - !! $\Longrightarrow$ Does my solution make sense with respect to small examples?

It is vitally important to know when you have found a correct solution.

Many mathematical statements, some true some false.

Ex: (1) There are infinitely many prime numbers.

(2) There is a largest integer.

(3) Given the program:

<u>Collatz</u>(n):

```
If n = 1 then halt
If n is even then
    Collatz(n/2)
else
    Collatz(3n + 1)
```

For each integer $n \geq 1$, Collatz(n) halts.

Ex: Collatz(3) $\mapsto$ Collatz(10) $\mapsto$ Collatz(5) $\mapsto$ Collatz(16) $\mapsto \dots \mapsto$ Collatz(1).

How can we tell which statements are true and which are false?

The only way is with a rigorous mathematical argument; we call these arguments <u>proofs</u>.

Think of a proof as a program which gives precise and mechanical instructions for understanding why a statement is true.

When we know a statement is true because we have found a proof, the statement is called a <u>theorem</u>.

Sets

- A **set** is a collection of objects

Ex:
- Emptyset $\emptyset$
- $\{1, 3, 5, 7\}$
- $\{1, 2, 3, \dots, 1000\}$
- $\{a, b, c, \dots, z\}$
- $\{\emptyset, \{1\}, \{1,3\}, \{1,3,5\}\}$
- $\{1, 2, 3, \dots\}$

- Recall: two sets are equal iff they contain the same objects.

$\Rightarrow$ Sets do not "remember"

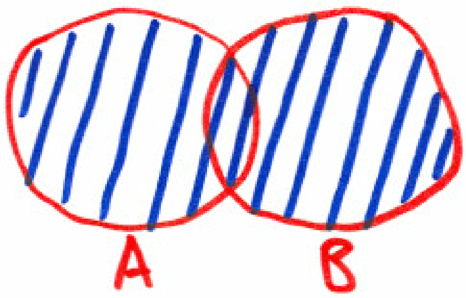
(·) order $\{1,3,5,7\} = \{3,5,7,1\}$

(·) multiplicity $\{1,3,5,7\} = \{1,3,3,5,7\}$

Set Notation

- **Membership** $5 \in \{1,3,5,7\}$, $6 \notin \{1,3,5,7\}$

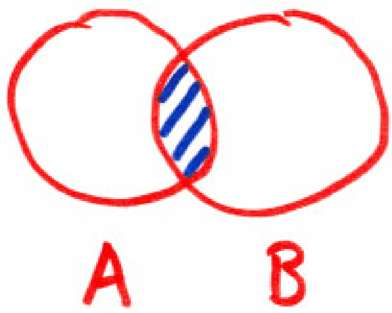
- **Union:**



$A \cup B$

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

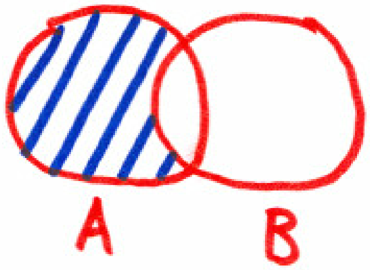
- **Intersection:**



$A \cap B$

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

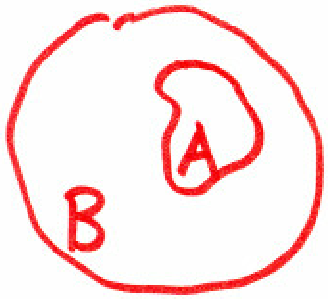
- **Set Difference:**



$A - B$

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

- **Containment:** If A and B are sets and each element of A is also an element of B, then A is a **subset** of B.



$$A \subseteq B$$

- **Power set:** If A is a set, the **powerset** of A is the set whose elements are all subsets of A

$$\mathcal{P}(\{1,2,4\}) = \{\emptyset, \{1\}, \{2\}, \{4\}, \{1,2\}, \{1,4\}, \{2,4\}, \{1,2,4\}\}$$

- **Cardinality** If A is a finite set, then $|A|$ is the number of elements in A.

