CSCE 222
Discrete Structures for Computing

Sets and Functions

Dr. Hyunyoung Lee

Based on slides by Andreas Klappenecker

Sets

Sets are the most fundamental discrete structure on which all other discrete structures are built.

We use naive set theory, rather than axiomatic set theory, since this approach is more intuitive. The drawback is that one can construct paradoxes using the naive set theory approach unless one is careful. The set theoretic complications have little bearing on the subsequent material, though, since we are mostly concerned with finite and countable sets.

Sets

A set is an unordered collection of objects, called elements, without duplication. We write $a \in A$ to denote that a is an element in A.

We can describe sets by listing their elements.

$A = \{1,2,3,4\}$ a set of four elements

$B = \{1,2,3,...,99\}$ a set of all natural numbers < 100

Much Ado about Nothing

We denote the empty set $\{\}$ by $\emptyset$.

A set can be an element of another set.

$\{\emptyset\}$ is the set containing one element, namely $\emptyset$.

Note that $\emptyset$ and $\{\emptyset\}$ are different sets, since they contain different elements (the first one none, and the second one contains the element $\emptyset$).

The set $\{\emptyset,\{\emptyset\}\}$ contains two elements.

Common Sets

N = {0,1,2,3,4,...} natural numbers (according to our book)

[Note that in 50% of the literature N contains 0 and in the other 50% it does not. This will not change, since each view has its merits.]

Z = {..., -2,-1,0,1,2,...} set of integers

R, set of real numbers

C, set of complex numbers

Set Builder Notation

The set builder notation describes all elements as a subset of a set having a certain property.

$Q = \{ p/q \in \boldsymbol{R} \mid p \in \boldsymbol{Z}, q \in \boldsymbol{Z}, \text{ and } q \neq 0 \}$

$[a,b] = \{ x \in \boldsymbol{R} \mid a <= x <= b \}$

$[a,b) = \{ x \in \boldsymbol{R} \mid a <= x < b \}$

$(a,b] = \{ x \in \boldsymbol{R} \mid a < x <= b \}$

$(a,b) = \{ x \in \boldsymbol{R} \mid a < x < b \}$

Equality of Sets

Two sets A and B are called equal if and only if they have the same elements.

$A = B$ *if and only if* $\forall x(x \in A \leftrightarrow x \in B)$

[To prove $A{=}B$, it is sufficient to show that both $\forall x(x \in A \rightarrow x \in B)$ and $\forall x(x \in B \rightarrow x \in A)$ hold. Why?]

Subset

A set A is a subset of B, written $A \subseteq B$, if and only if every element of A is an element of B.

Thus, $A \subseteq B$ *if and only if* $\forall x(x \in A \rightarrow x \in B)$

Example

Theorem: For every set S, we have $\varnothing \subseteq S$.

Proof: We have to show that

$$\forall x(x \in \varnothing \rightarrow x \in S)$$

is true. Since the empty set does not contain any elements, the premise is always false; hence, the implication $x \in \varnothing \rightarrow x \in S$ is always true. Therefore, $\forall x(x \in \varnothing \rightarrow x \in S)$ is true; hence, the claim follows.

Cardinality of a Set

Let S be a set with a finite number of elements. We say that the set has cardinality n if and only if S contains n elements. We write $|S|$ to denote the cardinality of the set.

For example, $|\varnothing| = 0$.

Power Sets

Given a set S, the power set $P(S)$ of S is the set of all subsets of S.

Example: $P(\{1\}) = \{\varnothing, \{1\}\}$

$P(\{1,2\}) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$

$P(\varnothing) = \{\varnothing\}$ since every set contains the empty set as a subset, even the empty set.

$P(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$.

Quiz

Determine the set $P(\ \{\ \varnothing,\ \{\varnothing\}\}\ )$.

