ITB8832 Mathematics for Computer Science
Lecture 4 – 25 September 2023

Contents

Next section

Sets

Definition (informal)

A *set* is an aggregate of objects, called the *elements* of the set.

Sets can be given as *lists* or as *descriptions*:

$$\begin{array}{lcll} A & ::= & \{2,3,5,7,11,13,17,19\} & \text{primes smaller than 20} \\ B & ::= & \{\{\mathsf{T}\},\{\mathsf{F}\},\{\mathsf{T},\mathsf{F}\}\} & \text{nonempty sets of Booleans} \\ C & ::= & \{1,2,3,4,\ldots\} & \text{positive integers} \\ D & ::= & \{\text{Sephiroth, Bowser, Diablo, } \ldots\} & \text{villains from video games} \end{array}$$

The symbol $::=$ is read "is equal by definition to", or "is defined as".
Order and repetition *do not* matter, only elements do:

$$\begin{aligned} \{\text{Sephiroth, Bowser, Diablo}\} &= \{\text{Bowser, Diablo, Sephiroth}\} \\ \{\text{Bowser, Bowser, Bowser}\} &= \{\text{Bowser}\} \end{aligned}$$

Elements of a set

Notation

"$x \in X$" means "the object x is an element of the set X".
"$x \notin X$" means "the object x is not an element of the set X".

Usually, when given generic names:

- *elements* are denoted by *uncapitalized* letters;
- *sets* are denoted by *capitalized* letters.

Examples:

- $17 \in \{2,3,5,7,11,13,17,19\}$.
- $\{\mathsf{T}\} \in \{\{\mathsf{T}\},\{\mathsf{F}\},\{\mathsf{T},\mathsf{F}\}\}$.
- $\text{Bowser} \in \{\text{Bowser, Diablo, Sephiroth}\}$.

Non-examples:

- $\mathsf{T} \notin \{\{\mathsf{T}\},\{\mathsf{F}\},\{\mathsf{T},\mathsf{F}\}\}$.
  Do not confuse the *object* T with the *singleton* $\{\mathsf{T}\}$ whose only element is T.
- $\text{Bowser} \notin \{2,3,5,7,11,13,17,19\}$.

Commonly used sets

Symbol	**Name**	**Elements**
$\emptyset$	empty set	
$\mathbb{B}$	Boolean values	T, F
$\mathbb{N}$	natural numbers	$0, 1, 2, 3, \ldots$
$\mathbb{Z}$	integers	$\ldots, -2, -1, 0, 1, 2, 3, \ldots$
$\mathbb{Q}$	rational numbers	$0, 1, -1, \frac{1}{2}, -\frac{3}{7}, 17, \ldots$
$\mathbb{R}$	real numbers	$0, 1, -1, \frac{1}{2}, -\frac{3}{7}, 17, \sqrt{2}, \pi, \ldots$
$\mathbb{C}$	complex numbers	$i, \frac{1}{2}, 17, 1 + i\sqrt{2}, e^{i\pi} + 1, \ldots$
$\mathbb{Z}^+$	positive integers	$1, 2, 3, \ldots, 17, \ldots$
$\mathbb{R}^+$	positive reals	$1, e, \pi, 17, 10^{10^{100}}, \ldots$
$\mathbb{R}^{\geq 0}$	non-negative reals	$0, 1, e, \pi, 17, 10^{10^{100}}, \ldots$
$\mathbb{Z}^-$	negative integers	$-1, -2, -3, \ldots, -17, \ldots$
$\mathbb{R}^-$	negative reals	$-1, -e, -\pi, -17, -10^{10^{100}}, \ldots$

Comparisons between sets

Definition

A set X is a *subset* of a set Y if every object which is an element of X is also an element of Y.
In this case, we write: $X \subseteq Y$.

If $X \subseteq Y$ but some elements of Y are not elements of X, we may write $X \subset Y$.
Examples:

- $\emptyset \subseteq X$ for every set X.
  Otherwise, there would exist $z \in \emptyset$ such that $z \notin X$...
- $\mathbb{Z}^+ \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.
- $\{2,3,5\} \subset \{2,3,5,7\}$.
- $\{2,3,5\} \nsubseteq \{2,3,7\}$. But $\{2,3,7\} \nsubseteq \{2,3,5\}$ either.