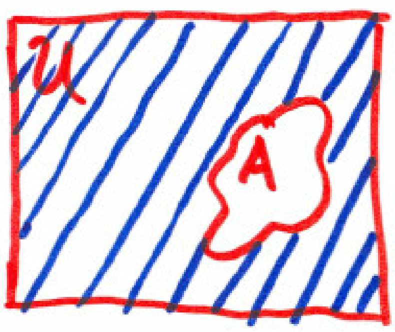
$$|\{1,3,5,7\}| = 4$$

$$|\emptyset| = 0$$

$$|\{a,b,\ldots,z\}| = 26$$

$$|\mathcal{P}(A)| = ?$$

- **Complementation** Relative to a universe $\mathcal{U}$, the complement of a set A is the set $\mathcal{U} - A$.

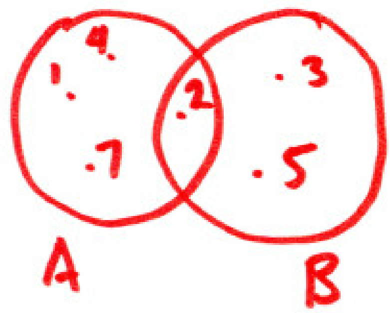


$$\overline{A}$$

$$\overline{A} = \{x \mid x \in \mathcal{U} \text{ and } x \notin A\}$$

Thrm If A and B are finite sets, then $|A \cup B| = |A| + |B| - |A \cap B|$.

Ex:



$A = \{1, 2, 4, 7\}$

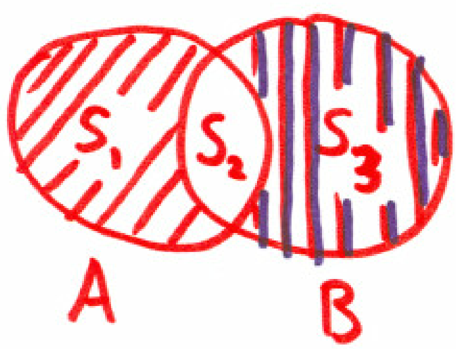
$B = \{2, 3, 5\}$

$A \cup B = \{1, 2, 3, 4, 5, 7\}$

$A \cap B = \{2\}$

$6 = |A \cup B|$ & $|A| + |B| - |A \cap B| = 4 + 3 - 1 = 6$

Proof: Let $S_1 = A - B$, $S_2 = A \cap B$, and $S_3 = B - A$.



Note that $|A \cup B| = |S_1| + |S_2| + |S_3|$

$|A| = |S_1| + |S_2|$

$|B| = |S_2| + |S_3|$

$|A \cap B| = |S_2|$.

Therefore $|A| + |B| - |A \cap B| = |S_1| + |S_2| + |S_3| = |A \cup B|$. ■

9.1

Cartesian Product

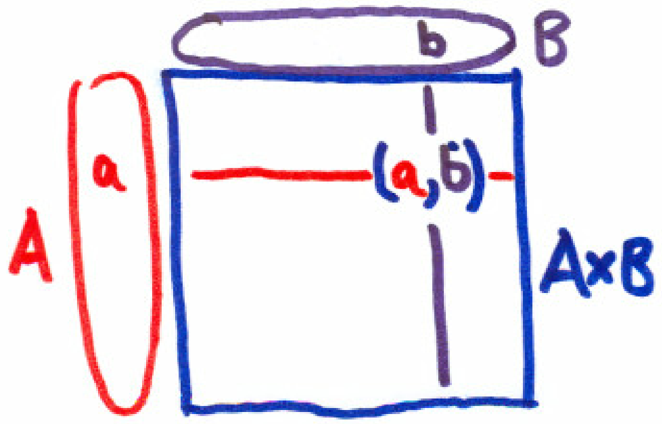
def Given sets A and B, the <u>product</u> of A and B, written $\underline{A \times B}$, is the set of ordered pairs whose first elt. is in A and whose second elt. is in B.

$$A \times B = \{(a,b) \mid a \in A \ \underline{\text{and}} \ b \in B\}$$

Ex: $A = \{a, b, c\}$, $B = \{1, 2\}$

$$A \times B = \{(a,1), (a,2), (b,1), (b,2), (c,1), (c,2)\}$$

Note:



$$|A \times B| = |A| \cdot |B|$$

def Given sets $A_1, A_2, \ldots, A_n$, the <u>product</u> $A_1 \times A_2 \times \cdots \times A_n$ is