Answer: $\left\{\ \varnothing,\ \{\ \varnothing\},\ \{\{\varnothing\}\},\ \{\ \varnothing,\ \{\varnothing\}\}\ \right\}$

Cartesian Products

Let A and B be sets. The Cartesian product of A and B, denote A x B, is the set of all pairs (a,b) with $a \in A$ and $b \in B$.

$$A \times B = \{ (a,b) \mid a \in A \wedge b \in B \}$$

Quiz

Let $A = \{1,2,3\}$.

What elements does the set $A \times \varnothing$ contain?

Answer: None

Set Operations

Union and Intersection

Let A and B be sets.

The union of A and B, denoted $A \cup B$, is the set that contains those elements that are in A or in B, or in both.

The intersection of A and B, denoted $A \cap B$, is the set that contains those elements that are in both A and B.

Set Difference

Let A and B be sets. The difference between A and B, denoted A-B or $A \backslash B$, is the set

$$A-B = \{ x \in A \mid x \notin B \}.$$

Universe and Complement

A set which has all the elements in the universe of discourse is called a universal set.

Let A be a set. The complement of A, denoted A^c or $\overline{A}$, is given by U - A.

Set Identities

Let U be the universal set.

Identity laws:

$$A \cap U = A$$

$$A \cup \varnothing = A$$

Domination laws:

$$A \cup U = U$$

$$A \cap \varnothing = \varnothing$$

Idempotent laws:

$$A \cup A = A$$

$$A \cap A = A$$

Also:
Commutative Laws

Associative Laws

Distributive Laws

De Morgan Laws

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

$Proof:$

$$\begin{aligned}
\overline{A \cap B} &= \{x \mid x \notin A \cap B\} \text{ by definition of complement} \\
&= \{x \mid \neg(x \in A \cap B)\} \\
&= \{x \mid \neg(x \in A \wedge x \in B)\} \text{ by definition of intersection} \\
&= \{x \mid \neg(x \in A) \vee \neg(x \in B)\} \text{ de Morgan's law from logic} \\
&= \{x \mid (x \notin A) \vee (x \notin B)\} \text{ by definition of } \notin \\
&= \{x \mid x \in \overline{A} \vee x \in \overline{B}\} \text{ by definition of complement} \\
&= \{x \mid x \in \overline{A} \cup \overline{B}\} \text{ by definition of union} \\
&= \overline{A} \cup \overline{B}
\end{aligned}$$

Generalized Unions and Intersections

$$\bigcup_{k=1}^{n} A_k = A_1 \cup A_2 \cup \cdots \cup A_n$$

$$\bigcap_{k=1}^{n} A_k = A_1 \cap A_2 \cap \cdots \cap A_n$$

More Unions and Intersections

$$\bigcup_{k=1}^{\infty} A_k = A_1 \cup A_2 \cup A_3 \cup \cdots$$

Example:

If $A_k = \{1, 2, \ldots, k\}$ then

$$\bigcup_{k=1}^{\infty} A_k = A_1 \cup A_2 \cup A_3 \cup \cdots = \{1, 2, 3, \cdots\}$$

Functions

Functions

Let A and B be nonempty sets.

A *function* f from A to B is an assignment of precisely one element of B to each element of A.

We write f: A -> B for a function from A to B.

Terminology

Let f: A -> B be a function.

We call

- A the domain of f and

- B the codomain of f.