Set construction: Union

Definition 4.1.1.

The *union* of the sets X and Y is the set $X \cup Y$ such that:

$$x \in X \cup Y \text{ iff } x \in X \text{ or } x \in Y$$

Examples:

- $\{2,3,5\} \cup \{2,3,7\} = \{2,3,5,7\}$.
- $\{2,3,5\} \cup \{\text{Bowser, Sephiroth}\} = \{2,3,5,\text{Bowser, Sephiroth}\}$.
- $X \cup \emptyset = \emptyset \cup X = X$ whatever the set X is.
  In particular: $\emptyset \cup \emptyset = \emptyset$.

Set construction: Intersection

Definition 4.1.1. (cont)

The *intersection* of the sets X and Y is the set $X \cap Y$ such that:

$$x \in X \cap Y \text{ iff } x \in X \text{ and } x \in Y$$

Examples:

- $\{2,3,5\} \cap \{2,3,7\} = \{2,3\}$.
- $\{2,3,5\} \cap \{\text{Bowser, Sephiroth}\} = \emptyset$.
- $X \cap \emptyset = \emptyset \cap X = \emptyset$ whatever the set X is.
  In particular: $\emptyset \cap \emptyset = \emptyset$.

Set construction: Difference

Definition 4.1.1. (cont)

The *difference* of the sets X and Y is the set $X - Y$ such that:

$$x \in X - Y \text{ iff } x \in X \text{ and not}(x \in Y)$$

Examples:

- $\{2,3,5\} - \{2,3,7\} = \{5\}$.
- $\{2,3,5\} - \{\text{Bowser, Sephiroth}\} = \{2,3,5\}$.
- $X - \emptyset = X$ and $\emptyset - X = \emptyset$ whatever the set X is.
  In particular: $\emptyset - \emptyset = \emptyset$.
- If X and Y are any two sets, then:

$$\begin{aligned} X &= (X \cap Y) \cup (X - Y) \\ X \cup Y &= (X \cap Y) \cup (X - Y) \cup (Y - X) \end{aligned}$$

Set construction: Complement

For this construction, it is necessary that a *domain* D be defined, such that every object which is element of any set is also an element of D.

Definition

The *complement* of the set X with respect to the domain D is the difference set

$$\overline{X} = D - X$$

Examples:

- If $D = \mathbb{Z}$ then $\overline{\mathbb{N}} = \mathbb{Z}^-$.
- If $D = \{\text{Bowser, Diablo, Sephiroth}\}$ then $\overline{\{\text{Bowser, Sephiroth}\}} = \{\text{Diablo}\}$.

Construction: Power set

Definition

The *power set* of a set X is the set $\mathrm{pow}(X)$ whose elements are all and only the subsets of X.

Examples:

- $\mathrm{pow}(\emptyset) = \{\emptyset\}$.
- $\mathrm{pow}(\{\mathsf{T},\mathsf{F}\}) = \{\emptyset, \{\mathsf{T}\}, \{\mathsf{F}\}, \{\mathsf{T},\mathsf{F}\}\}$.
- $\mathrm{pow}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.

Note: power sets are never empty as $\emptyset \in \mathrm{pow}(X)$ for every set X.

Set builder notation

The notation

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

means:

S is defined as the set of
all and only those elements x of the set X
such that the predicate $P(x)$ is true

The right-hand side is read: "the set of the x in X such that $P(x)$".
Examples:

- $D ::= \{z \in \mathbb{C} \mid \Re z = \Im z\}$.
  This is the *main diagonal* of the complex plane.
- $E ::= \{z \in \mathbb{C} \mid \exists x, y \in \mathbb{R}. (z = x + iy \wedge x^2 + 4y^2 = 1)\}$.
  This is the *ellipse* of width 2 and height 1.
- $\mathrm{Primes} ::= \{x \in \mathbb{N} \mid x > 1 \wedge \forall a, b \in \mathbb{N}. ((a \leq b \wedge ab = x) \longrightarrow (a = 1 \wedge b = x))\}$.