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid \forall j \ \ a_j \in A_j\}$$

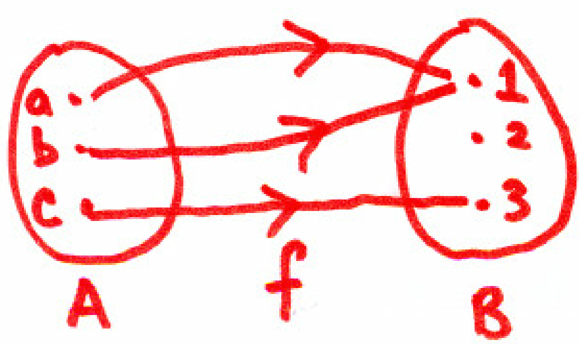
<u>Note</u>: $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|$

def Define A^n to be $\underbrace{A \times A \times \cdots \times A}_{n \text{ times}}$.

<u>Functions</u>

def A <u>function</u> f from a set A to a set B assigns to each $a \in A$ an element $b \in B$. We may write $f: A \to B$.

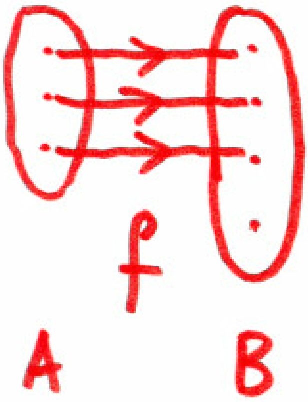
We say that the <u>domain</u> of f is A and the <u>codomain</u> of f is B.



$f(a) = 1$
$f(b) = 1$
$f(c) = 3$

def A function $f: A \to B$ is an **injection** (adj. **injective**) if for all $a_1, a_2 \in A$ with $a_1 \neq a_2$, we have $f(a_1) \neq f(a_2)$.

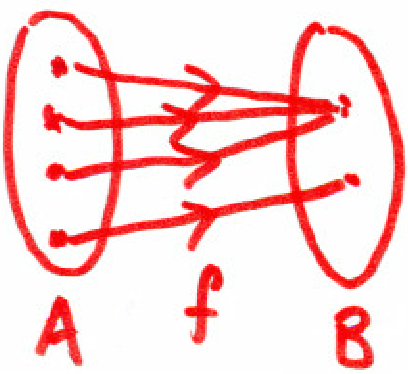
Ex:



f is an injection
f is not a surjection

def A function $f: A \to B$ is a **surjection** (adj. **surjective**) if forall $b \in B$ there exists $a \in A$ such that $f(a) = b$.
(Equivalently, $\forall b \in B \; \exists a \in A \; f(a) = b$.)

Ex:

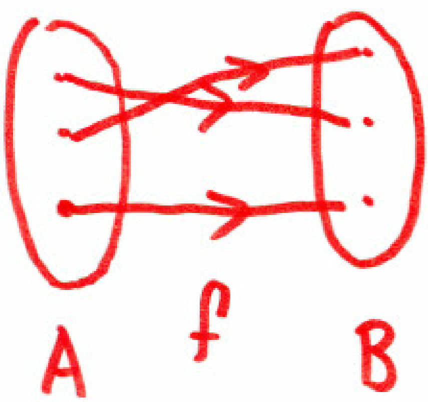


f is a surjection
f is not injective

(9.4)

def A function $f: A \to B$ is a **bijection** (adj. **bijective**) if it is both injective and surjective.

Ex:



f is a bijection

Note: If $f: A \to B$ is a

- injection, $|A| \le |B|$
- surjection, $|A| \ge |B|$
- bijection, $|A| = |B|$

This is actually <u>very</u> useful.

An Application: How large is the powerset?

<u>Thm</u> Let $n \geq 0$ and $\mathcal{U} = \{1, 2, \dots, n\}$. There is a bijection from $\mathcal{P}(\mathcal{U})$ to $\{0,1\}^n$.

Pf: We <u>construct</u> a bijection $f : \mathcal{P}(\mathcal{U}) \to \{0,1\}^n$.