The range of f is the set

$f(A) = \{ f(a) \mid a \text{ in } A \}$

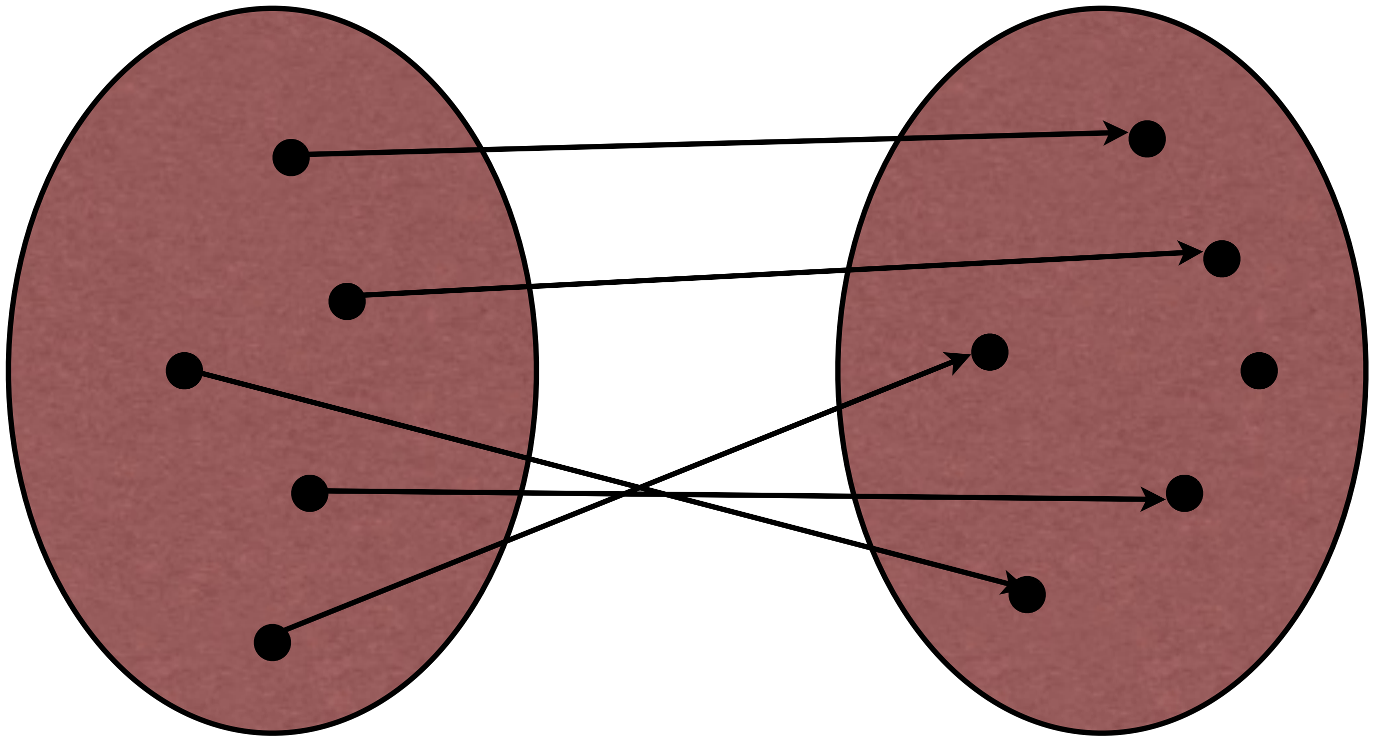
Injective Functions

A function f: A -> B is called injective or one-to-one if and only if $f(a)=f(b)$ implies that $a=b$.

In other words, f is injective if and only if different arguments have different values. [Contrapositive!]