A variant of the set builder notation

Let $E(x)$ be an expression that, for every $x \in X$, represents an element of Y.
Then:

$$S ::= \{E(x) \mid x \in X\}$$

means:

S is defined as the set of
all and only the objects of the form $E(x)$
where x is an element of X.

and defines the same set as:

$$S ::= \{y \in Y \mid \exists x \in X \,.\, y = E(x)\}$$

The right-hand side is read: "the set of the $E(x)$ for x in X".
Examples:

- $D ::= \{t + it \mid t \in \mathbb{R}\}$.
  This is again the main diagonal of the complex plane.
- $\mathbb{N} ::= \{0\} \cup \{x + 1 \mid x \in \mathbb{N}\}$.
  This is an example of a *recursive* definition.

Equality between sets

Definition

Two sets are *equal* if and only if they have the same elements.

Equivalently[1]:

$$X = Y \text{ iff } X \subseteq Y \text{ and } Y \subseteq X$$

Examples:

- $\emptyset = \{x \in \mathbb{N} \mid x \neq x\}$.
- $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$.
- $\{x \in \mathbb{R} \mid x^2 - 3x + 2 < 0\} = \{x \in \mathbb{R} \mid 1 < x < 2\}$.
- $\{p \in \mathrm{Primes} \mid p = 2 \text{ or } \exists k \in \mathbb{Z}\,.\, p = 4k + 1\} = \{p \in \mathrm{Primes} \mid \exists a, b \in \mathbb{Z}\,.\, p = a^2 + b^2\}$.
  (This nontrivial result is due to *Pierre de Fermat*.)

[1] Check that the equivalence is true!

Proving Set Equalities

A set equality is, in its essence, an "if and only if" proposition.

Theorem 4.1.2. (Distributive law for sets)

However given three sets A, B, and C,

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

1. Translate the set equality into an "if and only if" proposition:

$$\forall x. (x \in A \cap (B \cup C) \text{ iff } x \in (A \cap B) \cup (A \cap C))$$

2. Prove the "if and only if" proposition: however chosen x,

$$\begin{aligned} x \in A \cap (B \cup C) \quad & \text{iff} \quad x \in A \text{ and } (x \in B \text{ or } x \in C) \\ & \text{iff} \quad (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C) \\ & \text{iff} \quad x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

Cheat sheet for set equality

There is a good correspondence between operations on sets and operations on propositions:

- Logical `or` corresponds to set *union*.
- Logical `and` corresponds to set *intersection*.
- Logical not() corresponds to set *complementation*.
  (For this, a domain *must* have been defined.)
- Logical `implies` corresponds to set *inclusion*.
- Logical `iff` corresponds to set *equality*.

However, *do not* mix the two things, as they have different *types*:

- You can do an intersection of sets: not a conjunction of sets.
- You can do a conjunction of propositions: not an intersection of propositions.

Next section

Sequences

Definition

A *sequence* of *length* n is a list of n objects

$$(x_1, x_2, \ldots, x_n)$$

Where a set is a *collection*, a sequence is a *list*:

- Order counts:
  $(\text{Sephiroth}, \text{Bowser}, \text{Diablo}) \neq (\text{Bowser}, \text{Diablo}, \text{Sephiroth})$.
- Entry values can be repeated:
  $(\text{Bowser}, \text{Bowser}, \text{Bowser}) \neq (\text{Bowser})$.

As there is an empty set, so there is an *empty sequence* of length 0:
we denote it as λ.

Cartesian products

Definition

The *Cartesian product* of the sets $S_1, S_2, \ldots, S_n$ is the set

$$S_1 \times S_2 \times \ldots \times S_n$$

of the sequences of length n where, for each i from 1 to n, the ith object is an element of S_i.

If $S_1 = S_2 = \ldots = S_n = S$ we denote the Cartesian product as S^n.
Examples:

- $\mathbb{N} \times \mathbb{B} = \{(n, b) \mid n \in \mathbb{N}, b \in \mathbb{B}\} = \{(0, \mathsf{T}), (0, \mathsf{F}), (1, \mathsf{T}), (1, \mathsf{F}), \ldots\}$
- $(17, \text{Diablo}) \in \mathbb{N} \times \{\text{video game villains}\}$.
- $(1, e, \pi) \in \mathbb{R}^3$.