(·) Fix a set $A \in \mathcal{P}(\mathcal{U})$; we choose a value $f(A) \in \{0,1\}^n$ as follows. By definition of $\mathcal{P}(\mathcal{U})$, $A \subseteq \mathcal{U}$.
For each $1 \leq j \leq n$, define

$$x_j = \begin{cases} 0 & j \notin A \\ 1 & j \in A \end{cases}$$

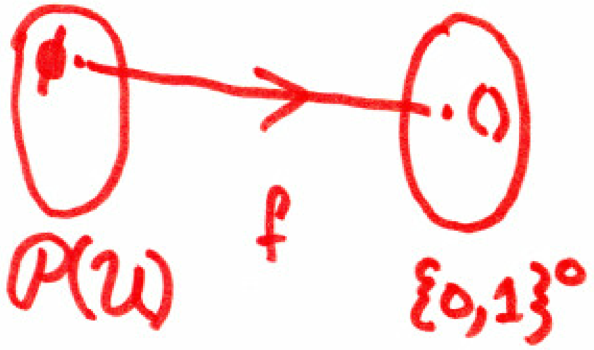
and we choose $f(A) = (x_1, x_2, \dots, x_n)$.

(·) Now f is <u>injective</u>: if $A_1, A_2 \in \mathcal{P}(\mathcal{U})$ and $A_1 \neq A_2$, then A_1 and A_2 disagree on the membership of some $j \in \mathcal{U}$. Hence, $f(A_1)$ and $f(A_2)$ differ in the jth coordinate, so $f(A_1) \neq f(A_2)$.

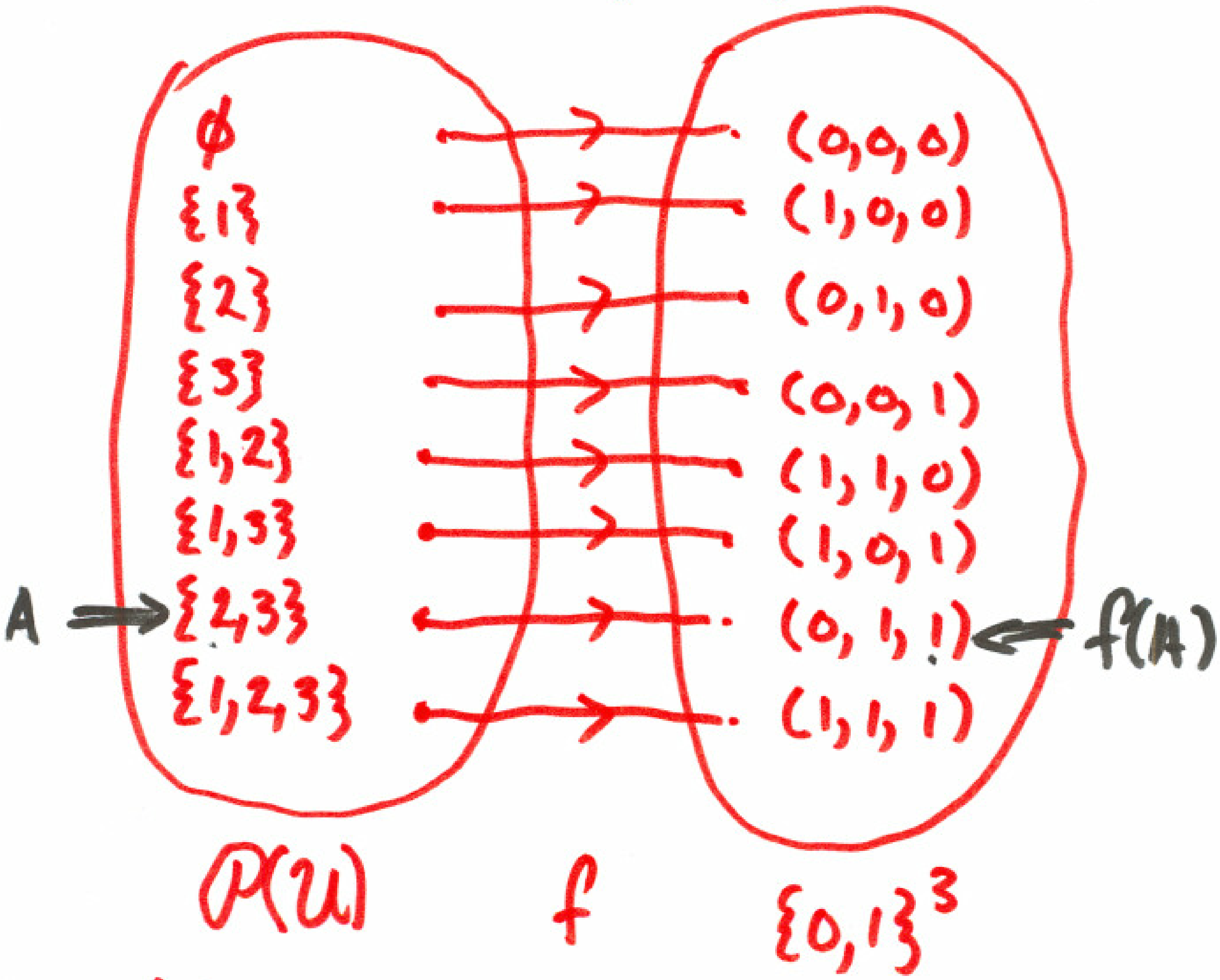
(·) Also, f is <u>surjective</u>: if $(x_1, \dots, x_n) \in \{0,1\}^n$, then we set $A = \{j \mid x_j = 1\}$ and note $f(A) = (x_1, \dots, x_n)$.