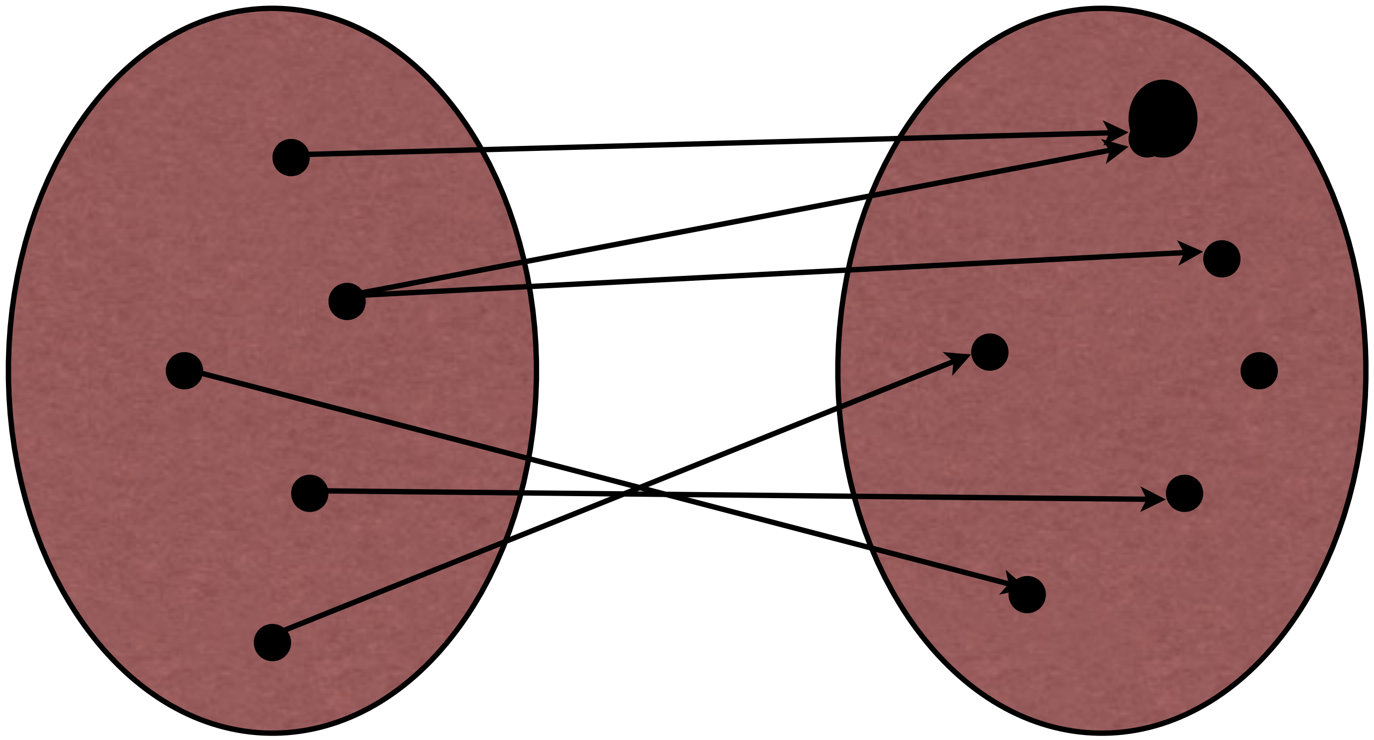
Injective Functions (cont.)

A function f is *injective* if any distinct pair of elements in the domain get mapped to distinct elements in the codomain.



Not Injective Function

A function f *fails* to be injective if there exist two distinct arguments that get mapped to the same value.