Next section

Functions

Definition

A *function* with *domain* A and *codomain* B is a rule f which assigns to each element x of the set A a unique element $f(x)$ (read "f of x") of the set B.

Notation:

- $f : A \to B$ means: f is a function with domain A and codomain B.
- $f(a) = b$ means: f assigns *value* b to object a.
  We can also say: b is the value of f at *argument* a.

Function definition: Formula

Functions can be given by a *formula:*

- $f_1(x) ::= 1/x^2$ where $x \in \mathbb{R}$.
  Here, $f_1(x)$ is not defined for $x = 0$: f_1 is a *partial* function.
- $f_2(x, y) ::= y10x$ where x and y are binary strings of finite length.
  For example: $f_2(10, 001) = 0011010$.
- $f_3(x, n) ::= \text{the length of the sequence } (x, x, \ldots, x) \text{ (} n \text{ repetitions)}$ where $x \in \mathbb{R}$ and $n \in \mathbb{N}$.
  You can think of a function with many arguments as a function with a single argument defined on a Cartesian product.
- $[P] ::= \text{the truth value of } P$ where P is a proposition.
  These are sometimes called *Iverson brackets*.

Function definition: Look-Up Table

A function with finite domain can be defined via its *look-up table*.

- Suppose $f_4(P,Q)$, where P and Q are Boolean variables, has the following look-up table:

P	Q	$f_4(P,Q)$
T	T	T
T	F	F
F	T	T
F	F	T

The look-up table above is the truth table of implication, so:

$$f_4(P,Q) = [P \text{ implies } Q]$$

Function definition: Procedure

Let x vary in the binary strings and let f_5 return the length of a left-to-right search on x until the first 1 is found.
That is:

$$f_5(x) ::= \begin{cases} 1 & \text{if } x = 1y\,, \\ 1 + f_5(y) & \text{if } x = 0y\,. \end{cases}$$

Then:

$$\begin{aligned} f_5(100) &= 1 \\ f_5(00111) &= 3 \\ f_5(00000) &= ??? \end{aligned}$$

So this is a partial function too. *Exercise:* how to make it total?

Image of a set by a function

Definition

If $f : A \to B$ and $S \subseteq A$, then:

$$f(S) = \{b \in B \mid \exists a \in S \,.\, f(a) = b\}$$

is the *image* of S under f.

Examples:

- If $S = [1,2] = \{x \in \mathbb{R} \mid 1 \leq x \leq 2\}$, then $f_1(S) = [1/4, 1]$.
- If $S = \mathbb{R}$, then $f_1(S) = \mathbb{R}^+$.
- If $S = \{(\mathrm{T},\mathrm{T}),(\mathrm{F},\mathrm{T}),(\mathrm{F},\mathrm{F})\}$, then $f_4(S) = \{\mathrm{T}\}$.
- If $S = \{100, 00111, 0010, 00000\}$, then $f_5(S) = \{1,3\}$.

Function composition

Definition 4.3.1.

If $f : A \to B$ and $g : B \to C$, the *composition* of g and f (in this order) is defined as:

$$(g \circ f)(x) ::= g(f(x))$$

(read: *g after f*) at every $x \in A$ such that f is defined on x and g is defined on $f(x)$.

$$\begin{tikzcd} A \arrow[rr, "g \circ f"] \arrow[dr, "f"'] & & C \\ & B \arrow[ur, "g"'] & \end{tikzcd}$$

Order matters:

- Wearing first your socks, then your shoes is not the same as wearing first your shoes, then your socks.
- If $A = B = C = \mathbb{R}$, $f(x) = x^2 + 1$, and $g(x) = 3x + 2$, then $g(f(x)) = 3(x^2 + 1) + 2 = 3x^2 + 5$, but $f(g(x)) = (3x + 2)^2 + 1 = 9x^2 + 12x + 5$.

Next section

Binary relations

Definition 4.4.1.

A *binary relation* with *domain* A, *codomain* B, and *graph* R is a subset of the Cartesian product $A \times B$.