(·) Therefore, f is <u>bijective</u>. ∎

Ex: $n = 0$ $\quad \mathcal{U} = \{\} = \emptyset$



Ex: $n = 3$ $\quad \mathcal{U} = \{1, 2, 3\}$



Cor $|\mathcal{P}(\mathcal{U})| = |\{0,1\}^n| = 2^n$

Consider an integer $n \geq 1$ and the universe $\mathcal{U} = \{1, 2, \ldots, n\}$.

def A family $\mathcal{A} \subseteq \mathcal{P}(\mathcal{U})$ of subsets of $\mathcal{U}$ is <u>pairwise intersecting</u> if for each pair $A, B \in \mathcal{A}$, $A \cap B \neq \emptyset$.

(Equivalently, $A, B \in \mathcal{A} \Longrightarrow A \cap B \neq \emptyset$.)

Thm If $\mathcal{A} \subseteq \mathcal{P}(\mathcal{U})$ is pairwise intersecting, then $|\mathcal{A}| \leq 2^{n-1}$.

Note: If $\mathcal{A} = \{A \subseteq \mathcal{U} \mid 1 \in A\}$, then $\mathcal{A}$ is pairwise intersecting and $|\mathcal{A}| = 2^{n-1}$

Ex: $\mathcal{U} = \{1, 2, 3\}$, $\mathcal{A} = \{\{1\}, \{1,2\}, \{1,3\}, \{1,2,3\}\}$

$|\mathcal{A}| = 4 = 2^{3-1}$

Thm If $\mathcal{A} \subseteq \mathcal{P}(\mathcal{U})$ is pairwise intersecting, then $|\mathcal{A}| \le 2^{n-1}$.

Pf: Let $\mathcal{A} \subseteq \mathcal{P}(\mathcal{U})$ be a pairwise intersecting family. Let $k = 2^n$ be the number of subsets of $\mathcal{U}$. Because $\overline{(\overline{A})} = A$, complementation groups the subsets of $\mathcal{U}$ into $k/2$ complementary pairs. Because $\mathcal{A}$ is pairwise intersecting, $\mathcal{A}$ includes at most one set from each complementary pair. Therefore $|\mathcal{A}| \le k/2 = 2^{n-1}$. ■

Ex: $n = 3$, $\mathcal{U} = \{1, 2, 3\}$

$$\mathcal{P}(\mathcal{U}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2,3\}, \{2,3\}, \{1,3\}, \{1,2\}\}$$

$$\mathcal{A} = \{\{1\}, \{1,2\}, \{1,3\}, \{1,2,3\}\}$$