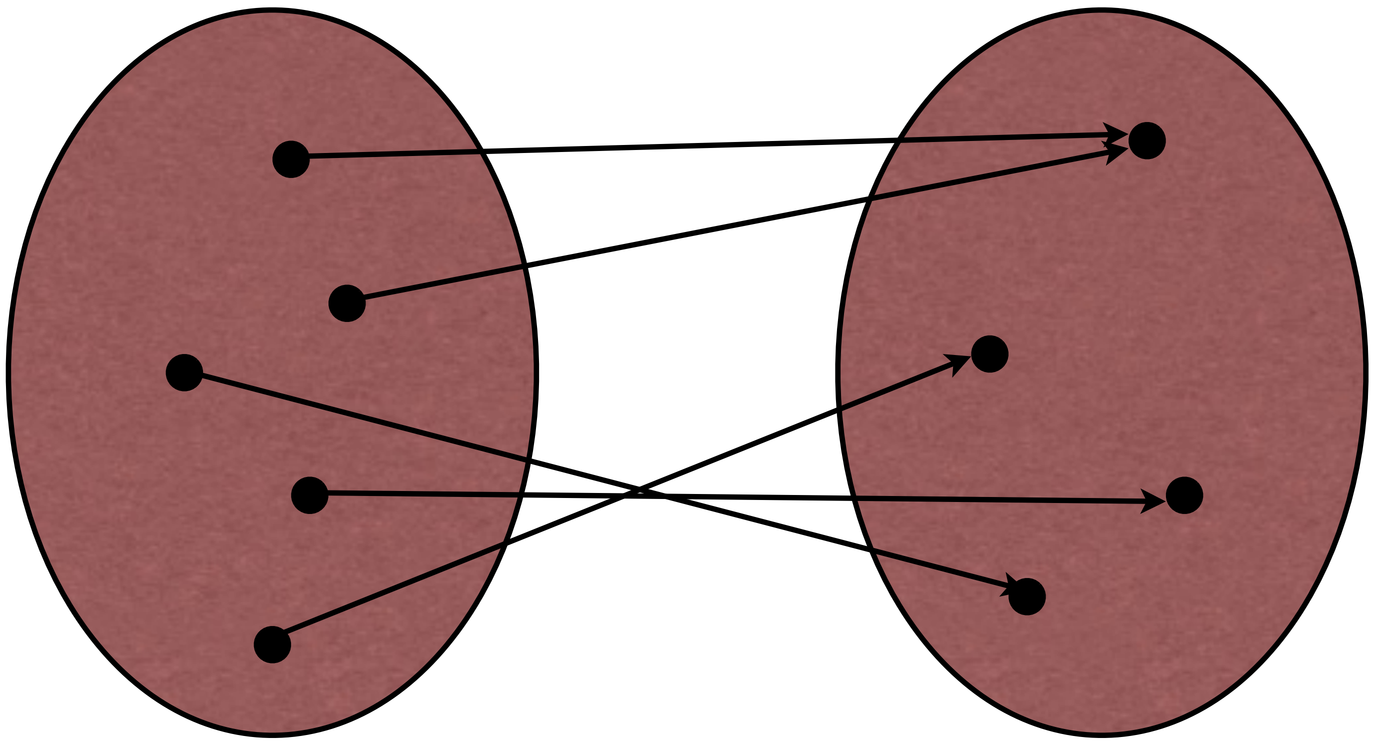
Surjective Functions

A function f: A -> B is called surjective or onto if and only if $f(A)=B$.

In other words, f is surjective if and only if for each element b in the codomain B there exists an element a in A such that $f(a)=b$.

Surjective Functions (cont.)

A function *f* is surjective if any element in the codomain is in the range of *f*.



Examples

The function $f : N \text{->} N$ with $f(x) = x^2$ is not surjective, since 3 is not a perfect square. It is injective, since any two distinct arguments have a distinct value.

The function $f : Z \text{->} Z$ with $f(x) = x^2$ is not injective, since we have $f(1) = f(-1)$. Thus, to answer questions about injectivity and surjectivity you need to know the domain and codomain!!!

Bijections

A function is called a bijection or one-to-one correspondence if and only if it is injective and surjective.

Composition of Functions

Let $g: A \rightarrow B$ and $f: B \rightarrow C$ be functions.

The composition of the functions f and g, denoted $f \circ g$, is a function from A to C given by

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

for all x in A.

Floor and Ceiling Functions

Floor Function

The floor function $\lfloor\ \rfloor$: ***R* –> *Z*** assigns to a real number *x* the largest integer <= *x*.

$\lfloor 3.2 \rfloor = 3$

$\lfloor -3.2 \rfloor = -4$

$\lfloor 3.99 \rfloor = 3$

Ceiling Function

The ceiling function $\lceil \rceil$: $\boldsymbol{R} \rightarrow \boldsymbol{Z}$ assigns to a real number x the smallest integer >= x.

$\lceil 3.2 \rceil = 4$

$\lceil -3.2 \rceil = -3$

$\lceil 0.5 \rceil = 1$

Remark

The floor and ceiling functions are ubiquitous in computer science. You will have to become familiar with these functions. Moreover, you need to know how to prove facts involving floor and ceiling functions.