- A relation is "a function without the unique image requirement".
- If the domain and codomain are given, we may identify the relation with its graph.
- $R : A \to B$ means: "R is a relation from A to B".
- If $a \in A$ and $b \in B$, then $a \, R \, b$ means: "a is in relation R with b".

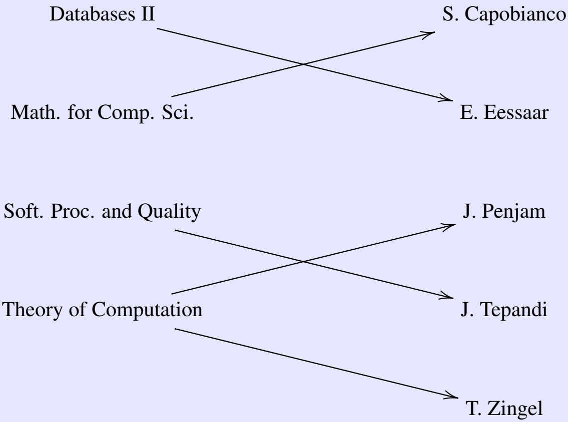
Relation diagrams

A binary relation $R : A \to B$ can be represented as two columns linked by arrows, where:

- The first column contains a list of elements of A.
- The second column contains a list of elements of B.
- There is an arrow from $a \in A$ to $b \in B$ if and only if aRb.

Example: What is taught by whom?

From the 2018-2019 course list:



Arrow properties

Let $R : A \to B$ be a binary relation. We say that:

R has the ... property if each object in its ... has ... arrows ... it

in the relation diagram, according to the following table:

$[\leq n \text{ in}]$	codomain	at most n	coming into
$[\geq m \text{ in}]$	codomain	at least m	coming into
$[= k \text{ in}]$	codomain	exactly k	coming into
$[\leq n \text{ out}]$	domain	at most n	going out of
$[\geq m \text{ out}]$	domain	at least m	going out of
$[= k \text{ out}]$	domain	exactly k	going out of

Arrow properties

Let $R : A \to B$ be a binary relation. We say that:

R has the ... property if each object in its ... has ... arrows ... it

in the relation diagram, according to the following table:

$[\leq n \text{ in}]$	codomain	at most n	coming into
$[\geq m \text{ in}]$	codomain	at least m	coming into
$[= k \text{ in}]$	codomain	exactly k	coming into
$[\leq n \text{ out}]$	domain	at most n	going out of
$[\geq m \text{ out}]$	domain	at least m	going out of
$[= k \text{ out}]$	domain	exactly k	going out of

Note that this depend on how domain and codomain are chosen:

- $f(x) = 1/x^2$ has both $[= 1 \text{ in}]$ and $[= 1 \text{ out}]$ if the choice for both its domain and codomain is $\mathbb{R}^+$...
- ...but if it is $\mathbb{R}$ instead, then $f(x)$ has neither $[\leq 1 \text{ in}]$, nor $[\geq 1 \text{ in}]$, nor $[\geq 1 \text{ out}]$.

Relation properties

Definition 4.4.2.

Let $R : A \to B$ be a binary relation. We say that:

R is ...	if it has ...
a function	the [≤ 1 out] property
total	the [≥ 1 out] property
injective	the [≤ 1 in] property
surjective	the [≥ 1 in] property
bijective	both the [$= 1$ out] and the [$= 1$ in] property

Important:

- Bijective relations are total.
- If $A = \emptyset$ then R is a total function:
  Otherwise, there would exist $x \in \emptyset$ with either no outgoing arrow, or more than one outgoing arrow...
- If $B = \emptyset$ then R is both injective and surjective:
  Otherwise, there would exist $y \in \emptyset$ with either more than one incoming arrow, or no incoming arrow...

Relational images

Let R be a relation with domain A and codomain B.

Definition 4.4.4.

The *image* of $S \subseteq A$ under R is:

$$R(S) ::= \{y \in B \mid \exists x \in S \,.\, xRy\}$$

For example, let $A = B = \mathbb{N}$ and let aRb if and only if b is a prime factor of a. Then:

- $R(\{2,4,6,8,10,17,26\}) = \{2,3,5,13,17\}$.
- $R(\{0\}) = \text{Primes}$.
  Remember that m is a factor of n if and only if there exists an integer k such that $km = n$; for $n = 0$ we can choose $k = 0$.

Relation composition

Composition of relations is defined similarly to composition of functions:

Definition

If $R : A \to B$ and $S : B \to C$, the *composition* of S and R (in this order) is the relation $S \circ R : A \to C$ (read: *S after R*) defined as:

$$a\,(S \circ R)\,c \text{ iff } \exists b \in B\,.\,a\,R\,b \text{ and } b\,S\,c$$

Again, order matters:

- The mother of the father is not the father of the mother.

Inverse relations and inverse images

Let $R : A \to B$ be a binary relation.

Definitions 4.4.5 and 4.4.6.

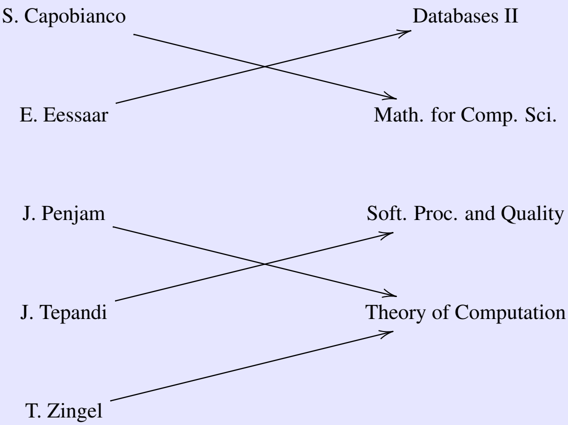
The *inverse* of R is the binary relation $R^{-1} : B \to A$ defined by:

$$yR^{-1}x \text{ iff } xRy$$

The *inverse image* of $T \subseteq B$ according to R is then its image under the inverse relation:

$$R^{-1}(T) = \{x \in A \mid \exists y \in T\,.\,xRy\}$$

Example: Who teaches what?



The empty relation

Let $E : A \to B$ be the *empty relation* such that $\text{not}((x,y) \in E)$ for any $x \in A$ and $y \in B$.

- E is *a function:*
  E clearly has the $[=0 \text{ in}]$ property, so it has the $[\leq 1 \text{ in}]$ property too.
- E is *injective:*
  E clearly has the $[=0 \text{ out}]$ property, so it has the $[\leq 1 \text{ out}]$ property too.
- E is *total if and only if $A = \emptyset$:*
  If A is nonempty then E doesn't have the $[\geq 1 \text{ out}]$ property.
  If E wasn't total with $A = \emptyset$, there would exist $x \in \emptyset$ such that $\text{not}((x,y) \in E)$ for any $y \in B$; but there is no $x \in \emptyset$.
- E is *surjective if and only if $B = \emptyset$:*
  If B is nonempty then E doesn't have the $[\geq 1 \text{ in}]$ property.
  If E wasn't surjective with $B = \emptyset$, there would exist $y \in \emptyset$ such that $\text{not}((x,y) \in E)$ for any $x \in A$; but there is no $y \in \emptyset$.

Next section

The cardinality of a finite set

Definition 4.5.1.

If A is a finite set, the *cardinality* of A is the number $|A|$ of its elements.

Examples:

- $|\{\text{Sephiroth, Bowser, Diablo}\}| = 3$.
- $|\{p \in \text{Primes} \mid p \leq 20\}| = 8$.
- $|\emptyset| = 0$.

Functions between finite sets

Let A and B be finite sets and R a relation from A to B.
Suppose the relation diagram of R has n arrows.

1. If R is a function, then it has the $[\leq 1 \text{ out}]$ property, so $|A| \geq n$.
2. If R is surjective, then it has the $[\geq 1 \text{ in}]$ property, so $n \geq |B|$.

We conclude that:

If A and B are finite sets and $f : A \to B$ is a surjective function, then $|A| \geq |B|$.

Surjectivity, injectivity, bijectivity

Definition 4.5.2.

Given any two (finite or infinite) sets A and B, we write:

- $A \,\mathrm{surj}\, B$ iff there exists a *surjective function* from A to B;
- $A \,\mathrm{inj}\, B$ iff there exists a *total injective relation* from A to B;
- $A \,\mathrm{bij}\, B$ iff there exists a bijection from A to B.