Basic Facts (1)

We have $\lfloor x \rfloor = n$ if and only if $n <= x < n+1$.

Theorem: Let m be an integer, x a real number such that $\lfloor x \rfloor = n$. Then $\lfloor x+m \rfloor = n+m$.

Proof: We have $\lfloor x \rfloor = n$ if and only if $n <= x < n+1$. Adding m yields $n+m <= x+m < n+m+1$. This shows that $\lfloor x+m \rfloor = n+m$.

Basic Facts (2)

We have $\lfloor x \rfloor = n$ if and only if $n <= x < n+1$.

We have $\lceil x \rceil = n$ if and only if $n-1 < x <= n$.

We have $\lfloor x \rfloor = n$ if and only if $x-1 < n <= x$.

We have $\lceil x \rceil = n$ if and only if $x <= n < x+1$.

Example 1

Theorem: For each real number x, we have

$$\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x+1/2 \rfloor.$$

Proof: Express the number x in the form $x=n+d$, where n is an integer and d is a real number such that $0<=d<1$.

Case 1 Suppose that d is in the range $0<=d<1/2$. Then $2x=2n+2d$, and $0<=2d<1$. Thus, $\lfloor 2x \rfloor = 2n$.

We have $\lfloor x \rfloor = n$, and $\lfloor x+1/2 \rfloor = \lfloor n+d+1/2 \rfloor = n$, since $0<=d+1/2<1$.

Therefore, $\lfloor 2x \rfloor = 2n = n+n = \lfloor x \rfloor + \lfloor x+1/2 \rfloor$.

Example 1 (cont.)

Recall that we expressed x in the form $x=n+d$, where n is an integer and d is a real number such that $0<=d<1$.

Case 2 Suppose that d is in the range $1/2<=d<1$. Then $2x=2n+2d$, and $1<=2d<2$. Thus, $\lfloor 2x \rfloor = 2n+1$.

We have $\lfloor x \rfloor = n$, and $\lfloor x+1/2 \rfloor = \lfloor n+d+1/2 \rfloor = n+1$, since $1<=d+1/2<2$.

Therefore, $\lfloor 2x \rfloor = 2n+1 = n+n+1 = \lfloor x \rfloor + \lfloor x+1/2 \rfloor$.

Since Case 1 and Case 2 exhaust the possibilities for d, we can conclude that the theorem holds.

Example 2

Theorem: For all real numbers x, we have $\lfloor -x \rfloor = -\lceil x \rceil$

Proof: Let $n=\lfloor -x \rfloor$. Then $n <= -x < n+1$.

Multiplying by -1 yields $-n >= x > -n-1$.

Therefore, $-n = \lceil x \rceil$ or $n = -\lceil x \rceil$.

Hence we can conclude that $\lfloor -x \rfloor = n = -\lceil x \rceil$ holds.

Example 3

Prove or disprove:

$$\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor = \lfloor \sqrt{x} \rfloor$$

Example 3 (cont.)

Let $m = \lfloor \sqrt{\lfloor x \rfloor} \rfloor$

Hence, $m \leq \sqrt{\lfloor x \rfloor} < m + 1$

Thus, $m^2 \leq \lfloor x \rfloor < (m+1)^2$

It follows that $m^2 \leq x < (m+1)^2$

Therefore, $m \leq \sqrt{x} < m + 1$

Thus, we can conclude that $m = \lfloor \sqrt{x} \rfloor$

This proves our claim.

Example 4

For an integer n, we have $n = \lceil n/2 \rceil + \lfloor n/2 \rfloor$

Indeed, this is clear if n is even.

If n is odd, say $n=2k+1$ for some integer k, then we have

$$n = 2k+1 = (k + 1) + k = \lceil k+1/2 \rceil + \lfloor k+1/2 \rfloor$$

$$= \lceil (2k+1)/2 \rceil + \lfloor (2k+1)/2 \rfloor = \lceil n/2 \rceil + \lfloor n/2 \rfloor.$$

Thus, the claim holds for all integers n.