Read: *A surject B*, *A inject B*, *A biject B*.

Surjectivity, injectivity, bijectivity

Definition 4.5.2.

Given any two (finite or infinite) sets A and B, we write:

- $A \,\mathrm{surj}\, B$ iff there exists a *surjective function* from A to B;
- $A \,\mathrm{inj}\, B$ iff there exists a *total injective relation* from A to B;
- $A \,\mathrm{bij}\, B$ iff there exists a bijection from A to B.

Read: *A surject B, A inject B, A biject B.*

Examples:

- If A is the set of video games and $B = \{\text{Bowser, Diablo, Sephiroth}\}$, then $A \,\mathrm{surj}\, B$:

v	Super Mario	Diablo II	Final Fantasy VII	Tetris	Diablo III	...
$f(v)$	Bowser	Diablo	Sephiroth	*undefined*	Diablo	...

  where $f(v)$ is the Big Bad Evil Guy of video game v, is a surjective function (but neither total nor injective).
- If $A \subseteq B$, then $A \,\mathrm{inj}\, B$:
  $f(x) = x$ for every $x \in A$ is injective and total (and also a function).
- If $A = \{p \in \text{Primes} \mid p \leq 20\}$ and $B = \{n \in \mathbb{N} \mid 1 \leq n \leq 8\}$, then $A \,\mathrm{bij}\, B$:

p	2	3	5	7	11	13	17	19
$f(p)$	1	2	3	4	5	6	7	8

Surjectivity, injectivity, bijectivity

Definition 4.5.2.

Given any two (finite or infinite) sets A and B, we write:

- $A \,\mathrm{surj}\, B$ iff there exists a *surjective function* from A to B;
- $A \,\mathrm{inj}\, B$ iff there exists a *total injective relation* from A to B;
- $A \,\mathrm{bij}\, B$ iff there exists a bijection from A to B.

Read: *A surject B, A inject B, A biject B.*

Important note:

- If $B = \emptyset$ then $A \,\mathrm{surj}\, B$ whatever A is:
  In this case, the empty relation is a surjective function.
- If $A = \emptyset$ then $A \,\mathrm{inj}\, B$ whatever B is:
  In this case, the empty relation is total and injective.

Finite sets and arrow properties

Lemma 4.5.3

Let A and B be *finite* sets. Then:

1. If $A \operatorname{surj} B$, then $|A| \geq |B|$.
2. If $A \operatorname{inj} B$, then $|A| \leq |B|$.
3. If $A \operatorname{bij} B$, then $|A| = |B|$.

Proof:

1. We proved this on the second slide of the section.
2. If $R : A \to B$ is injective and total, then R^{-1} is a surjective function, so $|B| \geq |A|$. *Bonus:* prove that $A \operatorname{inj} B$ iff $B \operatorname{surj} A$.
3. If $f : A \to B$ is a bijection, then it is a total function which is both injective and surjective.

Function and arrow properties: Summary

Theorem 4.5.4

Let A and B be finite sets. Then:

1. $|A| \geq |B|$ iff there exists a surjective function from A to B.
2. $|A| \leq |B|$ iff there exists an injective total relation from A to B.
3. $|A| = |B|$ iff there exists a bijection from A to B.

How Many Subsets of a Finite Set?

Theorem

A finite set with n elements has 2^n subsets.

Proof:

1. The thesis is true for the empty set, so let $n \geq 1$.
2. Let $a_1, \ldots, a_n$ be the elements of the set A.
3. Let B be the set of *binary strings* of length n.
4. Define $f : \mathrm{pow}(A) \to B$ so that the ith bit of $f(S)$ is 1 if and only if $a_i \in S$.
5. Then f is a bijection, because subsets with the same image have the same elements, and each string describes a subset.
   Alternatively: f is a bijection, because it is a total function whose inverse:

   $$g(s) = \{a_i \in A \mid b_i = 1\} \text{ where } s = b_1 b_2 \ldots b_n$$

   is also a total function.
6. Since there are 2^n binary strings of length n, the thesis follows.